Sun Java System Access Manager 7 2005Q4 版本說明

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

文件號碼：819–3476
2008 年 8 月 19 日

080909@20795

目錄

Sun Java System Access Manager 7 2005Q4 版本說明

2008 年 8 月 19 日

文件號碼 819-3476

此「Sun Java™ System Access Manager (Access Manager) 7 2005Q4 版本說明」包含 Sun Java Enterprise System (Java ES) 發行時可用的重要資訊，包括 Access Manager 的新增功能與已知問題及其解決方法 (如有提供)。安裝和使用此版本之前，請先閱讀本文件。

如需有關此版本之版本說明的資訊，請參閱第 6 頁的 「修訂歷程記錄」。

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` 及 `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。

目錄

「Access Manager 7 2005Q4 版本說明」包含下列各節：

修訂歷程記錄

下表顯示「Access Manager 7 2005Q4 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
2008 年 8 月 19 日	在 第 9 頁的 「Access Manager 7 2005Q4 修補程式版本」一節中增加了適用於 Windows 與 HP-UX 系統的修補程式 7 的資訊。
2008 年 5 月 12 日	■ 在 第 9 頁的 「Access Manager 7 2005Q4 修補程式版本」一節增加了關於修補程式 7 的資訊。 ■ 增加了第 63 頁的 「系統虛擬支援」一節。
2007 年 10 月 16 日	此修訂中所做的變更包括： ■ 在第 9 頁的 「Access Manager 7 2005Q4 修補程式版本」一節加入了關於修補程式 6 的資訊。 ■ 更新了第 39 頁的 「CR# 6522720：在 Windows 與 HP-UX 系統上，無法在主控台線上說明中搜尋多位元組字元」。修補程式 6 修正了 Windows 系統中的這個問題。然而，HP-UX 系統中仍存在此問題。
2007 年 7 月 10 日	此修訂中所做的變更包括： ■ 在第 9 頁的 「Access Manager 7 2005Q4 修補程式版本」一節加入了關於適用於 HP-UX 系統的修補程式 126371-05 的資訊。 ■ 加入了下列新問題：第 77 頁的 「若 Access Manager 指向 Directory Proxy，則空屬性 LDAP 搜尋會傳回錯誤 (6357975)」。
2007 年 3 月 16 日	此修訂中所做的變更包括： ■ 在第 9 頁的 「Access Manager 7 2005Q4 修補程式版本」一節加入了關於修補程式 5 的資訊。 ■ 在第 85 頁的 「文件問題」中加入了說明和新資訊。 ■ 根據審核者的意見與變更請求 (Change Request, CR) 進行了各種技術性和編輯上的變更。

表 1 修訂歷程記錄 (續)

日期	變更說明
2006 年 10 月 30 日	在第 9 頁的「Access Manager 7 2005Q4 修補程式版本」一節中的變更包括： ■ 加入了關於修補程式 4 的資訊。 ■ 更正了 *AccessManager-base* 使用上的不一致。 ■ 修訂了第 47 頁的「CR# 6440651：Cookie 重送需要 `com.sun.identity.session.resetLBCookie` 特性」的描述。
2006 年 8 月 25 日	在第 9 頁的「Access Manager 7 2005Q4 修補程式版本」一節中的變更包括： ■ 加入了關於修補程式 3 的資訊。 ■ 修訂並加入了關於修補程式 1 及 2 的資訊。
2006 年 5 月 25 日	此修訂中所做的變更包括： ■ 加入了新的第 50 頁的「Access Manager 7 2005Q4 修補程式 2」一節。 ■ 在表 4 中加入了關於對 HP-UX 與 Microsoft Windows 平台的支援的資訊。 ■ 在第 85 頁的「文件問題」中加入了下列問題： ■ 第 89 頁的「「版本說明」中對已知問題的解決方法有錯 (6422907)」 ■ 第 89 頁的「記錄 `AMConfig.properties` 中的 `com.iplanet.am.session.protectedPropertiesList` (6351192)」
2006 年 2 月 9 日	修訂了第 91 頁的「文件更新」，列出自從首次發行之後所出版的新的與修訂過的 Access Manager 7 2005Q4 文件。
2006 年 2 月 7 日	此修訂中所做的變更包括： ■ 在第 65 頁的「已知問題和限制」中加入了下列問題： ■ 第 68 頁的「將 Access Manager 和 Directory Server 安裝在不同機器上時，認證服務沒有初始化 (6229897)」 ■ 第 69 頁的「Access Manager `ampre70upgrade` 程序檔不會移除本土化的套裝軟體 (6378444)」 ■ 更新了第 91 頁的「文件更新」一節。

表 1 修訂歷程記錄 (續)

日期	變更說明
2006 年 1 月 18 日	此修訂中所做的變更包括： ■ 加入了新的第 54 頁的 「Access Manager 7 2005Q4 修補程式 1」一節。 ■ 修改了第 58 頁的 「分散式認證」中的描述，使之更易於瞭解。 ■ 在第 61 頁的 「硬體與軟體需求」中詳述了對 Solaris 10 區域的支援並加入了對 AMD64 平台上之 Solaris 10 OS 的支援。 ■ 在第 65 頁的 「已知問題和限制」中加入了下列問題： ■ 第 73 頁的 「使用 RSA 金鑰時，IBM WebSphere 中的 URL 簽署失敗 (6271087)」 ■ 第 82 頁的 「在 Application Server 上執行 Access Manager 時發生 JVM 問題 (6223676)」 ■ 第 82 頁的 「執行 Web 服務範例時傳回 [找不到資源提供](6359900)」 ■ 第 67 頁的 「套用修補程式 1 後，所有使用者皆有讀取 `/tmp/amsilent` 檔案的權限 (6370691)」 ■ 第 71 頁的 「於資料遷移之後增加 `ContainerDefaultTemplateRole` 屬性 (4677779)」 ■ 第 90 頁的 「記錄可支援 LDAPv3 外掛程式的角色和已篩選角色 (6365196)」 ■ 第 90 頁的 「記錄 `AMConfig.properties` 檔案中未使用的特性 (6344530)」 ■ 第 90 頁的 「記錄如何啓用 XML 加密 (6275563)」 ■ 加入了新的第 91 頁的 「文件更新」一節。
2005 年 11 月 8 日	針對與支援之 LDAP 版本 3 (LDAP v3) 相容的儲存庫，修訂了第 56 頁的 「識別儲存庫」。
2005 年 10 月 3 日	初期測試版。
2005 年 6 月 30 日	後期測試版。

關於 Sun Java System Access Manager 7 2005Q4

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
- 用於存取組織的網路型應用程式的單次登入 (Single Sign-On, SSO)
- 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。

Access Manager 7 2005Q4 修補程式版本

從 SunSolve Online 可以下載 Access Manager 7 2005Q4 修補程式的最新修訂：`http://sunsolve.sun.com`。最新的修補程式 ID 是：

- 基於 SPARC® 之系統上的 Solaris™ 作業系統 (Solaris OS)：**120954-07**
- x86 平台上的 Solaris OS：**120955-07**
- Linux 系統：**120956-07**
- Microsoft Windows 系統：**124296-07**
- HP-UX 系統：**126371-07**

備註 – Access Manager 7 2005Q4 修補程式是累增的。您可在未安裝修補程式 1、2、3、4、5 或 6 的情況下安裝修補補程式 7。但若您未安裝更舊的修補程式，請檢閱關於更舊之修補程式的小節中介紹的新增功能與問題，以判斷是否存在與您的部署相關的功能與問題。

Access Manager 7 2005Q4 修補程式的相關資訊包括：

- 第 9 頁的 「Access Manager 7 2005Q4 修補程式 7」
- 第 11 頁的 「安裝前注意事項」
- 第 14 頁的 「修補程式安裝說明」
- 第 18 頁的 「安裝後注意事項」
- 第 21 頁的 「Access Manager 7 2005Q4 修補程式 6」
- 第 25 頁的 「Access Manager 7 2005Q4 修補程式 5」
- 第 39 頁的 「Access Manager 7 2005Q4 修補程式 4」
- 第 41 頁的 「Access Manager 7 2005Q4 修補程式 3」
- 第 50 頁的 「Access Manager 7 2005Q4 修補程式 2」
- 第 54 頁的 「Access Manager 7 2005Q4 修補程式 1」

Access Manager 7 2005Q4 修補程式 7

Access Manager 7 修補程式 7 (修訂版 07) 修正了許多問題，這些問題列於修補程式隨附的讀我檔案中。

修補程式 7 包括下列變更：

- 第 10 頁的 「CR# 6637806：重新啓動後，Access Manager 傳送無效的應用程式 SSO 記號給代理程式」
- 第 10 頁的 「CR# 6612609：如果網路電纜與 Message Queue 伺服器的連線中斷，階段作業容錯移轉便會發揮作用」

- 第 10 頁的 「CR# 6570409：負載平衡器後方的互動服務可作爲「識別提供者」正常運作」
- 第 11 頁的 「CR# 6545176：重新導向 URL 可在認證後續處理 SPI 外掛程式中動態設定」

CR# 6637806：重新啓動後，Access Manager 傳送無效的應用程式 SSO 記號給代理程式

在 Access Manager 伺服器重新啓動後，Access Manager 用戶端 SDK 現在會傳送有意義的異常給代理程式，因此代理程式可重新認證其自身，以取得新的應用程式階段作業。以前在套用 Access Manager 7 2005Q4 修補程式 5 後，Access Manager 用戶端 SDK 會在 Access Manager 重新啓動之後傳送無效的應用程式 SSO 記號給代理程式。

這個問題已透過重複的 CR 6496155 修復。修補程式 7 也提供了一個選項 (`comp.iplanet.dpro.session.dnRestrictionOnly` 特性) 以便在限制環境中傳送應用程式 SSO 記號。依預設，代理程式會傳送安裝代理程式之伺服器的 IP 位址，但如果必須執行嚴格的 DN 檢查，則依下列方式在 `AMConfig.properties` 檔案中設定此特性：

```
com.iplanet.dpro.session.dnRestrictionOnly=true
```

CR# 6612609：如果網路電纜與 Message Queue 伺服器的連線中斷，階段作業容錯移轉便會發揮作用

在階段作業容錯移轉部署中，如果每個 Access Manager 實例與 Message Queue 代理程式安裝在相同的伺服器上，當網路電纜與其中一個伺服器的連線中斷時，階段作業容錯移轉便會發揮作用。依預設，Message Queue `imqAddressListBehavior` 連線出廠屬性設定爲 `PRIORITY`，這會導致 Message Queue 按照位址在代理程式位址清單中出現的順序來嘗試位址 (例如：`localhost:7777,server2:7777,server3:7777`)。如果屬性設定爲 `RANDOM`，則會以隨機順序嘗試位址。

若要將此屬性設定爲 RANDOM，請在 `amsessiondb` 程序檔中設定下列參數：

```
-DimqAddressListBehavior=RANDOM
```

如需 Message Queue 之 `PRIORITY` 與 `RANDOM` 屬性的資訊，請參閱「Sun Java System Message Queue 3.7 UR1 管理指南」中的「代理程式位址清單」。

CR# 6570409：負載平衡器後方的互動服務可作為「識別提供者」正常運作

如果部署中有兩部伺服器與負載平衡器連接並作爲單一「識別提供者」運作，您必須在 `AMConfig.properties` 檔案中設定下列特性：

```
com.sun.identity.liberty.interaction.lbWspRedirectHandler
com.sun.identity.liberty.interaction.trustedWspRedirectHandlers
```

目前唯一支援的類別是
`com.sun.identity.liberty.interaction.interactionConfigClass`。因此，依預設會使用與 Federation Liberty 隨附的互動配置類別存取互動配置參數。

CR# 6545176：重新導向 URL 可在認證後續處理 SPI 外掛程式中動態設定

重新導向 URL 現在可在認證後續處理 SPI 外掛程式中，針對登入成功、登入失敗與登出進行動態設定 。如果未執行後續處理外掛程式，就不會使用在後續處理 SPI 中設定的重新導向 URL，而是像先前一樣執行由其他任何方式設定的重新導向 URL。

如需詳細資訊，請參閱
`com.iplanet.am.samples.authentication.spi.postprocess.ISAuthPostProcessSample.java`
範例。

安裝前注意事項

- 第 11 頁的 「備份檔案」
- 第 13 頁的 「安裝及配置 Access Manager」

備份檔案

重要 如果在目前的安裝中有任何自訂的檔案，則在安裝修補程式之前，請先備份這些檔案。安裝修補程式之後，請比較備份的檔案與修補程式安裝的新檔案，以識別出自訂的部分。將自訂的部分與新檔案合併，並儲存它們。如需如何處理自訂檔案的更多資訊，請閱讀下列資訊。

安裝修補程式之前，亦請備份下列檔案。

Solaris 系統	■ *AccessManager-base*/SUNWam/bin/amsfo ■ *AccessManager-base*/SUNWam/lib/amsfo.conf ■ /etc/opt/SUNWam/config/xml/template/ 目錄中的檔案：idRepoService.xml、amSOAPBinding.xml、amDisco.xml、amAuthCert.xml、amAuth.xml、amSession.xml ■ *AccessManager-base*/SUNWam/locale/ 目錄中的檔案：amConsole.properties、amIdRepoService.properties、amAuthUI.properties、amAuth.properties、amPolicy.properties、amPolicyConfig.properties、amSessionDB.properties、amSOAPBinding.properties、amAdminCLI.properties、amSDK.properties、amAuthLDAP.properties、amSession.properties、amAuthContext.properties、amSAML.properties、amAuthCert.properties
Linux 和 HP-UX 系統	■ *AccessManager-base*/identity/bin/amsfo ■ *AccessManager-base*/identity/lib/amsfo.conf ■ /etc/opt/sun/identity/config/xml/template/ 目錄中的檔案：idRepoService.xml、amSOAPBinding.xml、amDisco.xml、amAuthCert.xml、amAuth.xml、amSession.xml ■ *AccessManager-base*/identity/locale/ 目錄中的檔案：amConsole.properties、amIdRepoService.properties、amAuthUI.properties、amAuth.properties、amPolicy.properties、amPolicyConfig.properties、amSessionDB.properties、amSOAPBinding.properties、amAdminCLI.properties、amSDK.properties、amAuthLDAP.properties、amSession.properties、amAuthContext.properties、amSAML.properties、amAuthCert.properties

Windows 系統	■ *AccessManager-base*\identity\setup\AMConfigurator.properties ■ *AccessManager-base*\identity\bin\amsfo ■ *AccessManager-base*\identity\lib\amsfo.conf ■ *AccessManager-base*\identity\config\xml\template 目錄中的檔案： idRepoService.xml、amSOAPBinding.xml、amDisco.xml、amAuthCert.xml、amAuth.xml、amSession.xml ■ *AccessManager-base*\identity\locale 目錄中的檔案： amConsole.properties、amIdRepoService.properties、amAuthUI.properties、amAuth.properties、amPolicy.properties、amPolicyConfig.properties、amSessionDB.properties、amSOAPBinding.properties、amAdminCLI.properties、amSDK.properties、amAuthLDAP.properties、amSession.properties、amAuthContext.properties、amSAML.properties、amAuthCert.properties

AccessManager-base 爲基底安裝目錄。預設的基底安裝目錄視平台而定：

- Solaris 系統：/opt
- Linux 和 HP-UX 系統：/opt/sun
- Windows 系統：*javaes-install-directory*\AccessManager。例如：C:\Program Files\Sun\AccessManager

安裝及配置 Access Manager

安裝本文件中描述的 Access Manager 修補程式時不會安裝 Access Manager。在安裝修補程式之前，伺服器上必須已經安裝 Access Manager 7 2005Q4。如需有關安裝的資訊，請參閱「Sun Java Enterprise System 2005Q4 安裝指南」。

如果在 Windows 系統上安裝修補程式，請參閱「Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows」。

您同樣應該熟悉執行 amconfig 程序檔以部署、重新部署與配置 Access Manager 的步驟，如「Sun Java System Access Manager 7 2005Q4 管理指南」中的第 1 章「Access Manager 7 2005Q4 配置程序檔」中所述。

若要取得由此修補程式淘汰的 Access Manager 修補程式清單，以及在安裝此修補程式之前必須安裝的任何修補程式，請參考此修補程式隨附的讀我檔案。

注意 – 將 Access Manager 修補程式 (以及其他任何修補程式) 用於生產環境之前，應該先在分段系統或部署前系統上測試它們。此外，修補程式安裝程式可能無法正確更新自訂的 JSP 檔案，因此可能需要在這些檔案中進行手動變更，才能使 Access Manager 正常運作。

修補程式安裝說明

適用於 Solaris 系統的修補程式安裝說明

在您安裝 Solaris 修補程式之前，請確定已備份列於第 11 頁的 「安裝前注意事項」中的檔案。

若要在 Solaris 系統上增加及移除修補程式，請使用 OS 提供的 `patchadd` 及 `patchrm` 指令。

patchadd 指令

使用 `patchadd` 指令可以在獨立式系統上安裝修補程式。例如：

```
# patchadd /var/spool/patch/120954-07
```

備註 – 如果您是將 Solaris 修補程式安裝在 Solaris 10 全域區域中，請呼叫含有 `-G` 引數的 `patchadd` 指令。例如：

```
patchadd -G /var/spool/patch/120954-07
```

`postpatch` 程序檔會顯示關於重新部署 Access Manager 應用程式的訊息，除非系統中只安裝了 Access Manager SDK 元件。

`postpatch` 程序檔會在以下目錄中建立 `amsilent` 檔案：

- Solaris 系統：*AccessManager-base*`/SUNWam`
- Linux 系統：*AccessManager-base*`/identity`

AccessManager-base 爲基底安裝目錄。預設基底安裝目錄在 Solaris 系統上爲 `/opt`，在 Linux 系統上爲 `/opt/sun`。

`amsilent` 基於 `amsamplesilent` 檔案，但根據系統上的 Access Manager 配置檔案設定了一些必要的參數。但是密碼參數包含預設值。請依照您的部署需求取消註釋並修改每個密碼參數的值，並且仔細檢查這個檔案中其他參數的值。

COMMON_DEPLOY_URI 參數 (共用網域 Web 應用程式的 URI 前綴) 亦包含預設值。如果您已爲此 URI 選擇了非預設值，請務必更新此值。否則，以 amconfig 和修補程式產生的 amsilent 檔案進行 Web 應用程式的重新部署時會失敗。

然後，執行下列指令 (以安裝在預設目錄中的 Access Manager 爲例)：

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

注意 – amsilent 檔案中包含一般文字形式的機密資料 (如管理員密碼)，因此請您務必妥善保管進行部署時所需要的檔案。

在您執行 amconfig 程序檔後，請執行 updateschema.sh 程序檔以載入 XML 和 LDIF 檔案。安裝修補程式 7 之後，就可在下列目錄中找到 updateschema.sh 程序檔：

- Solaris SPARC 系統：*patch-home-directory* /120954-07
- Solaris x86 系統：*patch-home-directory*/120955-07

執行 updateschema 程序檔之後，重新啓動 Access Manager 程序。例如：

```
# cd /opt/SUNWam/bin
# ./amserver stop
# ./amserver start
```

然後重新啓動 Access Manager Web 容器。

patchrm 指令

使用 patchrm 指令可以從獨立式系統移除修補程式。例如：

```
# patchrm 120954-03
```

backout 程序檔顯示的訊息與 patchadd 指令的類似，除非系統中只安裝了 Access Manager SDK 元件。

移除修補程式後，請使用 *AccessManager-base*/SUNWam 目錄中的 amsilent 檔案重新部署 Access Manager 應用程式，其中 *AccessManager-base* 爲基底安裝目錄。在 Solaris 系統上，預設基底安裝目錄爲 /opt。

依照您的部署需求在 amsilent 檔案中設定參數。

然後執行下列指令 (以安裝在 Solaris 系統上預設目錄中的 Access Manager 爲例)：

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

如需有關 patchadd 及 patchrm 指令的附加資訊及範例，請參閱對應的 Solaris **線上手冊**。

另請參閱第 18 頁的 「安裝後注意事項」，以瞭解更多資訊。

Solaris 10 區域

Solaris 10 作業系統推出了「區域」新概念。因此，patchadd 指令也包含新的 -G 選項，該選項只將修補程式加入全域區域。依預設，patchadd 指令在要修補之套裝軟體的 pkginfo 中尋找 SUNW_PKG_ALLZONES 變數。但是，對於所有 Access Manager 套裝軟體，SUNW_PKG_ALLZONES 變數都沒有設定。如果 Access Manager 7 2005Q4 安裝於全域區域，則需要 -G 選項。如果 Access Manager 安裝於本機區域，則 patchadd -G 選項沒有效果。

如果您要在 Solaris 系統上安裝 Access Manager 7 2005Q4 修補程式，建議您使用 -G 選項。例如：

```
# patchadd -G AM7_patch_dir
```

同樣地，如果 Access Manager 安裝於全域區域，則需要 -G 選項才能執行 patchrm 指令。例如：

```
# patchrm -G 120954-07
```

