Sun Java™ System Access Manager

版本說明

版本 6 2005Q1

2005 年 2 月 25 日

文件號碼：819-1949

此「版本說明」包括可以在此 Sun Java System Access Manager 6 2005Q1 版本發行時取得的重要資訊 (原來爲 Sun Java System Identity Server)。此處將介紹新功能和增強功能、已知的問題和限制以及其他資訊。安裝和使用此版本之前，請先閱讀本文件。

您能夠在下列 Sun Java System 文件網站中找到最新的版本說明：

http://docs.sun.com/prod/entsys.05q1 與

http://docs.sun.com/prod/entsys.05q1?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版本說明與產品文件。

此版本說明包含以下部分：

本文件會參考協力廠商的 URL，並提供其他相關資訊。

備註	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。

版本說明修訂記錄

表 1　修訂記錄

日期	變更說明
2005 年 2 月 25 日	修改了表 2「硬體與軟體需求」，列出了支援的 Red Hat™ Linux 版本。
2005 年 2 月 2 日	2005Q1 發行。首次發行此版本說明。

關於 Access Manager 6 2005Q1

Sun Java System Access Manager 是一個身份管理解決方案，專爲符合企業快速擴張的需要所設計。Access Manager 可以讓您爲您的員工、合作夥伴與供應商取得進入線上目錄的身份。它可提供一種方法，讓您可以建立有關在您的公司中哪些人可以存取哪些資訊的策略與權限。對於您所有的資料、服務、以及人員存取內容而言，Access Manager 無疑是關鍵，也就是您所有內部與外部業務關係的關鍵。

這個版本的新增功能

Access Manager 2005Q1 包括以下功能。如需這些功能更詳細的說明，請參閱「*Sun Java System Access Manager Technical Overview*」。

- 產品名稱從 Identity Server 改成 Access Manager
- Solaris 10 支援
- 新 Web 容器支援：Sun Java System Application Server Enterprise Edition 8 2005Q1 (8.1)
- 新增或修訂的認證模組：
  - Java 資料庫連接性 (Java Database Connectivity，JDBC)
  - 行動站台 (Mobile Station ISDN，MSISDN)
  - 作用中的目錄
  - 安全宣示標記語言 (Security Assertion Markup Language，SAML)：SAML 認證支援以認證模組的形式發行，使得 SAML 認證成爲認證堆疊的一部份。
- 階段作業防故障備用
  - 兩個以上的 Access Manager 6 2005Q1 實例，這些實例分別在不同主機伺服器支援的 Web 容器上執行。
  - 管理 Access Manager 實例與階段作業儲存資料庫之間的階段作業訊息的 Message Queue 代理程式叢集。
  - Sleepycat Software Inc. (http://www.sleepycat.com/) 的 Berkeley DB 作爲階段作業儲存資料庫。Berkeley DB 用戶端常駐程式爲 amsessiondb。
- 策略管理包括新的資源名稱外掛程式：`HttpURLResourceName`。
- 主控台增強功能：
  - 藉由顯示一個或多個物件屬性，以便在瀏覽窗格中自訂每個物件類型的檢視方式。
  - 能夠在瀏覽窗格下拉式功能表中新增物件類型 (例如，新增印表機或建築物的項目)。
- 用戶端 SDK：

- 重新封裝的 SDK (認證、服務管理、使用者管理、SAML、策略用戶端及階段作業元件)，好讓 Java 應用程式開發人員更容易整合 Access Manager。
- 移除對 serverconfig.xml 檔案的相依性，並將 Jar 檔案的佔用空間最小化。

- 聯合管理：
  - 支援 Liberty Alliance Project (LAP) 名稱識別碼對映通訊協定
  - 支援 LAP Identity Web Services Framework (ID-WSF) 探索服務規格，1.1 版
  - 支援 LAP ID-WSF 認證服務規格
  - 支援 LAP 中介資料描述和探索規格
  - 支援 LAP Liberty Identity Federation Framework (ID-FF) 延伸的設定檔：
    - 動態身份提供者代理
    - 附屬提供者聯合
    - 一次聯合
    - 名稱識別碼對映設定檔
    - 名稱識別碼加密設定檔
- 可使用效能調校程序檔將 Application Server Enterprise Edition 8 2005Q1 (8.1) 調校成 Web 容器

硬體與軟體需求

此版本 Access Manager 需要以下硬體與軟體。

表 2 硬體與軟體需求

元件	需求
作業系統	Solaris™ 作業系統 (OS)，SPARC® Platform Edition，8、9 及 10 版 Solaris™ OS，x86 Platform Edition，9 和 10 版 Red Hat™ Linux, WS/AS/ES 2.1 Update 2 Red Hat™ Linux, WS/AS/ES 3.0 Update 1
RAM	512 百萬位元組
磁碟空間	250 百萬位元組 (用於 Access Manager 及相關的應用程式)

支援的瀏覽器

此版本 Access Manager 支援下列瀏覽器：

瀏覽器	平台
Microsoft Internet Explorer™ 5.5 SP2	Windows™ 2000、Sun Linux、Red Hat™ Linux 8.0
Microsoft Internet Explorer 6.0	Windows 2000、Windows™ XP、Sun Linux、Red Hat Linux 8.0
Mozilla 1.7.1	Windows 2000、Sun Linux、Red Hat Linux 8.0、Solaris™ 9 和 10、Solaris™ OS、x86 Platform Edition (9 和 10 版)
Netscape™ 4.79	Windows NT、Solaris 8 和 9
Netscape™ 6.2.1	Windows NT、Windows 98、Sun Linux、Red Hat™ Linux Advanced Server 2.1、Solaris™ OS、x86 Platform Edition (9 和 10 版)
Netscape™ 7.0	Windows 2000、Sun Linux、Red Hat Linux 8.0、Solaris 9 和 10、Solaris™ OS、x86 Platform Edition (9 和 10 版)

