Sun Java System Access Manager 7.1 版本說明

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

文件號碼：820–0366
2007 年 7 月

070806@18135

目錄

Sun Java System Access Manager 7.1 版本說明

2007 年 7 月

文件號碼 820-0366

此「Sun Java™ System Access Manager 7.1 版本說明」包含 Sun Java Enterprise System (Java ES) 發行版本可用的重要資訊，包括 Access Manager 的新增功能與已知問題及其解決方法 (如有提供)。安裝和使用此發行版本之前，請先閱讀本文件。

若要檢視 Java ES 產品文件，包括 Access Manager 文件集，請參閱 `http://docs.sun.com/prod/entsys.05q4` 與 `http://docs.sun.com/prod/entsys.05q4?l=zh_TW`。

安裝與設定軟體之前請瀏覽此網站，之後請定期檢視最新的文件。

本版本說明包含以下章節：

修訂歷程記錄

下表顯示「Access Manager 7.1 版本說明」的修訂歷程記錄。

表 1 修訂歷程記錄

日期	變更說明
2006 年 7 月	後期測試版。
2007 年 3 月	Java Enterprise System 5 版
2007 年 5 月	加入了新的已知問題 6555040、6550261、6554379、6554372、6480354
2007 年 6 月	加入了新的已知問題 6562076、6490150
2007 年 7 月	加入了新的已知問題 6485695

關於 Sun Java System Access Manager 7.1

Sun Java System Access Manager 是 Sun 識別管理基礎架構的一部分，可讓組織管理企業內部及整個企業對企業 (B2B) 價值鏈間對 Web 應用程式和其他資源的安全存取。

Access Manager 提供以下主要功能：

- 使用基於角色及基於規則的存取控制之集中式認證與授權服務
- 以單次登入 (Single Sign-on, SSO) 方式存取組織基於 Web 的應用程式
- 透過 Liberty Alliance Project 與安全宣示標記語言 (SAML) 支援聯合識別
- 記錄 Access Manager 元件中管理員與使用者活動等重要資訊，以供後續分析、報告及稽核之用。

此版本的新增功能

此版本的新增功能如下：

- 第 7 頁的 「Java ES Monitoring Framework 整合」
- 第 7 頁的 「Web 服務安全性」
- 第 7 頁的 「單一 Access Manager WAR 檔案部署」
- 第 7 頁的 「核心服務的增強功能」
- 第 9 頁的 「停用的通知及通告」

Java ES Monitoring Framework 整合

Access Manager 7.1 透過 Java Management Extension (JMX) 整合了 Java Enterprise System Monitoring Framework。JMX 技術提供許多工具用來建立分散式、網路型、模組式及動態的解決方案，以便管理及監視裝置、應用程式及服務驅動的網路。JMX 技術的一般用法包括：查看及變更應用程式的配置、累積關於應用程式行爲、狀態變更通知與錯誤行爲的統計資料。資料會傳到集中的監視主控台。

Access Manager 7.1 使用「Java ES Monitoring Framework」來擷取統計資料及服務相關資料，例如：

- 嘗試、成功以及失敗的認證次數
- 策略快取統計資料
- 策略評估作業事件時間

Web 服務安全性

Access Manager 7.1 以下列方式將認證功能延伸到 Web 服務：

- 將記號插入到外寄的訊息
- 評估內送的訊息有無安全性記號
- 允許透過點按方式 (Point-and-Click) 選取新應用程式的認證提供者

單一 Access Manager WAR 檔案部署

Access Manager 包括一個單一的 WAR 檔案供您用來一致性地將 Access Manager 服務部署到任何受支援平台上的任何受支援容器。Access Manager WAR 檔案與 Java Enterprise System 安裝程式並存，後者可部署多個 JAR、XML、JSP、HTML、GIF 及各種特性檔案。

核心服務的增強功能

支援的 Web 容器

- Sun Java System Web Server 7.0
- Sun Java System Application Server 8.2
- BEA WL 8.1 SP4
- IBM WebSphere 5.1.1.6

Monitoring Framework 整合

Access Manager 可以使用「JES Monitoring Framework」來監視下列項目：

1. 認證

- 嘗試的認證次數
- 嘗試的遠端認證次數 (選用)
- 成功的認證次數
- 失敗的認證次數
- 成功的登出作業次數
- 失敗的登出作業次數
- 可能時，每個模組的作業事件時間 (執行中及等待中狀態)

2. 階段作業
   - 階段作業表格的大小 (亦即最大階段作業數目)
   - 使用中階段作業數目 (增量計數器)
3. 設定檔服務
   - 快取大小上限
   - 作業的作業事件時間 (執行中及等待中)
4. 策略
   - 內送和外傳請求的策略評估
   - 主體外掛程式之 LDAP 伺服器的策略連線池統計資料

認證模組

- 要進行負載平衡佈署，「分散式認證」服務不一定要在同一台伺服器上
- 要進行負載平衡佈署，認證服務與伺服器不一定要在同一台伺服器上
- 認證服務、策略代理程式及策略服務間支援複合建議。包括 `AuthenticateToRealm` 條件、AuthenticateToService 條件，以及所有條件的範圍限定。
- 建議組織 (範圍限定的「認證」條件)
- 認證配置 / 認證鏈 (`AuthServiceCondition`)
- 如果執行認證鏈接，則現在可以禁止以模組爲基礎的認證
- 「分散式認證」服務支援「憑證」認證模組
- 爲「分散式認證 UI」增加了 `CertAuth`，使它成爲全功能的憑證擷取器
- 新的「資料存放區」認證模組是拆封即用的模組，它會對照指定範圍的已配置資料存放區來進行認證
- 現在帳號封鎖配置在多個 AM 伺服器實例間是永久性的
- 處理後 SPI 類別的鏈接

策略模組

- 新增策略條件 `AuthenticateToServiceCondition`，用以強制在特定認證服務鏈接中認證使用者。
- 新增策略條件 `AuthenticateToRealmCondition`，用以強制在特定範圍中認證使用者。
- 新增策略條件 `LDAPFilterCondition`，用以強制使用者比對特定的 ldap 篩選器。

- 支援單層萬元字元比較，以便保護目錄的內容，但不保護子目錄。
- 如果已在全域策略配置中啓用組織別名參照，可在沒有來自父系範圍的明確參照策略的情況下，於子範圍中建立策略。
- `AuthLevelCondition` 除了指定認證層級以外，還可以指定範圍名稱。
- `AuthSchemeCondition` 除了指定認證模組名稱以外，還可以指定範圍名稱。

服務管理模組

- 支援將服務管理/策略配置存入 Active Directory

Access Manager SDK

- 支援用於向預設身份識別儲存庫架構資料庫認證使用者的 API

Web 服務支援

- Liberty ID-WSF SOAP 提供者：認證提供者，它會封裝 Access Manager 實作的 Liberty ID-WSF SOAP 連結它由用戶端及服務提供者組成。
- HTTP 層的 SSO 提供者：HttpServlet 層認證提供者，它會封裝伺服器端以 Access Manager 爲基礎的 SSO

安裝模組

- 將 Access Manager 重新封裝爲 J2EE 應用程式會產生單一 WAR 檔案，然後便可在 Web 上部署
- 支援 64 位元的 SJS Web Server 7.0 - 以支援 64 位元的 JVM

委派模組

- 支援將委派權限分組

升級

- 支援從下列版本升級到 Access Manager 7.1：Access Manager 7.0 2005Q4、Access Manager 6.3 2005Q1 及 Identity Server 6.2 2004Q2。

記錄

- 支援在記錄模組中委派 - 控制哪些身份識別有權寫入或讀取記錄檔。
- 支援以 JCE 爲基礎的 `SecureLogHelper` - 允許使用 JCE (而不只是 JSS) 當作安全記錄實作的安全性提供者

停用的通知及通告

Sun Java(TM) System Access Manager 7.1 身份識別管理 API 及 XML 範本可讓系統管理員在 Sun Java System Directory Server 中建立、刪除及管理身份識別項目。Access Manager 也提供用於身份識別管理的 API。開發者使用在 `com.iplanet.am.sdk` 套裝軟體中定義的

公用介面及類別將管理功能整合至 Access Manager 要管理的外部應用程式或服務。Access Manager API 提供了方法來建立或刪除與身份識別相關的物件，以及從 Directory Server 取得、修改、增加或刪除這些物件屬性的方法。

Access Manager `com.iplanet.am.sdk` 套裝軟體 (一般稱爲 AMSDK) 將不會包括在未來的 Access Manager 發行版本中。這包括所有相關的 API 及 XML 範本。現在沒有遷移選項可用，預期未來也不會有遷移選項。Sun Java System Identity Manager 提供的使用者佈建解決方案是您現在就可以開始使用的相容替代品。如需 Sun Java System Identity Manager 的詳細資訊，請參閱 `http://www.sun.com/software/products/identity_mgr/index.xml`。