適用於 Linux 系統的修補程式安裝說明

在您安裝 Linux 修補程式之前，請確定已備份列於第 11 頁的 「安裝前注意事項」中的檔案。

installpatch 可以在獨立式 Linux 系統上安裝修補程式。例如：

```
# ./installpatch
```

postpatch 程序檔輸出與 Solairs 系統上的訊息類似的訊息。但是，在 Linux 系統上取消修補程式的程序與 Solaris 系統上的不同。沒有用於取消 Linux 修補程式的通用程序檔。如果先前已安裝版本較低的修補程式，則可以重新安裝該版本，然後遵循修補後說明透過執行 amconfig 程序檔來重新部署 Access Manager 應用程式。

在您執行 amconfig 程序檔後，請執行 updateschema.sh 程序檔 (修補程式 5 及更新的修補程式) 以載入 XML 和 LDIF 檔案。當您安裝修補程式 7 之後，就可在 *patch-home-directory*/120956-07/scripts 目錄中找到 updateschema.sh 程序檔。

在您執行 amconfig 和 updateschema.sh 程序檔後，請重新啓動 Access Manager Web 容器。

如果修補程式安裝在 Access Manager 7 2005Q4 RTM 發行版本上，而且您想要移除該修補程式並將系統復原到 RTM 狀態，則您必須使用 reinstallRTM 程序檔來重新安裝 Access Manager RTM 套裝軟體。 此程序檔採用 Access Manager RTM RPM 儲存位置的路徑，並安裝 RTM RPM 將修補的 RPM 覆蓋。例如：

```
# ./scripts/reinstallRTM path_of_AM7_RTM_RPM_directory
```

在您執行 reinstallRTM 程序檔後，請執行 amconfig 程序檔以重新部署 Access Manager 應用程式，然後重新啓動 Web 容器。

另請參閱第 18 頁的 「安裝後注意事項」，以瞭解更多資訊。

適用於 Windows 系統的修補程式安裝說明

安裝 Windows 修補程式有以下要求：

- Access Manager 7 2005Q4 必須安裝在 Windows 系統上。如需有關安裝的資訊，請參閱「Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows」。
- 若要執行修補程式程序檔，Windows 系統上需要 ActivePerl 5.8 (或更新版本)。

安裝 Windows 修補程式

在您安裝 Windows 修補程式之前，請確定已備份列於第 11 頁的 「安裝前注意事項」中的檔案。

輸入至修補程式程序檔的基底目錄路徑時，請使用正斜線 (/)。例如：c:/sun

若要安裝 Windows 修補程式：

1. 以管理員群組成員的身份登入 Windows 系統。
2. 建立一個用於下載並解壓縮 Windows 修補程式檔案的目錄。例如：AM7p7
3. 將 124296-07.zip 檔案下載並解壓縮到上一個步驟所建立的目錄中。
4. 停止所有 Java ES 2005Q4 服務。
5. 執行 AM7p7\scripts\prepatch.pl 程序檔。
6. 執行 AM7p7\124296-07.exe 以安裝修補程式。
7. 執行 AM7p7\scripts\postpatch.pl 程序檔。
8. 重新啓動 Java ES 2005Q4 服務。
9. 重新部署 Access Manager 應用程式。請參閱第 18 頁的 「安裝後注意事項」，以瞭解更多資訊。
10. 執行 AM7p7\scripts\updateschema.pl 程序檔以更新 Directory Server 服務模式。程序檔會驗證您的輸入項目，然後載入檔案。程序檔也會寫入下列記錄檔：

    javaes-install-directory\AccessManager\AM70Patch-upgrade-schema-*timestamp*
11. 重新啓動 Java ES 2005Q4 服務。

取消 Windows 修補程式

若要取消 Windows 修補程式：

1. 以管理員群組成員的身份登入 Windows 系統。
2. 執行 Uninstall_124296-07.bat 檔案。

3. 執行 AM7p7\scripts\postbackout.pl 程序檔。
4. 重新部署 Access Manager 應用程式。
5. 重新啓動 Java ES 2005Q4 服務。

備註：如果您取消修補程式，由 AM7p7\scripts\updateschema.pl 程序檔所增加的模式變更不會從 Directory Server 中移除。不過您也不需要手動移除這些模式變更，因爲在取消修補程式作業之後，這些變更並不會影響 Access Manager 的功能或可用性。

適用於 HP-UX 系統的修補程式安裝說明

要安裝或移除 HP-UX 修補程式，請使用 swinstall 與 swremove 指令。例如，在獨立系統上安裝修補程式時可使用下列指令：

```
# swinstall /var/spool/patch/126371-07
```

從獨立系統上移除修補程式時則可使用下列指令：

```
# swremove 126371-07
```

如需有關 swinstall 與 swremove 指令的資訊，請參閱 swinstall 與 swremove 線上手冊。

在您安裝或移除修補程式之後，必須重新部署 Access Manager 應用程式，如第 18 頁的「安裝後注意事項」一節所述。

在您重新部署 Access Manager 應用程式之後，請執行 updateschema.sh 程序檔 (修補程式 5 或更新的修補程式) 以載入 XML 和 LDIF 檔案。當您安裝修補程式 7 之後，就可在 *patch-home-directory*/120956-07/scripts 目錄中找到 updateschema.sh 程序檔。當您執行 amconfig 和 updateschema.sh 程序檔之後，請重新啓動 Access Manager Web 容器。

備註：如果您移除修補程式，由 updateschema.sh 程序檔所增加的模式變更不會從 Directory Server 中移除。不過您也不需要手動移除這些模式變更，因爲在移除修補程式之後，這些變更並不會影響 Access Manager 的功能或可用性。

如需在 HP-UX 系統上部署 Access Manager 的更多資訊，請參閱「Sun Java System Access Manager 7 2005Q4 Release Notes for HP-UX」。

安裝後注意事項

安裝 Access Manager 7 2005Q4 修補程式之後的注意事項包括：

- 第 19 頁的「CR# 6254355：Access Manager 修補程式不在 postpatch 程序檔中部署 Access Manager 應用程式」
- 第 21 頁的「CR# 6436409：重新部署分散式認證及用戶端 SDK WAR 檔案」

CR# 6254355：Access Manager 修補程式不在 postpatch 程序檔中部署 Access Manager 應用程式

修補程式安裝程式可能不會保留某些自訂的 WAR 檔案，而以非自訂版本的檔案取代它們。若要識別 WAR 檔案的自訂內容然後手動更新，請參考下列程序。

在以下範例中，*AccessManager-base* 爲基底安裝目錄。預設基底安裝目錄在 Solaris 系統上爲 `/opt`，在 Linux 系統上爲 `/opt/sun`。

在 Windows 系統中，*AccessManager-base* 爲 *javaes-install-directory*`\AccessManager`。例如：`C:\Program Files\Sun\AccessManager`

修補的 WAR 檔案爲：

- `console.war`
- `password.war`
- `services.war`

在 Solaris 系統中這些檔案位於 *AccessManager-base*`/SUNWam` 下，在 Linux 系統中則位於 *AccessManager-base*`/identity` 下。

在 Windows 系統中：已修正的 WAR 檔案位於 *AccessManager-base*`\` 下。

在 WAR 檔案中可變更的內容包括：

- 特性檔案：
  - Solaris 系統：*AccessManager-base*`/SUNWam/locale/*.properties`
  - Linux 系統：*AccessManager-base*`/identity/locale/*.properties`
  - Windows 系統：*AccessManager-base*`\locale\*.properties`
- 標籤檔案庫描述元：
  - Solaris 系統：*AccessManager-base*`/SUNWam/web-src/applications/WEB-INF/*.tld`
  - Linux 系統：*AccessManager-base*`/identity/web-src/applications/WEB-INF/*.tld`
  - Windows 系統：*AccessManager-base*`\web-src\applications\WEB-INF\*.tld`
- `web.xml` 檔案以及用來建構它的檔案 (`WEB-INF/web.xml` 及 `WEB-INF/*.xml`)
- 應用程式特定的檔案：JSP (`*.jsp`) 檔案、影像 (`*.gif`) 檔案以及樣式表 -- 背景顏色、字型大小等 (`*.css`) 檔案

若要確保所有自訂變更均保留，請遵循下列步驟。在對檔案進行變更之前，一律先備份檔案。

1. 安裝修補程式。
2. 將 WAR 檔案解壓縮到暫存目錄中。例如，當 Access Manager 安裝在 Solaris 系統的預設目錄中時：

```
# cd temporary-directory
# jar -xvf /opt/SUNWam/console.war
```

```
# jar -xvf /opt/SUNWam/services.war
# jar -xvf /opt/SUNWam/password.war
```

3. 檢查解壓縮後的檔案，查看修補程式的安裝程式是否對您自訂的檔案進行了任何變更，並手動將原來的自訂變更加入暫存目錄中那些已變更的檔案。對於 *AccessManager-base*/web-src/ 目錄下進行過變更的檔案，若這些檔案沒有包括在修補的 WAR 檔案中，則不需要重新進行變更。
4. 使用修改後的檔案更新 WAR 檔案。例如，當 Access Manager 安裝在 Solaris 系統的預設目錄中時：

   ```
   # cd temporary-directory
   # jar -uvf /opt/SUNWam/console.war $path/$modified file
   # jar -uvf /opt/SUNWam/services.war $path/$modified file
   # jar -uvf /opt/SUNWam/password.war $path/$modified file
   ```

   例如，針對步驟 2-4：

   ```
   # mkdir /tmp/war.tmp
   # cd /tmp/war.tmp
   # jar -xvf /opt/SUNWam/services.war
   # vi index.html
   # jar -uvf /opt/SUNWam/services.war index.html
   ```

5. 重新使用修補程式產生的無訊息配置檔案 (amsilent)，或根據 amsamplesilent 範本檔案建立新的無訊息配置檔案，然後在檔案中設定適當的配置變數，包括：

   - DEPLOY_LEVEL=21
   - DIRECTORY_MODE=5
   - DS_DIRMGRPASSWD、ADMINPASSWD 及 AMLDAPUSERPASSWD 的密碼
   - Access Manager Web 容器變數

   在 Windows 系統中，重新使用由 postpatch.pl 程序檔產生的無訊息配置檔案 (amsilent)，並確定 *AccessManager-base*\setup\AMConfigurator.properties-tmp 包含有效值。然後將此檔案重新命名爲 *AccessManager-base*\setup\AMConfigurator.properties。

   如需有關 Web 容器變數的更多資訊，請參閱 Solaris 系統上 /opt/SUNWam/bin 目錄下，或 Linux 系統上 /opt/sun/identity/bin 目錄下的 amsamplesilent 檔案。

   在 Windows 系統上，配置檔案是 *AccessManager-base*\setup\AMConfigurator.properties。
6. 如下所示執行 amconfig 程序檔。在執行 amconfig 之前，必須執行 Directory Server 及 Access Manager Web 容器。例如，在 Access Manager 安裝於預設基底安裝目錄的 Solaris 系統上，若要執行 amconfig：

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

7. 執行 amconfig 程序檔之後，重新啓動 Access Manager 程序。例如：

```
# cd /opt/SUNWam/bin
# ./amserver stop
# ./amserver start
```

8. 確定所有的自訂 JSP 檔案均位於 Solaris 系統的 *AccessManager-base*/SUNWam/web-src/ (或 Linux 系統的 *AccessManager-base*/identity/web-src/) 目錄下的適當子目錄中，並已備份所有的自訂檔案。

   在 Windows 系統中，這些檔案位於 *AccessManager-base*\web-src\。

9. 重新啓動 Access Manager Web 容器。

如需有關執行 amconfig 程序檔的更多資訊，請參閱：「Sun Java System Access Manager 7 2005Q4 管理指南」中的第 1 章「Access Manager 7 2005Q4 配置程序檔」。

CR# 6436409：重新部署分散式認證及用戶端 SDK WAR 檔案

如果使用分散式認證或用戶端 SDK，請在安裝修補程式後，重新建立並重新部署分散式認證 WAR 檔案及/或用戶端 SDK WAR 檔案。如需相關資訊，請參閱下列文件：

- 建立分散式認證 WAR 檔案：「Technical Note: Using Access Manager Distributed Authentication」
- 建立用戶端 SDK WAR 檔案：「Sun Java System Access Manager 7 2005Q4 Developer's Guide」中的「Installing the Client SDK」
- 部署用戶端 SDK WAR 檔案：「Sun Java System Access Manager 7 2005Q4 Developer's Guide」中的「To Deploy amclientwebapps.war」

Access Manager 7 2005Q4 修補程式 6

Access Manager 7 修補程式 6 (修訂版 06) 修正了許多問題，這些問題列於修補程式隨附的讀我檔案中。修補程式 6 還包括下列新增功能、問題和文件更新。

修補程式 6 的新增功能

- 第 22 頁的「Access Manager 支援 JDK 1.5 HttpURLConnection setReadTimeout 方法」
- 第 22 頁的「主伺服器恢復之後，Access Manager SDK 會轉至主 Directory Server」
- 第 23 頁的「多個 Access Manager 實例會記錄至個別的記錄檔案」
- 第 23 頁的「Access Manager 7 允許多個 cookie 網域」
- 第 24 頁的「Microsoft IIS 6.0 認證後外掛程式支援 SharePoint Server」
- 第 24 頁的「Access Manager 支援 Internet Explorer 7」

修補程式 6 中的已知問題和限制

- 第 24 頁的「CR# 6379325 在作業階段容錯移轉期間存取主控台會丟出空指標異常」
- 第 25 頁的「CR# 6508103：在 Windows 上，按一下 [管理主控台] 的 [說明] 會傳回應用程式錯誤」
- 第 25 頁的「CR# 6564877：Access Manager 7 修補程式安裝會覆寫 SAML v2 檔案」

備註 – 安裝修補程式 6 之前，建議您升級或修正下列元件：

- 如果您使用的是 Sun Java System Web Server 6.1 SP5 或更舊的版本，請升級至 Web Server 6.1 SP7，您可以從網站下載該版本，網址爲：

  `http://www.sun.com/download/products.xml?id=45c90ca9`

  請遵循「Sun Java System Web Server 6.1 SP7 版本說明」中的「升級」。
- 從 SunSolve Online 下載並安裝 NSS、JSS 和 NSPR 的最新安全修補程式，網址爲：`http://sunsolve.sun.com`。
  - Solaris 8 SPARC 平台：119209
  - Solaris 8 x86 平台：119210
  - Solaris 9 SPARC 平台：119211
  - Solaris 9 x86 平台：119212
  - Solaris 10 SPARC 平台：119213
  - Solaris 10 x86 和 AMD64 平台：119214
  - Windows 系統：124392
  - HP-UX 系統：124379

Access Manager 支援 JDK 1.5 `HttpURLConnection` `setReadTimeout` 方法

爲支援 `setReadTimeout` 方法，`AMConfig.properties` 檔案具備下列新特性供您設定讀取逾時值：

```
com.sun.identity.url.readTimeout
```

若 Web 容器使用 JDK 1.5，爲避免開啓太多 `HttpURLConnection` 而導致伺服器當機，請爲此特性設置適當的值以讓連線逾時。預設值爲 30000 毫秒 (30 秒)。

若 `AMConfig.properties` 檔案中沒有 `com.sun.identity.url.readTimeout` 特性，或已將此特性設定爲空字串，則 `setReadTimeout` 方法會被忽略。

主伺服器恢復之後，Access Manager SDK 會轉至主 Directory Server

若 Sun Java System Directory Server 配置爲多個主伺服器複製 (multi-master replication, MMR)，Access Manager SDK 會在發生故障的主伺服器恢復之後轉至主 Directory Server。在這之前，即使主伺服器已恢復，Access Manager SDK 還是會繼續存取輔助 Directory Server。

爲支援這種新的運作方式，Access Manager 的 `AMConfig.properties` 檔案中加入了下列新特性：

```
com.sun.am.ldap.fallback.sleep.minutes
```

此特性設定主伺服器恢復之後，輔助 Directory Server 實例在轉至主伺服器前暫停的時間 (以分鐘爲單位)。預設值爲 15 分鐘。

com.sun.am.ldap.fallback.sleep.minutes 特性是隱藏的。若要將此特性設爲預設值 (15 分鐘) 以外的值，則需要在 AMConfig.properties 檔案中明確加入此值。例如，若要將該值設定爲 7 分鐘：

```
com.sun.am.ldap.fallback.sleep.minutes=7
```

爲使新值生效，請重新啓動 Access Manager Web 容器。

多個 Access Manager 實例會記錄至個別的記錄檔案

藉由在 AMConfig.properties 檔案中設定下列新特性，在相同主機伺服器上所執行的多個 Access Manager 實例可記錄至不同記錄子目錄內的個別記錄檔中：

```
com.sun.identity.log.logSubdir
```

除非您在 [管理主控台] 中變更預設記錄目錄，否則預設記錄目錄爲：

- Solaris 系統：/var/opt/SUNWam/logs
- Linux 和 HP-UX 系統：/var/opt/sun/identity/logs
- Windows 系統：C:\Sun\JavaES5\identity\logs

第一個 Access Manager 實例都會記錄至預設記錄目錄。若要爲其他 Access Manager 實例指定不同的記錄子目錄，請在 AMConfig.properties 檔案中爲其他每個 Access Manager 實例設定 com.sun.identity.log.logSubdir 特性。

例如，如果您擁有三個實例 (am-instance-1、am-instance-2 與 am-instance-3)，且全部在相同的 Solaris 主機伺服器上執行，請按照下列方法設定特性：

```
com.sun.identity.log.logSubdir=am-instance-2
com.sun.identity.log.logSubdir=am-instance-3
```

com.sun.identity.log.logSubdir 特性是隱藏的。必須明確依照您的需求在 AMConfig.properties 檔案中加入此特性，並重新啓動 Access Manager Web 容器才能讓子目錄值生效。

然後 Access Manager 實例就會記錄至下列目錄：

```
/var/opt/SUNWam/logs/log-files-for-am-instance-1
/var/opt/SUNWam/logs/am-instance-2/log-files-for-am-instance-2
/var/opt/SUNWam/logs/am-instance-3/log-files-for-am-instance-3
```

Access Manager 7 允許多個 cookie 網域

爲支援多個 cookie 網域，Access Manager 具有下列新特性：

```
com.sun.identity.authentication.setCookieToAllDomains
```

預設值爲 true。此新特性是隱藏的。要將此值設定爲 false，請明確在 AMConfig.properties 檔案中加入此特性，並重新啓動 Access Manager Web 容器。

Microsoft IIS 6.0 認證後外掛程式支援 SharePoint Server

Microsoft 網際網路資訊服務 (Internet Information Services, IIS) 6.0 認證外掛程式目前支援 Microsoft Office SharePoint Server。使用者可使用使用者 ID 或登入名稱登入 Access Manager。但 SharePoint Server 只接受登入名稱，使用者指定使用者 ID 時會出錯。

爲允許登入至 SharePoint Server，認證後外掛程式 (`ReplayPasswd.java`) 目前使用下列新特性：

```
com.sun.am.sharepoint_login_attr_name
```

此新特性指示 SharePoint Server 用於認證的使用者屬性。例如，下列特性指定用於認證的一般名稱 (common name, cn)：

```
com.sun.am.sharepoint_login_attr_name=cn
```

認證後外掛程式會讀取 `com.sun.am.sharepoint_login_attr_name` 特性，並從 Directory Server 中取得相對的使用者屬性值。然後外掛程式會設定授權標頭，以允許使用者存取 SharePoint Server。

此特性是隱藏的。要設定此特性，請明確在 `AMConfig.properties` 檔案中加入此特性，再重新啓動 Access Manager Web 容器以使該值生效。

Access Manager 支援 Internet Explorer 7

Access Manager 7 2005Q4 修補程式 6 目前支援 Microsoft Windows Internet Explorer 7。

CR# 6379325 在作業階段容錯移轉期間存取主控台會丟出空指標異常

在此情況下，多個 Access Manager 伺服器部署爲作業階段容錯移轉模式且位於負載平衡器之後，而負載平衡器配置爲基於 cookie 的居留式請求路由。Access Manager 管理員會透過負載平衡器存取 Access Manager 主控台。管理員登入主控台時，會在其中一個 Access Manager 伺服器上建立作業階段。若該伺服器當機，主控台作業階段會如預期那樣容錯移轉至另一個 Access Manager 伺服器。然而，管理員有時會在瀏覽器與 Web 容器錯誤記錄中遇到間歇性的空指標異常。

此問題只在容錯移轉時影響作用中的 Access Manager 主控台作業階段，並不影響 Access Manager 伺服器。

解決方法：若要避免這些間歇性空指標異常：

- 要暫時解決此問題，可重新整理瀏覽器，或者先登出，然後重新登入主控台。
- 要永久解決此問題，可在未參與作業階段容錯移轉的個別 Access Manager 實例中部署 Access Manager 主控台。

CR# 6508103：在 Windows 上，按一下 [管理主控台] 的 [說明] 會傳回應用程式錯誤

在 Windows 2003 Enterprise Edition 上，如果在非英文語言環境中將 Access Manager 部署於 Sun Java System Application Server 上，則按一下 [範圍管理主控台] 中的 [說明] 會傳回應用程式錯誤。