此版本中修正的錯誤

下表說明了在 Access Manager 2005Q1 中修正的錯誤：

表 3 Access Manager 2005Q1 中修正的錯誤

錯誤號碼	描述
5050332	在 Linux 系統中，amserver stop 並不會停止 amunixd 程序
5049218	當使用者管理停用時，如果搜尋使用者，主控台將會發生錯誤
5048378	AMConfig.properties 中的 smtp 伺服器連接埠特性不正確
5043752	執行 am2bak 時出現已失敗訊息
5042100	策略管理員無法修改自己的設定檔
5041529	BasicEntitySearch 過濾器已固化至 uid
5038600	使用者無法與 SAML 服務同時建立
5037978	將具有存取權限的角色建立爲組織管理員時會產生錯誤
5026635	未編譯主控台範例
5016725	在參考策略規則中所做的修改並未反映在子組織中

表 3　Access Manager 2005Q1 中修正的錯誤 *(續)*

錯誤識別號	描述
5013994	日文瀏覽器中，加入 Authlevel 參數時登入失敗
5008960	amadmin 傳回的錯誤訊息不正確
4996479	包含策略模式的服務向使用者顯示爲「可新增」
4961370	"**" 搜尋遮罩無法運作
4959895	實體描述符搜尋過濾器無法正常運作
4959071	並未清除閒置階段作業
4931907	服務類型角色的使用者登入時服務會消失
4931163	命名屬性應爲小寫
4930610	只有英文版本的 am2bak 和 bak2am 訊息
4922030	衝突解決層級不隨語言環境的改變而相應變化
4916683	backup_restore.po 中 msgid-msgstr 對的訊息未本地化
4853809	服務註冊問題
4853809	註冊所有服務可能不會註冊所有可用的服務

安裝注意事項

當您使用 Java Enterprise System 安裝程式安裝第一個實例後，`amconfig` 程序檔現在可支援使用 Application Server Enterprise Edition 8 2005Q1 (8.1) 當作 Web 容器來部署 Access Manager 的其他實例。

如需有關執行配置程序檔的相關資訊，請參閱「*Access Manager 6 2005Q1 管理指南*」。

另請參閱已知問題和限制中的安裝。

已知問題和限制

本節包含 Access Manager 2005Q1 發行時比較重要的已知問題清單。本節包含以下主題：

安裝

安全性已啓用的 SDK 上 amadmin 拋出異常 (#5107584)

在 Access Manager 2005Q1 中，如果您執行了安全 Access Manager 的完整安裝，然後又安裝 SDK 來使用此完整安裝，此時將會拋出異常。這是因爲 `com.iplanet.am.admin.sli.cerdb.prefix` 特性中 Web 伺服器的值錯誤。

解決方法

1. 編輯 `AMConfig.properties`。
2. 將特性 `com.iplanet.am.admin.cli.certdb.prefix` 變更爲 `https-<ws-instance-name>-<ws-hostname>-`。
3. 重新啓動 Web 伺服器。

當使用 Web 容器的 AMSDK 在 共用 Linux 平台上 元件連結 中斷(#6199933)

如果您在 Linux 平台上爲任何 Web 容器安裝 Access Manager SDK，數個共用元件連結便會中斷。

解決方法

移除錯誤連結並建立正確連結。

若要移除連結：

```
cd ${AM_INSTALL_DIR}/identity/lib
rm -rf jaxrpc-spi.jar relaxngDatatype.jar xsdlib.jar
```

若要建立新連結：

```
ln -s /opt/sun/private/share/lib/jaxrpc-spi.jar
ln -s /opt/sun/private/share/lib/relaxngDatatype.jar
ln -s /opt/sun/private/share/lib/xsdlib.jar
```

參考完整性外掛程式的引數拼寫錯誤影響效能 (#5029256)

當 Access Manager 爲 Directory Server 啓用參考完整性外掛程式時，此外掛程式的引數 11 的屬性名稱拼寫有誤。屬性名稱顯示爲 `iplanet-am-modifable-by`。當組織被刪除時，這會在目錄錯誤記錄檔中產生 `search not indexed` 警告。

參考完整性外掛程式要求其引數所提及的全部屬性均製作索引，而製作索引的屬性爲 `iplanet-am-modifiable-by`。Access Manager 效能可能會因此受到影響。

Application Server xercesImpl.jar 造成 JVM 故障 (#6223676)

在 RedHat Linux 的 `/opt/sun/appserver/lib` 中 (或 Solaris 的 `/opt/SUNWappserver/appserver/lib` 中)，Application Server 8.1 EE 的 `xercesImpl.jar` 比 RedHat Linux 的 `/opt/sun/share/lib` (或 Solaris 的 `/usr/share/lib`) 中的 `xercesImpl.jar` 之共用元件版本先載入。

Application Server 版本在共用元件版本之前即由類別載入程式載入。此時，過期的 Application Server 版本無法應付等待處理的數千個 JSP。JVM 可能會當機或發生故障。

解決方法

如果是 Red Hat AS 2.1 或 3.0，請重新命名 `/opt/sun/appserver/lib` 中的 `xercesImpl.jar`；如果是 SPARC 與 x86 的 Solaris 9 或 10，請重新命名 `/opt/SUNWappserver/appserver/lib` 中的此文件。JVM 類別載入程式便會強制使用 Red Hat AS 2.1 或 3.0 的 `/opt/sun/share/lib` (或 Solaris 9 和 10 的 `/usr/share/lib`) 內的共用元件之 `xerceImpl.jar`。

