Sun Java™ Desktop System Configuration Manager 版本 1 安裝指南

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054,
U.S.A. 650-960-1300

文件號碼 817-5594-10

2004 年 4 月，修訂版 A

版權和商標

目錄

1 介紹.....5

2 LDAP 伺服器.....7

概念.....7

設定.....7

其他注意事項.....11

3 Sun™ Web Console.....13

系統需求.....13

安裝 Sun Web Console.....14

執行主控台.....15

解除安裝 Sun Web Console.....15

Sun Web Console 連接埠資訊.....15

4 Sun Java™ Desktop System Configuration Manager 版本 1.....17

安裝 Configuration Manager.....17

執行 Configuration Manager.....18

解除安裝 Configuration Manager.....18

5 桌面元件.....19

資料存取/使用者認證.....19

Configuration Agent.....20

GConf 介面.....22

Mozilla 介面.....22

StarSuite 介面.....23

6 附錄 A — Sun Web Console.....25

已知問題.....25

安裝程序檔使用.....25

Sun Web Console 套裝軟體.....26

7 附錄 B — Configuration Manager.....27

Configuration Manager 套裝軟體.....27

8 附錄 C.....29

將 OpenLDAP 伺服器與 Configuration Manager 配合使用.....29

將 Active Directory 與 Configuration Manager 配合使用.....30

第 1 章

介紹

Sun Java™ Desktop System Configuration Manager 版本 1 旨在爲執行 Sun Java™ Desktop System 的桌面主機提供核心配置。可以將設定指定至組織結構的各種元素，從而讓管理員以簡單的方式管理多組使用者或主機。它的主元件包括：

- LDAP 伺服器，包含要管理的使用者和主機之組織結構，並將儲存配置資料，
- 基於 Web 的管理工具，可讓管理員定義配置資料並將其指定至該組織結構的元素，
- 安裝在用戶端主機上的桌面元件，可代表目前登入的使用者擷取配置資料，並將其提供給組成 Java Desktop System 的各種應用程式。

管理工具爲基於 Web 的應用程式，在 Sun Web Console 中執行。它可讓管理員瀏覽 LDAP 伺服器的組織結構並爲其元素指定策略。策略可依據策略範本來顯示和編輯，這些範本定義了管理工具將要處理的設定。

桌面元件是以 Sun Java™ Desktop System Configuration Agent 爲中心而組織的，該代理程式可代表使用者從 LDAP 伺服器擷取配置資料，並讓一些配置系統介面使用這些資料，這些介面透過策略設定來補充本機配置 (應用程式提供的預設設定和使用者設定)。目前受支援的配置系統爲 GConf (可處理 Gnome 桌面或 Evolution 等 Gnome 應用程式的配置)、Mozilla Preference 和 StarRegistry (StarSuite 的配置系統)。

第 2 章

LDAP 伺服器

概念

在 Java Desktop System Configuration Manager 架構中，配置資料與實體關聯，這些實體爲 LDAP 系統訊息庫中的項目並與公司組織結構的元素相對應。

可識別的實體爲：

- 組織：通常表示整個階層結構的組織單元 (部門、群組、團隊) 或地理單元 (大洲、國家/地區、站點)。
- 使用者：表示整個階層結構的葉節點，顧名思義，通常指使用者。
- 網域：表示網路組織的邏輯結構單元。
- 主機：也表示整個階層結構的葉節點，但指網路上的機器。
- 角色：表示屬性，通常指功能 (管理員和站點管理) 方面的區別，套用於一組使用者。

組織實體和使用者實體用於定義使用者樹，而網域實體和主機實體則定義主機樹。這兩種樹相互獨立，但在架構中的處理方法類似。

組織實體和網域實體與其他項目的關係由項目在系統訊息庫中的實體位置定義。即組織實體和網域實體可 包含在樹中位於這兩個實體下面的任何項目。角色與使用者或主機的關係則由使用者項目和主機項目的屬性定義。

與實體關聯的配置資料儲存在由架構所管理的特殊項目中。這些項目可透過與項目關聯的服務名稱和服務容器來識別。

設定

若要使用具有 Configuration Manager 的現有 LDAP 伺服器，您需要：

- 延伸伺服器綱目，以支援 Configuration Manager 用於儲存配置資料的自訂物件類別和屬性。
- 在伺服器中自訂和儲存系統訊息庫中項目的對映資訊，以及 Configuration Manager 所支援實體的對映資訊。

佈署工具

若要使用使用具有 Configuration Manager 的現有 LDAP 伺服器，需要以下位於安裝 CD 的佈署工具：

- `88apoc-registry.ldif` — 介紹儲存配置資料所需之物件類別和屬性的綱目檔案。
- `OrganizationMapping` — 描述 LDAP 項目與 Configuration Manager 實體之間對映的預設屬性檔。
- `UserProfileMapping` — 描述 LDAP 使用者項目屬性與 Configuration Manager 使用者設定檔屬性之間對映的預設屬性檔。
- `CreateServiceTree` — 在 LDAP 系統訊息庫中儲存對映檔案的程序檔。
- `DeployApoc` — 延伸 LDAP 伺服器的綱目並在 LDAP 系統訊息庫中儲存對映檔案的程序檔。

