Sun Java™ System Identity Server 版本說明

版本 2004Q2

文件編號 817-7136

此版本說明包括可以在 Sun Java System Identity Server 2004Q2 發行時取得的重要資訊。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。在您開始使用 Identity Server 2004Q2 之前，請先閱讀本文件。

此版本說明的最新版本可以在 Sun Java System 說明文件網站找到：

http://docs.sun.com/db/prod/entsys.04q2 與
http://docs.sun.com/db/prod/entsys.04q2?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說明文件。

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。

注意 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
2004 年 6 月 23 日	爲支援 Linux 發行的第二版版本說明。在「已知問題」清單中還新增了描述。
2004 年 5 月 18 日	首次發行此版本說明。

關於 Identity Server 2004Q2

Sun Java™ System Identity Server 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。Identity Server 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，Identity Server 無疑是重要的關鍵，也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

Identity Server 2004Q2 中包括以下新功能 (如需這些功能更詳細的說明，請參閱 「*Sun Java System Identity Server Technical Overview*」)：

- 聯合管理的增強功能
  - Identity Federation Framework 1.2
  - Liberty Identity Web Services Framework 1.0
  - Identity Service Instance Specification 1.0
- SAML 1.1 支援
- 自訂的 JAAS Authorization Framework
- 認證的增強功能
  - Windows Desktop SSO 認證服務
  - JAAS 共用狀態
  - Java 資料庫連接性認證模組範例
  - Java 卡數位身份認證模組範例
- Identity Server 主控台的增強功能
  - 巢式群組支援
  - 集中式的代理程式管理
  - 顯示選項與可用動作
- Application Server 的階段作業修復
- 配置與調校程序檔

硬體與軟體需求

本版次 Identity Server 需要以下硬體與軟體。

表 2 硬體與軟體需求

元件	Solaris 需求
作業系統	Solaris™ 作業系統 (OS)，SPARC® Platform Edition，8 和 9 版
	Solaris™ 9 OS，x86 Platform Edition
	Red Hat™ Linux，Advanced Server 2.1 Update 2
RAM	512 百萬位元組
磁碟空間	250 百萬位元組 (用於 Identity Server 及相關的應用程式)

本版次中修正的錯誤

下表說明了在 Identity Server 2004Q2 中修正的錯誤：

表 3 Identity Server 2004Q2 中的錯誤已修正

錯誤識別號	描述
4919897	匿名連結上的認證失敗。
4794971	啓動程序檔未正確刪除。
4922287	子組織名稱中的撇號會導致錯誤。
4925958, 4948665	zh_CN.GB18030 語言環境發生問題。
4921424	韓語字元集的預設全域設定錯誤。
4918930	已取消註冊的服務被錯誤地列爲註冊服務。

安裝注意事項

此 Identity Server 版次會將 Identity Server 套裝軟體的安裝從您必須採取的配置步驟中分開。在此版次中，您必須使用 Java Enterprise System 安裝程式以安裝 Identity Server 的第一個實例。

配置程序檔

在安裝第一個 Identity Server 實例之後，您可以使用 configuration scripts 在 Sun Java System Application Server 以及 Sun Java System Web Server 上建立其他的實例。

IS 安裝/配置程序檔執行下列動作：

- 爲單一主機上的 Web 容器部署其他的 Identity Server 實例。
- 重新配置 Identity Server 實例。例如：變更 Identity Server 實例的所有者和群組 (例如從超級使用者變更爲其他使用者或群組)。
- 使 Web 應用程式可以使用 Identity Server SDK。
- 解除安裝其他實例 (您應該會使用 JES 解除安裝程式來解除安裝第一個實例)。

如需詳細說明，請參閱「*Identity Server 管理指南*」。請注意，目前已不再支援 amserver 指令。

已知問題和限制

本節包含 Identity Server 2004Q2 發行時比較重要的已知問題清單。本節包含以下主題：

- 國際化 (i18n)
- Cookie
- Cookie 奪取

安裝

根字尾的逗號可能會造成安裝失敗 (#4750396)

在安裝期間，當系統要求您指定 Identity Server 根字尾時，請不要在根識別名稱 (RDN) 中使用逗號。

認證

永久的 Cookie 模式屬性不一致 (#5038544)

在永久的 Cookie 模式中，記號中設置的 UserId 屬性不一致。由於這個原因，視 UserID 屬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。

管理員無法從子系組織新增角色 (#5042217)