安裝程式不允許使用者在 AM SDK 安裝期間指定通訊協定 (#6180090)

如果安裝 Access Manager SDK，「Access Manager：用來執行 Sun Java System Access Manager 服務的 Web 容器」面板並不會詢問正在執行 Access Manager 服務的 Web 容器通訊協定。因爲安裝程式認定 Web 容器是使用 http 通訊協定；不過您可能需要指定 https 通訊協定來存取使用已啓用 SSL 之 Access Manager 安裝的 SDK。

解決方法

在 AMConfig.properties 檔案中，將與 Access Manager 伺服器安裝相關的協定設定爲 https。例如：

```
com.iplanet.am.server.protocol=https
com.iplanet.am.console.protocol=https
```

Access Manager 將 servlet.jar 新增至伺服器 CLASSPATH (#5016348)

Access Manager 爲其支援的 Web 容器將 servlet.jar 放置於伺服器 CLASSPATH 中。此檔案會導致無法預期的結果，因爲每個 Web 容器會在其執行過程中繫結一個 servlet.jar 檔案。

解決方法

從 CLASSPATH 中移除 servlet.jar。

Access Manager 範例

範例會在使用 JDK 1.5 進行編譯時傳回警告 (#5102149)

Access Manager 中的範例若以 JDK 1.5 進行編譯，則會傳回警告。

解決方法

使用以下方法可避免出現這些警告：

- 使用 JDK 1.5 時，請將 encoding="ISO-8859-1" 新增至編譯指令行。

  或

- 使用 JDK 1.4 編譯範例。

SAML xmlsig 範例中的省略會導致編譯失敗 (#5090925)

若使用 JDK 1.5 編譯，SAML xmlsig 範例中的省略會導致編譯失敗。若您使用 JDK 1.4.2 編譯，則不會發生該問題。

解決方法

若您使用 JDK 1.5 編譯，則請遵照以下步驟設定 LD_LIBRARY_PATH：

1. 在 `xmlsig` 目錄中，尋找 SAML 範例的 Readme.html 或 Readme.txt 檔案。
2. 在第 3 部分 "Instructions to set up the XMLSIG sample on Solaris" 之下的步驟 4 中，將 LD_LIBRARY_PATH 設定爲 *web-server-install-directory*`/bin/https/lib`。
3. 將 `/usr/lib/mps/secv1` 新增至 LD_LIBRARY_PATH 以選擇 JSS 程式庫與其相依性。

試譯

透過電子郵件的使用者修改通知無法運作(#6212964)

位於「管理服務」中的「透過電子郵件的使用者修改通知」機制，目前無法運作。

SafeWord 連線未關閉 (#5073718)

若您嘗試登入 Access Manager，請至 SafeWord 挑戰回應頁，且不要輸入密碼，則此連線不會有逾時發生。若您關閉瀏覽器，則 SafeWord 伺服器不會關閉連線。

LDAP 認證已執行 LDAP Directory Server 連線的匿名連結 (#5090018)

Access Manager 未將連結 DN 與密碼傳送至 LDAP 連線的 Directory Server，當停用 LDAP Directory Server 的匿名連結時，會影響認證結果。

解決方法

爲您的 Directory Server 啓用匿名連結。

永久的 Cookie 模式特性不一致 (#5038544)

在永久的 Cookie 模式中，記號中的 UserId 特性集不一致。由於這個原因，視 UserID 特性而定的策略代理程式可能會失敗。

解決方法

在非 DN 值中使用 `UserToken`，而在 DN 值中使用 `Principal`。

重新載入「階段作業逾時」頁面時使用者被提示輸入使用者名稱和密碼 (#4697120)

在登入頁面上，如果使用者等待頁面逾時，然後輸入有效的使用者名稱和密碼，則會看到階段作業逾時頁面。如果使用者重新載入該頁面，則無需重新輸入使用者名稱和密碼，即可認證至 Access Manager。

必須為 SafeWord 伺服器指定不同目錄 (#4756295)

配置多個使用各自 SafeWord 伺服器的組織時，必須在其 SafeWord 認證服務範本中指定各自的 .../serverVerification 目錄。如果保留預設值，並且所有伺服器都使用同一目錄，則第一個使用其 SafeWord 伺服器認證的組織將是唯一有效的組織。

指令行工具

/opt/SUNWam/bin 目錄中的 ldapsearch 與 ldapmodify 公用程式會傳回嚴重錯誤(#4954779)

/opt/SUNWam/bin 目錄中的 ldapsearch 與 ldapmodify 公用程式會傳回嚴重錯誤。

解決方法

將 *DirectoryServer-base*/lib/ 路徑新增至您的 LD_LIBRARY_PATH 環境變數中。

am2bak 和 bak2am 程序增在 Linux 中無法運作(#5053866)

若 Access Manager 在 Linux 系統上執行的話，則 am2bak 與 bak2am 復原程序檔將無法運作。

解決方法

1. 修正下列指令的路徑：
   - ECHO=/usr/bin/echo 應該爲 ECHO=/bin/echo
   - uid='/usr/xpg4/bin/id -un' 應該爲 uid='/usr/bin/id -un'
   - /usr/bin/tar 應該爲 /bin/tar
   - /usr/bin/rm 應該爲 /bin/rm
   - /usr/bin/grep 應該爲 /bin/grep
   - /usr/bin/ps 應該爲 /bin/ps
   - /usr/bin/ls 應該爲 /bin/ls

