

Novell Identity Manager

3.0

2005 年 12 月 8 日

IDENTITY MANAGER 使用者應用程式：
管理指南

www.novell.com



Novell®

法律聲明

Novell, Inc. 不對本文件的內容或使用做任何陳述或保證，且特別聲明不對任何特定用途的適銷性或適用性提供任何明示或隱喻的保證。此外，Novell, Inc. 保留隨時修改本出版品及其內容的權利，且在進行此類修正或更動時，不需另行通知任何人士或公司。

此外，Novell, Inc. 不對任何軟體作任何陳述或保證，且特別聲明不對任何特定用途的適銷性或適用性提供任何明示或隱喻的保證。此外，Novell, Inc. 保留隨時修改任何或全部 Novell 軟體的權利，且在進行此類更動時，不需通知任何人士或公司。

這份授權書中所提及的任何產品或技術資訊皆受到美國出口管制法 (U.S. Export Control) 及其他國家的交易法約束。您同意遵守所有出口管制法規，並取得出口、再出口或進口交付物品所需之任何必要的授權或類別。您同意不出口或再出口至目前美國出口排除清單上所列公司，或者至美國出口法所指定之禁運或恐怖份子的國家。您同意不將交付產品用在禁止的核子武器、飛彈或化學生物武器等用途上。如需更詳細的 Novell 軟體出口資訊，請參閱 www.novell.com/info/exports/。Novell 無須承擔您無法取得任何必要的出口核准之責任。

版權 © 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004-2005 Novell, Inc. 版權所有。未經出版者的書面同意，本出版品的任何部份皆不可複製、影印、傳送，或是儲存在可擷取系統上。

Novell, Inc. 擁有在此份文件中所描述產品內含技術的智慧財產權。尤其 (但不限於) 這些智慧財產權可能包含一或多個列於 <http://www.novell.com/company/legal/patents/> 的美國專利，以及一或多個在美國和其他國家的額外專利或申請中的專利。

軟體及其文件的所有權、專利、版權和其他所有適用的財產權專屬於 Novell 及其授權人，任何行為不得與此所有權相違背。此軟體受版權法及國際條約之條款的保護。不得從此軟體或其文件中移除任何著作權聲明或其他專利聲明，且必須將這些聲明複製到軟體或其文件的所有副本或擷取部份。您並未獲得該軟體的任何所有權。

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

線上文件：若要存取本產品及其他 Novell 產品的線上文件，或取得更新，請參閱 www.novell.com/documentation。

Novell 商標

Novell 是 Novell, Inc. 在美國與其他國家的註冊商標。

SUSE 是 Novell, Inc. 在美國與其他國家的註冊商標。

協力廠商資料

所有的協力廠商商標均為其個別擁有廠商的財產。

協力廠商法律聲明

Apache 軟體授權 1.1 版

版權 (c) 2000 The Apache Software Foundation。版權所有。

如果滿足下列條件，則無論是否修改，都允許以原始碼和二進位形式重新配送和使用：

1. 重新配送原始碼必須保留上述著作權聲明、此條件清單以及下列免責聲明。
2. 以二進位形式進行的重新配送必須在配送隨附的文件和 / 或其他資料中，複製上述著作權聲明、此條件清單和下列免責聲明。
3. 重新配送若包含任何一般使用者文件，則該文件必須包括下列認可訊息：「本產品內含由 The Apache Software Foundation (<http://www.apache.org/>) 開發的軟體。」

或者，此認可聲明也可出現於軟體中，在此類協力廠商認可聲明一般會顯示的區域。

4. 未經書面許可，不得以 "Apache" 和 "Apache Software Foundation" 之名義背書或推銷從此軟體所衍生的產品。若要獲取書面許可，請聯絡 apache@apache.org。
5. 未經 The Apache Software Foundation 書面許可，此軟體所衍生產品的名稱不得為 "Apache"，或含有 "Apache" 字樣。

本軟體係依「現況」提供，且不提供任何明示或隱喻的保證，包括（但不限於）特定用途之適銷性及適用性的隱喻保證。對於任何直接、間接、附帶、特殊、懲罰性或衍生的損害（包括但不限於代用品或服務的取得；使用、資料或利潤的損失；或者業務中斷），無論是契約責任、無過失責任，或是因使用本軟體所造成的任何侵權行為（包括過失或其他原因），THE APACHE SOFTWARE FOUNDATION 及其顧問即使事先已獲知有發生此種損害的可能性，亦不負擔任何責任。

Autonomy

版權 ©1996-2000 Autonomy, Inc.

Bouncy Castle

授權版權 (c) 2000 - 2004 The Legion Of The Bouncy Castle (<http://www.bouncycastle.org>)

在滿足下列條件的前提下，特此免費授與任何取得此軟體及相關聯文件檔案之副本（該「軟體」）的人員無限制經銷此「軟體」的權限，包括（但不限於）使用、複製、修改、合併、發行、配送、轉授和 / 或銷售該「軟體」副本的權限，並允許配備該「軟體」的人員享有同等權限：

上述著作權聲明和此許可聲明應包含於該「軟體」的所有副本或重要部份中。

本軟體係依「現況」提供，且不提供任何明示或隱喻的保證，包括（但不限於）特定用途之適銷性或適用性以及不侵害他人權益的保證。對於任何索賠、損害或其他責任，無論是否在合約行為中，因本軟體或因本軟體的使用或其他交易造成侵權行為或其他行為，原作者或版權所有人不負擔任何責任。

Castor 程式庫

原始授權位於 <http://www.castor.org/license.html> 中

此專案代碼的發行受到 BSD-like 授權 [license.txt] 制約：

版權 1999-2004 (C) Intalio Inc. 及其他。版權所有。

如果滿足下列條件，則無論是否修改，都允許重新配送和使用此軟體及相關聯文件（「軟體」）：

1. 重新配送原始碼必須保留著作權陳述和聲明。重新配送亦必須包含此文件的副本。
2. 以二進位形式進行的重新配送必須在配送隨附的文件和 / 或其他資料中，複製上述著作權聲明、此條件清單和下列免責聲明。
3. 未經 Intalio Inc. 書面許可，不得以 "ExoLab" 之名義背書或推銷從此「軟體」所衍生的產品。若要獲取書面許可，請聯絡 info@exolab.org。
4. 未經 Intalio Inc 書面許可，此軟體所衍生產品的名稱不得為 "Castor"，或含有 "Castor" 字樣。Exolab、Castor 和 Intalio 是 Intalio Inc 的商標。

5. 特此銘謝 ExoLab Project (<http://www.exolab.org/>)。

INTALIO 及其顧問係依「現況」提供本軟體，且不提供任何明示或隱喻的保證，包括（但不限於）特定用途之適銷性或適用性的隱喻保證。對於任何直接、間接、附帶、特殊、懲罰性或衍生的損害（包括但不限於代用品或服務的取得；使用、資料或利潤的損失；或業務中斷），無論是契約責任、無過失責任，或是因使用本軟體所造成的任何侵權行為（包括過失或其他原因），INTALIO 及其顧問即使事先已獲知有發生此種損害的可能性，亦不負擔任何責任。

Indiana University Extreme! Lab 軟體授權

1.1.1 版

版權 (c) 2002 Extreme! Lab, Indiana University。版權所有。

如果滿足下列條件，則無論是否修改，都允許以來源碼和二進位形式重新配送和使用：

1. 重新配送原始碼必須保留上述著作權聲明、此條件清單以及下列免責聲明。
2. 以二進位形式進行的重新配送必須在配送隨附的文件和 / 或其他資料中，複製上述著作權聲明、此條件清單和下列免責聲明。
3. 重新配送若包含任何一般使用者文件，則該文件必須包含下列認可訊息：「本產品內含由 Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>) 開發的軟體。」

或者，此認可聲明也可出現於軟體中，在此類協力廠商認可聲明一般會顯示的區域。

4. 未經書面許可，不得以 "Indiana University" 和 "Indiana University Extreme! Lab" 之名義背書或推銷從此軟體所衍生的產品。若要獲取書面許可，請聯絡 <http://www.extreme.indiana.edu/>。
5. 未經 Indiana University 書面許可，此軟體所衍生產品的名稱不得為 "Indiana University"，或含有 "Indiana University" 字樣。

本軟體係依「現況」提供，且不提供任何明示或隱喻的保證，包括（但不限於）特定用途之適銷性及適用性的隱喻保證。對於任何直接、間接、附帶、特殊、懲罰性或衍生的損害（包括但不限於代用品或服務的取得；使用、資料或利潤的損失；或業務中斷），無論是契約責任、無過失責任，或是因使用本軟體所造成的任何侵權行為（包括過失或其他原因），原著者、版權所有人及其顧問即使事先已獲知有發生此種損害的可能性，亦不負擔任何責任。

JDOM.JAR

版權 (C) 2000-2002 Brett McLaughlin & Jason Hunter。版權所有。

如果滿足下列條件，則無論是否修改，都允許以來源碼和二進位形式重新配送和使用：

1. 重新配送原始碼必須保留上述著作權聲明、此條件清單和下列免責聲明。
2. 以二進位形式進行的重新配送必須在配送隨附的文件和 / 或其他資料中，複製上述著作權聲明、此條件清單和遵循這些條件的免責聲明。
3. 未經書面許可，不得以 "JDOM" 之名義背書或推銷從此軟體所衍生的產品。若要獲取書面許可，請聯絡 license@jdom.org。
4. 未經 JDOM Project Management (pm@jdom.org) 書面許可，此軟體所衍生產品的名稱不得為 "JDOM"，或含有 "JDOM" 字樣。

此外，我們請求（但不要求）您在重新配送隨附的一般使用者文件和 / 或軟體本身中包含下列認可訊息：「本產品內含由 JDOM Project (<http://www.jdom.org/>) 開發的軟體。」

或者，可以使用 <http://www.jdom.org/images/logos> 中的標誌以圖形代表該認可訊息。

本軟體係依「現況」提供，且不提供任何明示或隱喻的保證，包括（但不限於）特定用途之適銷性或適用性的隱喻保證。對於任何直接、間接、附帶、特殊、懲罰性或衍生的損害（包括但不限於代用品或服務的取得；使用、資料或利潤的損失；或業務中斷），無論是契約責任、無過失責任，或是因使用本軟體所造成的任何侵權行為（包括過失或其他原因），JDOM 原著者或專案顧問即使事先已獲知有發生此種損害的可能性，亦不負擔任何責任。

Phaos

本「軟體」部份衍生自「SSLava™ 工具套件」，該工具套件為版權 ©1996-1998 by Phaos Technology Corporation。版權所有。客戶不得存取 Phaos 軟體的功能。

W3C

W3C® 軟體聲明和授權

本產品 (及內含軟體、文件，如 README 或其他相關項目) 由受下列授權保護的版權所有人提供。獲取、使用和 / 或複製此產品，即表示您 (使用人) 同意您已閱讀、理解並將遵守下列條款和條件。

特此授與無論出於任何目的，皆可免費或免版稅複製、修改和配送此軟體及其文件 (無論是否修改) 的權限，但軟體和文件的「全部」副本或部份副本 (包括修改) 中必須包括下列各項：

1. 此「聲明」的全文必須位於重新配送或派生產品上、使用者明顯可見之處。
2. 任何已存在智慧財產免責聲明、聲明或條款及條件。若不存在上述內容，則應在任何重新配送或派生的程式碼主體內，包括「W3C 軟體簡短聲明」(偏好使用超文字，但允許使用文字)。
3. 對檔案進行之任何變更或修改的聲明，包括日期變更 (建議您提供衍生程式碼之位置的 URI)。

本軟體和文件係依「現況」提供，版權所有人不作任何陳述或任何明示或隱喻的陳述或保證 (包括但不限於特定用途之適銷性或適用性的保證)，另使用本軟體或文件時亦不得侵害第三方的專利、版權、商標或其他權利。

對於因使用本軟體或文件所造成的任何直接、間接、特殊或衍生的損害，版權所有人不負擔任何責任。

未經特定的書面許可，不得將版權所有人的姓名和商標用於該軟體相關的廣告或宣傳。此軟體及任何相關聯文件中的版權所有權始終歸於版權所有人。

目錄

關於本書	9
I 綜覽	11
1 綜覽	13
1.1 支援的角色類型	15
1.1.1 LDAP 管理員	15
1.1.2 使用者應用程式管理員	16
1.1.3 一般使用者	16
1.1.4 委託使用者	17
1.1.5 代理使用者	18
1.2 資料抽象：靈活身份管理的關鍵	18
1.3 高層級結構綜覽	19
1.3.1 身份儲存區	20
1.3.2 JBoss	21
1.3.3 資料庫	21
1.3.4 Identity Manager 引擎	21
1.3.5 使用者應用程式驅動程式	22
1.3.6 目錄抽象層	23
1.3.7 工作流程引擎	24
1.3.8 使用者介面	24
1.4 設計和組態設定工具	24
1.5 使用案例	25
1.5.1 案例 A：使用者搜尋組織中其他人的資訊	25
1.5.2 案例 B：管理員建立新的使用者	27
1.5.3 案例 C：使用者提供	28
1.6 接下來的步驟	30
2 設計生產環境	31
2.1 拓樸	31
2.1.1 最少的設計	31
2.1.2 高可用性設計	32
2.1.3 設計條件約束	32
2.2 安全性	33
2.2.1 相互驗證	35
2.3 效能調整	35
2.3.1 記錄	35
2.3.2 Identity Vault	36
2.3.3 JVM	37
2.3.4 會期逾時值	38
2.4 叢集	38
2.4.1 叢集 JBoss	38
2.4.2 安裝使用者應用程式至 JBoss 叢集	40
2.4.3 設定使用者應用程式叢集群組快取組態	43
2.4.4 設定叢集的工作流程	43

II	設定使用者應用程式環境的組態	45
3	設定使用者應用程式驅動程式的組態	47
3.1	關於使用者應用程式驅動程式	47
3.2	建立使用者應用程式驅動程式	47
3.3	啓動使用者應用程式驅動程式	54
3.4	設定工作流程以自動啓動	55
3.4.1	關於規則	55
3.4.2	設定工作流程以根據 Identity Vault 中的事件啓動	55
4	設定目錄抽象層的組態	65
4.1	關於目錄抽象層定義	65
4.2	開始使用	66
4.2.1	完成使用者應用程式驅動程式組態	67
4.2.2	存取提供檢視窗	71
4.2.3	啓動目錄抽象層編輯器	72
4.3	使用實體和屬性	76
4.3.1	新增實體的步驟	76
4.3.2	分析資料需求	77
4.3.3	定義實體	77
4.4	使用清單	91
4.4.1	關於偏好的地區設定清單	93
4.4.2	關於提供類別清單	93
4.5	使用組織圖關係	94
4.5.1	關係內容參考	96
4.6	使用組態設定	97
4.7	當地語系化顯示文字	97
4.7.1	支援的語言	97
4.7.2	當地語系化文字	98
4.8	輸入、驗證和部署目錄抽象層定義	98
4.8.1	關於輸入	99
4.8.2	關於驗證	101
4.8.3	關於部署	101
5	設定記錄	105
5.1	關於事件記錄	105
5.1.1	關於記錄層級設定	105
5.2	記錄至 Novell Audit 伺服器	105
5.2.1	將 Identity Manager 應用程式網要做為記錄應用程式新增至 Novell Audit 伺服器	106
5.2.2	啓用 Audit 記錄	107
5.2.3	記錄的事件	107
5.2.4	記錄報告	109
III	管理使用者應用程式	113
6	使用管理索引標籤	115
6.1	關於管理索引標籤	115
6.2	可以使用管理索引標籤的人員	115
6.3	存取管理索引標籤	116
6.4	您可以執行的管理動作	118

7	頁面管理	121
7.1	關於頁面管理	121
7.1.1	關於容器頁面	121
7.1.2	關於共用頁面	127
7.1.3	頁面使用的例外	129
7.2	建立和維護容器頁面	129
7.2.1	建立容器頁面	129
7.2.2	新增內容至容器頁面	132
7.2.3	刪除容器頁面的內容	133
7.2.4	修改容器頁面的配置	134
7.2.5	安排容器頁面的內容	135
7.2.6	顯示容器頁面	137
7.3	建立和維護共用頁面	137
7.3.1	建立共用頁面	138
7.3.2	新增內容至共用頁面	140
7.3.3	刪除共用頁面的內容	142
7.3.4	修改共用頁面的配置	143
7.3.5	安排共用頁面的內容	144
7.3.6	顯示共用頁面	145
7.4	指定頁面的許可	145
7.4.1	指定頁面檢視權限	146
7.4.2	指定共用頁面擁有者	148
7.4.3	允許使用者存取建立使用者或群組頁面	149
7.4.4	允許使用者存取個別管理頁面	150
7.5	設定群組的預設頁面	150
7.6	選取容器頁面的預設共用頁面	152
8	主題組態	155
8.1	關於主題組態	155
8.2	預覽主題	156
8.3	選擇主題	157
8.4	自定主題的品牌	158
9	入口網站應用程式管理	161
9.1	關於入口網站應用程式管理	161
9.2	管理入口網站應用程式	161
9.2.1	存取伺服器上的入口網站應用程式	162
9.2.2	檢視入口網站應用程式的相關資訊	162
9.2.3	取消註冊入口網站應用程式	163
9.3	管理入口網站應用程式定義	164
9.3.1	存取已部署之入口網站應用程式中的入口網站應用程式定義	164
9.3.2	註冊入口網站應用程式定義	165
9.3.3	檢視入口網站應用程式定義的相關資訊	166
9.4	管理已註冊的入口網站應用程式	168
9.4.1	存取已部署之入口網站應用程式中的入口網站應用程式註冊	169
9.4.2	檢視入口網站應用程式註冊的相關資訊	169
9.4.3	指定入口網站應用程式註冊的類別	170
9.4.4	修改入口網站應用程式註冊的設定	171
9.4.5	修改入口網站應用程式註冊的優先設定	174
9.4.6	指定入口網站應用程式註冊的安全性權限	176
9.4.7	取消註冊入口網站應用程式	179

10	入口網站組態	181
10.1	關於入口網站組態	181
10.2	一般設定	181
10.2.1	您可以變更的設定	182
10.2.2	唯讀設定	183
10.3	LDAP 連接參數	184
10.3.1	您可以變更的設定	185
10.3.2	唯讀設定	185
11	安全性組態	187
11.1	關於安全性組態	187
11.2	指定使用者應用程式管理員	188
12	記錄組態	191
12.1	關於記錄組態	191
12.2	關於記錄	191
12.3	變更記錄層級	193
12.4	將記錄訊息傳送至 Novell Audit	194
12.5	沿用您的記錄設定	194
13	快取組態	197
13.1	關於快取組態	197
13.2	衝洗快取	198
13.2.1	衝洗目錄抽象層快取	199
13.2.2	在叢集中衝洗快取	199
13.3	設定快取設定的組態	199
13.3.1	如何實作快取	200
13.3.2	如何儲存快取設定	200
13.3.3	如何顯示快取設定	201
13.3.4	基本快取設定	202
13.3.5	叢集的快取設定	203
14	用於輸出和輸入入口網站資料的工具	205
14.1	關於輸出和輸入入口網站資料	205
14.1.1	用途	205
14.1.2	要求	205
14.1.3	限制	206
14.1.4	步驟	206
14.2	輸出入口網站資料	206
14.3	輸入口網站資料	208
IV	入口網站應用程式參考資訊	213
15	關於入口網站應用程式	215
15.1	附屬入口網站應用程式	215
15.2	管理入口網站應用程式	215
15.2.1	共用頁面導覽入口網站應用程式	216
15.3	身份入口網站應用程式	216
15.4	密碼入口網站應用程式	216

15.5	系統入口網站應用程式	217
16	建立入口網站應用程式參考資訊	219
16.1	關於建立入口網站應用程式	219
16.2	設定建立入口網站應用程式的組態	220
16.2.1	目錄抽象層設定	221
16.3	設定建立優先設定	222
17	詳細資料入口網站應用程式參考資訊	225
17.1	關於詳細資料入口網站應用程式	225
17.1.1	顯示實體資料	226
17.1.2	編輯實體資料	229
17.1.3	以電子郵件傳送實體資料	231
17.1.4	連結至組織圖	232
17.1.5	連結至其他實體的詳細資料	232
17.1.6	列印實體資料	233
17.2	先決條件	233
17.2.1	設定目錄抽象層的組態	234
17.2.2	指定實體的權限	234
17.3	從其他入口網站應用程式啟動詳細資料	234
17.3.1	從搜尋清單入口網站應用程式	235
17.3.2	從組織圖入口網站應用程式	235
17.4	在頁面上使用詳細資料	236
17.5	設定優先設定	236
17.5.1	關於優先設定	237
18	組織圖入口網站應用程式參考資訊	239
18.1	關於組織圖	239
18.1.1	關於組織圖關係	240
18.1.2	關於組織圖顯示	241
18.2	設定組織圖入口網站應用程式的組態	241
18.2.1	目錄抽象層設定	242
18.2.2	設定組織圖優先設定	242
18.2.3	動態載入影像	251
19	密碼管理入口網站應用程式參考資訊	253
19.1	準備密碼管理	253
19.1.1	關於密碼管理功能	253
19.1.2	eDirectory 中所需的設定	253
19.2	關於密碼入口網站應用程式	255
19.2.1	密碼自助服務入口網站應用程式模式	256
19.3	IDM 登入入口網站應用程式	257
19.3.1	要求	257
19.3.2	用法	257
19.4	IDM 處理安全回應入口網站應用程式	258
19.4.1	要求	258
19.4.2	用法	259
19.5	IDM 提示定義入口網站應用程式	259
19.5.1	要求	259
19.5.2	用法	260
19.6	IDM 變更密碼入口網站應用程式	260

19.6.1	要求	261
19.6.2	用法	261
19.7	IDM 忘記密碼入口網站應用程式	262
19.7.1	要求	263
19.7.2	用法	263
20	搜尋清單入口網站應用程式參考資訊	265
20.1	關於搜尋清單	265
20.1.1	關於結果清單顯示格式	268
20.2	設定搜尋清單入口網站應用程式的組態	270
20.2.1	目錄抽象層設定	271
20.2.2	設定搜尋清單優先設定	271
V	設計和管理提供申請	277
21	工作流程提供簡介	279
21.1	關於工作流程提供	279
21.1.1	高層級結構	280
21.1.2	提供和工作流程範例	282
21.2	提供組態和管理	287
21.3	提供安全性	287
22	設定提供申請定義的組態	291
22.1	關於提供申請組態外掛程式	291
22.2	使用已安裝的範本	291
22.3	設定提供申請定義的組態	294
22.3.1	選取驅動程式	294
22.3.2	建立或編輯提供申請	295
22.3.3	刪除提供申請	308
22.3.4	變更現有提供申請的狀態	309
22.3.5	定義現有提供申請的權限	310
23	管理提供工作流程	313
23.1	關於工作流程管理外掛程式	313
23.2	管理工作流程	313
23.2.1	連接至工作流程伺服器	314
23.2.2	尋找符合搜尋準則的工作流程	316
23.2.3	控制使用中工作流程顯示	319
23.2.4	終止工作流程例項	320
23.2.5	檢視工作流程例項的詳細資料	320
23.2.6	重新指定工作流程例項	321
23.3	設定電子郵件伺服器的組態	321
23.4	使用已安裝的電子郵件範本	322
23.4.1	預設內容和格式	322
23.4.2	編輯範本	323
23.4.3	修改範本的預設值	325

VI	附錄	327
A	綱要延伸	329
A.1	屬性綱要延伸	329
A.2	Objectclass 綱要延伸	331
A.3	LDIF 表示	332
B	設定應用程式歸檔的組態	343
B.1	關於使用者應用程式 WAR	343
B.2	設定會期逾時	343

關於本書

目的

本書說明如何管理 Novell Identity Manager 使用者應用程式，包含：

- ◆ Identity Manager 提供的身份自助服務功能
- ◆ 工作流程提供功能 (前提是您必須新增「Identity Manager 提供模組」)

若要瞭解如何管理 Identity Manager 的其他功能 (所有封裝的通用功能)，請參閱《Novell Identity Manager：管理指南》。

使用對象

本書中的資訊適用於負責設定、部署和管理 Identity Manager 使用者應用程式之身份自助服務功能和 / 或工作流程提供功能的系統管理員、設計師和顧問。

《Identity Manager 使用者應用程式：使用者指南》中已提供這些功能的一般使用者文件。

先決條件

本書假設：

- ◆ 您已安裝 Identity Manager，而且可能也已安裝「Identity Manager 提供模組」

如需安裝這些產品的指示，請參閱《Novell Identity Manager：安裝指南》。

- ◆ 您已設定其他 Identity Manager 功能的組態，使之適合於您的需要

請參閱《Novell Identity Manager：管理指南》。

組織

本書內容摘要如下：

部份	描述
「綜覽」，第 11 頁	介紹 Identity Manager 使用者應用程式，並協助您規劃其在您組織中的使用
「設定使用者應用程式環境的組態」，第 45 頁	如何設定不同方面的 Identity Manager 使用者應用程式環境組態 (包含使用者應用程式驅動程式、目錄抽象層和記錄)，以符合您組織的需要
「管理使用者應用程式」，第 113 頁	如何利用使用者介面的「管理」索引標籤，設定組態和管理 Identity Manager 使用者應用程式
「入口網站應用程式參考資訊」，第 213 頁	如何設定在 Identity Manager 使用者介面中使用之身份和系統入口網站應用程式的組態

部份	描述
「設計和管理提供申請」，第 277 頁	如何使用「Identity Manager 提供模組」，設定組態、部署和管理提供所需的資源、工作流程和申請定義
	附註：本部份僅在您擁有「Identity Manager 提供模組」時適用。
「附錄」，第 327 頁	Identity Manager 使用者應用程式的其他參考資訊 (綱要延伸) 和進階主題 (設定應用程式歸檔的組態)

並請參閱

如需其他相關手冊和讀我資訊，請前往 Novell 文件網站的 [Identity Manager 頁面 \(http://www.novell.com/idm/\)](http://www.novell.com/idm/)。

綜覽

下列各章介紹 Identity Manager 使用者應用程式，並協助您規劃其在您組織中的使用。

- ◆ 第 1 章 「綜覽」, 第 13 頁
- ◆ 第 2 章 「設計生產環境」, 第 31 頁

Novell Identity Manager 使用者應用程式是功能強大的 Web 應用程式，設計用於讓使用者能夠以豐富、直觀的方式有效地設定和管理複雜的身份服務架構。「Identity Manager 使用者應用程式」與「Identity Manager 提供模組」和 Novell Audit 一起使用時，可提供完整的端對端提供解決方案，該解決方案安全、可調整且易於管理。

使用者應用程式提供下列 Web 型態一般使用者功能：

- ◆ 白頁
- ◆ 組織圖
- ◆ 使用者搜尋 (可以儲存自定搜尋組態)
- ◆ 自助服務密碼管理
- ◆ 輕量使用者管理工具
- ◆ 工作流程的啓始和監控 (如果已安裝「提供模組」的話)
- ◆ 個人和 / 或小組任務管理 (如果已安裝「提供模組」的話)
- ◆ 委託和代理功能

針對系統管理員，使用者應用程式提供各種組態和管理功能，包含：

- ◆ 允許設定及管理代理和委託權限的介面
- ◆ 對記錄工具和自定 Crystal Reports 的存取
- ◆ 基於精靈的工作流程組態設定 (如果已安裝「提供模組」的話)
- ◆ 工作流程管理 (如果已安裝「提供模組」的話)，包含重新指定或終止處理中工作流程的能力
- ◆ 基於 Eclipse 的 Designer，用於建立自定目錄抽象定義和關係

下表顯示更完整的功能清單。

功能	描述
遵循標準、多樣化瀏覽器的可擴充 Web UI 使用者環境	管理員可以變更頁面配置、預設頁面 (首頁)、新增頁面，以及修改整體外觀 (主題)。 透過新增與 JSR-168 相容的入口網站應用程式可以擴充使用者應用程式。
提供工作流程 (如果已安裝「提供模組」的話)	管理員可以建立專門的工作流程，來處理提供申請。 之後，具有適當權限的一般使用者也可以啓始那些工作流程。
事件驅動的工作流程 (如果已安裝「提供模組」的話)	除了使用者啓始的工作流程，管理員還可以使用此方式設定工作流程的組態，以便在身份儲存區中發生指定事件時，可以自動引發該工作流程。
功能提升的白頁	按字母順序、地理位置、技能集等顯示使用者資訊。
組織圖	使用者應用程式包含進階的組織圖建立入口網站應用程式，它會運用 AJAX 以提供豐富的互動體驗。

功能	描述
使用者搜尋	使用者可以對身份執行搜尋，並儲存自定搜尋定義，以便稍後重複使用。
密碼自助服務	使用者應用程式可讓一般使用者存取密碼管理功能，而無需向 Help Desk 求助。
輕量使用者管理	使用者應用程式可讓非 IT 管理員的一般使用者執行一組有限的身份管理任務。
基於 Eclipse 的 Designer	系統管理員、開發人員、顧問和其他 IT 專家可以使用 Designer 應用程式，快速而輕鬆地執行各種組態設定和其他任務。例如， Designer 可讓您離線使用實體定義和關係、驅動程式規則和過濾器，以及各種驅動程式和驅動程式集組態設定任務。變更可以儲存在專案中，並 / 或上載至身份儲存區。
代理角色 (如果已安裝 「提供模組」 的話)	使用者應用程式使用者介面可讓合法的人員定義特定使用者的代理角色 (代理可以使用另一個使用者的所有權限，代表該使用者執行任務) 。
任務的委託 (如果已安裝 「提供模組」 的話)	使用者介面可讓管理員 (和具有適當權限的使用者) ，在指定使用者無法執行工作時，設定將任務自動委託給同儕。委託的設計非常精細，可以將特定類型的任務委派給不同的人。
目錄抽象層	爲了保證安全、強固的目錄抽象結構，執行時期架構會將 Web 應用程式邏輯與身份儲存區存取和工作流程這樣的低層構造相隔離。透過稱爲目錄抽象層 (或只是抽象層) 的調節層即可進行隔離。
對所有使用者可見資料的存取控制	抽象層 (運用 eDirectory 的複雜 「有效權限」 模式) 會對使用者，甚至入口網站應用程式本身都透明的方式，自動限制身份資料和工作流程的可見度，以及使用者修改資料的權限。
一般使用者身份資料驗證	使用者應用程式會提供一種方式，讓使用者在其自己的身份資訊顯示於身份儲存區內時，可以檢視和驗證 / 更新該資訊。
靈活記錄	輕鬆地將各種事件記錄到伺服器記錄 (透過 log4j) 或 Novell Audit ，或兩者中。
Novell Audit 報告	該產品包含預先範本化的 Crystal Reports ，其反映與提供相關的一般報告任務。
高可用性	可以將產品的使用者應用程式和核准流程元素形成叢集以便進行調整。
	重要：在此版本的 「提供模組」 中，不支援處理中工作流程例項的自動容錯移轉。不過，您可以透過手動介入步驟，在剩餘的伺服器節點上繼續完成已中斷的處理中流程。
電子郵件範本管理 UI	使用 iManager 關聯和自定工作流程的電子郵件範本。

功能	描述
附屬入口網站應用程式	使用者應用程式隨附之各種可用的入口網站應用程式，包含 GroupWise、Exchange、Lotus Notes、「Web 郵件」、「網路檔案」、NetStorage、HTML、「捷徑」、RDF 網站摘要 (RDF Site Summary, RSS) 和「訊息」入口網站應用程式。

以上是 Identity Manager 所提供之標準功能之外的附加功能。如需產品標準功能集的相關資訊，請參閱《Identity Manager 管理員指南》。

1.1 支援的角色類型

Identity Manager 使用者應用程式包含一套完善的身份管理功能。並非每一個使用者都需要使用 (或者都能夠查看) 每種類型的功能；能否使用或查看功能取決於人員的角色。

使用者應該都會屬於下列一或多個類別，每種類別都有不同的工具和功能 (本文件中全篇都會使用到下列詞彙)。

1.1.1 LDAP 管理員

輕量目錄存取協定 (Lightweight Directory Access Protocol, LDAP) 管理員是針對身份儲存區 (eDirectory 8.7.x 或 8.8)，具有最多組態設定和系統管理權限的人員。這是「使用者應用程式管理員」(如下)也可以共享的邏輯角色，「使用者應用程式管理員」是對應用程式伺服器 (JBoss)、資料庫 (例如，MySQL) 和 / 或入口網站型 Web UI 本身具有系統權限的人員或實體。

LDAP 管理員可選擇用以完成其工作的工具有兩種：基於 Eclipse 的 Designer for Identity Manager，用於處理罕見任務 (可能只有一次)，以及用於日常管理任務的 iManager 工具。

通常使用 Designer for Identity Manager 執行的罕見任務包含：

- ◆ 設定可用於 Identity Manager 使用者應用程式之抽象層定義、屬性和關係的組態 (如需相關資訊，請參閱第 4 章「設定目錄抽象層的組態」, 第 65 頁一章)。
- ◆ 驗證目錄抽象層定義 (請參閱第 4 章「設定目錄抽象層的組態」, 第 65 頁一章)。
- ◆ 變更「使用者應用程式驅動程式」設定 (請參閱第 3 章「設定使用者應用程式驅動程式的組態」, 第 47 頁一章)。
- ◆ 將實體和屬性顯示標籤、組織圖關係名稱以及全域和本地清單項目等的顯示文字當地語系化 (請參閱第 4 章「設定目錄抽象層的組態」, 第 65 頁一章)。
- ◆ 輸入或輸出「使用者應用程式驅動程式」及其設定。
- ◆ 其他類型的離線任務。

通常，管理員 (無論是 LDAP 管理員還是如下所述的「使用者應用程式管理員」) 在即時系統上操作的日常任務是在 iManager 中完成。此類任務可能包含：

- ◆ 管理電子郵件範本
- ◆ 定義或指定提供資源和提供申請定義。
- ◆ 啟用或停用工作流程定義，讓它成為使用中或非使用中。
- ◆ 終止處理中工作流程。
- ◆ 執行 Novell Audit 記錄資料的報告。

僅當已安裝「提供模組」時，才會套用其中某些任務（與工作流程相關的任務）。而且，很多任務可能是由「使用者應用程式管理員」（如下）而不是 LDAP 管理員完成。

1.1.2 使用者應用程式管理員

「使用者應用程式管理員」執行與管理 Web 應用程式（在 JBoss 上執行的瀏覽型應用程式）相關聯的任務。可以透過 Identity Manager 使用者介面的「管理」索引標籤，存取此角色的管理工具。

可以在使用者應用程式中執行的動作包含：

- ◆ 設定各種應用程式設定的組態，例如，告知使用者應用程式如何連接至身份儲存區（LDAP 提供者）的設定。如需詳細資訊，請參閱第 10 章「入口網站組態」，第 181 頁。
- ◆ 判定 Identity Manager 使用者介面中顯示的頁面，以及有權限可以存取該頁面的使用者（請參閱第 7 章「頁面管理」，第 121 頁）。
- ◆ 判定 Identity Manager 使用者介面中可用的入口網站應用程式，以及有權限可以存取該入口網站應用程式的使用者（請參閱第 9 章「入口網站應用程式管理」，第 161 頁）。
- ◆ 判定 Identity Manager 使用者介面的外觀和操作（請參閱第 8 章「主題組態」，第 155 頁）。
- ◆ 控制想要 Identity Manager 使用者應用程式產生的記錄訊息層級，以及其中會傳送至 Novell Audit 的訊息（如果有的話）（請參閱第 12 章「記錄組態」，第 191 頁）。
- ◆ 管理 Identity Manager 使用者應用程式維護的各種快取（請參閱第 13 章「快取組態」，第 197 頁）。
- ◆ 輸出或輸入 Identity Manager 使用者應用程式中使用的 Web 內容（頁面和入口網站應用程式）（請參閱第 14 章「用於輸出和輸入入口網站資料的工具」，第 205 頁）。
- ◆ 設定特定個人的代理權限。
- ◆ 其他許多與一般使用者看到之使用者介面相關的任務。

您在 iManager 中執行的任務包含：

- ◆ 管理電子郵件範本。
- ◆ 定義或指定提供資源和提供申請定義。
- ◆ 啓用或停用工作流程定義，讓它成為使用中或非使用中。
- ◆ 終止處理中的工作流程。
- ◆ 執行 Novell Audit 記錄資料的報告。

僅當已安裝「提供模組」時，才會套用其中某些任務（與工作流程相關的任務）。

1.1.3 一般使用者

一般使用者是檢視並與各種入口網站應用程式和 Web 頁面（共同構成使用者應用程式的使用者介面）互動的人員。在此情況下，一般使用者意指員工、管理員，或員工或管理員的代理或受託者。

根據管理員所啓用的功能數量，一般使用者可能具有執行許多工作的能力。一般使用者至少能夠使用 Identity Manager 使用者應用程式來：

- ◆ 使用「組織圖」入口網站應用程式檢視「使用者」物件之間的階層式關係。

- ◆ 檢視和編輯使用者資訊 (使用適當權限)。
- ◆ 使用進階搜尋準則搜尋使用者或資源 (可儲存以供稍後重複使用)。
- ◆ 復原忘記的密碼。
- ◆ 將電子郵件傳送給小組成員 (個別或全體)。

此外，安裝「提供模組」之後，使用者應用程式的 Web 介面可讓使用者：

- ◆ 申請資源 (啟動許多潛在預先定義工作流程的其中之一)。
- ◆ 檢視先前申請的狀態。
- ◆ 要求任務並檢視任務清單 (依資源、收件者或其他特性)。
- ◆ 檢視代理指定。
- ◆ 檢視委託指定。
- ◆ 指定使用者本身是否可以執行工作。
- ◆ 進入代理模式以代表其他使用者要求任務。
- ◆ 檢視小組任務、申請小組資源等 (僅限管理員)。



1.1.4 委託使用者

委託使用者或受託者是可以對其委託一或多個特定任務 (適合於該使用者的權限) 的一般使用者，所以受託者可以代表其他使用者處理那些特定任務。例如，John 要去度假，想要 Mary 在其離開期間處理他的任務。假設 Mary 對 John 委託之任務具有適當的權限，Mary 就可以成為 John 的受託者。當 John 在使用者應用程式中將自己標示為無法處理任務時，通常顯示在 John 任務清單中的所有任務就會改為顯示在 Mary 的任務清單中。因此，Mary 會扮演委託使用者的角色。她可以要求 John 的任務完全成為她的任務 (即不再是 John 的任務)。請將此詞彙與下面的代理使用者定義相對比。

請注意，委託是按個別任務執行，無需完全轉移職責 (雖然當實際上有需要時，使用者介面確實允許將使用者的所有任務都委託給特定受託者)。特定使用者可以指定多個受託者。每個受託者只能負責已指定給他 (或她) 的任務 (例如，John 可能想要 Mary 處理所有收到的新名片申請任務，但可能要 Bill 處理新的 Siebel 帳戶申請)。當任務的原始擁有者宣稱其無

法執行特定類型任務時，職責轉移（重新指定新任務）會自動發生（聲明者可以重新針對每個任務，選擇性地指定委託的過期期間）。此轉移會經過記錄以備確認之用。

《Identity Manager 使用者應用程式：使用者指南》的「第一章」中包含委託使用者之使用者介面功能的詳細描述。並請參閱本指南中「提供安全性」，第 287 頁。

1.1.5 代理使用者

代理使用者是藉由暫時擔任其他使用者的身份，扮演該使用者角色的一般使用者。原始使用者的所有權限都會套用至代理。原始使用者擁有的工作會繼續屬於該使用者。例如，John 想要其行政助理 Clive 在他到中國度假期間，能夠存取和處理其 (John) 所有任務。如果 John 擁有適當的權限，則可以指定 Clive 作為其代理（如果他沒有適當的權限，則「使用者應用程式管理員」會進行此設定）。建立代理關係之後，Clive 可以扮演兩個角色：Clive 的角色或 John 的角色。在 John 的角色中，他可以執行 John 可執行的任何動作。Clive 所完成的工作項目就像 John 自己執行了該工作項目一樣。

請注意，與前一節中說明的委託機制相比，代理關係可讓代理使用者完全看到（並可以執行）原始使用者的任務和設定。而且，John 的代理在代理角色期間，可以存取 John 可存取的任何屬性、關係或系統設定。

受託者和代理之間的另一個區別在於：使用者可以將某些任務委託給一個受託者，而將其他種類的任務委託給另一個受託者，但是代理始終是取得原始使用者的所有任務。換言之，當您指定某人作為代理時，就可以確定該人員可以看到並處理您的所有任務。如同此人員變成了您一樣。

請注意，代表其他使用者承擔的代理動作會記錄到 Novell Audit（以示確認）。

《Identity Manager 使用者應用程式：使用者指南》的「設定提供設定的組態」中，包含代理案例的其他資訊。

1.2 資料抽象：靈活身份管理的關鍵

瞭解 Identity Manager 使用者應用程式的關鍵概念是資料抽象概念，或者能夠定義、檢視和處理目錄抽象層定義例項的概念。

傳統儲存技術無論是否涉及關聯式資料庫、X.500 目錄或其他儲存機制，通常都需要資料項目（資料庫中的列、X.500 目錄中的物件等）嚴格符合定義明確的綱要。對已儲存資料進行查詢可能會相當複雜（理論上），而且資料可能包含索引和 / 或反向連結，但是實際資料項目本身應符合固定的定義。而且，要假設適合的綱要在一段時間內不會發生明顯的變更。

當需要集合資訊（可能來自不同資料來源，且依賴於不同綱要）以建立符合任意新（可能是暫時的）綱要的複合資料物件時，這會是個問題。身份資料是典型的範例，因為身份趨向於複合和非靜態的。而且，指定身份所依據的資料部份可以來自不同的來源，每個來源都可能盡責保護資訊的管理員。

身份資料的分散式性質是對身份管理的挑戰，在面對嚴格（與行政相結合）的綱要定義時很難解決。解決該問題的一種方式是：根據一或多個將傳統的 LDAP 物件和屬性（例如）映射至任意抽象層定義和屬性的邏輯綱要，視需要將身份資料集合到邏輯儲存區中（實作為目錄），並組合來源資料中的邏輯身份。如此，身份資料就會變得高度複合而動態。變更身份的定義不需要變更 LDAP 綱要。您可以隨意重新定義身份物件，以適應特定應用程式或特定應用程式之特定使用者的需要。

此整體方法經常又稱為資料抽象，即視需要以所需形式具體化身份。

身份資料的抽象具有許多優點：

- ◆ 可以避免對 LDAP 目錄綱要進行有潛在風險的破壞性變更
- ◆ 抽象技術無侵入性，無需變更已連接系統
- ◆ 資料之間可以建立新的關係
- ◆ 可隨時變更或延伸抽象層定義
- ◆ 視需要，物件屬性的數目可多可少
- ◆ 可以將不相關 LDAP 物件類別的屬性合併到一個抽象層定義中
- ◆ 可以使用任意名稱進行屬性命名（無需使用 LDAP 名稱）
- ◆ 精細的存取控制規則仍然適用（使用者只能看到有權查看的資料）
- ◆ 可針對新物件類型（或屬性組合）執行複雜搜尋，在純 LDAP 環境中可能就無法實作此功能

Identity Manager 運用抽象概念以達成這所有的甚至更多的目標。

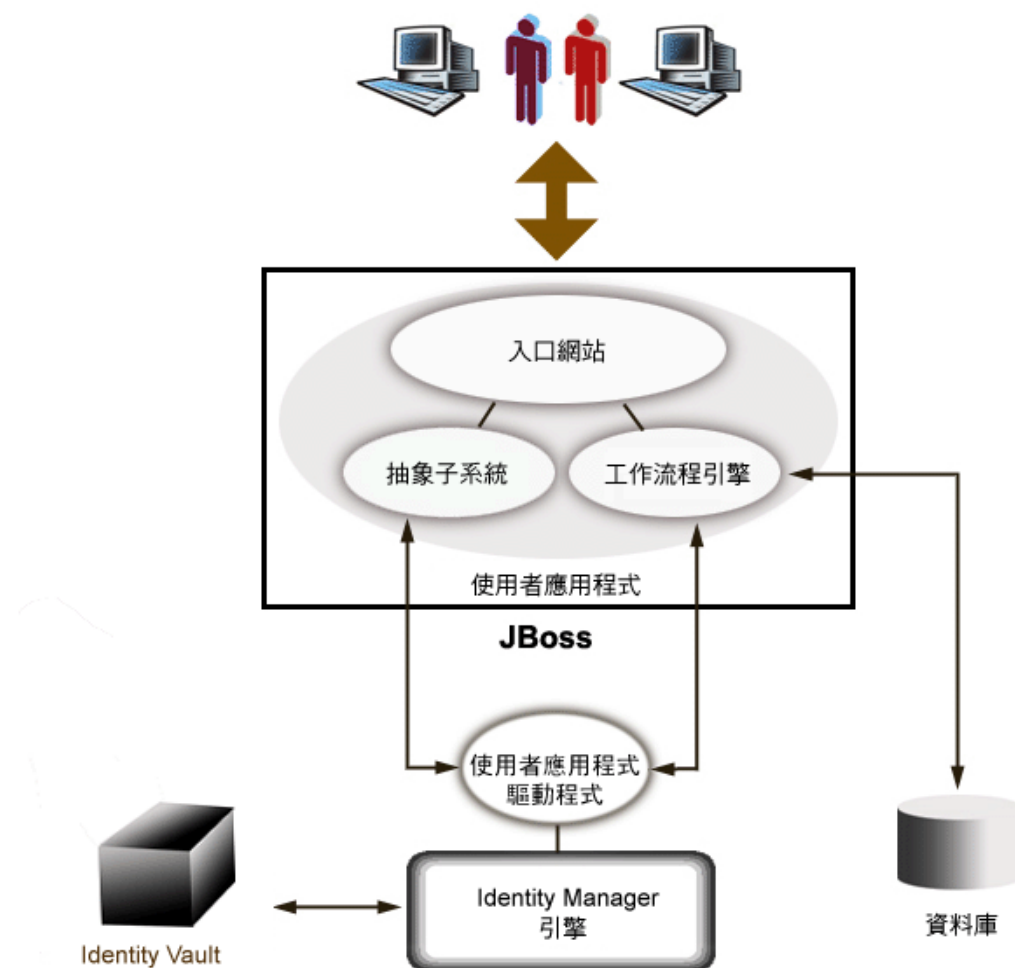
1.3 高層級結構綜覽

Identity Manager 使用者應用程式依賴於許多共同執行的獨立元件。下表說明了核心元件及其基本職責。

元件	描述
身份儲存區 (eDirectory 8.7.3 或 8.8)	使用者資料 (和其他身份資料) 與 IDM 驅動程式集和驅動程式，以及各種抽象層成品和工作流程成品 (如果已安裝「提供模組」的話) 的儲存機制。
Identity Manager 引擎	這是 Identity Manager 執行時期架構，它會監看 eDirectory (和已連接系統) 中的事件，強制執行規則並向身份儲存區往返輪遞資料。
使用者應用程式驅動程式	「使用者應用程式驅動程式」會與使用者應用程式通訊，以讓後者在抽象層定義變更時，重新整理其快取。若已安裝「提供模組」，還可設定「使用者應用程式驅動程式」的組態，以讓身份儲存區中的事件觸發工作流程。它還會將授權資訊傳遞回身份儲存區，以便在工作流程完成時，備有已授予 (或未授予) 授權的記錄。
使用者應用程式：Web UI	使用者應用程式的 Web UI 是基於瀏覽器的 Java 應用程式，其中會插入 JSR 168 相容入口網站應用程式。
使用者應用程式：抽象層	抽象層會將表示層邏輯與身份儲存區相隔離，因此身份資料的所有申請都必須經過抽象層。入口網站應用程式碼無法取得對身份資訊的直接存取權。所有申請都經過抽象層，且受限於其條件約束 (例如，存取控制)。
使用者應用程式：工作流程引擎 (僅適用於「提供模組」)	「工作流程引擎」是一組 Java 可執行檔，負責管理和執行管理員定義之工作流程中的步驟。
JBoss 應用程式伺服器	開放原始碼的 JBoss 應用程式伺服器會提供使用者應用程式、抽象層和「工作流程引擎」執行的執行時期架構。
資料庫 (預設為 MySQL)	資料庫 (如需受支援資料庫的清單，請參閱《安裝指南》) 會代表使用者應用程式儲存特定種類的組態資訊，並儲存工作流程狀態 (如果已安裝「提供模組」的話)。

元件	描述
編輯器服務驅動程式	「編輯器」服務驅動程式是「使用者應用程式驅動程式」的一部份，可自行設定組態為藉由引發工作流程來回應身份儲存區事件。
Novell Audit	Novell Audit 是一種獨立記錄伺服器，可以保留各種類型的資料 (如工作流程步驟產生的資料)。如需相關資訊，請參閱本書稍後的設定記錄一章。

就資訊流程而言，上面提及的元件會以下圖中所描述的方式在邏輯上進行連結。實際上，個別元件可能 (且在大多數情況下) 位於多部機器上。例如，雖然身份儲存區 (及其主要管理工具 iManager) 將會並列排置在代管 Identity Manager 引擎的機器上，但是通常會在另一台機器 (或已叢集的機器群組) 上代管 JBoss (及使用者應用程式)。同樣地，出於效能和安全性與災難復原的考量，資料庫 (MySQL) 通常位於其獨自的機器上。



1.3.1 身份儲存區

身份儲存區用於儲存各種身份資料和抽象層定義。因此，會使用 eDirectory 例項 (在 Windows、Solaris 或 Linux 上執行)。藉由使用 eDirectory，Identity Manager 可以強化已經充份證實可做極大調整之具有分割和複製功能的企業類別 LDAPv3 目錄，以及靈活的 Web 型

態管理和組態設定工具 (iManager)，該工具會提供 Identity Manager 與 eDirectory 本身之間的全方位管理整合點。

1.3.2 JBoss

使用者應用程式封裝為「Java Web 應用程式歸檔」或 WAR 檔案。將 WAR 部署至 JBoss，JBoss 是常見的開放原始碼 Java 應用程式伺服器（它使用 Tomcat 作為其伺服器常式引擎；未顯示於圖中）。使用 JBoss 作為執行環境會有很多優點，其中包含：

- ◆ 可隨意使用原始碼。
- ◆ 從 4.0.3 版開始，JBoss 可以叢集化。
- ◆ JBoss 與 J2EE 完全相容，這表示任何 J2EE 應用程式都可以在上面執行。您可以在執行使用者應用程式的同一 JBoss 例項上，代管其他應用程式（例如，「Web 服務」）。
- ◆ JBoss 支援標準的 JAAS 和 JACC Java 安全性和授權服務（使用者應用程式依賴於該服務存取身份儲存區）。
- ◆ JBoss 在許多不同的平台上執行，包含 Windows 和 Linux 的常用版本。

針對不同的考量，使用者應用程式 WAR 會包含使用者應用程式的可執行程式碼，而該使用者應用程式是使用模型檢視控制器 (Model-View-Controller, MVC) 架構所建立的。在使用者應用程式中，使用者可見的介面會做為模組化入口網站應用程式來執行。其中還有個別用於檢視組織圖、進行搜尋、檢視使用者詳細資料、重設密碼等的入口網站應用程式。

如需將 Web 應用程式部署到 JBoss 之各方面的相關資訊，請參閱位於 <http://www.jboss.org/products/jbossas/docs> (<http://www.jboss.org/products/jbossas/docs>) 的 JBoss 文件。

1.3.3 資料庫

使用者應用程式依賴於資料庫（預設為 MySQL，如需受支援資料庫的清單，請參閱《安裝指南》）儲存數種資訊：

- ◆ 使用者應用程式組態資料：例如，網頁定義、入口網站應用程式例項註冊和優先值。
- ◆ 如果已安裝「提供模組」，則會在資料庫中保留工作流程狀態資訊（實際的工作流程定義儲存在身份儲存區中）。
- ◆ Novell Audit 記錄

1.3.4 Identity Manager 引擎

Identity Manager 產品由執行時期引擎、驅動程式和規則組成。Identity Manager 引擎會回應身份儲存區中的事件，並管理與儲存區之間資料的流動和轉換。驅動程式物件會封裝可執行的程式碼和成品（如規則文件），該程式碼和成品是設計用來針對特殊已連接系統提供特定的資料處理行為。Identity Manager 使用者應用程式是已連接系統。身份儲存區、使用者應用程式的抽象層和「工作流程引擎」之間的通訊會透過「使用者應用程式驅動程式」（請參閱下文）進行。

因為使用者應用程式依賴於各種目錄物件來儲存抽象層成品，所以需要延伸 eDirectory 綱要，來容納使用者應用程式所需的自定 LDAP 物件和屬性。綱要的延伸是做為 Identity Manager 安裝程序的一部份而自動發生。不過，在安裝和啟用「使用者應用程式驅動程式」之前，不會填入具有預設值的自定物件和屬性。

1.3.5 使用者應用程式驅動程式

「使用者應用程式驅動程式」是使用者應用程式的重要啓用部份。「使用者應用程式驅動程式」的其中一個職責是，當身份儲存區中的重要資料值變更時，通知抽象層，以便抽象層可更新其快取。

如果已安裝「提供模組」，則可以設定「使用者應用程式驅動程式」的組態，以自動開始工作流程，回應身份儲存區中屬性值的變更。

「使用者應用程式驅動程式」不僅是執行時期元件，而且是目錄物件（構成使用者應用程式的執行時期成品）的儲存包裝函式。與「使用者應用程式驅動程式」相關聯之目錄成品的典型表示如下所示。