硬體與軟體需求

下表顯示此發行版本的硬體與軟體需求。

表 2 硬體與軟體需求

元件	需求
作業系統 (OS)	■ 基於 SPARC、x86 及 x64 之系統上的 Solaris™10，包括對完整根本機區域和稀疏根區域的支援。 ■ 基於 SPARC 及 x86 之系統上的 Solaris 9 ■ Red Hat™ Enterprise Linux 3 及 4，所有更新 Advanced Server (32 及 64 位元的版本) 以及 Enterprise Server (32 及 64 位元的版本) ■ Windows x86 上的 Windows 2000 Advanced Server、Data Center Server 版本 SP4 基於 x86 和 x64 之系統上的 Windows 2003 Standard (32 及 64 位元版本)、Enterprise (32 及 64 位元版本)、Data Center Server (32 位元版本) 基於 x86 之系統上的 Windows XP Professional SP2 PA-RISC 2.0 上的 64 位元 HP-UX 11i v1 (uname 傳回 11.11) 如需最新的支援作業系統清單，參閱「Sun Java Enterprise System 5 Release Notes for UNIX」中的「Platform Requirements and Issues」，或「Sun Java Enterprise System 5 Release Notes for Microsoft Windows」中的「Hardware and Software Platform Information」。
Java 2 Standard Edition (J2SE)	J2SE 平台 6.0、5.0 Update 9 (HP-UX：1.5.0.03) 及 1.4.2 Update 11
Directory Server	Access Manager 資訊樹：Sun Java System Directory Server 6.0 或 Sun Java System Directory Server 5.2 2005Q4 Access Manager 識別儲存庫：Sun Java System Directory Server 5.2 和 6.0 及 Microsoft Active Directory

表 2 硬體與軟體需求 (續)

元件	需求
Web 容器	支援的平台/OS 組合 (用於在 64 位元 JVM 中執行 Web Server 實例) 上的 Sun Java System Web Server 7.0。支援的平台：Solaris 9/SPARC、Solaris 10/SPARC、Solaris 10/AMD64、Red Hat AS 或 ES 3.0/AMD64、Red Hat AS 或 ES 4.0/AMD64
	Sun Java System Application Server Enterprise Edition 8.2
	BEA WebLogic 8.1 SP4
	IBM WebSphere Application Server 5.1.1.6
RAM	基本測試需求：512 MB
	實際部署：1 GB (針對執行緒、Access Manager SDK、HTTP 伺服器及其他內部元件)
磁碟空間	512 MB (針對 Access Manager 與相關應用程式)

若您對這些元件其他版本的支援有疑問，請連絡 Sun Microsystems 技術支援代表。

支援的瀏覽器

下表顯示 Sun Java Enterprise System 5 發行版本支援的瀏覽器。

表 3 支援的瀏覽器

瀏覽器	平台
Firefox 1.0.7	Windows XP
	Windows 2000
	Solaris OS 版本 9 及 10
	Red Hat Linux 3 及 4
	Mac OS X
Microsoft Internet Explorer™ 6.0 SP2	Windows XP
Microsoft Internet Explorer 6.0 SP1	Windows™ 2000

表 3 支援的瀏覽器 (續)

瀏覽器	平台
Mozilla™ 1.7.12	Solaris OS 版本 9 及 10
	Windows XP
	Windows 2000
	Red Hat Linux 3 及 4
	Mac OS X
Netscape™ Communicator 8.0.4	Windows XP
	Windows 2000
Netscape Communicator 7.1	Solaris OS 版本 9 及 10

一般相容性資訊

AMSDK 與 Access Manager 伺服器系統間不相容

下列 Java Enterprise System 發行版本中，AMSDK 和 Access Manager 伺服器的以下組合不相容：

- Java Enterprise System 2004Q2 AMSDK 與 Java Enterprise System 5 Access Manager 伺服器 (此發行版本) 不相容。
- Java Enterprise System 5 AMSDK (此發行版本) 與 Java Enterprise System Access Manger 2004Q2 (以前稱爲 Identity Server) 伺服器不相容。

Access Manager HPUX 版本不支援升級

HPUX 版本中不支援從 Access Manager 7 2005Q4 升級到 Access Manger 7.1 (此發行版本)。

Access Manager 舊有模式

若要將 Access Manager 與下列任一產品共同安裝，則必須選取 Access Manager 舊有模式 (6.x)：

- Sun Java System Portal Server

- Sun Java System Communication Services 伺服器，包括 Messaging Server、Calendar Server、Instant Messaging 或 Delegated Administrator

選取 Access Manager 舊有模式 (6.x) 的方式視您如何執行 Java ES 安裝程式而定：

- 第 14 頁的 「使用狀態檔案的 Java ES 無訊息安裝」
- 第 14 頁的 「圖形化模式中的 [立即配置] 安裝選項」
- 第 14 頁的 「文字模式中的 [立即配置] 安裝選項」
- 第 14 頁的 「[以後配置] 安裝選項」

如需判定 Access Manager 7.1 安裝模式的詳細資訊，請參閱第 15 頁的 「判定 Access Manager 模式」 。

使用狀態檔案的 Java ES 無訊息安裝

Java ES 安裝程式無訊息安裝爲非互動模式，可讓您將 Java ES 元件安裝於具有類似配置的多個主機伺服器上。首先您執行安裝程式產生一個狀態檔案 (未實際安裝任何元件)，然後爲每個計劃要在其上安裝 Access Manager 與其他元件的主機伺服器，編輯一份狀態檔案的副本。

若要在舊有模式 (6.x) 下選取安裝 Access Manager，請在以無訊息模式執行安裝程式之前，先設定狀態檔案中的下列參數 (以及其他參數)：

```
...
AM_REALM = disabled
...
```

如需使用狀態檔案在無訊息模式下執行 Java ES 安裝程式的詳細資訊，請參閱「Sun Java Enterprise System 5 Installation Guide for UNIX」中的第 5 章「Installing in Silent Mode」 。

圖形化模式中的 [立即配置] 安裝選項

若您是在圖形化模式中使用 [立即配置] 選項執行 Java ES 安裝程式，請在 [Access Manager: 管理 (1/6)] 面板中，選取預設值 [舊有 (版本 6.x 樣式)]。

文字模式中的 [立即配置] 安裝選項

若您是在文字模式中使用 [立即配置] 選項執行 Java ES 安裝程式，請針對 **[安裝類型 (範圍/舊有)] [舊有]** 選取預設值 **[舊有]** 。

[以後配置] 安裝選項

若您使用 [以後配置] 選項執行 Java ES 安裝程式，則必須在安裝後執行 `amconfig` 程序檔來配置 Access Manager。若要選取舊有 (6.x) 模式，請設定配置程序輸入檔 (`amsamplesilent`) 中的下列參數：

```
...
AM_REALM=disabled
...
```

如需有關執行 amconfig 程序檔來配置 Access Manager 的詳細資訊，請參閱「Sun Java System Access Manager 7.1 管理指南」。

判定 Access Manager 模式

若要判定執行的 Access Manager 7.1 安裝是在 [範圍] 還是 [舊有] 模式下配置的，請呼叫：

```
http(s)://host:port/amserver/SMSServlet?method=isRealmEnabled
```

結果爲：

- true：[範圍] 模式
- false：[舊有] 模式

Access Manager 策略代理程式

下表顯示策略代理程式與 Access Manager 7.1 模式的相容性。

表 4 策略代理程式與 Access Manager 7.1 模式的相容性

代理程式與版本	相容的模式
Web 與 J2EE 代理程式，版本 2.2	舊有模式與範圍模式
Access Manager 7.1 中不支援 Web 與 J2EE 代理程式，版本 2.1	

已知問題和限制

本節說明 Access Manager 7.1 版本發行時的已知問題和解決方法 (如有提供)。

安裝問題

Java System Enterprise 安裝問題的相關資訊包含於 JES5 版本說明中。請參閱「Sun Java Enterprise System 5 Release Notes for UNIX」中的「Access Manager Installation Issues」一節。

本節包含下列已知問題：

在 WebLogic 上的 Access Manager 單一 WAR 部署需要 JAX-RPC 1.0 JAR 檔案才可與用戶端 SDK 通訊 (6555040)

部署於 Weblogic 8.1 上的單一 WAR 在 JAX-RPC 初始化過程中會出現已知問題。爲了讓 Access Manager 與用戶端 SDK 通訊，需要以 JAX-RPC 1.0 jar 檔案替代 JAX-RPC 1.1 jar 檔案。