解決方法：

1. 將 *javaes-install-dir*`\share\lib\jhall.jar` 檔案複製到 `%JAVA_HOME%\jre\lib\ext` 目錄。

   其中 *javaes-install-dir* 是 Windows 安裝目錄

2. 重新啓動 Application Server 實例。

CR# 6564877：Access Manager 7 修補程式安裝會覆寫 SAML v2 檔案

若已安裝 SAML v2 外掛程式，則修補程式安裝會覆寫與 SAML v2 相關的檔案，且 `postpatch` 程序檔會顯示此訊息：

```
The postpatch script detected that the SAML v2 plug-in is installed in your
environment. When you run the amconfig script to redeploy the Access Manager
applications, the script will recreate the amserver.war file and the SAML v2
related files will be lost. Therefore, after you run amconfig, recreate and
redeploy the amserver.war file, as described in the Sun Java System SAML v2
Plug-in for Federation Services User's Guide.
```

解決方法：安裝修補程式並執行 `amconfig` 程序檔之後，請爲使用 SAML v2 外掛程式的 Federation Manager 或 Access Manager 部署重新建立並重新部署 `amserver.war` 檔案。

如需特定步驟，請參閱「Sun Java System SAML v2 Plug-in for Federation Services User's Guide」中的第 2 章「Installing the SAML v2 Plug-in for Federation Services」。

Access Manager 7 2005Q4 修補程式 5

Access Manager 7 修補程式 5 (修訂版 05) 修正了許多問題，這些問題列於修補程式隨附的讀我檔案中。修補程式 5 還包括下列新增功能、問題和文件更新。

修補程式 5 的新增功能

- 第 27 頁的「對 HP-UX 系統的支援」
- 第 27 頁的「對 Microsoft Windows 系統的支援」
- 第 27 頁的「用於載入 LDIF 和 XML 檔案的新 `updateschema.sh` 程序檔」
- 第 28 頁的「對特定應用程式閒置階段作業逾時值的支援」
- 第 29 頁的「CDC Servlet 可部署在分散式認證 UI 伺服器上」
- 第 29 頁的「可在 CDC servlet 重新導向至 Access Manager 登入 URL 時指定範圍」

修補程式 5 的已知問題和限制

全球化 (Globalization, g11n) 問題

文件更新

對 HP-UX 系統的支援

修補程式 **126371** 提供對 HP-UX 系統的支援。如需更多資訊，請參閱：

如需有關在 HP-UX 系統上的安裝資訊，請參閱「Sun Java Enterprise System 2005Q4 安裝指南」。

對 Microsoft Windows 系統的支援

修補程式 **124296** 提供對 Windows 系統的支援。如需更多資訊，請參閱：

如需有關在 Windows 系統上的安裝資訊，請參閱「Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows」。

用於載入 LDIF 和 XML 檔案的新 updateschema.sh 程序檔

修補程式 5 (及更新的修補程式) 包含 `updateschema.sh` 程序檔，可載入下列檔案以更新 Directory Server 服務模式：

- `AddLDAPFilterCondition.xml`
- `amPolicyConfig_mod_ldfc.xml`
- `accountLockoutData.xml`
- `accountLockout.ldif`
- `idRepoServiceAddAttrSchemaRequest_Cache.xml`
- `wsf1.1_upgrade.xml`
- `amAuth_mod.xml`
- `amAuthCert_mod.xml`

在先前的 Access Manager 修補程式版本中，您必須手動載入這些檔案。

若要執行 `updateschema.sh` 程序檔：

1. 以超級使用者 (root) 的身份登入或成爲超級使用者。
2. 移至修補程式目錄。
3. 執行程序檔。例如，在 Solaris 系統中：

   ```
   # cd /120954-07
   # ./updateschema.sh
   ```

   在 Windows 系統中，程序檔爲 updateschema.pl。
4. 當程序檔提示您時，請輸入下列項目：
   - Directory Server 主機名稱和連接埠號
   - Directory Server 管理使用者 DN 和密碼
   - amadmin DN 和密碼
5. 程序檔會驗證您的輸入項目，然後載入檔案。程序檔也會寫入下列記錄檔：
   - Solaris 系統：/var/opt/SUMWam/logs/AM70Patch.upgrade.schema. *timestamp*
   - Linux 系統：/var/opt/sun/identity/logs/AM70Patch.upgrade.schema. *timestamp*
6. 在程序檔結束之後，重新啓動 Access Manager Web 容器。

備註 如果您取消修補程式 5 作業，由 updateschema.sh 程序檔增加的模式變更並不會從 Directory Server 移除。不過您也不需要手動移除這些模式變更，因爲在取消修補程式作業之後，這些變更並不會影響 Access Manager 的功能或可用性。

對特定應用程式閒置階段作業逾時值的支援

修補程式 5 允許不同的應用程式具有不同的階段作業閒置逾時值。在企業中，某些應用程式所需的階段作業閒置逾時值可能要少於在階段作業服務中指定的階段作業閒置逾時。例如，您已在階段作業服務中指定階段作業的閒置逾時值爲 30 分鐘，但在使用 HR 應用程式時，如果使用者已閒置超過 10 分鐘時就應視爲逾時。

使用此功能的條件爲：

- 保護應用程式的代理程式必須配置爲從 Access Manager 強制執行 URL 策略決定。
- 代理程式必須配置爲在自我策略決定快取模式下執行。請參閱下列特性：
  - 對於 Web 代理程式：com.sun.am.policy.am.fetch_from_root_resource
  - 對於 J2EE 代理程式：com.sun.identity.policy.client.cacheMode
- Access Manager AMConfig.properties 檔案必須指定策略元件評估順序，使條件在最後進行評估。請參閱下列特性：

  com.sun.identity.policy.Policy.policy_evaluation_weights
- 代理程式根據在本機快取的決定而允許的應用程式存取不被 Access Manager 上的條件所知。因此，實際的應用程式閒置逾時將介於應用程式閒置逾時以及應用程式閒置逾時減去代理程式快取持續時間之間。

若要使用此功能：

- 將認證方案條件加入用來保護應用程式的策略中，該應用程式需有其特定的階段作業閒置逾時。
- 在認證方案條件中指定應用程式名稱和逾時值。
- 在套用至應用程式資源的所有策略中使用相同的應用程式名稱和逾時值。
- 指定「逾時值」(以分鐘爲單位)。如果該值爲 0 或大於在階段作業服務中指定的階段作業閒置逾時值，則該值會被忽略，並套用階段作業服務中的逾時。

例如，使用下列認證方案條件來考量策略 `http://host.sample.com/hr/*`：

- 認證方案：LDAP
- 應用程式名稱：HR
- 逾時值：10

如果已定義多重策略來保護 HR 應用程式的資源，您必須將該條件加入所有策略中。

當個別階段作業中的使用者嘗試存取由 Access Manager 代理程式所保護的 HR 應用程式時，系統會提示該使用者需取得 LDAP 方案的認證 (如果使用者尚未取得認證)。

如果使用者已取得 LDAP 方案的認證，則只有在上次認證之後的 10 分鐘以內，或在使用者上次存取 HR 應用程式時間後的 10 分鐘以內，該使用者才被允許進行存取。否則，系統會提示該使用者需再次取得 LDAP 方案的認證才能存取應用程式。

CDC Servlet 可部署在分散式認證 UI 伺服器上

CDC Servlet 能與分散式認證 UI 伺服器並存於 DMZ 中以啓用跨網域單次登入 (Cross-Domain Single Sign-On, CDSSO)。Access Manager 伺服器可部署在防火牆之後，分散式認證 UI 伺服器中的 CDC Servlet 會處理爲達成 CDSSO 而對 Access Manager 進行的所有存取。若要啓用 CDSSO，請參閱特定的策略代理程式文件並執行下列額外步驟：

- 修改代理程式的 `AMAgent.properties` 檔案以指向分散式認證端 (用戶端) 上的 CDC Servlet。例如，可對 Web 代理程式變更下列特性：

  ```
  com.sun.am.policy.agents.config.cdcservlet.url=
      http://DAhost.DAdomain:DAport/DISTAUTH_DEPLOY_URI/cdcservlet
  ```

- 視需要在 Access Manager 中爲必須由代理程式保護的資源定義策略。例如，如果代理程式位於 `host.example.com:80` ，則將資源的策略定義爲 `http://host.example.com:80/*` 。

可在 CDC servlet 重新導向至 Access Manager 登入 URL 時指定範圍

您現在可以指定範圍名稱給 CDC Servlet，如此一來，當重新導向至 Access Manager 登入 URL 時，範圍名稱便會納入其中，且使用者可登入特定範圍。例如：

```
com.sun.am.policy.agents.config.cdcservlet.url=
    http://lb.example.com/amserver/cdcservlet?org=realm1
```

憑證認證可使用 UPN 值來對映使用者設定檔

以前，憑證認證只能使用 subjectDN 中的 dn 元件來對映使用者設定檔。Access Manager 現在允許使用 SubjectAltNameExt 中的使用者主要名稱 (user principal name, UPN) 值進行設定檔對映。

在多重伺服器環境中會對登出執行後期認證處理

現在，在多重伺服器環境中，當使用者登出的伺服器與原來登入的伺服器不同時，將會執行後期認證處理 (無論是否已配置階段作業容錯移轉)。

SAML 支援新的名稱識別碼 SPI

SAML 現在可支援新的名稱識別碼服務提供者介面 (service provider interface, SPI)，使站點可自訂 SAML 宣示中的名稱識別碼。站點可實作新的 NameIdentifierMapper 介面，以將使用者帳號對映至 SAML 宣示之主體中的名稱識別碼。

站點監視的新配置特性

Access Manager 站點監視功能包含以下新特性，可讓您指定站點狀態檢查的運作方式。

特性	說明
com.sun.identity.urlchecker.invalidate.interval	識別當機或未回應站點的時間間隔 (以毫秒爲單位)。 預設值：70000 毫秒 (70 秒)。
com.sun.identity.urlchecker.sleep.interval	站點狀態檢查應暫停的時間間隔 (以毫秒爲單位)。 預設值：30000 毫秒 (30 秒)。
com.sun.identity.urlchecker.targeturl	用來檢查 Access Manager 程序狀態的不同目標 URL。 預設值："/amserver/namingservice"。

修補程式沒有將以上這些特性加入 AMConfig.properties 檔案。若要以預設值以外的值使用這些新特性，請執行下列動作：

1. 將這些特性及其值加入 AMConfig.properties 檔案。若爲策略代理程式，請將這些特性加入 AMAgents.properties 檔案。
2. 重新啓動 Access Manager Web 容器以使這些值生效。

使用者在認證鏈中不必再認證兩次

考慮以下情況。站點配置一個包含三個 LDAP 模組的認證鏈。所有模組皆已設爲 SUFFICIENT，並且 iplanet-am-auth-shared-state-enabled 和 iplanet-am-auth-store-shared-state-enabled 選項均已設爲 true。例如：

```
<AttributeValuePair>
   <Value>A-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
   <Value>B-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
   <Value>C-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
</AttributeValuePair>
```

修補程式 5 將新的 iplanet-am-auth-shared-state-behavior-pattern 選項加入模組選項，其兩個可能的值爲：tryFirstPass (預設值) 和 useFirstPass。

爲了避免使用者必須輸入兩次使用者 ID 和密碼以取得認證 (如之前的情況所述)，請將鏈接中所有模組的此新選項設爲 useFirstPass。以前，僅存在於第三個 LDAP 實例中的使用者必須輸入兩次使用者 ID 和密碼才能取得認證。

對效能調校程序檔的變更

修補程式 5 包含效能調校程序檔的下列變更：

- 第 31 頁的 「調校程序檔支援密碼檔案」
- 第 32 頁的 「調校程序檔從 Directory Server 移除不必要的 ACI」
- 第 32 頁的 「調校程序檔可調校分散式認證 UI 伺服器 Web 容器」
- 第 33 頁的 「單一 amtune-os 程序檔可調校 Solaris OS 和 Linux OS」
- 第 33 頁的 「調校程序檔在 Solaris 10 本機區域中會完整執行」
- 第 33 頁的 「Windows 系統可使用調校程序檔」
- 第 33 頁的 「Sun Fire T1000 和 T2000 伺服器的調校注意事項」

另請參閱 第 35 頁的 「CR# 6527663：com.sun.identity.log.resolveHostName 特性的預設值應爲 false 而非 true」。

調校程序檔支援密碼檔案

修補程式 5 可讓您在文字檔中指定調校程序檔的密碼。以前，您只能以指令行引數的形式輸入密碼，而這可能會引起安全問題。若要使用密碼檔案，請在檔案中依需要設定下列變數：

```
DS_ADMIN_PASSWORD=DirectoryServer-admin-password
AS_ADMIN_PASSWORD=ApplicationServer8-admin-password
```

例如，若要調校 Application Server 8：

```
# ./amtune-as8 password-file
```

其中 *password-file* 包含設爲 Application Server 8 管理員密碼的 `AS_ADMIN_PASSWORD`。

當調校程序檔呼叫 `ldapmodify`、 `ldapsearch`、`db2index` 和 `dsconf` Directory Server 公用程式時，會使用 `-j` *password-file* 選項。

調校程序檔從 Directory Server 移除不必要的 ACI

如果 Access Manager 7 2005Q4 是在範圍模式下安裝，則存取權限是使用委託權限來決定，因此將不再需要某些 Directory Server ACI。Access Manager 7 2005Q4 修補程式 5 可讓您執行 `amtune-prepareDSTuner` 程序檔以移除不必要的 ACI。此程序檔從 `remacis.ldif` 檔案中讀取 ACI 清單，然後呼叫 `ldapmodify` 公用程式將其移除。

您可以執行 `amtune-prepareDSTuner` 程序檔以在 Solaris、Linux、HP-UX 和 Windows 系統上移除不必要的 ACI。如需更多資訊，包括如何執行程序檔，請參閱「Technical Note: Sun Java System Access Manager ACI Guide」。

調校程序檔可調校分散式認證 UI 伺服器 Web 容器

當您在 Web 容器上部署分散式認證 UI 伺服器後，您可以執行 Access Manager 調校程序檔以調校 Web 容器。下列調校程序檔可設定對應 Web 容器的 JVM 和其他調校選項：

表 2 Access Manager Web 容器調校程序檔

Web 容器	調校程序檔
`amtune-ws61`	Web Server 6.1
`amtune-as7`	Application Server 7
`amtune-as8`	Application Server Enterprise Edition 8.1

若要調校分散式認證 UI 伺服器的 Web 容器：

1. 由於 Access Manager 伺服器並未安裝在已部署分散式認證 UI 伺服器的系統中，因此從 Access Manager 伺服器安裝中複製適當的 Web 容器調校程序檔 (如上表所示)、`amtune-env` 配置檔案和 `amtune-utils` 程序檔。如果要調校 Solaris 或 Linux 作業系統，還需複製 `amtune-os` 程序檔。
2. 編輯 `amtune-env` 配置檔案中的參數以指定 Web 容器和調校選項。若要在 REVIEW 模式下執行程序檔，請在 `amtune-env` 檔案中設定 `AMTUNE_MODE=REVIEW`。
3. 在 REVIEW 模式下執行 Web 容器調校程序檔。在 REVIEW 模式下，程序檔會根據 `amtune-env` 檔案中的值建議調校變更，但並不會實際變更部署。
4. 檢查除錯記錄檔中調校建議。如有需要，請根據此次執行來變更 `amtune-env` 檔案。
5. 若要進行調校變更，請在 `amtune-env` 檔案中設定 `AMTUNE_MODE=CHANGE`。
6. 在 CHANGE 模式下執行調校程序檔以對部署進行調校變更。

如需執行調校程序檔以調校 Access Manager Web 容器的更多資訊，請參閱「Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide」中的第 2 章「Access Manager Tuning Scripts」。

單一 amtune-os 程序檔可調校 Solaris OS 和 Linux OS

修補程式 5 包含可調校 Solaris OS 和 Linux OS 的單一 amtune-os 程序檔。該程序檔可透過 uname -s 指令決定 OS 的類型。以前，Access Manager 提供個別的 amtune-os 程序檔來調校每一類 OS。

調校程序檔在 Solaris 10 本機區域中會完整執行

如果 Access Manager 是安裝在 Solaris 10 本機區域，則除了 amtune-os 以外的所有調校程序檔都可以在本機區域執行。在本機區域中，amtune-os 程序檔會顯示警告訊息，而不會調校 OS。然後該程序檔會繼續執行您請求的其他調校程序檔。以前在本機區域中，amtune-os 程序檔會中斷，並且您請求的任何後續調校程序檔都不會執行。

在 Solaris 10 全域區域中，amtune 程序檔會呼叫 amtune-os 來調校 OS 以及您請求執行的其他程序檔。

Windows 系統可使用調校程序檔

修補程式 5 包含適用於 Windows 系統的調校程序檔。在 Windows 系統上執行調校程序檔與在 Solaris 系統或 Linux 系統上執行類似，但仍有以下差異：

- Windows 程序檔是以 Perl 撰寫，並且需要執行 Active Perl 5.8。
- 如果您調校 Directory Server，則在執行 amtune-prepareDSTuner.pl 程序檔之後，您必須將 amtune-utils.pl、amtune-directory.pl、remacis.ldif 和 amtune-samplepassordfile 檔案複製到 Directory Server 系統中，因爲該程序檔無法壓縮這些檔案。
- 沒有可調校 Windows 作業系統的程序檔。
- 未提供對區域的支援。
- 在執行程序檔之前，您必須將 amtune-env.pl 檔案中的 $BASEDIR 參數設爲 Access Manager 安裝目錄。

Sun Fire T1000 和 T2000 伺服器的調校注意事項

如果 Access Manager 是安裝在 Sun Fire T1000 或 T2000 伺服器中，則用於 Web Server 6.1 和 Application Server 8 的修補程式 5 調校程序檔會將 JVM GC ParallelGCThreads 參數設爲 8：

```
-XX:ParallelGCThreads=8
```

此參數可減少資源回收執行緒的數量，該數量在支援 32 個執行緒的系統上可能會很高 (但這沒必要)。不過，如果 32 位元虛擬 CPU 機器 (例如 Sun Fire T1000 或 T2000 伺服器) 將完整資源回收作業數量最小化，您仍可以將該值增加到 16 甚至 20。

同樣地，對於含有 CMT 處理器 (採用 CoolThreads 技術) 的 Solaris SPARC 系統，我們建議您在 `/etc/opt/SUNWam/config/AMConfig.properties` 檔案的結尾加入以下特性：

```
com.sun.am.concurrencyRate=value
```

預設 *value* 爲 16，但您可以根據 Sun Fire T1000 或 T2000 伺服器中的核心數將此特性設爲較低的值。

IIS 6.0 策略代理程式的基本認證

若要在 Microsoft 網際網路資訊服務 (Internet Information Services, IIS) 6.0 中啓用基本認證，則策略代理程式必須取得使用者的名稱和密碼。修補程式 5 包含以下的新類別以啓用此功能 (使用使用者密碼的 DES 加密)：

- `DESGenKey.java` 可產生用來加密和解密使用者密碼的唯一金鑰。
- `ReplayPasswd.java` 可在 `AMConfig.properties` 檔案中從 `com.sun.am.replaypasswd.key` 特性讀取加密金鑰值，將密碼加密，並將其指定給 `sunIdentityUserPassword` 階段作業特性。

若要在 IIS 6.0 中使用基本認證，您必須在 Access Manager 伺服器端和 IIS 6.0 策略代理程式端上執行下列步驟。

在 Access Manager 伺服器端：

1. 執行 `DESGenKey.java` 以產生用於密碼加密和解密的唯一加密金鑰。在 Solaris 系統中，`DESGenKey.java` 檔案位於 `com/sun/identity/common` 目錄之下，包含在 `/opt/SUNWam/lib` 目錄的 `am_sdk.jar` 檔案中。例如，以下指令會產生加密金鑰：

   ```
   # cd /opt/SUNWam/lib
   # java -cp am_sdk.jar com.sun.identity.common.DESGenKey
   ```

2. 將步驟 1 的加密金鑰值指定給 `AMConfig.properties` 檔案的 `com.sun.am.replaypasswd.key` 特性。
3. 將 `ReplayPasswd.java` 部署爲後期認證外掛程式。當您配置該外掛程式時，請使用完整的類別名稱：`com.sun.identity.authentication.spi.ReplayPasswd`。

在 IIS 6.0 策略代理程式端：

1. 將從伺服器端取得的加密金鑰值指定給 `AMAgent.properties` 檔案的 `com.sun.am.replaypasswd.key` 特性。Access Manager 伺服器和 IIS 6.0 策略代理程式必須使用相同的加密金鑰。
2. 在 IIS 6.0 Manager 中啓用基本認證。

IIS 6.0 策略代理程式會從作業階段回應中讀取加密密碼，從 `com.sun.am.replaypasswd.key` 特性中解密密碼，並設定認證標頭以啓用基本認證。