附註：所顯示的名稱代表 LDAP 公用名稱 (cn) 值。各種物件類別的實際綱要命名會在其他部份進行討論。

這些成品類別在下面有更詳細的討論。

驅動程式集物件

每個 Identity Manager 安裝都會要求將驅動程式分組成驅動程式集。一次只能有一個使用中的驅動程式集（在指定的目錄伺服器上）。該驅動程式集內的驅動程式可以個別開關，而不會影響整個驅動程式集。「使用者應用程式驅動程式」（像任何其他 IDM 驅動程式一樣）必須存在於驅動程式集內。使用者應用程式不會自動建立驅動程式集；您必須提前建立一個驅動程式集，然後在其中建立「使用者應用程式驅動程式」。

使用者應用程式驅動程式

「使用者應用程式驅動程式」物件（可指定任意名稱）是各種成品的容器。就像所有 Identity Manager 驅動程式一樣，「使用者應用程式驅動程式」會實作「發行者」與「訂閱者」通道物件和規則。雖然「發行者」通道可供自定使用，但是使用者應用程式不會使用該通道。

App Config 物件

AppConfig 物件是各種使用者應用程式組態物件的容器：

RequestDefs

這是「提供申請定義」的容器，「提供申請定義」是使用者應用程式執行時期可用之管理員設定組態的申請定義（如果「提供模組」存在的話）。此處儲存的定義（做為 XML）代表申請的類別，具有適當權限的一般使用者可以透過使用者應用程式例項化該申請。RequestDef 將 WorkflowDef（如下）與 ResourceDef 相關聯。

WorkflowDefs

「工作流程」物件的容器，包含設計階段描述與任何範本或未使用的流程。

ResourceDefs

「提供資源」定義的容器，包含設計階段描述與任何範本或未使用的目標。

ServiceDefs

「服務定義」物件的容器，會包裝由「工作流程」呼叫的「Web 服務」。

DirectoryModel

抽象層中繼層級物件 (ChoiceDefs、EntityDefs、RelationshipDefs)，代表「身份入口網站應用程式」可公開之目錄的不同類型內容（某些可由使用者定義，其他則由管理員設定）。

AppDefs

用於啓始化執行時期環境之組態物件（如快取組態資訊和電子郵件通知內容）的容器。

ProxyDefs

代理定義的容器。

DelegateeDefs

委託定義的容器。

1.3.6 目錄抽象層

入口網站應用程式透過查詢目錄抽象層來取得其身份資料，該目錄抽象層是將身份資料存取的詳細資料與用戶端程序相隔離的程式碼層。例如，當入口網站應用程式需要對身份資料執行搜尋時，抽象層就會代表入口網站應用程式，針對身份儲存區中的目標容器執行適當的 LDAP 查詢。任何入口網站應用程式都不會直接在身份儲存區中進行查詢。

抽象層也是一種程式碼層，透過這個程式碼層，可以建立或變更由管理員或其他合法的系統使用者所指定的抽象層定義。若要進行此類變更，系統專家會使用 Designer 應用程式的目錄抽象層編輯器，本指南稍後的第 4 章「設定目錄抽象層的組態」，第 65 頁會有說明。

在執行時期，抽象層會快取從身份儲存區取得的各種組態和實體定義資料。管理員可以很詳細地管理使用者應用程式所維護的各種快取。如需快取和快取管理的其他資訊，請參閱第 13 章「快取組態」，第 197 頁。

1.3.7 工作流程引擎

工作流程引擎 (可供「提供模組」使用) 是一組執行時期類別，負責執行由程序定義 (在例項化工作流程時建立的執行時期成品) 指定的工作流程步驟，和追蹤資料庫 (如 MySQL 或 Oracle) 中保留的狀態資訊，請參閱上面「[資料庫](#)」，第 21 頁。

您可以在本指南稍後第 21 章「[工作流程提供簡介](#)」，第 279 頁一章中，找到「[工作流程系統](#)」的其他詳細資料，包含如何建立工作流程。

1.3.8 使用者介面

Identity Manager 使用者介面由與 JSR168 相容之入口網站應用程式 (如果是「提供模組」，還會有部份 Java Server Pages) 的集合構成，這些入口網站應用程式在 JBoss 上的 Java Web 應用程式內執行。入口網站應用程式架構可提供高階的模組化、內容自訂和對頁面外觀的使用者控制。使用者應用程式架構會提供各種容器服務。它會管理視窗狀態、入口網站應用程式優先設定、持續性、快取、主題化、記錄等，並會做為安全性閘道管理員。而執行使用者應用程式的應用程式伺服器又會將各種服務做為整體提供給應用程式，如透過叢集的延展性、透過 JDBC 的資料庫存取，以及對基於證書之安全性的支援。

此架構所承擔的高階封裝會對 Identity Manager 使用者應用程式提供強固而安全的展示層環境。而且還會保證對使用者介面各方面的高階管理控制。

如需使用者介面各部份之管理的相關資訊，請參閱本指南「[管理使用者應用程式](#)」，第 113 頁下的各章。

1.4 設計和組態設定工具

您可以使用 Identity Manager Designer 工具 (該工具基於 Eclipse Rich Client Platform) 或透過 iManager 外掛程式，自定或自行設定各種 Identity Manager 使用者應用程式功能的組態。

下表說明可用的工具及其用法。

工具	目的
Designer for Identity Manager	Identity Manager 的一般組態設定工具，可讓開發人員、顧問或系統管理員詳細變更驅動程式集、驅動程式、規則定義和其他成品的組態。
Designer 的目錄抽象層編輯器外掛程式	可讓您定義自定物件和關係，並變更抽象層의各種組態設定。請參閱本指南稍後第 4 章「 設定目錄抽象層的組態 」，第 65 頁。
提供申請組態外掛程式	允許定義和設定可用的提供申請類型 (在 iManager 中)
提供資源編輯器 (即將提供)	允許建立和設定資源 (代表回應工作流程而授予之資源的物件) 的 Designer 外掛程式
工作流程定義編輯器 (即將提供)	Designer 的圖形化工作流程定義外掛程式
工作流程電子郵件範本編輯器	允許管理員新增、刪除和編輯電子郵件範本的 iManager 外掛程式。工作流程系統可使用這些範本來通知使用者工作流程事件。

工具	目的
Ireport.exe (記錄報告工具) 和「iManager 稽核與記錄」功能	許多預先定義的記錄報告 (隨附於 Identity Manager) 可以使用 Crystal Reports (.rpt) 格式, 以過濾記錄到 Novell Audit 資料庫的資料。 Ireport.exe 記錄報告工具 (僅限 Windows) 是可以產生報告的一種方式。您也可以使用其他方法來建立報告, 如需詳細資料, 請參閱第 5 章「設定記錄」, 第 105 頁。

系統設計專家通常會從使用目錄抽象層編輯器 (在 Designer for Identity Manager 中) 開始, 來設定使用者應用程式的自定抽象層定義。然後, 抽象層 (以及使用者介面的使用者) 即可使用這些物件。在這些物件的定義和使用中, 可以運用精細的存取控制設定, 以便管理員和一般使用者可以僅查看和處理其具有適當權限的那些物件 (和物件的屬性)。

如果已安裝「提供模組」, 則系統設計專家或管理員會使用 iManager 中的「提供申請組態」精靈, 來定義使用者應用程式之使用者可用的提供資源和工作流程。同時, 管理員還會使用電子郵件範本編輯器功能 (在 iManager 中), 來定義工作流程將傳送之任何電子郵件通知的本文內容。如需此工具的相關資訊, 請參閱第 23 章「管理提供工作流程」, 第 313 頁。

設定抽象層、提供申請定義、稽核要求和電子郵件範本的組態之後, 管理員通常會使用管理功能 (在第 10 章「入口網站組態」, 第 181 頁中說明), 執行影響使用者應用程式的各種組態操作 (包括安全性、快取和其他功能)。最後, 管理員會使用在本指南之「第四部份」各章中所說明的介面, 視需要設定個別入口網站應用程式的組態。

附註：下一章會更詳細地說明部份上述任務, 因此, 實作生產環境之前請先參閱該章節的內容。

1.5 使用案例

Identity Manager 使用者應用程式中可以使用的功能有很多。下列範例會讓您初步瞭解如何將使用者應用程式用於解決實際問題。

1.5.1 案例 A：使用者搜尋組織中其他人的資訊

常用案例是員工想要找出組織中其他人的資訊。例如：

- ◆ 取得同事的全名、聯絡資訊
- ◆ 尋找某地區具有特定技能集的所有人員
- ◆ 判定特定人員的管理員是誰

透過「目錄搜尋」介面, 可以很輕鬆地執行這些操作 (包含基於複雜查詢的更多進階搜尋)。通常, 一般使用者會登入使用者應用程式, 並將「身份自助服務」索引標籤置於前面 (如果它尚未處於最前面的話), 然後按一下左側導覽連結欄中的「目錄搜尋」連結。

在下面的螢幕中，登入的使用者已設定進階搜尋，來尋找其部門以「銷售」為開頭，且其「頭銜」包含「管理員」的任何使用者。



此搜尋完成時，會提供類似於下列的結果螢幕：



請注意底部的按鈕列，其可讓使用者「儲存」此特定進階查詢、「修訂」查詢、重新開始新搜尋等。也請注意所找到之人員清單上方的索引標籤。該人員目前是依「身份」列示，但是您也可以使用適當的索引標籤，依「位置」或「組織」檢視。

1.5.2 案例 B：管理員建立新的使用者

假設公司某部門僱用新的實習生、約聘人員或其他非公司員工（可能只是在公司停留一段時間）。新人需要加入系統，以便其可以取得受到適當限制的資源集（且可以透過上述「使用者搜尋」找到該人員）。因為此人不是正式員工，所以他不是公司正常「人力資源部門」系統的一部份。但是，需要以安全的方式管理該人員的身份（和對資源的存取）。

您做為該部門的經理，會被授予可以將使用者輸入系統的權限。若要執行此動作，您要登入系統，並找到頁面左側導覽連結欄中的「建立使用者或群組」連結（請參閱下文）：



附註：除非登入的使用者具有適當的權限，否則不會顯示此連結。

按一下此連結之後，您會看到一個螢幕，詢問您是否要建立新的「群組」、「任務群組」或「使用者」（如下所示）。



選取「使用者」並按一下「繼續」之後，下一個精靈面板可讓您輸入此使用者的個人資料：

下一個螢幕可讓您指定該新「使用者」的密碼：

最後一個螢幕會顯示程序的最終結果。

在此範例中，新輸入的人員會成為具有正常「使用者」所有權限的「使用者」。但是也可能會使用目錄抽象層編輯器定義像是「實習生」這樣的物件，讓其具有嚴格適用於該物件類型的唯一屬性和權限。此時，「實習生」會與「群組」、「任務群組」和「使用者」一起，顯示為先前挑選清單中的選項。

1.5.3 案例 C：使用者提供

常見狀況包括：員工需要取得的資源（無論是辦公室設備、公司信用卡，還是對資料庫的存取）需要其他人員核准。這稱為提供申請。在 Identity Manager 中，如果已安裝並設定「提供模組」的組態，則可透過工作流程處理此類申請。

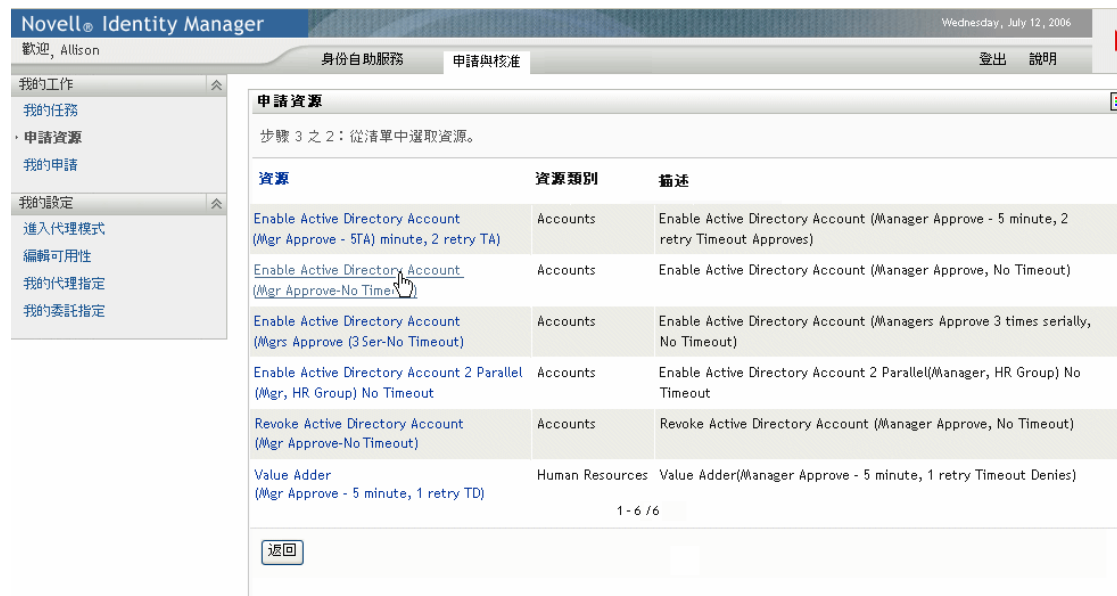
附註：與先前的範例不同，此範例需要安裝並設定「提供模組」的組態。

使用者首先要登入使用者應用程式，以進入其著陸頁面。在該頁面頂端，使用者按一下「申請與核准」索引標籤，然後在左側的導覽框架中尋找「申請資源」連結。當您按一下「申請資源」連結時，使用者應用程式會顯示啓始申請表單。



「資源類別」下拉式功能表可能包含任何數目的資源類型，包括具任意名稱的授權（如需授權及其建立方式的相關資訊，請參閱 Identity Manager 的主要「管理指南」）。若要檢視所有可用的提供資源（換言之，此特定使用者以其現有權限可申請的任何項目），您只需要選取「全部」，如圖所示。

如果使用者按一下「繼續」，則下一個螢幕會顯示允許此使用者存取的所有提供申請類型。



在此範例中，使用者想要申請 Active Directory 帳戶，這需要管理員核准。只要按一下適當的連結並填寫簡易表單，即可開始相關聯的工作流程，且該人員的管理員會收到與管理員需要執行之任務相關的電子郵件通知。接著，管理員可以登入其「申請與核准」頁面，並找到其任務清單中等待核准或否決的員工申請（如果管理員在度假，則其指定的代理會收到通知，並可登入和執行管理員通常執行的動作）。同時，瀏覽器螢幕會變為顯示摘要頁面，確認工作流程申請已順利提交。

授予公司目錄中的帳戶 (如此處所示) 是授權申請的範例。您可以在 Identity Manager 使用者應用程式中設定多種授權申請類型的組態，還可以建立多種工作流程 (單一或多位管理員核准、循序流程或平行流程、有無逾時等)。在任何情況下，您都可以使用精細的存取控制來管理工作流程和其他資訊的可見度。

在本指南的最後一章中，可以找到這些功能的更多資訊 (這些章節中的資訊主要針對管理員。在《Identity Manager 使用者應用程式使用者指南》中，有這些功能用法的更詳細說明)。

1.6 接下來的步驟

如果您已經準備好要瞭解設計生產環境的更多資訊，請前往下一章 (第 2 章「設計生產環境」, 第 31 頁)。否則，您可能想要直接跳至本書的最後幾章，以取得下列資訊：

若要瞭解使用者應用程式之記錄和稽核功能的詳細資訊，請參閱第 5 章「設定記錄」, 第 105 頁。

若要瞭解自定使用者介面外觀和操作的詳細資訊，請參閱第 8 章「主題組態」, 第 155 頁。

若要瞭解透過使用者應用程式的管理介面 (相對於 iManager) 管理之安全性的詳細資訊，請參閱第 11 章「安全性組態」, 第 187 頁。

若要瞭解使用者應用程式之快取管理功能的詳細資訊，請參閱第 13 章「快取組態」, 第 197 頁。

若要瞭解密碼管理功能的詳細資訊，請參閱第 19 章「密碼管理入口網站應用程式參考資訊」, 第 253 頁。

若要瞭解入口網站應用程式管理的詳細資訊，請參閱第 9 章「入口網站應用程式管理」, 第 161 頁。

若要瞭解入口網站資料輸入和輸出的詳細資訊，請參閱第 14 章「用於輸出和輸入入口網站資料的工具」, 第 205 頁。

若要瞭解組織圖功能的詳細資訊，請參閱第 18 章「組織圖入口網站應用程式參考資訊」, 第 239 頁。

若要瞭解目錄搜尋功能的詳細資訊，請參閱第 20 章「搜尋清單入口網站應用程式參考資訊」, 第 265 頁。

若要瞭解新物件建立 (「建立」入口網站應用程式) 選項及其管理方式的詳細資訊，請參閱第 16 章「建立入口網站應用程式參考資訊」, 第 219 頁。

若要瞭解工作流程設定和管理的詳細資訊，請參閱第 21 章「工作流程提供簡介」, 第 279 頁，以及第 22 章「設定提供申請定義的組態」, 第 291 頁和第 23 章「管理提供工作流程」, 第 313 頁。

設計生產環境

本章討論與設定生產環境相關的問題。它提供從沙箱 / 測試 (或其他生產前) 環境轉換為生產環境時，一些所需考量事項的指引。

本章根據下列主要小節來組織：

- ◆ 「拓樸」，第 31 頁
- ◆ 「安全性」，第 33 頁
- ◆ 「效能調整」，第 35 頁
- ◆ 「叢集」，第 38 頁

2.1 拓樸

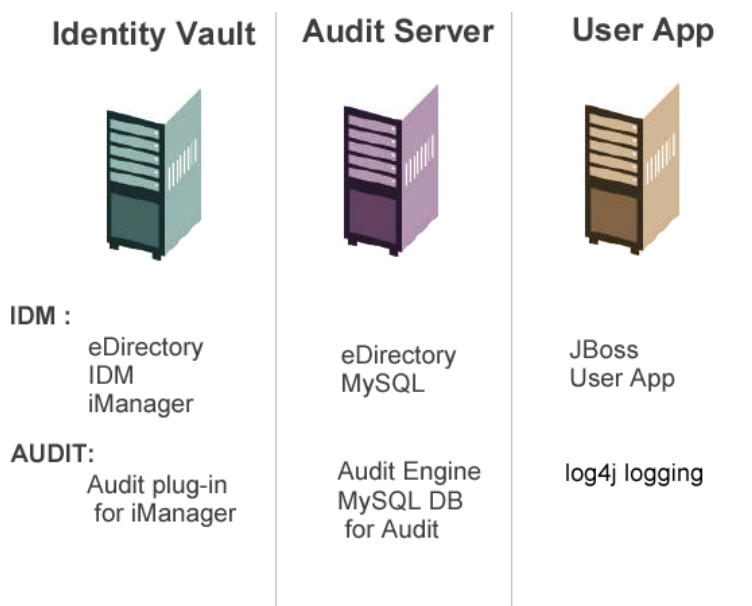
每個主要子系統的例項數目，以及該例項連接方式的數目可能會相當多。並不是每種可能的配置都受支援。不僅是瞭解可能性，而且瞭解選擇某些組態而不選擇其他組態的原因也很重要。

2.1.1 最少的設計

使用者應用程式的最簡單邏輯組態是全部安裝，包括一個身份儲存區網路樹、一個 Identity Manager 引擎和驅動程式例項，以及一個執行使用者應用程式單一例項的 JBoss 例項。就實體實作而言，理論上您可以在一個系統中執行所有動作。但是由於各種原因 (其中主要是安全性、可維護性和效能)，實際上並不能這樣做。在決定實際安裝所需的機器數目時，您 (至少) 需要考慮下列各項：

- ◆ *Novell Audit* 伺服器：負責在執行時期，從使用者應用程式環境擷取事件資訊 (可能還有許多其他資訊)。同時，它還可做為公司中其他應用程式的持續性儲存區。由於各種原因，您可能不想將 Identity Manager 系統的其他主要部份 (例如，JBoss 或身份儲存區)，與 Audit 伺服器置於相同的機器上。
- ◆ 身份儲存區：這是需要良好效能和延展性的大流量元件。您很可能要考慮將身份儲存區置於專屬的機器上。也就是說，您可能不想讓其他高流量系統 (如部署使用者應用程式的 JBoss) 與身份儲存區在相同的機器上執行。
- ◆ 資料庫：如果此 MySQL 例項 (或其他受支援的資料庫) 也是您的 *Novell Audit* 資料庫，則它可能在專屬的機器上。請考量使用者應用程式是以下列方式使用此項目：
 - ◆ 做為入口網站組態資料的持續性儲存區
 - ◆ 做為進行中工作流程之狀態資訊的持續性儲存區 (如果已安裝「提供模組」的話)
 - ◆ 選擇性地做為 *Novell Audit* 的記錄儲存庫。
- ◆ *JBoss*：由於效能和容量的原因，您可能要在專屬的機器上執行此項目。

基於這些考量因素，建議可採用下列最少的三機組態：



2.1.2 高可用性設計

本章稍後的一節會詳細討論高可用性 / 容量的叢集。現在，您應該瞭解：

- ◆ **Identity Manager** 透過多節點安裝和共享儲存區機制，支援身份儲存區、引擎和驅動程式的高可用性，這在主要《Identity Manager 管理指南》的「高可用性」一章中有所說明。詳細說明使用 SUSE Linux 設定此類系統的文章位於：
<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm> (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm>)
- ◆ 透過 **JBoss** 叢集可以取得使用者應用程式的高可用性。您可以設定 **JBoss** 叢集，讓每個節點執行一個使用者應用程式例項。例項都彼此相等（對等）。不過，例項之間沒有會期複製。每個例項都對其自己的工作單元負責，且不會完成在同級節點上啟動的會期。
- ◆ 不支援自動容錯移轉（原因如上所述）。但是，如果在線上的新節點與關閉的節點具有相同的工作流程引擎 ID，則已岔斷的工作流程可以在遺失叢集節點之後繼續（在此情況下，新的工作流程引擎啟動之後，已岔斷的工作流程會自動繼續）。

同樣，如需這些問題的詳細討論資訊，請參閱（下面的）「叢集」，第 38 頁。

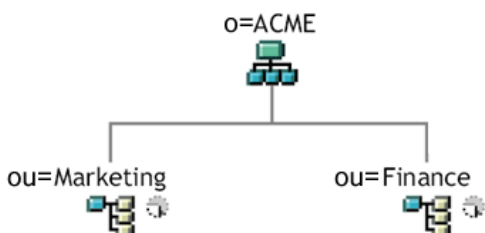
2.1.3 設計條件約束

一般而言，要瞭解之兩個最重要的結構條件約束如下：

- ◆ 任何使用者應用程式例項都不能為多個使用者容器提供服務（搜尋 / 查詢、新增使用者等）。同時，使用者容器與應用程式建立關聯之後，該關聯就會永久存在。
- ◆ 「使用者應用程式驅動程式」不能與多個使用者應用程式建立關聯，除非使用者應用程式安裝於相同 **JBoss** 叢集的同級節點上。換句話說，不支援驅動程式至使用者應用程式的一對多映射。

第一個約束條件在使用者應用程式設計中強制執行高階封裝。

假設您的組織結構如下：



在使用者應用程式的安裝期間，會要求您指定在身份儲存區中安裝所需要的高階層級使用者容器。在此情況下，您可以指定 *ou=Marketing,o=ACME* 或 *ou=Finance,o=ACME*。但不能同時指定兩者。所有使用者應用程式搜尋和查詢（以及管理員登入）都在指定的容器範圍內。

附註：在理論上，您可以指定 *o=ACME* 的範圍，以包含 Marketing 和 Finance。但是在較大的組織中，具有很多潛在的 *ou* 容器（而非僅與 Marketing 和 Finance 相關的兩個容器），這可能就不太實用。

當然，您也可以建立使用者應用程式的兩個獨立安裝（一般不會共享資源），分別用於 Marketing 和 Finance。每個安裝都有其自己的資料庫、適當設定組態的「使用者應用程式驅動程式」，並會分別管理每個使用者應用程式（可能具有唯一的主题）。

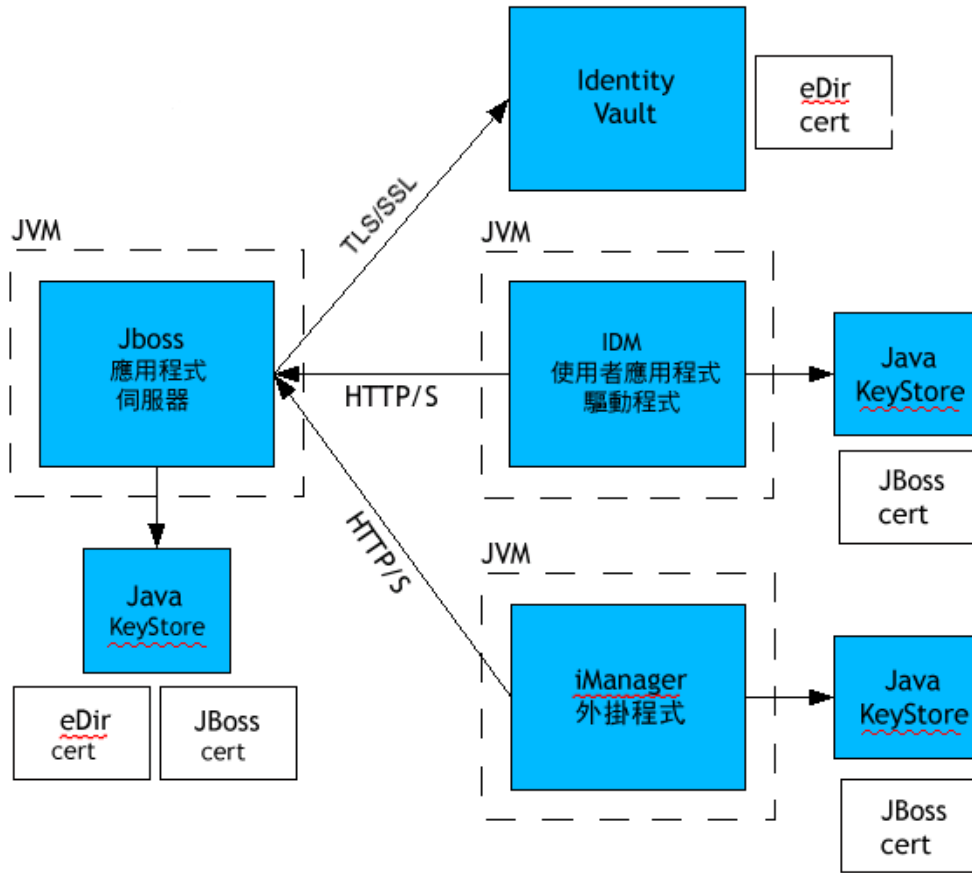
如果您確實需要將 Marketing 和 Finance 置於一個使用者應用程式安裝的相同範圍內，則可能需要考量兩種策略。一種是在階層中兩個同級節點上方插入新的容器物件（例如，*ou=MarketingAndFinance*），然後指向新容器做為範圍根部。另一種策略是建立會結合原始 ACME 網路樹之所需部份的過濾後複製本（特殊類型的 eDirectory 網路樹），並將使用者應用程式指向複製本的根容器（如需過濾後複製本的相關資訊，請參閱《Novell eDirectory 管理指南》）。

如果您對特定系統配置有任何問題，請與 Novell 代表聯絡，以取得協助或建議。

2.2 安全性

從生產前的作業移至生產過程通常涉及加強系統的安全性。在沙箱測試中，您可能已使用一般 HTTP 將使用者應用程式驅動程式連接至 JBoss，或者已使用自行簽署的證書（做為暫時措施），以進行驅動程式 / 應用程式伺服器通訊。另一方面，在生產過程中，您可能使用安全連接，根據公司的 Verisign（或其他託管提供者）證書進行伺服器驗證。

通常，在 Identity Manager 使用者應用程式環境中，許多地方都會用到 X.509 證書，如下圖所示。



使用者應用程式與身份儲存區之間的所有通訊都是安全的，且預設使用「輸送層安全性」。在安裝時，會自動將身份儲存區 (eDirectory) 證書安裝至 JBoss KeyStore 中。除非另外指定，否則使用者應用程式安裝程式會將 eDirectory 證書的副本置於 JRE 的預設 *cacerts* 儲存區中。

如圖所示，為了保障通訊的安全，伺服器證書需要置於數個位置。視您是要在圖中的不同 *JBoss cert* 方塊使用自行簽署的證書，還是要 (改爲) 使用託管證書權限 (Certificate authority, CA) 所發出的證書 (如 Verisign)，可能需要採取不同的步驟。

自行簽署的證書

如果您是使用來自知名託管發證者 (例如，Verisign) 的證書，則無需特殊的組態設定步驟。但是，如果您想要建立並使用自行簽署的證書，則需要執行下列步驟：

- 1 使用類似於下列內容的指令行語法，以自行簽署的證書建立 KeyStore：

```
keytool -genkey -alias tomcat -keyalg RSA -storepass changeit -
keystore jboss.jks -dname
"cn=JBoss,ou=exteNd,o=Novell,l=Waltham,s=MA,c=US" -keypass
changeit
```

請注意，您正在建立檔案 *jboss.jks* 和證書。

2 將 KeyStore 檔案 (jboss.jks) 複製到 JBoss 使用者應用程式目錄，例如：

```
cp jboss.jks ~/jboss-4.0.2/server/spitfire/conf
```

在 JBoss 中開啓 SSL

若要在 JBoss 中啓用保全插槽層 (Secure Socket Layer, SSL)，請尋找 `[IDM]/jboss/server/IDM/deploy/` 下的 `jbossweb-tomcat55.sar` 檔案。您可以在其中找到 `server.xml`，並在文字編輯器中開啓該檔案。新增類似於下列內容的區段或取消其註解，以啓用保全插槽層 (SSL)：

```
<Connector port="8443" address="{jboss.bind.address}"
maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
emptySessionPath="true" scheme="https" secure="true"
clientAuth="false" keystoreFile="{jboss.server.home.dir}/spitfire/
conf/jboss.jks" keystorePass="changeit" sslProtocol = "TLS" />
```

開啓 SOAP 安全性

在 `IDM.war` 中，找到 `web.xml` 檔案並在文字編輯器中開啓它。在檔案的底部，取消下列區段的註解：

```
<security-constraint> <web-resource-collection> <web-resource-
name>IDMProv</web-resource-name> <url-pattern>/*</url-pattern> <http-
method>POST</http-method> <http-method>GET</http-method>
<description>IDM Provisioning Edition</description> </web-resource-
collection> <user-data-constraint> <transport-guarantee>CONFIDENTIAL</
transport guarantee> </user-data-constraint> </security-constraint>
```

儲存檔案和歸檔。重新啓動 JBoss。

2.2.1 相互驗證

Identity Manager 使用者應用程式支援傳統的伺服器驗證案例 (通常用於 Web 上安全網頁的 https 會期中)，但是不支援內建的證書式雙向驗證。不過，您可以使用 Novell iChain 取得該功能。因此，如果 (例如) 您的組織需要讓使用者透過使用者證書 (而不是透過密碼) 登入，則您可藉由將 iChain 新增至環境來達成。

如需相關資訊，請洽詢 Novell 代表。

2.3 效能調整

效能調整是一個複雜的問題。Identity Manager 使用者應用程式依賴於具有許多互動的不同技術。無法預料所有可能造成效能不佳的單一組態案例或使用者互動案例。不過，某些子系統是可增進效能的最佳作法。對這些問題的具體討論如下。

2.3.1 記錄

使用者應用程式允許透過 Novell Audit 和開放原始碼 Apache `log4j` 架構進行記錄。預設會關閉透過 Novell Audit 的記錄。不過，預設會啓用透過 `log4j` 的檔案和主控台記錄。

附註：在本指南稍後的第 5 章「設定記錄」，第 105 頁和第 12 章「記錄組態」，第 191 頁中，您可以瞭解到可記錄的事件類型，以及如何啓用或停用記錄。

log4j 組態設定位於 `$IDMINSTALL/jboss/server/IDMProv/conf/` 下稱爲 *log4j.xml* 的檔案中。您可以在此檔案的底部附近，找到下列項目：

```
<root>      <priority value="INFO" />      <appender-ref ref="CONSOLE" />
>      <appender-ref ref="FILE" /> </root>
```

對 `root` 指定值可確保任何未明確指定層級的記錄附加程式會繼承 `root` 層級 (在此情況下爲 `INFO`)。例如，在預設狀態下，`FILE` 附加程式並沒有指定的限定值層級，所以它會採用根部的限定值層級。

log4j 可能使用的記錄層級是 `DEBUG`、`INFO`、`WARN`、`ERROR` 和 `FATAL` (如 *org.apache.log4j.Level* 類別中所定義)。不注意適當使用這些設定會導致效能的嚴重損失。

您最好只在除錯特定問題時才使用 `INFO` 或 `DEBUG`。

除非 (如上所述) 您正在除錯某些項目，否則未設定層級限定值之根部中包含的任何附加程式都應將限定值設爲 `ERROR`、`WARN` 或 `FATAL`。

與訊息的冗長相比，在 *log4j* 中主控台和檔案記錄涉及同步寫入對高記錄層級的效能影響較大。您可以使用 `AsyncAppender` 類別，但使用它並不能保證較好的效能。在 <http://logging.apache.org/log4j/docs/api-1.2.8/org/apache/log4j/performance/Logging.html> 中，會說明這些問題 (這些是眾所周知的問題，是 *Apache log4j* 問題，而不是 *Identity Manager* 問題)。

使用者應用程式之記錄設定檔案中的預設值 `INFO` (如上所述) 適用於很多環境，但是因爲效能十分重要，所以您應考慮將上述 *log4j.xml* 項目變更爲：

```
<root> <priority value="ERROR"/> <appender-ref ref="FILE"/> </root>
```

換句話說，移除 `CONSOLE` 並將記錄層級設爲 `ERROR`。針對完整測試 / 除錯的生產設定，不需要在 `INFO` 層級記錄，也不需要啓用 `CONSOLE` 記錄。關閉這些項目可以明顯改進效能。

如需 *log4j* 的相關資訊，請參閱位於 <http://logging.apache.org/log4j/docs> 的文件。

如需搭配使用 *Novell Audit* 和 *Identity Manager* 的相關資訊，請參閱《*Novell Identity Manager* 管理指南》。

2.3.2 Identity Vault

`LDAP` 查詢可能會在大量使用的目錄伺服器環境中造成瓶頸。爲了保持大量物件的高效能，*Novell eDirectory* (做爲 *Identity Manager* 中身份儲存區的基礎) 經常記錄所申請的資訊，並將其儲存在索引中。針對其屬性已編製索引的物件執行複雜查詢時，查詢的傳回速度會更快。

依預設 *eDirectory* 會隨附下列已編製索引的屬性：

```
Aliased Object Name cn dc Equivalent to Me extensionInfo Given Name
GUID ldapAttributeList ldapClassList Member NLS: Common Certificate
```

Obituary Reference Revision Surname uniqueID uniqueID_SS

當您安裝 Identity Manager 時，預設目錄綱要會延伸為具有與使用者應用程式相關的新物件類別類型和新屬性。在預設狀態下，不會對使用者應用程式特定的屬性編製索引。為了取得更好的效能，您可以為上述的某些屬性（或許還有一些其他傳統的 LDAP 屬性）編製索引，尤其是您的使用者容器包含的物件超過 5000 個時。

一般而言，僅對已知為經常查詢的那些屬性編製索引（不同的生產環境中屬性也有所不同）。確切瞭解經常使用之屬性的唯一方式是：在執行時期收集述詞統計資料（不過，收集程序本身會降低效能）。

在《eDirectory 管理指南》中會詳細討論收集述詞統計資料的程序。還會詳細討論編製索引的相關資訊。通常，您將需要進行下列幾項操作：

- ◆ 使用 Console One 啟用相關屬性的述詞統計資料收集
- ◆ 將系統置於載入狀態下
- ◆ 停用統計資料收集並分析結果
- ◆ 為每種可能從中獲益的屬性編製索引

如果您已經知道要為哪些屬性編製索引，則不需要使用 Console One。您可以透過「eDirectory 維護」>「索引」，在 iManager 中建立和管理索引。例如，如果您瞭解組織圖的使用者很可能會根據 *isManager* 屬性執行查詢，則可以嘗試為該屬性編製索引，以查看是否會增強效能。

附註：建議的最佳作法是至少建立 *manager* 和 *isManager* 屬性的索引。

如需屬性索引建立和效能的進一步討論，請參閱 Peter Kuo 和 Jim Henderson 所著之《Novell eDirectory 疑難排解指南》(QUE Books, ISBN 0-7897-3146-0) 中的「調整 eDirectory」一章。

另請參閱主要《eDirectory 管理指南》中的「維護 Novell eDirectory」一章（具有效能調整指導）。

2.3.3 JVM

配置至 Java 虛擬機器的堆積記憶體數會影響效能。如果您指定的最小或最大記憶體值過低或過高（過高表示多於機器的實體記憶體），則您可能會經歷過量的頁檔案交換。

您可以在文字編輯器中編輯 [IDM]/jboss/bin/ 下的 run.conf 或 run.bat 檔案（前者針對 Linux，後者針對 Windows），以設定 JBoss 伺服器的最大 Java 虛擬機器 (Java Virtual Machine, JVM) 大小。將 "-Xmx" 從 128m 增加為 512m，或儘可能更高。可能需要一些試驗來決定特定環境的最佳設定。

附註：您可以在 <http://wiki.jboss.org/wiki/Wiki.jsp?page=JBossASTuningSliming> (<http://wiki.jboss.org/wiki/Wiki.jsp?page=JBossASTuningSliming>) 中找到 JBoss 和 Tomcat 效能調整秘訣。

2.3.4 會期逾時值

您可以在 *IDM.war* 歸檔的 *web.xml* 檔案中變更會期逾時 (在伺服器導致會期逾時警告對話方塊出現之前，使用者可讓頁面在其 Web 瀏覽器中處於無人管理狀態的時間)。您應該調整此值，以符合要執行應用程式的伺服器和環境。通常，建議會期逾時越小越好。如果業務需求可以容忍 5 分鐘的會期逾時，則伺服器會以較逾時值為 10 分鐘時早兩倍的時間釋放未使用的資源。這可讓 Web 應用程式的效能和可調整性更好。

調節會期逾時時，請考慮下列各項：

- ◆ 如果很多使用者在較短的時間內登入，則較長的會期逾時可能會導致 JBoss 伺服器執行的記憶體不足。具有過多開放會期的任何應用程式伺服器都會發生這樣的情況。
- ◆ 當使用者登入使用者應用程式時，會為使用者建立 LDAP 連接並結合至會期。因此，開啓的會期越多，保留的 LDAP 連接數就越大。會期逾時越長，保持連接開啓的時間就越長。LDAP 伺服器的開放連接過多 (即使它們閒置) 會導致系統效能降低。
- ◆ 如果伺服器開始經歷 `OutOfMemoryErrors`，且針對伺服器和環境，已將 Java 虛擬機器 (JVM) 的堆積和垃圾回收調整參數做了最佳調整，則應考慮降低會期逾時。

若要調節會期逾時值，您需要開啓 *IDM.war* 歸檔，在其中找到 *web.xml* 檔案，並編輯該檔案的下列部份 (特別是此處顯示為 20 的數值表示 20 分鐘，它是預設值)：

```
<session-config>           <session-timeout>20</session-timeout> </session-  
config>
```

然後，您需要儲存檔案和歸檔，然後重新啓動伺服器。

附註：最好由具備 Java Web 應用程式開發和部署經驗的人員來手動編輯 Web 歸檔檔案。

2.4 叢集

在叢集環境中使用使用者應用程式時，您必須考量下列三項：

- ◆ JBoss 叢集組態 (請參閱「[叢集 JBoss](#)」，第 38 頁)
- ◆ 使用者應用程式快取組態 (請參閱「[設定使用者應用程式叢集群組快取組態](#)」，第 43 頁)
- ◆ 工作流程引擎組態 (請參閱「[設定叢集的工作流程](#)」，第 43 頁)

2.4.1 叢集 JBoss

叢集是提供一組服務的應用程式伺服器節點集合。叢集的目的是增加應用程式的效能和可靠度。通常，叢集會為企業應用程式提供三個主要優點：

- ◆ 高可用性
- ◆ 延展性 (更多功能)
- ◆ 載入平衡

高可用性表示應用程式是可靠的，且在部署的大部份時間內都可用。因為在所有節點上執行的都是相同的應用程式，所以叢集可以提供高可用性。如果一個節點失敗，則應用程式仍會在其他節點上執行。當 Identity Manager 使用者應用程式以叢集的方式執行時，會從較高的

可用性中獲益。不過，Identity Manager 使用者應用程式不支援 HTTP 會期複製。這表示如果某節點上的會期在進行中，而該節點失敗，則會期資訊將遺失。

載入平衡可以在叢集的成員之間分配工作量。載入平衡的目的是增進效能。您可以藉由各種方式 (例如，DNS 遞迴、硬體載入平衡)，以達到載入平衡。如需各種載入平衡方法的討論，請參閱 <http://www.onjava.com/pub/a/onjava/2001/09/26/load.html> (<http://www.onjava.com/pub/a/onjava/2001/09/26/load.html>)。無論選定方法為何，您都需要在叢集組態中包含載入平衡。

JBoss 叢集群組

JBoss 叢集基於名為 JGroups 的通訊模組。JGroups 與 JBoss 一起安裝 (沒有 JBoss 也可以使用它)。JGroups 提供群組之間的通訊，它們會共享公用名稱、多路廣播位址和多路廣播連接埠。

當您安裝叢集的 JBoss 伺服器時，JBoss 會定義兩個不同的 JGroups 群組，以用於管理叢集。其中一個稱為 *DefaultPartition*，並在 `/deploy/cluster-service.xml` 中定義。JBoss 會使用此叢集群組來提供核心叢集服務。JBoss 還會定義名為 *Tomcat-Cluster* 的第二個叢集群組。此叢集群組在 `/deploy/tc-cluster-service.xml` 中定義。此叢集群組為在 JBoss 內執行的 Tomcat 伺服器提供會期複製。

Identity Manager 使用者應用程式使用第三個叢集群組。此叢集群組使用通用唯一識別碼 (Universally Unique Identifier, UUID) 名稱，以將與使用者可能新增至其伺服器之其他叢集群組的衝突風險降至最低。叢集群組預設命名為 `c373e901aba5e8ee9966444553544200`。不使用 JBoss 服務檔案設定此叢集的組態。而是組態設定位於目錄中，且可利用使用者應用程式管理功能來設定組態。如果您熟悉 JGroups 和 JBoss 叢集，則可以使用此介面來調整使用者應用程式叢集組態。僅當重新啟動伺服器節點時，該節點的叢集組態變更才會生效。

使用者應用程式叢集群組僅用於調整叢集環境中的使用者應用程式快取。它獨立於兩個 JBoss 叢集群組，且不會以任何方式與它們互動。在預設狀態下，使用者應用程式叢集群組和兩個 JBoss 群組使用不同的群組名稱、多路廣播位址和多路廣播連接埠，所以不需要重新設定組態。

使用者應用程式叢集群組設定由任何共享目錄組態的 Identity Manager 3 應用程式共享。使用者應用程式管理介面中本地設定選項的目的是：可讓管理員從叢集移除節點，或在叢集中變更伺服器的成員資格。例如，您可以在全域停用叢集，然後針對共享目錄組態的伺服器子集，於本地啟用該叢集。

應用程式 Farming

藉由將應用程式 EAR、WAR 或 JAR 複製到一個叢集之 JBoss 例項的 `farm` 目錄，JBoss 可讓您在叢集中進行快速部署。當叢集在執行中時，在一個機器上快速部署會導致在叢集內的所有例項上自動部署元件。

不建議在 JBoss Application Server (4.0.2) 版次 (在撰寫此文件時，該版次包含於使用者應用程式安裝程式中) 中使用此種形式的應用程式部署，因為使用它會發生無法解決的問題。不過，我們已提供您必須執行的基本步驟 (請參閱「[使用 JBoss Farming 將使用者應用程式部署到叢集](#)」，第 42 頁)，以使用 JBoss Farming 技術順利部署使用者應用程式，因為我們預期在本文件出版之後會對此技術有所改進。

MySQL 資料庫

使用者應用程式安裝程式會安裝 MySQL 資料庫管理員，並建立與使用者應用程式搭配使用的資料庫，或使用現有的 Oracle、Microsoft SQL Server 或 MySQL 資料庫。資料庫負責資料

保存。JBoss 叢集中的所有節點都必須存取相同的資料庫例項。使用者應用程式會使用標準 JDBC 呼叫來存取和更新資料庫。使用者應用程式會使用結合至 JNDI 網路樹的 JDBC 資料來源，以開啓資料庫的連接。如果您利用使用者應用程式安裝程式來建立 JBoss 叢集，則會為您安裝資料來源。如果您選擇手動設定 JBoss 叢集，則需要將資料來源檔案 (IDM-ds.xml) 複製到叢集中所有節點上的部署目錄。同時，如果您是在使用 MySQL，則需要將位於 JBoss /server/IDM/lib 目錄的 MySQL JDBC 驅動程式 (*mysql-connector-java-3.1.10-utf8-clob-fix-bin.jar*)，複製到 JBoss server/IDM/lib 目錄。

記錄

若要啓用叢集的記錄，您需要編輯位於 JBoss 伺服器組態之 \conf 目錄 (例如，\server\IDM\conf) 上的 log4j.xml 組態檔案，並取消類似於如下內容之位於底部區段的註解：

```
<!-- Clustering logging --> - <!-- Uncomment the following to redirect
the org.jgroups and org.jboss.ha categories to a cluster.log file.
<appender name="CLUSTER"
class="org.jboss.logging.appender.RollingFileAppender"> <errorHandler
class="org.jboss.logging.util.OnlyOnceErrorHandler"/> <param
name="File" value="{jboss.server.home.dir}/log cluster.log"/> <param
name="Append" value="false"/> <param name="MaxFileSize" value="500KB"/
> <param name="MaxBackupIndex" value="1"/><layout
class="org.apache.log4j.PatternLayout"> <param
name="ConversionPattern" value="%d %-5p [%c] %m%n"/> </layout> </
appender> <category name="org.jgroups"> <priority value="DEBUG" />
<appender-ref ref="CLUSTER"/> </category> <category
name="org.jboss.ha"> <priority value="DEBUG" /> <appender-ref
ref="CLUSTER"/> </category> -->
```

您可以在 JBoss 伺服器組態的 log 目錄 (例如，\server\IDM\log) 中找到 *cluster.log* 檔案。

2.4.2 安裝使用者應用程式至 JBoss 叢集

將使用者應用程式安裝至叢集的建議方法是使用使用者應用程式安裝程式，將使用者應用程式安裝至叢集中的每個節點。雖然不建議使用 JBoss Farming 將使用者應用程式部署到叢集，但是我們已包含可遵循的程序做為替代方法。

在叢集中的每個節點上使用使用者應用程式安裝程式

JBoss 隨附三種不同的可用伺服器組態：*minimal*、*default* 和 *all*。僅在 *all* 組態中啓用叢集。/deploy 資料夾中的 *cluster-service.xml* 檔案描述預設叢集分割區的組態。當您安裝使用者應用

程式並指出要在叢集中安裝的安裝程式時，安裝程式會建立 *all* 組態的副本，將副本命名為 *IDM* (在預設狀態下，安裝程式可讓您變更名稱)，並在此組態中安裝使用者應用程式。

若要利用使用者應用程式「安裝程式」，在叢集中的每個節點上安裝使用者應用程式，請執行下列動作：

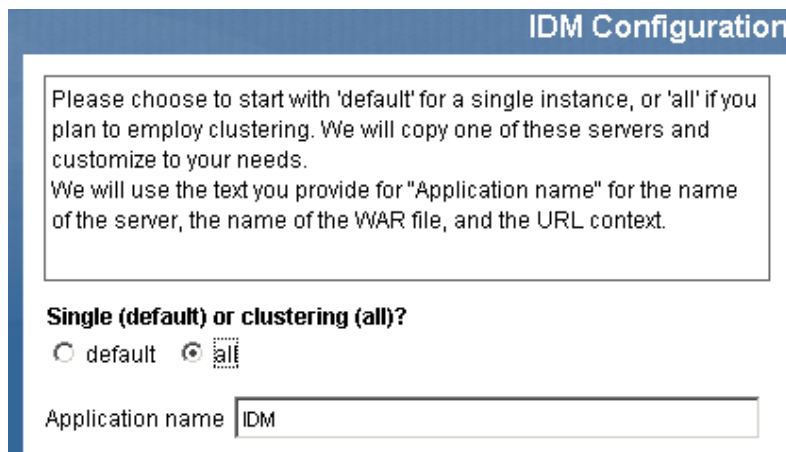
- 1 在第一個 JBoss 節點上，執行使用者應用程式 (MySQL、JBoss 和使用者應用程式) 的完整安裝。如需使用使用者應用程式安裝程式的相關資訊，請參閱《*Identity Manager 3* 安裝指南》。
 - ◆ 如果您是使用 MySQL 做為使用者應用程式的資料庫，則使用者應用程式安裝程式會建立 MySQL 的新安裝。請記下您指定的 MySQL 根部使用者密碼；當在叢集中的其餘節點上安裝使用者應用程式時，您將需要此資訊。
 - ◆ 在安裝程式的 *IDM* 組態螢幕中，選取「叢集 (全部)」選項。
 - ◆ 選取適合您環境的其他安裝選項。
- 2 如果 MySQL 尚未執行，請使用位於 */IDM/mysql* 目錄的 *start-mysql.bat* 檔案，啟動 MySQL。

附註：在 Linux 上，下列外圍程序指令將會協助您判斷 MySQL 精靈是否正在執行：

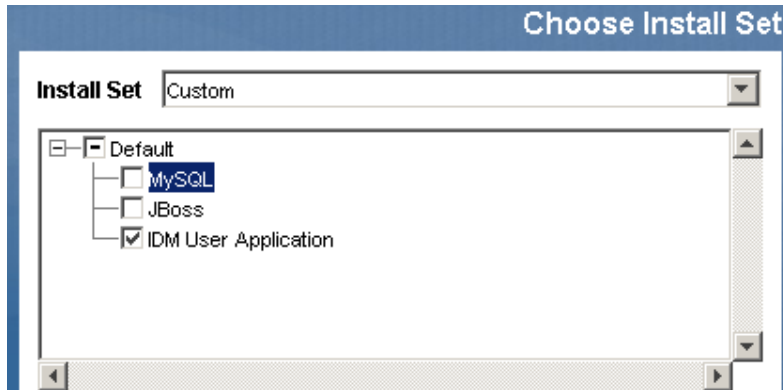
```
ps -A | grep mysqld
```

如果此指令傳回以 *mysqld* 結束的數行，則精靈正在執行。

- 3 使用位於 *IDM* 目錄的 *start-jboss.bat* (Windows) 或 *start-jboss.sh* (Linux) 檔案，啟動 JBoss 和使用者應用程式。



- 4 在 JBoss 叢集中的每個其他節點上，執行使用者應用程式的自定安裝。
 - ◆ 只選取要安裝的使用者應用程式：



- ◆ 指定要安裝使用者應用程式之資料庫的伺服器 IP 位址或主機名稱。
 - ◆ 指定使用者應用程式資料庫的資料庫使用者名稱和密碼。如果您是使用 MySQL，則使用者名稱是 root，而密碼是您在安裝程序之 **步驟 1** 中指定的內容。
 - ◆ 在安裝程式的 *IDM* 組態螢幕中，選取「叢集 (全部)」選項。
 - ◆ 選取適合您環境的其他安裝選項。
- 5 使用位於 *IDM* 目錄的 *start-jboss.bat* (Windows) 或 *start-jboss.sh* (Linux) 檔案，啟動 JBoss 叢集中的每個節點。

使用 JBoss Farming 將使用者應用程式部署到叢集

請勿將 JBoss Farming 與 JBoss 4.0.2 版或先前版本搭配使用，因為您可能會遇到問題 (請參閱 <http://jira.jboss.com/jira/browse/JBAS-1899> (<http://jira.jboss.com/jira/browse/JBAS-1899>))。建議您使用使用者應用程式安裝程式，在叢集中的每個節點上安裝使用者應用程式 (請參閱本章中「**在叢集中的每個節點上使用使用者應用程式安裝程式**」，第 40 頁)。不過，如果您想要使用 Farming，以將使用者應用程式部署至使用 JBoss 4.0.3 或更新版本的 JBoss 叢集，請遵循下面的步驟。

附註：這些步驟適用於要獨立以實驗方法使用 JBoss 4.0.3 的客戶。支援的正式版本是 4.0.2。

若要使用 JBoss Farming 將使用者應用程式部署至叢集，請執行下列動作：

- 1 選取要安裝的使用者應用程式和 MySQL (如果您是在使用 MySQL；否則，僅安裝使用者應用程式)，以在其中一個 JBoss 叢集節點上執行使用者應用程式的自定安裝。您可以在執行節點中所有叢集的同時，執行安裝，但是安裝使用者應用程式的節點應該是要啟動之叢集中的第一個節點。
- 2 將位於 */server/IDM/lib* 目錄的 JDBC 驅動程式檔案 (例如，如果您是使用 MySQL，則 JDBC 驅動程式是 *mysql-connector-java-3.1.10-utf8-clob-fix-bin.jar*)，複製到叢集中每個節點所對應的目錄中。
- 3 將 *cacerts* 檔案從與使用者應用程式一起安裝之 JRE 的 */lib/security* 目錄，複製到叢集中每個節點的 *JRE /lib/security* 目錄。
- 4 將 *IDM.war* 檔案和 *IDM-ds.xml* 資料來源檔案從伺服器組態目錄中的 */deploy* 目錄，移至伺服器組態目錄中的 */farm* 目錄。您必須確實移動檔案本身。請勿在 */deploy* 目錄中保留原始檔案。
- 5 啟動使用者應用程式的資料庫 (如果您是在使用所提供的 MySQL，請使用位於 */IDM/mysql* 目錄的 *start-mysql.bat* 檔案來啟動 MySQL)。