解決方法：

有兩種方法可取得 WAR 檔案。一種是透過將 Access Manager 設定爲 [以後配置] 選項執行 Java Enterprise System 5 安裝程式，另一種是透過 Sun 下載網站。

如果您已透過選擇 [以後配置] 選項執行 JES 5 安裝程式產生 WAR 檔：

1. 從 *AccessManager-base*`/SUNWam/web-src/WEB-INF/lib` 移除下列 JAXRPC 1.1 `.jar` 檔案：

- jaxrpc-api.jar
- jaxrpc-spi.jar
- jaxrpc-impl.jar

2. 將下列 .jar 檔案從其各自的位置複製到 *AccessManager-base*/SUNWam/web-src/WEB-INF/lib：
   - /opt/SUNWam/lib/jaxrpc 1.0 中的 jaxrpc-api.jar
   - /opt/SUNWam/lib/jaxrpc 1.0 中的 jaxrpc_ri.jar
   - /opt/SUNWmfwk/lib 中的 commons-logging.jar
3. 移至 *AccessManager-base*/SUNWam/bin/ 並執行下列指令：

   amconfig –s *samplesilent*

   如需使用 amconfig 程序檔配置 Access Manager 的詳細資訊，請參閱「Access Manager Post Installation Guide」中的「Running the Access Manager amconfig Script」。

如果您已透過 Sun 下載網站 (http://www.sun.com/download/index.jsp) 取得 WAR 檔案：

1. 取得 *ZIP_ROOT*/applications/jdk14/amserver.war 檔案，並將其解壓縮至暫存位置，例如 /tmp/am-staging。
2. 從 /tmp/am-staging/WEB-INF/lib 中移除下列 JAXRPC 1.1 .jar 檔案：
   - jaxrpc-api.jar
   - jaxrpc-spi.jar
   - jaxrpc-impl.jar
3. 將位於 *ZIP_ROOT*/applications/jdk14/jarFix 目錄中的下列 JAXRPC 1.0 .jar 檔案與共用記錄 .jar 檔案複製到 /tmp/am-staging/WEB-INF/lib：
   - jaxrpc-api.jar
   - jaxrpc-ri.jar
   - commons-logging.jar
4. 重新建立與部署 Access Manager WAR。如需詳細資訊，請參閱「Access Manager Post Installation Guide」中的「Deploying Access Manager as a Single WAR File」。

JES 5 安裝程式為 Websphere 5.1 產生的單一 WAR 需要其他 .jar 檔案 (6550261)

如果透過選擇 [以後配置] 選項執行 JES 5 安裝程式來產生 Access Manager 單一 WAR，則需要其他 .jar 檔案才能部署 Websphere 5.1。

解決方法：

1. 從 /usr/share/lib 中將 jsr173_api.jar 複製到 *AcessManager-base*/opt/SUNWam/web-src/WEB-INF/lib 目錄。
2. 移至 *AccessManager-base*/SUNWam/bin/ 並執行下列指令：

   amconfig –s *samplesilent*

如需使用 amconfig 程序檔來配置 Access Manager 的詳細資訊，請參閱「Access Manager Post Installation Guide」中的「Running the Access Manager amconfig Script」。

Websphere 的單一 WAR 部署必須變更 server.xml 才能與用戶端 SDK 通訊 (6554379)

爲了讓 Websphere 5.1 的 Access Manager 單一 WAR 部署與用戶端 SDK 成功通訊，您必須變更 `server.xml` 檔案。

解決方法：

若要正確變更 `server.xml` 檔案，請參閱下列步驟：

1. 取得 `amserver.war` 檔案。有兩種方法可取得單一 WAR 檔案：透過選擇 [以後配置] 選項執行 JES 5 安裝程式，或透過 Sun 下載網站。

   備註 – 如果您已透過 JES 5 安裝程式產生 WAR 檔案，請確定您已完成已知問題 #6550261 中所述的步驟。

   ---

2. 將 Access Manager WAR 解壓縮至暫存位置，例如 `/tmp/am-staging`。
3. 將下列共用 `.jar` 檔案從 `/tmp/am-staging/WEB-INF/lib` 複製到共用位置 (例如 `/export/jars`)：

jaxrpc-api.jar	jaxrpc-spi.jar	jaxrpc-impl.jar	saaj-api.jar
saaj-impl.jar	xercesImpl.jar	namespace.jar	xalan.jar
dom.jar	jax-qname.jar	jaxb-api.jar	jaxb-impl.jar
jaxb-libs.jar	jaxb-xjc.jar	jaxr-api.jar	jaxr-impl.jar
xmlsec.jar	swec.jar	acmecrypt.jar	iaik_ssl.jar
iaik_jce_full.jar	mail.jar	activation.jar	relaxngDatatype.jar
xsdlib.jar	mfwk_instrum_tk.jar	FastInfoset.jar	jsr173_api.jar

4. 從暫存位置的 `/tmp/am-staging/WEB-INF/lib` 中移除相同的 `.jar` 檔案。
5. 更新 Websphere 實例的 `server.xml`。如果 `server.xml` 中的 *jvmEntries* 的預設實例位置是 `/opt/WebSphere/AppServer/config/cells/`*node-name*`/nodes/`*node-name*`/servers/server1`，請如下所示進行變更：

   ```
   <classpath>/export/jars/jaxrpc-api.jar:/export/jars/jaxrpc-spi.jar:
       /export/jars/jaxrpc-impl.jar:/export/jars/saaj-api.jar:
       /export/jars/saaj-impl.jar:/export/jars/xercesImpl.jar:
       /export/jars/namespace.jar:/export/jars/xalan.jar:/export/jars/dom.jar:
       /export/jars/jax-qname.jar:/export/jars/jaxb-api.jar:/export/jars/jaxb-impl.jar:
       /export/jars/jaxb-libs.jar:/export/jars/jaxb-xjc.jar:/export/jars/jaxr-api.jar:
       /export/jars/jaxr-impl.jar:/export/jars/xmlsec.jar:/export/jars/swec.jar:
   ```

```
/export/jars/acmecrypt.jar:/export/jars/iaik_ssl.jar:
/export/jars/iaik_jce_full.jar:/export/jars/mail.jar:
/export/jars/activation.jar::/export/jars/relaxngDatatype.jar:
/export/jars/xsdlib.jar:/export/jars/mfwk_instrum_tk.jar:
/export/jars/FastInfoset.jar:/export/jars/jsr173_api.jar</classpath>
```

6. 重新啓動容器。
7. 從 /tmp/am-staging 重新建立與部署 Access Manager WAR。如需詳細資訊，請參閱「Access Manager Deployment Planning Guide」中的「Deploying Access Manager as a Single WAR File」。

分散式認證必須變更才能與 Weblogic 及 Websphere 的 Access Manager 單一 War 配合使用 (6554372)

因爲容器版本是 JDK14，所以分散式認證 WAR 需要其他 jar 檔案才能爲 Weblogic 8.1 與 Websphere 5.1 進行剖析。JDK14 `.jar` 檔案位於 `.zip` 檔案的下列目錄中：

ZIP-ROOT`/applications/jdk14/jarFix`

解決方法：

針對 Weblogic 8.1：

1. 使用設定程序檔來配置分散式認證。請參閱「Access Manager Post Installation Guide」中的「Deploying a Distributed Authentication UI Server」。
2. 將更新的分散式認證 WAR 解壓縮至暫存位置，例如 `/tmp/dist-auth`。
3. 將 `xercesImpl.jar`、`dom.jar` 與 `xalan.jar` 從 *ZIP-ROOT*`/applications/jdk14/jarFix` 複製到 `/tmp/dist_auth/WEB-INF/lib` 目錄。
4. 從暫存位置重新產生分散式認證 WAR 並部署它。如需詳細資訊，請參閱「Access Manager Post Installation Guide」中的「Deploying a Distributed Authentication UI Server WAR File」。

針對 Websphere 5.1：

1. 使用設定程序檔配置分散式認證。請參閱「Access Manager Post Installation Guide」中的「Deploying a Distributed Authentication UI Server」。
2. 將更新的分散式認證 WAR 解壓縮至暫存位置，例如 `/tmp/dist_auth/`。
3. 將 `xercesImpl.jar`、`dom.jar` 與 `xalan.jar` 從 *ZIP-ROOT*`/applications/jdk14/jarFix` 複製到 `/tmp/dist_auth/WEB-INF/lib` 目錄。
4. 編輯 `WEB-INF/web.xml` 檔案並以 `http://java.sun.com/dtd/web-app_2_3.dtd` 取代 `jar://web-app_2_3.dtd`。
5. 從暫存位置重新產生分散式認證 WAR 並部署它。如需詳細資訊，請參閱「Access Manager Post Installation Guide」中的「Deploying a Distributed Authentication UI Server WAR File」。