2. 修改 check_for_invalid_chars() 函數。例如：

```
check_for_invalid_chars() {
echo "$1" | grep '[^/_.a-zA-Z0-9a-]' > /dev/null
if [ $?= 0 ]; then
return 1
else
return 0
fi
}
```

amadmin 傳回不正確的錯誤訊息 (#5008960)

amadmin 的 import 選項不正確地針對所有相關錯誤拋出相同的錯誤訊息。

僅安裝主控台元件上的 amverifyarchive 公用程式「未交換」標籤 (#4993375)

如果您僅安裝 Access Manager 主控台，此程序檔中的 amverifyarchive 公用程式將不會有下列交換出的標籤：JSSHOME、JDK_HOME、BASEDIR 與 PRODUCT_DIR。

配置

在成功地配置於 Linux 後，無法啓動 WebSphere Application Server 5.1 (#6204646)

若您在 Linux 上安裝 WebSphere 的 Access Manager SDK 元件，然後使用正確的 amsamplesilent 檔案執行 amwas51config，WebSphere 則無法啓動。

解決方法

在 LD_LIBRARY_PATH 中新增 /opt/sun/private/lib，如下所示：

```
LD_LIBRARY_PATH="$WAS_LIBPATH":$LD_LIBRARY_PATH:/opt/sun/private/lib
export LD_LIBRARY_PATH ;;
```

在 server.xml 中，移除 -Djava.util.logging.config.class 選項之前的 **"/:"**。

沒有在 Web Server 上正確設定 certdb 別名 (#6212532)

若您爲 Access Manager 的 Web Server 啓用 SSL，然後執行 amadmin，則會拋出「namingservice not available（無法使用命名服務）」錯誤。透過瀏覽器，則可以依預期運作。

無論後端名稱是什麼，始終在 userRoot 建立索引 (#5002886)

index.ldif 會將固化用於建立屬性索引的 userRoot。有可能在位於任何強制後端資料庫名稱中的 rootsuffix 中安裝 Access Manager。可以使用 nsslapd-suffix=SUFFIX_NAME 作爲過濾器，透過 ldapsearch (含基礎 cn=config) 來取得後端名稱。

聯合

聯合管理聯結人拋出異常 (#6213102)

若建立新的提供者，然後新增新的聯絡人給該提供者，則可能會收到以下錯誤：

```
The server encountered an internal error () that prevented it from fulfilling this request
```

無法連接記錄 amFederation.access 日誌 (#6197608)

配置遠端記錄時，除了 amFederation.access 異常之外，所有記錄檔將被正確寫入至遠端 Access Manager 實例。但不會寫入記錄檔。

解決方法

使用 LogUtils 中的 AccessController.doPrivileged(AdminTokenAction.getInstance());。

fedCookie 共享未變更 (#6202574)

若您在 SP 與 IDP 上爲聯合使用者執行「聯合終止」，則 fedCookie 狀態仍將會顯示 YES。應顯示爲 NO。

個人設定檔容器無法查詢 / 修改 (#6189808)

以下「個人設定檔」容器無法進行查詢或修改作業：

```
LegalIdentity/Gender

EmploymentIdentity/Alt0
```

空白屬性值配置，將會拋出 PP Modify 的異常 (#5047103)

當您使用空白的屬性值執行 PP Modify 時，Access Manager 會拋出異常。例如，如果您建立設定以測試 sis-ep 範本，然後傳送 EP Modify 頁並按一下按鈕而不輸入屬性的任何值，將會不正確地拋出異常。

策略生效需要在伺服器重新啓動 (#5045036)

聯合策略實施必須等到您重新啓動伺服器之後才會生效。它對於 Application Server 和 Web Server 皆爲有效。只有在更新的安裝之後，以及當初次實施策略時，才必須重新啓動伺服器。

Access Manager 主控台

DIT 中擁有大量人物容器時無法建立使用者 (#5079609)

若您建立了大量人物容器（超過一千個），然後登入 Access Manager 主控台並建立新使用者，則使用者將無法建立，因爲找不到人物容器。

這是因爲搜尋時間限制錯誤而導致 `UMCreateUserModelImpl.getPeopleContainers()` 失敗，雖然 Directory Server 在到達時間限制之前就找到大量人物容器。

解決方法

在 Access Manager 主控台啓用「顯示人物容器」，至指定的「人物容器」，並在該處建立使用者。

具有說明桌面管理員權限的角色無法建立新使用者 (#5109348)

目前，「說明桌面管理員」角色的預設值設定爲「完全存取權」。將其變更爲「修改」將會停用「瀏覽」框架中的「新增」與「刪除」按鈕，但仍允許管理員修改使用者項目特性。

解決方法

顯示「說明桌面管理員」特性頁面，並將檢視變更爲可用的動作。找出使用者行並將設定從「完整存取權」變更爲「修改」。

選取附屬提供者實體的附屬提供者選項時，會拋出異常 (#6203563)

在「聯合管理」模組中，當您在「附屬提供者實體」頁面中選取「檢視」>「附屬提供者」時，將拋出異常。

解決方法

修改 JSP，則高度屬性將位於 JATO 關閉標籤之外。在 `FSAffiliateProfile.jsp` 中，第 104 行將變更爲：

```
<td width="1%"><img src="<%consoleImages%>/spacer.gif" width=<jato:text
name="defaultAttrNameWidth" /> height="1" alt=""></td>
```

請注意：/> 位於高度屬性之前。

附屬提供者顯示選項錯誤 (#6194139)

當「聯合管理」模組中的「附屬提供者顯示」選項是功能表中的唯一選項，且設定爲預設值時，Access Manager 將傳回錯誤頁面。

無法爲人物管理員角色的使用者修改服務 (#6174652)

若您以頂層「人物管理員角色」登入，則可以爲使用者新增服務，但無法修改任何服務。

解決方法

編輯「人物管理員」角色的顯示設定檔，並給予其必須的檢視功能表與可用的動作。

按「上一步」按鈕時，數值無法保留 (#4992972)