綱目延伸

配置資料儲存在與資料關聯的項目隨附的項目樹中。在 LDAP 伺服器上儲存這些樹所使用的物件類別和屬性之前，您必須將物件和類別加入 LDAP 伺服器綱目。例如，提供的綱目延伸檔案使用 LDIF 格式，以將這些物件和類別加入 Sun Java System Directory Server。若要將這些物件和類別加入其他 LDAP 伺服器，您需要使用伺服器可識別的格式。

組織對映

若要定義 LDAP 項目與 Configuration Manager 實體之間的對映，則必須編輯組織對映檔案。必須爲各種鍵提供符合 LDAP 系統訊息庫佈局的值。

使用者實體可透過所有實體均使用的物件類別來識別，也可由其值在整個系統訊息庫中唯一的屬性識別。可提供顯示名稱格式以決定使用者在管理應用程式中的顯示方式，或者如果組織中的使用者項目使用容器項目，則亦可定義該類項目。鍵名稱及其預設值包括：

```
# Object class that all user entries use
User/ObjectClass=inetorgperson
# Attribute whose value in user entries is unique within the repository
User/UniqueIdAttribute=uid
# Optional container in organization entries of the user entries, remove
line if not used
User/Container=ou=People
# Display name format within the management application
User/DisplayNameFormat=sn, givenname
```

角色實體可由其使用的可能物件類別清單以及相應的命名屬性清單來識別。這些清單使用格式 <項目 1>,<項目 2>,...,<項目 N>，而且各項必須對齊。即，各清單必須含有相同的項目數，且第 n 個物件類別必須與第 n 個命名屬性配合使用。兩個鍵定義角色與使用者之間的關係，以及角色與主機之間的關係。VirtualMemberAttribute 鍵必須指定可從使用者項目或主機項目查詢其值的屬性。該鍵還必須包含項目所從屬角色的完整 DN。MemberAttribute 鍵必須從使用者項目或主機項目爲搜尋過濾器指定屬性。該鍵還必須包含使用者或主機所從屬角色的完整 DN。VirtualMemberAttribute 鍵可爲服務類別虛擬屬性，而 MemberAttribute 鍵則必須爲可在過濾器中使用的實體屬性。鍵名稱及其預設值包括：

```
# List of object classes for roles
Role/ObjectClass=nsRoleDefinition
# Aligned list of corresponding naming attributes
Role/NamingAttribute=cn
# Physical attribute (usable in a filter) containing the DNs of the roles of
a user/host
Role/MemberAttribute=nsRoleDN
# Attribute whose query on a user or host return the DNs of the roles it
belongs to
Role/VirtualMemberAttribute=nsRole
```

識別組織實體的方法類似於識別角色的方法，即，使用兩個對齊清單 (物件類別清單和相應命名屬性清單)。鍵名稱及其預設值包括：

```
# List of object classes for organizations
Organization/ObjectClass=organization
# Aligned list of corresponding naming attributes
Organization/NamingAttribute=o
```

識別網域實體的方法類似於識別組織實體的方法。鍵名稱及其預設值包括：

```
# List of object classes for domains
Domain/ObjectClass=ipNetwork
# Aligned list of corresponding naming attributes
Domain/NamingAttribute=cn
```

識別主機實體的方法類似於識別使用者實體的方法。鍵名稱及其預設值包括：

```
# Object class that all host entries use
Host/ObjectClass=ipHost
# Attribute whose value in host entries is unique within the repository
Host/UniqueIdAttribute=cn
# Optional container in domain entries of the host entries, remove line if
not used
Host/Container=ou=Hosts
```

使用者設定檔對映

若要定義 LDAP 使用者項目屬性與 Configuration Manager 使用者實體屬性之間的對映，則必須編輯使用者設定檔對映檔案。每個鍵均對應一個 Configuration Manager 使用者屬性。由於鍵已被組織對映識別，因此可將其指定爲使用者項目中屬性名稱的值。User/DisplayNameFormat 設定中使用的屬性必須在使用者設定檔對映中指定。鍵名稱及其預設值包括：

```
# inetOrgPerson.givenName
org.openoffice.UserProfile/Data/givenname = givenname
# person.sn
org.openoffice.UserProfile/Data/sn = sn
# inetOrgPerson.initials
org.openoffice.UserProfile/Data/initials = initials
# organizationalPerson.street
org.openoffice.UserProfile/Data/street = street,postalAddress,streetAddress
# organizationalPerson.l (city)
```

```
org.openoffice.UserProfile/Data/l = l
# organizationalPerson.st (state)
org.openoffice.UserProfile/Data/st = st
# organizationalPerson.postalCode
org.openoffice.UserProfile/Data/postalcode = postalcode
# country.c (country)
org.openoffice.UserProfile/Data/c =
# organizationalPerson.o (company)
org.openoffice.UserProfile/Data/o = o,organizationName
# deprecated -- no LDAP corollary
org.openoffice.UserProfile/Data/position =
# organizationalPerson.title
org.openoffice.UserProfile/Data/title = title
# inetOrgPerson.homePhone
org.openoffice.UserProfile/Data/homephone = homephone
# organizationalPerson.telephoneNumber
org.openoffice.UserProfile/Data/telephonenumber = telephonenumber
# organizationalPerson.facsimileTelephoneNumber
org.openoffice.UserProfile/Data/facsimiletelephonenumber =
facsimiletelephonenumber,officeFax
# inetOrgPerson.mail
org.openoffice.UserProfile/Data/mail = mail
```