- 6 在安裝使用者應用程式和使用使用者應用程式資料庫的節點上，使用位於 *IDM* 目錄中的 *start-jboss.bat* (Windows) 或 *start-jboss.sh* (Linux)，啟動 JBoss 和使用使用者應用程式。
- 7 啟動叢集中的其他節點。

2.4.3 設定使用者應用程式叢集群組快取組態

熟悉 JGroups 和 JBoss 叢集的使用者可以使用使用者應用程式管理使用者介面，修改叢集群組快取組態 (請參閱「叢集的快取設定」，第 203 頁)。僅當重新啟動伺服器節點時，該節點的叢集組態變更才會生效。

2.4.4 設定叢集的工作流程

工作流程引擎叢集的運作與使用者應用程式快取架構無關。您必須執行數個步驟，以確保工作流程引擎在叢集環境中正確運作。

- ◆ 叢集中的所有伺服器都需要指向相同的資料庫。如果您使用建議的方法將使用者應用程式安裝至叢集 (請參閱「在叢集中的每個節點上使用使用者應用程式安裝程式」，第 40 頁)，則可藉由在安裝程序期間指定安裝使用者應用程式之資料庫的伺服器 IP 位址或主機名稱，來完成此步驟。如果您使用 Farming 將使用者應用程式部署至叢集節點 (請參閱「使用 JBoss Farming 將使用者應用程式部署到叢集」，第 42 頁)，則可將資料來源檔案 (*IDM-ds.xml*) 從 */deploy* 目錄移至首次安裝使用者應用程式之節點上的 */farm* 目錄，來完成此步驟。這樣會將資料來源部署至叢集中的所有節點。
- ◆ 叢集中的每個伺服器都需要使用唯一的引擎 ID 啟動。您可以藉由在伺服器啟動時，設定 *com.novell.afw.wf.engine-id* 系統屬性來完成此動作。例如，如果您要啟動 JBoss 並將引擎 ID *ENGINE1* 指定給該伺服器的工作流程引擎，則可以使用下列指令：

```
run.sh -Dcom.novell.afw.wf.engine-id=ENGINE1 (Linux)
```

```
run.bat -Dcom.novell.afw.wf.engine-id=ENGINE1 (Windows)
```

由在特定伺服器上執行的工作流程引擎啟動之後，工作流程程序例項就只能在該伺服器上執行和完成。這樣可確保工作流程程序安全地執行。不過，它不提供程序例項容錯移轉支援。如果叢集中的伺服器當機，則程序例項只有在重新啟動相同 ID 的引擎之後，才會重新啟動。

如果由於嚴重的硬體或軟體失敗而無法重新啟動伺服器電腦，則您可以使用在無法恢復之機器上使用的相同工作流程引擎 ID，在新電腦上啟動應用程式伺服器。因為引擎 ID 是邏輯名稱，而不是執行引擎之實體電腦的直接映射，所以在新電腦上會順利完成已岔斷的程序例項。

程序例項由啟動程序的引擎所擁有。不過，使用者可以登入叢集中的任何使用者應用程式，以檢視程序詳細資料、收回程序，或完成所指定的任務。收回的程序或在不擁有程序之引擎上完成的任務會進入待處理的狀態，一旦擁有它們的引擎發現它們，就會繼續執行。

設定使用者應用程式環境的組態



下列各章會告知您如何設定不同方面的 Identity Manager 使用者應用程式環境組態，以符合您組織的需要。

- ◆ 第 3 章 「設定使用者應用程式驅動程式的組態」, 第 47 頁
- ◆ 第 4 章 「設定目錄抽象層的組態」, 第 65 頁
- ◆ 第 5 章 「設定記錄」, 第 105 頁

設定使用者應用程式驅動程式的組態

3.1 關於使用者應用程式驅動程式

使用者應用程式驅動程式負責啟動提供工作流程，並通知使用者應用程式在 Identity Vault 中的變更 (例如，當您使用 Designer for Identity Manager 對目錄抽象層進行變更時)。在此驅動程式中只使用「訂閱者」通道。驅動程式將訊息從 Identity Vault 處理到應用程式伺服器上所執行的使用者應用程式。因為使用者應用程式中發生的事件會報告回 Identity Vault，所以這些事件不會透過使用者應用程式驅動程式的「發行者」通道流動。

當啟動應用程式伺服器時，驅動程式會使用應用程式伺服器建立會期。驅動程式會將訊息傳送至應用程式伺服器上執行的使用者應用程式 (例如，「取回一組新的虛擬目錄定義」)。

驅動程式的來源元件包含：

- ◆ ComposerDriverShim.jar – Composer 驅動程式 Shim。它安裝於 *lib* 目錄 `\Novell\NDS\lib` (Windows 中)，或 *classes* 目錄 `/usr/lib/dirxml/classes` (Linux 中)
- ◆ *srvprvUAD.jar* – 應用程式驅動程式 Shim。它安裝於 *lib* 目錄 `\Novell\NDS\lib` (Windows 中)，或 *classes* 目錄 `/usr/lib/dirxml/classes` (Linux 中)
- ◆ *UserApplicationDriver.xml* - 包含設定新驅動程式之預先組態設定資料的檔案。它安裝於 *DirXML.Drivers* 目錄 `\Tomcat\webapps\nps\DirXML.Drivers` (Windows 中) 或 `/usr/lib/dirxml/rules/DirXML.Drivers` (Linux 中)

在您安裝 Identity Manager 3 時，會安裝使用者應用程式驅動程式元件。您必須先將使用者應用程式驅動程式新增至新的或現有的驅動程式集，並啟用驅動程式，然後才能執行 Identity Manager 3 使用者應用程式。

視工作環境的不同，您可能需要稍微設定使用者應用程式驅動程式的組態，或者您可能要在驅動程式規則 (Policy) 中實作複雜的業務規則 (Rule) 集。使用者應用程式驅動程式與其他 Identity Manager 驅動程式提供同樣靈活的資料同步化機制。

本章描述如何建立、設定組態和啟動使用者應用程式驅動程式，以及如何設定驅動程式的組態，以根據 Identity Vault 中的事件自動觸發工作流程。它包含下列各節：

- ◆ 「[建立使用者應用程式驅動程式](#)」，第 47 頁
- ◆ 「[啟動使用者應用程式驅動程式](#)」，第 54 頁
- ◆ 「[設定工作流程以自動啟動](#)」，第 55 頁

3.2 建立使用者應用程式驅動程式

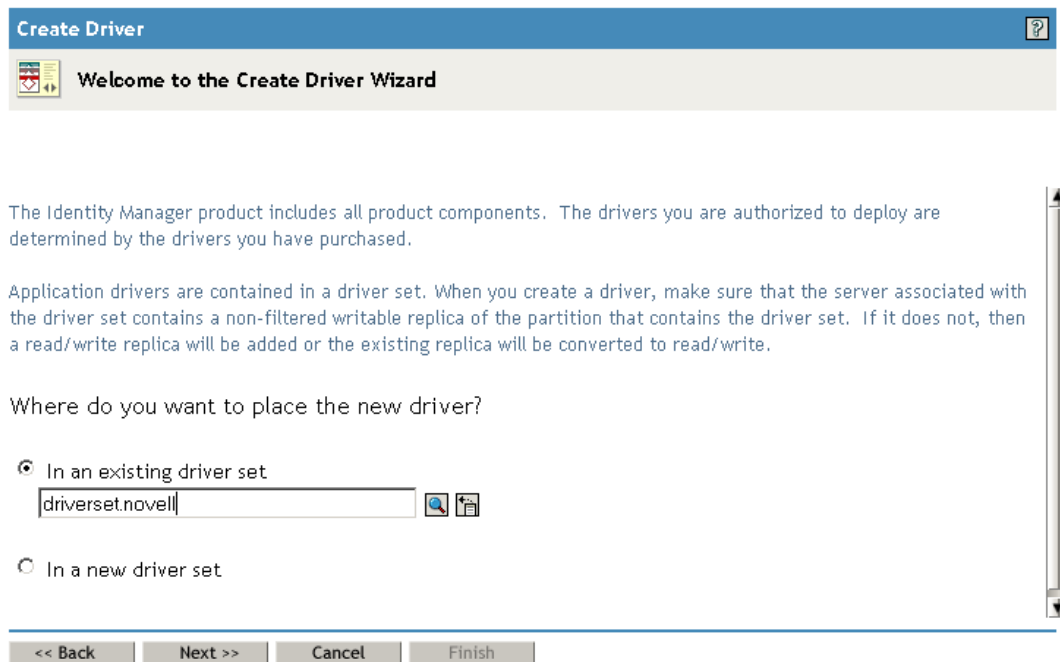
若要建立驅動程式，請執行下列動作：

- 1 登入管理 Identity Vault 之 iManager 的例項。

- 2 開啓 iManager 導覽框架中的「Identity Manager 公用程式」節點。



- 3 按一下「新驅動程式」。即會顯示「建立驅動程式精靈」：



下一步是選取要建立新驅動程式的位置。您可以在現有的驅動程式集中建立驅動程式，也可以建立新的驅動程式集。

- 4 如果您選取「在現有的驅動程式集中」，即會顯示一個精靈，您可用於瀏覽 Identity Vault 以尋找驅動程式集。選取現有的驅動程式集，然後選取「下一步」。

如果選取「在新的驅動程式集中」，即會顯示一個畫面，您可以在其中定義新驅動程式集的內容。指定驅動程式集的名稱、網路樹網路位置和伺服器，然後選取「下一步」。即會顯示「建立驅動程式精靈」中的下一個畫面：

Import or create a new Application Driver for this driver set.

Import a driver configuration from the server (.XML file)

Import a driver configuration from the client (.XML file)
File:

Create a new driver
Name:

- 5 按一下「從伺服器輸入驅動程式組態」選項，然後從 XML 檔案清單中選取「UserApplication.xml」。

Import or create a new Application Driver for this driver set.

Import a driver configuration from the server (.XML file)

Import a driver configuration from the client (.XML file)

Create a new driver

- MoveProxy.xml
- MTDAccess.xml
- MTDCellphone.xml
- MTDRoomNumber.xml
- MTDWelcome.xml
- Notes.xml
- NotesMoveSample.xml
- NotesReturnEmail.xml
- NT.xml
- PasswordSync1.xml
- PasswordSync2.xml
- PeopleSoft36.xml
- PeopleSoft50.xml
- RemedyARS.xml
- SAPHR.xml
- SAPUser.xml
- SIFAgent.xml
- SOAP-DSML.xml
- SOAP-SPML.xml
- UserApplication.xml

- 按「下一步」。「建立驅動程式精靈」會顯示可用於命名驅動程式和設定其組態的頁面：

UserApplication (Driver)

The driver writer requested that the following information be supplied in order to import this driver configuration file. An * indicates required information.

The name of the driver contained in the driver configuration file is "UserApplication". Enter the actual name you want to use for the driver.

Driver name: *	Existing drivers:
<input type="text" value="UserApplication"/>	<input type="text" value="<Select an existing driver to update>"/>

驅動程式的預設名稱是 UserApplication。您可以使用預設名稱，但是也可能想要為專案選擇更有意義的名稱。

- 如果願意，請在「驅動程式名稱」欄位中，輸入驅動程式的新名稱。
- 在「驗證 ID」欄位中，使用點格式 (例如，admin.orgunit.novell)，指定使用者應用程式管理員的 DN (如需使用者應用程式管理員的描述，請參閱「[使用者應用程式管理員](#)」，第 16 頁)。
- 在「應用程式密碼」和「重新輸入密碼」欄位中，指定在「驗證 ID」欄位中識別的使用者應用程式管理員密碼。
- 在「應用程式網路位置」欄位中，輸入安裝使用者應用程式時指定的應用程式名稱。預設名稱是 IDM。
- 在「主機」欄位中，指定執行使用者應用程式之應用程式伺服器的主機名稱或 IP 位址。
- 在「連接埠」欄位中，指定驅動程式用來與應用程式伺服器上執行之使用者應用程式通訊的連接埠 (例如，8080)。

- 13 按「下一步」。即會顯示一則訊息，指出正在輸入驅動程式組態，然後會顯示「建立驅動程式」精靈的下一頁：

UserApplication3 (驅動程式)

Novell 建議您在新建立的驅動程式上進行下列幾項操作：

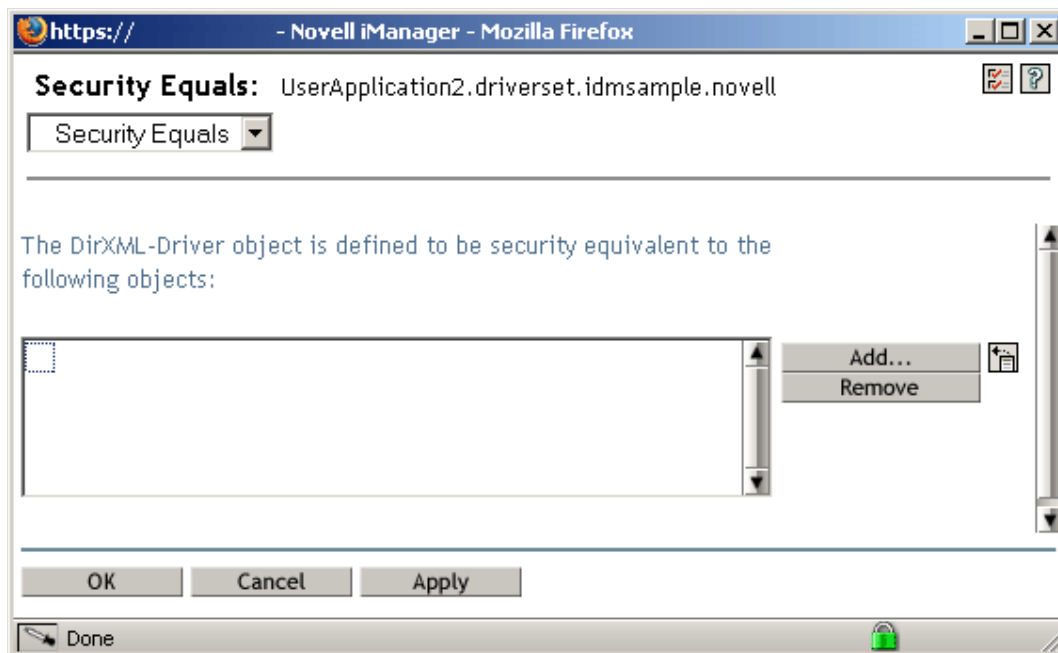
- 定義驅動程式的「安全性等值」。
- 識別所有代表「管理角色」的物件，並將它們自複寫中排除。

定義「安全性等值」

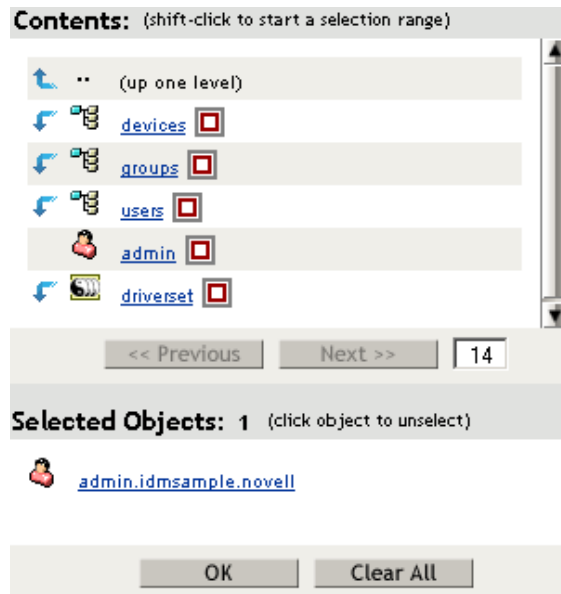
排除「管理角色」

必須授予驅動程式物件對其所讀取或寫入之任何物件具有足夠的 Identity Vault 權限。您可藉由將「安全性等值」授予驅動程式物件，以執行此動作。驅動程式必須擁有對使用者、郵局、資源和配送清單的「讀/寫」存取權限，以及對郵局容器的「建立」、「讀取」和「寫入」權限。通常應給予驅動程式與「管理員」相等的安全性。

- 14 按一下「定義安全性等值」。即會顯示新視窗：

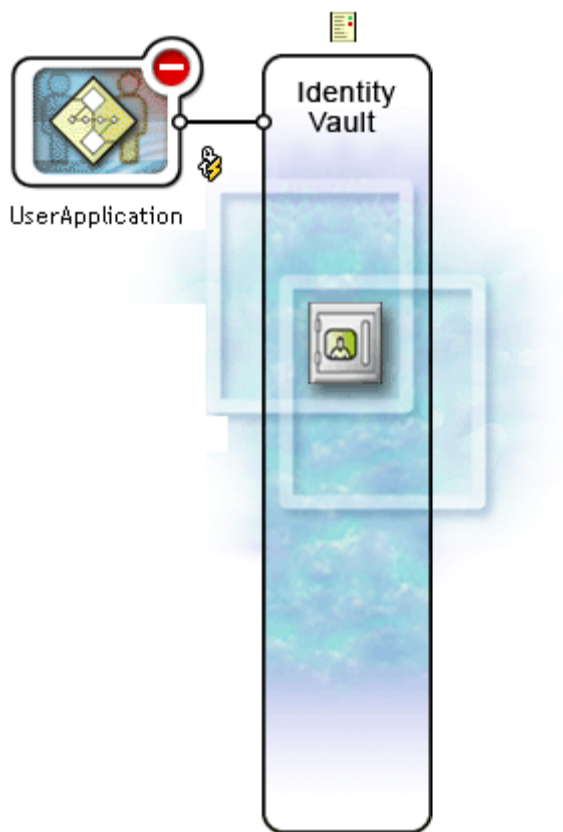


- 15 按一下「新增」。即會顯示一個視窗，您可在其中的網路樹中選取某一物件，該物件具有要指定給此驅動程式的適當權限層級（例如，管理員）：



- 16 從網路樹中，選取具有所需之 Identity Vault 權限層級的物件，然後按一下「確定」。您就會返回先前的視窗。
- 17 按一下「確定」。您就會返回「建立驅動程式」精靈。
- 18 按一下「排除管理角色」。即會顯示「排除使用者」視窗。如果在複製回此驅動程式所屬之網路樹的其他 Identity Vault 中，管理員密碼發生變更，則您可使用此功能，以避免將管理員鎖定在使用者應用程式驅動程式之外。
- 19 按一下「新增」。即會顯示一個視窗，您可使用它來瀏覽目錄樹，以找出應排除將他們的資料傳遞至驅動程式的使用者。因為在大多數情況下，最好不要在驅動程式連接中複製 ADMIN 物件的資料，所以您通常要排除這些物件。
- 20 選取要排除的管理角色，然後按一下「確定」。您就會返回先前的視窗。
- 21 按一下「確定」。您就會返回「建立驅動程式」精靈。
- 22 按「下一步」。即會顯示驅動程式摘要頁面。

23 按一下「完成概觀」。即會顯示 Identity Vault 中驅動程式的圖形化表示：



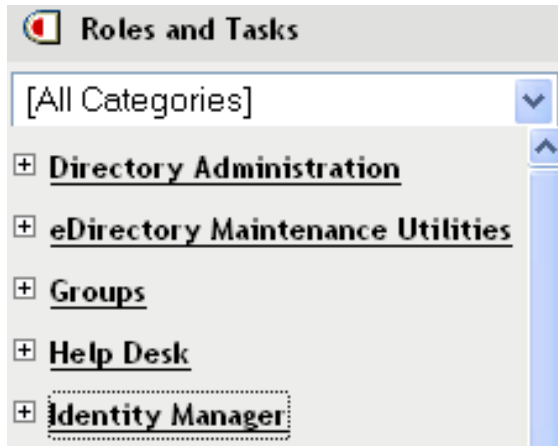
附註：您隨時可以使用 iManager 導覽網路樹中「*Identity Manager*」下的「*Identity Manager* 概觀」連結，再次檢視此畫面。

新的驅動程式會顯示為連接至 Identity Vault 幹線的大圖示。

3.3 啓動使用者應用程式驅動程式

若要啓動使用者應用程式驅動程式，請執行下列動作：

- 1 按一下 iManager 導覽網路樹中的「*Identity Manager*」連結，以查看 Identity Manager 類別中可用的指令：



- 2 在 iManager 導覽網路樹中的「*Identity Manager*」連結下，按一下「*Identity Manager* 概觀」連結。

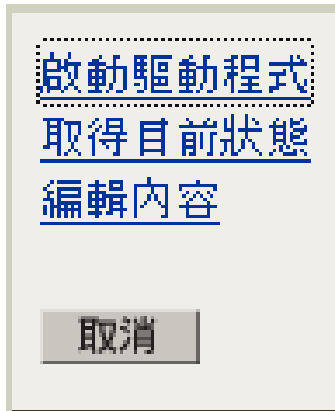


即會顯示一個精靈，您可使用它來瀏覽系統，以尋找包含要啓用之驅動程式的驅動程式集。

- 3 選取驅動程式集，然後按「下一步」。即會顯示「*Identity Manager* 概觀」頁面。
- 4 在驅動程式圖示的右上角按一下圓形的狀態指示器：



即會顯示一個功能表，它會列出啟動和停止驅動程式，以及編輯驅動程式內容的指令：



5 按一下「啟動驅動程式」。

3.4 設定工作流程以自動啟動

在安裝提供模組時，如果使用者藉由申請資源而啟動提供申請，則工作流程會自動啟動。此外，Identity Manager 使用者應用程式驅動程式會監聽 Identity Vault 中的事件，如果設定組態為執行此動作，則會啟動適當的提供工作流程以回應事件。例如，您可以設定使用者應用程式驅動程式的組態，在將使用者新增至 Identity Vault 時，自動啟動提供工作流程。您可以使用 Identity Manager 規則 (Policy) 和規則 (Rule) 來設定使用者應用程式驅動程式的組態，以自動啟動工作流程。

3.4.1 關於規則

您可以將過濾器與規則與使用者應用程式驅動程式搭配使用，使用方式與其他 Identity Manager 驅動程式搭配使用方式相同。當 Identity Vault 中發生事件時，Identity Manager 會建立描述該事件的 XML 文件。透過通道傳遞 XML 文件至已連接系統（在此情況下，已連接系統是使用者應用程式）。與驅動程式相關的過濾器和規則可讓您定義如何回應事件，以及如何如何在程序中將該 XML 文件轉換為已連接系統預期的格式。Identity Manager 提供數種規則（例如，「事件轉換」、「指令轉換」、「綱要映射」、「輸出轉換」），您可依指定順序套用，以轉換 XML 文件。在本節中，提供根據 Identity Vault 中事件啟動工作流程的範例。雖然任何規則都可用來觸發工作流程，但是此範例所示範的是最簡單且實用的方法。

當您建立使用者應用程式驅動程式時，會建立「事件轉換規則」以供驅動程式使用。「事件轉換規則」負責建立將由其餘「訂閱者」通道規則處理的 XML 文件。

附註：請勿變更在建立使用者應用程式驅動程式時，所建立的「事件轉換」規則。此規則的 DN 以 Manage.Modify.Subscriber 開頭。變更此規則可能會導致工作流程程序失敗。

還會建立空的「綱要映射規則」。您可以使用此規則做為開始點，以根據 Identity Vault 中的事件觸發工作流程。

3.4.2 設定工作流程以根據 Identity Vault 中的事件啟動

完成自動啟動工作流程的最簡單方法是使用「綱要映射規則編輯器」，且使用者應用程式驅動程式會提供空白規則讓您編輯。

使用「綱要映射規則編輯器」，將 Identity Vault 屬性 (包含 eDirectory *trigger* 屬性，在其變更時會啟動工作流程) 映射至目標工作流程的執行時期資料。執行時期資料由工作流程定義範本決定 (如需工作流程定義範本的相關資訊，請參閱第 22 章「設定提供申請定義的組態」, 第 291 頁)。工作流程需要有執行時期資料才能順利完成。建立工作流程後，會在 Identity Vault 中建立一些全域屬性，這些屬性可用於自定使用者應用程式驅動程式的行為。全域屬性是不屬於任何 Identity Vault 物件類別的屬性。這些屬性稱為 <workflowName>_StartWorkflow、<workflowName>_recipient 和 <workflowName>_reason。還有兩個始終存在的其他屬性，名為 AllWorkflows:reason 和 AllWorkflows:recipient。_StartWorkflow 屬性可用於啟動工作流程。_recipient 和 _reason 屬性可用於從 Identity Vault 接受工作流程所需的執行時期資料。

執行此程序之前，您應該瞭解要用做工作流程之觸發的 Identity Vault 屬性名稱。您還需要瞭解要啟動的工作流程名稱。所有工作流程都包含名為 <workflowName>_StartApprovalFlow 的特殊屬性。您可以設定工作流程組態，將所需的 eDirectory 屬性映射至工作流程的 <workflowName>_StartApprovalFlow 屬性，以根據 Identity Vault 中的事件自動啟動。

若要設定工作流程以根據 Identity Vault 中的事件啟動，請執行下列動作：

- 1 在 iManager 中，按一下 iManager 導覽網路樹中 Identity Manager 下的「Identity Manager 概觀」連結。



即會顯示「Identity Manager 概觀」頁面。此頁面會提示您選取驅動程式集。

- 2 按一下「搜尋整個網路樹」；然後按一下「搜尋」。即會顯示「Identity Manager 概觀」頁面，其中有一個圖形表示目前選定驅動程式集中的驅動程式。
- 3 按一下使用者應用程式驅動程式的驅動程式大圖示：

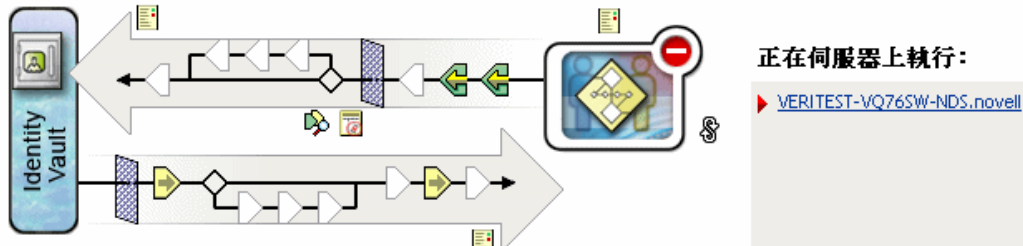


即會顯示「Identity Manager 驅動程式概觀」：

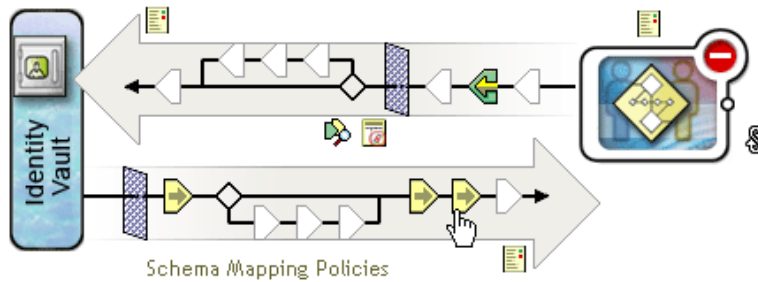
▶ [Identity Manager 概觀選取](#) ▶ [Identity Manager 概觀](#)

Identity Manager 驅動程式概觀

驅動程式：UserApplication.drsvset.novell



頂端的水平箭頭代表「發行者」通道（未在使用者應用程式驅動程式中使用），而底端的水平箭頭則代表「訂閱者」通道。當滑鼠指標放在圖形中的物件上時，會顯示物件的描述：



- 4 按一下「訂閱者」通道的「綱要映射規則」圖示。即會顯示「綱要映射規則」對話方塊，且會將預設綱要映射規則的名稱反白：

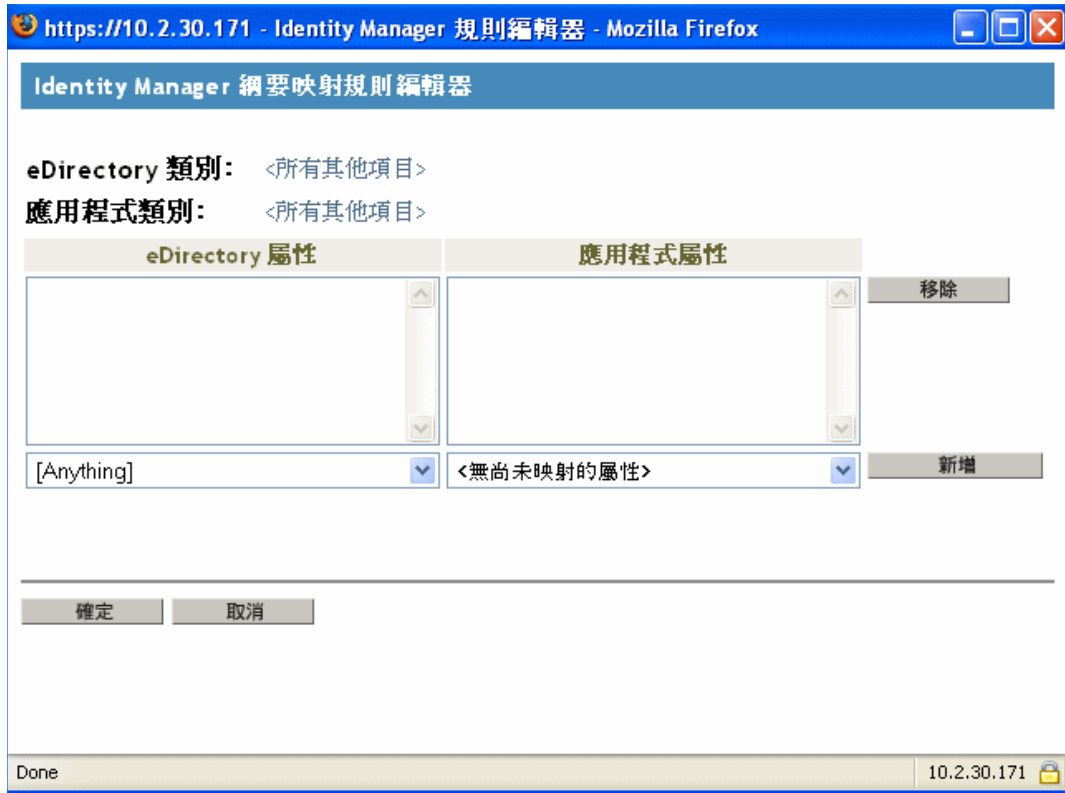


- 5 按一下「編輯」。即會顯示「*Identity Manager* 規則」對話方塊。此對話方塊可用於將 Identity Vault 類別映射至應用程式類別。此程序並未利用此功能。而是將 eDirectory 屬性映射至全域使用者應用程式屬性。



- 6 按一下「重新整理應用程式綱要」。即會顯示一則訊息，通知您必須停止驅動程式以讀取綱要，然後重新啓動。重新整理綱要大約需要 60 秒。此步驟會讀取最新工作流程資訊集，以準備下列步驟，它會指定要從 Identity Vault 移至將啓動之工作流程的資訊。
- 7 按一下「確定」，以重新整理綱要。完成綱要重新整理時會顯示訊息。
- 8 按一下「確定」，以關閉綱要重新整理訊息。您會返回「*Identity Manager* 規則」對話方塊。

- 9 按一下「非類別特定的屬性」。即會顯示「Identity Manager 綱要映射規則編輯器」。



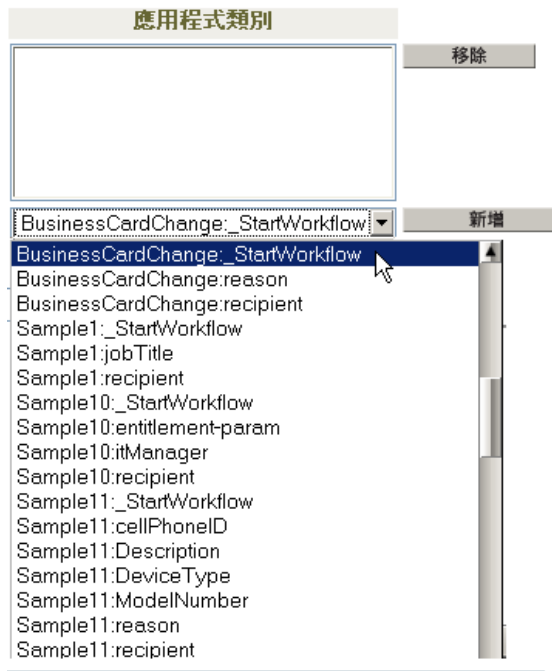
「eDirectory 屬性」下拉式清單包含所有 eDirectory 屬性。

「應用程式屬性」下拉式清單包含所有使用中「工作流程」中的屬性。清單中的屬性是以 AllWorkflows 開頭 (表示屬性可套用至所有工作流程)，或以特定工作流程的名稱開頭。如果您想要將相同的 eDirectory 屬性 (例如，manager) 映射至所有工作流程的 manager 屬性，則應將 manager 映射至 Allworkflows:manager。如果您想要將不同的 eDirectory 屬性 (例如，HRmanager) 用於特定工作流程，則應將 eDirectory 屬性映射至特定工作流程屬性 (例如，BusinessCardChange:manager)。

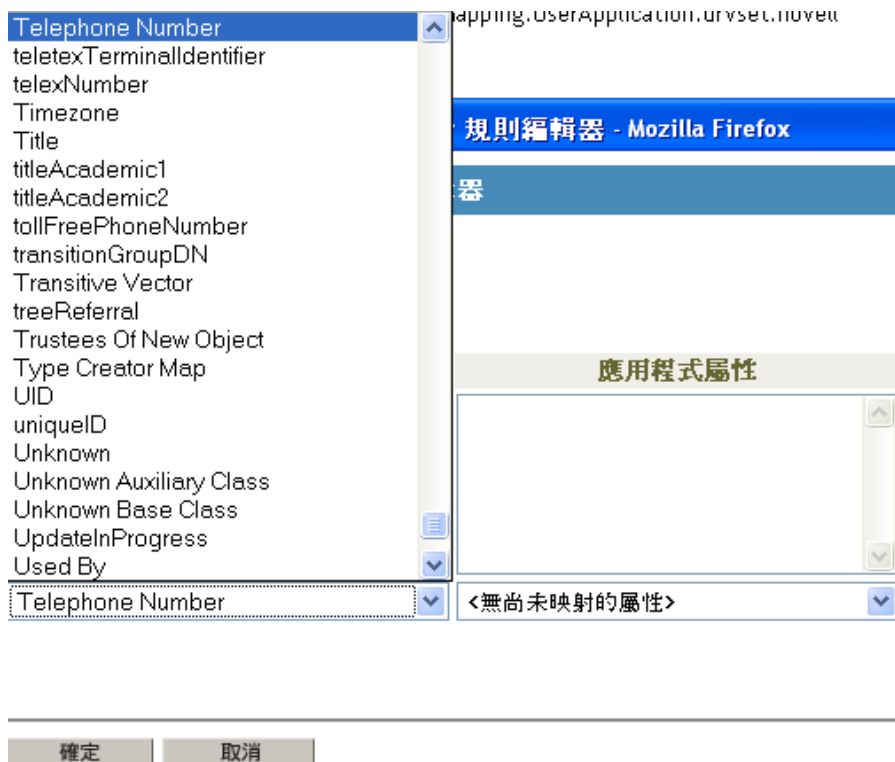
已映射的屬性會並排顯示在「eDirectory 屬性」和「應用程式屬性」欄中。

在下列步驟中，我們會將要用於啟動工作流程的 eDirectory 屬性，映射至該工作流程的 _StartWorkflow 屬性。如果工作流程預期其他 eDirectory 屬性，則您也應映射那些屬性。例如，如果 eDirectory Address 屬性是工作流程的觸發，則工作流程可能也需要 City 和 State 之類的屬性。此外，規則中也可能映射這些屬性。

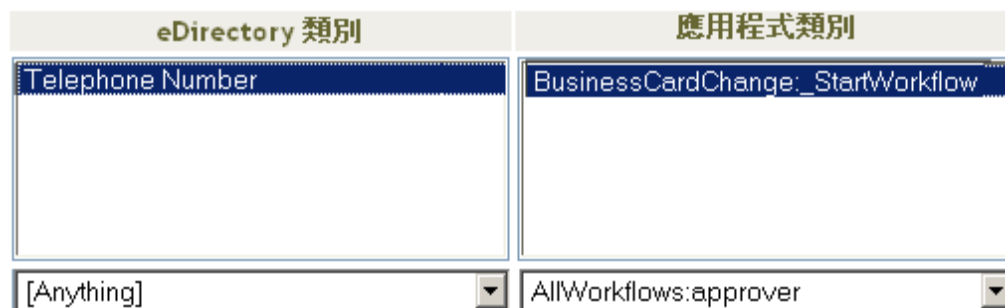
- 10 在「應用程式屬性」清單中，選取要設定組態之「工作流程」的 _StartWorkflow 屬性。下列範例顯示 BusinessCardChange 工作流程的 _StartWorkflow 屬性 (BusinessCardChange_StartWorkflow)。



- 11 在「eDirectory 屬性」清單中，選取要在該屬性變更時用於啟動工作流程的 eDirectory 屬性。在下列範例中，已選取 Telephone 屬性。這表示每當員工的電話號碼變更時，BusinessCardChange 工作流程都會啟動。



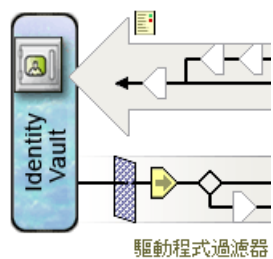
- 12 按一下「新增」，eDirectory 屬性就會映射至「應用程式」屬性。



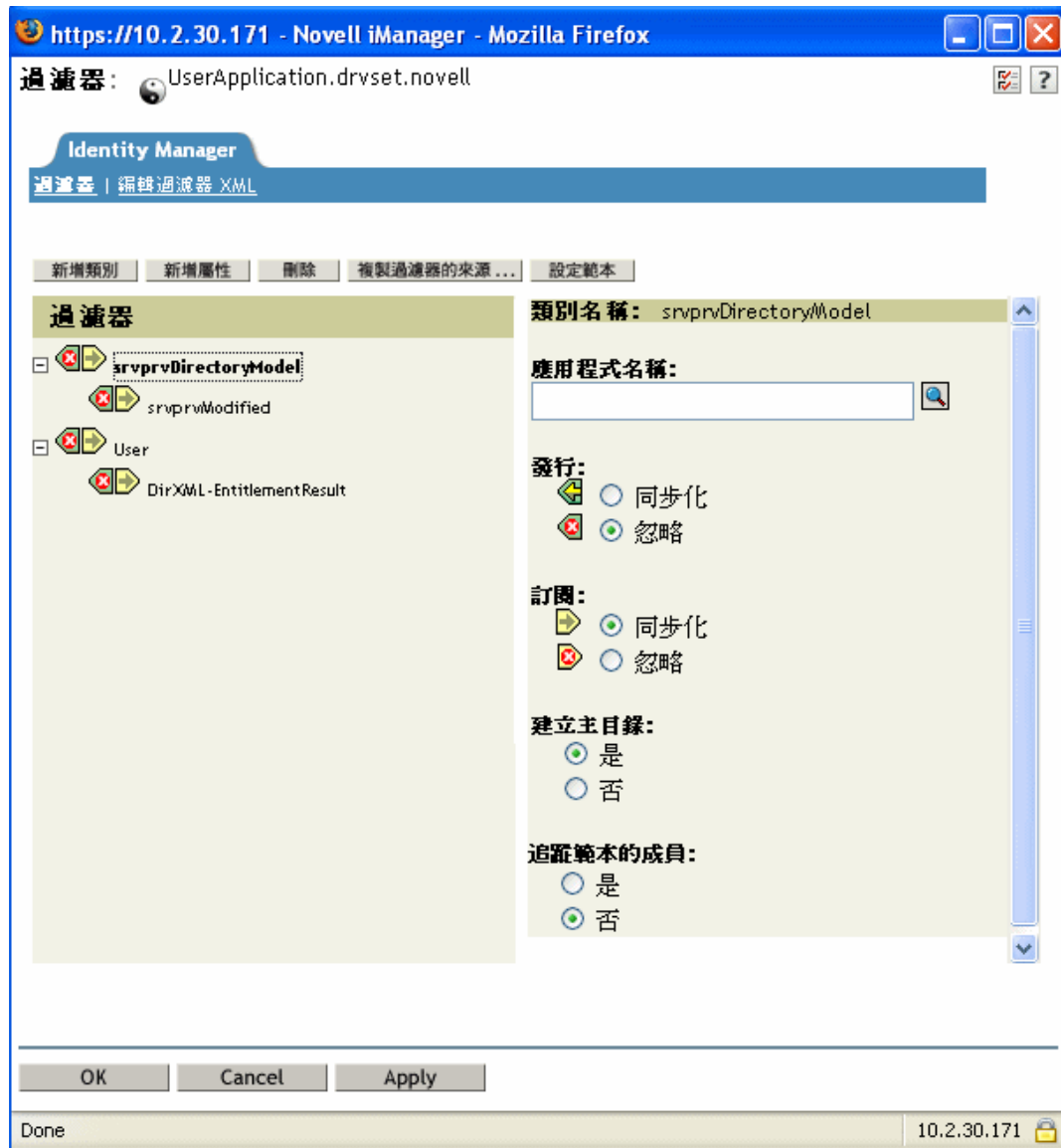
- 13 如果工作流程需要其他的 eDirectory 屬性，請重複步驟 10 至步驟 12，直到您已映射需要映射的所有屬性為止。

當映射到應用程式 _StartApprovalFlow 屬性的 eDirectory 屬性中發生變更時，工作流程將會自動啟動。不過，如果 eDirectory 屬性包含於「訂閱者」通道的「驅動程式過濾器」中，則 eDirectory 屬性將只會影響「綱要映射」規則。在下列步驟中，會將 eDirectory 屬性新增至「訂閱者」通道的「驅動程式過濾器」。

- 14 按一下「確定」，以關閉「*Identity Manager* 綱要映射規則編輯器」。
- 15 按一下「確定」，以關閉「*Identity Manager* 規則」對話方塊。
- 16 按一下「關閉」，以關閉「綱要映射規則」對話方塊。
- 17 按一下「訂閱者」通道的「驅動程式過濾器」圖示。



即會顯示過濾器視窗：



事件過濾器會指定 Identity Manager 引擎針對其處理事件的物件類別和屬性。左側的唯讀「過濾器」清單會顯示類別的屬性。右側的「類別名稱」清單會顯示與目標物件相關聯的選項。

- 18 按一下要新增至過濾器之屬性所屬的類別名稱 (例如,「使用者」)。
- 19 按一下「新增屬性」。即會顯示屬性清單。

- 20 選取屬性，然後按一下「確定」。即會將屬性新增至「過濾器」清單。



- 21 按一下屬性名稱。即會在右側面板上顯示屬性的同步化選項。



- 22 在「訂閱」下，按一下「同步化」。



- 23 指定過濾器的任何其他屬性。如果您想要報告和同步化對屬性值進行的變更，請選取「同步化」做為屬性。如果您不想報告和同步化對屬性值進行的變更，請選取「忽略」。
- 24 按一下「確定」。即會顯示一則訊息，詢問您是否要重新啓動驅動程式以讓變更生效。
- 25 按一下「確定」。您會返回「*Identity Manager* 驅動程式概觀」頁面。

設定目錄抽象層的組態

本章描述如何使用目錄抽象層編輯器，來定義 Identity Manager 使用者應用程式所使用的目錄抽象層資料定義。包含下列主題：

- ◆ 「關於目錄抽象層定義」，第 65 頁
- ◆ 「開始使用」，第 66 頁
- ◆ 「使用實體和屬性」，第 76 頁
- ◆ 「使用清單」，第 91 頁
- ◆ 「使用組織圖關係」，第 94 頁
- ◆ 「使用組態設定」，第 97 頁
- ◆ 「當地語系化顯示文字」，第 97 頁

4.1 關於目錄抽象層定義

目錄抽象層是一組資料定義，會提供身份儲存區的邏輯檢視窗。目錄抽象層會定義下列項目：

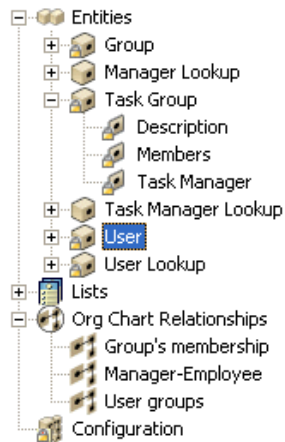
- ◆ 可在 Identity Manager 使用者應用程式中使用的身份儲存區物件和屬性。
- ◆ 身份儲存區資料在使用者介面中的顯示方式。
- ◆ 「組織圖」入口網站應用程式可用的關係。

如果您想要修改使用者應用程式外觀或功能，則可使用「目錄抽象層編輯器」來變更這些資料定義。您可以下列方式進行變更：

- ◆ 新增其他身份儲存區物件
- ◆ 變更身份儲存區物件可用的屬性集
- ◆ 變更清單的內容
- ◆ 顯示身份儲存區物件之間的不同關係

Identity Manager 使用者應用程式安裝程序會安裝和部署所需的基本抽象層定義集，以讓使用者應用程式正常運作。此安裝還會建立使用者應用程式驅動程式和使用使用者應用程式所使用的 eDirectory 綱要延伸。您可以在附錄 A 「綱要延伸」，第 329 頁中瞭解這些綱要延伸的詳細資訊。當您透過 Designer for Identity Manager 建立新的「使用者應用程式驅動程式」例項時，會在本地檔案系統上建立相同的基本檔案集。

必要的資料抽象層資料定義 當您開始自定自己的 Identity Manager 使用者應用程式時，可能想要對目錄抽象層物件進行變更。不過，不能移除或變更特定身份儲存區物件（已呼叫的實體）、屬性、關係和清單，否則使用者應用程式將不會正常運作。無法移除的定義會以掛鎖圖示進行識別。在此範例中，您可以看到「任務群組」實體及其所有屬性都已鎖定。



儲存目錄抽象層定義的位置 目錄抽象層定義是 XML 檔案：

- ◆ 本地儲存於 Designer 機器檔案系統之提供專案的 Provisioning\AppConfig\DirectoryModel 子目錄中。如果您的專案中有多個「使用者應用程式」，則會為目錄名稱編號。例如，AppConfig1、AppConfig2 等。
- ◆ 部署至「使用者應用程式驅動程式」的 AppConfig.DirectoryModel 容器。XML 檔案儲存於對應之目錄抽象層定義物件上的 XMLData 屬性中。每個實體、關係和清單都是「使用者應用程式驅動程式」之 AppConfig.DirectoryModel 容器中包含的唯一物件例項。
- ◆ 已在部署使用者應用程式的應用程式伺服器上快取。

4.2 開始使用

您將使用 Designer for Identity Manager 之「提供檢視窗」的功能和目錄抽象層編輯器，來定義目錄抽象層的內容。請遵循下列步驟開始使用：

步驟	任務	描述
1	建立 Identity Manager 專案	這包含： <ul style="list-style-type: none"> ◆ 設定 Identity Vault 的組態 ◆ 指定「驅動程式集」內容 請參閱 Identity Manager 文件。

步驟	任務	描述
2	新增「使用者應用程式」驅動程式至「模擬器」	您可以在「模擬器調色盤」的「提供」資料夾中，找到 Identity Manager 使用者應用程式驅動程式。
		
3	完成「使用者應用程式」驅動程式組態	關於此程序，請參閱「完成使用者應用程式驅動程式組態」，第 67 頁。
4	存取提供檢視窗	請參閱「存取提供檢視窗」，第 71 頁。
5	啟動目錄抽象層編輯器	請參閱「若要開啓目錄抽象層編輯器，請執行下列動作：」，第 72 頁。

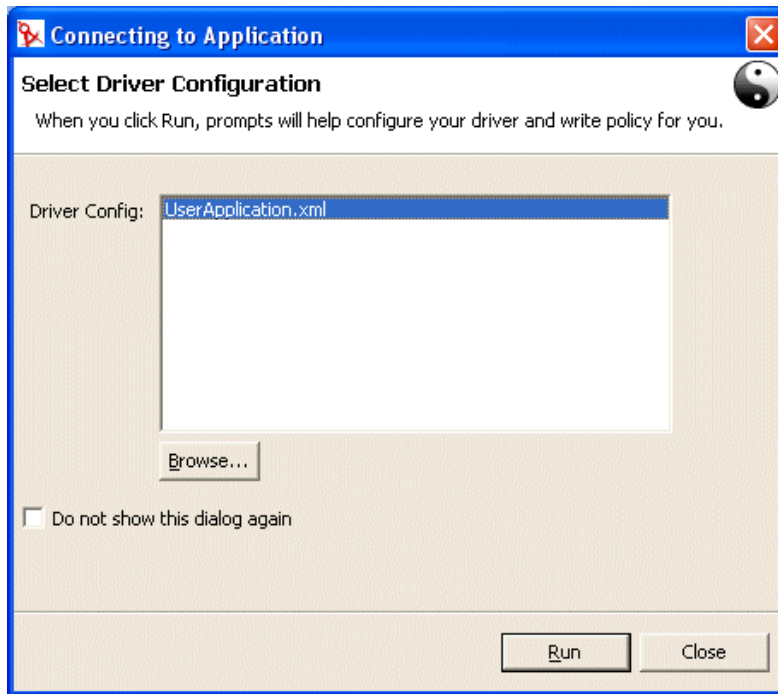
4.2.1 完成使用者應用程式驅動程式組態

建立 Identity Manager 專案之後，請遵循下列步驟。

若要完成「使用者應用程式」驅動程式組態，請執行下列動作：

- 1 在畫布上放下「使用者應用程式」驅動程式圖示。

將會提示您驅動程式組態。



- 2 選取「*UserApplication.xml*」(預設值)，然後按一下「執行」。

3 按一下「是」或「否」，以指定精靈應如何處理項目的驗證。

Import Information Requested

The driver writer requested that the following information be supplied in order to import this driver configuration file.

Information requested: * Required

Enter the driver name. Entering the name of or selecting an existing driver will overwrite its configuration. The Driver name 'UserApplication' was provided as a default value by the Configuration File.

Driver name: *

UserApplication

Enter the DN of the User Application Administrator. This value should match the user entered during the User Application installation. Use the DOT format i.e., admin.orgunit.novell or use browse. This is a required field.

Authentication ID: *

Application Password :

Reenter the password:

Enter the User Application Context. This is the context portion of the URL for the User Application WAR file. The default is: IDM.

Application Context:

IDM

OK Cancel

Enter the Host Name or IP address of the application server where the User Application is running. For example, 'http://ServerName' or 'https://123.456.78.99'. This is a required field.

Host: *

Enter the host port on the application server specified above. This is the port where the User Application is accessible e.g. 80, 8080, 8090.