每當有多重頁面處理 (例如建立群組與角色或新增條件至策略)，然後選取「上一步」按鈕時，前一個頁面中的數值將無法恢復。

聯合管理模組中身份提供者的新問題 (#4915894)

在聯合管理模組中，如果您修改並儲存託管提供者之「身份提供者」視區中的任何屬性，變更將被儲存，但不會自動更新顯示內容。

解決方法

透過選取不同模組 (例如，服務配置) 結束聯合管理模組，然後再返回聯合管理模組。這樣會更新顯示內容。

主控台不能更新使用者屬性變更 (#4931455)

Access Manage 主控台「瀏覽」框架不能更新以指示「資料」框架中使用者屬性值的變更。手動更新頁面以檢視變更的值。

Internet Explorer 中發生連接埠問題 (#4864133)

由於和 Internet Explorer 不相容的問題，在執行 http 時不應該使用連接埠 80 作爲 Access Manager 連接埠號碼，或是在執行 https 時不應該使用連接埠 443。

記錄服務

啓用 Java Security 時發生記錄問題 (#4926520)

啓用 Java Security 時，`jdk_logging.jar` 可能無法工作。

解決方法

啓用 Java Security 時，如果您擁有 JDK 1.4 之前的版本，請在 Java 安全檔案中納入以下許可權：

```
permission java.lang.RuntimePermission  shutdownHooks
```

策略

在到達 nslookthrough 限制時並未將傳回符合的項目 (#5013538)

即使已到達 nslookthrough 中所定義的管理限制，符合的項目仍然未傳回 Access Manager 主控台。

解決方法

調校 nslookthroughlimit 參數以補償項目數。

別名藉由成員身份強制執行 (#4985823)

如果您使用使用者別名藉由 LDAP 或成員身份以外的授權模組登入 Access Manager，然後嘗試存取受保護的資源，則存取將會被拒絕。

策略範例中的 Readme.html 不包括範例 (#4923898)

位於策略範例中的 Readme.html 不包括導致範例無法執行的資訊。

解決方法

若要執行範例，則 LD_LIBRARY_PATH 環境變數必須包括 NSPR、NSS 以及 JSS 共用程式庫的路徑。爲 Solaris 系統將 LD_LIBRARY_PATH 設定爲包含 /usr/lib/mps/secv1 或爲 Linux 系統設定爲包含 /opt/sun/private/lib。

Access Manager SDK

屬性唯一性在命名屬性的頂層組織中損壞 (#6204537)

命名屬性的屬性唯一性無法作用於頂層組織中。但是，使用者與組織屬性的唯一性則可以正確地強制執行。

當 EventService 沒有取得永久搜尋連線時，將會成爲緊密迴圈 (#6205443)

EventService (ES) 執行緒成功地新增偵聽程式 (LDAP JDK 成功地新增偵聽程式)，即使已到達永久搜尋連接的數目。但是當 ES 執行緒嘗試取得回應時，LDAP 回應會報告 （錯誤碼 51）無法使用永久搜尋連線。ES 之後會嘗試再次重新建立偵聽程式。所以，這會成爲緊密迴圈。

在使用 SSL 啓用器的 Access Manager SDK 中使用 certutil 功能 (#5027614)

使用者嘗試從僅有 SDK 的機器與啓用 SSL 的 Access Manager 伺服器進行通訊時，會發生安全性相關的錯誤和異常。在此方案中，可以不在 Web 容器或是在第三方的 Web 容器 (例如 BEA WebLogic Server 或 IBM WebSphere Application Server) 中部署 Access Manager SDK。

解決方法

在僅有 SDK 的機器上建立證書資料庫，並將 Access Manager 伺服器的根 CA 證書安裝至此資料庫：

1. 以超級使用者 (root) 的身份登入僅安裝 SDK 的機器。
2. 確認已安裝必要的 Netscape Security Services (NSS) 套裝軟體：
   - 在 Solaris 系統中：SUNWtlsu
   - 在 Linux 系統中：sun-nss RPM
3. 如果未安裝套裝軟體，請現在安裝。例如：

   在 Solaris 系統中：

   ```
   cd JavaEnterpriseSystem_base/Solaris_arch/Product/shared_components/Packages
   pkgadd -d . SUNWtlsu
   ```

   在 Linux 系統中：

   ```
   cd JavaEnterpriseSystem_base/Linux_x86/Product/shared_components/Packages
   rpm -Uvh sun-nss-3.3.10-1.i386.rpm
   ```

4. 爲該證書資料庫建立記號密碼的密碼檔案。例如：

   在 Solaris 系統中：

   ```
   echo "cert-database-password" > /etc/opt/SUNWam/config/.wtpass
   chmod 700 /etc/opt/SUNWam/config/.wtpass
   ```

   在 Linux 系統中：

   ```
   echo "cert-database-password" > /etc/opt/sun/identity/config/.wtpass
   chmod 700 /etc/opt/sun/identity/config/.wtpass
   ```

   其中 *cert-database-password* 爲記號密碼。

5. 檢查 LD_LIBRARY_PATH 變數：

   在 Solaris 系統中，請檢查 LD_LIBRARY_PATH 以了解 /usr/lib、/usr/lib/mps/secv1 和 /usr/lib/mps 目錄是否存在。如果不存在，請新增任何缺少的目錄。