單一 WAR 配置程式在 DS 上失敗 (6562076)

部署爲單一 WAR 的 Access Manager 在使用單一元件根尾碼 (例如 `dc=example`) 的 Directory Server 6 上配置會失敗，不過，使用多個元件根尾碼 (例如 `dc=example,dc=com`) 便可以成功配置。

解決方法：使用多個元件根尾碼，例如 `dc=example,dc=com`。

在相同主機上進行 AM 單一 WAR 的多伺服器配置會丟出異常 (6490150)

如果在相同主機上針對 Directory Server 配置 Access Manager 單一 WAR 的第二個實例，則會在更新組織別名時丟出異常。如果配置的第二個實例是在不同的主機上時，就不會發生此問題。

升級問題

升級問題的相關資訊包含在「Sun Java Enterprise System 5 Release Notes for UNIX」中的「Upgrade Issues」一節中。

相容性問題

- 第 20 頁的 「Access Manager 單次登入在通用 Web 用戶端上失敗 (6367058、6429573)」
- 第 20 頁的 「在 64 位元模式中執行的 Web Server 7.0 上發生 StackOverflowError (6449977)」
- 第 21 頁的 「舊有模式下核心認證模組中存有的不相容問題 (6305840)」
- 第 21 頁的 「Delegated Administrator `commadmin` 公用程式未建立使用者 (6294603)」
- 第 22 頁的 「Delegated Administrator `commadmin` 公用程式未建立組織 (6292104)」

Access Manager 單次登入在通用 Web 用戶端上失敗 (6367058、6429573)

如果安裝了 Access Manager、Messaging Server 及 Calendar Server，將它們配置成共同運作，然後安裝 JES5 120955-01 修補程式，就會發生這個問題。使用者遇到登入錯誤。錯誤原因在於 Policy Agent 2.1 特性與 AMSDK 之間不相容。目前沒有解決方法。

在 64 位元模式中執行的 Web Server 7.0 上發生 StackOverflowError (6449977)

如果 Access Manager 是配置在使用 64 位元 JVM 的 Web Server 7.0 實例上，則使用者在存取主控台登入頁面時，會遇到 [伺服器錯誤] 訊息。Web Server 錯誤記錄包含 `StackOverflowError` 異常。

解決方法：遵循下列步驟來修改 Web Server 配置：

1. 以 Web Server 管理員的身份登入 Web Server 管理主控台。
2. 按一下 [編輯配置]。

   在 [平台] 欄位中選取 [64]，再按一下 [儲存]。
3. 按一下 [Java] 標籤，再按一下 [JVM 設定] 標籤。
   - 在 [選項] 下尋找最小堆疊儲存區大小項目 (例如：-Xms)。最小堆疊儲存區大小的值應該至少爲 512m。例如，如果堆疊儲存區大小的值不等於或小於 -Xms512m，則請將這個值改成至少 -Xms512m。
   - 最大堆疊儲存區大小的值應該至少爲 768m。如果最大堆疊儲存區大小不等於或小於 -Xmx768m，則請將這個值改成至少 -Xmx768m。
   - 使用 `-Xss512k` 或 `-Xss768k` 將 Java 堆疊大小設定爲 512k 或 768k。在 Solaris Sparc 上您可以將它留爲空白，以將它保留爲 64 位元 JVM 之預設大小 (1024k)。
4. 按一下 [效能] 標籤，再按一下連結 [執行緒池設定]。

   將堆疊大小的值改爲至少 261144，然後按一下 [儲存]。
5. 按一下螢幕右上角的 [部署擱置] 連結。

   在 [配置部署] 頁面中，按一下 [部署] 按鈕。
6. 在 [結果] 視窗中，按一下 [確定] 以重新啓動 Web Server 實例。

   在重新啓動 Web Server 之後，按一下 [結果] 視窗中的 [關閉]。

舊有模式下核心認證模組中存有的不相容問題 (6305840)

Access Manager 7.1 舊有模式的核心認證模組與 Access Manager 6 2005Q1 存有下列不相容問題：

- 在舊有模式下會將組織認證模組移除。
- [管理員認證配置] 與 [組織認證配置] 的表示已變更。在 Access Manager 7.1 主控台中，預設會選取下拉式清單中的 `ldapService`。在 Access Manager 6 2005Q1 主控台中，會提供 [編輯] 按鈕，預設不會選取 LDAP 模組。

解決方法：無。

Delegated Administrator `commadmin` 公用程式未建立使用者 (6294603)

Delegated Administrator `commadmin` 公用程式 (具 `-S mail,cal` 選項) 未在預設網域內建立使用者。

解決方法：若將 Access Manager 升級至版本 7.1，但未將 Delegated Administrator 升級，就會發生此問題。

若不打算升級 Delegated Administrator，請遵循下列步驟執行：

1. 在 `UserCalendarService.xml` 檔案中，將 `mail`、`icssubcribed` 與 `icsfirstday` 屬性標示爲可選的而非必需的。依預設，此檔案位於 Solaris 系統上的 `/opt/SUNWcomm/lib/services/` 目錄中。
2. 在 Access Manager 中，透過執行 `amadmin` 指令移除現存的 XML 檔案，如下所示：

   ```
   # ./amadmin -u amadmin -w password -r UserCalendarService
   ```
3. 在 Access Manager 中，加入更新後的 XML 檔案，如下所示：

   ```
   # ./amadmin -u amadmin -w password
   -s /opt/SUNWcomm/lib/services/UserCalendarService.xml
   ```
4. 重新啓動 Access Manager Web 容器。

Delegated Administrator `commadmin` 公用程式未建立組織 (6292104)

Delegated Administrator `commadmin` 公用程式 (具 `-S mail,cal` 選項) 未建立組織。

解決方法：請參閱上一個問題之解決方法。

配置問題

負載平衡器後方出現主控台重新導向不正確 (6480354)

如果 Access Manager 實例部署於負載平衡器後方，登入 Access Manager 主控台可能會重新導向至其中一個 Access Manager 實例，而非負載平衡器。瀏覽器中的 URL 也會變更爲 Access Manager 實例。例如，如果您使用下列 URL 來登入主控台，就會發生此問題：

```
http://loadbalancer.example.com/amserver/realm
```

此重新導向在 [範圍] 模式與 [舊有] 模式部署中都可能發生。

針對此問題，有兩種解決方法：您可任選一種：

1. 使用下列任一 URL 來登入：

   `http://`*loadbalancer*`/amserver/UI/Login`

`http://`*loadbalancer*`/amserver`

2. 在 `AMConfig.properties` 中，將 `com.sun.identity.loginurl` 特性設定爲負載平衡器的名稱。這需要在負載平衡器後方的每個 Access Manager 實例上完成。

無 Web 容器的 Access Manager SDK 安裝需要更新通知 URL (6491977)

如果您執行 Java ES 5 安裝程式，並以 [立即配置] 選項來安裝無 Web 容器的 Access Manager SDK，則 AMConfig.properties 檔案中的 `com.iplanet.am.notification.url` 特性會設爲 `NOTIFICATION_URL` 。如果您不要執行任何額外的 Web 容器配置，使用者不會收到遠端 Access Manager 伺服器的任何通知。

解決方法：重設此特性如下： `com.iplanet.am.notification.url=""`

變更密碼時，「密碼重設」服務報告通知錯誤 (6455079)

當密碼變更時，Access Manager 會使用一個不合格的寄件者名稱 `Identity-Server` 來送出電子郵件通知，導致 `amPasswordReset` 記錄中出現錯誤項目。範例：

```
07/19/2006 10:26:04:010 AM PDT: Thread[service-j2ee,5,main]
ERROR: Could not send email to user [Ljava.lang.String;@999262
com.sun.mail.smtp.SMTPSendFailedException: 553 5.5.4 <Identity-Server>...
Domain name required for sender address Identity-Server
```

解決方法：變更 `/opt/SUNWam/locale/amPasswordResetModuleMsgs.properties` 中的配置。

- 變更 [從] 位址。將 `fromAddress.label=<Identity-Server>` 變更爲 `fromAddress.label=<IdentityServer@myhost.company.com>`
- 變更特性 `lockOutEmailFrom`，以確保封鎖通知使用正確的 **[從]** 位址。

平台伺服器清單與 FQDN 別名屬性未更新 (6309259、6308649)

在多重伺服器部署中，若將 Access Manager 安裝在第二個 (以及後續的) 伺服器上，平台伺服器清單與 FQDN 別名屬性不會更新。

解決方法：手動加入「範圍/DNS」別名與平台伺服器清單項目。如需步驟，請參閱「Sun Java System Access Manager 7.1 Postinstallation Guide」中的「Adding Additional Instances to the Platform Server List and Realm/DNS Aliases」。