如果您利用使用者動態設定檔建立角色來設定子組織的認證服務，然後啓用動態設定檔建立以登入服務，則當您檢視使用者屬性時，將沒有角色會被指定，原因是認證服務只允許屬於子組織的角色。

無法在新增代理程式屬性後登入 Identity Server (#4966788)

如果您將代理程式屬性新增至 server.xml，然後重新啓動 Identity Server，您將無法登入 Identity Server 主控台。這個情況僅在代理伺服器無法辨識 Identity Server 時發生。

解決方法

在 server.xml 中，設定 http.nonProxyHosts 爲具有完整主機名稱，然後重新啓動伺服器。例如：

```
<JVMOPTIONS>-Dhttp.nonProxyHosts=Identity_Server_FQDN</JVMOPTIONS>
```

爲了效能的目的，即使代理伺服器能夠辨識 Identity Server，仍然應設定此解決方式中所定義的屬性。

重新載入 [階段作業逾時] 頁面將使用者指派給前使用者名稱與密碼使用者 (#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 Identity Server。

必須設定 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

以 SSL 模式執行 amadmin 時，JVM 可能會中斷 (#5009031)

以安全模式執行伺服器時，連續使用 amadmin 可能會中斷 JVM。

如果您遇到此反應，請聯絡 Sun Java System 軟體支援服務。

am2bak 和 bak2am 程式檔在 Linux 上沒有作用 (#5053866)

am2bak 和 bak2am 復原程序檔在 Linux 上執行的 Identity Server 上無法運作。

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/lsv

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
}
```

在 Linux 系統中，amserver stop 並不會停止 amunixd 程序 (#5050332)

在 Linux 系統中，/etc/init.d/amserver stop 指令並不會停止 amunixd 認證說明程式程序。

解決方法
首先請使用 ps 指令加上 f 選項以決定 amunixd 程序 ID：

```
ps -efl | grep /opt/sun/identity/share/bin/amunixd
```

然後在此程序 ID 中使用 kill 指令以停止 amunixd 程序。

執行 am2bak 時會出現失敗訊息 (#5043752)

在使用 am2bak 執行備份程序時，您可能會收到一個錯誤訊息，表示備份程序已失敗，然而事實上備份程序並未失敗。

amadmin 傳回不正確的錯誤訊息 (#5008960)

amadmin 的 import 選項對所有相關錯誤不正確地拋出相同的錯誤訊息。

僅主控台上的 amverifyarchive 程序 [未列出] 標籤 (#4993375)

如果您執行 Identity Server 僅主控台安裝，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
- PRODUCT_DIR

配置

amconfig 程序檔無法配置本地化的 Identity Server 配置 [以後配置] 選項 (#5062437)

如果您使用 Java Enterprise System 安裝程式安裝了本地化的 Identity Server 2004Q2 版本，而且選擇 [以後配置] 選項，amconfig 程序檔隨後將無法配置 Identity Server。

解決方法
在您執行 amconfig 程序檔之前，請編輯 Web 容器程序檔 (視您使用何種 Web 容器執行 Identity Server)：

1. 找到 Web 容器程序檔：
   - Web Server：amws61config
   - Application Server：amas70config

   這兩個程序檔皆位於 Solaris 系統上的 *IdentityServer_base*/SUNWam/bin 目錄或 Linux 系統上的 *IdentityServer_base*/identity/bin 目錄。
2. 在 Web 容器程序檔中，新增 /WEB-INF 目錄至下列的 if 描述的 $DEPLOY_SRC 變數中：