   在 Linux 系統中，檢查 LD_LIBRARY_PATH 以了解 /opt/sun/private/lib 目錄是否存在。如果不存在，請新增目錄。

6. 使用證書資料庫工具 (certutil) 以建立認證與密鑰資料庫。如需有關 certutil 的資訊，請參考下列的網站：

   http://mozilla.org/projects/security/pki/nss/tools/certutil.html

   例如：

   certutil-home/certutil -N -d *cert-database-dir* -f *config-home*/.wtpass

   其中：

   certutil-home 是 certutil 的位置：

   - 在 Solaris 系統中：/usr/sfw/bin
   - 在 Linux 系統中：/opt/sun/private/bin

   cert-database-dir 是證書與密鑰資料庫的資料庫目錄。

   config-home 是 Access Manager 配置檔的位置：

   - 在 Solaris 系統中：/etc/opt/SUNWam/config
   - 在 Linux 系統中：/etc/opt/sun/identity/config

7. 在新建立的證書資料庫中，新增已經安裝在 Access Manager 伺服器中的 SSL 證書的根 CA 證書。例如：

   ```
   certutil-home/certutil -A -n "certificate-nickname" -t "TCu,TCu,TCuw" -d
   cert-database-dir -a -i path-to-file-containing-cert -f config-home/.wtpass
   ```

8. 使用編輯器來檢視 AMConfig.properties 檔案並確認下列值

   - 證書資料庫目錄：com.iplanet.am.admin.cli.certdb.dir
   - 前綴：com.iplanet.am.admin.cli.certdb.prefix
   - 密碼檔：com.iplanet.am.admin.cli.certdb.passfile

     如果內容不符，請視需要編輯。例如，前綴設定應該爲空 (也就是等於 “”)。

9. 如果已經對 AMConfig.properties 進行變更，而且 Access Manager SDK 已部署至 Web 容器，請重新啓動 Web 容器。

使用 DNSAlias 與 JCE 提供者進行 SSL 訊號交換失敗 (#5038876)

當使用 subjectaltname 中具有有效 DNSAlias 名稱的證書時，SSL 與 JCE 提供者進行訊號交換失敗。

過濾器 Init() 中的 Identity 方法造成 Weblogic 故障 (#5016283)

如果篩選的 init() 方法包含 Access Manager 相關的程式碼，則 WebLogic 伺服器將不會啓動。Access Manager API 是以 ServletFilter servlet 的 init 方法來呼叫的。

Access Manager 使用 JSS 作爲安全提供者，但是 WebLogic 依預設會使用 JCE。在啓動 init 方法時，WebLogic 會嘗試使用 JCE 驗證其授權，但是 JSS 正在進行初始化。

解決方法

將 AMConfig.properties 檔案中預設的安全性加密從 JSSEncryption 變更爲 JCEEncryption。

以 “{SSHA}” 符號開頭的任何密碼將無法使用 (#4966191)

Access Manager 不支援在密碼中使用隨機 {SSHA} 符號。

群組建立篩選器選項 – 無 memberURL 屬性 (#4931958)

如果您透過多重 LDAP 過濾器選項 (-f) 建立群組，則該群組不會被正確建立，且僅包含一個 memberURL 屬性。

調校

Solaris-x86 中沒有包括 amtune 和相關檔案 (#6213019)

在此版本中，amtune 程序檔及其相關檔案並不會安裝在 Solaris-x86 的對應目錄當中。

解決方法

使用 Sparc-Solaris 中的 amtune 檔案。

amtune-as8 程序檔會錯誤地建立暫時密碼檔案 (#6212380)

以 amtune 程序檔自動調校 Application Server 8 (amtune-as8) 並沒有作用，因爲是使用 asadmin 密碼建立的暫時密碼檔案。目前檔案中只有密碼。

解決方法

在 amtune-as8 中，請使用下列語法來輸入字串：

```
"TOKEN=Value"
```

例如：

```
"AS_ADMIN_PASSWORD=11111111"
```

輸入此內容變更 amtune-env：

```
#ASADMIN=$CONTAINER_BASE_DIR/bin/asadmin
ASADMIN=/opt/SUNWappserver/appserver/bin/asadmin
```

單次登入

使用不同的部署 URI 無法執行 SSO (#4770271)

如果兩個不同 Access Manager 實例的部署 URI 不同，則單次登入將無法正確發揮作用。

國際化 (i18n)

當群組名稱爲多位元組時，將不會列出群組成員 (#6197041)

在國際版的 Access Manager 6 2005Q1 中，當群組名稱爲多位元組時，將不會在 Access Manager 中列出群組成員。

Linux 中的開始與停止訊息無法讀取 (#6207421)

Access Manager 中 zh/zh_TW 字元集的開始與停止訊息無法讀取。此問題發生於 Linux 平台上。

無法在非英語的語言環境中以 HTTPBasic 和 WindowsDesktopSSO 登入 (#6209324)

您無法在非英語的語言環境中登入 HTTPBasic 和 WindowsDesktopSSO 認證模組。

解決方法

在下列 XML 檔案中將這些參數轉換成英文：

```
HTTPBasic.xml: <HttpHeader>Authorization</HttpHeader>

WindowsDesktopSSO.xml: <HttpHeader>Authorization</HttpHeader>
```

當 Access Manager 部署至 Application Server 時，通常會將這些檔案安裝在下列目錄中：

```
/var/opt/sun/appserver/domains/domain1/applications/j2ee-modules/amserver/config/auth/defa
ult_<lang>
```

當 Access Manager 部署至 Web Server 時，通常會將這些檔案安裝在下列目錄中：

```
/opt/sun/webserver/https-<host>/is-web-apps/services/config/auth/default_<lang>
```

日文線上說明的顯示不正確 (#5024138)

如果您執行的是日文版的 Access Manager 而將語言變更爲 en_US，則仍將顯示日文的說明內容。

解決方法

建立符號連結，從 docs_en 到 docs_en_US。

用戶端偵測服務中移除 UTF-8 無法正常運作(#5028779)