佈署

一旦檔案被自訂爲反映 LDAP 系統訊息庫的狀態，即可佈署這些對映檔案。如果 LDAP 伺服器的綱目已包含所需物件類別和屬性，則可直接執行程序檔 `createServiceTree`，否則必須執行程序檔 `deployApoc`。

`deployApoc` 程序檔旨在與 Sun Java System Directory Server 配合使用。它會將提供的綱目延伸檔案複製到適當的目錄並重新啓動 LDAP 伺服器，然後啓動 `createServiceTree` 程序檔。必須將它作爲具有在綱目系統訊息庫中複製檔案和重新啓動伺服器之許可權的使用者來執行，並且必須透過以下指令啓動它：

```
./deployApoc <directory server directory>
```

`<directory server directory>` 參數必須爲 Directory Server 安裝之 `slapd-<server name>` 子目錄的路徑。假定安裝已使用預設目錄且伺服器名爲 `myserver.mydomain`，則該目錄爲 `/var/Sun/mps/slapd-myserver.mydomain`。

`createServiceTree` 程序檔 (無論是直接啓動還是從 `deployApoc` 程序檔啓動) 將提示使用者輸入 LDAP 伺服器的位置 (主機名稱、連接埠號和基本 DN) 和具有管理權限之使用者的定義 (完整 DN 和密碼)。然後此程序檔會在 LDAP 伺服器中建立 bootstrap 服務樹並在其中儲存對映檔案。可將其作爲任何使用者執行，並可透過以下指令來啓動它：

```
./createServiceTree
```

然後提示使用者輸入：

- 主機名稱 (預設爲：localhost)：LDAP 伺服器的主機名稱，
- 連接埠號 (預設爲：389)：LDAP 伺服器的連接埠號，
- 基本 DN：LDAP 系統訊息庫的基本 DN，
- 使用者 DN (預設爲：cn=Directory Manager)：具有足夠權限以在基本 DN 下建立新項目之使用者的完整 DN，
- 密碼：該使用者的密碼，

建立其 DN 爲：

```
ou=ApocRegistry,ou=default,ou=OrganizationConfig,ou=1.0,ou=ApocService,ou=ser
vices,<base DN>
```

的項目，並使用兩個對映檔案的內容來填充。

如上所述，`deployApoc` 程序檔執行的作業假定 LDAP 伺服器的安裝目錄、佈局以及綱目延伸程序與 Sun Java System Directory Server 嚴格匹配。其他目錄將需要手動延伸綱目後才可以執行 `createServiceTree` 程序檔。

建立的樹 (符合將要儲存與實體關聯之配置資料的樹) 與 Sun Java System Identity Server 中用於服務管理的樹的結構一致。如需有關使用 OpenLDAP 和 ActiveDirectory 的詳細資訊，請參閱附錄 C。

其他注意事項

Configuration Manager 架構需要建立具有讀取和搜尋許可權的 LDAP 伺服器連接，以便識別哪個完整 DN 與來自桌面的指定使用者或主機識別碼關聯。爲此，必須配置系統訊息庫，以允許匿名連接，或者必須建立具有讀取和搜尋存取權的特殊使用者。

管理應用程式會在對映至實體的項目下建立服務樹，以儲存這些實體的配置資料。因此，用於管理的使用者項目需要具有在其管理的項目之下建立子項目的權限。

透過稱爲「匿名」和「GSSAPI」的兩種方法，可從桌面用戶端認證架構的使用者。由於桌面用戶端嘗試從 LDAP 伺服器擷取資料時不提供任何憑證，因此「匿名」方法需要在整個系統訊息庫中啓用讀取和搜尋的匿名存取。若要使用「GSSAPI」方法 (使用 Kerberos 進行認證)，必須依「Sun Java System Directory Server Administration Guide」的「Implementing Security」一章中的描述來配置 LDAP 伺服器。

第 3 章

Sun™ Web Console

Sun Web Console 的設計旨在產生適用於 Sun Microsystems 之共用的、基於 Web 的系統管理解決方案。使用者可以從中存取系統管理應用程式，而所有應用程式均提供一致的使用者介面。

主控台基於 Web 模型出於多種原因。但主要原因是讓系統管理員能夠使用 Web 瀏覽器來存取其系統管理應用程式。

Sun Web Console 提供：

- 共用認證與授權
- 共用記錄
- 單一進入點，即透過基於 HTTPS 的同一連接埠存取所有系統管理應用程式
- 共用的外觀和感覺

主控台的主要優勢是管理員僅登入一次即可使用主控台內部的任何應用程式。

系統需求

Sun Web Console 支援多種用戶端和伺服器作業系統以及多種瀏覽器。

用戶端

- Netscape 4.7x、6.2x 和 7.x (對於 Solaris 8 或更高版本)
- Netscape 4.7x、6.2x 和 7.x (對於 Windows 98、98 SE、ME、2000 和 XP)
- Internet Explorer 5.x 和 6.x (對於 Windows 98、98 SE、ME、2000 和 XP)
- Mozilla (對於 Linux 和 Solaris)