```
if [ ! -d $DEPLOY_SRC/WEB-INF ]; then
  mkdir -p $DEPLOY_SRC
  cd $DEPLOY_SRC
  jar xf $PKGDIR/$warfile
```

3. 執行 amconfig 程序檔以配置 Identity Server。如需有關 amconfig 程序檔的資訊，請參閱「*Identity Server 2004Q2 管理指南*」：

   http://docs.sun.com/doc/817-7012

請勿使用具有無訊息模式選項的 amconfig (#5003430、5003386、5000964)

請勿使用 amconfig 的互動模式。例如： amconfig -s。結果無法預測。

解決方法
在無訊息模式中啓動 amconfig。例如： amconfig -s *path-to-silent-file*

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

index.ldif 會寫死 userRoot 以便建立屬性索引。可以在位於任何名稱後端資料庫的 rootsuffix 中安裝 Identity Server。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

如果屬性值為空，將會拋出 PP Modify 異常 (#5047103)

當您使用空白的屬性值執行 PP Modify 時，Identity Server 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情況。

策略生效需要伺服器重新啓動 (#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。

Identity Server 主控台

將具有授權存取權限的角色建立為組織管理員時產生錯誤 (#5037978)

如果您是以組織管理員的身份登入並建立一個角色，然後爲其指派存取權限 (例如建立 [組織管理員] 或 [說明桌面管理員] 角色)，您將會收到錯誤訊息。

組織管理員的權限已設定爲使管理員無法修改組織中的任何值。在建立具有權限的角色時，將嘗試修改組織項目中的 ACI。

解決方法

1. 在安裝後，請至 XML 檔案所在的目錄中。依預設，它們是：

   /etc/opt/SUNWam/config/xml (Solaris)

   /etc/opt/sun/identity/config/xml (Linux)

2. 備份 amAdminConsole.xml 檔案。例如：

   cp amAdminConsole.xml amAdminConsole.bak

3. 編輯 amAdminConsole.xml。

   a. 搜尋所有以「S1IS Organization Admin Role access allow read」開始的行，然後刪除該 ACI。例如，刪除所有出現的用於組織管理員角色的 ACI：

      aci:(target="ldap:///ORGANIZATION")(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,dc=iplanet,dc=com)(nsroledn=cn=Top-level Help Desk Admin Role,dc=iplanet,dc=com))))(targetattr != "nsroledn")(version 3.0; acl "S1IS Organization Admin Role access allow read"; allow (read,search) roledn = "ldap:///ROLENAME";)

b. 搜尋所有以「S1IS Organization Admin Role access allow all」開始的行，然後編輯該 ACI 以移除此 ACI 開頭的 '*,'：

aci:(target="ldap:///*,

編輯所有出現的用於組織管理員角色的 ACI。例如：

修改此 ACI：

aci:(target="ldap:///*,ORGANIZATION")(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,dc=iplanet,dc=com)(nsroledn=cn=Top-level Help D esk Admin Role,dc=iplanet,dc=com))))(targetattr != "nsroledn")(version 3.0; acl "S1IS Organization Admin Role access allow all"; allow (all) roledn = "ldap:///ROLENAME?)

爲：

aci:(target="ldap:///ORGANIZATION")(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,dc=iplanet,dc=com)(nsroledn=cn=Top-level Help Desk Admin Role,dc=iplanet,dc=com))))(targetattr !="nsroledn")(version 3.0; acl "S1IS Organization Admin Role access allow all"; allow (all) roledn = "ldap:///ROLENAME";)

c. 儲存此檔案。

4. 使用 amadmin 指令行工具刪除 iPlanetAMAdminConsoleService：

/opt/SUNWam/bin/amadmin -u "uid=amAdmin,ou=People,dc=iplanet,dc=com" -w "iplanet1" -r "iPlanetAMAdminConsoleService"

5. 如果檔案已成功地刪除，將會顯示下列訊息：

Deleting Service Schema iPlanetAMAdminConsoleService

Success 0:Successfully completed.

6. 使用 amadmin 指令行工具重新以新修改的 amAdminConsole.xml 匯入相同的服務：

/opt/SUNWam/bin/amadmin -u "uid=amAdmin,ou=People,dc=iplanet,dc=com" -w "iplanet1" -s /etc/opt/SUNWam/config/xml/amAdminConsole.xml

7. 如果檔案已成功地載入，將會顯示下列訊息：

   Loading Service Schema XML /etc/opt/SUNWam/config/xml/amAdminConsole.xml

   Success 0:Successfully completed.

8. 重新啓動 Identity Server。

未編譯主控台範例 (#5026635)

某些 Identity Server 主控台範例未編譯，原因是此版次已變更檔案的位置。

解決方法

將 rules.mk 檔案中現有的 jato.jar 路徑變更爲下列路徑：

$*USER_DIR*/share/lib/identity/console-war/WEB-INF/lib/jato.jar

使用者無法與SAML 服務同時建立 (#5038600)

只有最頂層的管理員才能夠在指派 SAML 服務的同時建立使用者

解決方法

組織管理員需要在沒有 SAML 服務的情況下建立使用者。一旦使用者建立之後，管理員可以透過 [使用者設定檔] 頁面新增服務。

按 [上一步] 按鈕時，數值將無法保留 (#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回復。

策略管理員無法修改自己的設定檔(#5042100)

策略管理員無法透過 Identity Server 主控台修改他/她自己的設定檔。

解決方法

將 [導覽檢視] 的顯示選項設定爲 [使用者]，而將使用者的 [可用動作] 設定爲 [完全存取權]。