在用戶端偵測服務中，移除 UTF-8 無法正常運作。

解決方法

如果您移除 UTF-8 字元集，請在進行變更後重新啓動 Web 容器。

G11NSetting 中的 charset Q 係數中的空格 (#5008860)

當用戶端資料在 q 係數中或四周有空格，G11NSettings 碼將無法正確剖析，而且會傳回錯誤：

```
ERROR: G11NSettings::Fetchcharset() Unable toparse  charset entry invalid Q  q
```

使用多位元組角色參數登入 ja 字元集的 URL 時，登入頁產生故障 (#4905708)

如果您建立多位元組角色，然後嘗試以註冊多位元組角色的使用者登入 URL，則登入頁將會產生故障錯誤。

解決方法

爲使認證框架解碼 URL 中指定的多位元組角色值，需要隨參數指定 gx_charset。例如：

```
http://hostname:port/amserver/UI/Login?role=manager?role=%E3%81%82%&gx_charset=utf-8
```

記錄檔在 Ja 語言環境中顯示亂碼 (#4882286)

下列記錄檔包含日文字元，在開啓時會顯示爲亂碼：

/var/opt/SUNWam/debug 目錄中的所有檔案，但是 deploy.log 和 undeploy.log 除外。

URL 中的語言環境參數顯示混雜的登入頁面 (#4915137)

如果您使用的是基於非英文的瀏覽器，並且將 Access Manager 實例與 Web Server 一同安裝，則登入 http://*host*:*port*/amserver/UI/Login?locale=en 時，登入頁面顯示的字元既有英文又有非英文。

解決方法

變更以下符號式連結：

AccessManager-base/SUNWam/web-apps/services/config/auth/default

變更爲

AccessManager-base/SUNWam/web-apps/services/config/auth/default_en

Application Server 以 ja 時，登入視窗中顯示的語言環境 (#4932089)

當瀏覽器語言設定爲 en 而 Application Server 的語言環境設定爲 ja 時，Access Manager 登入視窗將無法依預設恢復爲英文。

解決方法

執行語言環境設定爲 en 的 Application Server。

鎖定通知傳送的電子郵件不可讀 (#4938511)

如果您所執行的 Access Manager 之 Web 容器的喜好語言環境設定爲 C 以外的任何語言環境，並且使用者被鎖定於伺服器之外，則系統將傳送鎖定通知電子郵件，但電子郵件不可讀。

解決方法

在「傳送鎖定通知的電子郵件位址」屬性中設定 email|local|charset (而不只是 email 參數)。例如：

```
user1@example.com|zh|GB2312
```

多位元組名稱在自行註冊時無效 (#4732470)

如果您在自我註冊 (成員身份認證服務) 模組中以重複的使用者 ID 和多位元組姓氏和名字建立使用者，將會發生錯誤。不支援多位元組使用者 ID。

解決方法

如果使用者在多位元組環境中使用自我註冊登入，則管理員必須確定沒有選取核心認證中的「使用者產生器模式」屬性。

或

使用者可以在「自我註冊」登入頁中選取「建立自己的」選項。

日文版的 Access Manager 無法與 Netscape 6.22 和 6.23 配合使用 (#4902421)

在日文版 Access Manager 中，您無法使用 Netscape 6.22 或 6.23 登入主控台。

時間條件格式沒有改變 (#4888416)

在策略定義的時間條件中，不論語言環境爲何，以下時間顯示格式均不會改變：

```
Hour:Minute AM/PM
```

「用戶端偵測」畫面未本地化 (#4922013)

在此版本中，「用戶端偵測」介面的「目前樣式特性」畫面部分未本地化。

更新的 genericHTML 用戶端特性中缺少 UTF-8 (#4922348)

如果您從用戶端偵測服務之 genericHTML 用戶端特性中的字元集清單內移除 UTF-8，儲存變更，啓用用戶端偵測，然後登出再登入，登入頁面仍爲 UTF-8 字元集。

解決方法

使用 amserver 手動重新啓動伺服器。

記錄檔標頭未本地化 (#4923536)

所有記錄檔的頭兩行未本地化，特別是 Version 和 Fields 區段及其欄位清單。

amSSO.access 中的資料欄位值未本地化 (#4923549)

在 amSSO.access 記錄檔中，Data 欄位下的所有值都未本地化。

Exception.jsp 具有固化程式碼訊息 (#4772313)

Exception.jsp 未本地化，且包含固化程式碼標題、錯誤訊息以及版權資訊。只有在特別極端的情況下，才會啓動此異常錯誤 jsp 頁。這些情況包括 Directory Server 關閉，或是無法提供 Access Manager 服務並且沒有此 jsp 頁可用的本地化版本。

Cookie

Cookieless 模式無法運作(#4967866)

如果支援 cookie 的瀏覽器存取 Access Manager 並且關閉 cookie 支援的話，瀏覽器會繼續傳送較舊的 Access Manager cookie。這個問題會造成存取 Access Manager 資源被拒絕。

解決方法

選擇下列其中一個解決方法：

- 清除瀏覽器 cookie 快取以移除所有 Access Manager cookie。
- 停用瀏覽器中的 cookie。

Cookie 奪取

當應用程式使用無法信任的瀏覽器作業 cookie 時，可能會有安全性。

在您的 Access Manager 部署中啓用單次登入 (SSO) 或跨網域單次登入時，會在使用者的瀏覽器中設定 http(s) 階段作業 cookie。可以跨多個應用程式驗證這些 cookie。當您跨多個 DNS 網域部署 Access Manager 時，Liberty 協定會將 http(s) 階段作業 cookie 從驗證的 DNS 網域遷移至 Web 應用程式的目標網域。