伺服器

- Solaris 8 或更高版本
- Redhat 8 或更高版本、Redhat Enterprise Linux 2.1
- SuSE Linux 2.1 或更高版本
- J2SE 版本 1.4.1_03 或更高版本
- 如果在您的伺服器上偵測到 J2SE 1.4.1 或早期版本，則安裝程式會提示您使用 Java Desktop System Management Tools CD 中的 J2SE 版本來升級安裝。
- Tomcat：4.0.3 或更高版本

  Tomcat 包含在 Java Desktop System Management Tools CD 中。

安裝 Sun Web Console

安裝 Sun Web Console 之前，請先閱讀本指南附錄 A 中的套裝軟體摘要和已知問題小節。

Java Desktop System Management Tools CD 包含適用於 Solaris SPARC (版本 8 或更高版本) 和 Linux 作業系統的 Sun Web Console 二進制安裝檔案。

1. 於 Java Desktop System Management Tools CD 之上，變更至與要在其上安裝主控台之作業系統對應的 Sun Web Console 目錄。

   對於 Linux 系統，變更至 `/linux/swc`；對於 Solaris SPARC，變更至 `/solsparc/swc`。

2. 輸入 `./setup`

   依預設，Sun Web Console 不會建立安裝日誌檔。若要建立名爲「logfile」的安裝日誌，請輸入 `./setup | tee logfile`

   注意：當您執行 `setup` 時，Web 主控台的大部分安裝與配置將自動執行。如需有關 Sun Web Console 之 `setup` 應用程式的更多詳細資訊，請參閱附錄 A。

3. 如果您要本土化 Sun Web Console，需要爲每種語言安裝兩個附加套裝軟體。請使用下表來確定所需語言的套裝軟體名稱，並執行以下作業之一：

1. 對於 Solaris，請輸入 `pkgadd -d path/pkgname.pkg pkgname`，其中 *pkgname* 爲您要加入的語言套裝軟體的名稱。
2. 對於 Linux，請輸入 `rpm -i path/pkgname<...>.rpm`，其中 *pkgname* 爲您要加入的套裝軟體的名稱。

套裝軟體名稱	描述
SUNWcmcon，SUNWcmctg	簡體中文 Sun(TM) Web Console 2.0
SUNWdmcon，SUNWdmctg	德文 Sun(TM) Web Console 2.0
SUNWemcon，SUNWemctg	西班牙文 Sun(TM) Web Console 2.0
SUNWfmcon，SUNWfmctg	法文 Sun(TM) Web Console 2.0
SUNWhmcon，SUNWhmctg	繁體中文 Sun(TM) Web Console 2.0
SUNWimcon，SUNWimctg	義大利文 Sun(TM) Web Console 2.0
SUNWjmcon，SUNWjmctg	日文 Sun(TM) Web Console 2.0
SUNWkmcon，SUNWkmctg	韓文 Sun(TM) Web Console 2.0
SUNWsmcon，SUNWsmctg	瑞典文 Sun(TM) Web Console 2.0

執行主控台

如果您要註冊新的應用程式，通常僅需停止並重新啓動 Sun Web Console 伺服器。

初次啓動 Sun Web Console 之前，請確保已完成 Configuration Manager 安裝。

- 若要啓動 Sun Web Console，請輸入 `smcwebserver start`。
- 若要停止 Sun Web Console，請輸入 `smcwebserver stop`。

- 若要存取 Sun Web Console，請在瀏覽器中輸入以下 URL：`https://<host-name>.<domainname>:6789`

依預設，Sun Web Console 支援基於 Unix 的認證和基於角色的存取控制 (RBAC)。然而，您還可以配置其他認證機制，如 LDAP 認證。

注意：預設階段作業逾時爲 15 分鐘。您可以使用 `smreg` 指令來配置逾時長度。例如，若要將逾時長度設定爲 5 分鐘，請輸入 `smreg add -p -c session.timeout.value=5`。

如需有關 Sun Web Console 指令的更多資訊，請參閱 smcwebserver 和 smreg 線上援助頁。

解除安裝 Sun Web Console

若要解除安裝 Sun Web Console，請執行 `/usr/lib/webconsole/setup -u`。

注意：如果您位於 `/usr/lib/webconsole` 目錄或任何相關子目錄中，請勿執行此指令，否則 `pkgrm` 會失敗。

Sun Web Console 連接埠資訊

Configuration Manager 使用 Sun Web Console 的連接埠：

- 8005 以關閉服務，及
- 6789 以用於 `https` 存取。

這兩個連接埠可以在 `/etc/opt/webconsole/server.xml` 中變更。變更連接埠後，請使用 `/usr/sbin/smcwebserver restart` 重新啓動 Sun Web Console。