驗證服務中必需屬性的資料 (6308653)

Access Manager 7.1 會強制服務 XML 檔案中的必需屬性必須具備預設值。

解決方法：如果服務的必需屬性沒有值，請爲屬性加入值後，重新載入服務。

於安全 WebLogic 8.1 實例中的部署解決方法 (6295863)

若將 Access Manager 7.1 部署至安全 (啓用 SSL) BEA WebLogic 8.1 SP4 實例，則會在部署每個 Access Manager Web 應用程式時發生異常。

解決方法：依照以下步驟：

1. 套用 WebLogic 8.1 SP4 修補程式 JAR `CR210310_81sp4.jar` ，其可從 BEA 取得。
2. 在 `/opt/SUNWam/bin/amwl81config` 程序檔 (Solaris 系統) 或 `/opt/sun/identity/bin/amwl81config` 程序檔 (Linux 系統) 中，更新 `doDeploy` 函數與 `undeploy_it` 函數，將修補程式 JAR 的路徑前置於 `wl8_classpath` 之前 (此變數包含用來部署與解除部署 Access Manager Web 應用程式的 `classpath`)。

   尋找下列包含 `wl8_classpath` 的指令行：

   ```
   wl8_classpath= ...
   ```
3. 在步驟 2 中找到的指令行後加入下列指令行：

   ```
   wl8_classpath=path-to-CR210310_81sp4.jar:$wl8_classpath
   ```

amconfig 程序檔未更新範圍/DNS 別名及平台伺服器清單項目 (6284161)

在多重伺服器部署中，`amconfig` 程序檔未更新其他 Access Manager 實例的範圍/DNS 別名及平台伺服器清單項目。

解決方法：手動加入「範圍/DNS」別名與平台伺服器清單項目。如需步驟，請參閱「Sun Java System Access Manager 7.1 Postinstallation Guide」中的「Adding Additional Instances to the Platform Server List and Realm/DNS Aliases」。

配置狀態檔範本中的預設 Access Manager 模式為範圍 (6280844)

依預設，會啓用配置狀態檔範本中的 Access Manager 模式 (`AM_REALM` 變數)。

解決方法：若要在「舊有」模式下安裝或配置 Access Manager，請重設狀態檔中的變數：

```
AM_REALM = disabled
```

效能問題

在範圍模式中，建立新群組時會產生帶有 ACI 的群組管理員，而這些 ACI 永遠不會被使用 (6485695)

如果 Access Manager 安裝於範圍模式下，則不論何時建立新群組，Access Manager 都會動態建立一個群組管理員，且該管理員具有管理群組所需的 ACI。在範圍模式中，不會使用這些群組管理員 ACI。然而，Directory Server 處理尾碼下的項目時，仍會評估它們，這樣可能會降低 Access Manager 的效能，特別是在部署建立了大量群組時。

解決方法：針對此問題的解決方法包含兩個部分：

- 防止 Access Manager 在建立新群組時建立群組管理員與對應的 ACI
- 從 Directory Server 移除所有現存的 ACI

防止建立群組管理員 ACI

下列程序會防止 Access Manager 在建立新群組時，建立群組管理員與對應的 ACI。

備註 – 此程序會永遠防止在建立新群組時，建立群組管理員與對應的 ACI。僅在此行爲適用於您的特定部署時，才使用此程序。

---

1. 備份 `amAdminConsole.xml` 檔案。此檔案位於下列目錄中，視您的平台而定：
   - Solaris 系統：`/etc/opt/SUNWam/config/xml`
   - Linux 與 HP-UX 系統：`/etc/opt/sun/identity/config/xml`
   - Windows 系統：*javaes-install-dir*`\identity\config\xml`

     javaes-install-dir 代表 Java ES 5 安裝目錄。預設值是 `C:\Program Files\Sun\JavaES5`。
2. 在 `amAdminConsole.xml` 檔案中，移除下列顯示於註釋行間的群組管理員項目：

```
<AttributeSchema name="iplanet-am-admin-console-dynamic-aci-list"
    type="list"
    syntax="string"
    i18nKey="g111">
    <DefaultValues>
...
# Beginning of entry to delete
                <Value>Group Admin|Group Admin Description|ORGANIZATION:aci:
(target="ldap:///GROUPNAME")(targetattr = "*")
(version 3.0; acl "Group and people container admin role";
allow (all) roledn = "ldap:///ROLENAME";)##ORGANIZATION:aci:
(target="ldap:///ORGANIZATION")
(targetfilter=(&amp;FILTER(!(|(nsroledn=cn=Top-level Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Top-level Help Desk Admin Role,dc=iplanet,dc=com)
```

```
(nsroledn=cn=Top-level Policy Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Organization Admin Role,ORGANIZATION)
(nsroledn=cn=Container Admin Role,ORGANIZATION)
(nsroledn=cn=Organization Policy Admin Role,ORGANIZATION)))))
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-web-agent-access-not-enforced-list||
iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list ||nsroledn")
(version 3.0; acl "Group admin's right to the members"; allow (read,write,search)
roledn = "ldap:///ROLENAME";)</Value>
# End of entry to delete
...
    </DefaultValues>
</AttributeSchema>
```

3. 使用 `amadmin` 從 Access Manager 刪除 Admin Console 服務。例如，在 Solaris 系統上：

```
# cd /opt/SUNWam/bin
# ./amadmin -u amadmin -w amadmin_password
--deleteService iPlanetAMAdminConsoleService
```

4. 使用 `amadmin` 將 Admin Console 服務從步驟 2 中已編輯的 `amAdminConsole.xml` 檔案重新載入至 Access Manager 。例如：

```
# ./amadmin -u amadmin -w amadmin_password
-t /etc/opt/SUNWam/config/xml/amAdminConsole.xml
```

5. 重新啓動 Access Manager Web 容器。(如果您如下一程序所描述，規劃從目錄伺服器刪除 ACI，請在完成該程序後，等候並重新啓動 Web 容器。)

移除現存的群組管理員 ACI

備註 – 下列程序使用 `ldapsearch` 與 `ldapmodify` 公用程式來搜尋與移除群組管理員 ACI。如果您的部署是使用 Directory Server 6.0，則也可以使用 Directory Server Control Center (DSCC) 或 `dsconf` 指令來實現這些功能。如需詳細資訊，請參閱 Directory Server 6.0 文件：

`http://docs.sun.com/app/docs/coll/1224.1` 及
`http://docs.sun.com/app/docs/coll/1632.1`

下列程序會移除已經存在於 Directory Server 中的群組管理員 ACI。

1. 建立 LDIF 檔案以配合 `ldapmodify` 使用來移除群組管理員 ACI。若要找到這些 ACI，請使用 `ldapsearch` (或您偏好的目錄搜尋工具)。

   例如，在名爲 `Remove_Group_ACIs.ldif` 的 LDIF 檔案範例中的下列項目會移除群組名稱爲 New Group 的 ACI：

```
dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///cn=New Group,ou=Groups,o=isp")(targetattr = "*")
(version 3.0; acl "Group and people container admin role"; allow (all)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)

dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///ou=People,o=isp")(targetattr="nsroledn")
(targattrfilters="add=nsroledn:(!(nsroledn=*)),
del=nsroledn:(!(nsroledn=*))") (version 3.0;
acl "Group admin's right to add user to people container"; allow (add)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)

dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///o=isp")
(targetfilter=(&(|(memberof=*cn=New Group,ou=Groups,o=isp)
(iplanet-am-static-group-dn=*cn=New Group,ou=Groups,o=isp))
(!(|(nsroledn=cn=Top-level Admin Role,o=isp)
(nsroledn=cn=Top-level Help Desk Admin Role,o=isp)
(nsroledn=cn=Top-level Policy Admin Role,o=isp)
(nsroledn=cn=Organization Admin Role,o=isp)(
nsroledn=cn=Container Admin Role,o=isp)
(nsroledn=cn=Organization Policy Admin Role,o=isp)))))
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-web-agent-access-not-enforced-list ||
iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list ||nsroledn")
(version 3.0; acl "Group admin's right to the members";
allow (read,write,search)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)
aci: (target="ldap:///o=isp")(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the root suffix";
allow (all) userdn = "ldap: ///cn=dsameuser,ou=DSAME Users,o=isp"; )
```

2. 使用 `ldapmodify` 配合前一個步驟中的 LDIF 檔案來從 Directory Server 中移除群組 ACI。例如：

```
# ldapmodify -h ds-host -p 389 -D "cn=Directory Manager"
-w ds-bind-password -f Remove_Group_ACIs.ldif
```