如需有關 IIS 6.0 策略代理程式的資訊，請參閱「Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft Internet Information Services 6.0」。

CR# 6567746：在 HP-UX 系統上，若密碼重試次數超出限制，Access Manager 修補程式 5 會報告錯誤的 errorCode 值

使用者帳號被鎖定時，若密碼重試次數超出限制，HP-UX 系統上的 Access Manager 7 2005Q4 修補程式 5 會報告 `errorCode = null` 而非 `errorCode = 107`。

解決方法：無。

CR# 6527663：com.sun.identity.log.resolveHostName 特性的預設值應為 false 而非 true

在您執行 `amtune-identity` 調校程序檔之前，我們建議您將以下特性 (設爲 `false`) 加入 `AMConfig.properties` 檔案：

```
com.sun.identity.log.resolveHostName=false
```

值爲 `false` 可將解析主機名稱的影響減到最低，以藉此提升效能。不過，如果您要將用戶端機器的主機名稱輸出在 `amAuthentication.access` 記錄中，請將該值設爲 `true`。

CR# 6527528：移除修補程式後，XML 檔案的 amldapuser 密碼成為明文形式

如果您從 Access Manager 完整伺服器安裝中移除修補程式 5，`amAuthLDAP.xml` 和 `amPolicyConfig.xml` 檔案會包含明文形式的 `amldapuser` 密碼。這些檔案位於以下的目錄中 (依您的平台而定)：

- Solaris 系統：`/etc/opt/SUNWam/config/xml`
- Linux 和 HP-UX 系統：`/etc/opt/sun/identity/config/xml`

解決方法：編輯 `amAuthLDAP.xml` 和 `amPolicyConfig.xml` 檔案並刪除明文密碼。

CR# 6527516：WebLogic 的完整伺服器需要 JAX-RPC 1.0 JAR 檔案與用戶端 SDK 進行通訊

在 Access Manager 7 2005Q4 修補程式中，BEA WebLogic Server 的 Access Manager 配置程序檔 (`amwl81config`) 會將 JAX-RPC 1.1 JAR 檔案加入 WebLogic 實例的 `classpath`。雖然此修改對於 Sun Java System Portal Server 等產品是有益的，但部署在 WebLogic Server 上的完整伺服器安裝 (`DEPLOY_LEVEL=1`) 會無法與用戶端 SDK 安裝進行通訊，且之後將發生異常。

如果 Access Manager 7 2005Q4 伺服器是安裝在 BEA WebLogic Server 上，則 `startWebLogic.sh` 程序檔中的 `CLASSPATH` 必須設爲 JAX-RPC 1.0 JAR 檔案的位置，以同 Access Manager 用戶端 SDK 進行通訊。

解決方法：套用 Access Manager 修補程式之前，請在 `startWebLogic.sh` 程序檔中設定 `CLASSPATH`，以讓 WebLogic Server 實例使用 JAX-RPC 1.0 JAR 檔案而非 JAX-RPC 1.1 JAR 檔案：

1. 在 Access Manager 伺服器上，以超級使用者 (root) 的身份登入或成爲超級使用者。
2. 編輯 startWebLogic.sh 程序檔並將 CLASSPATH 改爲使用 JAX-RPC 1.0 JAR 檔案。例如：

目前的值：

```
CLASSPATH=/etc/opt/SUNWam/config:
AccessManager-base/AccessManager-package-dir/lib/jax-qname.jar:
AccessManager-base/AccessManager-package-dir/lib/namespace.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-api.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-spi.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-impl.jar:
```

新的值：

```
CLASSPATH=/etc/opt/SUNWam/config:
AccessManager-base/AccessManager-package-dir/lib/jax-qname.jar:
AccessManager-base/AccessManager-package-dir/lib/namespace.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc_1.0/jaxrpc-api.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-ri.jar:
```

其中 *AccessManager-base* 爲基底安裝目錄。Solaris 系統上的預設值爲 /opt，Linux 和 HP-UX 系統上的預設值爲 /opt/sun。*AccessManager-package-dir* 爲 Access Manager 套裝軟體目錄。

5. 重新啓動 WebLogic Server 實例。

CR # 6523499：修補程式 5 amsilent 檔案可供 Linux 系統上的所有使用者讀取

在 Linux 系統上，postpatch 程序檔會建立具有 644 權限的 /opt/sun/identity/amsilent 檔案，允許所有使用者對其進行讀取。

解決方法：在執行 installpatch 程序檔後，請變更 amsilent 檔案的權限以僅允許所有者擁有讀取和寫入權限。例如：

```
# chmod 600 /opt/sun/identity/amsilent
```

CR# 6520326：將修補程式 5 套用至伺服器上的第二個 Access Manager 實例會覆寫第一個實例的 serverconfig.xml

在該部署方案中，兩個 Access Manager 實例部署在相同的主機伺服器上，且每個實例部署在不同的 Web 容器實例上。然後您執行下列步驟：

1. 套用修補程式 5。
2. 修改 amsilent 檔案並重新部署第一個 Access Manager 實例。
3. 再次修改第二個 Access Manager 實例的 amsilent，然後重新部署該實例。

如果 amsilent 檔案中 NEW_INSTANCE=false，則第一個 Access Manager 實例的 serverconfig.xml 檔案會由第二個 Access Manager 實例的資訊所覆寫。之後重新啓動第一個 Access Manager 實例會失敗。serverconfig.xml 檔案位於以下目錄 (依您的平台而定)：

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

解決方法：當您部署第二個 Access Manager 實例時，請設定 amsilent 檔案中的 NEW_INSTANCE=true。然後第二個 Access Manager 實例的 serverconfig.xml 檔案會以正確的資訊更新，且第一個 Access Manager 實例的 serverconfig.xml 檔案也不會被覆寫。

CR# 6520016：修補程式 5 的僅 SDK 安裝會覆寫範例 makefile

將修補程式 5 套用至僅安裝了 SDK 的機器會覆寫範例 makefile。

解決方法：將修補程式 5 套用至僅安裝了 SDK 的機器並不需要進行重新配置；不過，若您要使用範例 makefile，請依照下列步驟來更新範例 makefile 的 LDIF 和特性檔案 (即執行標記交換)：

1. 以 DEPLOY_LEVEL=14 執行 amconfig 程序檔以解除安裝 SDK 並取消配置 Web 容器。
2. 以 DEPLOY_LEVEL=4 執行 amconfig 程序檔以重新安裝 SDK 並重新配置 Web 容器。

CR# 6515502：LDAPv3 儲存庫外掛程式無法總是正確處理別名搜尋屬性

對於大部分的搜尋來說，此問題已獲得修正。不過，在設定別名搜尋屬性時必須特別小心。別名搜尋屬性的值在組織中必須是唯一的。如果設定了多個別名搜尋屬性，則有可能資料存放區的一個項目與一個屬性相符，而另一個項目與另一個屬性相符。在此情況中，Access Manager 伺服器會丟出以下錯誤：

發生內部認證錯誤。請與您的系統管理員連絡。

解決方法：無

CR# 6515383: 無法在同一 Web 容器中使用分散式認證和 J2EE 代理程式

如果分散式認證 UI 伺服器和 J2EE 策略代理程式安裝在相同的 Web 容器中，它們將無法運作。

解決方法：再建立一個 Web 容器實例並將分散式認證 UI 伺服器和 J2EE 策略代理程式部署在該容器的不同實例中。

CR# 6508103：Application Server 在 Windows 系統中時，線上說明會傳回應用程式錯誤

如果您將 Access Manager 部署在 Windows 系統中的 Sun Java System Application Server 上，在範圍模式的說明螢幕左面板中按一下 [說明] 將傳回應用程式錯誤。

解決方法：將 *javaes-install-dir*`\share\lib\jhall.jar` 檔案複製到 `JAVA_HOME\jre\lib\ext` 目錄，然後重新啓動 Application Server。

CR# 6507383 和 CR# 6507377：分散式認證需要明確的 goto URL 參數

如果未指定明確的 `goto` URL 參數，則分散式認證 UI 伺服器會嘗試重新導向至 Access Manager 中所指定之成功 URL 的 `goto`。此重新導向會因爲下列原因而失敗：

- URL 爲相對路徑，在分散式認證 UI 伺服器中沒有可用的對應頁面。
- URL 爲絕對路徑，瀏覽器無法到達該 URL。

解決方法：對於分散式認證 UI 伺服器，始終指定明確的 `goto` URL 參數。

CR# 6402167：LDAP JDK 4.18 引起 LDAP 用戶端/Directory Server 問題

在 Java ES 2005Q4 發行版本中，Access Manager 7 2005Q4 是隨 LDAP JDK 4.18 一起發行的，因而造成許多 Access Manager 和 Directory Server 的連線問題。

解決方法：套用以下一種 Sun Java System LDAP Java Development Kit 修補程式：

- Solaris OS、SPARC 和 x86 平台：119725-04
- Linux OS：120834-02

這些修補程式可從 SunSolve Online 上取得，網址爲：`http://sunsolve.sun.com`。

CR# 6352135：分散式認證 UI 伺服器檔案安裝在錯誤的位置上

在 Solaris 系統中，Java ES 安裝程式將分散式認證 UI 伺服器的 `Makefile.distAuthUI`、`README.distAuthUI` 和 `amauthdistui.war` 檔案安裝在錯誤的位置上：`/opt/SUNComm/SUNWam`。

解決方法：將這些檔案複製到其正確的位置：`/opt/SUNWam`。

備註：任何已在修補程式中修正的分散式認證 UI 伺服器問題都將移至 `/opt/SUNComm/SUNWam/amauthdistui.war` 檔案，因此，每當您將修補程式套用至 Access Manager 伺服器，然後重建並部署 WAR 檔案時，您也必須將這些檔案複製到 `/opt/SUNWam` 目錄。

CR# 6522720：在 Windows 與 HP-UX 系統上，無法在主控台線上說明中搜尋多位元組字元

若 Access Manager 安裝於使用多位元組字元語言環境 (如日文) 的 Windows 或 HP-UX 系統上，無法在主控台線上說明中使用透過多位元組字元輸入的關鍵字進行搜尋。

解決方法：無

修補程式 6 更新：Access Manager 7 2005Q4 修補程式 6 修正了 Windows 系統中的這個問題。然而，HP-UX 系統中仍存在此問題。

CR# 6524251：在 Windows 系統上進行 Access Manager 的配置時，輸出訊息的多位元組字元顯示為亂碼

如果在 Windows 系統上，Access Manager 是安裝在使用多位元組字元的語言環境 (例如日文或中文)，則在 Access Manager 配置期間，終端機視窗的輸出訊息中會出現亂碼。

解決方法：無，但此問題並不會影響配置本身。

CR# 6526940：在 Windows 系統的非英文語言環境中安裝修補程式 5 時會出現特性碼，而不是訊息文字

如果您在 Windows 系統的非英文語言環境中安裝修補程式 5 (124296-05)，則安裝面板中的某些字串會顯示爲特性碼，而不是實際的訊息文字。特性碼的範例有 `PRODUCT_NAME`、`JES_Patch_FinishPanel_Text1` 和 `JES_Patch_FinishPanel_Text2`。

解決方法：無

CR# 6513653：與 com.iplanet.am.session.purgedelay 特性設定相關的問題

Access Manager `amtune` 程序檔會將 `com.iplanet.am.session.purgedelay` 特性設爲 1，以盡可能允許更多的 Access Manager 階段作業。此特性可指定清除階段作業要延遲的分鐘數。不過，對於像 Sun Java System Portal Server 這樣的用戶端來說，僅將該值設爲 1 可能還不夠。

解決方法：在執行 `amtune` 程序檔後重設 `com.iplanet.am.session.purgedelay` 特性：

1. 在 `AMConfig.properties` 檔案中，將該特性設爲新值。例如：

   ```
   com.iplanet.am.session.purgedelay=5
   ```

2. 重新啓動 Access Manager Web 容器以使該新值生效。

Access Manager 7 2005Q4 修補程式 4

Access Manager 7 2005Q4 修補程式 4 (修訂版 04) 修正了下列問題：

- CR# 6463796：停用 genericHTML 的 iPlanetAMClientDetection 服務會阻止存取任何 Access Manager HTML 頁面
- CR# 6463779：分散式認證 amProfile_Client 和 Access Manager 伺服器 amProfile_Server 充滿無害的異常
- CR# 6463730：goto 和 gx-charset 參數存在跨站點程序檔 (Cross-site scripting, XSS) 漏洞
- CR# 6435889：方法 Session.getSession 會由於未設定 RestrictedTokenContext 而失敗

修補程式 4 的已知問題和限制

- 第 40 頁的 「CR# 6470055：分散式認證 UI 伺服器效能改善」
- 第 40 頁的 「CR# 6455079：密碼重設服務會在密碼變更時報告通知錯誤」

CR# 6470055：分散式認證 UI 伺服器效能改善

若要改善分散式認證 UI 伺服器使用者對於使用者屬性的讀取、搜尋和比較之效能，請遵循下列步驟：

1. 在 Makefile.distAuthUI 檔案中，將應用程式使用者名稱從 anonymous 變更爲其他使用者。例如：

   ```
   APPLICATION_USERNAME=user1
   ```

2. 在 Directory Server 中，增加新使用者 (如範例中的 user1) 和 ACI 以允許對使用者屬性進行讀取、搜尋和比較。以下範例會增加新的 ACI：

   ```
   dn:ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com
   changetype:modify add:aci
   aci: (target="ldap:///ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com")
   (targetattr = *")(version 3.0;
   acl "SunAM client data access to a Distributed Auth App User";
   allow (read, search, compare)
   userdn =  "ldap:///uid=user1,ou=people,dc=example,dc=com";)
   ```

CR# 6455079：密碼重設服務會在密碼變更時報告通知錯誤

當密碼被變更時，Access Manager 會使用不合格的寄件者名稱 Identity-Server 送出電子郵件通知，這將在 amPasswordReset 記錄檔中產生錯誤項目。例如：

```
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：變更寄件者位址，變更爲 amPasswordResetModuleMsgs.properties 檔案中包含的主機伺服器之完全合格的網域名稱。

1. 變更寄件者位址標籤。例如：

   ```
   fromAddress.label=<Identity-Server@amhost.example.com>
   ```

2. 變更 `lockOutEmailFrom` 特性以確保鎖住通知使用正確的寄件者位址。例如：

   ```
   lockOutEmailFrom=<Identity-Server@amhost.example.com>
   ```

   `amPasswordResetModuleMsgs.properties` 檔案在 Solaris 系統上是位於 *AccessManager-base*`/SUNWam/locale` 目錄，在 Linux 系統上是位於 *AccessManager-base*`/identity/locale` 目錄。

   AccessManager-base 爲基底安裝目錄。預設基底安裝目錄在 Solaris 系統上爲 `/opt`，在 Linux 系統上爲 `/opt/sun`。

Access Manager 7 2005Q4 修補程式 3

Access Manager 7 修補程式 3 (修訂版 03) 修正了許多問題，這些問題列於修補程式隨附的讀我檔案中。修補程式 3 也包含下列新增功能及已知問題：

修補程式 3 的新增功能

- 第 42 頁的 「站點監視的新配置特性」
- 第 43 頁的 「Liberty Identity Web Services Framework (ID-WSF) 1.1 支援」

修補程式 3 的已知問題和限制

- 第 43 頁的 「CR# 6463779 分散式認證的 `amProfile_Client` 記錄檔及 Access Manager 伺服器的 `amProfile_Server` 記錄檔充滿無害的異常」
- 第 44 頁的 「CR# 6460974 預設的分散式認證應用程式使用者不應爲 `amadmin`」
- 第 44 頁的 「CR# 6460576 主控台線上說明的 [篩選的角色] 下沒有 [使用者服務] 的連結」
- 第 44 頁的 「CR# 6460085 在執行 `reinstallRTM` 並重新部署 Web 應用程式後，無法存取 WebSphere 上的伺服器」
- 第 45 頁的 「CR# 6455757：必須在升級前將 `sunISManagerOrganization` 記號類別加入組織」
- 第 45 頁的 「CR# 6454489：Access Manager 7 2005Q4 修補程式 2 升級導致主控台的 [目前階段作業] 標籤中出現錯誤」
- 第 46 頁的 「CR# 6452320：在用戶端 SDK 中使用輪詢會丟出異常」
- 第 46 頁的 「CR# 6442905 已認證使用者的 `SSOToken` 可能意外洩漏給居心不良的站點」
- 第 47 頁的 「CR# 6441918：站點監視間隔及逾時特性」
- 第 47 頁的 「CR# 6440697：分散式認證應以非 amadmin 使用者的身份執行」
- 第 47 頁的 「CR# 6440695：含有負載平衡器的分散式認證 UI 伺服器」
- 第 47 頁的 「CR# 6440651：Cookie 重送需要 `com.sun.identity.session.resetLBCookie` 特性」

站點監視的新配置特性

Access Manager 站點監視功能包含下列新特性：

特性	說明
com.sun.identity.sitemonitor.interval	站點監視的間隔時間 (以毫秒爲單位)。站點監視功能會在指定的時間間隔內檢查每一個站點的可用性。預設值：60000 毫秒 (1 分鐘)。
com.sun.identity.sitemonitor.timeout	站點可用性檢查的逾時時間 (以毫秒爲單位)。站點監視功能會在指定的逾時值內，等待來自站點的回應。預設值：5000 毫秒 (5 秒)。

修補程式沒有將以上這些特性加入 AMConfig.properties 檔案。若要以預設值以外的值使用這些新特性，請執行下列動作：

1. 將特性及其值加入下列目錄 (依您的平台而定) 中的 AMConfig.properties 檔案內：
   - Solaris 系統：/etc/opt/SUNWam/config
   - Linux 系統：/etc/opt/sun/identity/config

   若爲策略代理程式，請將這些特性加入 AMAgents.properties 檔案。
2. 重新啓動 Access Manager Web 容器以使這些值生效。

自訂實作。此外，com.sun.identity.sitemonitor.SiteStatusCheck 類別可讓您自訂自己的實作，以使用下列介面檢查站點可用性：

```
package com.iplanet.services.naming.WebtopNaming$SiteStatusCheck
```

每一個實作類別都必須使用 doCheckSiteStatus 方法。

```
public interface SiteStatusCheck {
public boolean doCheckSiteStatus(URL siteurl);
}
```

Liberty Identity Web Services Framework (ID-WSF) 1.1 支援

在 Access Manager 7 修補程式 3 中，ID-WSF 的預設版本爲 WSF1.1。您不需要個別的配置來觸發 ID-WSF，除非範例需要使用新安全機制。ID-WSF1.1 的新安全性機制有：

```
urn:liberty:security:2005-02:null:X509
urn:liberty:security:2005-02:TLS:X509
urn:liberty:security:2005-02:ClientTLS:X509
urn:liberty:security:2005-02:null:SAML
urn:liberty:security:2005-02:TLS:SAML
urn:liberty:security:2005-02:ClientTLS:SAML
urn:liberty:security:2005-02:null:Bearer
urn:liberty:security:2005-02:TLS:Bearer
urn:liberty:security:2005-02:ClientTLS:Bearer
```

Liberty ID-WSF 支援的新特性

Access Manager 用作 WCS 時，如果無法依據傳入訊息或資源提供確定 Liberty ID-WSF 架構，則 `com.sun.identity.liberty.wsf.version` 特性可確定 Liberty ID-WSF 架構。特性值可以是 1.0 或 1.1。預設值是 1.1。

備註 修補程式安裝不會將 `com.sun.identity.liberty.wsf.version` 特性加入 `AMConfig.properties` 檔案 (CR# 6458184)。若要使用此新特性，請在安裝修補程式後，將它及適當的值加入 `AMConfig.properties` 檔案，然後重新啓動 Access Manager Web 容器。

在安裝 Access Manager 7 修補程式 3 之後，請執行下列指令來載入模式變更 (以安裝在 Solaris 系統上預設目錄中的 Access Manager 爲例)：