第 4 章

Sun Java™ Desktop System Configuration Manager 版本 1

Configuration Manager 提供於 Sun Web Console 之上執行的管理工具。這個基於 Web 的使用者介面可讓管理員遍歷組織的階層結構，以定義用於桌面應用程式的策略。可以爲階層結構中的每個項目 (如組織、角色、使用者、網域和主機) 定義這些策略。Configuration Manager 使用多種配置範本來顯示不同桌面應用程式 (如 Gnome、Mozilla、StarSuite 和 Evolution) 的特定設定。

安裝 Configuration Manager

在安裝 Configuration Manager 之前，您需要有可用的 Sun Web Console。

1. 於 Java Desktop System Management Tools CD 之上，變更至相應的 Configuration Manager 目錄。

   對於 Linux 系統，請變更至 `/linux/apoc`。對於 Solaris SPARC，請變更至 `/solsparc/apoc`。

2. 輸入 `./setup`

3. 輸入 LDAP 伺服器的主機名稱。

   預設名稱爲 localhost。

4. 輸入 LDAP 伺服器的連接埠號 (預設爲：389)。

5. 輸入 LDAP 系統訊息庫的基本 DN。

6. 輸入用於識別使用者實體之物件類別的名稱。預設物件類別爲 inetorgperson。

   如需更多詳細資訊，請參閱「LDAP 伺服器」一章中的「組織對映」小節。

7. 輸入在整個 LDAP 系統訊息庫中唯一的屬性名稱。預設屬性爲 uid。

   如需更多詳細資訊，請參閱「LDAP 伺服器」一章中的「組織對映」小節。

8. 輸入具有所需存取權限以在 LDAP 伺服器上執行查詢之使用者的完整 DN。

   使用具有讀取和搜尋存取權的任何完整 DN。對於匿名存取，請保留此欄位爲空白。

9. 輸入您爲其指定了 LDAP 存取權限之使用者的密碼。

   如果您已設定匿名存取 LDAP 伺服器，請忽略此步驟。

在安裝過程中，附加登入模組將加入 Sun Web Console，此模組可讓您透過 LDAP 認證使用者。

安裝結束時，Sun Web Console 將自動重新啓動，以便您可以存取 Configuration Manager。

注意：透過使用 `/usr/share/webconsole/apoc/configure` 程序檔，您可以隨時修改先前的 Configuration Manager 設定。例如，您可使用該程序檔變更至不同的 LDAP 伺服器，而無需重新安裝 Configuration Manager。

執行 Configuration Manager

1. 若要存取 Configuration Manager，請在瀏覽器中輸入以下 URL：

```
https://<hostname>.<domainname>:6789
```

2. 系統提示時，請輸入現有 LDAP 使用者的使用者名稱 (uid) 和密碼。

   Sun Web Console 將開啓。

3. 在主控台視窗中，按一下 **[Sun Java™ Desktop System Configuration Manager** 版本 **1]**。

注意：如果您要略過 Sun Web Console 的啓動頁面而直接移至 Configuration Manager，請在瀏覽器中輸入以下 URL：

```
https://<hostname>.<domainname>:6789/apoc
```

解除安裝 Configuration Manager

若要從 Sun Web Console 解除安裝 Configuration Manager，請變更至 Java Desktop System Management Tools CD 中相應的 Configuration Manager 目錄，然後執行 `./setup -u`。

注意：當您解除安裝 Configuration Manager 時，LDAP 登入模組會從 Sun Web Console 中移除。

第 5 章

桌面元件

若要從 Configuration Manager 存取配置資料，桌面用戶端將需要 Sun Java™ Desktop System Configuration Agent。Configuration Agent 會與遠端配置資料系統訊息庫和介面通訊，並將資料整合至特定配置系統中。目前受支援的配置系統爲 GConf、Mozilla Preference 和 StarSuite Registry。

所有這些元件均作爲 Java Desktop System 的一部分提供和安裝。

資料存取/使用者認證

Configuration Agent 依據桌面使用者的登入 ID，從 LDAP 伺服器擷取資訊。組織對映檔案的 User/UniqueIdAttribute 設定將登入 ID 對映至 LDAP 伺服器中的使用者實體。Configuration Agent 還擷取有關主機的資訊，如主機的名稱或 IP 位址。此資訊經由組織對映檔案的 Host/UniqueIdAttribute 設定對映至 LDAP 伺服器中的主機實體。

存取 LDAP 伺服器有兩種方法，即匿名存取或使用 GSSAPI 存取。對於匿名存取，不需要在桌面上執行動作。對於 GSSAPI 方法，則必須在桌面上獲取 Kerberos 憑證。若要整合 Kerberos 憑證獲取與使用者登入，則必須在 Java Desktop System 主機上安裝並配置 `pam_krb5` 模組。在 Java Desktop System CD 上的 `/usr/share/doc/packages/pam_krb5/README.SuSE` 目錄中，您可以找到 pam 模組的範例配置。您還可以使用 gdm 來整合 Kerberos 和使用者登入，例如，經由使用以下 /etc/pam.d/gdm 檔案：

```
#%PAM-1.0
auth   required    pam_unix2.so  nullok #set_secrpc
auth   optional  pam_krb5.so use_first_pass missing_keytab_ok
ccache=SAFE putenv_direct
account required    pam_unix2.so
password required    pam_unix2.so  #strict=false
session required    pam_unix2.so  # trace or none
session required    pam_devperm.so
session optional    pam_console.so
```