3. 重新啓動 Access Manager Web 容器。

Access Manager 主控台問題

新的 Access Manager 主控台無法設定 CoS 範本優先權 (6309262)

新的 Access Manager 7.1 主控台無法設定或修改服務類別 (Class of Service，CoS) 範本優先權。

解決方法：登入 Access Manager 6 2005Q1 主控台以設定或修改 CoS 範本優先權。

加入 Portal Server 相關服務時出現舊的主控台 (6293299)

Portal Server 與 Access Manager 安裝於同一伺服器上。在「舊有」模式下安裝 Access Manager 後，使用 `/amserver` 登入新的 Access Manager 主控台。在您選擇現存使用者後嘗試加入服務 (如 NetFile 或 Netlet) 時，會突然出現舊的 Access Manager 主控台 (`/amconsle`)。

解決方法：無。目前版本的 Portal Server 必須搭配 Access Manager 6 2005Q1 主控台使用。

達到資源限制後，主控台未傳回 Directory Server 設定的結果 (6239724)

使用現存的 DIT 選項安裝 Directory Server ，然後安裝 Access Manager。登入 Access Manager 主控台並建立群組。編輯群組中的使用者。例如，使用篩選器 `uid=*999*` 增加使用者。產生的清單方塊是空的，但主控台未顯示任何錯誤、資訊或警告訊息。

解決方法：群組成員不得大於 Directory Server 搜尋大小限制。如果群組成員大於搜尋大小限制，請據此變更搜尋大小限制。

於資料遷移之後新增 `ContainerDefaultTemplateRole` 屬性 (4677779)

在 [舊有] 模式中，對不是在 Access Manager 中建立的組織，不會顯示該組織的使用者角色。在除錯模式中，會顯示下列訊息：

錯誤：`DesktopServlet.handleException()`
`com.iplanet.portalserver.desktop.DesktopException:`
`DesktopServlet.doGetPost():` **無權限可執行桌面**

此錯誤在執行 Java ES 安裝程式遷移程序檔時會更明顯。當組織是由現存目錄資訊樹 (Directory Information Tree, DIT) 或其他來源中遷移出來，`ContainerDefaultTemplateRole` 屬性不會自動新增至組織中。

解決方法：使用 [Directory Server] 主控台來複製其他 Access Manager 組織的 `ContainerDefaultTemplateRole` 屬性，然後將其新增至受影響的組織。

指令行問題

組織管理員角色無法使用 amadmin 指令行公用程式建立新的使用者 (6480776)

因爲錯誤的登入權限，指定了組織管理員角色的管理員無法使用 amadmin 指令行公用程式建立新的使用者。

解決方法：組織管理員和頂層管理員均可設定權限。請透過管理主控台來進行設定：

1. 移至組織管理員所屬的組織。
2. 按一下 [權限] 標籤。
3. 按一下 [組織管理員角色] 連結。
4. 選取 [**對所有記錄檔的讀取和寫入存取**] 或 [**對所有記錄檔的寫入存取**]。
5. 按一下 [儲存]。

SDK 與用戶端問題

- 第 29 頁的 「伺服器重新啓動後，用戶端沒有收到通知 (6309161)」
- 第 29 頁的 「服務模式變更後，SDK 用戶端必須重新啓動 (6292616)」

伺服器重新啓動後，用戶端沒有收到通知 (6309161)

使用用戶端 SDK (`amclientsdk.jar`) 撰寫的應用程式在伺服器要重新啓動時，不會收到通知。

解決方法：無。

服務模式變更後，SDK 用戶端必須重新啓動 (6292616)

若修改了任何服務模式，`ServiceSchema.getGlobalSchema` 會傳回舊的模式而非新的模式。

解決方法：服務模式變更後重新啓動用戶端。

這個問題會在修補程式 1 中修正。

認證問題

當應用程式使用者的權限不足時，「分散式認證 UI」伺服器效能降低 (6470055)

使用預設的應用程式使用者來部署「分散式認證 UI」伺服器時，效能會因爲預設應用程式使用者的權限有限而大幅降低。

解決方法：使用適當的權限建立新使用者。

遵循下列步驟使用適當的 ACI 建立新使用者：

1. 在 Access Manager 主控台中建立新使用者。例如，建立稱爲 `AuthUIuser` 的使用者。
2. 在 Directory Server 主控台中加入下列 ACI。

```
dn:ou=1.0,ou=SunAMClientData,ou=ClientData,<ROOT_SUFFIX>
changetype:modifyadd:aci
aci: (target="ldap:///ou=1.0,ou=SunAMClientData,ou=ClientData,<ROOT_SUFFIX>")
(targetattr = "*"(version 3.0; acl "SunAM client data anonymous access";
allow (read, search, compare) userdn = "ldap:///<AuthUIuser's DN>";)
```

   請注意，`userdn` 是設爲「`ldap:///<AuthUIuser's DN>`」。
3. 請參閱「Sun Java System Access Manager 7.1 Postinstallation Guide」中的「To Install and Configure a Distributed Authentication UI Server」，以取得關於編輯 `amsilent` 檔案和執行 `amadmin` 指令的指示。
4. 在 `amsilent` 檔案中，設定下列特性：

   APPLICATION_USER　　輸入 `AuthUIuser`。

   APPLICATION_PASSWD　　輸入 `AuthUIuser` 的密碼。
5. 儲存檔案。
6. 使用新的配置檔案執行 `amconfig` 程序檔。例如，在 Access Manager 安裝於預設目錄的 Solaris 系統上：

```
# cd /opt/SUNWam/bin
# ./amconfig -s ./DistAuth_config
```
7. 在「分散式認證 UI」伺服器上重新啓動 Web 容器。

在舊有 (相容) 模式下，Access Manager 統計服務的預設配置不相容 (6286628)

在舊有模式下安裝 Access Manager 後，「統計服務」的預設配置已變更：

- 依預設，會開啓服務 (`com.iplanet.services.stats.state=file`)。之前它是關閉的。
- 預設間隔 (`com.iplanet.am.stats.interval`) 已從 3600 變更爲 60。
- 預設的 stats 目錄 (`com.iplanet.services.stats.directory`) 已從 `/var/opt/SUNWam/debug` 變更爲 `/var/opt/SUNWam/stats`。

解決方法：無。

頂層組織中命名屬性的屬性唯一性遭破壞 (6204537)

安裝 Access Manager 之後，以 `amadmin` 身份登入，並將 `o`、`sunPreferredDomain`、`associatedDomain`、`sunOrganizationAlias`、`uid` 與 `mail` 屬性加入 [唯一的屬性清單]。若要建立兩個名稱相同的新組織，作業會失敗，但 Access Manager 會顯示 [組織已存在] 訊息，而不是按預期顯示 [違反屬性唯一性] 訊息。

解決方法：無。忽略不正確的訊息。Access Manager 運作正常。

階段作業與 SSO 問題

- 第 31 頁的「負載平衡器之 SSL 終止時，系統會建立無效的服務主機名稱 (6245660)」
- 第 32 頁的「搭配協力廠商的 Web 容器使用 `HttpSession`」

負載平衡器之 SSL 終止時，系統會建立無效的服務主機名稱 (6245660)

如果部署 Access Manager 的 Web 容器爲 Web Server，其負載平衡器終止了 SSL，則用戶端將不會被導向至正確的 Web Server 頁面。按一下 Access Manager 主控台中的 [階段作業] 標籤會傳回錯誤訊息，因爲主機無效。

解決方法：在下列範例中，Web Server 會使用連接埠 3030 偵聽。負載平衡器則使用連接埠 80 偵聽，並將請求重新導向至 Web Server。

在 *web-server-instance-name*`/config/server.xml` 檔案中，視您使用的 Web Server 版本而定，編輯 `servername` 屬性以指向負載平衡器。

針對 Web Server 6.1 Service Pack (SP) 版本，以如下方式編輯 `servername` 屬性：

```
<LS id="ls1" port="3030" servername="loadbalancer.example.com:80"
defaultvs="https-sample" security="false" ip="any" blocking="false"
acceptorthreads="1"/>
```

Web Server 6.1 SP2 (或更新版本) 可將通訊協定從 `http` 切換爲 `https`，或從 `https` 切換爲 `http`。因此，請以如下方式編輯 `servername`：

```
<LS id="ls1" port="3030"
servername="https://loadbalancer.example.com:443" defaultvs="https-sample"
security="false" ip="any" blocking="false" acceptorthreads="1"/>
```