Port:

OK Cancel

4 完成面板，如下所示：

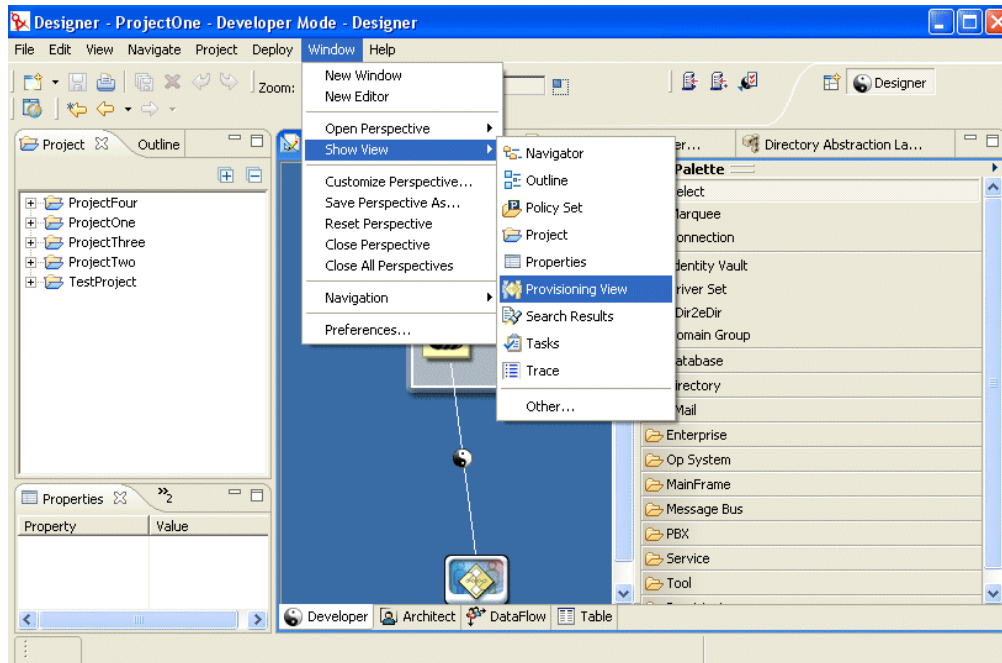
內容	要指定的項目
驅動程式名稱	<ul style="list-style-type: none">◆ 現有驅動程式的名稱 (在使用者應用程式安裝期間，所指定之驅動程式集內的驅動程式)。◆ 新驅動程式的名稱。
驗證 ID	「使用者應用程式管理員」的 DN。
應用程式密碼 / 重新輸入密碼	「使用者應用程式管理員」(上述) 的密碼。
應用程式網路位置	使用者應用程式網路位置的名稱 (在安裝時指定，例如 IDM)。
主機	部署 Identity Manager 使用者應用程式之應用程式伺服器的主機名稱或 IP 位址。此資訊可用於： <ul style="list-style-type: none">◆ 觸發要連接之應用程式伺服器上的工作流程，以存取工作流程 (終止、收回等)。◆ 更新快取的資料定義。
連接埠	上面「主機」的連接埠。

5 按一下「確定」。

4.2.2 存取提供檢視窗

若要存取「提供檢視窗」，請執行下列動作：

- 1 選擇下列其中一種方式：
 - ◆ 選取「視窗 > 顯示檢視窗 > 提供檢視窗」。



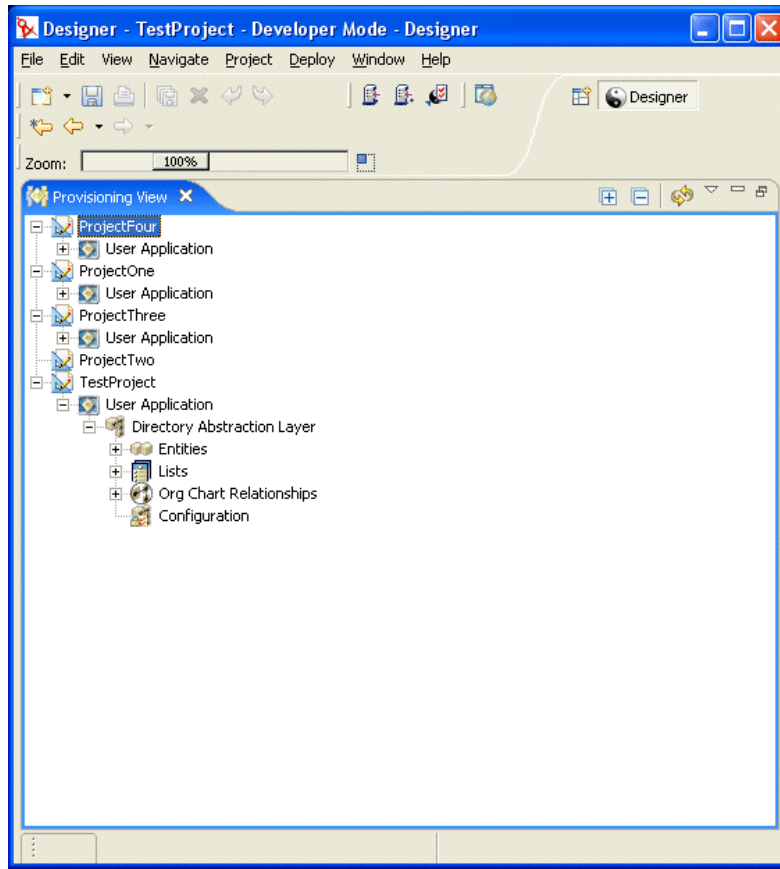
- ◆ 開啓「提供」資料夾，並選取「提供檢視窗」。
- ◆ 按一下「確定」。

或

- ◆ 選取「使用者應用程式」圖示，按一下滑鼠右鍵，然後選取「應用程式 > 顯示提供檢視窗」。

在「提供檢視窗」中，您將看到剛剛建立的專案，以及位於相同工作空間的任何其他提供專案。

提示：如果您在檢視窗中看不到預期的應用程式，可能是因為專案已損毀。如果您的專案已損毀，您必須重新建立它。



關於提供檢視窗

「提供檢視窗」提供對提供功能的持續存取。在「提供檢視窗」中按兩下項目即會開啓該項目的編輯器。您將使用提供檢視窗，以針對目錄抽象層定義執行下列動作：

- 輸入來自身份儲存區的一或多個物件定義。
- 驗證資料定義的結構。
- 部署定義至專案中指定的身份儲存區。
- 建立和刪除目錄抽象層定義。

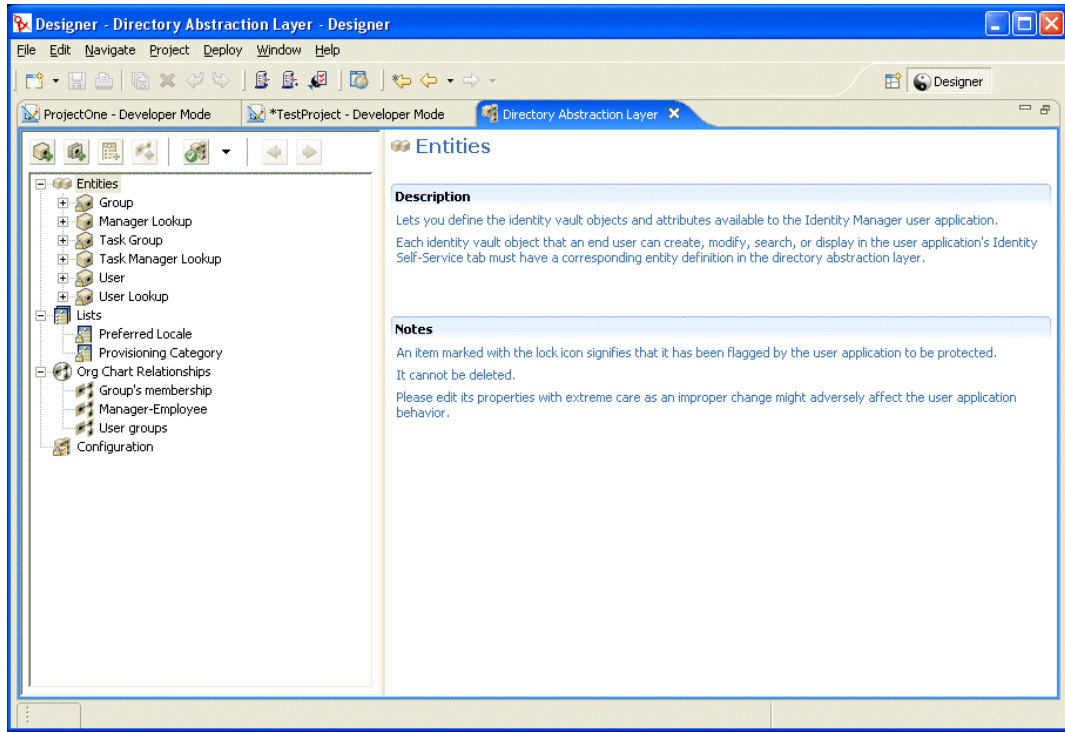
如需相關資訊，請參閱「[輸入、驗證和部署目錄抽象層定義](#)」，第 98 頁。

4.2.3 啓動目錄抽象層編輯器

若要開啓目錄抽象層編輯器，請執行下列動作：

- 1 保持「提供檢視窗」開啓，並導覽至「目錄抽象層」節點。
- 2 按兩下「目錄抽象層」節點。

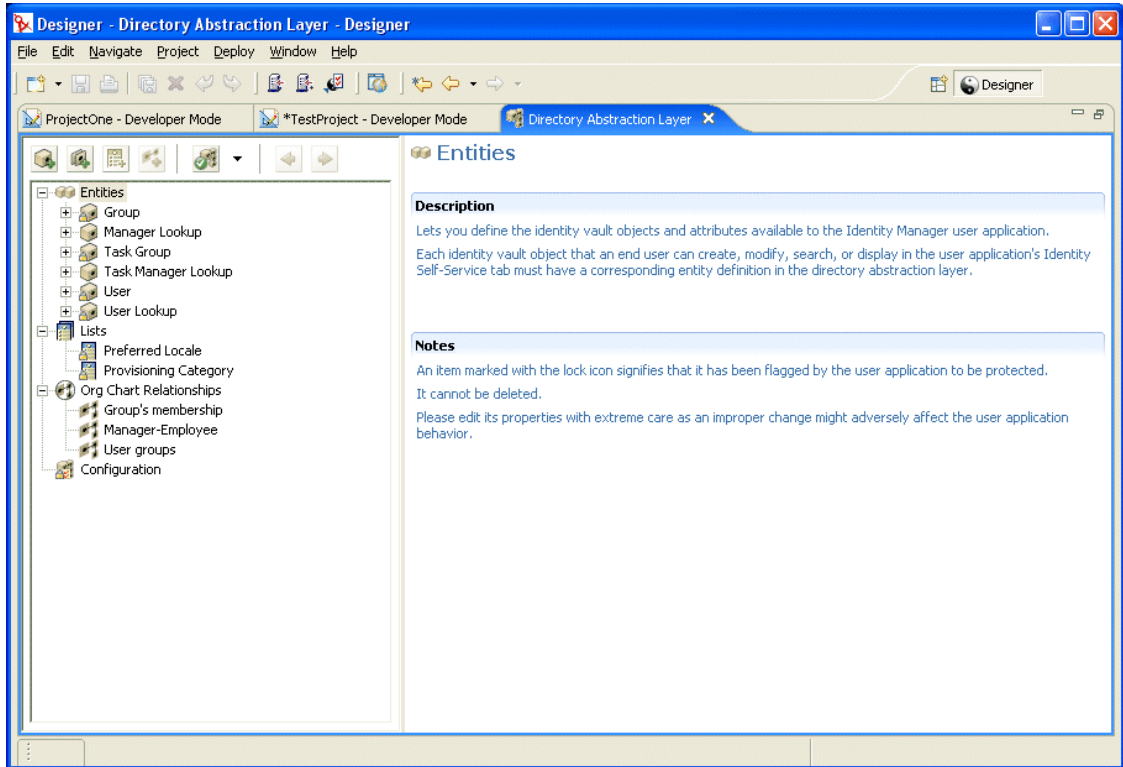
您將看到包含「實體」、「清單」、「組織圖關係」和「組態」的網路樹。



關於目錄抽象層編輯器

目錄抽象層編輯器會提供一種圖形化方式，以定義組成目錄抽象層的 XML 檔案集。目錄抽象層編輯器是一種基於 Eclipse 的工具，您可以從 Identity Manager 專案的「提供檢視窗」進行存取。

第一次開啓目錄抽象層編輯器時，您將看到基本的抽象層物件集，每次建立新提供物件時都會自動建立它：



目錄抽象層編輯器的節點包含：

元素	描述
實體	<p>實體代表針對此專案設定組態的身份儲存區物件，且可用於使用者應用程式。現有兩種類型的實體：</p> <ul style="list-style-type: none">◆ 從綱要映射的實體。這些實體代表身份儲存區中存在的物件，它們透過使用者應用程式直接向使用者公開。通常，使用者可以建立、搜尋和修改這些類型的物件屬性。◆ 代表 LDAP 關係的實體。也稱為 DNLookup。這些實體代表已編製索引的搜尋，並可用於支援要公開的特定類型屬性。DNLookup 實體提供 LDAP 物件之間關係的資訊。DNLookup 實體由下列各項使用：<ul style="list-style-type: none">◆ 決定關係的「組織圖」入口網站應用程式。◆ 提供快顯選擇清單和 DN 網路位置的「搜尋清單」、「建立」和「詳細資料」入口網站應用程式。 <p>如需相關資訊，請參閱「定義實體」，第 77 頁。</p>

元素	描述
清單	<p>可讓您定義全域清單的內容。全域清單會：</p> <ul style="list-style-type: none"> ◆ 與屬性相關聯。屬性在使用者應用程式中顯示時，會顯示為下拉式清單。 ◆ 用於顯示 iManager 之「提供申請組態外掛程式」所使用的類別。 <p>如需相關資訊，請參閱「使用清單」，第 91 頁。</p>
組織圖關係	<p>由使用者應用程式之「身份自助服務」索引標籤的「組織圖」動作所使用。可讓您映射基於綱要之實體之間的階層式關係。</p> <p>如需相關資訊，請參閱「使用組織圖關係」，第 94 頁。</p>
組態	<p>一般組態參數。</p> <p>如需相關資訊，請參閱「使用組態設定」，第 97 頁。</p>

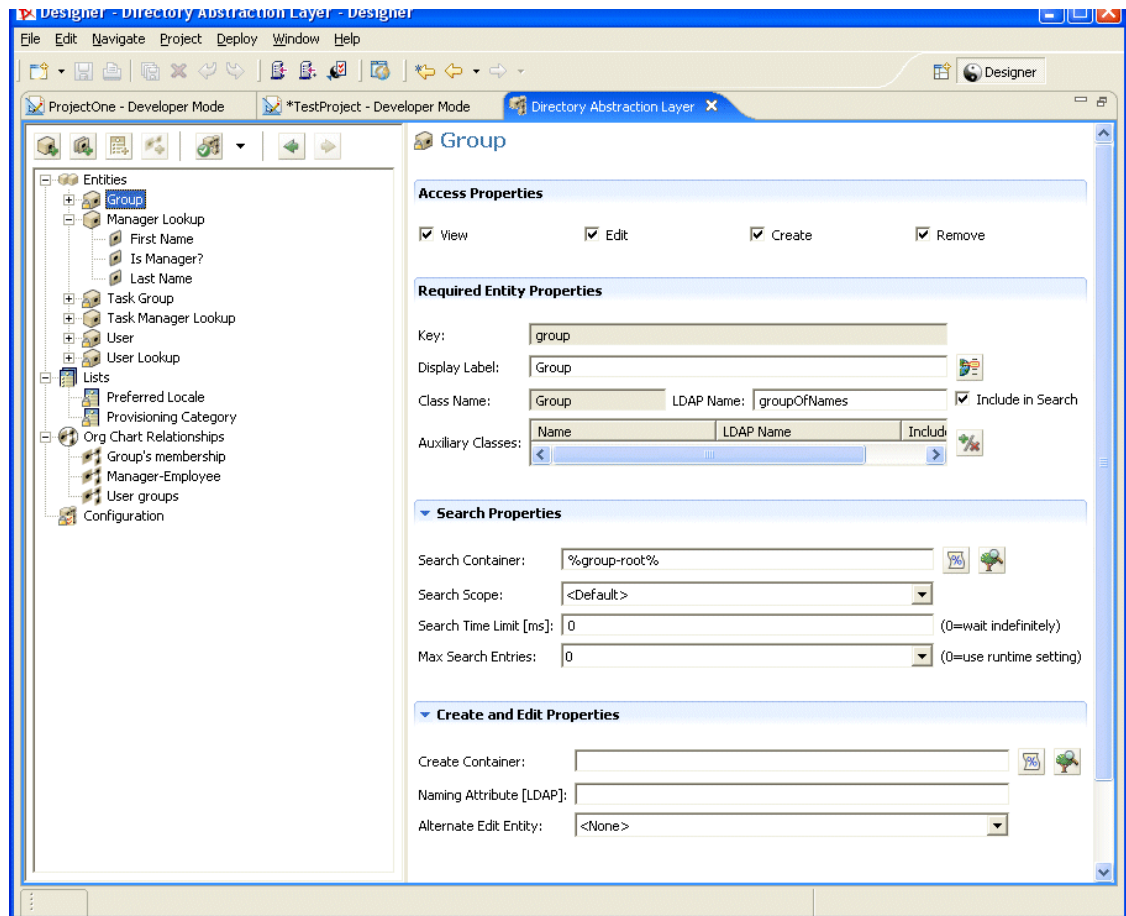
在本地儲存 XML 檔案的位置 目錄抽象層編輯器會為每個實體、清單或關係產生單一 XML 檔案。檔案儲存在專案的 Provisioning\AppConfig\DirectoryModel 資料夾中。檔案名稱是基於物件的索引鍵。包含：

目錄	描述
ChoiceDefs	包含定義全域清單的檔案。檔案的副檔名為 .choice。
EntityDefs	包含定義實體和屬性的檔案。檔案的副檔名為 .entity。
RelationshipDefs	包含定義「組織圖」入口網站應用程式可用關係的檔案。這些檔案的副檔名為 .relation。

您將使用目錄抽象層編輯器的功能，來新增模型化您自己之身份儲存區綱要的定義。您將使用「提供檢視窗」的功能，來將新定義部署至身份儲存區。

使用目錄抽象層編輯器

目錄抽象層編輯器分為兩個窗格：左窗格提供目錄抽象層內容的檢視窗。當您在左窗格中選取項目時，右窗格會顯示選定項目的屬性和設定。



4.3 使用實體和屬性

要使用者在 Identity Manager 使用者應用程式中搜尋、顯示或編輯的任何身份儲存區物件，都必須定義為目錄抽象層中的實體。例如，若要在使用者應用程式中使用 inetOrgPerson 身份儲存區物件，您必須建立其實體定義。

4.3.1 新增實體的步驟

請遵循下列步驟，以將實體新增至目錄抽象層：

步驟	任務	相關資訊
1	決定要在使用者應用程式中使用的身份儲存區物件	「分析資料需求」，第 77 頁
2	使用目錄抽象層編輯器，以定義目錄抽象層中的身份儲存區物件	「定義實體」，第 77 頁
3	使用「提供檢視窗」來驗證資料定義	「輸入、驗證和部署目錄抽象層定義」，第 98 頁

步驟	任務	相關資訊
4	將定義部署至身份儲存區	「關於部署」 ，第 101 頁
5	更新應用程式伺服器的快取，以包含新的抽象層定義	第 13 章 「快取組態」 ，第 197 頁
6	測試 Identity Manager 使用者應用程式，以確保正確顯示變更	

4.3.2 分析資料需求

若要在目錄抽象層中模型化身份儲存區資料，您需要瞭解下列項目：

- ◆ 要讓 Identity Manager 使用者應用程式可使用的目錄部份。

例如，使用者可以搜尋和顯示的物件清單。針對基本的抽象層定義集，檢查此清單以確定需要新增的項目。

- ◆ 包含自定延伸和輔助類別的綱要結構
- ◆ 資料結構包含：
 - ◆ 必要項目和選擇性項目
 - ◆ 驗證規則
 - ◆ 物件之間的關係 (DN 參考)
 - ◆ 定義屬性的方式 (例如，代表電話號碼的屬性可能有多個值：家中電話號碼、辦公室電話號碼和行動電話號碼。
- ◆ 將看到資料的使用者
這是公用還是私人網站？

具有此資訊之後，您就可以使用它，將身份儲存區物件映射至抽象層實體。

附註：eDirectory ACL 適用於所有抽象層物件。對物件和屬性的有效權限是基於應用程式登入時建立的已驗證使用者。

4.3.3 定義實體

根據您要在使用者應用程式中公開的內容而定，將定義兩種實體：

- ◆ 從綱要映射的實體。這些實體代表身份儲存區中存在的物件，它們在使用者應用程式中直接向使用者公開。定義此類型的實體時，您將公開要使用者使用的所有屬性。此實體類型的範例包含：「使用者」、「群組」和「任務群組」。如果您要向不同類型的使用者公開不同的屬性集，則也可以針對相同的物件建立多個實體定義。如需相關資訊，請參閱 [「建立單一物件的多個實體定義」](#)，第 78 頁。
- ◆ 代表 LDAP 關係的實體。此類型的實體稱為 DNLookup，由使用者應用程式用於：
 - ◆ 將相關實體間 DN 搜尋的結果填入清單
 - ◆ 在更新和刪除期間維護 DN 參考之屬性中的參考完整性

「組織圖」入口網站應用程式使用支援 DNLookup 的實體來確定關係，且「搜尋」、「建立」和「詳細資料」入口網站應用程式也可以使用它來提供快顯選擇清單和 DN 網路位置。此類型實體的範例包含：「管理員查閱」、「任務管理員查閱」和「使用者查閱」。如需相關資訊，請參閱 [「使用 DNLookup 控制項類型」](#)，第 88 頁。

建立單一物件的多個實體定義

您可以建立代表相同身份儲存區物件的多個實體定義，但提供不同的資料檢視窗。您可以在實體定義內：

- ◆ 定義不同的屬性 (針對每個實體定義)

或

- ◆ 定義相同的屬性，但是指定不同的存取內容以控制屬性的搜尋、檢視、編輯或隱藏的方式。

附註：實體定義可選擇性地包含過濾器，以從結果集隱藏特定實體。

然後，您可以在使用者介面中的不同部份，使用這些不同的實體定義。例如，假設您想要分別針對公用網站和內部網站，建立員工的目錄。在公用網站上，您想要提供姓、名和電話號碼，但在內部網站上，您想要列出其他的資訊 (例如，頭銜、經理等)。以下是您完成此步驟的方式：

- 1 建立兩個實體定義 (具有不同的索引鍵)。

兩個實體定義都會公開相同的身份儲存區物件，但是一個實體定義鍵是公用員工資訊，而另一個是內部員工資訊。

- 2 在每個實體定義內，定義不同的屬性集：分別針對公用員工資訊和內部員工資訊。

- 3 使用 Identity Manager 使用者應用程式的「入口網站管理」索引標籤，分別為公用頁面和內部頁面建立入口網站應用程式例項。

如需建立入口網站應用程式例項的相關資訊，請參閱第 9 章「入口網站應用程式管理」，第 161 頁。

建立實體定義的程序

當要公開的實體和屬性已決定時，您可以使用編輯器，開始將它們新增至目錄抽象層。您將遵循下列這組步驟：

步驟	操作	參閱此程序
1.	決定要開始處理的檔案集。 <ul style="list-style-type: none">◆ 您想要新增至基本的定義集◆ 您想要從已部署的定義開始	<p>「新增實體的步驟」，第 76 頁</p> <p>「關於輸入」，第 99 頁</p>
1a.	您要使用的部份實體不屬於 eDirectory 基本綱要。在編輯器的可選物件和屬性清單中，不會自動顯示對 eDirectory 綱要的任何延伸。這表示您必須更新 Designer 的本地綱要檔案，以包含這些自定物件和屬性。	「若要更新可用綱要元素的清單，請執行下列動作：」，第 79 頁
2.	新增一或多個實體至目錄抽象層	「新增實體」，第 79 頁
3.	新增屬性至實體	「新增屬性」，第 81 頁

更新可用綱要元素的清單

若要更新可用綱要元素的清單，請執行下列動作：

- 1 保持 Identity Manager 專案開啓，選取 Identity Vault，按一下滑鼠右鍵，然後選取「即時操作 > 輸入綱要」。
- 2 選擇「從 eDirectory 輸入」，並提供 eDirectory 主機的規格。
- 3 按「下一步」。
- 4 選取要輸入的類別和屬性，然後按一下「完成」。

新增實體

您可以透過「新增實體精靈」（說明如下），或按一下編輯器工具列中的「新增實體」按鈕，來新增實體。

附註：使用「新增實體」按鈕時，會提示您選取要建立之實體的物件類別。編輯器會自動將必要屬性新增至實體。然後，您可以使用「新增屬性」對話方塊來完成實體定義。

若要使用「新增實體精靈」新增實體，請執行下列動作：

- 1 以下列其中一種方式啓動「新增實體精靈」：

從「提供檢視窗」：

- ◆ 選取「實體」節點，按一下滑鼠右鍵，然後選取「新增」。
- ◆ 選取「檔案 > 新增 > 提供」。選擇「目錄抽象層實體」。按「下一步」。

從目錄抽象層編輯器：

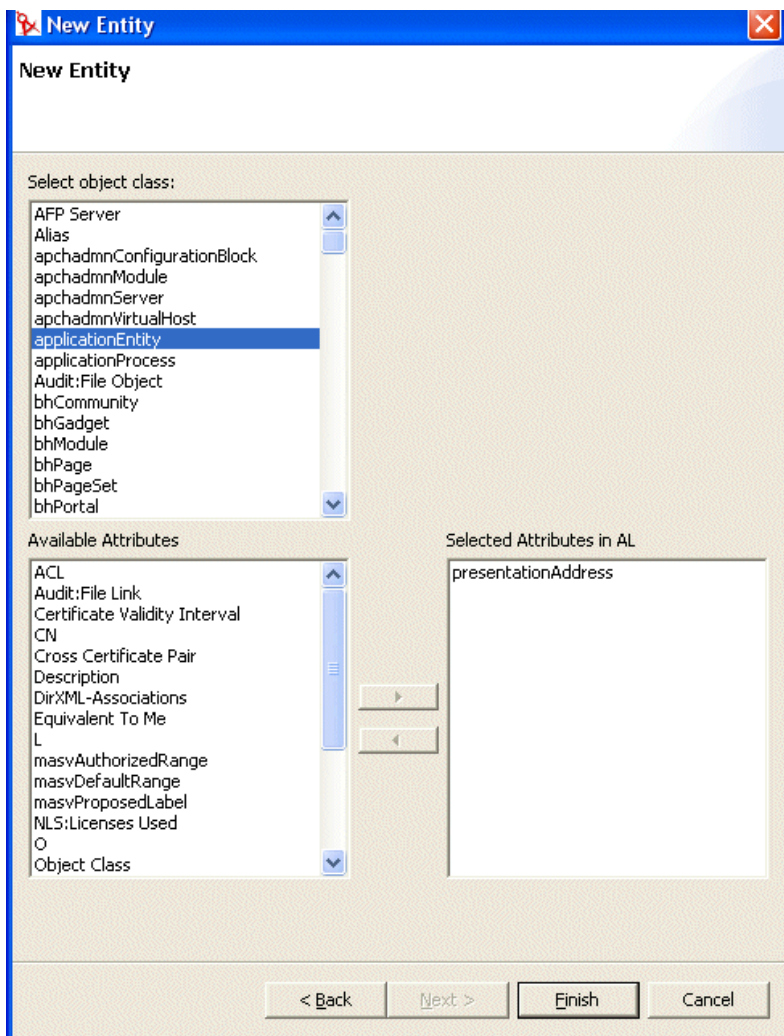
- ◆ 選取「實體」節點，按一下滑鼠右鍵，然後選擇「新實體屬性精靈」。
- 即會顯示「新實體」對話方塊。

附註：如果從「檔案」功能表啓動，則對話方塊包含以其中一種其他方式啓動時未顯示的欄位。其顯示如下。

2 完成面板，如下所示：

欄位	描述
Identity Manager 專案和提供應用程式	在您需要新增實體和屬性的位置，選取 Identity Manager 專案和「提供應用程式」。 附註：當您從「檔案」功能表啟動精靈時會顯示這些欄位。
實體鍵	實體的唯一識別碼。
顯示標籤	在使用者介面中參考此實體時所顯示的字串。

3 按「下一步」。即會顯示「新實體」對話方塊：



4 選擇要建立之實體的「物件類別」，然後從「可用屬性」清單中選取想要的屬性。

提示：如果要建立之實體的物件類別未顯示在「可用物件類別」清單中，則您可能需要更新 Designer 的本地綱要檔案。遵循「若要更新可用綱要元素的清單，請執行下列動作：」，第 79 頁中描述的步驟。

5 按一下「完成」。

即會顯示內容表，以進行編輯。

如需相關資訊，請參閱「實體內容參考」，第 83 頁。

附註：若要讓使用者應用程式可以使用屬性，您必須部署包含該屬性的實體。

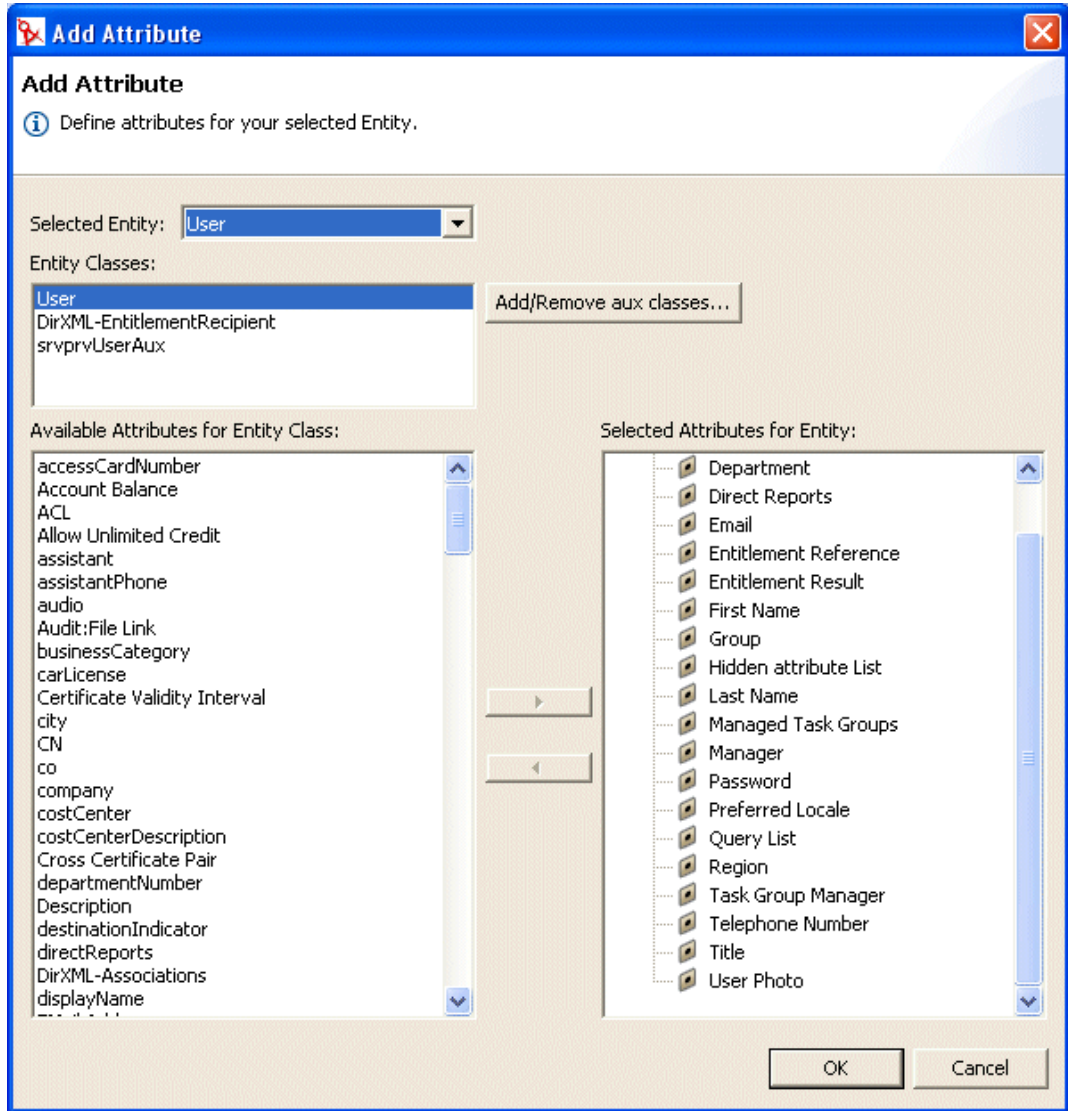
新增屬性

若要新增屬性，請執行下列動作：

1 選取實體。

- 2 以下列方式新增屬性：
 - ◆ 按一下滑鼠右鍵，並選取「新增屬性」。或
 - ◆ 按一下「新增屬性」圖示。

將會提示您下列內容：



- 3 從「實體類別的可用屬性」清單中選擇屬性，並將其新增至「實體的選定屬性」清單。

提示：如果要建立的屬性未顯示在「實體類別」清單的「可用屬性」中，則您可能需要更新 Designer 的本地綱要檔案。遵循「若要更新可用綱要元素的清單，請執行下列動作：」，第 79 頁中描述的步驟。

- 4 按一下「確定」。

即會顯示內容表，以進行編輯。

如需相關資訊，請參閱「[屬性內容參考](#)」，第 85 頁。

附註：若要讓使用者應用程式可以使用屬性，您必須部署屬性。

實體內容參考

您可以在實體上設定下列類型的內容：

- ◆ 「[實體存取內容](#)」，第 83 頁
- ◆ 「[實體必要內容](#)」，第 83 頁
- ◆ 「[實體搜尋內容](#)」，第 84 頁
- ◆ 「[實體建立和編輯內容](#)」，第 84 頁
- ◆ 「[密碼管理內容](#)」，第 85 頁

實體存取內容

「存取內容」會控制使用者應用程式與實體互動的方式。包含：

內容	描述
建立	選取 ：此物件可由使用者應用程式建立。
編輯	不選 ：無論基礎 ACL 為何，都無法由使用者應用程式變更此物件。 選取 ：此物件也許可以變更，但要使用身份儲存區 ACL 來判斷。
檢視	選取 ：此物件可由使用者應用程式顯示。
移除	選取 ：此物件可由使用者應用程式刪除。

實體必要內容

「必要」的實體內容為：

內容名稱	描述
鍵	此實體的唯一識別碼。它定義使用者應用程式參考此物件的方式。
顯示標籤	定義物件在使用者介面中的顯示方式。
類別名稱	「Novell 目錄服務 (Novell Directory Service, NDS)」類別名稱。
LDAP 名稱	LDAP 物件類別名稱。
搜尋	選取 ：可以搜尋此實體。必須選取 (true) 身份入口網站應用程式 (例如，「實體搜尋清單」或「實體組織圖」) 在查詢中所使用的實體。
輔助類別	此實體的零或多個輔助類別清單。 如果新增輔助類別，則您必須指定輔助類別「LDAP 名稱」、「NDS 名稱」，以及是否可以進行搜尋。

實體搜尋內容

「實體搜尋內容」為：

內容名稱	描述
搜尋容器	搜尋啟動位置 (搜尋根部) 之 LDAP 節點或容器的可辨識名稱。 例如： <code>ou=sample,o=ourOrg</code> 您可以瀏覽身份儲存區來選取容器，也可以使用「 使用預先定義的參數 」， 第 85 頁 中描述的其中一個預先定義參數。
搜尋範圍	指定與搜尋根部相關之搜尋發生的位置。 值為： < 預設值 > ：此搜尋範圍與選取「容器」和次容器相同。 容器 ：搜尋發生於搜尋根部 DN 和搜尋根部層級上的所有項目。 容器和次容器 ：搜尋發生於搜尋根部 DN 和所有次容器。作用與選取「< 預設值 >」相同。 物件 ：限制為只搜尋指定的物件。此搜尋用於驗證指定的物件是否存在。
搜尋時間限制 [ms]	指定一個以毫秒為單位的值，如果沒有時間限制，則指定 0。
搜尋項目上限	指定要在搜尋中傳回的最大搜尋結果項目數。 如果您要使用執行時期設定，請指定 0。 建議： 設定 100 至 200 之間 的值，以取得最大效率。 請勿設定超過 1000 的值

實體建立和編輯內容

「實體建立和編輯內容」為：

內容名稱	定義
建立容器	在其中建立此類型新實體的容器名稱。 您可以瀏覽身份儲存區來選取容器，也可以使用「 使用預先定義的參數 」， 第 85 頁 中描述的其中一個預先定義參數。 如果未指定此值，則「建立」入口網站應用程式會提示使用者指定新物件的容器。入口網站應用程式會將實體定義中指定的 search-root 做為基礎，並可讓使用者從此處向下切入。如果實體定義中沒有指定任何 search-root ，則它會使用使用者應用程式安裝期間指定的根部 DN。
命名屬性	實體的命名屬性 (相對可辨識名稱 (Relative Distinguished Name, RDN))。只有選取存取參數「建立」的實體需要此值。

內容名稱	定義
替代編輯實體	「編輯實體」屬性以「詳細資料」入口網站應用程式的編輯模式顯示。 從下拉式功能表選擇實體，如果「詳細資料」入口網站應用程式未顯示此實體，則選擇「<無>」。

密碼管理內容

「密碼管理內容」為：

內容名稱	定義
密碼屬性	在儲存此實體密碼的位置，選擇屬性。
建立屬性時需要密碼	選取 ：表示建立此實體時需要密碼。

使用預先定義的參數

目錄抽象層編輯器可讓您將預先定義的參數用於某些值。參數為：

預先定義的參數	描述
%driver-root%	代表「提供驅動程式 DN」。在安裝時的使用者應用程式組態設定期間，或者在稍後的組態設定期間指定此值。它儲存在使用者應用程式的領域組態中。
%user-root%	代表「使用者容器 DN」。在安裝時的使用者應用程式組態設定期間，或者在稍後的組態設定期間指定此值。它儲存在使用者應用程式的領域組態中。
%group-root%	代表「群組容器 DN」。在安裝時的使用者應用程式組態設定期間，或者在稍後的組態設定期間指定此值。它儲存在使用者應用程式的領域組態中。

屬性內容參考

您可以在屬性上設定下列類型的內容：

- ◆ 「屬性存取內容」，第 85 頁
- ◆ 「屬性必要內容」，第 86 頁
- ◆ 「屬性過濾器 and 格式內容」，第 86 頁
- ◆ 「屬性 UI 控制項內容」，第 87 頁

屬性存取內容

「屬性存取內容」為：

名稱	描述
編輯	選取 ：此屬性可由使用者應用程式編輯 / 修改。即使已選取 (true)，如果基礎身份儲存區 ACL / 有效權限阻止，則仍無法編輯該屬性。
啓動	不選 ：此屬性無法由使用者應用程式使用。作用與從檔案移除項目一樣。

名稱	描述
隱藏	<p>控制是啓用還是停用使用者應用程式中的「隱藏」核取方塊。「隱藏」核取方塊可讓使用者控制是否由應用程式顯示屬性（例如，他們的照片）。</p> <p>不選：針對此屬性停用「隱藏」核取方塊，因此使用者無法選擇隱藏此屬性。</p> <p>選取：可以在使用者應用程式中啓用「隱藏」核取方塊。然而，登入的使用者必須滿足下列條件。他們：</p> <ul style="list-style-type: none"> ◆ 是屬性的擁有者或「使用者應用程式管理員」。 ◆ 具有更新身份儲存區上 <code>srvprvHideAttributes</code> 屬性的「託管者」權限。 <p>如果不符合這些要求，則即使此設定為選取 (true)，在使用者介面中仍會停用「隱藏」核取方塊。</p> <hr/> <p>提示：當使用者隱藏包含影像的屬性時，檢視影像的使用者可能會在重新整理其瀏覽器快取之前繼續看到它。</p>
多值	<p>指定此屬性是否是多值的，例如，電話號碼。</p> <p>選取：屬性可以是多值的。</p>
讀取	<p>選取：使用者應用程式可以查詢此屬性。針對大部份屬性，應選取 (true) 此項，但是對於部份屬性（如密碼），則應不選。</p>
必要	<p>選取：必須提供屬性。</p>
搜尋	<p>選取：使用者應用程式可以針對此屬性進行搜尋。必須選取身份入口網站應用程式（例如，「實體搜尋清單」或「實體組織圖」）在查詢中所使用的屬性。</p> <hr/> <p>提示：如果在 <code>eDirectory</code> 中，也對搜尋中使用的屬性編製索引，則搜尋會更快。</p>
檢視	<p>選取：使用者應用程式可以顯示此屬性。在大多數情況下為 true，但是對於部份屬性，例如密碼，則很可能不會選取此項。</p>

屬性必要內容

名稱	描述
鍵	屬性的唯一識別碼。
顯示標籤	使用者應用程式中顯示的標籤。
屬性名稱	此屬性的 Novell 目錄服務 (NDS) 名稱。
LDAP 名稱	此屬性的 LDAP 名稱。

屬性過濾器 and 格式內容

名稱	描述
過濾器：WHERE 屬性	讓您指定在身份儲存區上搜尋此屬性的 LDAP 過濾器。
啓動	選取： 啓用過濾器。

屬性 UI 控制項內容

名稱	描述
資料類型	從下列清單選擇資料類型： <ul style="list-style-type: none">◆ 二進位◆ 布林◆ DN◆ 整數◆ 當地語系化字串◆ 字串◆ 時間
格式類型	由使用者應用程式使用，以格式化資料。格式類型包含： <ul style="list-style-type: none">◆ 無◆ AOL IM◆ 電子郵件◆ Groupwise IM◆ 影像◆ 電話號碼◆ Yahoo IM◆ 影像 URL◆ 日期◆ 日期時間 <p>「格式類型」取決於資料類型。例如，「時間」資料類型只可與「日期」和「日期時間」格式相關。</p>

名稱	描述
----	----

控制項類型

類型包含：

DNLookup：定義使此屬性包含 DN 參考。當您要執行下列動作時使用：

- ◆ 將在相關實體之間的 DN 搜尋結果填入清單
- ◆ 在更新和刪除期間維護 DN 參考之屬性中的參考完整性

使用者應用程式使用此資訊產生特殊的使用者介面元素，並根據 DNLookup 定義執行最佳化搜尋。

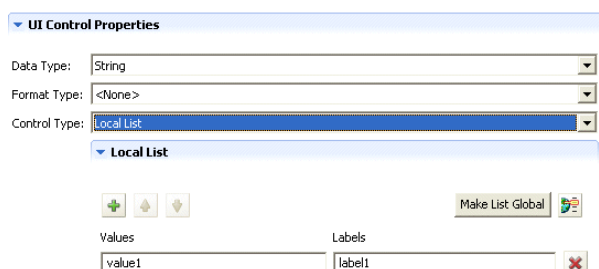
如需相關資訊，請參閱「使用 DNLookup 控制項類型」，第 88 頁

全域清單：將此屬性以下拉式清單的形式顯示，該清單內容是在此屬性定義之外的檔案中定義。

如需相關資訊，請參閱「使用清單」，第 91 頁。

本地清單：將此屬性以下拉式清單的形式顯示，該清單內容是與此屬性一起定義的。若要定義本地清單，請執行下列動作：

1. 選取屬性，將控制項類型設為「本地清單」。



2. 按一下「新增」按鈕，以新增多個值。使用向上和向下箭頭按鈕，來變更清單中項目的位置。

在「值」欄中，輸入要寫入身份儲存區的值。它只可以包含小寫字母、數字和底線 (_) 字元。

3. 在「標籤」欄中，輸入要在使用者介面中顯示的文字。

範圍：搭配使用「範圍」控制項類型和「整數」資料類型，將使用者輸入限制為循序值範圍。您會提供範圍的起始和結束值。

使用 DNLookup 控制項類型

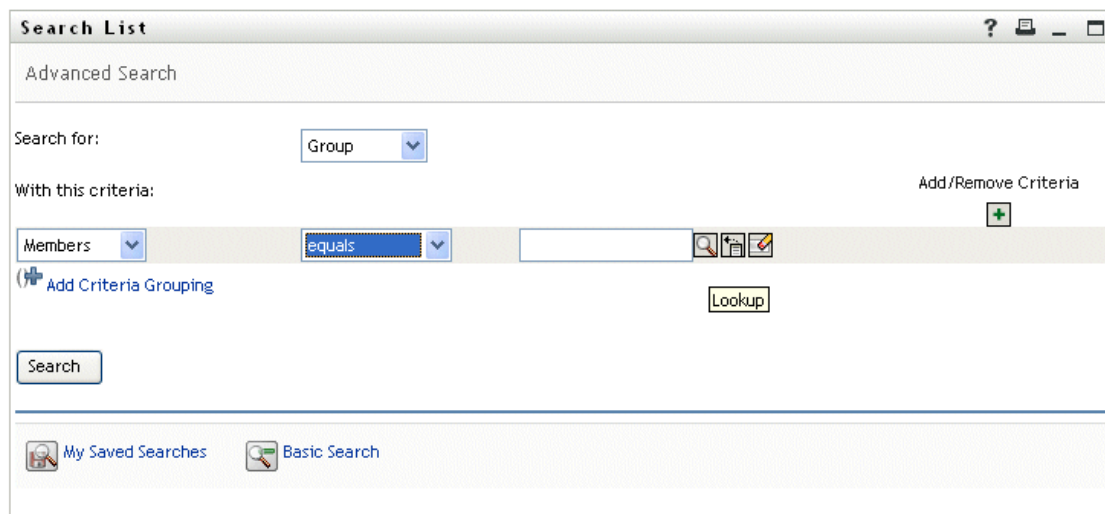
當您將控制項類型定義為 DNLookup 時，表示：

- ◆ 在此屬性上搜尋時，使用者可以從可能值的清單進行選取。
- ◆ 建立、填入或刪除此屬性時，會視使用者動作（建立、刪除、更新）而適當更新相關實體上的屬性，以維護參考完整性。

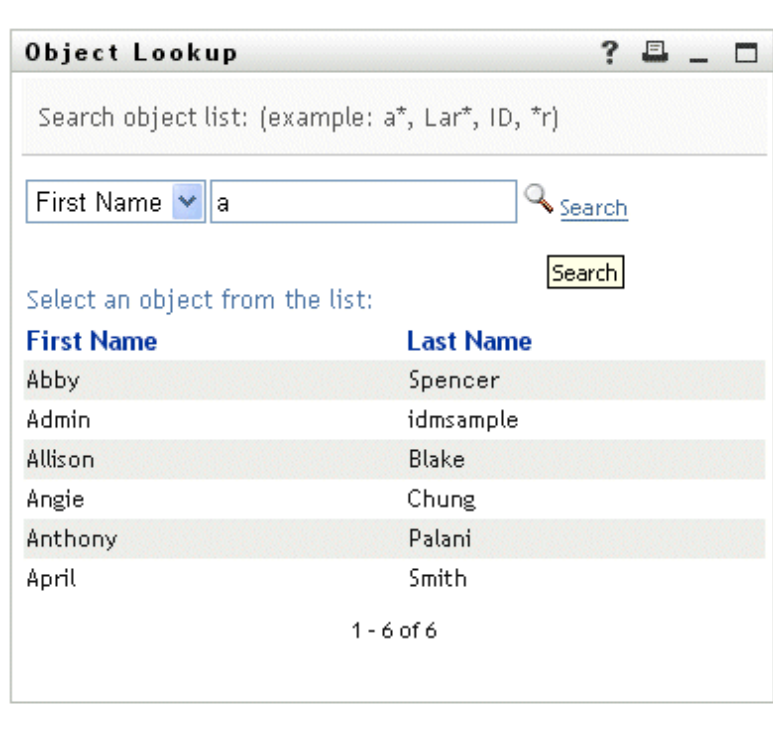
選項清單的 DNLookup

安裝的使用者應用程式包含「使用者」和「群組」的實體定義。「使用者」實體定義包含定義為 DNLookup 控制項類型之稱為「群組」的屬性。這可讓任何身份入口網站應用程式為特定使用者提供群組的選擇清單。例如，使用者選擇進行「目錄搜尋」。他們想要在群組

中尋找使用者，但是不瞭解群組名稱。他們會選取「使用者」做為要搜尋的物件，並併入「群組」做為搜尋準則，如下所示：



因為針對「使用者」實體，將「群組」定義為 DNLookup 控制項類型，所以會顯示「查閱」圖示。如果使用者選取它，則會顯示可能群組的清單：



使用者可以從清單選取群組。

用於參考完整性的 DNLookup

因為 LDAP 可讓群組關係雙向映射，所以更新和同步化的 DNLookup 很重要。例如，可能會設定您的資料，以便：

- ◆ 使用者物件包含群組屬性。群組屬性：
 - ◆ 為多值的
 - ◆ 列出使用者所屬的所有群組
- ◆ 群組物件包含使用者屬性。使用者屬性：
 - ◆ 為多值的
 - ◆ 列出屬於群組的所有使用者

這表示您在使用者物件上具有顯示使用者所屬之所有群組的屬性，而在「群組」物件上，您具有包含該群組之所有成員的 DN 屬性。

當使用者申請更新時，使用者應用程式必須承認關係，並確保同步化目標和來源屬性。在 DNLookup 中，您將指定必須同步化的兩個屬性。您可以使用此技術，提供任何相關物件（不僅是群組結構物件）之間的同步化。您可以指定「DNLookup 關聯式完整性」內容參考中描述的進階 DNLookup 內容，來建立此類的 DNLookup 控制項類別。

DNLookup 內容參考

「DNLookup 顯示」內容為：

欄位	定義
查詢實體	要搜尋的實體名稱，例如，「任務群組」實體包含「任務管理員」的屬性。若要填入該欄位，您需要瞭解哪些使用者為「任務管理員」。
詳細資料實體	實體鍵，當使用者藉由按一下使用者應用程式中的超文字連結而申請更多資訊時，您想要顯示其詳細資料。當您定義 DNLookup 時，身份入口網站應用程式可以提供超文字連結，讓使用者顯示已連結物件的詳細資料。
要顯示的屬性	選擇搜尋完成時要顯示的一或多個屬性。
執行自動查詢	定義「要顯示的屬性」（上述）的顯示方式。 <ul style="list-style-type: none">◆ 選取：執行實體的自動查詢並在可選取清單中呈現結果。如果傳回的資料數量很大，則您可能不想選擇此選項，因為此選項會強制使用者在大型結果集中捲動。◆ 不選：可讓使用者指定實體查詢的搜尋準則，然後在可選取清單中呈現結果。

「DNLookup 關聯式完整性」內容：這些內容用於同步化兩個物件（例如，群組和群組成員）之間的資料。

內容	定義
要更新的來源屬性	要更新的屬性名稱。屬性必須包含「要更新的目標屬性」的 DN 參考。這對同步化兩個不同物件上的屬性來說是必要的。

內容	定義
要更新的目標屬性	必須與「 要更新的來源屬性 」一起更新之屬性的名稱。此名稱是 LDAP 屬性名稱。這對同步化兩個不同物件上的屬性來說是必要的。屬性必須包含 DN 參考。
目標輔助類別 (如果有的話)	包含「 要更新的目標屬性 」的輔助類別名稱。

4.4 使用清單

清單節點可讓您定義全域清單的內容。Identity Manager 使用者應用程式使用全域清單來：

- ◆ 提供屬性值清單。在使用者介面中顯示屬性以進行編輯時，可能的值會以下拉式清單的形式顯示。
- ◆ 用於定義可用於 iManager 之「提供申請組態」外掛程式的類別。這是特殊清單。如需詳細資訊，請參閱「[關於提供類別清單](#)」，第 93 頁。

若要建立新的全域清單，請執行下列動作：

- 1 以下列其中一種方式啟動「新清單精靈」：

從「提供檢視窗」：

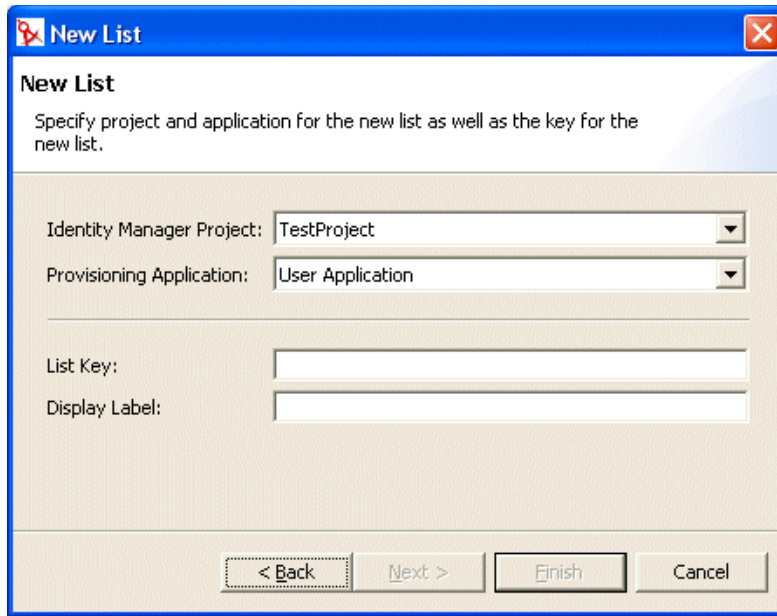
- ◆ 選取「檔案 > 新增 > 提供」。選擇「目錄抽象層清單」，然後按「下一步」。
- ◆ 選取「清單」節點，按一下滑鼠右鍵，並選擇「新增」。

從「目錄抽象層編輯器」：

- ◆ 按一下「新清單」按鈕。
- ◆ 選取「清單」節點，按一下滑鼠右鍵，並選擇「新增清單」。

即會顯示「新清單」對話方塊。

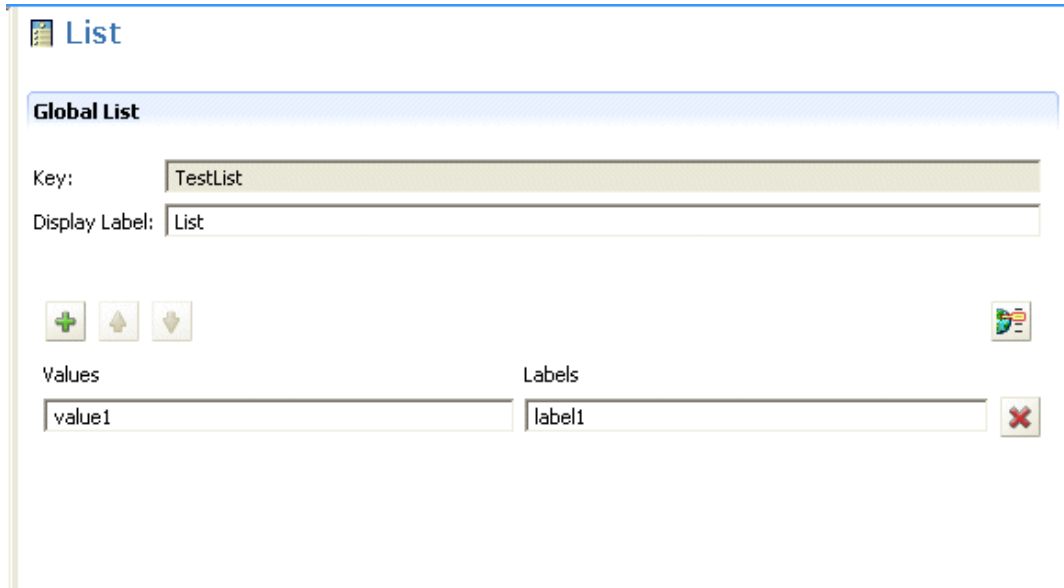
附註：如果從「檔案」功能表啟動，則對話方塊包含以其中一種其他方式啟動時未顯示的欄位。