當使用者管理停用時，執行搜尋使用者，主控台將會發生錯誤(#5049218)

如果使用者管理已停用而您執行搜尋使用者的動作，您可能會收到伺服器錯誤的訊息。

解決方法

將 PMAdminRoldSelect.jsp 以新的 JSP 來取代。它可以在下列的位置中找到：

IdentityServer_base/applications/console/policy

實體描述搜尋篩選器無法正常運作(#4959895)

在 [聯合模組] 的 [實體描述元] 檢視中，如果您使用 [搜尋] 欄位來尋找實體描述元，則搜尋結果有時會不準確。

「**」搜尋選單沒有作用 (#4961370)

如果您在 Identity Server 主控台中使用「**」而沒有使用額外字元作爲搜尋篩選器遮罩，則搜尋將會失敗。搜尋欄位接受包含額外字元的「**」，例如 **a 或 a**。

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)

Identity Server 主控台 [導覽] 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 80 作爲 Identity Server 連接埠號碼，或是在執行 https 時不應該使用 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 可能無效。

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

在參考策略規則中所做的修改並未反映在子組織中 (#5016725)

在刪除根組織的參考策略之後，子組織中的一般策略規則並未刪除 (而且無法刪除)。

在到達 nslookthrough 限制時並未傳回符合的項目 (#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 Identity Server 主控台。

解決方法

調校 nslookthroughlimit 參數以補償項目數。

別名underlying 未強制策略 (#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 Identity Server，然後嘗試存取受保護的資源，則存取將會被拒絕。

策略範例問題 (#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。爲執行範例，LD_LIBRARY_PATH 需要包括 NSPR、NSS 以及 JSS 共用程式庫的路徑。

將環境變數 LD_LIBRARY_PATH 設定爲 /usr/lib/mps/secv1 (Solaris 適用) 或 /opt/sun/pirvate/lib (Linux)。如果未正確設定此項，則將發生錯誤。

階段作業服務

不能清除閒置階段作業 (#4959071)

目前不能正確清除閒置階段作業。請與支援人員聯絡，以取得解決此問題的修補程式。如需詳細資料，請參閱如何報告問題和提供回饋。

SDK

在使用 SSL 與啓用 Identity Server SDK 的機器上使用 certutil 時發生 (#5027614)

使用者嘗試從僅安裝 SDK 的機器與啓用 SSL 的 Identity Server 2004Q2 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，是在無 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 Identity Server SDK。

解決方法
在僅安裝 SDK 的機器上建立證書資料庫，並將 Identity Server 伺服器的根 CA 認證安裝至此資料庫：

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 目錄是否已經存在，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 Identity Server 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 Identity Server 伺服器中的 SSL 認證的根 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 Identity Server 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。

BasicEntitySearch 篩選器不會對 uid (#5041529)

如果您在安裝 Identity Server 時是將使用者命名屬性設定爲 cn，然後登入 Identity Server 主控台並建立代理實體，則代理實體將不會在瀏覽窗格中顯示。這是由於實體搜尋範本已寫死至 uid。

解決方法

從 Directory Server 管理主控台將篩選器從 uid 變更爲 cn，然後重新啓動伺服器。

篩選器 Init() 中的 Identity 方法造成 Weblogic 故障 (#5016283)

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

Identity Server 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無法使用 (#4966191)

Identity Server 不支援在密碼中使用隨機 {SSHA} 符號。

AMConfig.properties 中的 smtp Server Port 屬性不正確 (#5048378)

AMConfig.properties 中的 smtp server port 屬性不正確。已傳送郵件尋找 com.iplanet.am.smtpport 的方式不正確。

命名屬性應爲小寫 (#4931163)

由於 SDK 中的限制，命名屬性必須爲小寫。例如，如果您在 Directory Server 上安裝 Identity Server 實例，並在使用者命名屬性定義爲 CN 的情況下載入 Identity Server 模式，則建立使用者將失敗。

解決方法

在 Directory Server 主控台中變更命名屬性。例如，將建立範本的 basicuser 使用者命名屬性從 CN 變更爲 cn。

群組建立選項會產生 – 個 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。

服務註冊問題 (#4853809)

如果您建立服務範本並在父系組織中註冊它們，然後嘗試爲子組織註冊它們，則在父系組織中註冊的某些服務不會被註冊，但 amConsole.access 卻顯示這些服務已被註冊。

解決方法

更新 Identity Server 主控台並重新註冊這些服務。

「服務類型」角色的使用者登入時服務消失 (#4931907)

如果「服務類型」角色中的使用者在管理員啓動視區設定爲 orgDN 的情況下登入 Identity Server，然後嘗試取消註冊服務，則所有列出的服務都會消失。

解決方法

重新啓動伺服器，則所有服務會重新顯示。

單次登入

使用不同的部署 URI 無法執行 SSO (#4770271)

如果兩個不同 Identity Server 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)

並非所有服務都並非所有已註冊的服務 (#4853809)

如果您透過 Identity Server 主控台註冊所有服務，則某些服務不能列在 [可用服務] 中。

解決方法

請勿按下 [新增] 按鈕超過一次以上。

自含式註冊的服務在使用者顯示為「已新增」(#4996479)

在新增服務至使用者時，wsrp 使用者服務將顯示爲可用。但是如果已經被選擇，它將不會被新增，因此將會失敗。再者，如果多重服務和使用者服務一同檢查，則所有新增的服務都會失敗。

解決方法

不要從身份管理模組新增 WSRP 服務。

日文瀏覽器中的 Authlevel 登入失敗 (#5013994)