搭配協力廠商的 Web 容器使用 HttpSession

維護認證階段作業的預設方法是「內部階段作業」，而不是 `HttpSession`。3 分鐘的預設無效階段作業最大時間值已經足夠。`amtune` 程序檔會將 Web Server 或 Application Server 的該值設爲一分鐘。然而，若您是使用協力廠商 Web 容器 (IBM WebSphere 或 BEA WebLogic Server) 和選用的 `HttpSession`，可能需要限制 Web 容器的最大 `HttpSession` 時間限制以避免效能發生問題。

策略問題

- 第 32 頁的 「刪除策略配置服務中的動態屬性會導致策略編輯發生問題 (6299074)」

刪除策略配置服務中的動態屬性會導致策略編輯發生問題 (6299074)

刪除 [策略配置服務] 中的動態屬性會導致編輯以下方案的策略時發生問題：

1. 在 [策略配置服務] 中建立兩個動態屬性。
2. 建立策略並在回應提供者中選取動態屬性 (來自步驟 1)。
3. 移除 [策略配置服務] 中的動態屬性，然後再建立兩個屬性。
4. 試著編輯於步驟 2 建立的策略。

結果爲：[錯誤：設定了無效的動態特性。]依預設，清單中不會顯示任何策略。完成搜尋後，策略會顯示出來，但您無法編輯或刪除現存策略，或建立新策略。

解決方法：從 [策略配置服務] 移除動態屬性之前，請先從策略移除對這些屬性的參照。

伺服器啓動問題

- 第 33 頁的 「Access Manager 啓動時發生除錯錯誤 (6309274、6308646)」

Access Manager 啓動時發生除錯錯誤 (6309274、6308646)

Access Manager 7.1 啓動時傳回 `amDelegation` 與 `amProfile` 除錯檔案中的除錯錯誤：

- `amDelegation`：無法取得委派的外掛程式實例
- `amProfile`：出現委派異常

解決方法：無。您可忽略這些訊息。

AMSDK 問題

執行 AMIdentity.modifyService 時出現錯誤 (6506448)

使用 `AMIdentity.modifyService` 在範圍中設定桌面服務動態屬性時，Access Manager 會傳回空指標異常。

解決方法：將以下特性增加至 `AMConfig.properties`，再重新啓動伺服器:

```
com.sun.am.ldap.connnection.idle.seconds=7200
```

群組成員沒有顯示在選取的清單中 (6459598)

在下列情況下會發生這個問題：

1. 使用下列範圍配置來定義範圍：
   - 頂層範圍是 `amroot`。子範圍是 `example.com`。
   - 子範圍 `example.com` 有兩個資料存放區：`exampleDB` 及 `exampleadminDB`。
   - 資料存放區 `exampleDB` 包含開頭爲 `dc=example,dc=com` 的所有使用者。支援的 LDAPv3 作業設爲 `user=read,write,create,delete,service`。
   - 資料存放區 `exampleadminDB` 包含範圍的管理群組。管理群組是 `DN: cn=example.com Realm Administrators,ou=Groups,dc=example,dc=com`。這個群組有個單一成員 `scarter`。支援的 LDAPv3 作業設爲 `group=read,write,create,delete`。
2. 按一下 [主體] 標籤，再按一下 [群組]，然後按一下 `example.com Realm Administrators` 的項目。
3. 按一下 [使用者] 標籤。

在 exampleDB 資料存放區中的所有使用者都會顯示爲可用，但 scarter 不會顯示在 [選取的] 欄位中。

解決方法：將作業 user=read 加入 exampleadminDB 資料存放區中支援的 LDAPv3 作業。

Access Manager 登入 URL 傳回訊息 [找不到這樣的組織] (6430874)

這個問題原因可能是在完全合格網域名稱 (Fully Qualified Domain Name, FQDN) 中使用了大小寫混合 (同時包括大寫與小寫) 的字元。

範例：HostName.PRC.Example.COM

解決方法：在安裝之後，不要使用預設的 Access Manager 登入 URL。而是在登入 URL 中包括預設組織的 LDAP 位置。例如：

```
http://HostName.PRC.Example.COM/amserver/UI/Login?org=dc=PRC,dc=Example,dc=COM
```

一旦順利登入到 Access Manager 之後，即可免除每次登入 Access Manager 都要輸入使用者組織完整路徑的需要。依照以下步驟：

1. 進入 [範圍] 模式下的 [範圍] 標籤，或進入 [舊有] 模式下的 [組織] 標籤。
2. 按一下預設的範圍或組織名稱。

   在此範例中，按一下 prc。
3. 將**範圍**/DNS **別名**值中的所有大寫字元改爲小寫字元。

   在此範例中，將所有小寫值 hostname.prc.example.com 加入清單，然後從清單中移除混合大小寫的 HostName.PRC.Example.COM 值。
4. 按一下 [儲存]，並登出 Access Manager 主控台。

您現在可以使用下列任何一個 URL 登入：

- http://hostname.PRC.Example.COM/amserver/UI/Login
- http://hostname.PRC.Example.COM/amserver
- http://hostname.PRC.Example.COM/amserver/console

使用 amadmin 時無法從 Access Manager 建立子組織 (5001850)

在兩個 Directory Server 之間啓用多個主伺服器複製並嘗試使用 amadmin 公用程式建立子組織時，就會發生這個問題。

解決方法：在這兩個 Directory Server 中，將 nsslapd-lookthroughlimit 特性設爲 -1。

SSL 問題

- 第 35 頁的 「當 SSL 憑證過期時，amconfig 程序檔失敗。(6488777)」

當 SSL 憑證過期時，amconfig 程序檔失敗。(6488777)

如果 Access Manager 容器是在 SSL 模式中執行，而且容器的 SSL 憑證已過期，則 amconfig會失敗，並可能導致類別路徑毀損。

解決方法：如果您使用了過期憑證來執行 amconfig，且類別路徑已毀損，則應該先取得有效的 SSL 憑證。復原爲類別路徑未毀損的原始 domain.xml 檔案，或該檔案的副本。然後重新執行 amconfig 指令：

```
/opt/SUNWam/bin/amconfig -s $PWD/amsamplesilent
```

範例問題

- 第 35 頁的 「Clientsdk 範例目錄包含不要的 makefile (6490071)」

Clientsdk 範例目錄包含不要的 makefile (6490071)

範例檔案包含於用戶端 SDK 中。這些範例示範如何撰寫獨立程式，以及如何撰寫 Web 應用程式。這些範例位於您產生 Makefile.clientsdk 的目錄下，以及下列子目錄中：

```
.../clientsdk-samples/

.../clientsdk-webapps/
```

Clientsdk-samples 包括認證、記錄、策略和 SAML 獨立程式的範例。Clientsdk-webapps 包括使用者管理、服務管理和策略程式的範例。每個範例都有 Readme.html 檔案，其中包含編譯和執行範例程式的指示。

爲了編譯範例，makefile 應在對應的子目錄中執行。頂層 makefile 不會編譯子目錄中的範例。

Linux OS 問題

- 第 35 頁的 「在 Application Server 上執行 Access Manager 時發生 JVM 問題 (6223676)」

在 Application Server 上執行 Access Manager 時發生 JVM 問題 (6223676)

若您是在 Red Hat Linux 上執行 Application Server 8.1，Red Hat OS 爲 Application Server 所建立之執行緒的堆疊大小爲 10 MB，當 Access Manager 使用者階段作業達到 200 時，這會造成 JVM 資源問題。

解決方法：在您啓動 Application Server 之前先執行 `ulimit` 指令，將 Red Hat OS 作業堆疊大小設爲較小的值，如 2048，甚至是 256 KB。在您將用來啓動 Application Server 的同一主控台上執行 `ulimit` 指令。例如：

```
# ulimit -s 256;
```

Windows 與 HP-UX 問題

- 第 36 頁的「在 zh_TW 和 es 語言環境上安裝時，Access Manager 自動配置失敗 (6515043)」
- 第 36 頁的「完整安裝 JES 時，HP-UX 需要 AM 的 gettext 二進位 (6497926)」

在 zh_TW 和 es 語言環境上安裝時，Access Manager 自動配置失敗 (6515043)

解決方法：在 HP-UX 平台的 `zh_TW` 和 `es` 語言環境中，Access Manager 只能在「以後配置」模式中進行配置。啓動 JavaES 安裝程式，安裝 Access Manager 產品並結束 JavaES 安裝程式。接著呼叫 Access Manager 配置程式，如下所示：

1. `LANG=C`
2. `export LANG`
3. 編輯 *accessmanager-base*`/bin/amsamplesilent` **檔案**
4. 執行 *accessmanager-base*`/bin/amconfig -s amsamplesilent`

完整安裝 JES 時，HP-UX 需要 AM 的 gettext 二進位 (6497926)