2 完成面板，如下所示：

欄位	描述
Identity Manager 專案和提供應用程式	在您需要新增實體和屬性的位置，選取 Identity Manager 專案和提供應用程式。 附註：當您從「檔案」功能表啟動精靈時會顯示這些欄位。
清單鍵	清單的唯一識別碼。
顯示標籤	在使用者介面中參考此清單時所使用的字串。

3 按一下「完成」。即會顯示「全域清單」內容表。



4 完成下列欄位：

欄位	描述
顯示標籤	此清單的名稱，如 Designer 中所顯示。
標籤	要在使用者介面中顯示的清單項目文字。
值	要儲存在身份儲存區中的清單項目值。它只可以包含小寫字母、數字和底線 (_) 字元。

目前您可以在設計環境中使用該清單。

5 儲存專案。

附註：若要在執行時期環境中可以使用該清單，您必須部署它。

4.4.1 關於偏好的地區設定清單

「偏好的地區設定」清單代表預設語言，如果瀏覽器語言不是其中一種受支援的語言，則會使用該預設語言。在使用者應用程式中，此清單的內容會依「編輯使用者」動作的預設組態顯示。

4.4.2 關於提供類別清單

「提供類別」清單會定義協助您組織「提供資源(授權)」和「提供申請」的類別集。此清單中的類別顯示於：

- ◆ *iManager*：「提供申請組態」外掛程式
- ◆ 使用者應用程式：「申請與核准」索引標籤

您無法變更「提供申請」清單鍵，但可以將多個項目新增至清單，或變更現有的類別值和標籤。

若要修改「提供類別清單」的內容，請執行下列動作：

- 1 確保在編輯器中開啓正確的專案。
- 2 按一下「清單節點」。
- 3 選取「提供類別」。
- 4 使用全域清單內容窗格進行修改。

附註：「值」欄位用於填入類別鍵。因為類別鍵中只有小寫字母、數字和底線 (_) 字元是有效的字元，所以「值」欄位限制您只能使用這些字元。在內部，將類別鍵用做類別的識別碼。

- 5 儲存然後部署您的變更。記住要更新應用程式伺服器的快取。
部署變更之後，就會在使用者應用程式和 iManager 外掛程式中有所反映。

4.5 使用組織圖關係

「組織圖關係」節點可讓您定義在目錄抽象層中定義之實體間的階層式關係。可以是相似實體 (例如，使用者 / 使用者) 或非相似實體 (例如，使用者 / 設備) 之間的關係。

針對使用者應用程式，定義下列關係：

- ◆ 群組的成員資格
- ◆ 經理與員工
- ◆ 使用者群組

為了順利地部署關係，必須先部署關係的所有元件 (實體和屬性)。

若要建立新關係，請執行下列動作：

- 1 以下列任何方式建立新關係：

從「提供檢視窗」：

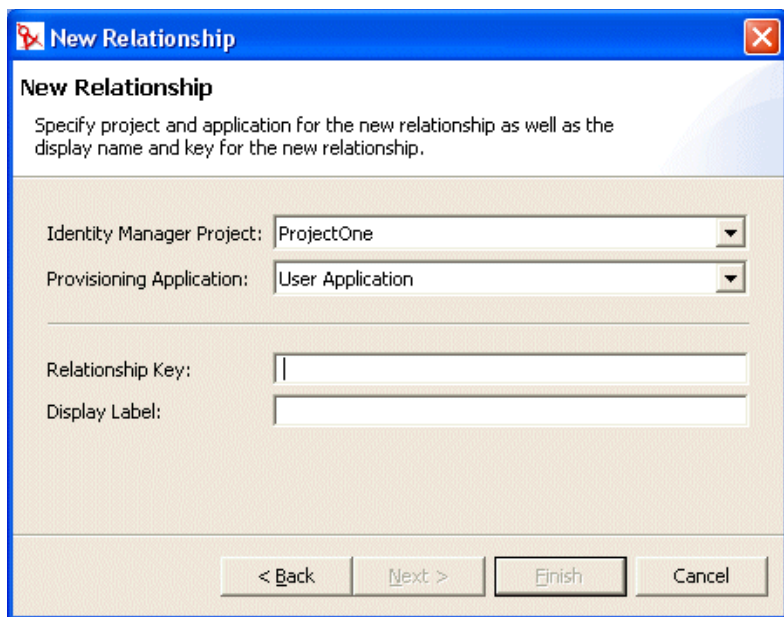
- ◆ 選取「檔案 > 新增 > 提供」。選擇「目錄抽象層關係」，然後按「下一步」。
- ◆ 選取「組織圖關係」節點，按一下滑鼠右鍵，並選擇「新增」。

從「目錄抽象層編輯器」：

- ◆ 按一下「新增關係」按鈕。
- ◆ 選取「組織圖關係」節點，按一下滑鼠右鍵，並選擇「新增關係」。

即會顯示「新關係」對話方塊。

附註：從「檔案」功能表啓動時，對話方塊會包含以其中一種其他方式啓動時未顯示的欄位。

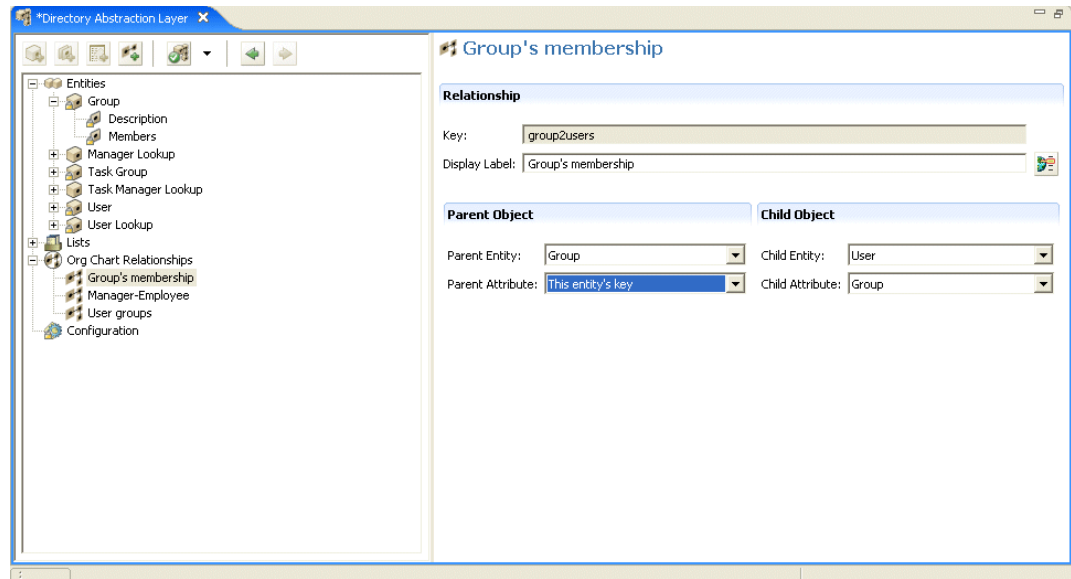


2 完成面板，如下所示：

欄位	操作
Identity Manager 專案和提供應用程式	確保選取正確的 Identity Manager 專案和「提供應用程式」。 附註：當您從「檔案」功能表建立關係時，會顯示此欄位。
關係鍵	針對關係鍵輸入唯一值。
顯示標籤	鍵入 Identity Manager 使用者介面上顯示關係時要顯示的字串。

3 按一下「完成」。

關係便會建立，並開啓其內容表，以供編輯。



4.5.1 關係內容參考

欄位	描述
關係鍵	<p>關係的唯讀唯一識別碼。</p> <p>提示：您要在「組織圖入口網站應用程式」優先設定表中指定此值。</p>
顯示標籤	<p>指定其他身份入口網站應用程式參考此關係時要顯示的名稱。例如，使用者從「詳細資料」入口網站應用程式按一下「選擇組織圖」圖示時，會顯示此值。</p> <p>按一下「當地語系化」，以提供該顯示標籤文字的翻譯。</p>
父代實體	<p>從下拉式清單中選擇實體。</p> <p>您選擇的實體會成為組織圖階層中的父代物件。例如，在 Manager-Employee 關係中，「父代實體」是「使用者」。而在 Group-Member 關係中，「父代實體」是「群組」。</p> <p>目錄抽象層要求：此清單中的實體是在目錄抽象層中定義之實體的子集。父代實體必須選取檢視存取內容 (true)</p>
父代屬性	<p>從下拉式清單中選擇屬性。</p> <p>此屬性用來尋找相符的子代實體。當此屬性的值符合子代實體屬性相對應的值時 (請參閱下述「子代屬性」)，便可以建立關係。</p> <p>目錄抽象層要求：此屬性清單是使用選定「父代實體」的屬性填入的。它僅包含定義為 DNLookup 控制類型的屬性</p>

欄位	描述
子代實體	選擇要成為階層中子代物件的實體。若為 Manager-Employee 關係，該實體是使用者。若為 Employee-Resources 關係，該實體是「設備」。 此實體必須包含與「父代屬性」相關的屬性。
子代屬性	選擇符合「父代屬性」的屬性。 這會指定子代實體上用來尋找相符父代實體的屬性。當此屬性的值符合父代實體屬性相對應的值時(請參閱上述「父代屬性」)，便可以建立關係。

附註：「組織圖」入口網站應用程式並不完全支援動態群組。您無法將動態群組定義為關係中的「父代實體」，但是可以將動態群組定義為關係中的子代實體。

若要刪除關係，請執行下列動作：

- 1 選取要刪除的關係。
- 2 按一下滑鼠右鍵，並選擇「刪除」。

4.6 使用組態設定

「組態」節點可讓您設定使用者應用程式的一般組態內容。包含：

內容	描述
預設的「我的設定檔」實體	定義使用者按一下使用者介面中「 我的設定檔 」時要顯示的實體。 此欄位會限制為僅顯示物件類別為使用者 (或 LDAP <code>inetOrgPerson</code>) 的實體。
預設的地區設定	定義用來顯示使用者應用程式之顯示標籤的預設語言。如果瀏覽器設定的語言不受支援，便會改用此地區設定。 附註：瀏覽器的地區設定會置換受支援語言的預設地區設定。
容器類別	這會為「建立使用者或群組」動作提供容器類別選擇清單的內容。使用者可以從選擇清單中選取容器，做為放置新建立物件的位置。

4.7 當地語系化顯示文字

目錄抽象層編輯器可提供簡便方法，將下列各項之顯示文字予以當地語系化：

- ◆ 實體和屬性顯示標籤
- ◆ 組織圖關係名稱
- ◆ 全域和本地清單項目

4.7.1 支援的語言

您可以將顯示文字當地語系化為下列一種或多種語言：

- ◆ 英文

- ◆ 法文
- ◆ 德文
- ◆ 義大利文
- ◆ 日文
- ◆ 韓文
- ◆ 葡萄牙文
- ◆ 俄文
- ◆ 簡體中文
- ◆ 西班牙文
- ◆ 繁體中文

4.7.2 當地語系化文字

目錄抽象層編輯器可提供數種方式來當地語系化抽象層定義。您可以下列方式來存取當地語系化對話方塊：

定義下列項目的當地語系化文字	動作
目錄抽象層中每個可當地語系化的項目	<ul style="list-style-type: none"> ◆ 按一下「設定全域當地語系化」(位於目錄抽象層編輯器工具列上)。 <p>請確定先選取「目標語言」,然後在目標欄位中輸入當地語系化的文字。</p>
特定實體、關係或清單	<ul style="list-style-type: none"> ◆ 從目錄抽象層編輯器網路樹檢視窗中,選取要當地語系化的物件。 ◆ 按一下滑鼠右鍵,並選取「當地語系化」。 <p>請確定先選取「目標語言」,然後在目標欄位中輸入當地語系化的文字。</p>
單一顯示標籤	<ul style="list-style-type: none"> ◆ 選取特定實體或屬性。 ◆ 按一下「當地語系化顯示標籤」(位於內容窗格的「顯示標籤」欄位旁邊)。

這些對話方塊外觀上雖然稍微有些差異,但是每個對話方塊都包含下列欄位：

- ◆ 原始：通常是物件類型(例如,實體、清單或關係)和鍵
- ◆ 來源：要轉譯的文字(顯示標籤)
- ◆ 目標語言：其中一種支援的語言
- ◆ 目標：轉譯文字

4.8 輸入、驗證和部署目錄抽象層定義

輸入、驗證和部署目錄抽象層定義是從 Designer 的「提供檢視窗」執行的動作。

- ◆ 「[關於輸入](#)」,第 99 頁
- ◆ 「[關於驗證](#)」,第 101 頁

- ◆ 「關於部署」，第 101 頁

4.8.1 關於輸入

輸入功能可讓您輸入現有的定義集。下列情況下，您可能要使用輸入：

- ◆ 您要以已部署的專案為基礎，開始新的專案。
- ◆ 您要與處理相同專案的其他開發人員共享定義。例如，其他開發人員新增屬性至使用者實體，或新增全域清單。如果該開發人員部署新定義至身份儲存區，則您可以輸入該定義，並確保您和他使用的是相同的定義。

若要輸入現有的定義，請執行下列動作：

- 1 開啓「提供檢視窗」。
- 2 決定您是否要輸入：
 - ◆ 完整的定義集
 - ◆ 一種定義類型集，例如全部實體或全部關係。
 - ◆ 特定物件（例如「使用者」實體）
- 3 若要輸入：
 - ◆ 特定物件，請從清單中選取該物件，按一下滑鼠右鍵，並選取「輸入物件」。
 - ◆ 完整的定義集，請選取「目錄抽象層」節點，按一下滑鼠右鍵，並選取「全部輸入」或「輸入物件」。
- 4 按一下 eDirectory 的「瀏覽」圖示，導覽至 DirectoryModel 節點，並選取要輸入的物件，然後按一下「確定」。
 - ◆ 如果物件相符，系統會通知您不存在差異，且不會繼續輸入。
 - ◆ 如果物件不符，則您可以確認要輸入的物件。檢視選定要輸入的項目，進行所需的任何變更，然後按一下「確定」。

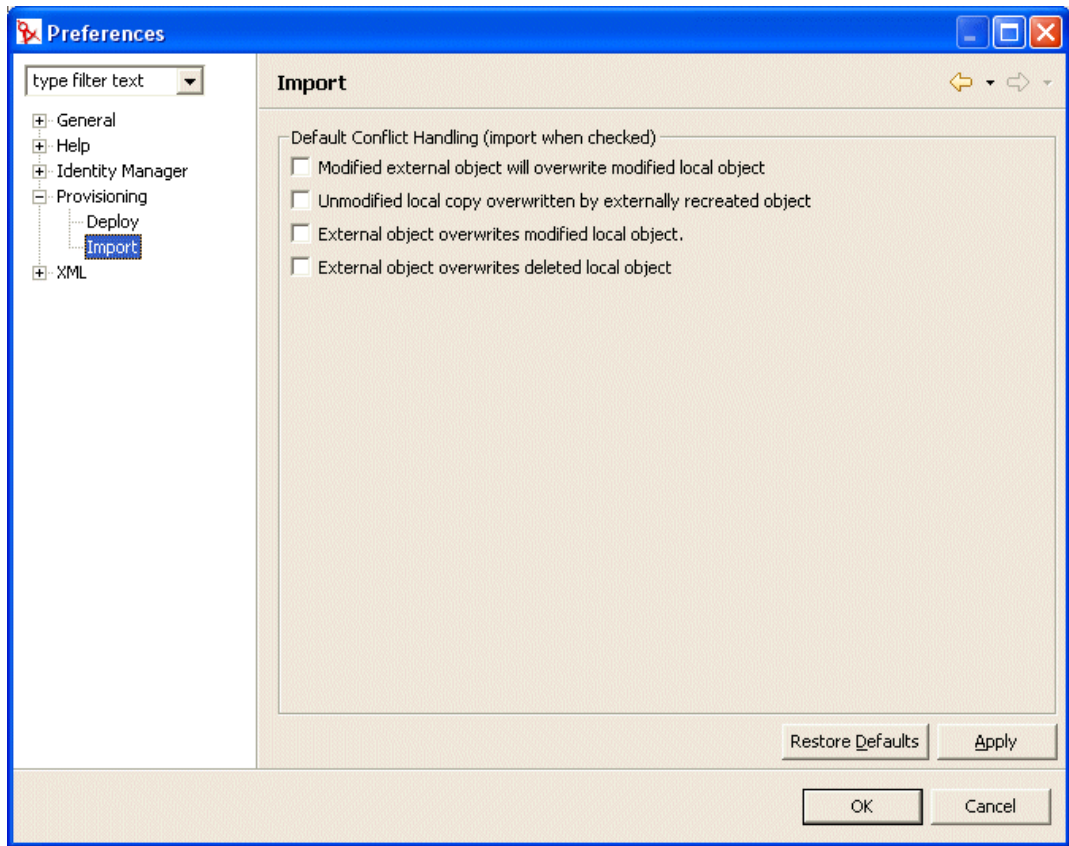
設定輸入優先設定

輸入優先設定可讓您指定您希望 Designer 如何解決身份儲存區中資料與本地目錄抽象層檔案之間的衝突。因為不同的使用者和工具都可以存取身份儲存區的目錄抽象層定義，所以會發生這些衝突。其他管理員或開發人員可以使用 iManager 工具或他們自己的本地 Designer 型專案，來變更此定義。當本地檔案系統上的定義與身份儲存區上的定義發生衝突時，這些優先設定可讓您指定如何處理這些衝突。

若要設定「輸入」優先設定，請執行下列動作：

- 1 選擇「視窗 > 優先設定」。

2 開啓網路樹的「提供」節點，並按一下「輸入」。



3 選擇優先設定：

優先設定	描述
已修改的外部物件會覆寫已修改的本地物件	本地檔案和身份儲存區定義都包含變更。尚未部署本地變更。 如果您想讓身份儲存區物件覆寫您對本地檔案所做的變更，請選取此選項。
在外部重新建立的物件會覆寫未修改的本地副本	身份儲存區物件會被刪除，然後重新建立。本地檔案集包含未變更的原始定義。 如果您想讓輸入覆寫本地副本，請選取此選項。
外部物件會覆寫已修改的本地物件	本地檔案包含未部署至身份儲存區的變更。如果您想讓輸入覆寫本地檔案，請選取此選項。
外部物件會覆寫已刪除的本地物件	您已在本地刪除定義，但是尚未部署變更。這表示物件仍然存在於身份儲存區中。 如果您想將身份儲存區物件複製到本地檔案系統，請選取此選項。如果您選擇此選項，則會遺失未部署的變更。

4.8.2 關於驗證

您可以先在本地檔案系統上驗證目錄抽象層資料定義，然後再嘗試部署它們。驗證包括：

- ◆ 驗證 XML 格式是否正確，且符合定義實體、屬性、清單、關係等所需元素的綱要。
- ◆ 檢查每個實體，以確保其他實體和全域清單的參考都是有效的。

例如，當驗證實體及其屬性時，驗證器會檢查透過「編輯實體」、「DN 查閱」和「實體詳細資料」欄位對其他實體進行的所有參考，是否都參考實際存在的實體。

- ◆ 確定每個實體都至少已定義一個屬性。
- ◆ 確定每個本地和全域清單都至少包含一個項目。

您可以從「提供檢視窗」中選擇性地驗證定義。若要驗證，請執行下列動作：

- ◆ 節點內的所有項目，請選取該節點，按一下滑鼠右鍵，並選取「驗證」。
- ◆ 節點內的單一物件，請選取該物件，按一下滑鼠右鍵，並選取「驗證」。

您可以從目錄抽象層工具列按一下「驗證抽象層」按鈕，來驗證所有定義。

附註：驗證並不會檢查身份儲存區是否存在任何物件。

4.8.3 關於部署

您必須先將定義部署至身份儲存區，才能看到 Identity Manager 使用者應用程式內產生的變更。

若要將定義集部署至身份儲存區，請執行下列動作：

- 1 使用目錄抽象層編輯器，儲存您所做的所有變更。

如果您未儲存變更即嘗試部署，則編輯器會顯示對話方塊表示定義尚未儲存。它會提示您儲存最近的變更。如果您不儲存變更，仍會將物件部署至伺服器，但是部署的內容不會包含未儲存的變更。選擇不儲存變更並不會取消部署。

- 2 開啓「提供檢視窗」。
- 3 決定是要使用目錄抽象層編輯器部署已定義的所有物件還是子集。
 - ◆ 若要部署所有物件，請執行下列動作：
選取根部節點，按一下滑鼠右鍵，並選擇「全部部署」
 - ◆ 部署特定實體、關係、清單或組態設定：
選取該項，按一下滑鼠右鍵，並選擇「部署物件」。

系統可能會提示您提供身份儲存區身分證明。編輯器會執行驗證，並在對話方塊中顯示任何驗證訊息。選取 / 不選要部署的項目，以回應驗證訊息。在您選取並提交部署之後，系統會通知您部署是成功還是失敗。

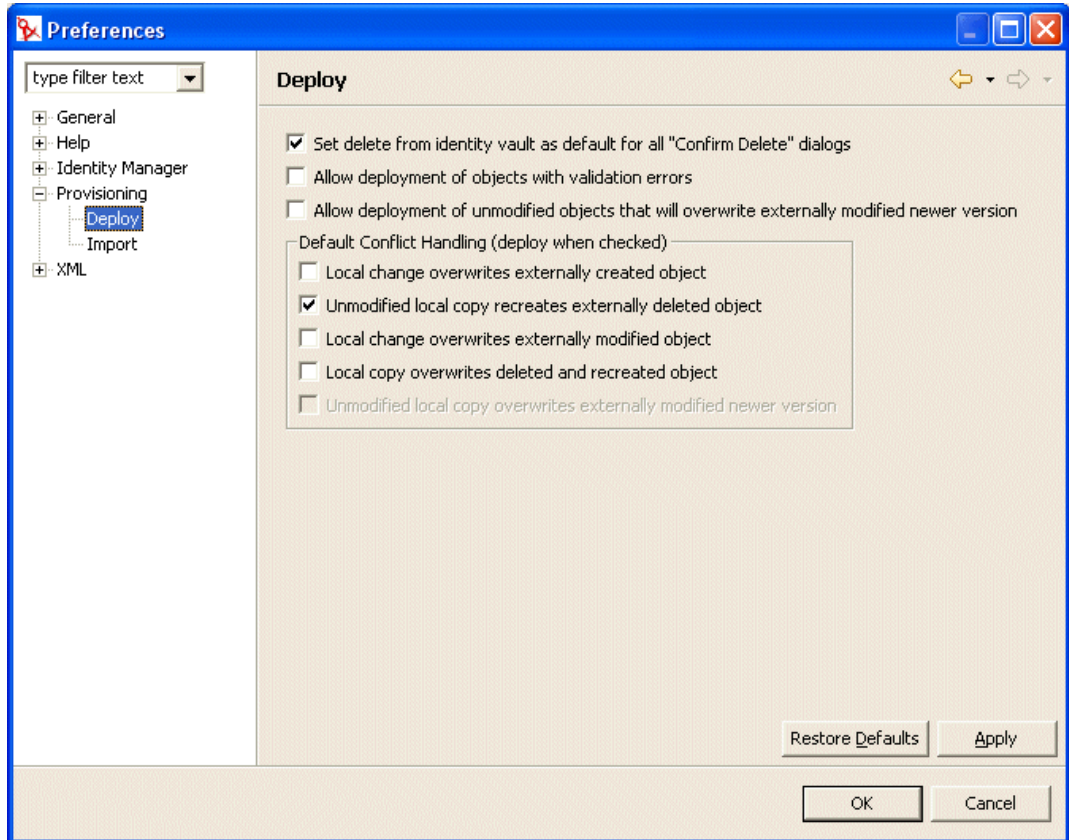
設定部署優先設定

部署優先設定可讓您指定您希望 Designer 如何解決身份儲存區中資料與本地目錄抽象層檔案之間的衝突。因為其他使用者已將變更部署至身份儲存區，但是本地檔案系統的定義中未

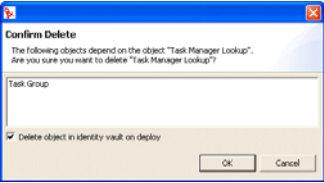
反映這些變更，所以可能會發生衝突。若要確保以您想要的方式處理衝突，您可以設定優先設定，以指定衝突的解決方法。

若要設定「部署」優先設定，請執行下列動作：

- 1 選擇「視窗 > 優先設定」。
- 2 開啓網路樹的「提供」節點，並按一下「部署」。



- 3 指定一般部署優先設定：

優先設定	描述
將「從身份儲存區中刪除」設為所有「確認刪除」對話方塊的預設值	<p>如果您嘗試在「提供檢視窗」或目錄抽象層編輯器中刪除物件，系統會提示您確認刪除，顯示的對話方塊如下所示：</p>  <p>此優先設定會決定預設是否會選取標示為「部署時刪除身份儲存區中的物件」的刪除確認對話核取方塊。選取此優先設定表示預設值是一律刪除身份儲存區物件。</p> <p>一律刪除本地物件。</p>
允許部署具有驗證錯誤的物件	<p>選取：如果您要部署無法驗證的物件，請選取此選項。部署時，Designer 會遵循「輸入、驗證和部署目錄抽象層定義」，第 98 頁中概述的驗證規則，來驗證正在部署的定義。</p> <p>不選：防止部署無法驗證的定義。</p>
允許部署會覆寫在外部修改之較新版本的未修改物件	<p>選取：如果本地檔案尚未變更，但是身份儲存區物件已變更。您想要本地檔案覆寫身份儲存區檔案嗎？如果是，請選取此優先設定。</p> <p>不選：如果您要保留較新的身份儲存區版本。</p> <p>選取此項時，您還可以同時選取衝突解決優先設定「未修改的本地副本會覆寫在外部修改的較新版本」，將此項設為預設行為。</p>

4 指定衝突解決優先設定：

優先設定	描述
本地變更會覆寫在外部建立的物件	<p>選取：如果想要讓您正在部署的物件覆寫身份儲存區中的物件。</p> <p>不選：發生此衝突時不會進行部署。</p>
未修改的本地副本會重新建立在外部刪除的物件	<p>選取：如果想讓您正在部署的本地物件建立已從身份儲存區中刪除的物件。</p> <p>不選：發生此衝突時不會進行部署。</p>
本地變更會覆寫在外部修改的物件	<p>選取：如果想要一律部署本地定義，即使其他使用者已變更身份儲存區。</p> <p>不選：發生此衝突時不會進行部署。</p>
本地副本會覆寫已刪除或已重新建立的物件	<p>選取：如果想要一律部署本地物件，即時身份儲存區物件已被刪除，或者已被刪除但已重新建立。</p> <p>不選：發生此衝突時不會進行部署。</p>

優先設定	描述
未修改的本地副本會覆寫在外部修改的較新版本	<p data-bbox="841 260 1414 317">僅當選取一般部署優先設定「允許部署會覆寫在外部修改之較新版本的未修改物件」時，才能設定此優先設定。</p> <p data-bbox="841 344 1414 426">選取：如果本地檔案尚未變更，但是身份儲存區物件已變更，且您一律要本地檔案覆寫身份儲存區檔案做為預設行為。</p> <p data-bbox="841 453 1305 478">不選：如果您要保留較新的身份儲存區版本。</p>

設定記錄

本章包含下列內容：

- ◆ 「關於事件記錄」，第 105 頁
- ◆ 「記錄至 Novell Audit 伺服器」，第 105 頁

5.1 關於事件記錄

Identity Manager 使用者應用程式會使用 *log4j* (The Apache Software Foundation 配送的開放原始碼記錄套件) 來實作記錄。在預設狀態下，事件訊息是以記錄層級 INFO 或更高，記錄至系統主控台和應用程式伺服器的記錄檔案。您也可以設定使用者應用程式的組態，以記錄至 Novell Audit。事件會記錄至所有已啓用的記錄器。

重要：如果您要記錄至 Novell Audit，建議您檢視 Novell Audit 文件 (<http://www.novell.com/documentation/nsureaudit>)。

5.1.1 關於記錄層級設定

主控台記錄包括同步化寫入。這表示記錄會成為處理器使用問題，同時也會成為阻礙。您可以修改 `<installdir>/jboss/server/IDMProv/conf/log4j.xml` 中的設定，將優先程度值的預設設定變更為 ERROR。找出如下所示的根部節點：

```
<root> <appender-ref ref="CONSOLE"/> <appender-ref ref="FILE"/> </root>
```

將優先程度值變更為：

```
<root> <priority value="ERROR"/> <appender-ref ref="FILE"/> </root>
```

指定一個值給根部可確保任何未明確指定層級的附加程式，都會繼承根部的層級。在預設狀態下，檔案附加程式並沒有指定的限定值層級，所以它會採用根部的限定值層級。根部中所包含具有層級限定值的任何附加程式都應該是 ERROR 或 WARN。WARN 以上的錯誤層級設定會影響效能。

5.2 記錄至 Novell Audit 伺服器

若要記錄至 Novell Audit 伺服器，請遵循下列步驟：

步驟	操作	相關資訊
1	將 Identity Manager 應用程式綱要做為記錄應用程式新增至 Novell Audit 伺服器	「將 Identity Manager 應用程式綱要做為記錄應用程式新增至 Novell Audit 伺服器」，第 106 頁

步驟	操作	相關資訊
2	在應用程式伺服器上設定 Novell Audit 平台代辦的組態	<p>會回報事件給 Novell Audit 的任何用戶端都需要「平台代辦」。您可以透過 logevent 組態 檔案設定平台代辦。此檔案會提供平台代辦與 Novell Audit 伺服器通訊所需的組態資訊。此檔案在應用程式伺服器上的預設位置是：</p> <ul style="list-style-type: none"> ◆ Linux：/etc/logevent.conf ◆ Windows：/<WindowsDir>/logevent.cfg (通常是 c:\windows) <p>確定在 LogHost 設定中指定 Novell Audit 伺服器 的 IP 位址或 DNS 名稱。例如：</p> <pre>LogHost=xxx.xxx.xxx.xxx</pre> <p>指定環境所需的其他設定。</p> <hr/> <p>重要：建立或修改 logevent 組態檔案之後，您必須重新啟動 JBoss 應用程式伺服器，這些變更才會生效。</p> <hr/> <p>如需 logevent 組態檔案結構的相關資訊，請參閱《Novell Audit 管理指南》中關於登入系統一章的設定平台代辦 (http://www.novell.com/documentation/nsureaudit) 一節。</p>
3	啟用 Novell Audit 記錄	「啟用 Audit 記錄」，第 107 頁

5.2.1 將 Identity Manager 應用程式綱要做為記錄應用程式新增至 Novell Audit 伺服器

若要設定 Audit 的組態，以使用 Identity Manager 使用者應用程式做為記錄應用程式，請遵循下列步驟：

- 1 找出下列檔案：

DirXML.lsc

平台	位置
Linux	安裝後：

/opt/novell/naudit/logschema/dirxml.lsc

平台	位置
Windows	在安裝媒體上： /nt/dirxml/nsure_audit/nauditextensions/lsc/ dirxml.lsc

- 2 使用網頁瀏覽器存取 *iManager*，並以管理員身份登入。
- 3 移至「角色和任務 > 稽核和記錄」，並選取「記錄伺服器選項」。
- 4 瀏覽至網絡樹中的「記錄服務容器」，並選取適當的「*Audit* 安全記錄伺服器」，然後按一下「確定」。
- 5 移至「記錄應用程式」索引標籤，然後選取適當的「容器名稱」，再按一下「新記錄應用程式」連結。
- 6 當「新記錄應用程式」對話方塊顯示時，請指定下列內容：

針對下列設定	執行下列動作
記錄應用程式名稱	鍵入對您環境有意義的任何名稱
輸入 LSC 檔案	使用「 瀏覽 」按鈕，以選取 DirXML.lsc 檔案

按一下「確定」。「記錄應用程式」索引標籤即會顯示新增的應用程式名稱。

- 7 按一下「確定」，以完成您的 Novell Audit 伺服器組態。
- 8 確定「記錄應用程式」的狀態設為「開啓」（狀態下面的圓圈應該是綠色。如果它是紅色的，請按一下，將其切換為「開啓」）。
- 9 重新啓動 Novell Audit 伺服器，以啓用新記錄應用程式設定。

5.2.2 啓用 Audit 記錄

在 Identity Manager 使用者應用程式中啓用 Novell Audit 記錄

- 1 以管理員使用者身份登入使用者應用程式。
- 2 選取「管理」索引標籤。
- 3 選取「記錄」索引標籤。
- 4 核取「同時傳送記錄訊息至 *Audit*」核取方塊（位於索引標籤的底部附近）。
- 5 對於任何後續應用程式伺服器重新啓動時，若要沿用變更，請確定已選取「沿用記錄變更」。

5.2.3 記錄的事件

Identity Manager 使用者應用程式會自動從工作流程、搜尋、詳細資料和密碼申請中記錄事件集。在預設狀態下，Identity Manager 使用者應用程式會自動將下列事件記錄至所有使用中記錄通道：

事件 ID	程序	事件	嚴重程度
31400	詳細資料入口網站應用程式	Delete_Entity	資訊
31401		Update_Entity	資訊
31410	變更密碼入口網站應用程式	Change_Password_Failure	錯誤
31411		Change_Password_Success	資訊
31420	忘記密碼入口網站應用程式	Forgot_Password_Change_Failure	錯誤
31421		Forgot_Password_Change_Success	資訊
31430	搜尋入口網站應用程式	Search_Request	資訊
31431		Search_Saved	資訊
31440	建立入口網站應用程式	Create_Entity	資訊
31520	工作流程	Workflow_Error	錯誤
31521		Workflow_Started	資訊
31522		Workflow_Forwarded	資訊
31523		Workflow_Reassigned	資訊
31524		Workflow_Approved	資訊
31525		Workflow_Refused	資訊
31526		Workflow_Ended	資訊
31527		Workflow_Claimed	資訊
31528		Workflow_Unclaimed	資訊
31529		Workflow_Denied	資訊
3152A		Workflow_Completed	資訊
3152B		Workflow_Timedout	資訊
3152C		User_Message	資訊
31533		Workflow_Retracted	資訊
3152D	提供	Provision_Error	錯誤
3152E		Provision_Submitted	資訊
3152F		Provision_Success	資訊
31530		Provision_Failure	錯誤
31531		Provision_Granted	資訊
31532		Provision_Revoked	資訊

事件 ID	程序	事件	嚴重程度
31450	安全性網路位置	Create_Proxy_Definition_Success	資訊
31451		Create_Proxy_Definition_Failure	錯誤
31452		Update_Proxy_Definition_Success	資訊
31453		Update_Proxy_Definition_Failure	錯誤
31454		Delete_Proxy_Definition_Success	資訊
31455		Delete_Proxy_Definition_Failure	錯誤
31456		Create_Delegatee_Definition_Success	資訊
31457		Create_Delegatee_Definition_Failure	錯誤
31458		Update_Delegatee_Definition_Success	資訊
31459		Update_Delegatee_Definition_Failure	錯誤
3145A		Delete_Delegatee_Definition_Success	資訊
3145B		Delete_Delegatee_Definition_Failure	錯誤
3145C		Create_Availability_Success	資訊
3145D		Create_Availability_Failure	錯誤
3145E		Delete_Availability_Success	資訊
3145F		Delete_Availability_Failure	錯誤

5.2.4 記錄報告

如果您將事件記錄到 Novell Audit 資料庫通道，則您可以執行資料報告。對於記錄到 Novell Audit 資料庫的資料，有數種方法可產生報告：

- ◆ 使用 Novell Audit Report 應用程式，執行您自己的報告，或執行預先定義的報告，如下面「預先定義的記錄報告」，第 109 頁中所述。
- ◆ 使用 iManager，選取「稽核和記錄 > 查詢」，針對已記錄的資料撰寫查詢。
- ◆ 針對已記錄的資料，撰寫您自己的 SQL 查詢。

預設的 Novell Audit 表格稱為 NAUDITLOG。

預先定義的記錄報告

下列預先定義的記錄報告是以 Crystal Reports (.rpt) 格式建立，用於過濾記錄到 Novell Audit 資料庫的資料：

報告名稱	描述
管理動作報告	顯示從 Identity Manager 使用者應用程式入口網站啓始的所有管理動作。此報告包含啓始動作的管理員。 它不包含使用 iManager 或 Designer for IDM 所進行的任何管理變更

報告名稱	描述
歷程核准流程報告	顯示指定時間範圍的所有核准流程活動。
資源提供報告	顯示所有提供活動，按照資源排序。
特定使用者稽核追尋	顯示與使用者相關的所有活動。活動包含提供和自助服務活動。
特定使用者提供報告	顯示特定使用者的所有提供活動。
使用者提供報告	顯示所有提供活動，按照使用者排序。

範例報告 以下是「特定使用者稽核追尋」報告的範例：

Novell® Audit Report for Identity Manager

Specific User Audit Trail

Report Period: - 10/13/2005 8:51:32AM

User ID: ablake

Report Last Modified: 10/13/2005

Report Generated On: 10/13/2005

Total pages: 8

Approval Flow

Workflow Event: fecedbe80a3d4abd83c9476a1b576ea2

Date / Time	Action	Initiator ID
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Denied	System

Workflow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator

Workflow Event: efaa8304e07641edb9e6375a1a36e396

Date / Time	Action	Initiator ID
10/12/2005 11:58:13AM	Workflow Started	cn=ablake,ou=users,ou=idm sample-qatest,o=novell
10/12/2005 11:58:13AM	Workflow Forwarded	Workflow Administrator

Workflow Event: ea341eb11a824e669e356837745fe264

Date / Time	Action	Initiator ID
9/27/2005 4:24:44PM	Workflow Started	cn=m m ackenzie,ou=users,ou=idm sample-Jeff,o=novell
9/27/2005 4:24:44PM	Workflow Forwarded	Workflow Administrator

Page 1 of 8

Specific User Audit Trail

報告檔案位置 報告檔案位於：

平台

位置

Windows

/nt/dirxml/reports

您可以使用這些報告做為範本，在 Crystal Reports Designer 中建立自定報告，或使用 *Audit Report (lreport.exe)* (隨 Novell Audit 提供的 Windows 程式)，來執行這些報告。預先定義的報告會查詢來自預設 Novell Audit 記錄資料庫 (名為 *naudit*) 和資料庫表格 (名為 *nauditlog*) 的資料。如果您的 Novell Audit 記錄資料庫具有不同的名稱，請使用 Crystal Reports Designer 中的「設定資料來源位置」功能表項目，以您環境中的資料庫名稱取代 *naudit* 資料庫名稱。

如需相關資訊，請參閱 Novell Audit 文件 (<http://www.novell.com/documentation/nsureaudit>) 中有關使用報告一節。

管理使用者應用程式



以下章節說明如何利用使用者介面的「管理」索引標籤，來設定 Identity Manager 使用者應用程式的組態，並對其進行管理。

- ◆ 第 6 章 「使用管理索引標籤」, 第 115 頁
- ◆ 第 7 章 「頁面管理」, 第 121 頁
- ◆ 第 8 章 「主題組態」, 第 155 頁
- ◆ 第 9 章 「入口網站應用程式管理」, 第 161 頁
- ◆ 第 10 章 「入口網站組態」, 第 181 頁
- ◆ 第 11 章 「安全性組態」, 第 187 頁
- ◆ 第 12 章 「記錄組態」, 第 191 頁
- ◆ 第 13 章 「快取組態」, 第 197 頁
- ◆ 第 14 章 「用於輸出和輸入入口網站資料的工具」, 第 205 頁

使用管理索引標籤

本章介紹 Identity Manager 使用者介面的「管理」索引標籤。您將瞭解如何使用「管理」索引標籤，來設定和管理 Identity Manager 使用者應用程式的組態。主題包含：

- ◆ 「關於管理索引標籤」，第 115 頁
- ◆ 「可以使用管理索引標籤的人員」，第 115 頁
- ◆ 「存取管理索引標籤」，第 116 頁
- ◆ 「您可以執行的管理動作」，第 118 頁

6.1 關於管理索引標籤

Identity Manager 使用者介面主要是由一般使用者存取，他們會使用該介面提供的索引標籤，進行身份自助服務和工作流程提供（具有 Identity Manager 的提供模組）。但是，這個瀏覽器為主的使用者介面也會提供「管理」索引標籤，管理員可以存取此索引標籤，來設定基礎 Identity Manager 使用者應用程式各種特性的組態。

例如，「管理」索引標籤可用來：

- ◆ 變更用於使用者介面外觀和操作的主題
- ◆ 自定一般使用者可用的身份自助服務功能
- ◆ 指定允許執行管理動作的人員
- ◆ 管理使用者應用程式及其執行方式的其他詳細資料

6.2 可以使用管理索引標籤的人員

Identity Manager 使用者介面的一般使用者看不到「管理」索引標籤。以下兩種使用者可以看見並存取此索引標籤：

- ◆ 使用者應用程式管理員

「使用者應用程式管理員」有權執行與 Identity Manager 使用者應用程式相關的所有管理功能。這包含存取 Identity Manager 使用者介面的「管理」索引標籤，以執行其支援的任何管理動作。

在安裝期間，會將某使用者指定為「使用者應用程式管理員」。安裝之後，該使用者可以使用「管理」索引標籤上的「安全性」頁面，視需要指定其他的「使用者應用程式管理員」。

如需詳細資料，請參閱第 11 章「安全性組態」，第 187 頁。

- ◆ 使用者應用程式管理員允許的使用者

必要時，「使用者應用程式管理員」可以指定權限，讓一或多個一般使用者能夠看見及存取「管理」索引標籤上的特定頁面。使用「管理」索引標籤上的「頁面管理」頁面，來指定這些權限。

如需詳細資料，請參閱第 7 章「頁面管理」，第 121 頁。

6.3 存取管理索引標籤

一旦您成為「使用者應用程式管理員」(或其他允許的使用者)，您便可以在需要管理 Identity Manager 使用者應用程式時，存取 Identity Manager 使用者介面的「管理」索引標籤。您只需要有受支援的網頁瀏覽器。

如需受支援網頁瀏覽器的清單，請參閱《Novell Identity Manager：安裝指南》。

附註：若要使用 Identity Manager 使用者介面，請確定您的網頁瀏覽器已啟用 *JavaScript*。

若要存取「管理」索引標籤，請執行下列動作：

- 1 在網頁瀏覽器中，前往 Identity Manager 使用者介面的 URL (如同在您網站設定的一樣)。例如：

`http://myappserver:8080/IDM`

即會顯示使用者介面的訪客歡迎頁面：



- 2 按一下頁面標題中的「登入」連結。

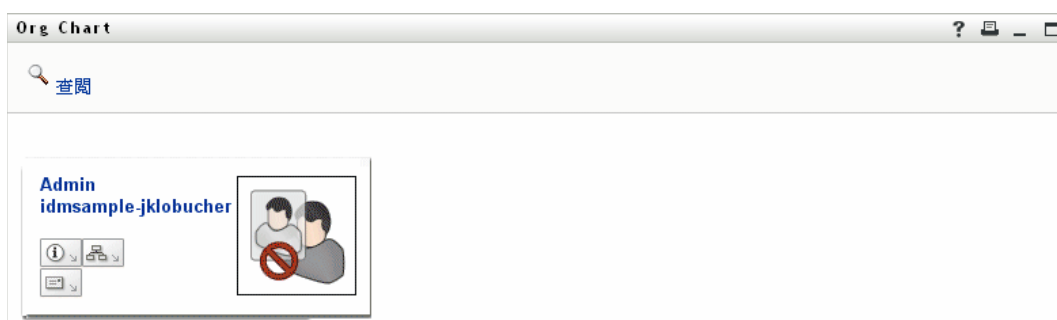
使用者介面會提示您輸入使用者名稱和密碼：



The image shows the Novell Identity Manager login interface. It features a blue header with the text "Novell® Identity Manager". Below the header, there are two input fields: "使用者名稱：" (Username) and "密碼：" (Password). A link for "忘記密碼?" (Forgot password?) is located below the password field. At the bottom left, there is a red "N" logo, and at the bottom right, there is a red button labeled "...登入" (Login).

- 3 輸入使用者應用程式管理員 (或具有部份「管理」索引標籤權限的使用者) 的使用者名稱和密碼，然後按一下「登入」。

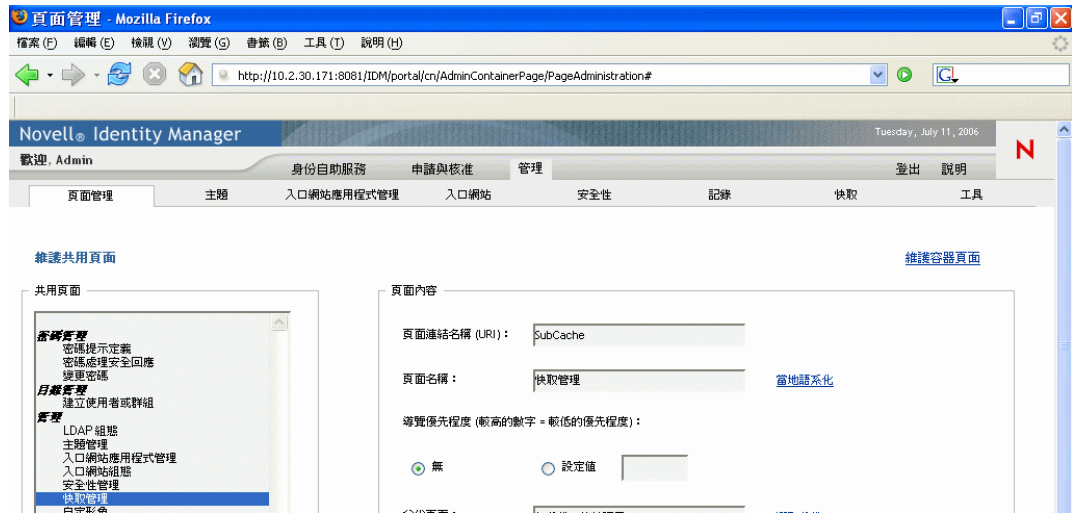
登入後，您會看見適合該使用者的使用者介面內容。例如：



在預設狀態下，您會在「身份自助服務」索引標籤處。

- 4 按一下「管理」索引標籤。

「管理」索引標籤會顯示您可以執行管理動作的功能表。每個選項都會顯示設定和控制的對應頁面。在預設狀態下，您會看到「頁面管理」頁面：



如需存取和使用 Identity Manager 使用者介面的一般資訊，請參閱《Identity Manager 使用者應用程式：使用者指南》。

6.4 您可以執行的管理動作

一旦您在「管理」索引標籤，便可以使用任何可用的動作，來設定 Identity Manager 使用者應用程式的組態，並對其進行管理。以下為其摘要：

動作	描述
頁面管理	控制在 Identity Manager 使用者介面中顯示的頁面，以及有權存取它們的人員 如需詳細資料，請參閱第 7 章「頁面管理」，第 121 頁。
主題	控制 Identity Manager 使用者介面的外觀和操作 如需詳細資料，請參閱第 8 章「主題組態」，第 155 頁。
入口網站應用程式管理	控制在 Identity Manager 使用者介面中可用的入口網站應用程式，以及有權存取它們的人員 如需詳細資料，請參閱第 9 章「入口網站應用程式管理」，第 161 頁。
入口網站	控制 Identity Manager 使用者應用程式的入口網站特性，並指定使用者應用程式如何連接到身份儲存區 (LDAP 提供者) 如需詳細資料，請參閱第 10 章「入口網站組態」，第 181 頁。
安全性	指定誰是 Identity Manager 使用者應用程式的「使用者應用程式管理員」 如需詳細資料，請參閱第 11 章「安全性組態」，第 187 頁。
記錄	控制您要讓 Identity Manager 使用者應用程式產生的記錄訊息層級，並指定是否要將那些訊息傳送至 Novell Audit 如需詳細資料，請參閱第 12 章「記錄組態」，第 191 頁。

動作	描述
快取	管理由 Identity Manager 使用者應用程式維護的各種快取 如需詳細資料，請參閱第 13 章 「快取組態」，第 197 頁。
工具	可讓您輸出或輸入 Identity Manager 使用者應用程式中所使用的入口網站內容 (頁面和入口網站應用程式) 如需詳細資料，請參閱第 14 章 「用於輸出和輸入入口網站資料的工具」，第 205 頁。

頁面管理

本章說明如何使用 Identity Manager 使用者介面「管理」索引標籤上的「頁面管理」頁面。主題包含：

- ◆ 「關於頁面管理」，第 121 頁
- ◆ 「建立和維護容器頁面」，第 129 頁
- ◆ 「建立和維護共用頁面」，第 137 頁
- ◆ 「指定頁面的許可」，第 145 頁
- ◆ 「設定群組的預設頁面」，第 150 頁
- ◆ 「選取容器頁面的預設共用頁面」，第 152 頁

如需存取和使用「管理」索引標籤的一般資訊，請參閱第 6 章「使用管理索引標籤」，第 115 頁。

7.1 關於頁面管理

您可以使用「頁面管理」頁面，來控制在 Identity Manager 使用者介面中顯示的頁面，以及具有許可存取它們的人員。使用者介面包含兩種類型的頁面：

頁面類型	描述
容器	容器頁面以一致的外觀和操作、公司品牌和導覽方法來包裝共用頁面。
共用	共用頁面會提供用於特定目的（例如更新使用者的設定檔）的一致內容集。因為它們提供可多個人員使用的服務，所以稱為共用頁面。

這兩種頁面類型都包含使用入口網站應用程式（隨插即用使用者介面元素的 Java 標準）格式的內容。

若要瞭解更多入口網站應用程式的相關資訊，請參閱第 9 章「入口網站應用程式管理」，第 161 頁和「入口網站應用程式參考資訊」，第 213 頁。

7.1.1 關於容器頁面

本節介紹在 Identity Manager 使用者介面中，具有重要作用的部份容器頁面：

- ◆ 「GuestContainerPage」，第 122 頁
- ◆ 「DefaultContainerPage」，第 124 頁
- ◆ 「管理容器頁面」，第 126 頁

請記住，必要時，您可以修改這些容器頁面。您也可以選擇新增自己的容器頁面。

若要瞭解使用容器頁面的相關資訊，請參閱「建立和維護容器頁面」，第 129 頁。

GuestContainerPage

在預設狀態下，當使用者在登入之前先到達 Identity Manager 使用者介面時，他們會看見名為 *GuestContainerPage* 的容器頁面。該容器頁面顯示如下：



在內部，GuestContainerPage 具有下列配置：



GuestContainerPage 配置會分成三個區域，顯示下列入口網站應用程式：

入口網站應用程式	描述
HeaderPortlet	顯示使用者介面的標題資訊和頂層索引標籤控制項
共用頁面導覽	顯示垂直功能表，使用者可以從中選取要顯示的共用頁面
入口網站頁面控制器	顯示使用者目前透過「共用頁面導覽」入口網站應用程式選取的共用頁面

請注意，在預設狀態下，使用者在登入之前，僅可在那些入口網站應用程式中看見下列各項：

- ◆ 標題中的單一連結：登入
- ◆ 單一共用頁面：歡迎

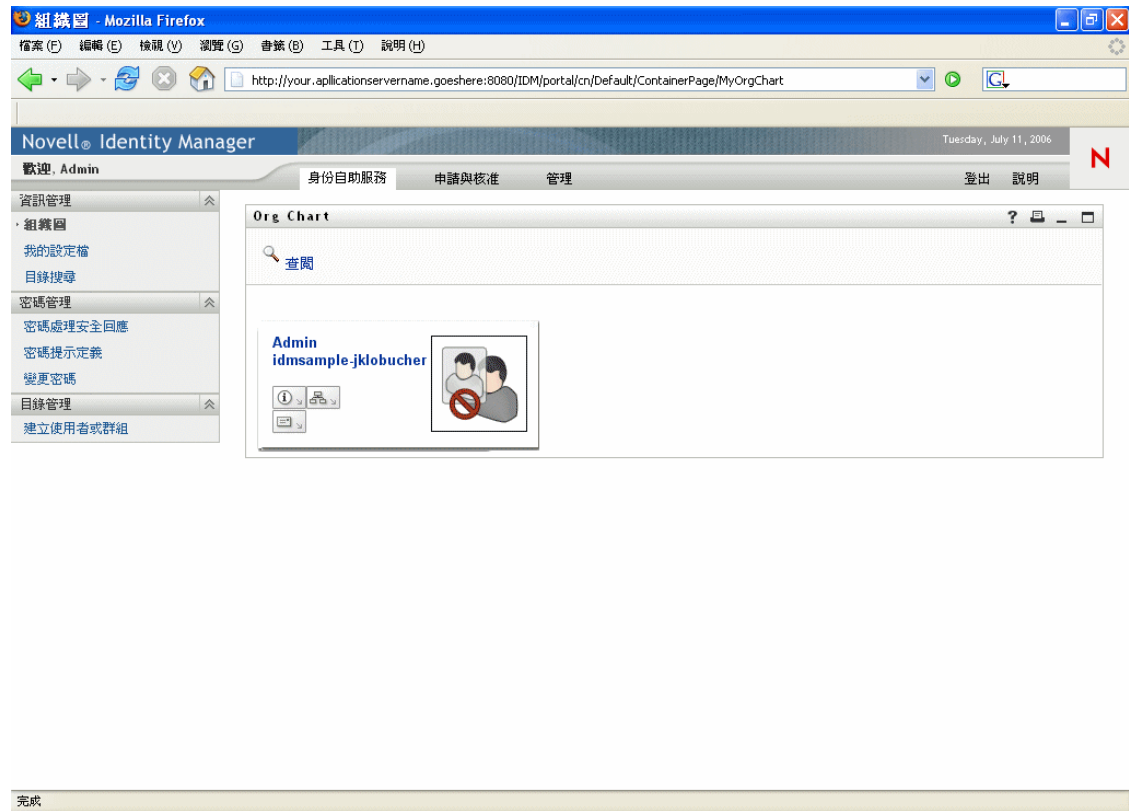
因為使用者尚未登入，所以「共用頁面導覽」入口網站應用程式只會顯示位於「訪客頁面」類別的共用頁面；它會過濾出所有其他類別。在預設狀態下，「歡迎」是「訪客頁面」類別中的唯一頁面。