```
# /opt/SUNWam/bin/amadmin -u amadmin -w amadmin_password
-t /etc/opt/SUNWam/wsf1.1_upgrade.xml
```

ID-WSF 探索註冊可以在註冊時使用這些新安全性機制。此外，WSC 與 WSP 通訊時會自動偵測要使用哪個版本。若要針對 ID-WSF1.1 進行配置，請遵循產品隨附的 Liberty ID-FF 範例 1 以及 ID-WSF 範例的讀我檔案。

CR# 6463779 分散式認證的 `amProfile_Client` 記錄檔及 Access Manager 伺服器的 `amProfile_Server` 記錄檔充滿無害的異常

透過分散式認證 UI 向 Access Manager 伺服器提出請求時，會觸發異常並記錄到 `distAuth/amProfile_Client` 記錄檔及 Access Manager 伺服器的 `debug/amProfile_Server` 記錄檔中。經過許多階段作業之後，`amProfile_Client` 記錄檔大小可能會擴充到數個 GB，而 Access Manager 伺服器的 `amProfile_Server` 記錄檔也可能增長到數個 MB。記錄檔中的異常不會導致功能失常，但會造成向使用者傳送假警報，而且記錄檔可能填滿硬碟空間。

解決方法：執行 `cron` 工作，如此可清空記錄檔內容。例如：

- 在分散式認證 UI 用戶端機器上，視流量每隔幾小時執行一次「`cat /dev/null > distAuth/amProfile_Client`」。
- 在 Access Manager 伺服器上，每隔幾天 (而非幾個小時) 執行一次「`cat /dev/null > /var/opt/SUNWam/debug/amProfile_Server`」。

CR# 6460974 預設的分散式認證應用程式使用者不應為 amadmin

如果部署分散式認證 UI 伺服器，則分散式認證管理員不應爲 `amadmin`。`Makefile.distAuthUI` 檔案中預設的分散式認證應用程式使用者是 `amadmin`，在用戶端部署了 `distAuth.war` 檔案之後，在 `AMConfig.properties` 檔案中也是 `amadmin`。`amadmin` 使用者具有在 `amadmin` 階段作業時間執行完畢之後到期的 `AppSSOToken`，因此會在 `amSecurity` 記錄檔 (預設位於 `/tmp/distAuth` 目錄) 中造成 FATAL ERROR。

解決方法：指定 `UrlAccessAgent` 做爲分散式認證應用程式使用者。例如：

在用戶端 Web 容器中部署 `distAuth.war` 檔案之前，請變更 `Makefile.distAuthUI` 檔案中的下列參數：

```
APPLICATION_USERNAME=UrlAccessAgent
APPLICATION_PASSWORD=shared-secret-password 或 amldapuser-password
```

或

在用戶端 Web 容器中部署 `distAuth.war` 檔案之後，請爲每個 Access Manager 伺服器變更 `AMConfig.properties` 檔案中的下列特性：

```
com.sun.identity.agents.app.username=UrlAccessAgent
com.iplanet.am.service.password=shared-secret-password 或 amldapuser-password
```

另請參閱第 47 頁的 「CR# 6440697：分散式認證應以非 amadmin 使用者的身份執行」。

CR# 6460576 主控台線上說明的 [篩選的角色] 下沒有 [使用者服務] 的連結

Access Manager 主控台線上說明的 [篩選的角色] 下沒有 [使用者服務] 的連結。在線上說明中，前往 [內容]、[篩選的角色] 及 [建立篩選的角色]。將頁面往下拉，依據您所選取的身份識別類型，畫面上會顯示一份服務清單，但其中沒有 [使用者服務] 連結。

解決方法：無

CR# 6460085 在執行 reinstallRTM 並重新部署 Web 應用程式後，無法存取 WebSphere 上的伺服器

在 Red Hat Linux AS 3.0 Update 4 的 IBM WebSphere Application Server 5.1.1.6 上對 `DEPLOY_LEVEL=1` 的部署套用 Access Manager 7 修補程式 3 之後，執行 `reinstallRTM` 程序

檔來復原 RTM RPM。然後，在編輯 reinstallRTM 程序檔產生的 amsilent 檔案後，重新部署 Web 應用程式。使用 stopServer.sh 及 startServer.sh 程序檔重新啓動 WebSphere。但是，在存取登入頁面時，WebSphere 顯示與 amlcontroller 篩選器有關的 500 錯誤。

發生此問題的原因在於 reinstallRTM 程序檔所產生的新 server.xml 檔案已毀壞。

解決方法：amconfig 程序檔所備份的 server.xml 檔案仍然有效。請使用此舊副本，方法如下：

1. 停止伺服器。
2. 將毀壞的 server.xml 替代爲 amconfig 程序檔所備份的副本。

   amconfig 程序檔所備份的 server.xml 檔案的名稱爲 server.xml-orig-*pid*，其中 *pid* 是 amwas51config 程序檔的程序 ID。該檔案位於下列目錄中：

   WebSphere-home-directory/config/cells/*WebSphere-cell*/nodes/*WebSphere-node*/servers/*server-name*
3. 重新啓動伺服器。

CR# 6455757：必須在升級前將 sunISManagerOrganization 記號類別加入組織

在 Access Manager 7 發行之前建立的 Access Manager DIT 中的組織可能沒有 sunISManagerOrganization 物件類別。此外，由 Access Manager 以外的產品建立的組織在其定義中也不會有 sunISManagerOrganization 物件類別。

解決方法：在升級到 Access Manager 7 2005Q4 之前，請確定 DIT 中所有組織的定義中都包含 sunISManagerOrganization 物件類別。必要時，請在升級前手動加入這個物件類別。

CR# 6454489：Access Manager 7 2005Q4 修補程式 2 升級導致主控台的 [目前階段作業] 標籤中出現錯誤

升級導致 Access Manager 主控台的 [目前階段作業] 標籤上出現下列錯誤：

無法由指定的伺服器取得有效的階段作業

對於從根尾碼格式爲 o=orgname 的 Access Manager 6 版本升級的部署，會發生此問題。

解決方法：在安裝 Manager 7 2005Q4 之後，請套用 Manager 7 修補程式 3，然後執行 amupgrade 程序檔來遷移資料，方法如下：

1. 備份 Access Manager 6 DIT。
2. 執行 ampre70upgrade 程序檔。
3. 選取 [以後配置] 選項來安裝 Access Manager 7 2005Q4。

4. 取消部署 Access Manager Web 應用程式。
5. 部署 Access Manager Web 應用程式。
6. 套用 Access Manager 7 修補程式 3，但不套用 XML/LDIF 變更。必須在下一步執行 `amupgrade` 程序檔之後再套用 XML/LDIF 變更。
7. 執行 `amupgrade` 程序檔。
8. 重新部署 Access Manager Web 應用程式，因爲 Access Manager 7 修補程式 3 進行了變更。
9. 存取 Access Manager 主控台。

CR# 6452320：在用戶端 SDK 中使用輪詢會丟出異常

部署 Access Manager 用戶端 SDK (`amclientsdk.jar`) 並啓用輪詢時，會發生如下錯誤：

```
ERROR: Send Polling Error:
com.iplanet.am.util.ThreadPoolException:
amSessionPoller thread pool's task queue is full.
```

在部署分散式認證 UI 伺服器、J2EE 代理程式之後，或在用戶端機器上部署了 Access Manager 用戶端 SDK 的情況下，都可能發生此類錯誤。

解決方法：如果只有幾百個同步運作的階段作業，請將下列特性及值加入 `AMConfig.properties` 檔案或 `AMAgents.properties` 檔案：

```
com.sun.identity.session.polling.threadpool.size=10
com.sun.identity.session.polling.threadpool.threshold=10000
```

如果有數千個或數萬個階段作業，則這些值應該設定成與執行 `amtune-identity` 程序檔後，Access Manager `AMConfig.properties` 檔案中通知的值相同。例如，對於具有 4 GB RAM 的機器，Access Manager `amtune-identity` 程序檔會設定下列值：

```
com.sun.identity.session.notification.threadpool.size=28
com.sun.identity.session.notification.threadpool.threshold=76288
```

當分散式認證 UI 伺服器或 Access Manager 用戶端 SDK 部署在具有 4GB RAM 的用戶端機器上時，請在用戶端的 `AMAgent.properties` 或 `AMConfig.properties` 檔案中設定類似的值。

CR# 6442905 已認證使用者的 SSOToken 可能意外洩漏給居心不良的站點

Access Manager 的已認證使用者按居心不良站點的 URL 時，可能會意外地將 `SSOToken` 洩漏給該站點。

解決方法：針對所有參與的策略代理程式，一律在 Access Manger 中建立唯一的代理程式使用者設定檔，以確保站點無不良企圖。此外，確保這些唯一的代理程式使用者都

沒有使用與共用機密密碼或 amldapuser 密碼相同的密碼。依預設，Access Manager 應用程式認證模組會將策略代理程式認證爲 UrlAccessAgent 使用者。

如需使用 Access Manager 管理主控台建立代理程式的更多資訊，請參閱「Sun Java System Access Manager 7 2005Q4 管理指南」中的「代理程式」。

CR# 6441918：站點監視間隔及逾時特性

Access Manager 站點容錯移轉包括下列新特性：

```
com.sun.identity.sitemonitor.interval
com.sun.identity.sitemonitor.timeout
```

如需更多資訊，請參閱第 42 頁的 「站點監視的新配置特性」。

CR# 6440697：分散式認證應以非 amadmin 使用者的身份執行

對於分散式認證應用程式認證，若要建立預設管理使用者 (amadmin) 以外的分散式認證管理員，請遵循下列程序：

1. 爲分散式認證管理員建立 LDAP 使用者。例如：

   ```
   uid=DistAuthAdmin,ou=people,o=am
   ```

2. 將分散式認證管理員加入特殊使用者清單中。例如：

   ```
   com.sun.identity.authentication.special.users=cn=dsameuser,
   ou=DSAME Users,o=am|cn=amService-UrlAccessAgent,ou=DSAME Users,
   o=am|uid=DistAuthAdmin,ou=People,o=am
   ```

   將此特性加入所有 Access Manager 伺服器的 AMConfig.properties 檔案，這樣分散式認證管理員的 AppSSOToken 在階段作業過期時也不會過期。

CR# 6440695：含有負載平衡器的分散式認證 UI 伺服器

如果在您的部署中，多個分散式認證 UI 伺服器前有負載平衡器，請在部署 WAR 檔案後在 AMConfig.properties 檔案中設定下列特性。

```
com.iplanet.am.lbcookie.name=DistAuthLBCookieName
com.iplanet.am.lbcookie.value=DistAuthLBCookieValue
```

CR# 6440651：Cookie 重送需要 com.sun.identity.session.resetLBCookie 特性

若要讓用於 Access Manager 階段作業容錯移轉的 cookie 重送功能正常運作，請爲策略代理程式和 Access Manager 伺服器增加值爲 true 的 com.sun.identity.session.resetLBCookie 特性。例如：

```
com.sun.identity.session.resetLBCookie='true'
```

- 若爲策略代理程式，請將該特性加入 AMAgent.properties 檔案。
- 若爲 Access Manager 伺服器，請將該特性加入 AMConfig.properties 檔案。

備註：只有在您已實作 Access Manager 階段作業容錯移轉後才需要該特性。

CR# 6440648：com.iplanet.am.lbcookie.name 特性假設預設值為 amlbcookie

依預設，策略代理程式及 Access Manager 伺服器都假設負載平衡器 cookie 名稱爲 amlbcookie。如果在後端伺服器上變更了 cookie 的名稱，則必須在 AMAgent.properties 檔案中爲策略代理程式使用相同的名稱。同樣，如果使用的是 Access Manager 用戶端 SDK，也必須使用與後端伺服器相同的 cookie 名稱。

CR# 6440641： com.iplanet.am.lbcookie.value 特性已停用

Access Manager 不再支援在伺服器上使用 com.iplanet.am.lbcookie.value 特性來自訂負載平衡器 cookie。Access Manager 現在改用伺服器 ID，伺服器 ID 配置爲階段作業配置的一部份，用於代理程式要重送的 cookie 值及名稱。

CR# 6429610：無法在 ID-FF SSO 使用案例中建立 SSO 記號

設定 Liberty Identity Federation Framework (ID-FF) 範例 1 之後，聯合成功，但 SSO 失敗。

解決方法：將 dsameuser 的 uuid 加入 AMConfig.properties 檔案的 com.sun.identity.authentication.special.users 特性中。若爲應用程式認證，dsameuser 需要 Access Manager 伺服器不會到期的 SSO 記號。

CR# 6389564：Access Manager 登入期間，在 LDAP v3 資料存放區中對使用者的角色成員身份進行重複不斷的查詢

當使用者登入 Access Manager 時，會對使用者的 nsRoleDN 屬性進行重複的 LDAP 搜尋。

解決方法：在安裝 Access Manager 7 修補程式 3 之後，請執行下列指令 (以安裝在 Solaris 系統上預設目錄中的 Access Manager 爲例)：

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/idRepoServiceAddAttrSchemaRequest_Cache.xml
```

CR# 6385185：認證模組必須可以置換「goto」URL 並指定不同的 URL

認證模組可以置換「goto」URL 並請求重新導向至其他外部網站的 URL，以便驗證使用者狀態。

若要在認證完成後置換「goto」URL，請在 SSOToken 中設定下列範例所示的特性。可使用實作 AMPostAuthProcessInterface 的 PostProcess 類別的 onLoginSuccess 方法來設定此特性。例如，在下例中 *OverridingURL* 即爲置換「goto」URL 的 URL：

```
public class <..> implements AMPostAuthProcessInterface {
...
    public void onLoginSuccess(...) {
        try {
            ssoToken.setProperty("PostProcessSuccessURL", OverridingURL);
         } catch (Exception ...) {
         ...         }
...
}
```

CR# 6385184：當 SSO 記號仍處於無效狀態時，從自訂認證模組重新導向

自訂認證模組中的新 RedirectCallback 允許透過認證 UI 重新導向至外部網站，以便驗證使用者。如果認證成功，則會將使用者重新導向回原來的 Access Manager 伺服器 URL。範例檔案包括：

- LoginModuleSample.java
- LoginModuleSample.xml
- testExtWebSite.jsp

若要實作此功能：

1. 使用範例 LoginModuleSample.java 建立自訂認證模組。
2. 將該模組載入 Access Manager 伺服器。
3. 使用範例 LoginModuleSample.xml 在 XML 檔案中建構 RedirectCallback。
4. 將範例 testExtWebSite.jsp 檔案用於外部網站，以測試該模組。
5. 使用下列 URL 登入：

   ```
   http://example.com/amserver/UI/Login?module=LoginModuleSample
   ```

使用者名稱及密碼會重新導向至外部網站進行驗證。如果名稱及密碼有效，則認證成功，而且會將使用者重新導向回到原來的 Access Manager 伺服器 URL。

例如，請思考這樣的情況，在此情況中，部署使用自訂認證模組來存取佈建/信用卡站點：

1. 使用者呼叫自訂認證模組的認證程序/登入頁面。
2. 使用者輸入憑證 (使用者名稱及密碼)，並向自訂認證模組提交請求。
3. 自訂認證模組將使用者重新導向至外部佈建/信用卡站點，同時隨附請求及必要的使用者資訊。

4. 外部佈建/信用卡站點檢查使用者的狀態，並傳回請求成功或失敗的訊息，該訊息設定爲所傳回之請求的一部分。
5. 自訂認證模組根據步驟 4 中傳回的狀態驗證使用者，並將對應狀態傳回認證服務。
6. 使用者認證完成，結果爲成功或失敗。

CR# 6324056：使用工件設定檔時聯合失敗

解決方法：若要修正此問題，請根據您的平台套用最新版本的「Core Mobile Access」修補程式：

- 基於 SPARC 之系統上的 Solaris OS：119527
- x86 平台上的 Solaris OS：119528
- Linux 系統：119529

套用修補程式後，重新啓動 Web 容器。

Access Manager 7 2005Q4 修補程式 2

Access Manager 7 2005Q4 修補程式 2 (修訂版 02) 修正了許多問題，這些問題列於修補程式隨附的讀我檔案中。修補程式 2 也包含下列新增功能及已知問題：

修補程式 2 的新增功能

- 第 50 頁的「用於使用者管理、識別儲存庫及服務管理快取的新特性」
- 第 52 頁的「用於聯合服務提供者的新特性」
- 第 52 頁的「LDAP 篩選器條件支援 」

修補程式 2 的已知問題和限制

- 第 52 頁的「CR# 6283582：Access Manager 實例之間沒有共用登入失敗次數」
- 第 53 頁的「CR# 6293673：傳送階段作業逾時通知時，需要保留原始階段作業資訊」
- 第 53 頁的「CR# 6244578：Access Manager 應該警告使用者瀏覽器 cookie 支援已停用/無法使用」
- 第 53 頁的「CR# 6236892：登入後，CDCServlet 處理 AuthNResponse 出現影像/文字預留位置」
- 第 53 頁的「CR# 6363157：新特性會在絕對必要時停用持續搜尋」
- 第 54 頁的「CR# 6385696：看不見現有的和新的 IDP 和 SP」

用於使用者管理、識別儲存庫及服務管理快取的新特性

修補程式 2 包含下列用於使用者管理 (Access Manager SDK)、識別儲存庫 (Identity Repository, IdRepo) 及服務管理快取的新特性。這些特性讓您可以根據部署需求獨立地啓用和停用不同的快取，以及設定快取項目的存活時間 (Time to Live, TTL)。

表 3 用於使用者管理、識別儲存庫及服務管理快取的新特性

特性	說明
用於啓用和停用快取的新特性	
`com.iplanet.am.sdk.caching.enabled`	全域特性，可啓用 (true) 或停用 (false) 識別儲存庫 (IdRepo)、使用者管理及服務管理快取。若爲 true，或是 `AMConfig.properties` 檔案中無此特性，則這三個快取皆會被啓用。
備註：下列三個特性用於啓用或停用指定的快取，但只在前述的全域特性設爲 false 時才有用。	
`com.sun.identity.amsdk.cache.enabled`	僅啓用 (true) 或停用 (false) 使用者管理 (Access Manager SDK) 快取。
`com.sun.identity.idm.cache.enabled`	僅啓用 (true) 或停用 (false) 識別儲存庫 (IdRepo) 快取。
`com.sun.identity.sm.cache.enabled`	僅啓用 (true) 或停用 (false) 服務管理快取。
TTL 的新使用者管理快取特性.	
`com.iplanet.am.sdk.cache.entry .expire.enabled`	啓用 (true) 或停用 (false) 使用者管理快取的過期時間 (由下列兩個特性所定義)。
`com.iplanet.am.sdk.cache.entry.user .expire.time`	指定使用者管理快取的使用者項目自從前一次修改後保持有效的時間，以分鍾爲單位。亦即，超過此指定時間後 (在前一次修改或從目錄讀取之後)，快取項目的資料即會過期。然後，若有針對這些項目之資料的新請求，則必須從目錄讀取。
`com.iplanet.am.sdk.cache.entry.default .expire.time`	指定使用者管理快取的非使用者項目自從前一次修改後保持有效的時間，以分鍾爲單位。亦即，超過此指定時間後 (在前一次修改或從目錄讀取之後)，快取項目的資料即會過期。然後，若有針對這些項目之資料的新請求，則必須從目錄讀取。TTL 的新識別儲存庫快取特性。
`com.sun.identity.idm.cache.entry .expire.enabled`	啓用 (true) 或停用 (false) IdRepo 快取的過期時間 (由下列特性所定義)。
`com.sun.identity.idm.cache.entry.default .expire.time`	指定 IdRepo 快取的非使用者項目自從前一次修改後保持有效的時間，以分鍾爲單位。亦即，超過此指定時間後 (在前一次修改或從儲存庫讀取之後)，快取項目的資料即會過期。然後，若有針對這些項目之資料的新請求，則必須從儲存庫讀取。

使用新的快取特性

Access Manager 7 2005Q4 修補程式不會自動將新的快取特性加入 `AMConfig.properties` 檔案中。

若要使用新的快取特性：

1. 使用文字編輯器，將特性及它們的值加入下列目錄 (依您的平台而定) 中的 `AMConfig.properties` 檔案：
   - Solaris 系統：`/etc/opt/SUNWam/config`
   - Linux 系統：`/etc/opt/sun/identity/config`
2. 重新啓動 Access Manager Web 容器以使這些值生效。

用於聯合服務提供者的新特性

新的 `com.sun.identity.federation.spadapter` 特性定義了 `com.sun.identity.federation.plugins.FederationSPAdapter` 的實作類別，該類別用於在服務提供者端的聯合處理期間，增加應用程式特定的處理。

另請參閱第 54 頁的 「CR# 6385696：看不見現有的和新的 IDP 和 SP」 。

LDAP 篩選器條件支援

修補程式 2 中增加了 [LDAP 篩選器條件] 支援。策略管理員現在可以在定義策略時在 [條件] 中指定 LDAP 篩選器。只有當使用者的 LDAP 項目符合 [條件] 中指定的 LDAP 篩選器時，才會對使用者套用策略。使用者的 LDAP 項目是在 [策略配置] 服務所指定的目錄內查詢。

若要註冊並使用 [LDAP 篩選條件]，請在安裝 Access Manager 7 修補程式 2 之後執行下列指令 (以安裝在 Solaris 系統上預設目錄中的 Access Manager 爲例)：

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-s /etc/opt/SUNWam/AddLDAPFilterCondition.xml
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/amPolicyConfig_mod_ldfc.xml
```

修補程式 5 備註 如果您已增加 Access Manager 7 2005Q4 修補程式 5 並執行 `updateschema.sh` 程序檔，則不需要使用 `amadmin` 來載入這些檔案。如需更多資訊，請參閱第 27 頁的 「用於載入 LDIF 和 XML 檔案的新 `updateschema.sh` 程序檔」 。

CR# 6283582：Access Manager 實例之間沒有共用登入失敗次數

在安裝 Access Manager 7 修補程式 2 之後，請執行下列指令 (以安裝在 Solaris 系統上預設目錄中的 Access Manager 爲例)：