雖然使用者會自動登入 Web 資源，當應用程式使用無法信任的階段作業 cookie 時，仍然有已知的安全弱點存在。當身份提供者將有關使用者的認證、授權和設定檔資訊提供給由協力廠商或企業中未經授權的群組所開發的應用程式 (或服務提供者) 時，弱點就有可能會出現。可能的安全性問題是：

- 所有應用程式會共用相同的 `http` 階段作業 cookie。這樣有可能會使得惡意的應用程式奪取階段作業 cookie 並在另一個應用程式中假冒使用者。
- 如果應用程式沒有使用 `https` 協定，階段作業 cookie 容易遭到網路竊聽。
- 只要有一個應用程式能夠被奪取，整個基礎架構的安全性就有受到危害的風險。
- Rouge 應用程式可以使用階段作業 cookie 來取得使用者的設定檔屬性並有可能進行修改。如果使用者擁有管理權限，應用程式將能夠造成更大的災害。

解決方法

依照以下步驟：

1. 使用 Access Manager 管理主控台爲每個代理程式建立項目。
   a. 在包含要建立的代理程式的組織中，選擇「檢視」功能表中的「代理程式」，然後按一下「新增」。
   b. 提供以下資訊：

      名稱。輸入代理程式的名稱或身份。例如： `agent123`

      密碼。輸入代理程式密碼。例如： `agent123`

      確認密碼。確認密碼。

      描述。輸入代理程式的簡要描述。例如，您可以輸入代理程式實例名稱或它所保護之應用程式的名稱。

      代理程式鍵值。使用鍵/值對設定代理程式特性。此特性由 Access Manager 用來接收有關使用者憑證假設的代理程式請求。

      輸入 `agentRootURL` 的特性值，此值等於具有連接埠號的代理程式 URL。請注意，`agentRootURL` 值區分大小寫。

      例如： `agentRootURL=http://server_name:99/`

      裝置狀態。輸入代理程式的裝置狀態。如果設定爲「作用中」，代理程式將能夠向 Access Manager 進行認證並與其通訊。如果設定爲「非作用中」，代理程式將不能向 Access Manager 進行認證。

   c. 按一下「確定」。

2. 使用在步驟 1b 中輸入的密碼執行下列指令。

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

   如此將提供下列輸出：

   WnmKUCg/y3l404ivWY6HPQ==

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

```
# The username and password to use for the Application authentication module.


com.sun.am.policy.am.username = agent123
com.sun.am.policy.am.password = WnmKUCg/y3l404ivWY6HPQ==


# Cross-Domain Single Sign On URL
# Is CDSSO enabled.
com.sun.am.policy.agents.cdsso-enabled=true


# This is the URL the user will be redirected to after successful login
# in a CDSSO Scenario.
com.sun.am.policy.agents.cdcservletURL =
http://server.example.com:port/amserver/cdcservlet
```

4. 變更 AMConfig.properties 以反映新值，然後重新啓動 Access Manager。例如：

```
com.sun.identity.enableUniqueSSOTokenCookie=true
com.sun.identity.authentication.uniqueCookieName=sunIdentityServerAuthNServer


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

5. 在 Access Manager 管理主控台中，選擇「服務配置」>「平台」。

6. 在 Cookie 網域清單中，變更 cookie 網域名稱：

   a. 選取預設的 iplanet.com 網域，然後按一下「移除」。

   b. 輸入安裝 Access Manager 的主機名稱，然後按一下「新增」。

   例如： server.example.com

   您應該會在瀏覽器上看見兩組 cookie：

Cookie	主機名稱
iPlanetDirectoryPro	server.example.com
sunIdentityServerAuthNServer	example.com

可再分發的檔案

Sun Java System Access Manager 2005Q1 並沒有包含任何您可以再分發給未授權的產品使用者的檔案。

如何與 Sun 聯絡以取得支援

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

- Sun 軟體支援線上服務，位於 http://www.sun.com/supportraining

  該網站可連結至知識庫、線上支援中心、ProductTracker 以及維護規劃和支援聯絡電話號碼。

- 與您的維護合約相關之電話派遣維護號碼

爲便於我們最有效地協助您解決問題，請在聯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
- 您用於再現問題的方法之詳細步驟
- 所有錯誤記錄檔或記憶體傾印

Sun 歡迎您提出意見

Sun 有志於改善其文件，並歡迎您提出意見和建議。使用 Web 式表單將意見提供給 Sun：

http://www.sun.com/hwdocs/feedback/

請在對應的欄位中提供完整的文件標題以及文件號碼。文件號碼爲 7 或 9 位數，可以在指南的標題頁中或文件頂部找到。例如，這個版本說明的文件號碼是 819-1949。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 817-7642，完整標題爲「Sun Java Enterprise System Access Manager 6 2005Q1 Release Notes」。

其他 Sun 資源

您可在以下網際網路位置找到有用的 Sun Java System 資訊：

- Sun Java System 文件
  http://docs.sun.com/prod/entsys.05q1 與
  http://docs.sun.com/prod/entsys.05q1?l=zh_TW
- Sun Java System 專業服務
  http://www.sun.com/service/products/software/javaenterprisesystem/
- Sun Java System 軟體產品和服務
  http://wwws.sun.com/software/
- Sun Java System 軟體支援服務
  http://www.sun.com/supportraining
- Sun Java System 支援和知識庫
  http://sunsolve.sun.com
- Sun Java System 諮詢和專業服務
  http://www.sun.com/service/products/software/javaenterprisesystem

- Sun Java System 開發人員資訊
  http://developers.sun.com/
- Sun 開發人員支援服務
  http://www.sun.com/developers/support