當您初次依認證級別登入 Identity Server 時，如果您的瀏覽器語言設定爲 ja，則它將無法在下列的日文瀏覽器中運作：

- IE6.0ja
- IE7.0ja
- Mozilla1.2.1

解決方法

當出現「Authentication Module has Denied」(認證模組被拒絕) 錯誤時，請按一下「Go Back To Login Page」(返回登入頁) 連結。您也可以輸入下列 URL：

http://*server*:*port*/amserver/UI/Login?*authlevel*=*number*

日文線上說明的顯示不正確 (#5024138)

如果您執行的是日文版的 Identity Server 而將語言變更爲 en_US，則仍然將會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。

使用者 ID 產生模式會從名字 / 姓氏產生使用者 ID (#5028750)

Identity Server 並不支援多位元組使用者 ID。依預設，使用者 ID 產生模式會從名字和姓氏產生使用者 ID。

用戶端偵測服務無法正常運作 (#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 並不處理 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 子集的 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

日誌檔在 Ja 區域環境中無法讀取 (#4882286)

下列日誌檔包含日文字元，在開啓時會顯示爲亂碼：

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

URL 中的區域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 Identity Server 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：

I*dentityServer_base*/SUNWam/web-apps/services/config/auth/default

爲

IdentityServer_base/SUNWam/web-apps/services/config/auth/default_en

HTTP Basic 的錯誤訊息未本地化 (#4921418)

如果使用 HTTP Basic 認證模組登入，則按一下 [取消] 按鈕，螢幕上會顯示非本地化錯誤訊息。此爲 Application Server 的已知問題；它僅會在 Identity Server 與 Application Server 共同部署時發生。

Application Server 的 ja 等，[登入] 視窗中的預設語言環境 (#4932089)

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

解決方法

執行語言環境設定爲 en 的 Application Server。

鎖定通知傳送不可讀的電子郵件 (#4938511)

如果您所執行的 Identity Server 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

在修正的語言環境中的衝突解決層級 (#4922030)

如果使用者以特定語言環境 (例如，zh) 登入 Identity Server 主控台，註冊 [認證配置] 服務，建立服務範本，然後登出再以不同的語言環境重新登入，[衝突解決層級] 項目將會以原始語言環境格式的方式不正確地列出。

am2bak 和 bak2am 時之訊息僅爲英文 (#4930610)

am2bak 和 bak2am 復原公用程式的版本訊息在此版次中僅有英文版。

多位元組名稱在自我註冊中無效 (#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 Identity Server 無法與 Netscape 6.22 和 6.23 配合使用 (#4902421)

在日文版 Identity Server 6.1 中，您無法使用 Netscape 6.22 或 6.23 登入主控台。

時間條件格式不變 (#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變：

Hour:Minute AM/PM

backup_restore.po 中 msgid-msgstr 對的訊息未本地化 (#4916683)

如果收到說明 backup_restore.po 程序檔中遺漏 msgid-mgstr 對且 Directory Server 證書未備份的訊息，仍會備份 Directory Server 證書。本訊息未被本地化。

[用戶端偵測] 畫面未本地化 (#4922013)

在本版次中，[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 用戶端特性未移除 (#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，請儲存變更，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。

日誌檔標頭未本地化 (#4923536)

所有日誌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 日誌檔中，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，或是當無法帶出 Identity Server 服務，以及沒有此 jsp 頁可用的本地化。

Cookie

Cookieless 模式未運作(#4967866)

如果瀏覽器存取 Identity Service 而關閉 cookie 支援，而且如果瀏覽器支援 cookie，則瀏覽器會繼續傳送較舊的 Identity Server cookie。這樣會造成存取 Identity Server 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 Identity Server cookie。
- 停用瀏覽器中的 cookie。

Cookie 奪取

當應用程式使用無法信任的階段作業 cookie 時，可能會有安全性。

在您的 Identity Server 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 Identity Server 時，Liberty 協定會將 `http(s)` 階段作業 cookie 從驗證的 DNS 網域移轉至 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驗證、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 rouge 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 Identity Server 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 / 值對設定代理程式內容。此內容由 Identity Server 用來接收有關使用者憑證假設的代理程式請求。

      輸入 `agentRootURL` 的屬性值，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 Identity Server 進行認證並與之通訊。如果設定爲 [非作用中]，代理程式將不能向 Identity Server 進行認證。

   c. 按一下 [確定]。

2. 使用在步驟 2b 中輸入的密碼執行下列指令。

   /opt/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
```