```
# cd DirectoryServer-base/shared/bin
# ./ldapmodify -h DirectoryServerHost -p DirectoryServerPort
-D "cn=Directory Manager" -w DirectoryMangerPassword
-a -f /etc/opt/SUNWam/accountLockout.ldif
```

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/accountLockoutData.xml
```

DirectoryServer-base 的預設值在 Solaris 系統上是 `/var/opt/mps/serverroot`，在 Linux 系統上是 `/var/opt/sun/directory-server`。

修補程式 5 備註 如果您已增加 Access Manager 7 2005Q4 修補程式 5 並執行 `updateschema.sh` 程序檔，則不需要使用 `amadmin` 來載入這些檔案。如需更多資訊，請參閱第 27 頁的 「用於載入 LDIF 和 XML 檔案的新 `updateschema.sh` 程序檔」。

CR# 6293673：傳送階段作業逾時通知時，需要保留原始階段作業資訊

`AMConfig.properties` 檔案中的新 `com.sun.identity.session.property.doNotTrimList` 特性可包含階段作業特性名稱清單 (以逗號分隔)。一旦階段作業逾時，在此清單中定義的特性也不會被移除，這樣在清除階段作業之前仍可存取它們。例如：

```
com.sun.identity.session.property.doNotTrimList=UserId,HostName
```

CR# 6244578：Access Manager 應該警告使用者瀏覽器 cookie 支援已停用/無法使用

`AMConfig.properties` 檔案中的新 `com.sun.identity.am.cookie.check` 特性指示伺服器是否應該檢查瀏覽器有無支援/啓用 cookie。值爲 `true` 時，伺服器將檢查瀏覽器是否支援/啓用 cookie，如果瀏覽器不支援或尚未啓用 cookie，則丟出錯誤頁面。如果希望伺服器爲認證功能提供無 cookie 模式支援，則應該將值設爲 false (即預設值)。

CR# 6236892：登入後，CDCServlet 處理 AuthNResponse 出現影像/文字預留位置

`AMConfig.properties` 檔案中加入了下列新特性，並且這些特性由 CDCServlet 讀取：

- `com.iplanet.services.cdc.WaitImage.display` 如果設定爲 true，則當使用者在 CDSSO 分析藍本中等待受保護的頁面時，瀏覽器中會顯示影像。預設值是 false。
- `com.iplanet.services.cdc.WaitImage.name` 指定影像名稱。預設值是 `waitImage.gif`。此影像是從 `login_images` 目錄中複製的。
- `com.iplanet.services.cdc.WaitImage.width` 指定影像寬度。預設值是 420。
- `com.iplanet.services.cdc.WaitImage.height` 指定影像高度。預設值是 120。

CR# 6363157：新特性會在絕對必要時停用持續搜尋

`AMConfig.properties` 檔案中的新 `com.sun.am.event.connection.disable.list` 特性指定可以停用的事件連線。可能的值 (大小寫不需相符) 有：

`aci` - 對 `aci` 屬性的變更，使用 LDAP 篩選器 (`aci=*`) 進行搜尋

sm - 在 Access Manager 資訊樹狀結構 (或服務管理節點) 中進行的變更，其中包含 sunService 或 sunServiceComponent 記號物件類別的物件。例如，您可能需要建立策略來定義受保護資源的存取權限，或者需要修改現有策略的規則、主旨、條件或回應提供者。

um - 在使用者目錄 (或使用者管理節點) 中進行的變更。例如，您可能要變更使用者的名稱或位址。

例如，若要停用持續搜尋以變更 Access Manager 資訊樹狀結構 (或服務管理節點)：

```
com.sun.am.event.connection.disable.list=sm
```

若要指定多個值，請以逗號分隔每個值。

注意 – 持續搜尋可能會使 Directory Server 增加效能負荷。如果您確定在生產環境中移除一部分效能負荷有絕對的必要性，則可以使用 com.sun.am.event.connection.disable.list 特性來停用一個或多個持續搜尋。

不過，在您停用持續搜尋之前，必須先瞭解上述限制。我們強烈建議您除非絕對必要，否則請不要變更該特性。引入此特性的主要目的是，避免在使用多個 2.1 J2EE 代理程式時由於每個代理程式都會建立這些持續搜尋而導致 Directory Server 發生超負荷。2.2 J2EE 代理程式不再建立這些持續搜尋，因此您可能不需要使用此特性。

如需更多資訊，請參閱第 86 頁的 「記錄有關停用持續搜尋的更多資訊 (6486927)」。

CR# 6385696：看不見現有的和新的 IDP 和 SP

AMConfig.properties 檔案中的新 com.sun.identity.federation.spadapter 特性指定聯合服務提供者介面的預設實作，應用程式可以從中取得宣示及回應資訊。例如：

```
com.sun.identity.federation.spadapter=com.sun.identity.federation.plugins.FSDefaultSPAdapter
```

Access Manager 7 2005Q4 修補程式 1

Access Manager 7 2005Q4 修補程式 1 (修訂版 01) 修正了許多問題，這些問題列於修補程式隨附的讀我檔案中。修補程式 1 也包含下列新增功能及已知問題：

建立除錯檔案

預設情況下，Access Manager 除錯檔案建立於除錯目錄中，即使 `AMConfig.properties` 檔案中的 `com.iplanet.services.debug.level` 特性設定爲 error 也是如此。Access Manager 7 修補程式 1 發行以前，只有第一則除錯訊息記錄到檔案時才會建立除錯檔案。

支援 LDAPv3 外掛程式中的角色及已篩選角色

如果資料儲存於 Sun Java System Directory Server 中，則 Access Manager 7 修補程式 1 會增加對 LDAPv3 外掛程式中角色及已篩選角色的支援。如需更多資訊，請參閱第 90 頁的 「記錄可支援 LDAPv3 外掛程式的角色和已篩選角色 (6365196)」。

CR# 6320475：伺服器端的 `com.iplanet.am.session.client.polling.enable` 不得為 true

伺服器端的 `AMConfig.properties` 檔案中的 `com.iplanet.am.session.client.polling.enable` 特性預設爲 false，且不應重設爲 true。

CR# 6358751：如果在加密金鑰中有內嵌的空格，則套用 Access Manager 7 修補程式 1 會失敗

如果密碼加密金鑰包含空格，則套用修補程式會失敗。

解決方法：使用不含空格的新加密金鑰。如需變更加密金鑰的詳細步驟，請參閱：「Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide」中的附錄 B「Changing the Password Encryption Key」。

此版本的新增功能

如需 Access Manager 修補程式版本的新增功能清單，請參閱第 9 頁的 「Access Manager 7 2005Q4 修補程式版本」。Access Manager 7 2005Q4 的初期測試版包含下列新增功能：

- 第 59 頁的 「策略模組增強功能」
- 第 60 頁的 「站點配置」
- 第 60 頁的 「大量聯合」
- 第 60 頁的 「記錄增強功能」

Access Manager 模式

Access Manager 7 2005Q4 包含「範圍」模式與「舊有」模式。兩種模式皆支援：

- Access Manager 7 2005Q4 的新增功能
- Access Manager 6 2005Q1 功能，但是有以下限制：
  - 已建立範圍，但未在 Sun Java System Directory Server 中建立對應的組織。
  - 新的 Access Manager 7 2005Q4 主控台無法設定「服務類別 (CoS)」範本優先權。請參閱第 75 頁的 「新的 Access Manager 主控台無法設定 CoS 範本優先權 (6309262)」。
- Sun Java System Directory Server 的識別儲存庫及其他資料儲存區

以下情形必須使用「舊有」模式：

- Sun Java System Portal Server
- Sun Java System Communication Services 伺服器，包括 Messaging Server、Calendar Server、Instant Messaging 或 Delegated Administrator
- Access Manager 6 2005Q1 與 Access Manager 7 2005Q4 存取同一個 Directory Server 時，不同部署共存的情形

新的 Access Manager 主控台

Access Manager 主控台已針對此版本進行了重新設計。但是，如果 Access Manager 與 Portal Server、Messaging Server、Calendar Server、Instant Messaging 或 Delegated Administrator 共同部署，則必須於「舊有」模式下安裝 Access Manager 並使用 Access Manager 6 2005Q1 主控台：

如需更多資訊，請參閱第 63 頁的 「相容性問題」。

識別儲存庫

Access Manager 識別儲存庫包含與使用者、群組及角色等身份識別相關的資訊。您可使用 Access Manager 或其他佈建產品，如 Sun Java System Identity Manager 來建立和維護識別儲存庫。

在目前的版本中，識別儲存庫可以位在 Sun Java System Directory Server 或 Microsoft Active Directory 之中。Access Manager 可具有對識別儲存庫的讀取/寫入存取權或唯讀存取權。

Access Manager 資訊樹

Access Manager 資訊樹包含與系統存取相關的資訊。每個 Access Manager 實例都會在 Sun Java System Directory Server 中分別建立與維護一個資訊樹。一個 Access Manager 資訊樹可具有任何名稱 (字尾)。Access Manager 資訊樹包含範圍 (必要時也包含子範圍)，下面的小節將進行說明。

Access Manager 範圍

範圍和任何的子範圍都是 Access Manager 資訊樹的一部分，包含下列定義使用者集與/或群組的配置資訊：使用者認證方式、使用者可以存取的資源以及核准使用者存取資源後應用程式可用的資訊。範圍或子範圍也可包含其他配置資訊，其中包括：全域配置、密碼重設配置、階段作業配置、主控台配置及使用者喜好設定。範圍或子範圍可以爲空。

您可使用 Access Manager 主控台或 `amadmin` CLI 公用程式來建立範圍。如需更多資訊，請參閱主控台線上說明，或「Sun Java System Access Manager 7 2005Q4 管理指南」中的第 14 章「amadmin 指令行工具」。

階段作業容錯移轉變更

Access Manager 提供一個 Web 容器的獨立階段容錯移轉備用實作，其中以 Sun Java System Message Queue (Message Queue) 做爲通訊代理程式，以 Sleepycat Software, Inc. 開發的 Berkeley DB 做爲階段作業儲存資料庫。Access Manager 7 2005Q4 的增強功能包括：配置階段作業容錯移轉環境的 `amsfoconfig` 程序檔、啓動及停止 Message Queue 代理程式與 Berkeley DB 用戶端的 `amsfo` 程序檔。

如需更多資訊，請參閱「Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide」中的「Implementing Access Manager Session Failover」。

階段作業特性變更通知

階段作業特性變更通知功能可讓 Access Manager 於特定階段作業特性發生變更時，傳送通知給特定偵聽程式。在 Access Manager 管理員主控台中啓用 [啓用特性變更通知] 屬性時，此功能便生效。例如，在單次登入 (Single Sign-On, SSO) 環境中，多個應用程式可以共用一個 Access Manager 階段作業。當 [通知特性] 清單中定義的特定階段作業特性發生變更時，Access Manager 就會傳送通知給所有已註冊的偵聽程式。

如需更多資訊，請參閱「Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide」中的「Enabling Session Property Change Notifications」。

階段作業配額限制

階段作業配額限制功能可讓 Access Manager 管理員 (amadmin) 設定 [使用中的使用者階段作業] 屬性，以限制允許使用者使用的最大同步運作階段作業數。管理員可在全域層級設定所有使用者的階段作業配額限制，或設定僅適用於一或數位特定使用者之單一實體，如組織、範圍、角色或使用者的階段作業配額限制。

依預設，會停用階段作業配額限制 (「關閉」)，但管理員可將 Access Manager 管理員主控台的 [啓用配額限制] 屬性設定爲啓用，來啓用它們。

若使用者用盡階段作業限制配額，管理員也可將 [若用盡階段作業的配額將導致] 屬性設爲以下值，來配置配額用盡時要進行的動作：

- DENY_ACCESS。Access Manager 會拒絕登入新階段作業的請求。
- DESTROY_OLD_SESSION。Access Manager 會刪除同一位使用者的下一個即將到期之現有階段作業，並接受新的登入請求繼續作業。

[免除頂層管理員的限制檢查] 屬性會指定階段作業限制配額是否適用於具「頂層管理員角色」的管理員。

如需更多資訊，請參閱「Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide」中的「Setting Session Quota Constraints」

分散式認證

Access Manager 7 2005Q4 包含分散式認證 UI，這是一個遠端認證 UI 元件，可在部署中提供跨越兩道防火牆之安全的分散式認證。若沒有分散式認證 UI 元件，Access Manager 服務 URL 會曝露在一般使用者之前。要避免曝露在一般使用者之前，可使用代理伺服器；然而，在許多部署中，代理伺服器不是可接受的解決方案。

分散式認證 UI 元件是安裝在 Access Manager 部署的非安全 (DMZ) 層中一或數個伺服器上。分散式認證 UI 伺服器不會執行 Access Manager；它僅用來提供透過 Web 瀏覽器的認證介面給一般使用者。

一般使用者傳送 HTTP 請求至分散式認證 UI，此介面會先傳送登入頁面給使用者。然後分散式認證元件會經由第二道防火牆將使用者的請求傳送給 Access Manager 伺服器，免除了在一般使用者和 Access Manager 伺服器防火牆之間打開通道的需要。

如需更多資訊，請參閱「Technical Note: Using Access Manager Distributed Authentication」。

多重認證模組實例支援

所有認證模組 (預設配置) 均已延伸爲支援能支援主控台 UI 的子模式。針對每個模組類型 (已載入的模組類別) 分別可以建立多個認證模組實例。例如，對 LDAP 模組類型之名稱爲 `ldap1` 與 `ldap2` 的實例而言，每個實例均可指向不同的 LDAP 目錄伺服器。其名稱與類型名稱相同的模組實例具備向下相容性。其呼叫方法爲：

server_deploy_uri`/UI/Login?module=`*module-instance-name*

認證「已命名配置」或「鏈接」名稱空間

單獨的名稱空間是建立在組織/範圍之下，是認證模組實例的鏈接。相同鏈接可重複使用，並指定給組織/範圍、角色或使用者。「認證服務」實例等同於「認證鏈」。其呼叫方法爲：

server_deploy_uri`/UI/Login?service=`*authentication-chain-name*

策略模組增強功能

個人化屬性

除了「規則」、「主體」及「條件」以外，現在策略也有個人化屬性 (`IDResponseProvider`)。從策略評估傳送至用戶端的策略決定現在包括適用策略中的基於策略的回應個人化屬性。受支援的個人化屬性類型有以下兩種：

- 靜態屬性。在策略中定義屬性名稱與值。
- 動態屬性。在策略中列示屬性名稱，於評估策略時從「識別儲存庫」資料儲存區擷取值。

「策略執行點 (代理程式)」通常會將這些屬性值以 HTTP 標頭、Cookie 或請求屬性的形式轉遞至受保護的應用程式。

Access Manager 7 2005Q4 不支援客戶自行實作的「回應提供者」介面。

階段作業特性條件

階段作業特性條件實作 (`SessionPropertyCondition`) 會根據使用者的 Access Manager 階段作業中設定之特性值，決定策略是否適用於某個請求。評估策略時，只有在使用者的 Access Manager 階段作業之每個特性值於條件中皆有定義時，條件才會傳回「true」。若條件中將特性定義爲具多重值，則條件中只需列出使用者階段作業特性的一個值便已足夠。

策略主體

策略主體實作 (Access Manager 識別主體) 允許您使用已配置識別儲存庫中的項目做爲策略主體值。

策略匯出

您可使用 amadmin 指令，以 XML 格式將策略匯出。amAdmin.dtd 檔案中的新元素 GetPolices 與 RealmGetPolicies 支援此功能。

策略狀態

現在策略具有狀態屬性，可將其設爲使用中或非使用中。策略評估時會忽略非使用中的策略。

站點配置

Access Manager 7 2005Q4 引進了「站點概念」，可提供對 Access Manager 部署的集中式配置管理。將 Access Manager 配置爲站點時，用戶端請求一律會通過負載平衡器，如此可簡化部署程序並解決如用戶端和後端 Access Manager 伺服器之間防火牆阻隔的問題。

如需更多資訊，請參閱「Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide」中的「Configuring an Access Manager Deployment as a Site」。

大量聯合

Access Manager 7 2005Q4 對外包給企業合作夥伴的應用程式提供大量聯合使用者帳號之功能。之前，服務提供者 (SP) 與識別提供者 (IDP) 間帳號的聯合需要每位使用者分別存取 SP 與 IDP 的站點、建立帳號 (若尚未建立)、然後透過 Web 連結將兩個帳號聯合起來。如此的處理程序非常耗時。而且對現有帳號的部署或對將本身當作識別提供者，或使用其夥伴之一做爲認證提供者的站點而言，不一定都適合此方式。

如需更多資訊，請參閱「Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide」。

記錄增強功能

Access Manager 7 2005Q4 包含數個新的記錄增強功能：

- 新增欄位 (或欄)：MessageID 欄位內含已記錄事件的訊息識別碼。ContextID 欄位內含內容識別碼，其類似階段作業識別碼，會套用至特定使用者登入階段作業的所有事件。對使用者的特定登入階段作業而言，已記錄事件的所有記錄檔之 ContextID 均相同。
- 記錄 API。API 包含了讀取記錄檔記錄的新增功能，如果已配置資料庫 (DB) 記錄時，也包括讀取 DB 的記錄。請參考 /opt/SUNWam/samples/logging 目錄下的 LogReaderSample.java，其會顯示從平面檔案或 DB 表格儲存庫擷取記錄檔記錄的方法。

注意 – 資料庫表格會比平面檔案記錄大。因此，請不要在請求中要求擷取資料庫表格內的所有記錄，因爲資料數量過大，會消耗所有 Access Manager 伺服器資源。

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 4 硬體與軟體需求

元件	需求
作業系統 (OS)	基於 SPARC™ 之系統上的 Solaris OS 版本 8、9 及 10，包含對 Solaris 10 上整個本機根區域的支援 在 x86 平台上的 Solaris OS，版本 9 和 10，包括對 Solaris 10 上整個本機根區域的支援 在 AMD64 平台上的 Solaris OS，版本 10，包括對整個本機根區域的支援 Red Hat™ Linux, WS/AS/ES 2.1 Update 6 或更高版本 Red Hat Linux WS/AS/ES 3.0 Red Hat Linux, WS/AS/ES 3.0 Update 1、2、3 和 4 HP-UX OS。請參閱適用於 HP-UX 的 Sun Java Enterprise System 2005Q4 文件集：`http://docs.sun.com/coll/1258.2` 及 `http://docs.sun.com/coll/1530.1` Windows OS。請參閱適用於 Microsoft Windows 的 Sun Java Enterprise System 2005Q4 文件集：`http://docs.sun.com/coll/1259.2` 及 `http://docs.sun.com/coll/1513.1`
Java 2 Standard Edition (J2SE)	J2SE 平台 1.5.0_04、1.5_01、1.5 及 1.4.2
Directory Server	Access Manager 資訊樹：Sun Java System Directory Server 5 2005Q4 Access Manager 識別儲存庫：Sun Java System Directory Server 5 2005Q4 或 Microsoft Active Directory

表 4 硬體與軟體需求 (續)

元件	需求
Web 容器	Sun Java System Web Server 6.1 2005Q4 SP5
	Sun Java System Application Server Enterprise Edition 8.1 2005Q2
	BEA WebLogic Server 8.1 SP4
	IBM WebSphere Application Server 5.1 與 5.1.1 (及相關的不斷增加的修正程式)
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 2005Q4 版本支援的瀏覽器。

表 5 支援的瀏覽器

瀏覽器	平台
Microsoft Internet Explorer™ 5.5 SP2	Windows™ 2000
Microsoft Internet Explorer 6.0	Windows 2000
	Windows XP
Mozilla 1.7.1	Solaris OS 版本 9 及 10
	Java Desktop System
	Windows 2000
	Red Hat Linux 8.0
Netscape™ 7.0	Solaris OS 版本 9 及 10
	Java Desktop System
	Windows 2000
	Red Hat Linux 8.0

系統虛擬支援

系統虛擬是一種可讓多個作業系統 (OS) 實例在共用硬體上獨立執行的技術。就功能性而言，針對虛擬化環境中代管的作業系統所部署的軟體，通常不會知道底層的平台已經虛擬化。Sun 會在選定系統虛擬與 OS 組合上執行其 Sun Java System 產品的測試，以協助驗證 Sun Java System 產品在適當規模及正確配置的虛擬環境上是否能夠繼續運作，如同在非虛擬系統上一樣。如需 Sun 對於虛擬化環境中的 Sun Java System 產品所提供的支援的相關資訊，請參閱 http://docs.sun.com/doc/820-4651。

相容性問題

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：

如需判定 Access Manager 7 2005Q4 安裝方式的詳細資訊，請參閱第 64 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
...
```

如需有關使用狀態檔案以無訊息模式執行 Java ES 安裝程式的更多資訊，請參閱「Sun Java Enterprise System 2005Q4 安裝指南」中的第 5 章「以無訊息模式安裝」。

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)]** `[Legacy]` 選取預設值 `Legacy`。

[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
...
```