登入之後，「共用頁面導覽」入口網站應用程式會過濾出「訪客頁面」類別。因此，它會顯示共用頁面的其他類別（按照其優先設定中所指定的）。

如需「共用頁面導覽」入口網站應用程式的相關資訊，請參閱第 15 章「關於入口網站應用程式」，第 215 頁。

DefaultContainerPage

在預設狀態下，當使用者在登入 Identity Manager 使用者介面之後，他們會前往名為 *DefaultContainerPage* 的容器頁面。該容器頁面顯示如下：



在內部，DefaultContainerPage 具有下列配置：



DefaultContainerPage 配置會分成三個區域，顯示下列入口網站應用程式：

入口網站應用程式	描述
HeaderPortlet	顯示使用者介面的標題資訊和頂層索引標籤控制項
共用頁面導覽	顯示垂直功能表，使用者可以從中選取要顯示的共用頁面
入口網站頁面控制器	顯示使用者目前透過「共用頁面導覽」入口網站應用程式選取的共用頁面
會期逾時警告	只要使用者的會期即將逾時，就會顯示警示訊息

請注意，在使用者登入之後，DefaultContainerPage 會自動在 HeaderPortlet 中開啓「身份自助服務」索引標籤。

管理容器頁面

在預設狀態下，當「使用者應用程式管理員」(和其他授權的使用者)按一下 *Identity Manager* 使用者介面的「管理」索引標籤時，他們會前往名為「管理容器頁面」的容器頁面。該容器頁面顯示如下：



在內部，「管理容器頁面」具有下列配置：



「管理容器頁面」配置會分成兩個區域，顯示下列入口網站應用程式：

入口網站應用程式	描述
HeaderPortlet	顯示使用者介面的標題資訊和頂層索引標籤控制項
管理清單顯示	顯示索引標籤的第二個層級，使用者可以從中選取要執行的管理動作
入口網站頁面控制器	顯示共用頁面，該頁面相當於使用者目前透過「管理清單顯示」入口網站應用程式選取的索引標籤
會期逾時警告	只要使用者的會期即將逾時，就會顯示警示訊息

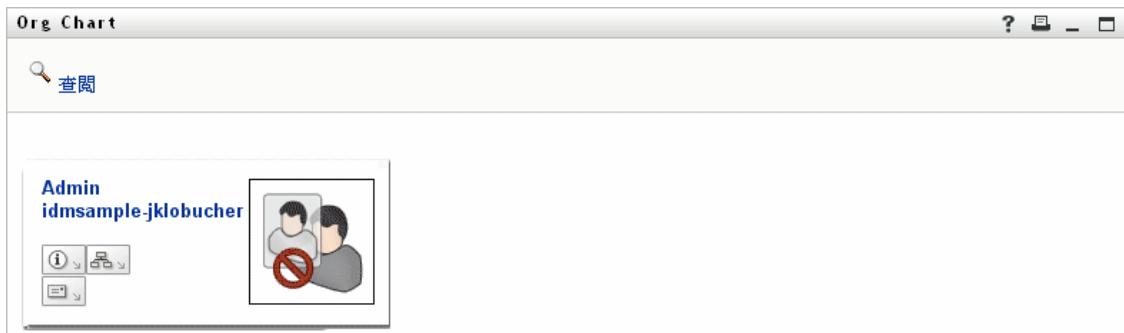
7.1.2 關於共用頁面

Identity Manager 使用者介面包含許多共用頁面，這些頁面會提供其容器頁面中的主要內容。必要時，您可以修改這些共用頁面。您也可以選擇新增自己的共用頁面。

若要瞭解使用共用頁面的相關資訊，請參閱「[建立和維護共用頁面](#)」，第 137 頁。

一般共用頁面

我們來看看其中一個共用頁面。「組織圖」是在使用者登入 Identity Manager 使用者介面之後，DefaultContainerPage 顯示的預設共用頁面。



在內部，「組織圖」具有下列配置：



「組織圖」配置僅包含一個區域，只顯示一個入口網站應用程式（「組織圖」入口網站應用程式）。

7.1.3 頁面使用的例外

在本章中，您會看到 Identity Manager 使用者介面的這些頂層索引標籤如何以頁面為基礎：

- 「身份自助服務」索引標籤會使用 *DefaultContainerPage*
- 「管理」索引標籤會使用「管理容器頁面」

但是，請注意，「申請與核准」索引標籤是以不同的結構為基礎，您無法透過「頁面管理」來處理該索引標籤。

7.2 建立和維護容器頁面

建立和維護容器頁面的程序包括下列步驟：

- 1 建立新的容器頁面，或選取現有的容器頁面（如「[建立容器頁面](#)」，第 129 頁中所述）。
- 2 新增內容（以入口網站應用程式的形式）至頁面（如「[新增內容至容器頁面](#)」，第 132 頁中所述）。
您也可能會要從頁面刪除內容（如「[刪除容器頁面的內容](#)」，第 133 頁中所述）。
- 3 選擇入口網站配置（如「[修改容器頁面的配置](#)」，第 134 頁中所述）。
- 4 在選定配置上安排內容的順序和位置（如「[安排容器頁面的內容](#)」，第 135 頁中所述）。
- 5 在瀏覽器中輸入容器頁面 URL，以立即顯示新的頁面（如「[顯示容器頁面](#)」，第 137 頁中所述）。

容器頁面和配置 容器頁面並不會嚴格受限於入口網站配置。這表示您可以切換容器頁面的配置，而不會遺失任何頁面內容。當您將新的配置套用至容器頁面時，新增至頁面的任何入口網站應用程式都會使用新的配置自動顯示。只是，您可能需要細調新配置中的內容位置。

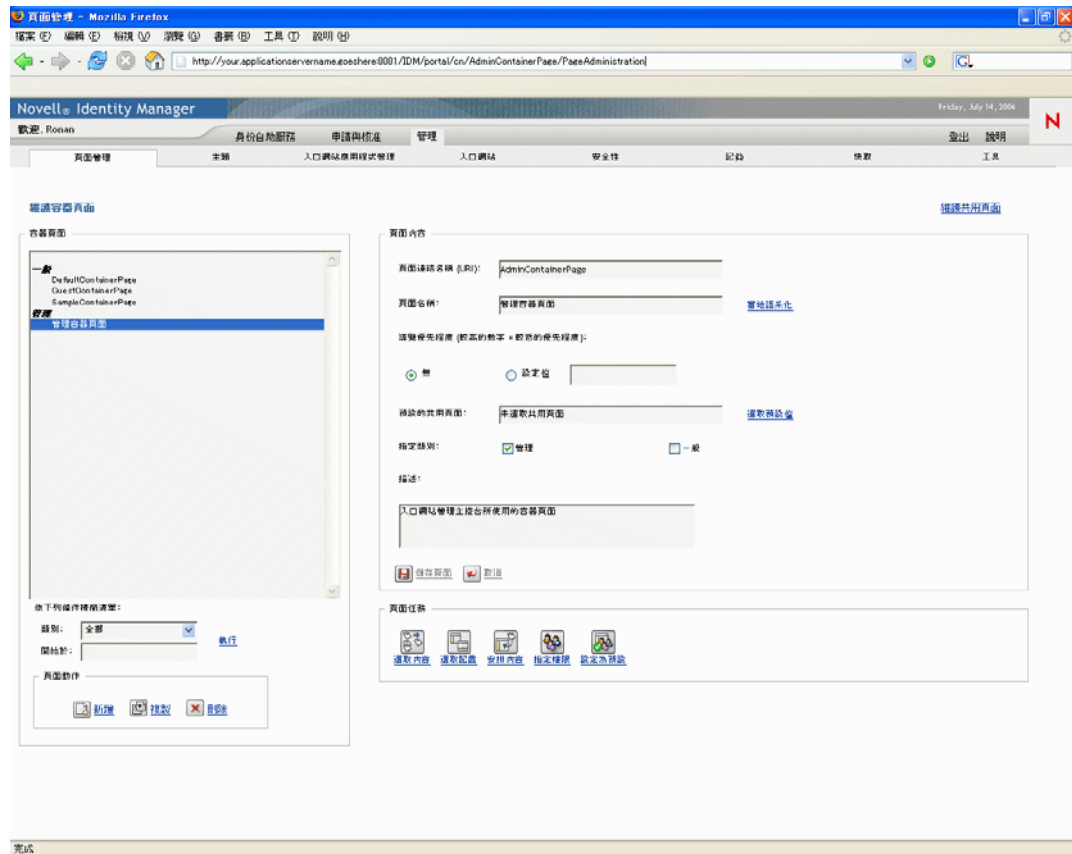
7.2.1 建立容器頁面

您可以從頭建立容器頁面，也可以複製現有的頁面來建立容器頁面。本節描述這兩個程序。

若要從頭建立容器頁面，請執行下列動作：

- 1 在「頁面管理」頁面上，選取「維護容器頁面」。

即會顯示「維護容器頁面」面板：



2 選取「新增」頁面動作 (位於面板的左下區段)。

即會建立無標題且未分類的容器頁面。

3 指定容器頁面的頁面內容：

內容	操作
頁面連結名稱 (URI)	指定頁面的 URI 名稱 (如同使用者介面 URL 中所顯示的)。例如，如果您指定 URI： MyContainerPage 它在 URL 中會顯示如下： <code>http://myappserver:8080/IDM/portal/cn/MyContainerPage</code>

內容	操作
頁面名稱	指定頁面的顯示名稱。例如： My Container Page 您可以按一下「 當地語系化 」，針對其他語言指定此名稱的當地語系化版本。
導覽優先程度	指定下列其中一項： <ul style="list-style-type: none"> ◆ 無：如果您不需要指定此容器頁面的優先程度。 ◆ 設定值：指定此容器頁面相對於其他容器頁面的優先程度。優先程度必須是 -1 到 9999 之間的整數，其中 -1 是最高優先程度，而 9999 是最低優先程度。 <p>如果您要在按照優先程度列出頁面時確保特定的順序，或在有多個預設頁面時確保特定的選擇（在使用者屬於多個群組的情況下），則設定優先程度值會非常有用。</p>
預設的共用頁面	請參閱「 選取容器頁面的預設共用頁面 」，第 152 頁。
指定類別	選取您要讓頁面歸屬的零個或多個下列類別： <ul style="list-style-type: none"> ◆ 管理 ◆ 一般 <p>如果您要在按照類別列出頁面時確保合適的組織，或在按照類別過濾頁面時確保適當的子集，則指定類別非常有用。</p>
描述	鍵入描述頁面的文字。

4 按一下「儲存頁面」（位於頁面內容區段的底部）。

若要複製現有的頁面來建立容器頁面，請執行下列動作：

- 1 在「頁面管理」頁面上，選取「維護容器頁面」。
即會顯示「維護容器頁面」面板（如先前程序所示）。
- 2 在容器頁面的清單中，選取您要複製的頁面。

提示：如果清單很長，您可以精簡該清單（按照類別或開始文字），以便更輕鬆地找到想要的頁面。

- 3 選取「複製」頁面動作（位於面板的左下區段）。
即會建立名為 *OriginalPageName* 的副本的新容器頁面。
- 4 指定容器頁面的頁面內容（如先前程序所示）。
- 5 按一下「儲存頁面」（位於頁面內容區段的底部）。

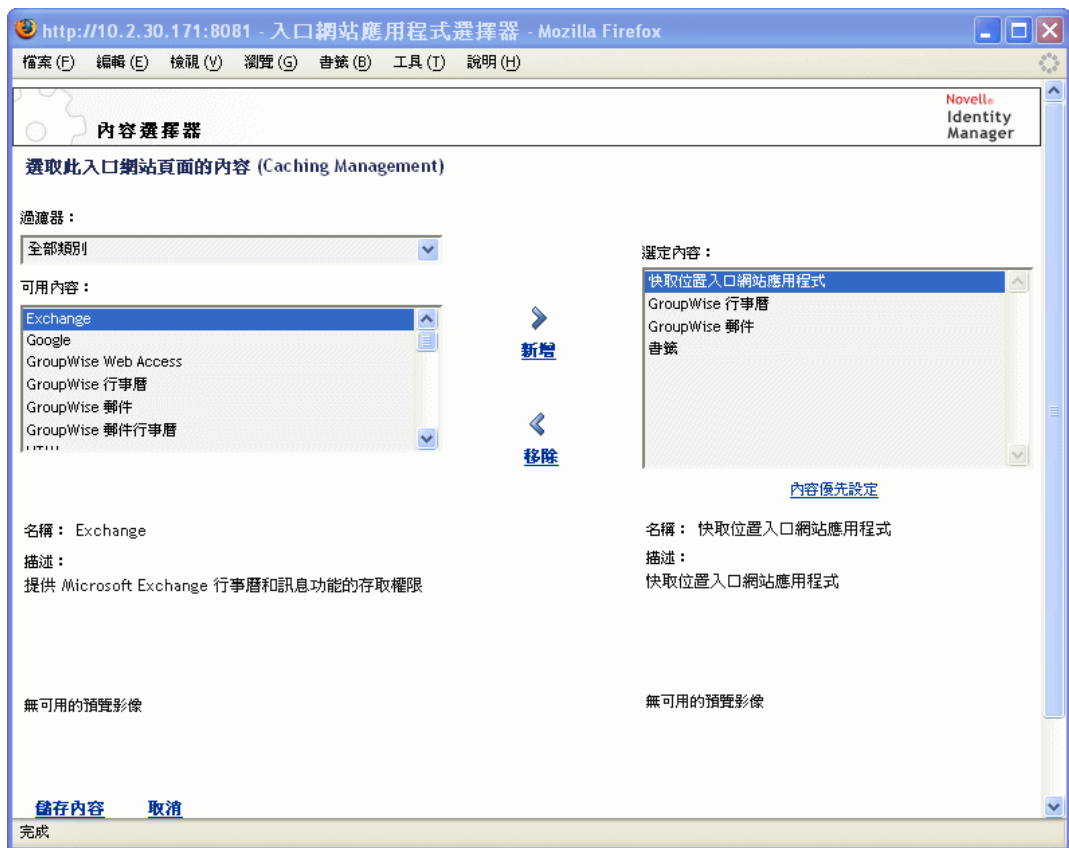
7.2.2 新增內容至容器頁面

在您建立容器頁面之後，下一步是選取要置於頁面的入口網站應用程式，以新增內容。您可以使用隨附於 Identity Manager 使用者應用程式的預先建立入口網站應用程式，或其他已註冊的入口網站應用程式。

若要新增內容至容器頁面，請執行下列動作：

- 1 開啟「維護容器頁面」面板上新的或現有的頁面，然後按一下「選取內容」頁面任務（位於面板的底部）。

「內容選擇器」即會在新的瀏覽器視窗中顯示：



- 2 如果您要顯示特定類別的可用內容，請從「過濾器」下拉式功能表選取類別。
- 3 從「可用內容」清單中選取一或多個入口網站應用程式。

提示：按住 *Ctrl* 鍵，從清單中選取多個非連續的入口網站應用程式；使用 *Shift* 鍵，則可連續選取多個項目。

- 4 按一下「新增」，將您的選擇移至「選定內容」的清單中。
- 5 您可以按一下「內容優先設定」，以編輯您針對容器頁面所選取之任何入口網站應用程式的優先設定。您指定的優先設定值會對頁面上顯示的入口網站應用程式例項生效。
- 6 按一下「儲存內容」。

既然您已選擇容器頁面的內容，就可以選取新的配置 (如「[修改容器頁面的配置](#)」，[第 134 頁](#)中所述)，或安排目前配置上的內容 (如「[安排容器頁面的內容](#)」，[第 135 頁](#)中所述)。

7.2.3 刪除容器頁面的內容

在建立容器頁面的程序中，您應該要從頁面移除入口網站應用程式，藉此來刪除內容。您可以使用「內容選擇器」或「配置選擇器」，如下列程序中所述。

若使用「內容選擇器」刪除容器頁面的內容，請執行下列動作：

- 1 開啓「維護容器頁面」面板上的頁面，然後按一下「選取內容」頁面任務 (位於面板的底部)。
「內容選擇器」即會顯示在新的瀏覽器視窗中 (如先前程序所示)。
- 2 選取您要從「選定內容」清單中刪除的入口網站應用程式，並按一下「移除」。
入口網站應用程式即會從頁面中移除。
- 3 按一下「儲存內容」。

若使用「配置選擇器」刪除容器頁面的內容，請執行下列動作：

- 1 開啓「維護容器頁面」面板上的頁面，然後按一下「安排內容」頁面任務 (位於面板的底部)。

「配置選擇器」即會顯示在新的瀏覽器視窗中，顯示該頁面上的入口網站應用程式：



- 2 針對您要移除的入口網站應用程式，按一下「X」按鈕。
- 3 系統提示您確認時，按一下「確定」。
入口網站應用程式即會從頁面中移除。
- 4 按一下「儲存配置」。

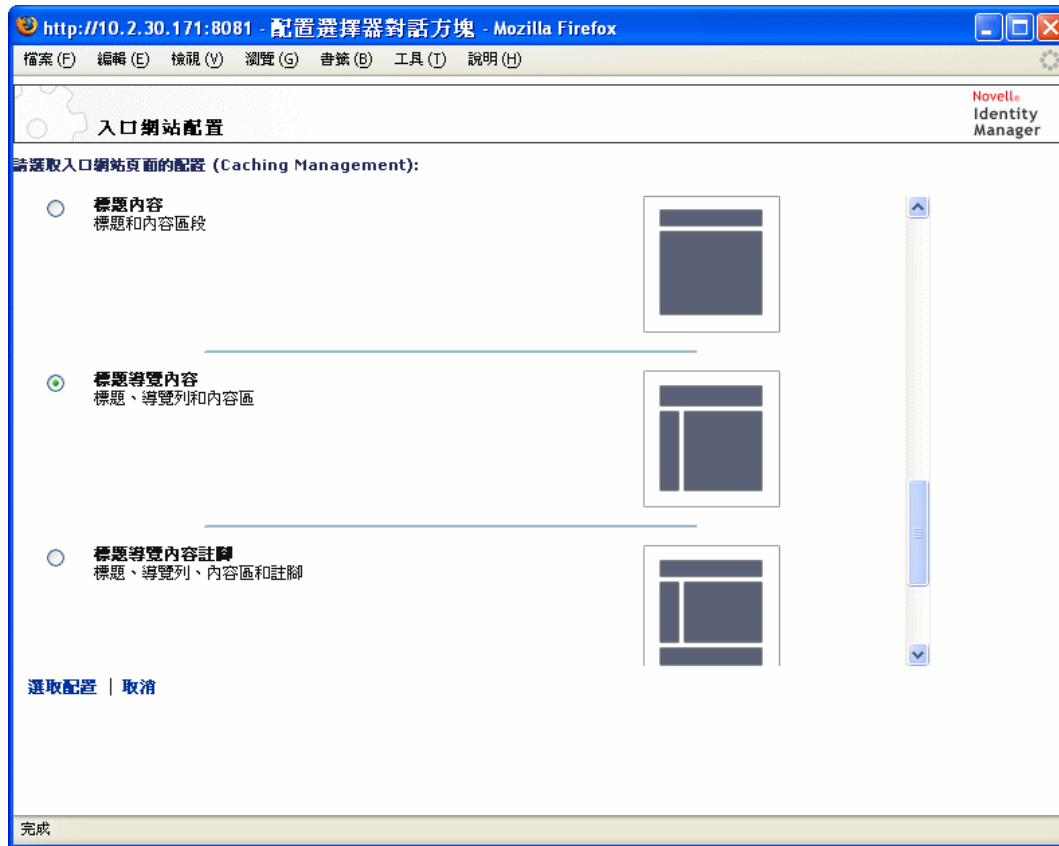
7.2.4 修改容器頁面的配置

修改容器頁面的配置時，現有內容會移位，以容納新的配置。在某些狀況下，您可能需要細調最終結果。

若要修改容器頁面的配置，請執行下列動作：

- 1 開啓「維護容器頁面」面板上的頁面，然後按一下「選取配置」頁面任務（位於面板的底部）。

「入口網站配置」清單即會顯示在新的瀏覽器視窗中：



- 2 捲動整個選項，並選取您所要的配置。
- 3 按一下「選取配置」。

7.2.5 安排容器頁面的內容

在指定容器頁面的內容和配置之後，您可以將內容置於選定配置、在特定位置新增其他入口網站應用程式，或刪除入口網站應用程式。

若要安排容器頁面的內容，請執行下列動作：

- 1 開啓「維護容器頁面」面板上的頁面，然後按一下「安排內容」頁面任務（位於面板的底部）。

「配置選擇器」即會顯示在新的瀏覽器視窗中，顯示該頁面上的入口網站應用程式：



2 如果您要新增入口網站應用程式至頁面，請遵循下列步驟：

2a 在所要的配置框架中按一下「新增內容」。

「入口網站應用程式選擇器」即會顯示在新的瀏覽器視窗中。

2b 如果您要顯示特定類別的可用內容，請從「過濾器」下拉式功能表選取類別。

2c 從「可用內容」清單中選取想要的入口網站應用程式。

2d 按一下「選取內容」。

「入口網站應用程式選擇器」即會關閉，而您選擇的入口網站應用程式會顯示在「配置選擇器」的目標配置框架中。

3 如果您要移動入口網站應用程式至配置中的不同位置，請遵循下列瀏覽器特定的步驟：

瀏覽器	操作
Internet Explorer	<ol style="list-style-type: none"> 1. 將游標移至入口網站應用程式的標題列，直到游標變為手的形狀為止。 2. 按住滑鼠左鍵，並將入口網站應用程式拖曳至配置中所要的位置。

瀏覽器	操作
Mozilla	<ol style="list-style-type: none"> 1. 按一下您要移動的入口網站應用程式。 2. 按一下目的配置框架的內部。 <p>入口網站應用程式即會移至目的地。</p>

- 4 如果您要從配置移除入口網站應用程式，請遵循下列步驟：
 - 4a 針對您要移除的入口網站應用程式，按一下「X」按鈕。
 - 4b 系統提示您確認時，按一下「確定」。
入口網站應用程式即會從配置中移除。
- 5 如果您要對入口網站應用程式編輯優先設定，請遵循下列步驟：
 - 5a 針對您要編輯的入口網站應用程式，按一下「鉛筆」按鈕。
入口網站應用程式的「內容優先設定」即會顯示在瀏覽器中。
 - 5b 視情況變更優先設定值。
您指定的優先設定值會對頁面上顯示的入口網站應用程式例項生效。
 - 5c 按一下「儲存優先設定」。
- 6 按一下「儲存配置」，以記錄變更，並關閉「配置選擇器」。

7.2.6 顯示容器頁面

您可以在瀏覽器中移至容器頁面 URL，來顯示頁面。

若要顯示容器頁面，請執行下列動作：

- ◆ 在網頁瀏覽器中，移至下列 URL：

```
http://server:port/IDM-war-context/portal/cn/container-page-name
```

例如，若要顯示名為 *MyContainerPage* 的容器頁面，請移至：

```
http://myappserver:8080/IDM/portal/cn/MyContainerPage
```

7.3 建立和維護共用頁面

建立和維護共用頁面的程序包括下列步驟：

- 1 建立新的共用頁面，或選取現有的共用頁面（如「[建立共用頁面](#)」，第 138 頁中所述）。
- 2 新增內容（以入口網站應用程式的形式）至頁面（如「[新增內容至共用頁面](#)」，第 140 頁中所述）。
您也可能會要從頁面刪除內容（如「[刪除共用頁面的內容](#)」，第 142 頁中所述）。
- 3 選擇入口網站配置（如「[修改共用頁面的配置](#)」，第 143 頁中所述）。

- 4 在選定配置上安排內容的順序和位置 (如「安排共用頁面的內容」，第 144 頁中所述)。
- 5 在瀏覽器中輸入共用頁面 URL，以立即顯示新的頁面 (如「顯示共用頁面」，第 145 頁中所述)。

共用頁面和配置 共用頁面並不會嚴格受限於入口網站配置。這表示您可以切換共用頁面的配置，而不會遺失任何頁面內容。當套用新的配置時，新增至頁面的任何入口網站應用程式都會使用新的配置自動顯示。您可能需要細調新配置中的內容位置。

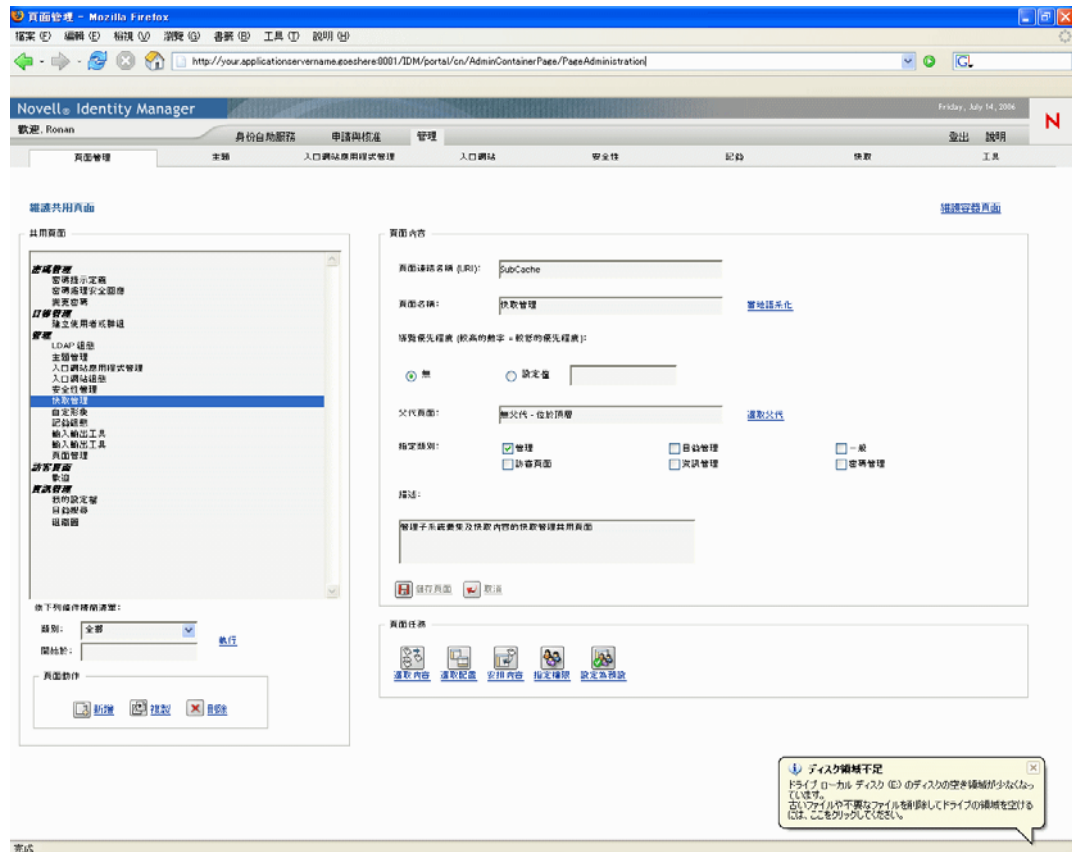
7.3.1 建立共用頁面

您可以從頭建立共用頁面，也可以複製現有的頁面來建立共用頁面。本節描述這兩個程序。

若要從頭建立共用頁面，請執行下列動作：

- 1 在「頁面管理」頁面上，選取「維護共用頁面」。

即會顯示「維護共用頁面」面板：



- 2 選取「新增」頁面動作 (位於面板的左下區段)。即會建立無標題且未分類的共用頁面。
- 3 指定共用頁面的頁面內容：

內容	操作
頁面連結名稱 (URI)	<p>指定頁面的 URI 名稱 (如同使用者介面 URL 中所顯示的)。例如，如果您指定 URI：</p> <p>MySharedPage</p> <p>它在 URL 中會顯示如下：</p> <p>http://myappserver:8080/IDM/portal/cn/MyContainerPage/MySharedPage</p>
頁面名稱	<p>指定頁面的顯示名稱。例如：</p> <p>My Shared Page</p> <p>您可以按一下「當地語系化」，針對其他語言指定此名稱的當地語系化版本。</p>
導覽優先程度	<p>指定下列其中一項：</p> <ul style="list-style-type: none"> ◆ 無：如果您不需要指定此共用頁面的優先程度。 ◆ 設定值：指定此共用頁面相對於其他共用頁面的優先程度。優先程度必須是 -1 到 9999 之間的整數，其中 -1 是最高優先程度，而 9999 是最低優先程度。 <p>如果您要在按照優先程度列出頁面時確保特定的順序，或在有多個預設頁面時確保特定的選擇 (在使用者屬於多個群組的情況下)，則設定優先程度值會非常有用。</p>
父代頁面	<p>如果您想讓此共用頁面成為另一個共用頁面的子代，請按一下「選取父代」。請確定父代和子代頁面屬於相同的類別 (以防止發生顯示問題)。</p> <p>在執行時期，當使用「共用頁面導覽」入口網站應用程式時，一般使用者會看到此關係。顯示共用頁面的清單時，會縮排顯示在它們父代下的子代。</p> <p>(請注意，子代頁面不會承襲其父代頁面的內容、優先設定或設定。相反地，父代頁面不會在顯示其自己內容時，自動顯示子代頁面的內容)。</p>

內容	操作
指定類別	<p>選取您要讓頁面歸屬的零個或多個下列類別：</p> <ul style="list-style-type: none"> ◆ 管理 ◆ 目錄管理 ◆ 一般 ◆ 訪客頁面 ◆ 資訊管理 ◆ 密碼管理 <p>如果您要在按照類別列出頁面時確保合適的組織，或在按照類別過濾頁面時確保適當的子集，則指定類別非常有用。</p> <hr/> <p>附註：「訪客頁面」是特定的類別，用於識別在使用者登入之前（不是在使用者登入之後）可能顯示的共用頁面。如需相關資訊，請參閱第 15 章「關於入口網站應用程式」，第 215 頁中關於「共用頁面導覽」入口網站應用程式一節。</p>
描述	<p>鍵入描述頁面的文字。</p>

4 按一下「儲存頁面」（位於頁面內容區段的底部）。

若要複製現有的頁面來建立共用頁面，請執行下列動作：

- 1 在「頁面管理」頁面上，選取「維護共用頁面」。
即會顯示「維護共用頁面」面板（如先前程序所示）。
- 2 在共用頁面的清單中，選取您要複製的頁面。

提示：如果清單很長，您可以精簡該清單（按照類別或開始文字），以便更輕鬆地找到想要的頁面。

- 3 選取「複製」頁面動作（位於面板的左下區段）。
即會建立名為 *OriginalPageName* 的副本的新共用頁面。
- 4 指定共用頁面的頁面內容（如先前程序所示）。
- 5 按一下「儲存頁面」（位於頁面內容區段的底部）。

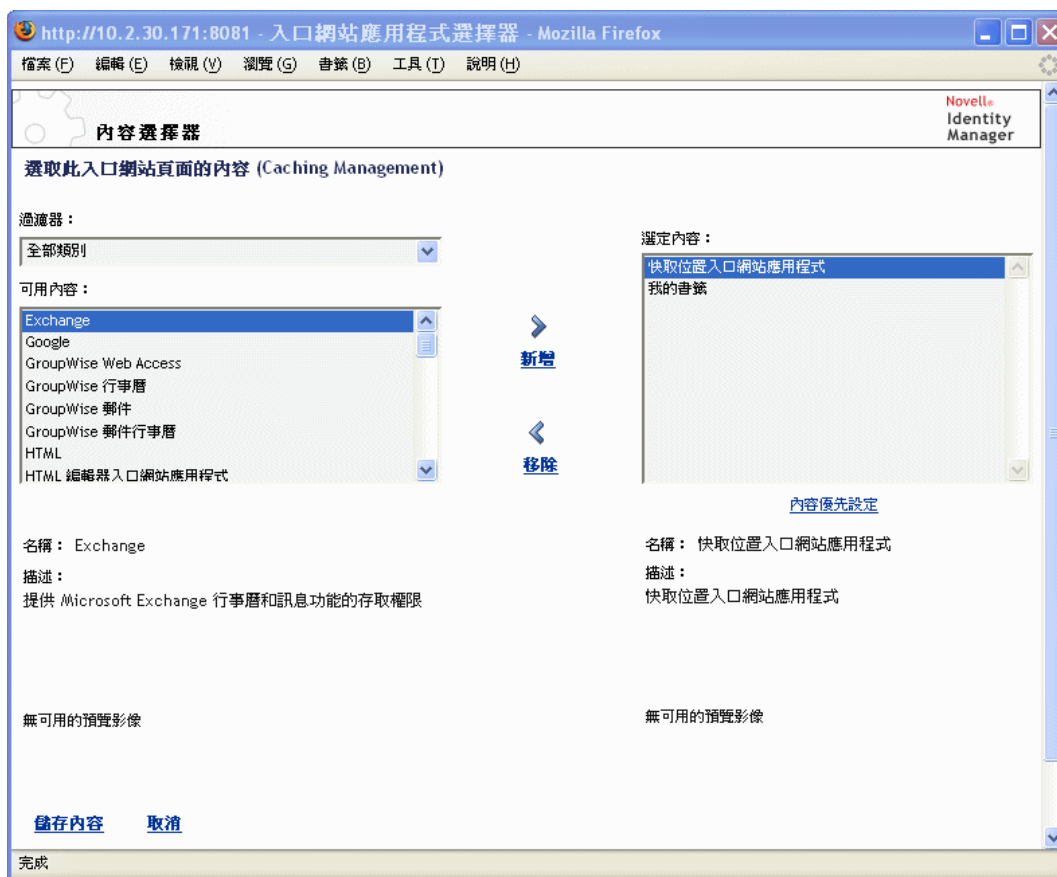
7.3.2 新增內容至共用頁面

在您建立共用頁面之後，下一步是選取要置於頁面的入口網站應用程式，以新增內容。您可以使用隨附於 Identity Manager 使用者應用程式的預先建立入口網站應用程式，或其他已註冊的入口網站應用程式。

若要新增內容至共用頁面，請執行下列動作：

- 1 開啓「維護共用頁面」面板上新的或現有的頁面，然後按一下「選取內容」頁面任務（位於面板的底部）。

「內容選擇器」即會顯示在新的瀏覽器視窗中：



- 2 如果您要顯示特定類別的可用內容，請從「過濾器」下拉式功能表選取類別。
- 3 從「可用內容」清單中選取一或多個入口網站應用程式。

提示：按住 *Ctrl* 鍵，從清單中選取多個非連續的入口網站應用程式，使用 *Shift* 鍵，則可連續選取多個項目。

- 4 按一下「新增」，將您的選擇移至「選定內容」的清單中。
- 5 您可以按一下「內容優先設定」，以編輯您針對共用頁面選取之任何入口網站應用程式的優先設定。您指定的優先設定值會對頁面上顯示的入口網站應用程式例項生效。
- 6 按一下「儲存內容」。

既然您已選擇共用頁面的內容，就可以選取新的配置（如「修改共用頁面的配置」，第 143 頁中所述），或安排目前配置上的內容，如（「安排共用頁面的內容」，第 144 頁中所述）。

7.3.3 刪除共用頁面的內容

在建立共用頁面的程序中，您應該要從頁面移除入口網站應用程式，藉此來刪除內容。您可以使用「內容選擇器」或「配置選擇器」，如下列程序所述。

若使用「內容選擇器」刪除共用頁面的內容，請執行下列動作：

- 1 開啓「維護共用頁面」面板上的頁面，然後按一下「選取內容」頁面任務（位於面板的底部）。

「內容選擇器」即會顯示在新的瀏覽器視窗中（如先前程序所示）。

- 2 選取您要從「選定內容」清單中刪除的入口網站應用程式，並按一下「移除」。

入口網站應用程式即會從頁面中移除。

- 3 按一下「儲存內容」。

若使用「配置選擇器」刪除共用頁面的內容，請執行下列動作：

- 1 開啓「維護共用頁面」面板上的頁面，然後按一下「安排內容」頁面任務（位於面板的底部）。

「配置選擇器」即會顯示在新的瀏覽器視窗中，顯示該頁面上的入口網站應用程式：



- 2 針對您要移除的入口網站應用程式，按一下「X」按鈕。

- 3 系統提示您確認時，按一下「確定」。

入口網站應用程式即會從頁面中移除。

- 4 按一下「儲存配置」。

7.3.4 修改共用頁面的配置

當您修改共用頁面的配置時，現有內容會移位，以容納新的配置。在某些狀況下，您可能需要細調最終結果。

若要修改共用頁面的配置，請執行下列動作：

- 1 開啓「維護共用頁面」面板上的頁面，然後按一下「選取配置」頁面任務（位於面板的底部）。

「入口網站配置」清單即會顯示在新的瀏覽器視窗中：



- 2 捲動整個選項，並選取您所要的配置。
- 3 按一下「選取配置」。

7.3.5 安排共用頁面的內容

在指定共用頁面的內容和配置之後，您可以將內容置於選定配置、在特定位置新增其他入口網站應用程式，或刪除入口網站應用程式。

若要安排共用頁面的內容，請執行下列動作：

- 1 開啟「維護共用頁面」面板上的頁面，然後按一下「安排內容」頁面任務（位於面板的底部）。

「配置選擇器」即會顯示在新的瀏覽器視窗中，顯示該頁面上的入口網站應用程式：



- 2 如果您要新增入口網站應用程式至頁面，請遵循下列步驟：
 - 2a 在所要的配置框架中按一下「新增內容」。
「入口網站應用程式選擇器」即會顯示在新的瀏覽器視窗中。
 - 2b 如果您要顯示特定類別的可用內容，請從「過濾器」下拉式功能表選取類別。
 - 2c 從「可用內容」清單中選取想要的入口網站應用程式。
 - 2d 按一下「選取內容」。
「入口網站應用程式選擇器」即會關閉，而您選擇的入口網站應用程式會顯示在「配置選擇器」的目標配置框架中。
- 3 如果您要移動入口網站應用程式至配置中的不同位置，請遵循下列瀏覽器特定的步驟：

瀏覽器	操作
Internet Explorer	<ol style="list-style-type: none"> 1. 將游標移至入口網站應用程式的標題列，直到游標變為手的形狀為止。 2. 按住滑鼠左鍵，並將入口網站應用程式拖曳至配置中所要的位置。
Mozilla	<ol style="list-style-type: none"> 1. 按一下您要移動的入口網站應用程式。 2. 按一下目的配置框架的內部。 <p>入口網站應用程式即會移至目的地。</p>

- 4 如果您要從配置移除入口網站應用程式，請遵循下列步驟：
 - 4a 針對您要移除的入口網站應用程式，按一下「X」按鈕。
 - 4b 系統提示您確認時，按一下「確定」。
入口網站應用程式即會從配置中移除。
- 5 如果您要對入口網站應用程式編輯優先設定，請遵循下列步驟：
 - 5a 針對您要編輯的入口網站應用程式，按一下「鉛筆」按鈕。
入口網站應用程式的「內容優先設定」即會顯示在瀏覽器中。
 - 5b 視情況變更優先設定值。
您指定的優先設定值會對頁面上顯示的入口網站應用程式例項生效。
 - 5c 按一下「儲存優先設定」。
- 6 按一下「儲存配置」，以記錄變更，並關閉「配置選擇器」。

7.3.6 顯示共用頁面

您可以在瀏覽器中移至共用頁面 URL，來顯示頁面。

若要顯示共用頁面，請執行下列動作：

- ◆ 在網頁瀏覽器中，移至下列 URL：

```
http://server:port/IDM-war-context/portal/pg/shared-page-name
```

例如，若要顯示名為 *MySharedPage* 的共用頁面，請移至：

```
[XXX]  
http://myappserver:8080/IDM/portal/pg/MySharedPage
```

7.4 指定頁面的許可

您可以指定許可給其他使用者、群組和容器，以使用特定的容器頁面和共用頁面。您可以指定兩個安全性層級的許可：

許可	描述	可以被指定的對象
檢視	允許使用者、群組或容器存取頁面，並且可以在可用頁面的清單中看到它	容器頁面和共用頁面
擁有權	允許使用者、群組或容器修改頁面的內容和配置，並將「檢視」和「擁有權」權限指定給其他使用者、群組和容器	共用頁面

7.4.1 指定頁面檢視權限

當您對使用者指定容器頁面或共用頁面的「檢視」許可時，使用者就可以存取該頁面，並在可用頁面的清單中看到頁面。

若要指定容器頁面或共用頁面的「檢視」許可，請執行下列動作：

- 1 開啟「維護容器頁面」面板或「維護共用頁面」面板上的頁面，然後按一下「指定權限」頁面任務（位於面板的底部）。

「頁面權限」對話方塊即會顯示在新的瀏覽器視窗中：



- 2 移至「檢視」索引標籤。
- 3 指定下列搜尋設定的值：

設定	操作
搜尋	<p>從下拉式功能表選取下列其中一項：</p> <ul style="list-style-type: none"> ◆ 使用者 ◆ 群組 ◆ 容器
開頭為	<p>如果想要：</p> <ul style="list-style-type: none"> ◆ 若要尋找所有指定類型的可用物件 (使用者、群組或容器)，請將此設定留為空白。 ◆ 若要在那些物件中尋找子集，請輸入您想要之 CN 值的開始字元 (不考量大小寫，不支援萬用字元)。 <p>例如，搜尋開頭為 S 的群組會縮小您的搜尋結果，如下所示：</p> <pre>cn=Sales,ou=groups,o=MyOrg</pre> <pre>cn=Service,ou=groups,o=MyOrg</pre> <pre>cn=Shipping,ou=groups,o=MyOrg</pre> <p>搜尋開頭為 Se 的群組會傳回：</p> <pre>cn=Service,ou=groups,o=MyOrg</pre>

4 按一下「執行」。

搜尋的結果即會顯示在「結果」清單中。

5 選取您想要指定給頁面的使用者、群組或容器，然後按一下「新增 (>)」按鈕。

提示：按住 *Ctrl* 鍵以選取多個項目。

6 啟用或停用頁面鎖定，如下所示：

如果想要	執行下列動作
鎖定頁面，以便只有「使用者應用程式管理員」才可以檢視它	核取「 檢視權限設定為僅限於管理者身份 」
允許所有指定的使用者、群組和容器檢視頁面	取消核取「 檢視權限設定為僅限於管理者身份 」

附註：如果您取消核取此設定，但是沒有將任何使用者、群組或容器明確地指定給頁面，則對於此頁面，**每個人都具有「檢視」權限**。

7 按一下「儲存」，然後按一下「關閉」。

7.4.2 指定共用頁面擁有者

擁有共用頁面的使用者可以修改其擁有之頁面的內容，還可以變更那些頁面上的入口網站應用程式優先設定。

若要指定共用頁面的「擁有權」權限，請執行下列動作：

1 開啓「維護共用頁面」面板上的頁面，然後按一下「指定權限」頁面任務（位於面板的底部）。

「頁面權限」對話方塊即會顯示在新的瀏覽器視窗中（如先前程序所示）。

2 移至「擁有權」索引標籤。

3 指定下列搜尋設定的值：

設定	操作
搜尋	從下拉式功能表選取下列其中一項： <ul style="list-style-type: none">◆ 使用者◆ 群組◆ 容器
開頭為	如果想要： <ul style="list-style-type: none">◆ 若要尋找所有指定類型的可用物件（使用者、群組或容器），請將此設定留為空白。◆ 若要在那些物件中尋找子集，請輸入您想要之 CN 值的開始字元（不考量大小寫，不支援萬用字元）。 例如，搜尋開頭為 S 的群組會縮小您的搜尋結果，如下所示： <pre>cn=Sales,ou=groups,o=MyOrg</pre> <pre>cn=Service,ou=groups,o=MyOrg</pre> <pre>cn=Shipping,ou=groups,o=MyOrg</pre> 搜尋開頭為 Se 的群組會傳回： <pre>cn=Service,ou=groups,o=MyOrg</pre>

4 按一下「執行」。

搜尋的結果即會顯示在「結果」清單中。

- 5 選取您想要指定給頁面的使用者、群組或容器，然後按一下「新增 (>)」按鈕。

提示：按住 *Ctrl* 鍵以選取多個項目。

- 6 啓用或停用頁面鎖定，如下所示：

如果想要	執行下列動作
鎖定頁面，以便只有「使用者應用程式管理員」才可以使用它	核取「擁有權權限設定為僅限於管理者身份」
允許所有指定的使用者、群組和容器使用頁面	取消核取「擁有權權限設定為僅限於管理者身份」

附註：如果您取消核取此設定，但是沒有將任何使用者、群組或容器明確地指定給頁面，則對於此頁面，每個人都具有「擁有權」權限。

- 7 按一下「儲存」，然後按一下「關閉」。

7.4.3 允許使用者存取建立使用者或群組頁面

在預設狀態下，只有「使用者應用程式管理員」才可以查看和使用「建立使用者或群組」頁面，該頁面是 Identity Manager 使用者介面「身份自助服務」索引標籤上的共用頁面。但是必要時，「使用者應用程式管理員」可以針對一或多位一般使用者指定許可，以便該使用者也可以存取頁面。例如，居於管理職位的選定使用者自己可能需要具有建立使用者、群組或任務群組的能力。

若要授予使用者存取「建立使用者或群組」頁面的權限，請執行下列動作：

- 1 在「維護共用頁面」面板上，開啓名為「建立使用者或群組」的頁面。
- 2 使用「指定權限」頁面任務，將「檢視」權限授予適當的使用者、群組或容器，以用於「建立使用者或群組」共用頁面。
- 3 從「頁面管理」切換至「入口網站應用程式管理」，並開啓名為 *CreatePortlet* 的入口網站應用程式註冊（其用在「建立使用者或群組」頁面上）。
- 4 使用「安全性」面板，將「清單」與「執行」許可授予適當的使用者、群組或容器，以用於 *CreatePortlet* 入口網站應用程式註冊。

如需指定入口網站應用程式許可的相關資訊，請參閱第 9 章「入口網站應用程式管理」，第 161 頁。

- 5 移至 *iManager*，並針對身份儲存區，使用管理員帳戶登入網路樹。
- 6 確定要使用「建立使用者或群組」的使用者，對於要建立物件（使用者、群組或任務群組）的容器，具有 [項目權限] 內容的建立權限。

例如，您可以為選擇的容器修改託管者，並將適當的使用者、群組或容器新增為託管者。然後，針對每位託管者，您可以指定下列權限：

內容名稱	指定的權限	承襲
[所有屬性權限]	<ul style="list-style-type: none"> ◆ 比較 ◆ 讀取 ◆ 寫入 	是 (選取此核取方塊)

內容名稱	指定的權限	承襲
[項目權限]	<ul style="list-style-type: none"> ◆ 瀏覽 ◆ 建立 	是 (選取此核取方塊)

如果您沒有在身份儲存區中指定必要權限 (或者那些權限不知何故無法衍生)，則一般使用者可能會從「建立使用者或群組」得到錯誤訊息，如下所示：

```
User 'cn=mmackenzie,ou=users,ou=idmsample,o=novell' does not have
permission to create
'cn=MyNewGroup,ou=groups,ou=idmsample,o=novell' or modify related
objects.
```

若要瞭解如何使用「建立使用者或群組」頁面 (由那些對它具有存取權限的使用者)，請參閱《*Identity Manager* 使用者應用程式：使用者指南》。

7.4.4 允許使用者存取個別管理頁面

在預設狀態下，只有「使用者應用程式管理員」才可以存取 Identity Manager 使用者介面的「管理」索引標籤，以及該索引標籤上包含的頁面 (「頁面管理」、「主題」、「入口網站應用程式管理」、「入口網站」、「安全性」、「記錄」、「快取」、「工具」)。但是必要時，「使用者應用程式管理員」可以針對一或多位一般使用者指定許可，以便該使用者可以查看並使用「管理」索引標籤上的特定頁面。例如，可能有一小群需要定期變更主題的使用者，即使他們不是「使用者應用程式管理員」。

若要授予使用者對個別「管理」頁面的存取權限，請執行下列動作：

- 1 在「維護容器頁面」面板上，開啓「管理容器頁面」。

這是容器頁面，當您移至 Identity Manager 使用者介面的「管理」索引標籤時，您會使用該容器頁面。
- 2 使用「指定權限」頁面任務，將「檢視」權限授予適當的使用者、群組或容器，以用於「管理容器頁面」。
- 3 在「維護共用頁面」面板上，開啓適當的「管理」頁面 (「管理」類別下的其中一個共用頁面)。
- 4 使用「指定權限」頁面任務，將「檢視」和「擁有權」權限授予適當的使用者、群組或容器，以用於共用頁面。
- 5 確定特定的使用者、群組或容器，對於特定頁面上使用的每一個入口網站應用程式，都具有「執行」許可 (如果您已限制那些入口網站應用程式)。

如需指定入口網站應用程式許可的相關資訊，請參閱第 9 章「入口網站應用程式管理」，第 161 頁。

7.5 設定群組的預設頁面

您可以針對任何已授權的使用者群組，指定預設容器頁面和預設共用頁面。這些設定會影響那些使用者登入時可以看見哪個容器頁面，以及在容器頁面上可以看見哪個共用頁面。

當使用者屬於指定了預設頁面的多個群組時，可以使用「導覽優先程度」來決定要顯示的容器頁面和共用頁面。

若要對群組指定預設容器頁面或預設共用頁面，請執行下列動作：

- 1 開啟「維護容器頁面」面板或「維護共用頁面」面板上的頁面，然後按一下「設定為預設」頁面任務（位於面板的底部）。

「頁面預設值」對話方塊即會顯示在新的瀏覽器視窗中：



- 2 指定下列搜尋設定的值：

設定	操作
搜尋	(自動選取「群組」。)

設定	操作
開頭為	<p>如果想要：</p> <ul style="list-style-type: none"> ◆ 尋找所有可用群組，請將此設定留為空白。 ◆ 在那些群組中尋找子集，請輸入您想要之 CN 值的開始字元 (不考量大小寫，不支援萬用字元)。 <p>例如，搜尋開頭為 S 的群組會縮小您的搜尋結果，如下所示：</p> <pre>cn=Sales,ou=groups,o=MyOrg</pre> <pre>cn=Service,ou=groups,o=MyOrg</pre> <pre>cn=Shipping,ou=groups,o=MyOrg</pre> <p>搜尋開頭為 Se 的群組會傳回：</p> <pre>cn=Service,ou=groups,o=MyOrg</pre>

- 3 按一下「執行」。
搜尋的結果即會顯示在「結果」清單中。
- 4 選取要將此頁面做為預設頁面的群組，然後按一下「新增(>)」按鈕。
提示：按住 *Ctrl* 鍵以選取多個項目。
- 5 按一下「儲存」，然後按一下「關閉」。