Configuration Agent

Configuration Agent 爲 `APOC` 套裝軟體的一部分。當您安裝相應的 RPM 時，此 API 所需的檔案也被安裝並使用 inetd 註冊。您可手動安裝 RPM 或經由 Java Desktop System 安裝來安裝 RPM。

啓動程式資訊

若要存取遠端配置資料，則必須爲 Configuration Agent 提供 LDAP 伺服器的位置。您可以經由 YaST2 配置工具、autoYaST，或透過手動編輯 `/opt/apoc/lib` 目錄中的 `policymgr.properties` 屬性檔，來加入此位置。在 YaST2 中，您可以在 Network/Advanced 區段中加入該資料。

圖 1 YaST 中的 Java Desktop System Configuration Agent

執行 Configuration Agent 需要以下資訊：

- 主機名稱 (Server)：LDAP 伺服器的主機名稱。
- 連接埠 (Port)：LDAP 伺服器的連接埠號。
- 複合資料存取使用者名稱 (AuthDn)：具有系統訊息庫讀取和搜尋存取權之使用者的完整 DN。

  注意：如果已在目錄中啓用匿名存取，則此設定可保留爲空白。
- 複合資料存取密碼 (Password)：已註冊 LDAP 使用者的密碼。

  注意：如果已在目錄中啓用匿名存取，則此設定可保留爲空白。
- 策略資料存取認證機制 (AuthType)：依據 LDAP 伺服器認證使用者的方法，可爲「匿名」或「GSSAPI」。
- 根位置 (BaseDn)：LDAP 系統訊息庫的基本 DN。
- 主機識別碼 (HostIdentifier)：可以是主機名稱或 IP 位址，且必須設定爲符合用於識別主機的 LDAP 屬性的內容。此屬性在對映檔案中定義爲 Host/UniqueIdAttribute。
- 連接逾時 (Connect Timeout)：指定對 LDAP 伺服器的連接嘗試逾時的秒數。預設值爲 1 秒鐘。

注意：無論您在何時變更這些設定，均必須重新啓動 Configuration Agent。

若要在 Desktop 上重新啓動 Configuration Agent，請確保沒有執行任何相關用戶端應用程式，以超級使用者登入，然後輸入指令 `/opt/apoc/bin/apocd restart`。

操作設定

您可以本機或遠端配置 Configuration Agent 的操作設定。若要本機配置設定，請編輯 `/opt/apoc/lib` 目錄中的 `apocd.properties` 檔案。若要遠端配置設定，請使用 Configuration Manager 中的 Configuration Agent 策略。可在屬性檔中配置以下設定：

- DaemonPort：Configuration Agent 用於偵聽桌面上其用戶端的通訊的連接埠
- MaxClientThreads：可同時處理的用戶端要求的最大數目
- MaxClientConnections：用戶端連接的最大數目
- MaxRequestSize：用戶端要求的最大大小
- DaemonChangeDetectionInterval：此配置設定清單之變更偵測循環的間隔 (以分鐘爲單位)
- ChangeDetectionInterval：用戶端配置資料之變更偵測循環的間隔 (以分鐘爲單位)
- GarbageCollectionInterval：本機配置資料庫中資源回收循環的間隔 (以分鐘爲單位)
- TimeToLive：非離線配置資料在本機資料庫中保留的間隔 (以分鐘爲單位)
- LogLevel：代理程式日誌檔中詳細資訊的級別

DaemonPort 設定僅可本機修改，並需要重新啓動代理程式以使變更生效。所有其他設定將在代理程式配置的下一次變更偵測循環開始時生效。LogLevel 中指定的記錄級別必須是與 Java 記錄程式級別一致的值。這些級別依嚴重性遞減的次序爲：SEVERE、WARNING、INFO、CONFIG、FINE、FINER 和 FINEST。

傳遞配置資料變更

您可以使用「操作設定」一節中所描述的 ChangeDetectionInterval 設定，來調諧遠端配置資料變更至用戶端應用程式的傳遞。您爲該設定提供的值，是遠端所做變更在用戶端應用程式中反映出來之前所需的最大時間長度 (以分鐘爲單位)。爲 ChangeDetectionInterval 設定較小的值將導致 Configuration Agent 和 LDAP 伺服器活動增加。因此，調整設定值時應該謹慎。例如，在初始佈署階段中，您可以將此值設定爲一分鐘，以便可以輕鬆地測試遠端配置對用戶端應用程式的影響。完成測試之後，請將此設定恢復爲初始值。

Configuration Agent 連接埠資訊

Configuration Agent 使用兩個連接埠：

1. 常駐程式連接埠 (預設爲 38900)，常駐程式使用其與用戶端應用程式進行通訊。

2. 常駐程式管理連接埠 (預設爲 38900)，常駐程式控制器程式 `apocdct1` 使用其與常駐程式進行通訊。

變更常駐程式連接埠：

若要變更常駐程式連接埠，您必須在常駐程式的 `apocd.properties` 檔案中修改 `DaemonPort` 屬性，並在 `/etc/services` 和 `/etc/inetd.conf` 中修改 `apocd` 項目。然後，請重新啓動常駐程式並重新載入 `inetd`。