在 Windows 系統上，配置檔案爲 *AccessManager-base*`\setup\AMConfigurator.properties`。

如需透過執行 `amconfig` 程序檔配置 Access Manager 的更多資訊，請參閱「Sun Java System Access Manager 7 2005Q4 管理指南」。

判定 Access Manager 模式

若要判定執行的 Access Manager 7 2005Q4 安裝是在「範圍」或「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 2005Q4 模式的相容性。

表 6 策略代理程式與 Access Manager 7 2005Q4 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
Web 代理程式，版本 2.1	舊有模式與範圍模式
J2EE 代理程式，版本 2.1	僅限舊有模式

安裝注意事項

Access Manager 安裝注意事項包括下列資訊：

- 第 63 頁的 「Access Manager 舊有模式」
- 第 67 頁的 「安裝問題」

已知問題和限制

本節說明此版本發行時的已知問題和解決方法 (如有提供)。

- 第 65 頁的 「相容性問題」
- 第 67 頁的 「安裝問題」
- 第 69 頁的 「升級問題」
- 第 71 頁的 「配置問題」
- 第 74 頁的 「Access Manager 主控台問題」
- 第 76 頁的 「SDK 與用戶端問題」
- 第 77 頁的 「指令行公用程式問題」
- 第 78 頁的 「認證問題」
- 第 79 頁的 「階段作業與 SSO 問題」
- 第 81 頁的 「策略問題」
- 第 81 頁的 「伺服器啓動問題」
- 第 82 頁的 「Linux OS 問題」
- 第 82 頁的 「聯合與 SAML 問題」
- 第 83 頁的 「全球化 (Globalization, g11n) 問題」
- 第 85 頁的 「文件問題」

相容性問題

- 第 66 頁的 「Java ES 2004Q2 伺服器與 Java ES 2005Q4 上 IM 之間的不相容問題 (6309082)」
- 第 66 頁的 「舊有模式下核心認證模組中存有的不相容問題 (6305840)」
- 第 66 頁的 「代理程式無法登入，因爲 [設定檔不在組織中] (6295074)」
- 第 66 頁的 「Delegated Administrator `commadmin` 公用程式未建立使用者 (6294603)」

- 第 67 頁的 「Delegated Administrator commadmin 公用程式未建立組織 (6292104)」

Java ES 2004Q2 伺服器與 Java ES 2005Q4 上 IM 之間的不相容問題 (6309082)

下列部署方案造成了此問題：

- server-1：Java ES 2004Q2：Directory Server
- server-2：Java ES 2004Q2：Application Server、Access Manager 及 Portal Server
- server-3：Java ES 2004Q2：Calendar Server 與 Messaging Server
- server-4：Java ES 2005Q4：Application Server、Instant Messaging 及 Access Manager SDK

於 server-4 上執行 `imconfig` 公用程式配置 Instant Messaging 時，配置不成功。Access Manager 7 2005Q4 SDK 由 server-4上的 Instant Messaging (IM) 使用時，其與 Java ES 2004Q2 版本不相容。

解決方法：理論上，Access Manager 伺服器版本應與 Access Manager SDK 的版本相同。如需更多資訊，請參閱「Sun Java Enterprise System 2005Q4 升級指南」。

舊有模式下核心認證模組中存有的不相容問題 (6305840)

Access Manager 7 2005Q4 舊有模式自 Access Manager 6 2005Q1 開始，於核心認證模組中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 2005Q4 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。

代理程式無法登入，因為 [設定檔不在組織中] (6295074)

在 Access Manager 主控台中，於「範圍」模式下建立一個代理程式。若登出後使用代理程式名稱再次登入，Access Manager 會傳回錯誤訊息，因爲代理程式不具存取該範圍的權限。

解決方法：修改權限以允許代理程式的讀取/寫入存取。

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 2005Q4，但未將 Delegated Administrator 升級，就會發生此問題。如需升級 Delegated Administrator 的資訊，請參閱「Sun Java Enterprise System 2005Q4 升級指南」。

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` 及 `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` 指令移除現有的 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。

安裝問題

套用修補程式 1 後，所有使用者皆有讀取 `/tmp/amsilent` 檔案的權限 (6370691)

在您套用修補程式 1 後，所有使用者皆有讀取 `/tmp/amsilent` 檔案的權限。

解決方法：在您套用修補程式後，重設檔案的權限，只允許 Access Manager 管理員的讀取權限。

使用容器配置安裝 SDK 時，通知 URL 不正確 (6327845)

使用容器配置 (DEPLOY_LEVEL=4) 執行 SDK 安裝時，通知 URL 不正確。

解決方法：

1. 在 `AMConfig.properties` 檔案中設定下列特性：

   ```
   com.iplanet.am.notification.url=
   protocol://fqdn:port/amserver/servlet/com.iplanet.services.comm.client.
   PLLNotificationServlet
   ```

2. 重新啓動 Access Manager 以使新值生效。

Access Manager `classpath` 參照過期的 JCE 1.2.1 套裝模組 (6297949)

Access Manager `classpath` 參照 2005 年 7 月 27 日到期的 Java Cryptography Extension (JCE) 1.2.1 套裝模組 (簽署憑證)。

解決方法：無。雖然在 `classpath` 中存在套裝模組參照，Access Manager 並不會使用此套裝模組。

要將 Access Manager 安裝於現有 DIT，必須重建 Directory Server 索引 (6268096)

爲了改善搜尋效能，Directory Server 有數個新增的索引。

解決方法：使用現有的「目錄資訊樹 (DIT)」安裝 Access Manager 後，請執行 `db2index.pl` 程序檔重建 Directory Server 索引。例如：

```
# ./db2index.pl -D "cn=Directory Manager" -w password -n userRoot
```

`db2index.pl` 程序檔可從 *DS-install-directory/slapd-hostname/* 目錄中取得。

非超級使用者的記錄檔與除錯目錄權限不正確 (6257161)

在無訊息安裝配置檔中指定了非超級使用者時，除錯、記錄檔及啓動目錄的權限未正確設定。

解決方法：變更這些目錄的權限以讓非超級使用者可以存取。

將 Access Manager 和 Directory Server 安裝在不同機器上時，認證服務沒有初始化 (6229897)

雖然 `classpath` 和其他 Access Manager Web 容器環境變數會在安裝過程中更新，安裝程序不會重新啓動 Web 容器。若您在安裝後但 Web 容器尚未重新啓動之前試著登入 Access Manager，會傳回下列錯誤：

認證服務沒有初始化。請與您的系統管理員連絡。

解決方法：請先重新啓動 Web 容器，再登入 Access Manager。登入前，您還必須先執行 Directory Server。

安裝程式未針對現有目錄安裝加入平台項目 (6202902)

Java ES 安裝程式未針對現有目錄伺服器安裝 (DIRECTORY_MODE=2) 加入平台項目。

解決方法：手動加入「範圍/DNS」別名與平台伺服器清單項目。如需有關步驟，請參閱「Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide」中的「Adding Additional Instances to the Platform Server List and Realm/DNS Aliases」。

升級問題

Access Manager `ampre70upgrade` 程序檔不會移除本土化的套裝軟體 (6378444)

若您正將 Access Manager 升級到 Access Manager 7 2005Q4， `ampre70upgrade` 程序檔不會移除您系統上任何的 Access Manager 本土化套裝軟體。

解決方法：在您升級爲 Access Manager 7 2005Q4 之前，使用 `pkgrm` 指令手動移除安裝在您系統上的所有本土化 Access Manager 套裝軟體。

`AMConfig.properties` 檔案使用的 Web 容器版本是舊的 (6316833)

Access Manager 與 Application Server 升級至 Java ES 2005Q4 版本後，Access Manager `AMConfig.properties` 檔案中的 Application Server 版本是舊的。

解決方法：執行 Delegated Administrator 配置程式 (`config-commda`) 之前，請先變更 `AMConfig.properties` 檔案中的下列特性：

```
com.sun.identity.webcontainer=IAS8.1
```

節點代理程式 server.policy 檔案未隨著 Access Manager 升級而更新 (6313416)

升級 Access Manager 之後，節點代理程式 server.policy 檔案未更新。

解決方法：以下列檔案取代節點代理程式的 server.policy 檔案：

```
/var/opt/SUNWappserver/domains/domain1/config/server.policy
```

升級後，條件清單中缺少階段作業特性條件 (6309785)

將 Access Manager 從版本 2005Q1 升級至版本 2005Q4 後，若您試圖將一個條件加入策略，在 [策略條件] 清單中並未將 [階段作業特性條件] 做爲一個選項顯示出來。

解決方法：選取對應範圍的策略配置服務範本中之 [階段作業特性條件] 類型。

升級後，策略主體清單中缺少識別主體類型 (6304617)

將 Access Manager 從版本 2005Q1 升級至版本 2005Q4 後，在策略主體清單中未將新加入的策略主體類型 [識別主體] 做爲一個選項顯示出來。

解決方法：在策略配置服務範本中選取 [識別主體] 類型做爲預設的主體類型。

Access Manager 升級失敗，因為 classpath 未遷移 (6284595)

Access Manager 從 Java ES 2004Q2 升級至 Java ES 2005Q4 期間，從 Java ES 2004Q2 升級至 Java ES 2005Q1 失敗。Access Manager 已安裝在 Application Server 上，亦從 Java ES 2004Q2 升級至 Java ES 2005Q4。 domain.xml 檔案中的 classpath 沒有 Access Manager JAR 檔案路徑。

解決方法：依照以下步驟：

1. 執行 amupgrade 程序檔之前，重新建立 Directory Server 的索引；這是 comm_dssetup.pl 程序檔發生問題所致。
2. 將 Access Manager 的項目加入節點代理程式的 server.policy 檔案。只需要預設伺服器策略 (/var/opt/SUNWappserver/domains/domain1/config/server.policy) 的一份 server.policy 副本便已足夠。
3. 如下所示，更新節點代理程式的 domain.xml 檔案中之 classpath。將 classpath-suffix 與相關的 classpath (取自 server.xml 檔案的 java-config 元素之 server-classpath 屬性)，複製到 domain.xml 的 java-config 元素之各個屬性。java-config 元素可在 domain.xml 中的 config 元素下找到。

升級後，amadmin 指令傳回錯誤版本 (6283758)

Access Manager 從版本 6 2005Q1 升級至版本 7 2005Q4 後，amadmin --version 指令傳回了錯誤的版本：Sun Java System Access Manager 版本 2005Q1。

解決方法：將 Access Manager 升級後，執行 `amconfig` 程序檔以配置 Access Manager。執行 `amconfig` 時，指定配置 (`amsamplesilent`) 檔案的完整路徑。例如，在 Solaris 系統中：

```
# ./amconfig -s ./config-file
```

或

```
# ./amconfig -s /opt/SUNWam/bin/config-file
```

於資料遷移之後增加 `ContainerDefaultTemplateRole` 屬性 (4677779)

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。當組織是由現有目錄資訊樹 (DIT) 或其他來源中遷移出來時，`ContainerDefaultTemplateRole` 屬性不會自動加入組織。

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

配置問題

使用非預設 URI 時，必須編輯 Application Server 8.1 `server.policy` 檔案 (6309759)

若您是將 Access Manager 7 2005Q4 部署在 Application Server 8.1 上，並對服務、主控台及密碼 Web 應用程式使用非預設 URI，但這些應用程式分別具有預設的 URI 值 `amserver`、`amconsole` 及 `ampassword`，則嘗試透過 Web 瀏覽器存取 Access Manager 之前，必須先編輯應用程式伺服器網域的 `server.policy` 檔案。

解決方法：以如下方式編輯 `server.policy` 檔案：

1. 停止部署 Access Manager 的 Application Server 實例。
2. 變更至 `/config` 目錄。例如：

```
cd /var/opt/SUNWappserver/domains/domain1/config
```

3. 製作 `server.policy` 檔案的備份副本。例如：

```
cp server.policy server.policy.orig
```

4. 在 `server.policy` 檔案中，尋找下列策略：

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amserver/-" { ...
};
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amconsole/-" { ...
};
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/ampassword/-" { ...
};
```

5. 在下列指令行中，以服務 Web 應用程式的非預設 URI 取代 `amserver`：

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amserver/-" {
```

6. 若是在舊有模式下進行安裝，請在下列指令行中，以主控台 Web 應用程式的非預設 URI 取代 `amconsole`：

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amconsole/-" {
```

7. 在下列指令行中，以密碼 Web 應用程式的非預設 URI 取代 `ampassword`：

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/ampassword/-" {
```

8. 啓動部署 Access Manager 的 Application Server 實例。

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。如需有關步驟，請參閱「Sun Java System Access Manager 7 2005Q4 Deployment Planning 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 2005Q4 會強制服務 XML 檔案中的必需屬性必須有預設值。

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 2005Q4 部署至安全 (使用 SSL) BEA WebLogic 8.1 SP4 實例，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` (包含用來部署與解除部署 Access Manager Web 應用程式之 `classpath` 的變數)。

   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。如需有關步驟，請參閱「Sun Java System Access Manager 7 2005Q4 Deployment Planning 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
```

使用 RSA 金鑰時，IBM WebSphere 中的 URL 簽署失敗 (6271087)

在 IBM WebSphere 中使用 RSA 金鑰時，URL 字串的簽署失敗，並有下列異常：

```
ERROR: FSSignatureUtil.signAndReturnQueryString: FSSignatureException
occured while signing query string: no such provider: SunRsaSign
```

解決方法：WebSphere 隨附的 JDK 中缺少「SunRsaSign」提供者。若要修正此問題，編輯 *websphere_jdk_root*`/jre/lib/security/java.security` 檔案，加入下列內容以將「SunRsaSign」啓用爲提供者之一：

```
security.provider.6=com.sun.rsajca.Provider
```

Access Manager 主控台問題

針對 SAML，於控制台中複製 [可信任合作夥伴] 會發生錯誤 (6326634)

在 Access Manager 主控台中，於 [聯合] > [SAML] 標籤下建立 [SAML 可信任合作夥伴]。若您嘗試複製 [可信任合作夥伴]，就會發生錯誤。

解決方法：無。此問題已在修補程式 1 中修正。有關如何針對特定平台套用修補程式的資訊，請參閱第 54 頁的 「Access Manager 7 2005Q4 修補程式 1」。

遠端記錄對 `amConsole.access` 與 `amPasswordReset.access` 無法使用 (6311786)

配置遠端記錄時，所有的記錄都會寫入遠端 Access Manager 實例，但是在 `amConsole.access` 與 `amPasswordReset.access` 中不會寫入密碼重設資訊。不會寫入該記錄檔。

解決方法：無。

在主控台加入更多 amadmin 特性將變更 amadmin 使用者密碼 (6309830)

在管理主控台中加入或編輯 amadmin 使用者的部分特性，導致 amadmin 使用者密碼發生改變。

解決方法：無。此問題已在修補程式 1 中修正。有關如何針對特定平台套用修補程式的資訊，請參閱第 54 頁的 「Access Manager 7 2005Q4 修補程式 1」。

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

新的 Access Manager 7 2005Q4 主控台無法設定「服務類別 (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。

將群組做為策略管理使用者加入使用者時發生異常錯誤 (6299543)

當您將群組做爲策略管理使用者加入使用者時，Access Manager 主控台會傳回異常錯誤。

解決方法：無。

在舊有模式下，無法從角色刪除所有使用者 (6293758)

在舊有模式下，若嘗試從角色刪除所有使用者，將會留下一位使用者。

解決方法：再次嘗試從角色刪除該使用者。

無法加入、刪除或修改探索服務資源提供 (6273148)

Access Manager 管理主控台不允許您加入、刪除或修改使用者、角色或範圍的資源提供。

解決方法：無。此問題已在修補程式 1 中修正。有關如何針對特定平台套用修補程式的資訊，請參閱第 54 頁的 「Access Manager 7 2005Q4 修補程式 1」。

使用錯誤的 LDAP 連結密碼時，應傳回主體搜尋錯誤訊息 (6241241)

使用錯誤的 LDAP 連結密碼時，Access Manager 管理主控台不會傳回錯誤訊息。

解決方法：無。

在舊有模式下，Access Manager 無法在容器下建立組織 (6290720)

若您建立容器，然後嘗試在該容器下建立組織，Access Manager 會傳回 [唯一性違規錯誤] 訊息。

解決方法：無。

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。在您選擇現有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)

使用現有的 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*` 加入使用者。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。

SDK 與用戶端問題

無法移除子範圍的階段作業服務配置 (6318296)

建立頂層範圍的子範圍，並對其加入階段作業服務後，後續嘗試移除階段作業服務配置時會產生錯誤訊息。

解決方法：移除預設的頂層 ID 儲存庫 AMSDK1，然後將此儲存庫加回配置中。

此問題已在修補程式 1 中修正。有關如何針對特定平台套用修補程式的資訊，請參閱第 54 頁的 「Access Manager 7 2005Q4 修補程式 1」。

指定策略條件時，CDC servlet 重新導向至無效的登入頁面 (6311985)

將 Apache agent 2.2 設於 CDSSO 模式下，當存取代理程式保護的資源時，CDC servlet 重新導向使用者至匿名認證頁面，而不是預設的登入頁面。

解決方法：無。此問題已在修補程式 1 中修正。有關如何針對特定平台套用修補程式的資訊，請參閱第 54 頁的 「Access Manager 7 2005Q4 修補程式 1」。

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，沒有收到通知。

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。

此問題已在修補程式 1 中修正。有關如何針對特定平台套用修補程式的資訊，請參閱第 54 頁的 「Access Manager 7 2005Q4 修補程式 1」 。

指令行公用程式問題

若 Access Manager 指向 Directory Proxy，則空屬性 LDAP 搜尋會傳回錯誤 (6357975)

如果您使用的是 Sun Java System Directory Proxy Server，則空屬性 LDAP 搜尋會傳回錯誤。例如：

```
# ldapsearch -b base-dn uid=user ""
```

若 Access Manager 直接指向 LDAP 目錄伺服器，則會成功進行相同的搜尋。

解決方法：如果您使用的是 Directory Proxy Server，則啓用空屬性搜尋或提供搜尋的屬性名稱。

`amserveradmin` 程序檔缺少新的模式檔案 (6255110)

安裝後，執行 `amserveradmin` 程序檔以將服務載入 Directory Server 時，程序檔缺少 `defaultDelegationPolicies.xml` 與 `idRepoDefaults.xml` 模式檔案。

解決方法：使用含有 `-t` 選項的 `amadmin` CLI 工具手動載入 `defaultDelegationPolicies.xml` 與 `idRepoDefaults.xml` 檔案。

無法在 Internet Explorer 6.0 中儲存具有退出字元的 XML 文件 (4995100)

若在 XML 檔案中加入特殊字元 (例如在「&」之後加上字串「amp;」)，檔案會正確儲存，但是若稍後使用 Internet Explorer 6.0 擷取該 XML 設定檔，檔案無法正確顯示。如果接著嘗試再次儲存該設定檔，系統會傳回錯誤訊息。

解決方法：無。

認證問題

- 第 78 頁的 「UrlAccessAgent SSO 記號到期 (6327691)」
- 第 78 頁的 「更正密碼後，無法登入具 LDAPV3 外掛程式/動態設定檔的子範圍 (6309097)」
- 第 78 頁的 「舊有 (相容) 模式下 Access Manager 統計服務的預設配置不相容 (6286628)」
- 第 79 頁的 「頂層組織中命名屬性的屬性唯一性遭破壞 (6204537)」

UrlAccessAgent SSO 記號到期 (6327691)

UrlAccessAgent SSO 記號到期，因爲應用程式模組未傳回特殊使用者 DN，導致特殊使用者 DN 相符而使得尚未到期的記號到期。

解決方法：無。此問題已在修補程式 1 中修正。有關如何針對特定平台套用修補程式的資訊，請參閱第 54 頁的 「Access Manager 7 2005Q4 修補程式 1」。

更正密碼後，無法登入具 LDAPV3 外掛程式/動態設定檔的子範圍 (6309097)

在範圍模式下，如果使用「錯誤」密碼在範圍中建立 ldapv3 資料儲存區，並稍後將密碼變更爲 amadmin，則當您嘗試以使用變更後密碼的使用者身份再次登入時，登入會失敗，顯示不存在設定檔的訊息。

解決方法：無。

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，將 `o`、`sunPreferredDomain`、`associatedDomain`、`sunOrganizationAlias`、`uid` 及 `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 79 頁的 「跨時區的 Access Manager 實例使其他使用者階段作業逾時 (6323639)」
- 第 79 頁的 「階段作業容錯移轉 (`amsfoconfig`) 程序檔在 Linux 2.1 系統上的權限不正確 (6298433)」
- 第 79 頁的 「階段作業容錯移轉 (`amsfoconfig`) 程序檔在 Linux 2.1 系統上無法執行 (6298462)」
- 第 80 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 80 頁的 「透過協力廠商Web 容器使用 `HttpSession` (無 CR 編號)」

跨時區的 Access Manager 實例使其他使用者階段作業逾時 (6323639)

跨不同時區安裝的 Access Manager 實例在同一個信任圈內導致使用者階段作業逾時。

階段作業容錯移轉 (`amsfoconfig`) 程序檔在 Linux 2.1 系統上的權限不正確 (6298433)

階段作業容錯移轉配置程序檔 (`/opt/sun/identity/bin/amsfoconfig`) 的權限不正確，無法在 Linux 2.1 系統上執行。

解決方法：變更權限以使 `amsfoconfig` 程序檔可執行 (例如 755)。

此問題已在修補程式 1 中修正。有關如何針對特定平台套用修補程式的資訊，請參閱 第 54 頁的 「Access Manager 7 2005Q4 修補程式 1」。

階段作業容錯移轉 (`amsfoconfig`) 程序檔在 Linux 2.1 系統上無法執行 (6298462)

階段作業容錯移轉配置程序檔 (`amsfoconfig`) 無法在 Linux 2.1 伺服器上執行，原因是未正確解析定位字元 (`\t`)。

解決方法：手動配置階段作業容錯移轉。如需步驟，請參閱「Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide」中的「Configuring Session Failover Manually」。

此問題已在修補程式 1 中修正。有關如何針對特定平台套用修補程式的資訊，請參閱第 54 頁的 「Access Manager 7 2005Q4 修補程式 1」。

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` 切換至 `https`，或從 `https` 切換至 `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"/>
```