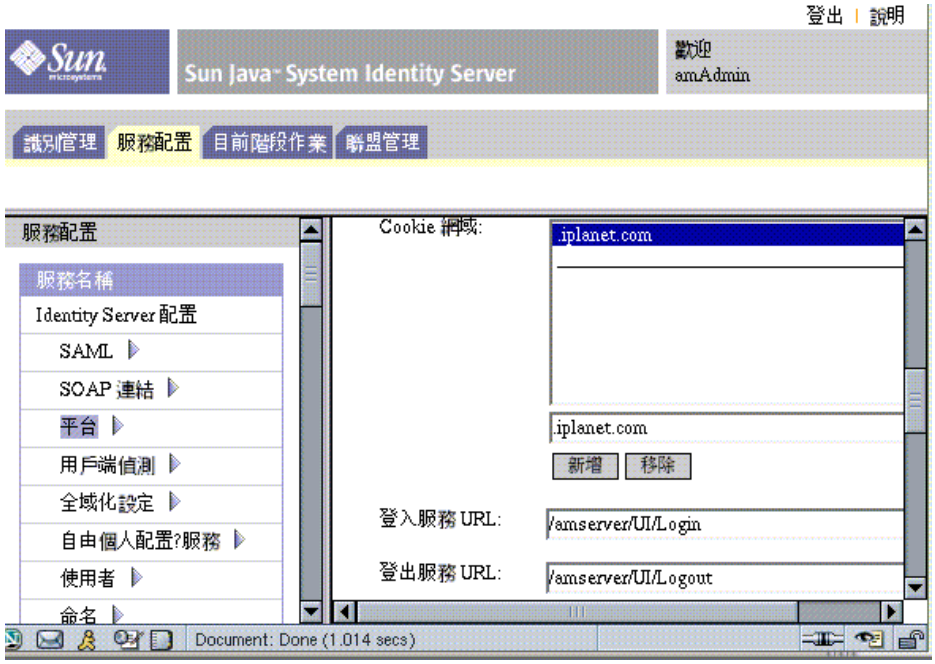
4. 變更 AMConfig.properties 以反映新值，然後重新啓動 Identity Server。例如：

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

com.sun.identity.authentication.uniqueCookieName=sunIdentityServerAuthNServer


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

5. 在 Identity Server 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 Identity Server 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`

可重新分配的檔案

Sun Java System Identity Server 2004Q2 沒有包含任何您可以重新分配的檔案。

如何與 Sun 聯絡以提供回饋

如果您遇到有關 Sun Java System Identity Server 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的熱線電話號碼

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
- 所有錯誤日誌或記憶體傾印

Sun 歡迎您提出意見

Sun 有志於改善其說明文件，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://docs.sun.com/db/coll/IdentityServer_04q2 與
http://docs.sun.com/db/coll/IdentityServer_04q2_zh_TW

請在對應的欄位中提供完整的文件標題以及文件編號。文件編號爲 7 或 9 位數，可以在指南的標題頁中或文件頂部找到。例如，這個版本說明文件的文件編號是 817-7136。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 817-5712，完整標題爲「Sun Java Enterprise System Identity Server 2004Q2 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 說明文件
  http://docs.sun.com/db/prod/entsys.04q2 與
  http://docs.sun.com/db/prod/entsys.04q2 ?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 開發人員支援服務
  http://www.sun.com/developers/support