變更常駐程式管理連接埠：

若要變更常駐程式管理連接埠，您必須在常駐程式的 `apocd.properties` 檔案中修改 `Daemon-AdminPort` 屬性。然後，請重新啓動常駐程式。

GConf 介面

GConf 介面是 `apoc-adapter-gconf` 套裝軟體的一部分。當您從相應的 RPM 安裝介面時，`/etc/gconf/2/path` 中的 GConf 資料來源路徑會被更新，以包含 Configuration Manager 來源。舊路徑備份儲存在 `/etc/gconf/2/path.apocBackup` 中。如果舊路徑包含自訂資料來源，您需要將預設路徑的變更合併至新安裝的 Manager 路徑中，以更新路徑。介面提供的兩種資料來源包括：

- 「apoc:readonly:」：提供從策略對不受保護設定的存取。請在使用者設定與本機預設值之間插入此資料來源。
- 「apoc:readonly:mandatory@」：提供從策略對受保護設定的存取。請在本機強制設定與使用者設定之間插入此資料來源。

Mozilla 介面

Mozilla 介面是 `mozilla-apoc-integration` 套裝軟體的一部分。當您從相應的 RPM 安裝介面時，所需檔案會被加入現有 Mozilla 中並會被自動註冊。

StarSuite 介面

StarSuite 介面包含在標準 StarSuite 安裝中，可讓您存取策略配置資料，而不需要任何特殊修改。

第 6 章

附錄 A — Sun Web Console

已知問題

安全性

某些使用者動作可在使用者不知道的情況下讓階段作業保持作用中狀態。例如，使用者關閉瀏覽器視窗時，該使用者不會自動登出 Sun Web Console。如果要結束作用中狀態，使用者必須在關閉應用程式視窗之前，明確地登出 Sun Web Console 中的階段作業。

安裝程序檔使用

提要：`setup [-h] | [-n] | [-d <ver>,<arch>[,用戶端 1,用戶端 2,...]][-u [-f]]`

-h = 列印使用說明

-n = 安裝結束時不啓動伺服器

-u = 解除安裝 Sun Web Console

-f = 如果 Tomcat 和 Java 1.4 已隨附安裝應用程式一起安裝，則解除安裝這些套裝軟體。您僅可將此參數與 -u 參數結合使用。

如需可用安裝參數的完整描述，請執行 `setup -h`。

若要解除安裝 Sun Web Console，請執行 `/usr/lib/webconsole/setup -u`

注意：如果您位於 `/usr/lib/webconsole` 目錄或任何相關子目錄中，請勿執行此指令，否則 `pkgrm` 會失敗。

Sun Web Console 套裝軟體

Solaris 套裝軟體

套裝軟體名稱	*描述*
SUNWmctag	Sun Web Console UI 標記程式庫
SUNWmcon	Sun Web Console
SUNWmcos	Sun Web Console 的共用 Solaris 服務
SUNWmcosx	Sun Web Console 的 Solaris 特定版次服務
SUNWmconr	Sun Web Console 超級使用者
SUNWjato	Sun One 應用程式架構執行階段
SUNWtcatu	Tomcat

Linux RPM

套裝軟體名稱	*描述*
SUNWmctag	Sun Web Console UI 標記程式庫
SUNWmcon	Sun Web Console
SUNWmcos	Sun Web Console 的共用 Linux 服務
SUNWmcosx	Sun Web Console 的 Linux 特定版次服務
SUNWmconr	Sun Web Console 超級使用者
SUNWjato	Sun One 應用程式架構執行階段
tomcat4	Tomcat

附錄 B — Configuration Manager

Configuration Manager 套裝軟體

Solaris 套裝軟體

套裝軟體名稱	*描述*
SUNWapm	Configuration Manager
SUNWapmca	Configuration Agent 範本
SUNWapmev	Evolution 範本
SUNWapmgo	Gnome 範本
SUNWapmmo	Mozilla 範本
SUNWapmso	StarSuite 範本

Linux RPM

套裝軟體名稱	*描述*
apoc-manager	Configuration Manager
apoc-agent-templates	Configuration Agent 範本
apoc-evolution-templates	Evolution 範本
apoc-gnome-templates	Gnome 範本
apoc-mozilla-templates	Mozilla 範本
apoc-starsuite-templates	StarSuite 範本

第 8 章

附錄 C

將 OpenLDAP 與 Configuration Manager 配合使用

若要將 OpenLDAP 伺服器用作 Configuration Manager 資料的系統訊息庫，必須延伸伺服器綱目以支援用於儲存配置資料的物件類別和屬性。名爲 apoc.schema 的自訂綱目檔案可以在 Java Desktop System Management Tools CD 提供之 Configuration Manager 佈署工具的 openldap 子目錄中找到。