透過協力廠商Web 容器使用 `HttpSession` (無 CR 編號)

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

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有策略，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 81 頁的 「Access Manager 啓動時發生除錯錯誤 (6309274、6308646)」
- 第 81 頁的 「使用 BEA WebLogic Server 做爲 Web 容器」

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

Access Manager 7 2005Q4 啓動時傳回 `amDelegation` 與 `amProfile` 除錯檔案中的除錯錯誤：

- `amDelegation`：無法取得委託的外掛程式實例
- `amProfile`：出現委託異常

解決方法：無。您可忽略這些訊息。

使用 BEA WebLogic Server 做為 Web 容器

若您是使用 BEA WebLogic Server 做爲 Web 容器來部署 Access Manager，就可能無法存取 Access Manager。

解決方法：再次重新啓動 WebLogic Server 以便可以存取 Access Manager。

Linux OS 問題

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：解決方法是在您啓動 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;
```

聯合與 SAML 問題

- 第 82 頁的 「執行 Web 服務範例時傳回 [找不到資源提供](6359900)」
- 第 83 頁的 「使用工件設定檔時聯合失敗 (6324056)」
- 第 83 頁的 「應將 SAML 敘述中的特殊字元 (&) 進行編碼 (6321128)」
- 第 83 頁的 「嘗試將 Disco 服務加入角色時發生異常 (6313437)」
- 第 83 頁的 「除非您先配置並儲存其他屬性，否則無法配置 Auth Context 屬性 (6301338)」
- 第 83 頁的 「若根字尾包含「&」字元，就無法加入 EP 範例 (6300163)」
- 第 83 頁的 「聯合過程中發生登出錯誤 (6291744)」

執行 Web 服務範例時傳回 [找不到資源提供](6359900)

當 Access Manager 配置爲存取 Solaris 系統的 *AccessManager-base*`/SUNWam/samples/phase2/wsc` (或 Linux 系統的 *AccessManager-base*`/identity/samples/phase2/wsc`) 目錄之下的 Web 服務範例時，查詢 [探索服務] 或修改 [資源提供] 時會傳回錯誤訊息：[找不到資源提供]。

AccessManager-base 爲基底安裝目錄。預設基底安裝目錄在 Solaris 系統上爲 `/opt`，在 Linux 系統上爲 `/opt/sun`。

解決方法：

1. 前往下列範例目錄：Solaris 系統的 *AccessManager-base*`/SUNWam/samples/phase2/wsc` 目錄，或 Linux 系統的 *AccessManager-base*`/identity/samples/phase2/wsc` 目錄
2. 在 `index.jsp` 檔中搜尋下列字串：

   ```
   com.sun.org.apache.xml.security.utils.XMLUtils.outputDOM
   ```
3. 在包含前一個步驟所找到字串的那一行之前，插入如下新的一行：

```
com.sun.org.apache.xml.security.Init.init();
```

4. 重新執行範例。(您不需要重新啓動 Access Manager。)

使用工件設定檔時聯合失敗 (6324056)

若設定了識別提供者 (IDP) 與服務提供者 (SP)，將通訊協定變更爲使用瀏覽器的工件設定檔，然後試著在 IDP 與 SP 之間聯合使用者，結果聯合失敗。

解決方法：無。

應將 SAML 敘述中的特殊字元 (&) 進行編碼 (6321128)

以 Access Manager 做爲來源站點與目的地站點，並且配置了 SSO，結果目的地站點中發生錯誤，原因是 SAML 敘述中的特殊字元 (&) 未編碼，因此造成宣示的剖析失敗。

解決方法：無。此問題已在修補程式 1 中修正。有關如何針對特定平台套用修補程式的資訊，請參閱第 54 頁的 「Access Manager 7 2005Q4 修補程式 1」。

嘗試將 Disco 服務加入角色時發生異常 (6313437)

在 Access Manager 主控台中，若試著將資源提供加入 Disco 服務，會發生未知的異常。

解決方法：無。

除非您先配置並儲存其他屬性，否則無法配置 Auth Context 屬性 (6301338)

除非您已配置並儲存其他屬性，否則將無法配置 Auth Context 屬性。

解決方法：先配置並儲存提供者設定檔，再配置 Auth Context 屬性。

若根字尾包含「&」字元，就無法加入 EP 範例 (6300163)

若 Directory Server 有一個根字尾包含「&」字元，而您試著加入 [雇員配置檔服務資源提供]，就會丟出一個異常。

解決方法：無。

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 (Globalization, g11n) 問題

- 第 84 頁的 「使用者語言環境喜好設定未套用至整個管理主控台 (6326734)」

使用者語言環境喜好設定未套用至整個管理主控台 (6326734)

部分 Access Manager 管理主控台的元件不會遵守使用者語言環境喜好設定，而會使用瀏覽器語言環境設定。此問題會影響 [版本]、[登出] 及 [線上說明] 按鈕，以及 [版本] 和線上說明的內容。

解決方法：將瀏覽器設定變更爲與使用者喜好設定相同的語言環境。

Access Manager 部署在 IBM WebSphere 上時，無法任意使用歐洲語言線上說明 (6325024)

在所有歐洲語言環境 (西班牙語、德語及法語) 中，當 Access Manager 部署在 IBM WebSphere Application Server 實例上時，無法任意存取線上說明。針對以下框架，線上說明會顯示 [應用程式錯誤]：

- 上方框架，其中包含 [說明] 與 [關閉] 按鈕。
- 左方框架，其中包含 [內容]、[索引] 及 [搜尋] 按鈕。

解決方法：將瀏覽器語言設定爲英語，然後重新整理頁面以便能存取左方框架。不過上方框架仍會顯示 [應用程式錯誤]。

Access Manager 部署在 IBM WebSphere 上時，版本資訊是空的 (6319796)

在任何語言環境中，Access Manager 部署在 IBM WebSphere Application Server 實例上時，當您按一下 [版本] 按鈕，不會看見產品版本資訊，而會顯示空白頁面。

解決方法：無。

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 2005Q4 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` 目錄下的記錄檔中之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 Access Manager 無法將範圍模式復原為舊有模式 (6508473)

如果您在範圍模式下安裝 Access Manager 7 2005Q4，將無法復原爲舊有模式。

不過，如果您在舊有模式下安裝 Access Manager 7 2005Q4，則可使用含 `-M` 選項的 `amadmin` 指令變更爲範圍模式。例如：

```
amadmin -u cn=amAdmin,ou=People,dc=example,dc=com -w amadmin-password -M
dc=example,dc=com
```

記錄有關停用持續搜尋的更多資訊 (6486927)

Access Manager 會使用持續搜尋來接收關於 Sun Java System Directory Server 項目變更的資訊。依預設，Access Manager 會在伺服器啓動期間建立下列持續搜尋連線：

`aci` - 對 `aci` 屬性的變更，使用 LDAP 篩選器 (`aci=*`) 進行搜尋

`sm` - 在 Access Manager 資訊樹狀結構 (或服務管理節點) 中進行的變更，其中包含 `sunService` 或 `sunServiceComponent` 記號物件類別的物件。例如，您可能需要建立策略來定義受保護資源的存取權限，或者需要修改現有策略的規則、主旨、條件或回應提供者。

`um` - 在使用者目錄 (或使用者管理節點) 中進行的變更。例如，您可能要變更使用者的名稱或位址。

注意 – 我們不建議您停用這些元件的持續搜尋，因爲停用持續搜尋後的元件將無法從 Directory Server 接收通知。因此，元件快取將不會收到 Directory Server 中該特殊元件的變更通知，使得元件快取的內容會變得比較陳舊。

例如，如果您停用使用者目錄 (`um`) 變更的持續搜尋，Access Manager 伺服器將不會從 Directory Server 收到通知。因此，代理程式將不會從 Access Manager 取得通知，從而不會以使用者屬性的新值來更新其本機使用者快取。然後，當應用程式查詢代理程式的使用者屬性時，它可能會收到該屬性的舊值。

只有在特殊情況下有絕對必要時才使用此特性。例如，當您知道生產環境中不會發生 [服務配置] 變更 (涉及變更諸如 [階段作業服務] 和 [認證服務] 等服務的值) 時，則可以停用 [服務管理] (`sm`) 元件的持續搜尋。不過，如果任何服務發生任何變更，將需要重新啓動伺服器。相同的條件也會套用到由 `aci` 和 `um` 值所指定的其他持續搜尋。

如需更多資訊，請參閱第 53 頁的 「CR# 6363157：新特性會在絕對必要時停用持續搜尋」 。

記錄 Access Manager 支援和不支援的權限 (2143066)

權限用於定義做爲某範圍內角色或群組成員的管理員所具備的存取權限。Access Manager 允許您配置下列管理員類型的權限：

- 範圍管理員可執行所有與範圍相關的作業，包括定義識別儲存庫 (資料存放區)、配置認證及定義策略。
- 策略管理員可配置現有範圍內的策略。

支援下列權限：

- 所有範圍與策略特性的讀取與寫入存取權。定義範圍管理員的讀取和寫入存取權限。
- 僅針對策略特性的讀取與寫入存取權。定義策略管理員的讀取和寫入存取權限。
- 支援的權限組合：僅針對策略特性的讀取與寫入存取權，以及資料存放區的唯讀存取權。不支援其他的權限組合。

記錄基於 cookie 的居留式請求路由 (6476922)

若 Access Manager 伺服器部署在負載平衡器之後，基於 cookie 的居留式請求路由可避免將用戶端請求誤送到不正確的 Access Manager 伺服器 (也就是未代管階段作業的伺服器)。Access Manager 7 2005Q4 修補程式 3 已實作此功能。

依照以前的運作方式，若沒有基於 cookie 的居留式請求路由，則非瀏覽器式用戶端 (例如策略代理程式及使用遠端 Access Manager 用戶端 SDK 的用戶端) 請求通常都會誤送到未代管階段作業的 Access Manager 伺服器。然後，爲將請求傳送到正確的伺服器，Access Manager 伺服器必須使用回返通道通訊來驗證階段作業，而這通常會造成效能降低。基於 cookie 的居留式請求路由不需要此回返通道通訊，因此可改善 Access Manager 的效能。

若要實作基於 cookie 的居留式請求路由，必須將 Access Manager 部署配置爲站點。如需相關資訊，請參閱「Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide」中的「Configuring an Access Manager Deployment as a Site」。

若要配置基於 cookie 的居留式請求路由：

1. 若要指定 cookie 名稱，請設定 `AMConfig.properties` 檔案中的 `com.iplanet.am.lbcookie.name` 特性。然後 Access Manager 便會使用兩個位元組的伺服器 ID (例如 01、02 和 03) 來產生負載平衡器 cookie 值。如果不指定 cookie 名稱，Access Manager 會使用預設名稱 `amlbcookie` 加上兩個位元組的伺服器 ID 來產生負載平衡器 cookie 值。

   如果在 Access Manager 伺服器上設定了 cookie 的名稱，則策略代理程式的 `AMAgent.properties` 檔案中必須使用相同的名稱。同樣，如果使用的是 Access Manager 用戶端 SDK，也必須使用與 Access Manager 伺服器相同的 cookie 名稱。

   備註：請勿設定 `com.iplanet.am.lbcookie.value` 特性，因爲 Access Manager 會使用兩個位元組的伺服器 ID 來設定 cookie 值。
2. 使用步驟 1 中的 cookie 名稱來配置負載平衡器。您可以在 Access Manager 部署使用硬體或軟體負載平衡器。
3. 如果已實作階段作業容錯移轉，請啓用策略代理程式和 Access Manager 伺服器的 `com.sun.identity.session.resetLBCookie` 特性。
   - 若爲策略代理程式，請增加並啓用 `AMAgent.properties` 檔案中的特性。
   - 若爲 Access Manager 伺服器，請增加並啓用 `AMConfig.properties` 檔案中的特性。

   例如：

```
com.sun.identity.session.resetLBCookie='true'
```

如果發生容錯移轉的情況，階段作業會被路由到輔助 Access Manager 伺服器，並使用輔助 Access Manager 伺服器的伺服器 ID 來設定負載平衡器的 cookie 值。然後任何後續階段作業請求也將路由到輔助 Access Manager 伺服器。

記錄 Windows 2003 的 Windows Desktop SSO 配置 (6487361)

要在 Windows 2003 上配置 Windows Desktop SSO， 如「Sun Java System Access Manager 7 2005Q4 管理指南」中的「配置 Windows Desktop SSO」中所述，請使用下列 `ktpass` 指令：

```
ktpass /out filename /mapuser username
/princ HTTP/hostname.domainname /crypto encryptiontype /rndpass
/ptype principaltype /target domainname
```

例如：

```
ktpass /out demo.HTTP.keytab
/mapuser http /princ HTTP/demo.identity.sun.com@IDENTITY.SUN.COM
/crypto RC4-HMAC-NT /rndpass /ptype KRB5_NT_PRINCIPAL /target IDENTITY.SUN.COM
```

如需語法定義，請參閱下列網站：

```
http://technet2.microsoft.com/
WindowsServer/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?
mfr=true
```

記錄設定分散式認證 UI 伺服器密碼的步驟 (6510859)

下列程序描述如何設定分散式認證 UI 伺服器與 Access Manager 伺服器進行通訊的加密密碼。

若要設定分散式認證 UI 伺服器的密碼：

1. 在 Access Manager 伺服器中：
   a. 使用 `ampassword -e` 公用程式將 `amadmin` 密碼加密。例如，在 Solaris 系統中：

      ```
      # cd /opt/SUNWam/bin
      # ./ampassword -e amadmin-password
      AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
      ```

      儲存該加密值。
   b. 從 Access Manager 伺服器的 `AMConfig.properties` 檔案複製並儲存 `am.encryption.pwd` 特性值。例如：

      ```
      am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
      ```

2. 在分散式認證 UI 伺服器上，對 AMConfig.properties 檔案進行如下變更：
   a. 將 com.iplanet.am.service.password 特性標記爲註釋。
   b. 將 com.iplanet.am.service.secret 特性設爲在步驟 1a 中加密的 amadmin 密碼。
   c. 增加從步驟 1b 中複製的 am.encryption.pwd 及加密值。例如：

```
com.sun.identity.agents.app.username=username
#com.iplanet.am.service.password=password
com.iplanet.am.service.secret=AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
```

3. 重新啓動分散式認證 UI 伺服器。

有關「建立新站點名稱」的線上說明需要更多資訊 (2144543)

Access Manager 主控台線上說明中，未描述在 [配置] > [系統特性] > [平台] 之下「建立新站點名稱」的 [儲存] 步驟。如果您在增加新站點名稱後沒有按一下 [儲存]，當您再嘗試增加實例名稱時，該程序會失敗。因此，在增加站點名稱後請務必按一下 [儲存]，然後再增加實例名稱。

記錄 Windows 系統上的管理員密碼配置參數為 ADMIN_PASSWD (6470793)

在 Solaris 和 Linux 系統中，amsamplesilent 中的 Access Manager 管理員 (amadmin) 密碼配置參數爲 ADMINPASSWD。不過，在 Windows 系統中，AMConfigurator.properties 檔案中的參數爲 ADMIN_PASSWD。

如果您在 Windows 系統中執行 amconfig.bat，請使用 ADMIN_PASSWORD 參數而不要使用 ADMINPASSWD 設定 AMConfigurator.properties 檔案中的 amadmin 密碼。

「版本說明」中對已知問題的解決方法有錯 (6422907)

已更正針對第 82 頁的 「執行 Web 服務範例時傳回 [找不到資源提供](6359900)」 之解決方法的步驟 3。

記錄 AMConfig.properties 中的 com.iplanet.am.session.protectedPropertiesList (6351192)

com.iplanet.am.session.protectedPropertiesList 參數讓您可以保護特定的核心或內部階段作業特性，使它們不會被階段作業服務的 SetProperty 方法從遠端更新。藉由設定此「隱藏」的關鍵安全性參數，您可自訂階段作業屬性以便參與授權以及其他的 Access Manager 功能。若要使用此參數：

1. 使用文字編輯器，將參數加入 AMConfig.properties 檔案。
2. 將參數設定爲要保護的階段作業特性。例如：

```
com.iplanet.am.session.protectedPropertiesList =
PropertyName1,PropertyName2,PropertyName3
```

3. 重新啓動 Access Manager Web 容器以使這些值生效。

記錄可支援 LDAPv3 外掛程式的角色和已篩選角色 (6365196)

如果資料儲存於 Sun Java System Directory Server 中，則套用對應的修補程式後，可爲 LDAPv3 外掛程式配置角色和已篩選角色 (可修正 CR 6349959)。在 Access Manager 7 2005Q4 管理員主控台中，在 LDAPv3 配置的 [LDAPv3 外掛程式支援的類型和作業] 欄位中，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
```

伺服器端的 com.iplanet.am.session.client.polling.enable 不得爲 true (6320475)

AMConfig.properties 檔案中的 com.iplanet.am.session.client.polling.enable 特性在伺服器端永遠不可以設定爲 true。

解決方法：依預設，此特性設爲 false，應永遠不得重設爲 true。

主控台線上說明中的預設成功 URL 不正確 (6296751)

service.scserviceprofile.iplanetamauthservice.html 線上說明檔案中的預設成功 URL 不正確。[預設成功 URL] 欄位接受多重值清單，此清單指定認證成功後，會將使用者重新導向至的 URL。此屬性格式爲 clientType|URL，您僅能指定 URL 的值，預設爲 HTML 類型。

"/amconsole" 預設值不正確。

解決方法：正確的預設值爲「/amserver/console」。

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 版本早於 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，前往對應的 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. 若您使用的 JDK 版本早於 JDK 1.5，則編輯 *jdk_root*`/jre/lib/security/java.security` 檔案，增加 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

Sun Java System Access Manager 7 2005Q4 文件集

下表列出自從首次發行之後所出版的新的與修訂過的 Access Manager 7 2005Q4 文件。若要存取這些文件，請參閱 Access Manager 7 2005Q4 文件集：

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

表 7 Access Manager 7 2005Q4 文件更新記錄

標題	出版日期
Sun Java System Access Manager 7 2005Q4 版本說明	請參閱「表 1」。
Sun Java System Access Manager 7 2005Q4 管理指南	2006 年 2 月

表 7 Access Manager 7 2005Q4 文件更新記錄 (續)

標題	出版日期
Sun Java System Access Manager 7 2005Q4 Developers Guide	2006 年 2 月
Sun Java System Access Manager Policy Agent 2.2 User's Guide	2006 年 2 月
Sun Java System Access Manager 7 2005Q4 C API Reference	2006 年 2 月
Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide	2006 年 2 月
Technical Note: Using Access Manager Distributed Authentication	2006 年 2 月
Technical Note: Installing Access Manager to Run as a Non-Root User	2006 年 2 月
Sun Java System SAML v2 Plug-in for Federation Services User's Guide	2006 年 2 月
Sun Java System SAML v2 Plug-in for Federation Services Release Notes	2006 年 2 月
Sun Java System SAMLv2 Plug-in for Federation Services Java API Reference	2006 年 2 月
Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide	2006 年 1 月
Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide	2005 年 12 月
Sun Java System Access Manager 7 2005Q4 Technical Overview	2005 年 12 月

Sun Java System Federation Manager 7.0 2005Q4 文件集

若要存取 Federation Manager 7.0 2005Q4 文件集中的文件，請參閱：

http://docs.sun.com/coll/1321.1

Sun Java System Access Manager Policy Agent 2.2 文件集

Access Manager Policy Agent 2.2 文件集還在不斷進行修訂，以記錄新的代理程式。若要存取此文件集中的文件，請參閱：

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

可再分發的檔案

Sun Java System Access Manager 7 2005Q4 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 819-3476，文件標題爲「Sun Java System Access Manager 7 2005Q4 版本說明」。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 819-2134-20，完整標題爲「Sun Java System Access Manager 7 2005Q4 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。