目前沒有此問題的解決方法。

聯合與 SAML 問題

- 第 36 頁的「聯合過程中發生登出錯誤 (6291744)」

聯合過程中發生登出錯誤 (6291744)

在範圍模式下，若您聯合識別提供者 (IDP) 與服務提供者 (SP) 上的使用者帳號，然後在終止聯合後登出，會發生以下錯誤：[錯誤：找不到子組織。]

解決方法：無。

全球化 (g11n) 問題

在 zh 語言環境中，管理主控台元件以英文顯示 (6470543)

設定瀏覽器的語言環境爲 zh 時，管理主控台元件以英文顯示，例如 [Version] (版本)、[Help] (說明) 和 [Logout] (登出) 按鈕。

解決方法：將瀏覽器語言環境設定設定爲 `zh-cn`，而非 `zh`。

「目前的值」和「新的值」在主控台中顯示錯誤 (6476672)

在主控台的本土化版本中，「目前的值」和「新的值」兩個屬性的標籤分別錯誤顯示爲 label.current.value 和 label.new.value。

必須根據英文習慣指定策略條件日期 (6390856)

在中文語言環境下的策略條件日期格式標籤不會根據中文習慣顯示。標籤所使用的日期格式類似英文日期格式。相關欄位也接受英文日期格式值。

解決方法：對於每一個欄位，請遵循在欄位標籤中指定的日期格式範例。

在「用戶端偵測」中無法移除 UTF-8 (5028779)

「用戶端偵測」功能無法正常運作。在 Access Manager 7.1 主控台中所做的變更未自動傳遞至瀏覽器。

解決方法：有二種解決方法：

- 在 [用戶端偵測] 區段中進行變更後，重新啓動 Access Manager Web 容器。

  或

- 在 Access Manager 主控台中依照以下步驟執行：
  1. 按一下 [**配置**] 標籤下的 [**用戶端偵測**]。
  2. 按一下 `genericHTML` 的 [**編輯**] 連結。
  3. 按一下 HTML 標籤下的 `genericHTML` 連結。
  4. 在字元集清單中輸入下列項目：`UTF-8;q=0.5` (請確定 UTF-8 `q` 因子小於語言環境中的其他字元集。)
  5. 儲存、登出後再登入一次。

記錄檔中多位元組字元以問號顯示 (5014120)

`/var/opt/SUNWam/logs` 目錄下的記錄檔中，多位元組訊息以問號 (?) 顯示。記錄檔爲原生編碼且不一定是 UTF-8 格式。在特定語言環境啓動 Web 容器實例時，該語言環境的記錄檔將使用原生編碼格式。若切換至其他語言環境並重新啓動 Web 容器實例，後續的訊息將以該語言環境的原生編碼呈現，但使用先前編碼方式的訊息將以問號顯示。

解決方法：確定每次均使用同一種原生編碼啓動任何 Web 容器實例。

文件問題

記錄可支援 LDAPv3 外掛程式的角色和已篩選角色 (6365196)

若資料是儲存在 Sun Java System Directory Server 中，套用修補程式後，您可爲 LDAPv3 外掛程式配置角色和已篩選角色 (可修正問題 ID 6349959)。在 Access Manager 7.1 管理主控台中，在 [LDAPv3 外掛程式支援的類型和作業] 欄位的 LDAPv3 配置中，輸入下列值：

```
role: read,edit,create,delete
filteredrole: read,edit,create,delete
```

您可輸入上述項目之一或二者皆輸入，依您計劃在 LDAPv3 配置中使用的角色和已篩選角色而定。

記錄 `AMConfig.properties` 檔案中未使用的特性 (6344530)

`AMConfig.properties` 檔案中未使用下列特性：

```
com.iplanet.am.directory.host
com.iplanet.am.directory.port
```

記錄如何啓用 XML 加密 (6275563)

若要啓用 Access Manager 或 Federation Manager 的 XML 加密 (使用 Bouncy Castle JAR 檔來產生傳輸的金鑰)，依下列步驟操作：

1. 若您使用的 JDK 版本低於 JDK 1.5，從 Bouncy Castle 網站 (`http://www.bouncycastle.org/`) 下載 Bouncy Castle JCE 提供者。例如，若使用 JDK 1.4，則下載 `bcprov-jdk14-131.jar` 檔。
2. 若您已依前述步驟下載 JAR 檔，將檔案複製到 *jdk_root*`/jre/lib/ext` 目錄中。

3. 有關各國的 JDK 版本資訊，從 Sun 網站 (http://java.sun.com) 下載針對您的 JDK 版本的 JCE Unlimited Strength Jurisdiction Policy Files。若使用 IBM WebSphere，前往相應的 IBM 網站下載所需的檔案。
4. 將下載的 `US_export_policy.jar` 和 `local_policy.jar` 檔案複製到 *jdk_root*`/jre/lib/security` 目錄。
5. 如果您使用的 JDK 版本低於 JDK 1.5，請編輯 *jdk_root*`/jre/lib/security/java.security` 檔案，並加入 Bouncy Castle 做爲提供者之一。例如：

   ```
   security.provider.6=org.bouncycastle.jce.provider.BouncyCastleProvider
   ```

6. 在 `AMConfig.properties` 檔案中將下列特性設定爲 true：

   ```
   com.sun.identity.jss.donotInstallAtHighestPriority=true
   ```

7. 重新啓動 Access Manager Web 容器。

如需更多資訊，請參考問題 ID 5110285 (XML 加密需有 Bouncy Castle JAR 檔)。

文件更新

若要存取這些文件，請參閱 Access Manager 7.1 文件集：

http://docs.sun.com/coll/1292.1 及 http://docs.sun.com/coll/1414.1

Access Manager 7 2005Q4 文件集已加入了「Technical Note: Deploying Access Manager to an Application Server Cluster」中的第 1 章「Technical Note: Deploying Access Manager Instances to an Application Server Cluster」。

Sun Java System Access Manager Policy Agent 2.2 文件集已修訂，以記錄新的代理程式：

http://docs.sun.com/coll/1322.1

可再分發的檔案

Sun Java System Access Manager 7.1 並不包含任何您可以再分發給未授權的產品使用者的檔案。

如何報告問題和提供建議

如果您遇到有關 Access Manager 或 Sun Java Enterprise System 的問題，請使用以下機制之一與 Sun 客戶支援人員連絡：

- Sun 支援資源 (SunSolve) 服務，網址爲：http://sunsolve.sun.com/。

  該網站可連結至知識庫、線上支援中心、ProductTracker 以及維護程式與支援人員連絡電話號碼。
- 與您的維護合約相關之電話派遣維護號碼。

爲便於我們有效地協助您解決問題，請在連絡支援人員時準備好以下資訊：

- 問題的描述，包括問題發生時的狀況以及該問題對您作業的影響
- 機器類型、作業系統版本和產品版本，包括可能影響該問題的所有修補程式和其他軟體
- 詳細描述您使用的方法步驟以重建問題
- 所有錯誤記錄檔或記憶體傾印

Sun 歡迎您提出寶貴意見

Sun 致力於提高文件品質，因此誠心歡迎您提出意見與建議。請至下列網址提出您對本文件的意見：http://docs.sun.com/，並按一下 [Send Comments] (傳送您的意見)。

請在適當的欄位中提供完整的文件標題以及文件號碼。文件號碼可以在文件的標題頁或文件頂部找到，通常是一個七位或九位數的數字。例如，此「Access Manager 版本說明」的文件號碼是 820-0366。提出意見時您還需要在表格中輸入此文件的英文標題和文件號碼。例如，本文件的英文文件號碼爲 819-4683-13，完整標題爲「Sun Java System Access Manager 7.1 Release Notes」。

其他 Sun 資源

您可在以下位置找到有用的 Access Manager 資訊及資源：

- Sun Java Enterprise System 文件：http://docs.sun.com/prod/entsys.05q4 及 http://docs.sun.com/prod/entsys.05q4?l=zh_TW
- Sun 服務：http://www.sun.com/service/consulting/
- 軟體產品和服務：http://wwws.sun.com/software/
- 支援資源：http://sunsolve.sun.com/
- 開發者資訊：http://developers.sun.com/
- Sun 開發者支援服務：http://www.sun.com/developers/support/

為殘障人士提供的無障礙功能

欲獲得此媒體發佈以來已發行的無障礙功能，請向 Sun 索取依據美國 「Section 508」法規進行產品評估所得之結果文件，以便決定最適合佈署無障礙功能解決方案的版本。以下網址將提供應用程式的更新版本：
http://sun.com/software/javaenterprisesystem/get.html

如需有關 Sun 在無障礙功能方面之成果的資訊，請至 http://sun.com/access

相關的協力廠商網站

本文件提供了協力廠商的 URL 及其他相關資訊做爲參考。

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