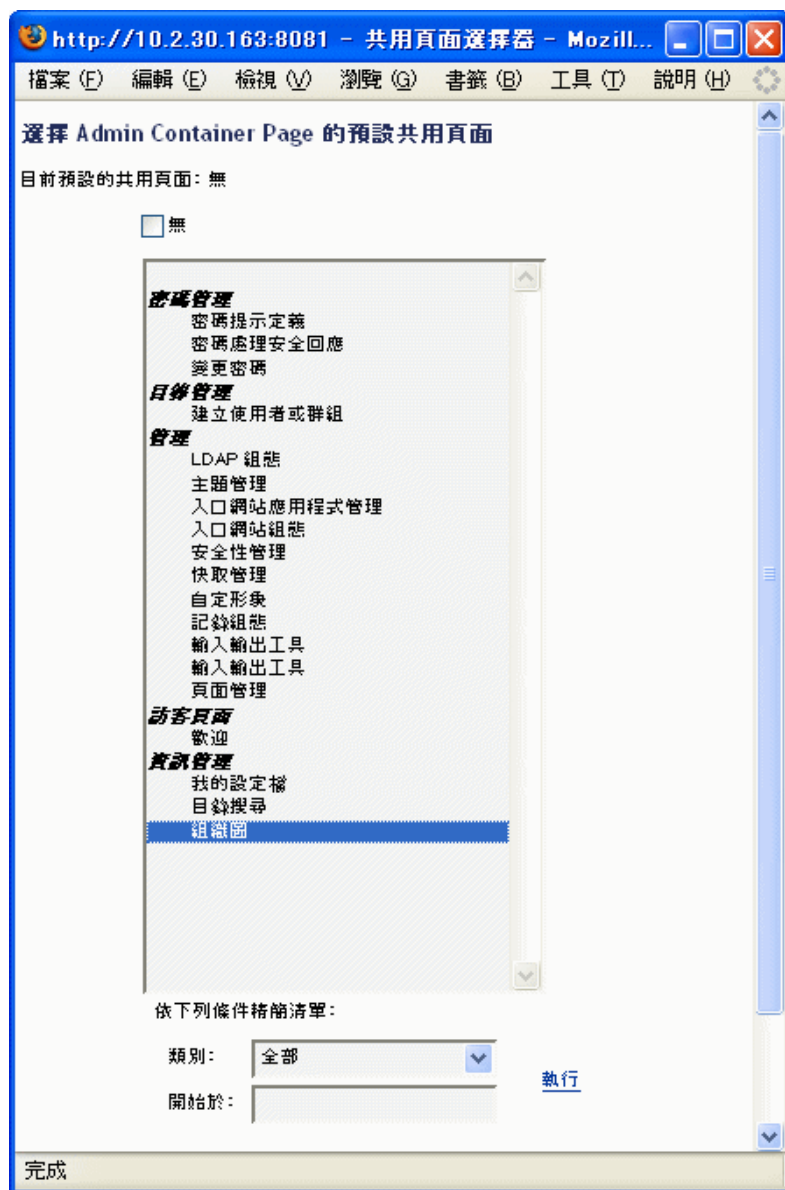
7.6 選取容器頁面的預設共用頁面

您可以針對您擁有的每個容器頁面指定預設共用頁面。使用者介面在決定要顯示的內容時便會考量此頁面指定。

若要指定容器頁面的預設共用頁面，請執行下列動作：

- 1 在「維護容器頁面」面板上，開啓容器頁面。
- 2 在頁面內容區段中，尋找「預設的共用頁面」，然後按一下「選取預設值」。

「選擇預設共用頁面」對話方塊即會顯示在新的瀏覽器視窗中：



- 3 如果共用頁面清單很長，您可以精簡)該清單(按照類別或開始文字)，以便更輕鬆地找到想要的頁面。
- 4 選取要做為容器頁面預設共用頁面的共用頁面(如果沒有預設頁面，請核取「無」)。
- 5 按一下「儲存」，以接受您的選擇，然後關閉對話方塊。
- 6 按一下「儲存頁面」(位於頁面內容區段的底部)。

本章說明如何使用 Identity Manager 使用者介面「管理」索引標籤上的「主題」頁面。主題包含：

- ◆ 「關於主題組態」，第 155 頁
- ◆ 「預覽主題」，第 156 頁
- ◆ 「選擇主題」，第 157 頁
- ◆ 「自定主題的品牌」，第 158 頁

如需存取和使用「管理」索引標籤的一般資訊，請參閱第 6 章「使用管理索引標籤」，第 115 頁。

8.1 關於主題組態

您可以使用「主題」頁面，來控制 Identity Manager 使用者介面的外觀和操作。

主題是一組套用至整個使用者介面的視覺特性（包含訪客和登入頁面、「身份自助服務」索引標籤、「申請與核准」索引標籤和「管理」索引標籤）。對於使用者介面而言，總會有一個主題起作用。「主題」頁面會提供數個主題選項，您可以切換到不同的主題。

「主題」頁面還可讓您：

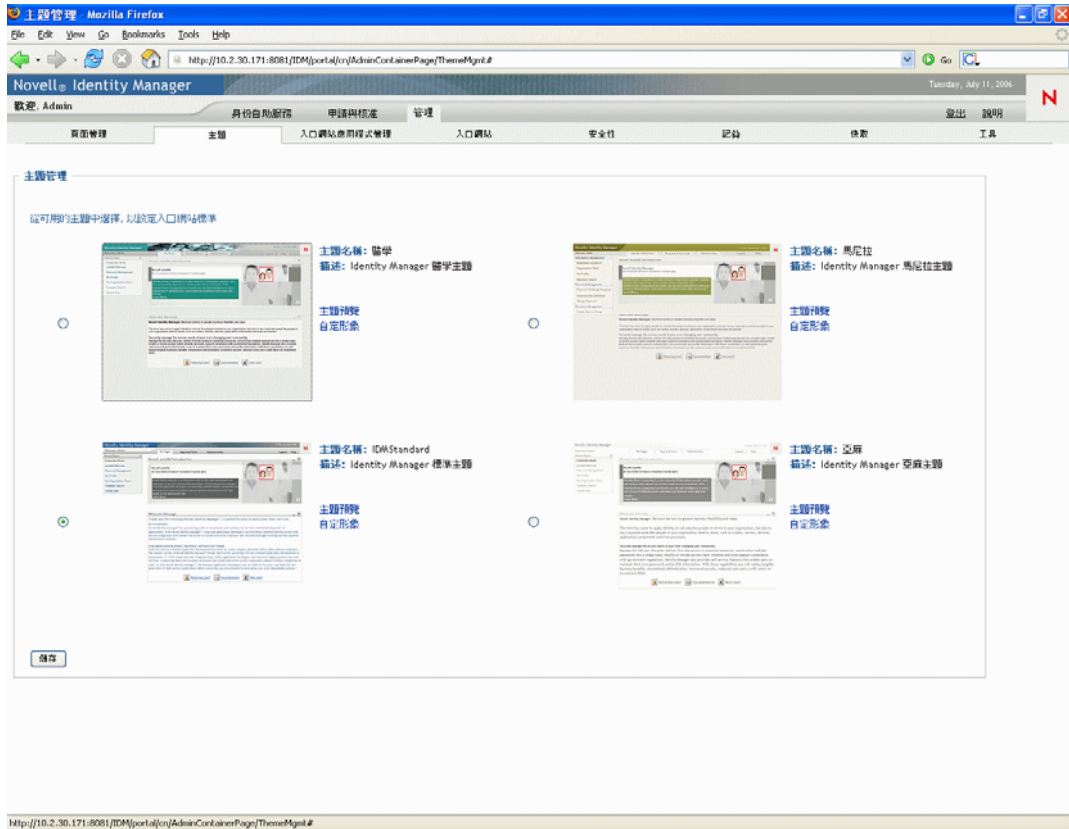
- ◆ 預覽每個主題選項，以查看它的外觀
- ◆ 自定任何主題選項，以反映您自己的品牌（標誌等）

8.2 預覽主題

選擇主題之前，您可以預覽它如何變更 Identity Manager 使用者界面的外觀。

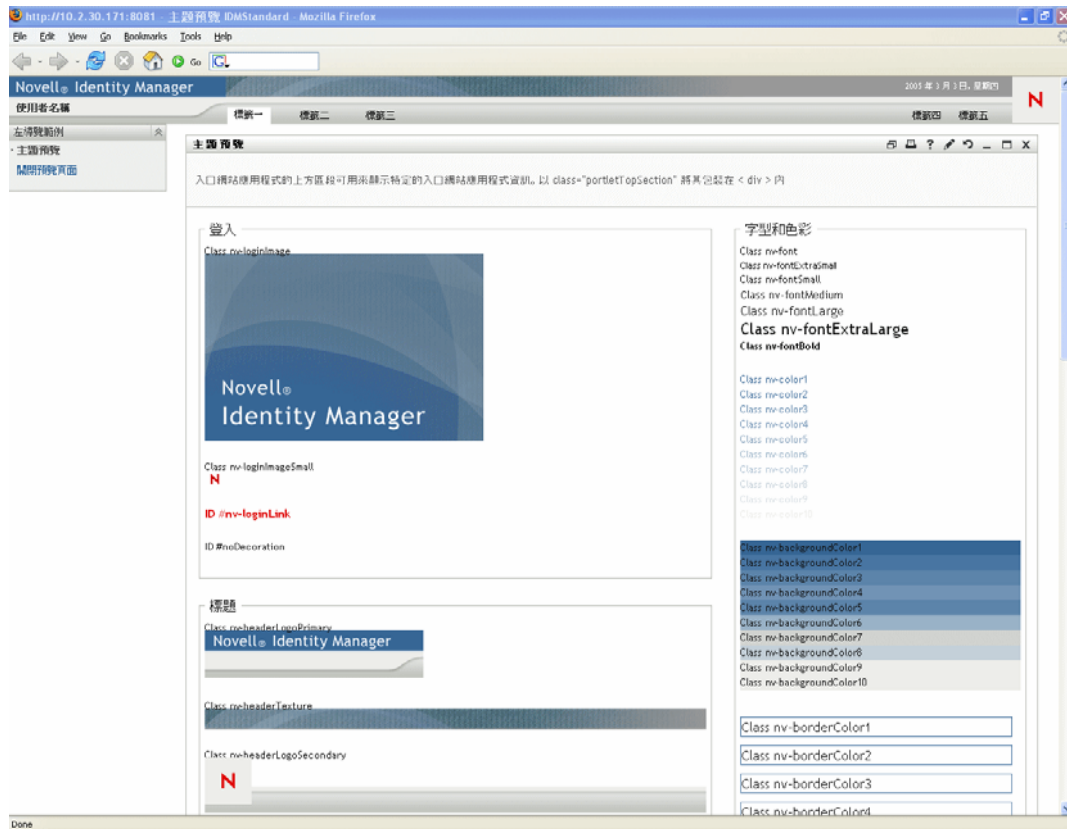
若要預覽主題，請執行下列動作：

- 1 移至「主題」頁面：



- 2 尋找您感興趣的主題，然後按一下對應的「主題預覽」連結。

該主題的預覽即會顯示在新的瀏覽器視窗中：



- 3 捲動整個預覽，以查看此主題的特性。
- 4 完成查看時，按一下「關閉預覽頁面」（在左上角），或者手動關閉預覽視窗。

8.3 選擇主題

當您找到喜歡的主題，可以選擇讓它成為 Identity Manager 使用者介面的目前主題。

若要選擇主題，請執行下列動作：

- 1 移至「主題」頁面。
 - 2 按一下您所要主題的選項圓鈕。
 - 3 按一下「儲存」按鈕。
- 使用者介面的外觀會變更，以反映您選擇的主題。

8.4 自定主題的品牌

您可以替換自己的影像，並變更部份色彩設定，來修改任何主題。這可讓您提供給 Identity Manager 使用者介面一個自定外觀，以滿足您公司或組織的品牌需求。

若要自定主題的品牌，請執行下列動作：

- 1 移至「主題」頁面。
- 2 尋找您想要修改的主題，然後按一下對應的「自定品牌」連結。
「主題」頁面即會顯示該主題的「自定品牌」設定：





3 在這些設定中指定您的自訂 (視需要), 包含:

- ◆ 標題影像
- ◆ 導覽區域色彩
- ◆ 登入影像

遵循畫面上的指示, 以指定每個設定。

4 按一下「儲存」按鈕。

如果您在編輯目前主題, 則使用者介面的外觀會變更, 以反映您的自訂 (如果您想要復原對主題的所有自訂, 請按一下「重設」按鈕)。

附註: 在您進行自訂時, 可以使用「主題預覽」按鈕, 但是要知道, 它會一直顯示主題的原始特性。它不會顯示您的變更。

5 當完成對此主題的自訂時, 按一下「返回主題選擇器」按鈕。

入口網站應用程式管理

本章說明如何使用 Identity Manager 使用者介面「管理」索引標籤上的「入口網站應用程式管理」頁面。主題包含：

- 「關於入口網站應用程式管理」，第 161 頁
- 「管理入口網站應用程式」，第 161 頁
- 「管理入口網站應用程式定義」，第 164 頁
- 「管理已註冊的入口網站應用程式」，第 168 頁

如需存取和使用「管理」索引標籤的一般資訊，請參閱第 6 章「使用管理索引標籤」，第 115 頁。

9.1 關於入口網站應用程式管理

您可以使用「入口網站應用程式管理」頁面，來控制 Identity Manager 使用者介面中可用的入口網站應用程式，以及誰具有存取它們的許可。入口網站應用程式是隨插即用的使用者介面元素（根據 Java 標準），這些元素會提供使用者介面中的頁面內容（包含容器頁面和共用頁面）。

管理入口網站應用程式包括使用下列項目：

使用的項目	描述
入口網站應用程式	與 Java Portlet 1.0 相容的 WAR，包含入口網站應用程式部署描述元 <code>portlet.xml</code> 和其他執行時期成品（選擇性）。 請參閱「管理入口網站應用程式」，第 161 頁。
入口網站應用程式定義	指定入口網站應用程式組態參數的描述元（從 <code>portlet.xml</code> 讀取）。應用程式中，每個入口網站應用程式都有一個定義。 請參閱「管理入口網站應用程式定義」，第 164 頁。
入口網站應用程式註冊	入口網站應用程式的註冊（根據它們的定義）。相同入口網站應用程式的多個註冊可以存在於單一入口網站應用程式中。 請參閱「管理已註冊的入口網站應用程式」，第 168 頁。

如需隨附於 Identity Manager 使用者介面之入口網站應用程式的詳細資料，請參閱「入口網站應用程式參考資訊」，第 213 頁。若要瞭解在容器頁面和共用頁面使用入口網站應用程式的相關資訊，請參閱第 7 章「頁面管理」，第 121 頁。

9.2 管理入口網站應用程式

安裝 Identity Manager 使用者應用程式時，`IDM.war` 會自動部署至應用程式伺服器，並會自動註冊為入口網站應用程式。`IDM.war`（在安裝期間可能會重新命名）包含 Identity Manager 使用者介面預設組態中所使用的所有入口網站應用程式。它還包含預設狀態下不使用的部份其他入口網站應用程式（在「入口網站應用程式參考資訊」，第 213 頁中有 `IDM.war` 入口網站應用程式的描述）。

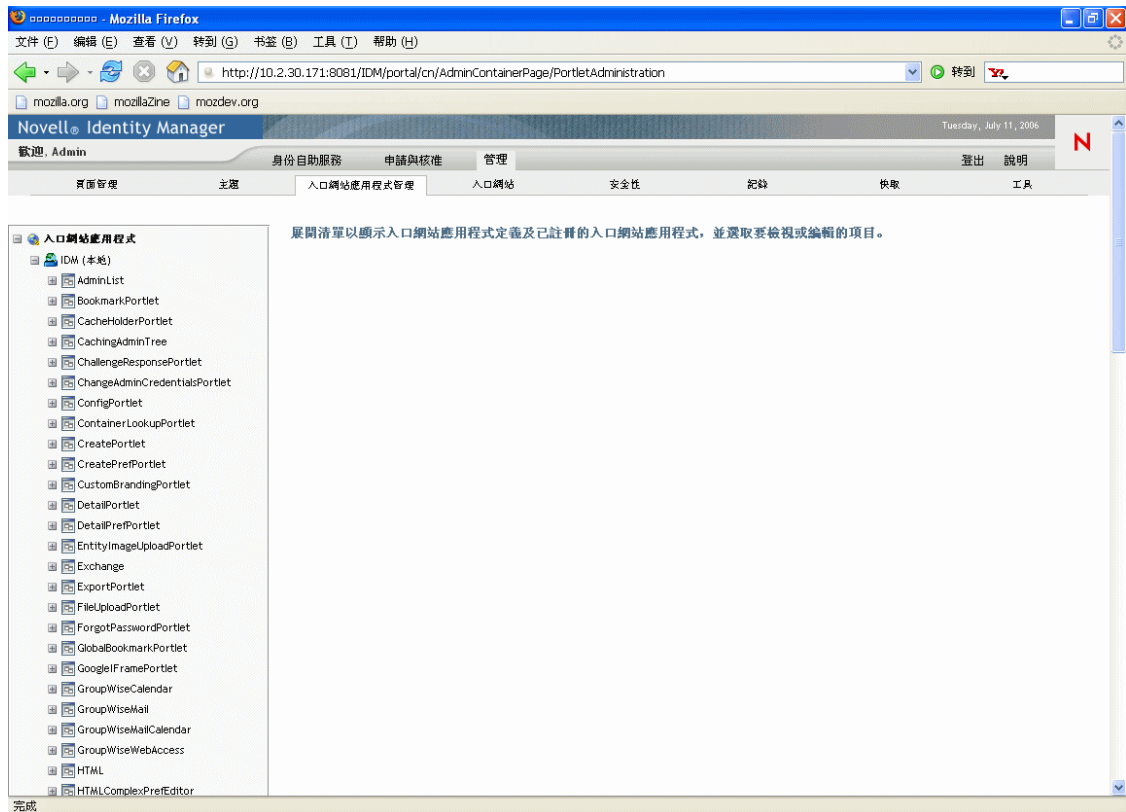
但是，不會限制您從 *IDM.war* 使用入口網站應用程式。如果您部署其他任何標準入口網站應用程式（與 Java Portlet 1.0 相容的 WAR）至應用程式伺服器，則可以使用那些入口網站應用程式，以及它們在 Identity Manager 使用者介面中的入口網站應用程式。例如，您可以在「入口網站應用程式管理」頁面上看到與 *IDM.war* 一起列出的那些入口網站應用程式。

「入口網站應用程式管理」頁面可讓您以下列方式管理 *IDM.war* 和其他入口網站應用程式：

- ◆ 「存取伺服器上的入口網站應用程式」，第 162 頁
- ◆ 「檢視入口網站應用程式的相關資訊」，第 162 頁
- ◆ 「取消註冊入口網站應用程式」，第 163 頁

9.2.1 存取伺服器上的入口網站應用程式

移至「入口網站應用程式管理」頁面時，它會自動針對部署至應用程式伺服器的入口網站應用程式（*IDM.war* 和其他任何應用程式）顯示清單。此清單會在左邊顯示為網路樹，您可以展開並導覽，以管理選定入口網站應用程式及其內容：



9.2.2 檢視入口網站應用程式的相關資訊

您可以檢視已列出之入口網站應用程式的下列唯讀資訊：

- ◆ 名稱
- ◆ 狀態（已啟用或已停用）
- ◆ 上次修改日期
- ◆ 上次修改應用程式的使用者

- ◆ 自定應用程式資訊 (如果有的話) : 入口網站應用程式模式、視窗狀態、安全性條件約束和使用者屬性

若要檢視入口網站應用程式的相關資訊，請執行下列動作：

- ◆ 在「入口網站應用程式」清單中，選取您想要瞭解的入口網站應用程式。
「一般」面板即會顯示在右側，顯示選定入口網站應用程式的相關資訊：



9.2.3 取消註冊入口網站應用程式

想要從應用程式伺服器移除入口網站應用程式時，您必須先取消註冊入口網站應用程式，才能取消部署。否則，入口網站應用程式會在伺服器重新啟動時自動重新部署。

當您取消註冊入口網站應用程式時，所有相關的優先設定和設定都會從儲存應用程式資料的資料庫移除。

附註：您無法取消註冊本地入口網站應用程式容器，即對入口網站而言是本地的入口網站應用程式。本地入口網站應用程式容器會管理包含在入口網站 (Identity Manager 使用者應用程式) 中的入口網站應用程式。

若要取消註冊入口網站應用程式，請執行下列動作：

- 1 在「入口網站應用程式」清單中，選取您要取消註冊的入口網站應用程式。
「一般」面板即會顯示在右側 (如先前程序所示)。
- 2 按一下「取消註冊」。

確認視窗即會出現。

- 3 按一下「確定」以確認動作。

程序完成時，取消註冊的入口網站應用程式會從「入口網站應用程式」清單中移除。

- 4 若要從應用程式伺服器移除入口網站應用程式，請使用伺服器工具，以取消部署包含入口網站應用程式的歸檔。

附註：若要重新註冊已取消註冊的入口網站應用程式，您必須重新部署它。

9.3 管理入口網站應用程式定義

「入口網站應用程式管理」頁面可讓您執行入口網站應用程式中，與入口網站應用程式定義相關的下列任務：

- 「存取已部署之入口網站應用程式中的入口網站應用程式定義」，第 164 頁
- 「註冊入口網站應用程式定義」，第 165 頁
- 「檢視入口網站應用程式定義的相關資訊」，第 166 頁

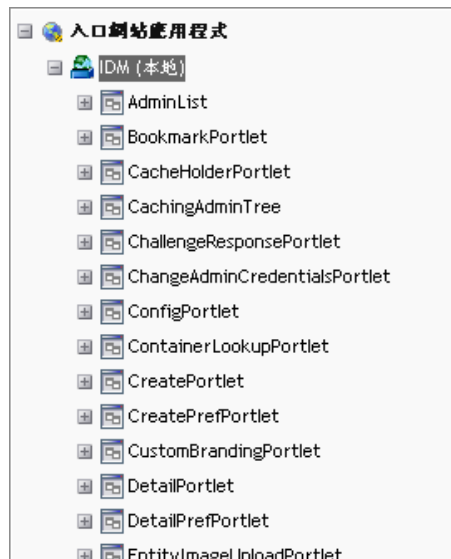
9.3.1 存取已部署之入口網站應用程式中的入口網站應用程式定義

「入口網站應用程式」清單會顯示選定入口網站應用程式中的入口網站應用程式定義。

若要存取已部署之入口網站應用程式中的入口網站應用程式定義，請執行下列動作：

- 在「入口網站應用程式」清單中，展開您要存取其入口網站應用程式定義的入口網站應用程式。

網路樹即會顯示該入口網站應用程式下的所有入口網站應用程式定義：



9.3.2 註冊入口網站應用程式定義

在您可以使用入口網站應用程式之前，您必須在入口網站 (Identity Manager 使用者應用程式) 上註冊該入口網站應用程式定義。已註冊的入口網站應用程式定義稱為入口網站應用程式註冊。您可以為單一入口網站應用程式建立多個註冊，這可讓您在同一頁面上放置入口網站應用程式的多個例項。

入口網站應用程式註冊會承襲入口網站應用程式類別的所有優先設定和設定，不過，您可以使用下列方法修改這些值：

- ◆ 當註冊入口網站應用程式定義時，請參閱「[管理已註冊的入口網站應用程式](#)」，第 168 頁
- ◆ 當新增入口網站應用程式的例項至頁面時，請參閱第 7 章「[頁面管理](#)」，第 121 頁

所有隨附於 Identity Manager 使用者應用程式的入口網站應用程式都會自動註冊。

編輯模式 如果入口網站應用程式定義提供「編輯」模式，則一般使用者可以根據入口網站應用程式 doEdit() 方法的邏輯，在執行時期修改入口網站應用程式註冊的特定優先設定。

Identity Manager 使用者應用程式也提供「編輯」模式的預設實作。如果沒有明確地實作 doEdit() 方法，則會顯示預設的優先設定表。

若要註冊入口網站應用程式定義，請執行下列動作：

- 1 在「入口網站應用程式」清單中，選取您要針對其建立入口網站應用程式註冊的入口網站應用程式定義。

「一般」面板即會顯示在右側：



請注意，選定入口網站應用程式的所有現有註冊都會在「入口網站應用程式」網路樹(在左側)中列出，並位於相對應的入口網站應用程式定義名稱之下。

- 2 在「註冊新的入口網站應用程式例項」文字方塊中，輸入入口網站應用程式註冊的唯一名稱，然後按一下「註冊」。

新的入口網站應用程式註冊即會建立，並列在「入口網站應用程式」網路樹中。

- 3 如果您要修改新入口網站應用程式註冊的優先設定和設定，請參閱「[管理已註冊的入口網站應用程式](#)」，第 168 頁。

9.3.3 檢視入口網站應用程式定義的相關資訊

您可以檢視已列出之入口網站應用程式定義的下列唯讀資訊：

- ◆ 顯示名稱
- ◆ 類別名稱
- ◆ 入口網站應用程式標題
- ◆ 執行類型 (同步或非同步)
- ◆ 簡稱
- ◆ 註冊類型
- ◆ 樣式名稱
- ◆ 快取過期時間
- ◆ 描述
- ◆ 啓始參數
- ◆ 關鍵字
- ◆ 支援的 Mime 類型
- ◆ 入口網站應用程式支援的模式
- ◆ 支援的地區設定
- ◆ 支援的裝置
- ◆ 安全性角色

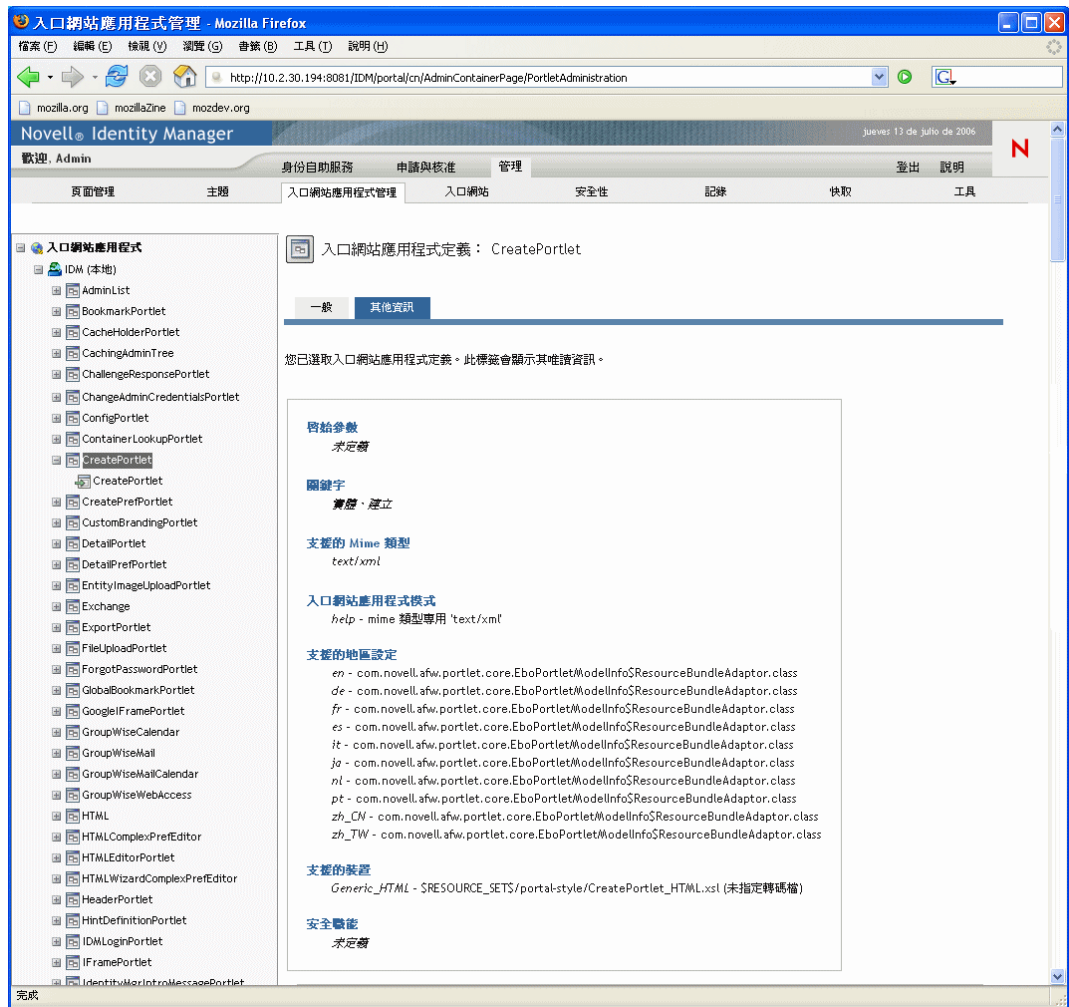
若要檢視入口網站應用程式定義的相關資訊，請執行下列動作：

- 1 在「入口網站應用程式」清單中，選取您要瞭解的入口網站應用程式定義。

「一般」面板即會顯示在右側，顯示選定入口網站應用程式定義的相關資訊：



2 移至「其他資訊」面板，以進一步檢視選定入口網站應用程式定義的詳細資訊：



9.4 管理已註冊的入口網站應用程式

「入口網站應用程式管理」頁面可讓您執行入口網站應用程式中，與入口網站應用程式註冊相關的下列任務：

- ◆ 「存取已部署之入口網站應用程式中的入口網站應用程式註冊」，第 169 頁
- ◆ 「檢視入口網站應用程式註冊的相關資訊」，第 169 頁
- ◆ 「指定入口網站應用程式註冊的類別」，第 170 頁
- ◆ 「修改入口網站應用程式註冊的設定」，第 171 頁
- ◆ 「修改入口網站應用程式註冊的優先設定」，第 174 頁
- ◆ 「指定入口網站應用程式註冊的安全性權限」，第 176 頁
- ◆ 「取消註冊入口網站應用程式」，第 179 頁

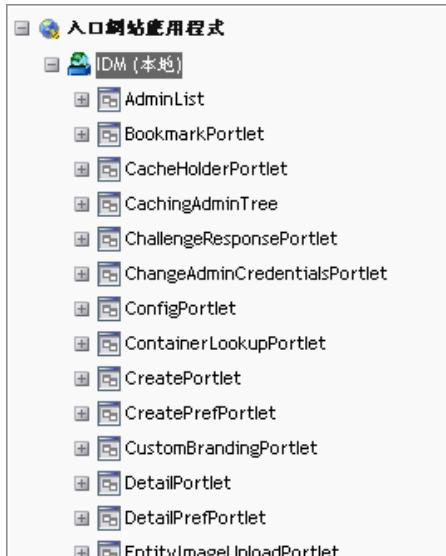
9.4.1 存取已部署之入口網站應用程式中的入口網站應用程式註冊

「入口網站應用程式」清單會顯示選定入口網站應用程式中，每個入口網站應用程式定義的入口網站應用程式註冊。

若要存取已部署之入口網站應用程式中的入口網站應用程式註冊，請執行下列動作：

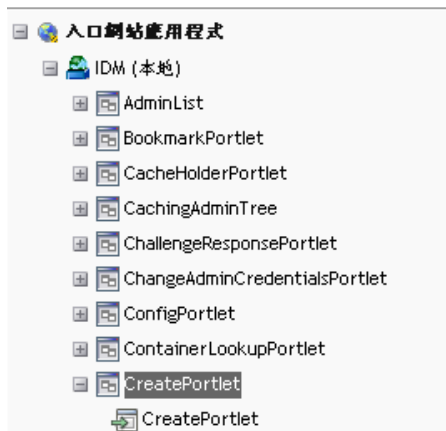
- 1 在「入口網站應用程式」清單中，展開您要存取其入口網站應用程式定義和註冊的入口網站應用程式。

網路樹即會顯示該入口網站應用程式下的所有入口網站應用程式定義：



- 2 展開您要存取其入口網站應用程式註冊的入口網站應用程式定義。

網路樹即會顯示該入口網站應用程式定義下的所有入口網站應用程式註冊：



9.4.2 檢視入口網站應用程式註冊的相關資訊

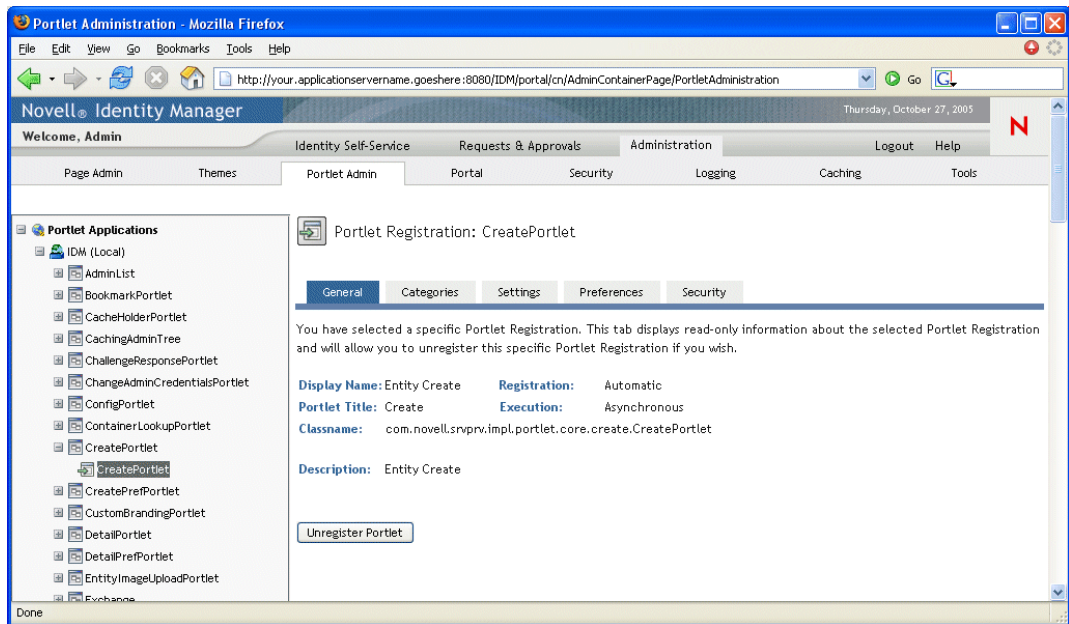
您可以檢視已列出之入口網站應用程式註冊的下列唯讀資訊：

- ◆ 顯示名稱

- ◆ 註冊類型
- ◆ 入口網站應用程式標題
- ◆ 執行類型 (同步或非同步)
- ◆ 類別名稱
- ◆ 描述

若要檢視入口網站應用程式註冊的相關資訊，請執行下列動作：

- ◆ 在「入口網站應用程式」清單中，選取您要瞭解的入口網站應用程式註冊。
- 「一般」面板即會顯示在右側，顯示選定入口網站應用程式註冊的相關資訊：



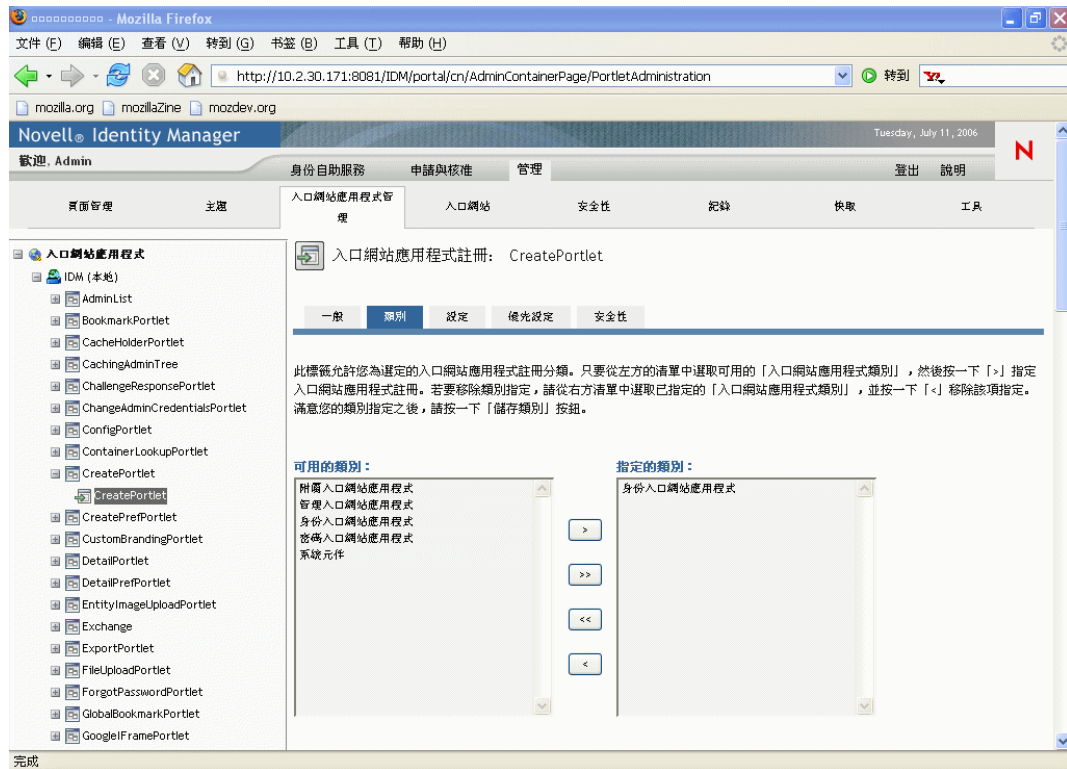
9.4.3 指定入口網站應用程式註冊的類別

若要加速在入口網站應用程式中對於特定入口網站應用程式的搜尋，您可以按照類別來組織入口網站應用程式註冊。

若要指定入口網站應用程式註冊的類別，請執行下列動作：

- 1 在「入口網站應用程式」清單中，選取您要分類的入口網站應用程式註冊。
「一般」面板即會顯示在右側。
- 2 移至「類別」面板。

此面板會顯示選定入口網站應用程式註冊之可用且已指定的類別清單：



3 視情況更新「指定的類別」清單：

如果想要	執行下列動作
指定一或多個類別給入口網站應用程式註冊	選取您想要指定的每個類別，然後按一下「>」
將所有類別指定給入口網站應用程式註冊	按一下「>>」
移除一或多個類別指定	選取要移除的每個類別，然後按一下「<」
移除所有類別指定	按一下「<<」

4 按一下「儲存類別」。

9.4.4 修改入口網站應用程式註冊的設定

入口網站應用程式設定會定義入口網站 (Identity Manager 使用者應用程式) 如何與個別入口網站應用程式互動。每個入口網站應用程式都會以下列設定進行組態的設定：

- ◆ 標題
- ◆ 最大逾時
- ◆ 需要驗證
- ◆ 顯示標題列
- ◆ 對使用者隱藏

- ◆ 在入口網站應用程式中定義的選項

在入口網站應用程式 WAR 的入口網站應用程式部署描述元 (portlet.xml) 中定義有標準 Java Portlet 1.0 設定。您可以使用「入口網站應用程式管理」頁面，以逐步註冊的方式，來變更這些設定的值。在這種情況下，新的值僅會對選定入口網站應用程式註冊生效。

若要修改入口網站應用程式註冊的設定，請執行下列動作：

- 1** 在「入口網站應用程式」清單中，選取您要修改其設定的入口網站應用程式註冊。
「一般」面板即會顯示在右側。
- 2** 移至「設定」面板。

此面板會顯示選定入口網站應用程式註冊的目前設定：

The screenshot shows the 'Novell Identity Manager' interface in Mozilla Firefox. The browser address bar shows the URL: `http://10.2.30.194:8081/IDM/portal/cn/AdminContainerPage/PortletAdministration`. The page title is '入口網站應用程式註冊：CreatePortlet'. The interface is in Chinese and includes a navigation menu on the left with '入口網站應用程式' expanded to show 'CreatePortlet' selected. The main content area has tabs for '一般', '類別', '設定', '優先設定', and '安全性', with '設定' (Settings) selected. Below the tabs, there is a warning message: '此標籤可讓您修改此內容列項的任何可用設定。對於這些設定所進行的任何修改僅會對此特定的內容列項生效。' (This tag allows you to modify any available settings for this content item. Any changes made to these settings will only apply to this specific content item.)

The '設定' (Settings) section contains two tables:

標題	設定名稱	設定值	描述
重設	預設值	Create	內容標題。
重設	inglés	Create	
重設	alemán	Erstellen	
重設	francés	Créer	
重設	español	Crear	
重設	italiano	Creazione entità	
重設	japonés	作成	
重設	holandés	Maken	
重設	portugués	Criar	
重設	chino (China)	創建	
重設	chino (Taiwán)	建立	

選項	設定名稱	設定值	描述
重設	最大逾時	0	要使用的最大逾時。請指定零秒數目或 0 表示無逾時。
重設	需要驗證	<input checked="" type="radio"/> True <input type="radio"/> False	執行前需要驗證。
重設	顯示標題列	<input checked="" type="radio"/> True <input type="radio"/> False	標題列功能在顯示時應為啟用狀態。
重設	向使用者隱藏	<input type="radio"/> True <input checked="" type="radio"/> False	使用者修改使用者頁面的內容時，在「內容選擇器」中隱藏註冊。
重設	說明	<input checked="" type="radio"/> True <input type="radio"/> False	提供關於此內容的其他資訊。
重設	編輯	<input type="radio"/> True <input checked="" type="radio"/> False	顯示編輯優先設定的螢幕。
重設	列印	<input type="radio"/> True <input checked="" type="radio"/> False	顯示入口網站應用程式之內容的友善列印格式版本。
重設	最小化	<input checked="" type="radio"/> True <input type="radio"/> False	將此內容最小化，僅顯示標題列。
重設	還原	<input checked="" type="radio"/> True <input type="radio"/> False	還原最小化或最大化的內容至其正常觀看狀態。
重設	最大化	<input checked="" type="radio"/> True <input type="radio"/> False	將內容最大化，以便使其能以瀏覽器的整個畫面顯示。

At the bottom of the settings section, there are three buttons: '儲存設定' (Save Settings), '取消' (Cancel), and '重設全部' (Reset All).

3 視情況修改設定。

使用此面板時，請注意您還可以執行下列動作：

如果想要	執行下列動作
丟棄未儲存的變更	按一下「取消」
將此入口網站應用程式註冊的所有設定還原為預設值 (如對應的入口網站應用程式定義中所定義)	按一下「全部重設」
將個別設定還原為預設值	按一下設定旁邊的「重設」連結

4 按一下「儲存設定」。

9.4.5 修改入口網站應用程式註冊的優先設定

入口網站應用程式優先設定是由入口網站應用程式開發人員於設計時期，在入口網站應用程式部署描述元中加以定義。根據入口網站應用程式開發人員的實作，每個入口網站應用程式的優先設定都會不同。

您可以使用「入口網站應用程式管理」頁面，以逐步註冊的方式，來變更這些優先設定的值。在這種情況下，新的值僅會對選定入口網站應用程式註冊生效。

若要修改入口網站應用程式註冊的優先設定，請執行下列動作：

- 1 在「入口網站應用程式」清單中，選取您要修改其優先設定的入口網站應用程式註冊。
「一般」面板即會顯示在右側。
- 2 移至「優先設定」面板。

此面板會顯示選定入口網站應用程式註冊的目前優先設定：



3 視情況修改優先設定。

使用此面板時，請注意您還可以執行下列動作：

如果想要	執行下列動作
顯示優先設定的相關資訊	按一下「 描述 」
丟棄未儲存的變更	按一下「 取消 」
將此入口網站應用程式註冊的所有優先設定還原為預設值 (如對應的入口網站應用程式定義中所定義)	按一下「 全部重設 」
將個別優先設定還原為預設值	按一下優先設定旁邊的「 重設 」連結

4 若要修改入口網站應用程式定義中指定之每個地區設定的優先設定當地語系化版本，請遵循下列步驟：

- 4a** 按一下優先設定旁邊的「詳細資料」連結 (如果可用)。
 - 面板即會顯示每個地區設定的優先設定值。
- 4b** 視情況修改這些值。
- 4c** 按一下「確定」，以套用您的變更，並返回主優先設定清單。

5 按一下「儲存優先設定」。

9.4.6 指定入口網站應用程式註冊的安全性權限

您可以針對入口網站應用程式註冊，指定下列安全性權限給使用者、群組和容器：

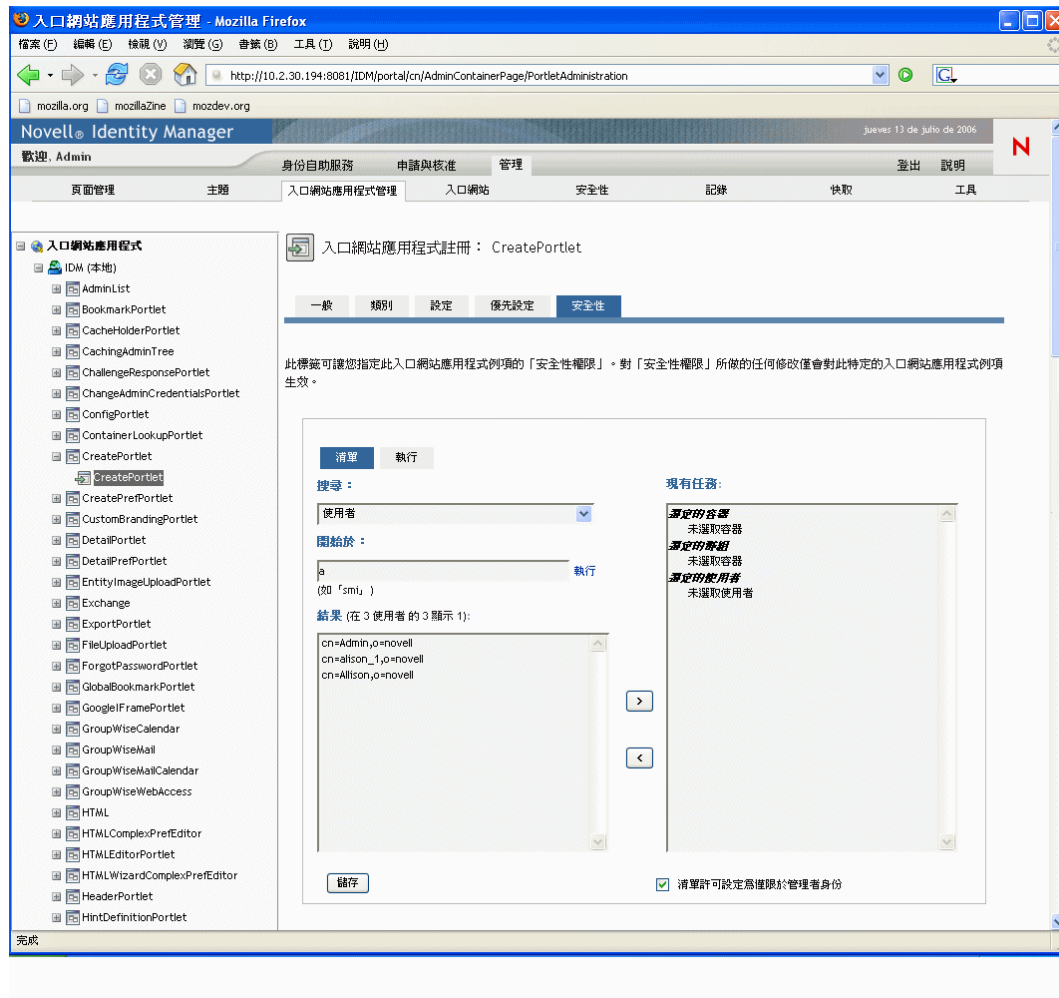
許可	描述
列出	使用者可以從選項清單 檢視 入口網站應用程式註冊
執行	使用者可以在入口網站頁面上， 執行 入口網站應用程式註冊

當您修改安全性權限時，新值僅會對選定入口網站應用程式註冊生效。

若要指定入口網站應用程式註冊的安全性權限，請執行下列動作：

- 1 在「入口網站應用程式」清單中，選取您要修改其安全性權限的入口網站應用程式註冊。
「一般」面板即會顯示在右側。
- 2 移至「安全性」面板。

此面板會顯示選定入口網站應用程式註冊的目前安全性權限：



3 視您要指定的許可類型而定，移至「清單」或「執行」索引標籤。

4 指定下列搜尋設定的值：

設定	操作
搜尋	從下拉式功能表選取下列其中一項： <ul style="list-style-type: none"> ◆ 使用者 ◆ 群組 ◆ 容器

設定	操作
開頭為	<p>如果您想要：</p> <ul style="list-style-type: none"> ◆ 尋找所有指定類型的可用物件 (使用者、群組或容器)，請將此設定留為空白。 ◆ 在那些物件中尋找子集，請輸入您想要之 CN 值的開始字元 (不考量大小寫，不支援萬用字元)。 <p>例如，搜尋開頭為 S 的群組會縮小您的搜尋結果，如下所示：</p> <pre>cn=Sales,ou=groups,o=MyOrg</pre> <pre>cn=Service,ou=groups,o=MyOrg</pre> <pre>cn=Shipping,ou=groups,o=MyOrg</pre> <p>搜尋開頭為 Se 的群組會傳回：</p> <pre>cn=Service,ou=groups,o=MyOrg</pre>

5 按一下「執行」。

搜尋的結果即會顯示在「結果」清單中。

6 選取您想要指定給入口網站應用程式註冊的使用者、群組或容器，然後按一下「新增(>)」按鈕。

提示：按住 *Ctrl* 鍵以選取多個項目。

7 啟用或停用入口網站應用程式註冊的「鎖定」，如下所示：

如果您想要	執行下列動作
鎖定入口網站應用程式註冊，以便只有「使用者應用程式管理員」可以列出/執行它	核取「 清單 sol; 執行許可設定為僅限於管理者身份 」
允許所有指定的使用者、群組和容器列出/執行入口網站應用程式註冊	取消核取「 清單 sol; 執行許可設定為僅限於管理者身份 」

附註：如果您取消核取此設定，但是沒有將任何使用者、群組或容器明確地指定給入口網站應用程式註冊，則針對此入口網站應用程式註冊，**每個人都具有「清單/執行」許可**。

8 按一下「儲存」。

9.4.7 取消註冊入口網站應用程式

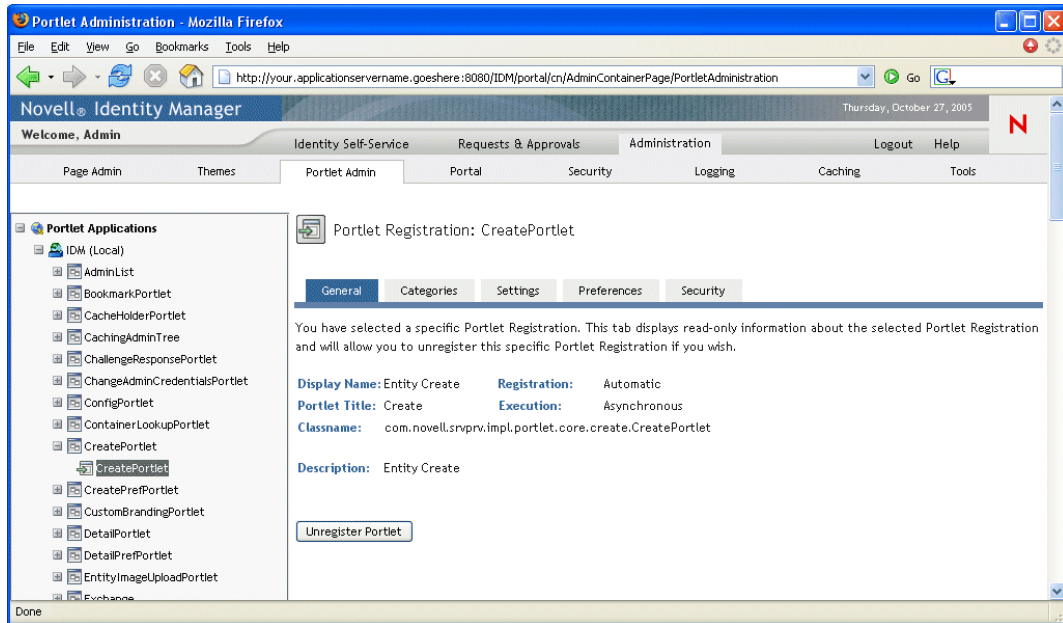
您可以使用「入口網站應用程式管理」頁面來視需要取消註冊入口網站應用程式。

附註：如果您取消註冊定義為自動註冊的入口網站應用程式，則當您重新啟動應用程式伺服器時，會重新自動註冊該入口網站應用程式。

若要取消註冊入口網站應用程式，請執行下列動作：

- 1 請在「入口網站應用程式」清單中，選取您想要取消註冊的入口網站應用程式註冊。

即會在右邊顯示「一般」面板，其顯示已選取入口網站註冊的相關資訊：



- 2 按一下「取消註冊入口網站應用程式」。
- 3 當提示您確認取消註冊操作時，按一下「確定」。

入口網站組態

本章說明如何使用 Identity Manager 使用者介面之「管理」索引標籤上的「入口網站」頁面。主題包含：

- ◆ 「關於入口網站組態」，第 181 頁
- ◆ 「一般設定」，第 181 頁
- ◆ 「LDAP 連接參數」，第 184 頁

如需存取和使用「管理」索引標籤的一般資訊，請參閱第 6 章「使用管理索引標籤」，第 115 頁。

10.1 關於入口網站組態

您可以使用「入口網站」頁面，來控制 Identity Manager 使用者應用程式的入口網站特性，並指定使用者應用程式如何連接到身份儲存區 (LDAP 提供者)。

10.2 一般設定

「入口網站應用程式」頁面提供您可以用於進行下列動作的「一般設定」面板：

- ◆ 暫時對 Identity Manager 使用者應用程式變更部份入口網站特性 (直到下一次應用程式伺服器重新啟動或使用者應用程式重新部署為止)
- ◆ 針對 Identity Manager 使用者應用程式檢視其他入口網站特性

若要管理一般設定，請執行下列動作：

- 1 在「入口網站」頁面上，從左導覽功能表選取「一般設定」。

「一般設定」面板即會顯示：



- 2 如果您有多個「War 網路位置」，則選取您想要存取其設定的一個 War 網路位置。重新整理面板，以顯示您選擇之網路位置的目前設定。
- 3 視情況檢查並修改這些設定。如需詳細資料，請參閱：
 - ◆ 「您可以變更的設定」，第 182 頁
 - ◆ 「唯讀設定」，第 183 頁
- 4 如果要套用所做的變更，請按一下「儲存」。

10.2.1 您可以變更的設定

您可以修改「一般設定」面板上的若干入口網站設定。您的值會在下一次應用程式伺服器重新啟動或使用者應用程式重新部署之前保持有效。若重新啟動或重新部署，這些設定就會回復為使用者應用程式 WAR 的預設值。