該檔案必須要在 OpenLDAP 配置目錄 (`/etc/openldap`) 的 `schema` 子目錄中進行複製，並透過將它包含在位於該目錄的 `slapd.conf` 檔案中而將其加入 OpenLDAP 綱目。透過在該檔案中包含的綱目內容序列末尾插入一行 `/etc/openldap/schema/apoc.schema`，可以完成此作業。如需有關延伸 OpenLDAP 伺服器綱目的更多資訊，請參閱伺服器的使用手冊。

爲準備 OpenLDAP 資料庫以儲存配置資料，必須使用 Configuration Manager 隨附的佈署工具。由於已在先前的安裝步驟中延伸了綱目，因此僅需要執行 `createServiceTree` 程序檔。該程序檔必須從佈署工具目錄以任何使用者的身份透過以下指令執行：`./createServiceTree`。該程序檔會提示使用者輸入有關 OpenLDAP 資料庫的資訊，如本文件的佈署工具一節中所指示。佈署工具的 `openldap` 子目錄中提供了預設對映檔案，其使用 OpenLDAP 中特有的典型物件類別與屬性。該檔案稱爲 `OrganisationalMapping`，並可以透過在啓動 `createServiceTree` 之前用其覆蓋主佈署工具目錄中的同名檔案來進行佈署。

請注意，Configuration Manager Agent 將透過提供要爲其要求資料的使用者之 DN (但無需密碼) 來匿名地嘗試並連接至 OpenLDAP 伺服器。這種匿名認證模式在 OpenLDAP 伺服器的某些版本中依預設可能會被停用，在此種情況下，必須透過在位於 OpenLDAP 配置目錄 (`/etc/openldap`) 的 `slapd.conf` 檔案中所定義之共用伺服器參數中加入一行 allow `bind_anon_cred` 來啓用它。如需有關該參數的更多資訊，請參閱該伺服器的使用手冊。

將 Active Directory 伺服器與 ConfigurationManager 配合使用

若要將 Active Directory 伺服器用作 Configuration Manager 資料的系統訊息庫，必須延伸該伺服器的綱目，以支援用於儲存配置資料的物件類別和屬性。名爲 `apocad.ldf` 的綱目延伸檔案可以在 Enterprise CD 提供之 Configuration Manager 佈署工具的 `ad` 子目錄中找到。請參閱佈署工具一節，以取得更多資訊。

必須使用以下步驟將 apoc-ad.ldf 檔案匯入 Active Directory 網目中：

1. 啓用網目延伸。請參閱 Active Directory 說明文件，以取得有關如何執行該作業的更多資訊，
2. 從指令提示符號處執行以下指令：`ldifde -i -c "DC=Sun,DC=COM" <Base DN> -f apoc-ad-registry.ldf`。

   備註： 使用 Active Directory 基本 DN 取代 <*Base DN*>。

爲準備 Active Directory 伺服器以儲存配置資料，必須使用佈署工具。由於已在先前的安裝步驟中延伸了網目，因此僅需要執行 createServiceTree 程序檔。該程序檔必須從佈署工具目錄以任何使用者的身份透過以下指令執行：./createServiceTree。該程序檔會提示使用者輸入有關 Active Directory 資料庫的資訊。佈署工具目錄的 ad 子目錄中提供了預設對映檔案，其使用 Active Directory 中特有的典型物件類別與屬性。該檔案名爲 OrganisationalMapping，並可以透過在啓動 createServiceTree 之前用其覆蓋主佈署工具目錄中的同名檔案來進行佈署。

因此，Active Directory 伺服器可以與 Configuration Manager 配合使用。請在安裝 Configuration Manager 時提供具有該樹讀取權限之使用者的完整 DN 和密碼。此使用

者可以是無法將 Active Directory 用於其他目的的使用者。請參閱 Active Directory 說明文件，以取得有關如何設定此類使用者的更多資訊。此外，Active Directory 的網域名稱對執行 Configuration Manager 的機器必須是已知的。您可以透過將對映 ActiveDirectory 伺服器 IP 位址及其網域名稱的行加入該機器的 /etc/hosts 檔案來完成此作業。

爲從 Java Desktop System (JDS) 主機上擷取配置資料，Active Directory 的網域名稱對該主機也必須是已知的。JDS 使用者的認證可以透過兩種方法執行：匿名認證與使用 GSSAPI 認證。

- 若要使用匿名連接認證，則必須將 Active Directory 伺服器配置爲授與每個人讀取權限。請參閱 Active Directory 說明文件，以取得有關如何執行該作業的更多資訊。
- 若要使用 GSSAPI 認證，則必須修改指定 Kerberos 參數的檔案/etc/krb5.conf，以定義 Active Directory 範圍並指向 Active Directory 伺服器，以將其作爲主要分配中心 (KDC)。作爲預設加密類型，該檔案還必須指定 Active Directory 支援的 DES 類型，即 des-cbc-crc 與 des-cbc-md5。請參閱 Kerberos 說明文件，以取得有關如何執行該作業的更多資訊。存取配置資料之前，必須獲取 JDS 中所記錄使用者的有效憑證。透過執行 kinit 指令並提供 ActiveDirectory 中定義的密碼，可以手動執行此作業。其他網目可能會在登入時自動產生這些憑證。請參閱 JDS 說明文件，以取得進一步的資訊。