設定	操作
預設申請逾時	<p>指定申請在逾時前等待的預設時間 (以毫秒為單位)。</p> <p>如果沒有任何非同步入口網站應用程式定義逾時，或者沒有任何入口網站應用程式定義超過其值的逾時，則會使用此預設值。如果要轉換的一或多個入口網站應用程式定義的逾時超過此預設值，則會使用較大的值來代替預設值。</p> <p>此設定可用來保護應用程式，以免收到過多指出該入口網站應用程式已逾時的訊息 (如果入口網站應用程式定義的逾時值太小，就可能出現這種情況)。</p> <hr/> <p>附註：如果在逾時前即可轉換所有入口網站應用程式，便會立即將申請傳回給用戶端。</p>
申請逾時最大值	<p>指定阻礙完成申請的最大時間值 (以毫秒為單位)。這表示在經過這段時間後，無論任何入口網站應用程式是否定義較大的逾時值，都會將每個申請傳回給用戶端。</p> <p>此設定可以用於確保即使一或多個入口網站應用程式定義較大的逾時值，入口網站仍會及時回應。</p>
平行入口網站應用程式轉換	<p>啟用或停用入口網站中的非同步入口網站應用程式轉換。</p> <p>這是在預設狀態下停用的進階功能。如果您啟用此功能，則入口網站會將非同步轉換申請指定給個別線串 (允許入口網站應用程式平行轉換內容)。</p> <p>停用此功能時，所有入口網站應用程式都會同步轉換主要申請線串中的內容。</p>
強制入口網站應用程式轉換逾時	<p>決定是否將非同步入口網站應用程式委派給主要申請線串，以便在線串儲存池中沒有足夠可用的個別線串時轉換內容。</p> <p>如果您選擇「否」，則在沒有任何可用的個別線串時，會在主要申請線串中執行非同步入口網站應用程式。</p> <p>選擇「是」會強制非同步入口網站應用程式等待，直到轉換內容前有可用的個別線串為止。如果入口網站應用程式在執行轉換申請之前逾時，則會在入口網站應用程式視窗中產生入口網站應用程式特定的錯誤訊息。</p>
強制同步入口網站應用程式序列轉換	<p>決定如何執行同步入口網站應用程式。</p> <p>如果您選擇「是」，則所有同步入口網站應用程式都會在主要申請線串中執行。</p> <p>選擇「否」可讓入口網站配置個別的線串，以處理同步轉換申請 (從而防止在主要申請線串中出現瓶頸)。</p>

10.2.2 唯讀設定

下列顯示的設定僅供參考，並且無法在「一般設定」面板上進行變更：

入口網站首頁路徑	預設配置
入口網站控制器之伺服器常式路徑	預設樣式

入口網站應用程式路徑

預設主題

入口網站登入頁面路徑

入口網站資源路徑

預設容器頁面

這些設定值是在使用者應用程式 WAR 中設定 (請注意,「預設主題」反映您在「主題」頁面中選擇的目前主題)。

10.3 LDAP 連接參數

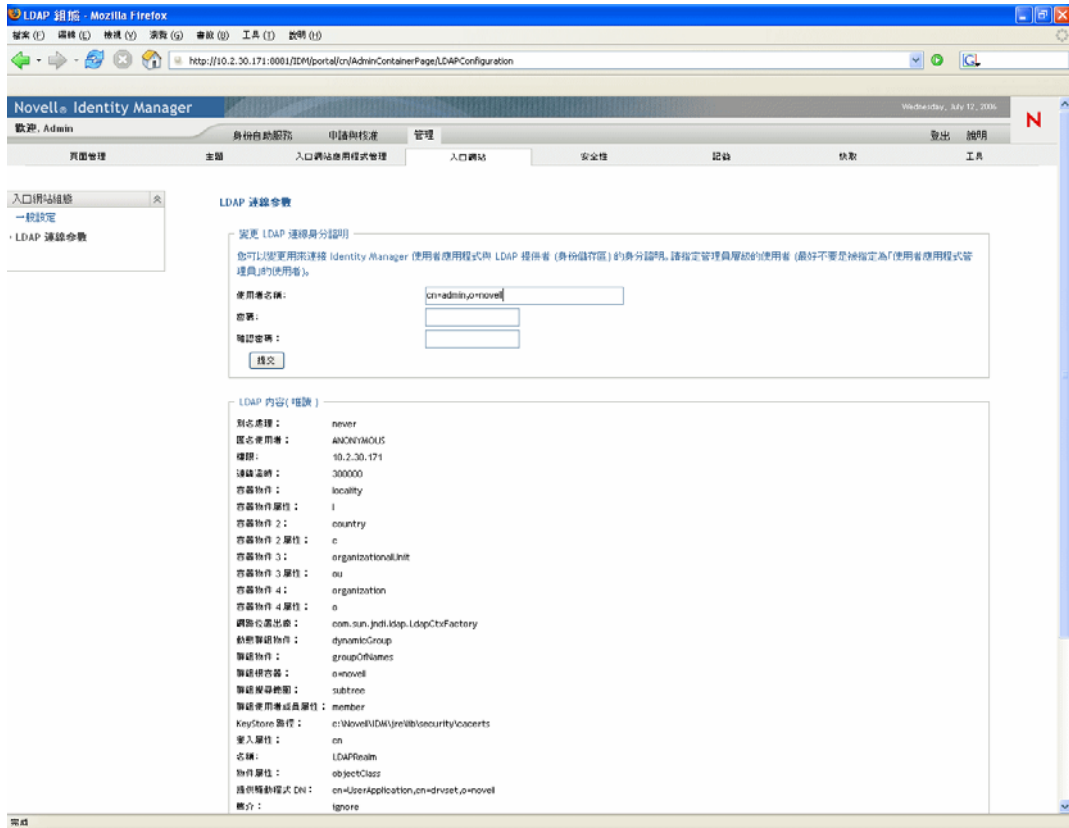
「入口網站」頁面提供您可以用於執行下列動作的「LDAP 連接參數」面板：

- ◆ 連接至身份儲存區 (LDAP 提供者) 時,變更身分證明 (由 Identity Manager 使用者應用程式所使用)
- ◆ 針對 Identity Manager 使用者應用程式,檢視其他 LDAP 內容

若要管理 LDAP 連接參數,請執行下列動作：

- 1 請在「入口網站」頁面上,從左導覽功能表選取「LDAP 連接參數」。

「LDAP 連接參數」即會顯示：



- 2 視情況檢查並修改這些設定。如需詳細資訊,請參閱：

- ◆ 「您可以變更的設定」,第 182 頁

- ◆ 「唯讀設定」，第 185 頁

3 如果要套用所做的變更，則按一下「提交」。

10.3.1 您可以變更的設定

在「LDAP 連接參數」面板上，您可以修改每當 Identity Manager 使用者應用程式連接至身份儲存區 (LDAP 提供者) 時要使用之身分證明的設定。您在此面板上進行的變更會儲存到使用者應用程式的資料庫，供執行時期使用，並且對照身份儲存區進行檢查 (請注意，此面板不會更新安裝期間使用者應用程式 WAR 中記錄的原始身分證明值)。

設定	操作
使用者名稱	<p>輸入在身份儲存區中具有完整管理員權限之使用者的名稱。Identity Manager 使用者應用程式需要以管理員的身份存取身份儲存區，以進行運作。</p> <p>通常是將身份儲存區的根部管理員指定為 LDAP 連接使用者名稱。根部管理員可完全控制網路樹，因此，您無需指定任何特殊的託管者權限。</p> <p>例如：</p> <pre>cn=admin,o=myorg</pre> <p>如果您指定其他使用者，則您需要將可承襲之託管者權限，指定給您使用者應用程式驅動程式上的內容「所有屬性權限」和「項目權限」。</p> <hr/> <p>附註：若要避免混淆，建議您不要將使用者應用程式的「使用者應用程式管理員」指定為 LDAP 連接使用者名稱。對於這兩種不同的目的，最好使用不同的帳戶。</p>
密碼	輸入目前為身份儲存區中該使用者名稱設定的密碼。
和	
確認密碼	

10.3.2 唯讀設定

下列顯示的設定僅供參考，並且無法在「LDAP 連接參數」面板上進行變更：

ALIAS_HANDLING	GROUP_USER_MEMBER_ATTRIB
ANONYMOUS_USER	KEYSTORE_PATH
AUTHORITY	LOGIN_ATTRIBUTE
CONNECTION_TIMEOUT	NAME
CONTAINER_OBJECT	OBJECT_ATTRIB
CONTAINER_OBJECT_ATTRIB	PROVISION_ROOT
CONTAINER_OBJECT2	REFERRAL

CONTAINER_OBJECT2_ATTRIB	ROOT_NAME
CONTAINER_OBJECT3	USE_DYNAMIC_GROUPS
CONTAINER_OBJECT3_ATTRIB	USE_REGISTERED_DYNAMIC_GROUPS
CONTAINER_OBJECT4	USE_SSL
CONTAINER_OBJECT4_ATTRIB	USER_GROUP_MEMBER_ATTRIB
CONTEXT_FACTORY	USER_OBJECT
DYNAMIC_GROUP_OBJECT	USER_ROOT_CONTAINER
GROUP_OBJECT	USER_SEARCH_SCOPE
GROUP_ROOT_CONTAINER	UUID_ATTRIB
GROUP_SEARCH_SCOPE	UUID_AUX_CLASS

這些設定值是在您安裝使用者應用程式時決定的。

安全性組態

本章說明如何使用 Identity Manager 使用者介面之「管理」索引標籤上的「安全性」頁面。主題包含：

- ◆ 「關於安全性組態」，第 187 頁
- ◆ 「指定使用者應用程式管理員」，第 188 頁

如需有關存取和使用「管理」索引標籤的一般資訊，請參閱第 6 章「使用管理索引標籤」，第 115 頁。

11.1 關於安全性組態

您可以使用「安全性」頁面，指定 Identity Manager 使用者應用程式的「使用者應用程式管理員」。

「使用者應用程式管理員」有權執行與 Identity Manager 使用者應用程式相關的所有管理功能。這包含存取 Identity Manager 使用者介面的「管理」索引標籤，以執行其支援的任何管理動作。

在安裝期間，會將使用者指定為「使用者應用程式管理員」。安裝之後，該使用者可以使用「安全性」頁面，視需要指定其他的「使用者應用程式管理員」。

做為「使用者應用程式管理員」的使用者通常應該位於使用者根容器下，其在使用者應用程式的 LDAP 組態中指定；這樣會讓使用者依使用者名稱即可登入（而不是每次都需要完全可辨識名稱）。通常此使用者在網路樹中具有維護和建立物件的權限，不過，這並不是必要的。

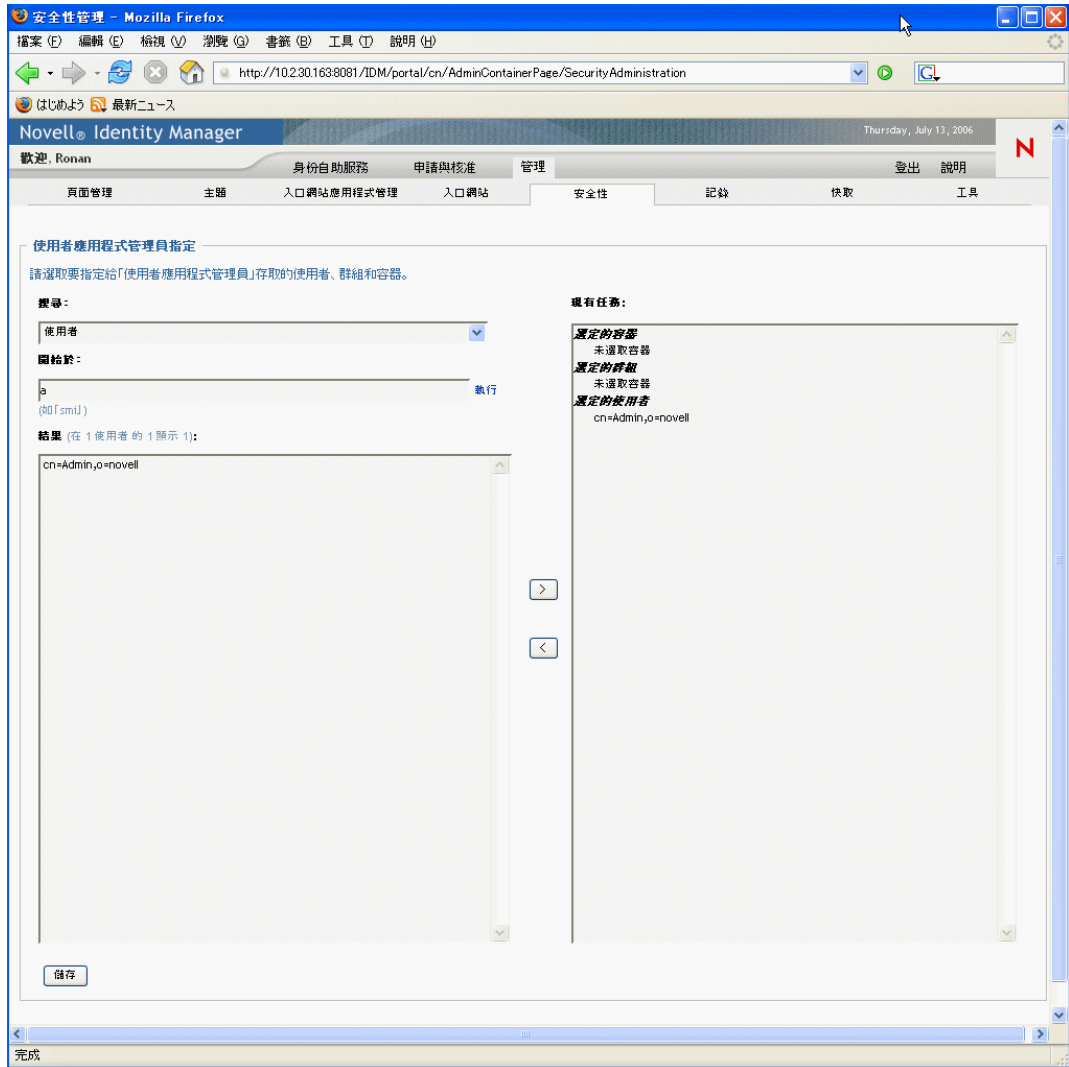
附註：必要時，「使用者應用程式管理員」可以指定許可，讓一或多位一般使用者可以看見及存取「管理」索引標籤上的特定頁面。而這些許可可使用「管理」索引標籤上的「頁面管理」頁面，來予以指定（如需詳細資料，請參閱第 7 章「頁面管理」，第 121 頁）。

11.2 指定使用者應用程式管理員

指定「使用者應用程式管理員」時，您可以指定使用者、群組或容器。

若要指定使用者應用程式管理員，請執行下列動作：

- 1 移至「安全性」頁面：



- 2 指定下列搜尋設定的值：

設定	操作
搜尋	從下拉式功能表選取下列其中一項： <ul style="list-style-type: none">◆ 使用者◆ 群組◆ 容器

設定	操作
開頭為	<p>如果您想要：</p> <ul style="list-style-type: none"> ◆ 尋找所有指定類型的可用物件 (使用者、群組或容器)，請將此設定留為空白。 ◆ 在那些物件中尋找子集，請輸入您想要之 CN 值的開始字元 (不考量大小寫，不支援萬用字元)。 <p>例如，搜尋開頭為 S 的群組會縮小您的搜尋結果，如下所示：</p> <pre>cn=Sales,ou=groups,o=MyOrg</pre> <pre>cn=Service,ou=groups,o=MyOrg</pre> <pre>cn=Shipping,ou=groups,o=MyOrg</pre> <p>搜尋開頭為 Se 的群組會傳回：</p> <pre>cn=Service,ou=groups,o=MyOrg</pre>

3 按一下「執行」。

您搜尋的結果會顯示在「結果」清單中。

4 選取您想要指定為「使用者應用程式管理員」的使用者、群組或容器，然後按一下「新增 (>)」按鈕。

提示：按住 *Ctrl* 鍵以選取多個項目。

5 按一下「儲存」。

若要取消指定「使用者應用程式管理員」，請執行下列動作：

1 在「現有任務」清單中，選取您想要取消其「使用者應用程式管理員」身份的使用者、群組或容器，然後按一下「移除 (<)」按鈕。

提示：按住 *Ctrl* 鍵以選取多個項目。

2 按一下「儲存」。

記錄組態

本章說明如何使用 Identity Manager 使用者介面之「管理」索引標籤上的「記錄」頁面。主題包含：

- ◆ 「關於記錄組態」，第 191 頁
- ◆ 「關於記錄」，第 191 頁
- ◆ 「變更記錄層級」，第 193 頁
- ◆ 「將記錄訊息傳送至 Novell Audit」，第 194 頁
- ◆ 「沿用您的記錄設定」，第 194 頁

如需存取和使用「管理」索引標籤的一般資訊，請參閱第 6 章「使用管理索引標籤」，第 115 頁。

12.1 關於記錄組態

您可以使用「記錄」頁面，控制想要讓 Identity Manager 使用者應用程式產生的記錄訊息層級，並指定是否要將那些訊息傳送至 *Novell Audit*。

Identity Manager 使用者應用程式會使用 *log4j* (The Apache Software Foundation 配送的開放原始碼記錄套件) 來實作記錄。在預設狀態下，事件訊息會記錄到下列各項：

- ◆ 部署了 Identity Manager 使用者應用程式之應用程式伺服器的系統主控台。
- ◆ 該應用程式伺服器上的記錄檔案，例如：

```
jboss/server/IDM/log/server.log
```

這是可以延展的記錄檔，一旦它達到某個大小，就會延展至其他檔案(等等)。

如果您已設定環境的組態以包含 *Novell Audit*，則您同時可以選擇在其中記錄事件訊息。

如需設定記錄環境和 *Novell Audit* 之組態的詳細資料，請參閱第 5 章「設定記錄」，第 105 頁。

12.2 關於記錄

「記錄」頁面會列出各種記錄，其中每個記錄都從 Identity Manager 使用者應用程式的不同部份輸出事件訊息。每個記錄本身都具有獨立的輸出層級。

記錄名稱以 *log4j* 慣例為基礎。您會在產生的事件訊息中看到這些記錄名稱，它們表示訊息輸出的網路位置。

記錄名稱	描述
com.novell	其他 Identity Manager 使用者應用程式記錄的父記錄
com.novell.afw.portal.aggregation	與入口網站頁面處理相關的訊息

記錄名稱	描述
com.novell.afw.portal.persist	與入口網站資料持續性相關的訊息 (包含入口網站頁面和入口網站應用程式註冊)
com.novell.afw.portal.portlet	入口網站核心入口網站應用程式和附屬入口網站應用程式的訊息
com.novell.afw.portal.util	入口網站輸入 / 輸出和導覽入口網站應用程式的訊息
com.novell.afw.portlet.consumer	與入口網站應用程式轉換相關的訊息
com.novell.afw.portlet.core	與核心入口網站應用程式 API 相關的訊息
com.novell.afw.portlet.persist	與入口網站應用程式資料持續性相關的訊息 (包含入口網站應用程式優先設定和設定值)
com.novell.afw.portlet.producer	與入口網站中入口網站應用程式之註冊和組態相關的訊息
com.novell.afw.portlet.util	與入口網站應用程式所使用之公用程式程式碼相關的訊息
com.novell.afw.theme	主題子系統的訊息
com.novell.afw.util	與入口網站公用程式類別相關的訊息
com.novell.soa.af.impl	核准流程 (提供工作流程) 子系統的訊息
com.novell.srvprv.apwa	「申請和核准」 Web 應用程式 (動作和標籤) 的訊息
com.novell.srvprv.impl.portlet.core	核心身份入口網站應用程式和密碼入口網站應用程式的訊息
com.novell.srvprv.impl.portlet.util	身份相關之公用程式入口網站應用程式的訊息
com.novell.srvprv.impl.servlet	UI 控制架構之 ajax 伺服器常式和 ajax 服務的訊息
com.novell.srvprv.impl.uictrl	UI 控制登錄 API 和核准格式轉換的訊息
com.novell.srvprv.impl.vdata	目錄抽象層的訊息
com.novell.srvprv.spi	UI 控制登錄 API 的訊息
com.sssw.fw.cachemgr	與架構快取子系統相關的訊息
com.sssw.fw.core	與架構核心子系統相關的訊息
com.sssw.fw.directory	與架構目錄子系統相關的訊息
com.sssw.fw.event	與架構事件子系統相關的訊息
com.sssw.fw.factory	與架構出廠子系統相關的訊息
com.sssw.fw.persist	與架構持續性子系統相關的訊息
com.sssw.fw.resource	與架構資源子系統相關的訊息
com.sssw.fw.security	與架構安全性子系統相關的訊息
com.sssw.fw.server	與架構伺服器子系統相關的訊息
com.sssw.fw.servlet	與架構伺服器常式子系統相關的訊息
com.sssw.fw.session	與架構會期子系統相關的訊息
com.sssw.fw.usermgr	與架構使用者子系統相關的訊息
com.sssw.fw.util	與架構公用程式子系統相關的訊息

記錄名稱	描述
com.sssw.portal.manager	與「入口網站管理員」相關的訊息
com.sssw.portal.persist	與入口網站持續性相關的訊息

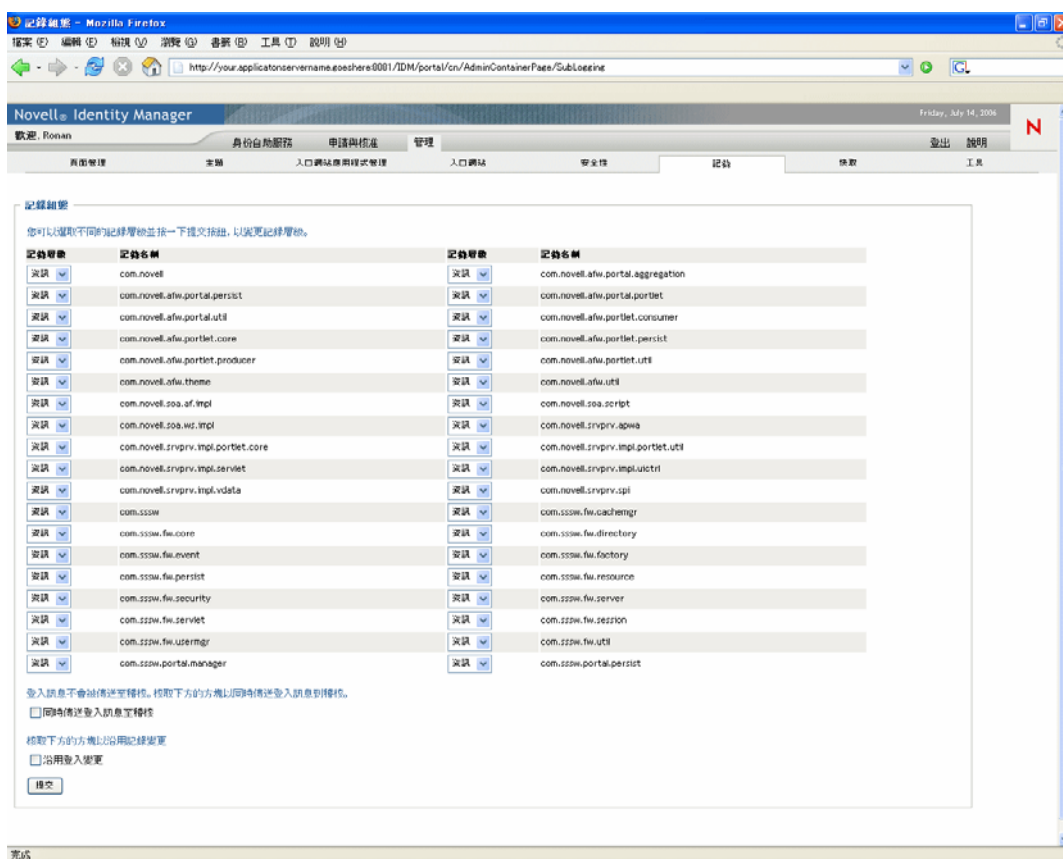
請注意，使用者應用程式的記錄是階層式的。例如，com.novell 是其下面其他記錄的父代。任何其他記錄都會承襲它的內容。

12.3 變更記錄層級

您可以藉由變更為其設定的層級，來控制寫入特定記錄的資訊量。在預設狀態下，所有記錄都會設為 *Info*，而這是中介層級。

若要變更記錄層級，請執行下列動作：

- 1 移至「記錄」頁面：



- 2 在頁面頂端，尋找記錄（該記錄的層級是您想要變更的）。
- 3 使用下拉式功能表來選取下列其中一個層級：

層級	描述
嚴重	最少的詳細資料： 將嚴重錯誤寫入記錄
錯誤	將錯誤 (和上述所有項目) 寫入記錄
警告	將警告 (和上述所有項目) 寫入記錄
資訊	將資訊訊息 (和上述所有項目) 寫入記錄
除錯	將除錯資訊 (和上述所有項目) 寫入記錄
追蹤	最多的詳細資料： 將追蹤資訊 (和上述所有項目) 寫入記錄

4 視需要，針對其他記錄重複 [步驟 2](#) 和 [步驟 3](#)。

5 按一下「提交」。

12.4 將記錄訊息傳送至 Novell Audit

您可以使用「記錄」頁面，控制 Identity Manager 使用者應用程式是否要將事件訊息輸出傳送至 Novell Audit。除非您在安裝使用者應用程式時開啓 Novell Audit 記錄，否則在預設狀態下，是關閉狀態。

若要將 Novell Audit 記錄在開啓 / 關閉之間切換，請執行下列動作：

- 1 移至「記錄」頁面。
- 2 視情況核取或取消核取下列設定：

Audit

- 3 按一下「提交」。

12.5 沿用您的記錄設定

在預設狀態下，除非下一次應用程式伺服器重新啓動或使用者應用程式重新部署，否則您在「記錄」頁面上進行的變更會一直保持有效。之後，記錄設定會回復為其預設值。

但是「記錄」頁面可讓您選擇沿用其設定的變更。如果您開啓此功能，會將記錄設定值儲存在部署 Identity Manager 使用者應用程式之應用程式伺服器上的記錄組態檔案中。例如：

```
jboss/server/IDM/conf/extendlogging.xml
```

若要切換設定的持續性為開啓 / 關閉，請執行下列動作：

- 1 移至「記錄」頁面。
- 2 視情況核取或取消核取下列設定：

™u•EµnSŸ< ßÛ

3 按一下「提交」。

快取組態

本章說明如何使用 Identity Manager 使用者介面之「管理」索引標籤上的「快取」頁面。主題包含：

- ◆ 「關於快取組態」，第 197 頁
- ◆ 「衝洗快取」，第 198 頁
- ◆ 「設定快取設定的組態」，第 199 頁

如需存取和使用「管理」索引標籤的一般資訊，請參閱第 6 章「使用管理索引標籤」，第 115 頁。

13.1 關於快取組態

您可以使用「快取」頁面，管理 Identity Manager 使用者應用程式所維護的各種快取。使用者應用程式會使用這些快取，在應用程式伺服器上儲存可重複使用的暫時資料，以便其可以最佳化效能。

您可以藉由衝洗其內容以及變更其組態設定，在必要時控制這些快取。

13.2 衝洗快取

快取的命名是根據在 Identity Manager 使用者應用程式中使用快取的子系統。通常，由於使用者應用程式會基於其資料的使用頻率或來源資料的變更時間自動進行衝洗，因此您無需自行衝洗。但是，如果您有特定的需求，則可以手動衝洗已選取的快取或所有的快取。

若要衝洗快取，請執行下列動作：

- 1 移至「快取」頁面：

快取管理

衝洗快取

從清單中選擇快取，然後按一下「衝洗快取」按鈕以衝洗快取。

全部衝洗

衝洗快取

叢集快取狀態

叢集狀態

對於目前叢集狀態的所有變更將在應用程式下次啟動時生效。群組 ID 必須是與 JBoss 所保留的叢集名稱 DefaultPartition 或 TrueCache 不符合的唯一名稱。只有具備經驗的管理員才能更改叢集內容。進行變更之前，請先參考 JBoss 文件。

	目前	全補	應用本地	本地
叢集已開啟：	是	是	<input type="checkbox"/>	
群組 ID：	c373e901aba5e8ee996644453544200	c373e901aba5e8ee996644453544200	<input type="checkbox"/>	
叢集內容：	機核	[[OF@ncost_addr+228.8.8,ymcost_po]	<input type="checkbox"/>	

快取狀態

對於目前快取狀態的所有變更將在應用程式下次啟動時生效。(* 表示需要)

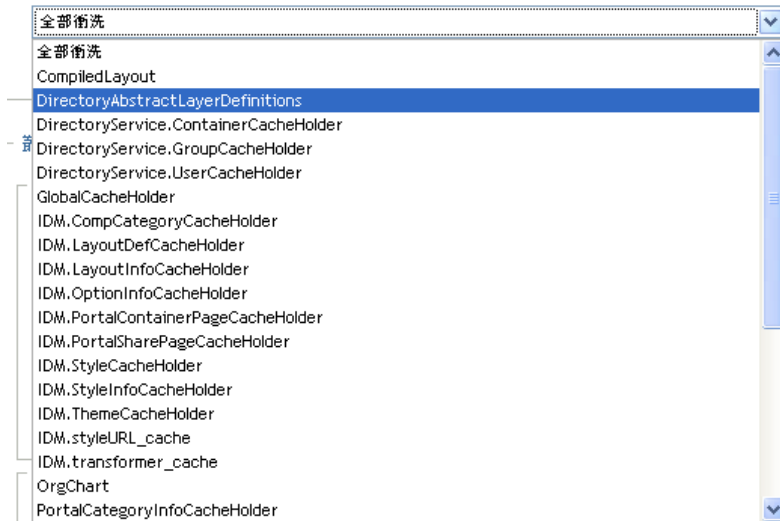
	目前	全補	應用本地	本地
綁定清除策略：	15000	15000	<input type="checkbox"/>	
收回規則類別：	org.jboss.cache.eviction.LRUPolicy	org.jboss.cache.eviction.LRUPolicy	<input type="checkbox"/>	
喚醒間隔秒數：	5	5	<input type="checkbox"/>	
最大容點數：	10000	10000	<input type="checkbox"/>	
存活時間秒數：	0	0	<input type="checkbox"/>	

保存

- 2 在頁面的「衝洗快取」區段，使用下拉式功能表來選取要衝洗的特定快取（或者選取「全部衝洗」）：

衝洗快取

從清單中選擇快取，然後按一下「衝洗快取」按鈕以衝洗快取。



請注意，可用快取的清單是動態的，它會根據當時快取的資料而變更。

- 3 按一下「衝洗快取」按鈕。

13.2.1 衝洗目錄抽象層快取

使用者應用程式的目錄抽象層也有快取。*DirectoryAbstractLayerDefinitions* 快取會將抽象層定義儲存在應用程式伺服器中，以最佳化所有資料模型操作的效能。

在一般情況下，使用者應用程式會自動將 *DirectoryAbstractLayerDefinitions* 快取與儲存在身份儲存庫中的抽象層定義同步化。但必要時，您可以手動衝洗 *DirectoryAbstractLayerDefinitions* 快取（如上所述），以強制從身份儲存區載入最新的定義。

如需使用者應用程式目錄抽象層的相關資訊，請參閱第 4 章「設定目錄抽象層的組態」，第 65 頁。

13.2.2 在叢集中衝洗快取

在叢集和非叢集應用程式伺服器環境中都支援快取衝洗。如果您的應用程式伺服器是叢集的一部份，並且您是手動衝洗快取，則該快取將會自動在叢集中的每個伺服器上衝洗。

13.3 設定快取設定的組態

您可以使用「快取」頁面來顯示和變更叢集或非叢集應用程式伺服器環境的快取組態設定。系統會立即儲存您的變更，但是它們要到下一次重新啟動使用者應用程式時才會生效。

提示：若要重新啟動使用者應用程式，您可以進行下列其中一個動作：將應用程式伺服器重新開機；重新部署應用程式（如果已透過某種方法變更 WAR）；或者強制讓應用程式重新啟動（如應用程式伺服器文件中所述）。

若要設定快取設定的組態，您需要瞭解：

- 「如何實作快取」，第 200 頁
- 「如何儲存快取設定」，第 200 頁
- 「如何顯示快取設定」，第 201 頁
- 「基本快取設定」，第 202 頁
- 「叢集的快取設定」，第 203 頁

13.3.1 如何實作快取

在 Identity Manager 使用者應用程式中，快取是透過 *JBoss* 快取來實作。「JBoss 快取」是開放原始碼快取結構，其包含在 JBoss Application Server 中，但也會在其他應用程式伺服器上執行。

若要瞭解「JBoss 快取」的相關資訊，請至 www.jboss.org/products/jboss-cache (<http://www.jboss.org/products/jboss-cache>)。

13.3.2 如何儲存快取設定

您可以使用兩個層級的設定來控制快取組態。您可以共同使用它們，以調整 Identity Manager 使用者應用程式的快取行爲。

層級	描述
全域設定	<p>全域設定是儲存在中心位置 (身份儲存區)，如此多個應用程式伺服器才能使用相同的設定值。例如，具有應用程式伺服器叢集的使用者通常會使用叢集組態值的全域設定。</p> <p>若要在您的身份儲存區中尋找全域設定，請查看位於 Identity Manager 使用者應用程式驅動程式下的下列物件：</p> <pre>configuration.AppDefs.AppConfig</pre> <p>例如：</p> <pre>configuration.AppDefs.AppConfig.MyUserApplicationDriver.MyDriverSet.MyOrg</pre> <p>組態物件的 XmlData 屬性包含全域設定資料。</p>

層級	描述
本地設定	<p>本地設定是分別儲存在每個應用程式伺服器上，如此個別伺服器才能置換一或多個全域設定的值。例如，您應該要指定本地設定，從全域設定所指定的叢集中移除應用程式伺服器，或者將伺服器重新指定至不同的叢集。</p> <p>若要在您的應用程式伺服器上尋找本地設定，請查看位於 JBoss 伺服器組態 conf 目錄下的下列檔案：</p> <pre>sys-configuration-xmldata.xml</pre> <p>例如：</p> <pre>jboss/server/IDM/conf/sys-configuration-xmldata.xml</pre> <p>如果您的伺服器具有本地設定，則該資料會包含在此檔案中 (如果尚未指定任何本地設定，則該檔案不存在)。</p>

對於每個使用使用者應用程式驅動程式特定例項的應用程式伺服器，您應該將全域設定視為預設值。當您變更全域設定時，會影響其中每個伺服器 (在下次重新啟動使用者應用程式時)，但其中個別伺服器指定本地置換的情況除外。

13.3.3 如何顯示快取設定

「快取」頁面顯示目前快取設定 (最近一次使用者應用程式重新啟動)。它還會顯示那些設定相對應的全域和本地值，並可讓您變更它們 (用於下次使用者應用程式重新啟動)。

叢集與快取組態

叢集組態
對於目前叢集組態的所有變更將在應用程式下次啟動時生效。群組 ID 必須是與 JBoss 所保留的叢集名稱 DefaultPartition 或 TreeCache 不符合的唯一名稱。只有具備經驗的管理員才可修改預設叢集內容。進行變更之前，請先參考 JBoss 文件。

	目前	全域	啟用本地	本地
叢集已開啟：	是	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
群組 ID：	c373e901aba5e8ee9966444553544200	<input type="text" value="c373e901aba5e8ee9966444553544200"/>	<input type="checkbox"/>	<input type="text"/>
叢集內容：	檢視	<input type="text" value="UDP(mcast_addr+228.8.8.8;mcast_po"/>	<input type="checkbox"/>	<input type="text"/>

快取組態
對於目前快取組態的所有變更將在應用程式下次啟動時生效。(* 表示需要)

	目前	全域	啟用本地	本地
鎖定擷取論時：*	15000	<input type="text" value="15000"/>	<input type="checkbox"/>	<input type="text"/>
收回規則類別：*	org.jboss.cache.eviction.LRUPolicy	<input type="text" value="org.jboss.cache.eviction.LRUPolicy"/>	<input type="checkbox"/>	<input type="text"/>
喚醒間隔秒數：*	5	<input type="text" value="5"/>	<input type="checkbox"/>	<input type="text"/>
最大節點數：*	10000	<input type="text" value="10000"/>	<input type="checkbox"/>	<input type="text"/>
存活時間秒數：*	0	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="text"/>

請注意，全域設定一直都具有值。本地設定是選擇性的。

13.3.4 基本快取設定

這些快取設定適用於叢集和非叢集應用程式伺服器。

若要設定基本快取設定的組態，請執行下列動作：

- 1 移至「快取」頁面。
- 2 在該頁面的「快取組態」區段中，視情況為下列設定指定全域或本地值：

設定	操作
鎖定擷取逾時	指定當在物件上取得鎖定時，快取要等待的 時間間隔 (以毫秒為單位) 。如果使用者應用程式在應用程式記錄中取得許多鎖定逾時例外，則您可能要增加此設定。預設值為 15000 毫秒。
收回規則類別	指定要使用之快取收回規則的 類別名稱 。預設值是「JBoss 快取」提供的「近來最少使用 (Least Recently Used, LRU)」收回規則： <code>org.jboss.cache.eviction.LRUPolicy</code> 如有需要，您可以將此規則變更為「JBoss 快取」支援的另一個收回規則。 若要瞭解受支援的收回規則，請至 www.jboss.org/products/jboss-cache (http://www.jboss.org/products/jboss-cache)。
喚醒間隔秒數	指定在喚醒快取收回規則以進行下列動作之前，該規則要等待的 時間間隔 (以秒為單位) ： <ul style="list-style-type: none">◆ 處理收回的節點事件◆ 清理大小限制和過期節點
最大節點數	指定快取中允許的 最大節點數 。如果沒有限制，請指定： 0
存活時間秒數	指定在清除節點之前 要閒置的時間 (以秒為單位) 。如果沒有限制，請指定： 0

這些設定是必要的，其表示對於每個設定都必須有一個全域值和一個選擇性的本地值。如果您要將設定的全域值置換為本地值，則選取該設定的「啟用本地」核取方塊。然後指定本地值 (請確定您的所有本地值都是有效的。否則，您將無法儲存變更)。

附註：對於那些沒有選取「啟用本地」的設定，任何現有的本地值會在您儲存時被刪除。

- 3 按一下「儲存」。

- 4 當您準備讓儲存的設定生效時，請在適合的應用程式伺服器上重新啓動使用者應用程式。

13.3.5 叢集的快取設定

本節討論當您在應用程式伺服器叢集間執行 Identity Manager 使用者應用程式時，如何設定快取的組態。您需要瞭解：

- ◆ 「如何實作叢集」，第 203 頁
- ◆ 「快取如何與叢集搭配使用」，第 203 頁
- ◆ 「準備使用叢集」，第 203 頁
- ◆ 「設定叢集的快取設定組態」，第 204 頁

如何實作叢集

在 Identity Manager 使用者應用程式中，快取的叢集支援會透過 *JGroups* 實作。*JGroups* 是開放原始碼叢集結構，其包含在 JBoss Application Server 中，但也會在其他應用程式伺服器上執行。

使用者應用程式的叢集包含網路上執行 *JGroups* 和使用公用群組 ID 的節點。在預設狀態下，提供給使用者應用程式叢集的「群組 ID」是通用唯一識別碼 (UUID)，如下所示：

```
c373e901aba5e8ee9966444553544200
```

通用唯一識別碼 (UUID) 可協助您確保獨特性，如此使用者應用程式叢集的「群組 ID」才不會與您環境中其他叢集的「群組 ID」發生衝突。例如，JBoss Application Server 本身使用兩個 *JGroups* 叢集，並為它們保留「群組 ID」*DefaultPartition* 和 *TreeCache*。

若要瞭解 *JGroups* 的相關資訊，請至 www.jboss.org/products/jgroups (<http://www.jboss.org/products/jgroups>)。

快取如何與叢集搭配使用

當您啓動使用者應用程式時，該應用程式的快取組態設定會決定是否要參與叢集，並將快取變更複製到叢集中的其他節點。如果已啓用叢集，則使用者應用程式會藉由在發生變更時將快取項目無效訊息傳送至每個節點，以完成此複製。

準備使用叢集

透過叢集使用快取需要下列兩個主要步驟：

- 1 設定您的 *JGroups* 叢集

這包括安裝 JBoss Application Server 以使用所有組態，然後通常會透過將 Identity Manager 使用者應用程式 (IDM.war) 置於 *farm* 目錄中，將其配送至叢集中的每個伺服器。

- 2 在使用者應用程式快取組態設定中開始使用該叢集

請參閱「設定叢集的快取設定組態」，第 204 頁 (如下)。

設定叢集的快取設定組態

在準備使用叢集時，您可以針對透過該叢集的快取支援指定設定。

若要設定叢集的快取設定組態，請執行下列動作：

- 1 移至「快取」頁面。
- 2 在該頁面的「叢集組態」區段中，視情況為下列設定指定全域或本地值：

設定	操作
叢集已開啓	選取「 True 」以複製快取變更到由「群組 ID」指定之叢集中的其他節點。如果您不想參與叢集，請選取「 False 」。
群組 ID	<p>指定您要參與之 JGroups 叢集的「群組 ID」。不需要變更預設之提供給使用者應用程式叢集的「群組 ID」，除非您想要使用不同的叢集。</p> <p>請注意，保留下列「群組 ID」以用於 JBoss Application Server：DefaultPartition 和 TreeCache。</p> <hr/> <p>提示：若要查看記錄訊息中的「群組 ID」，請確定快取記錄 (com.sssw.fw.cachemgr) 的層級是設為 Info 或更高。</p>
叢集內容	<p>指定由「群組 ID」所指定之叢集的 JGroups 通訊協定堆疊。請注意，此設定是針對具備經驗的管理員，這些管理員可能需要調整叢集內容。否則，您不應該變更預設通訊協定堆疊。</p> <p>若要查看目前的叢集內容，請按一下「檢視」。</p> <p>如需 JGroups 通訊協定堆疊的詳細資料，請至 www.jboss.org/wiki/Wiki.jsp?page=JGroups (http://www.jboss.org/wiki/Wiki.jsp?page=JGroups)。</p>

如果您要將設定的全域值置換為本地值，則選取該設定的「啓用本地」核取方塊。然後指定本地值。

附註：對於那些沒有選取「啓用本地」的設定而言，任何現有的本地值會在您儲存時被刪除。

請確定您叢集中的所有節點都指定相同的「群組 ID」和「叢集內容」（若要查看這些特定節點的設定，您必須藉由瀏覽至該伺服器上使用者介面的 URL，存取在該節點上執行的 Identity Manager 使用者介面，然後在該處顯示「快取」頁面）。

- 3 按一下「儲存」。
- 4 當您準備讓儲存的設定生效時，請在適合的應用程式伺服器上重新啓動使用者應用程式。

用於輸出和輸入入口網站資料的工具

本章說明如何使用 Identity Manager 使用者介面之「管理」索引標籤上的「工具」頁面。主題包含：

- ◆ 「關於輸出和輸入入口網站資料」，第 205 頁
- ◆ 「輸出入口網站資料」，第 206 頁
- ◆ 「輸入入口網站資料」，第 208 頁

如需存取和使用「管理」索引標籤的一般資訊，請參閱第 6 章「使用管理索引標籤」，第 115 頁。

14.1 關於輸出和輸入入口網站資料

您可以使用「工具」頁面輸出或輸入 Identity Manager 使用者應用程式中使用的入口網站內容（頁面和入口網站應用程式）。此內容又稱為入口網站組態狀態，它包含：

- ◆ 容器和共用頁面（包含每個頁面指定的入口網站應用程式，以及每個入口網站應用程式的優先設定和設定）
- ◆ 入口網站應用程式註冊

輸出和輸入工具可讓您視需要將入口網站組態狀態從一個入口網站（使用者應用程式）移至另一個入口網站。下面說明這些工具的運作方式：

工具	運作方式
入口網站資料輸出	產生一組選定容器和共用頁面以及入口網站應用程式的 XML 描述。XML 檔會儲存在「入口網站資料輸出」ZIP 檔案中，可做為「入口網站資料輸入」工具的輸入使用。
入口網站資料輸入	接受「入口網站資料輸出」ZIP 檔做為輸入。使用「入口網站資料輸出」ZIP 檔案在入口網站（使用者應用程式）中產生容器和共用頁面以及入口網站應用程式。

14.1.1 用途

您可以使用「入口網站資料輸出/輸入」工具來執行下列動作：

- ◆ 將您的入口網站組態狀態從測試（來源）環境移至生產（目標）環境
- ◆ 漸進式更新入口網站的組態狀態
- ◆ 複製入口網站
- ◆ 選擇性地覆寫目標入口網站上的組態狀態

14.1.2 要求

若要使用「入口網站資料輸出/輸入」工具，請確定 Identity Manager 使用者應用程式（入口網站）在您的來源和目標應用程式伺服器上部署並執行。

您的來源和目標伺服器不需要存取相同的身份儲存區，如必要，它們可以存取不同的儲存區。在那些身份儲存區中的使用者、群組和容器不需要相同。

14.1.3 限制

您無法使用「入口網站資料輸出/輸入」工具來執行下列動作：

- ◆ 當伺服器目前正在回應使用者申請時，輸出或輸入入口網站組態狀態
- ◆ 輸出或輸入入口網站類別和資源
- ◆ 輸出或輸入入口網站應用程式類別和資源
- ◆ 輸出或輸入入口網站中使用的身份和提供資料
- ◆ 輸出或輸入並非針對頁面和入口網站應用程式的管理設定
- ◆ 將組態狀態從之前的入口網站版本移轉至更新版本（入口網站必須是同一版本）

14.1.4 步驟

若要輸出和輸入入口網站資料，請執行下列動作：

- 1 如果您執行漸進式更新，請則備份目標入口網站。
- 2 從來源入口網站，藉由使用「入口網站資料輸出」工具輸出入口網站資料。
請參閱「[輸出入口網站資料](#)」，第 206 頁。
- 3 從目標入口網站，藉由使用「入口網站資料輸入」工具輸入入口網站資料。
請參閱「[輸入入口網站資料](#)」，第 208 頁。
- 4 測試目標入口網站，以確保已輸入想要的資料。

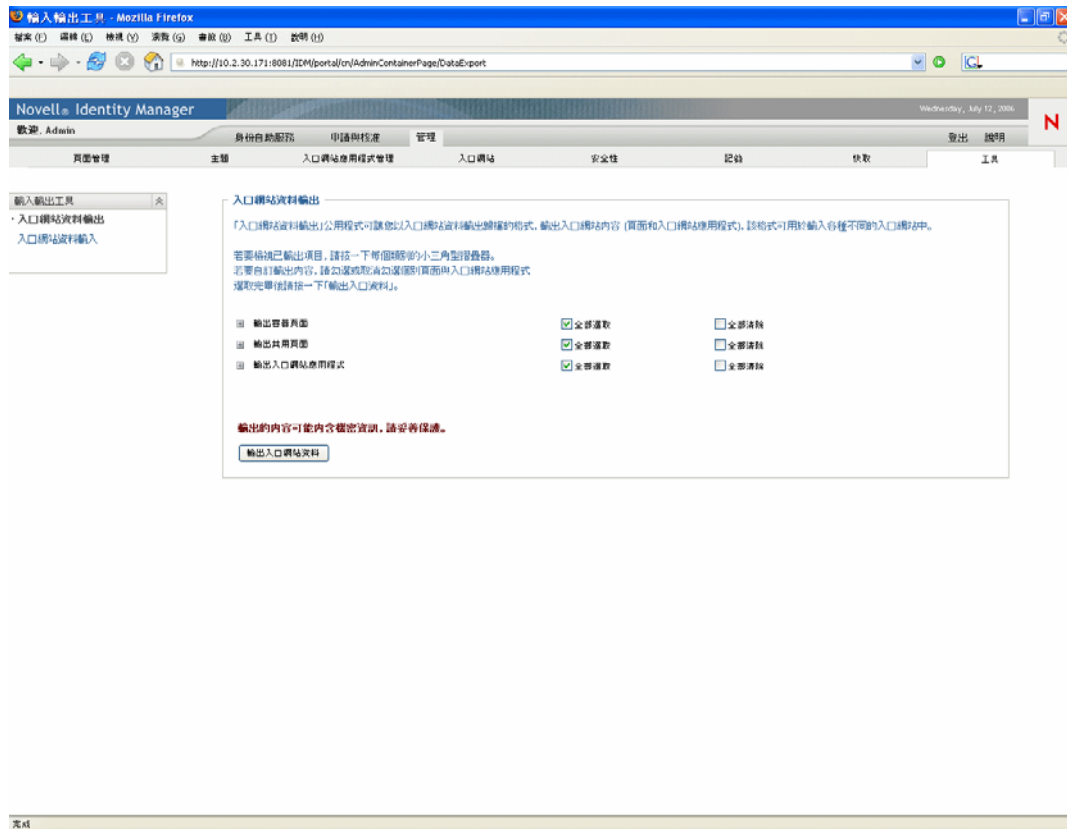
14.2 輸出入口網站資料

本節描述如何將入口網站的組態狀態輸出至「入口網站資料輸出」ZIP 檔。

若要輸出入口網站資料，請執行下列動作：

- 1 在「工具」頁面上，從左導覽功能表選取「入口網站資料輸出」。

「入口網站資料輸出」面板會顯示：



- 2 請遵循畫面指示，按照想要輸出的項目選取入口網站頁面和入口網站應用程式。

附註：部份沒有為輸出而選取的入口網站應用程式仍可能會予以輸出。如果您輸出含有入口網站應用程式的頁面，但是未將該入口網站應用程式選為輸出，則仍會輸出該入口網站應用程式（以確保輸出頁面不會發生執行時期錯誤）。

- 3 當您完成選取之後，按一下「輸出入口網站資料」按鈕。

即會產生新的「入口網站資料輸出」ZIP 檔，其預設名稱包含目前日期和時間。例如：

PortalData.21-Oct-05.09.12.16.zip

然後會提示您在本地儲存此 ZIP 檔案 (或在適當的歸檔公用程式中開啓它)。例如：



4 將「入口網站資料輸出」ZIP 檔儲存至適當的位置。

14.3 輸入入口網站資料

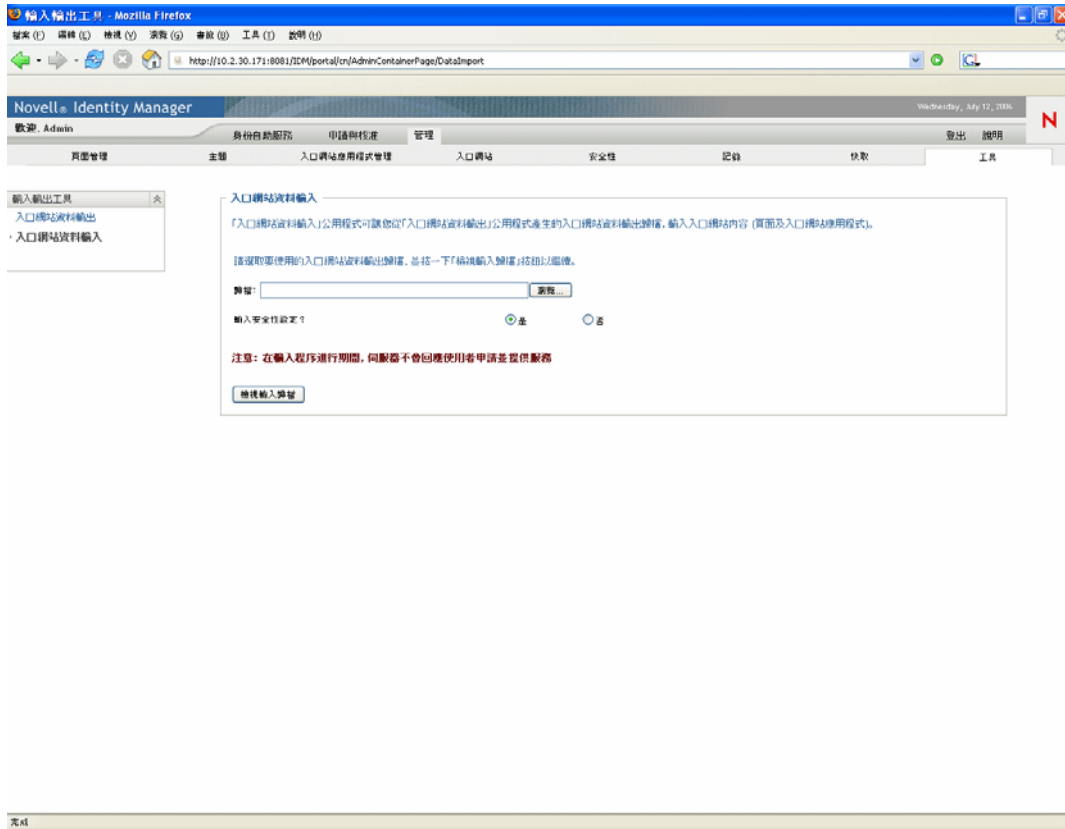
本節描述如何將「入口網站資料輸出」ZIP 檔輸入至入口網站。

附註：請記住，在輸入期間，您的目標應用程式伺服器必須處於執行中，但目前不是在回應使用者申請。

若要輸入入口網站資料，請執行下列動作：

- 1 在「工具」頁面上，從左導覽功能表選取「入口網站資料輸入」。

「入口網站資料輸入」面板即會顯示：

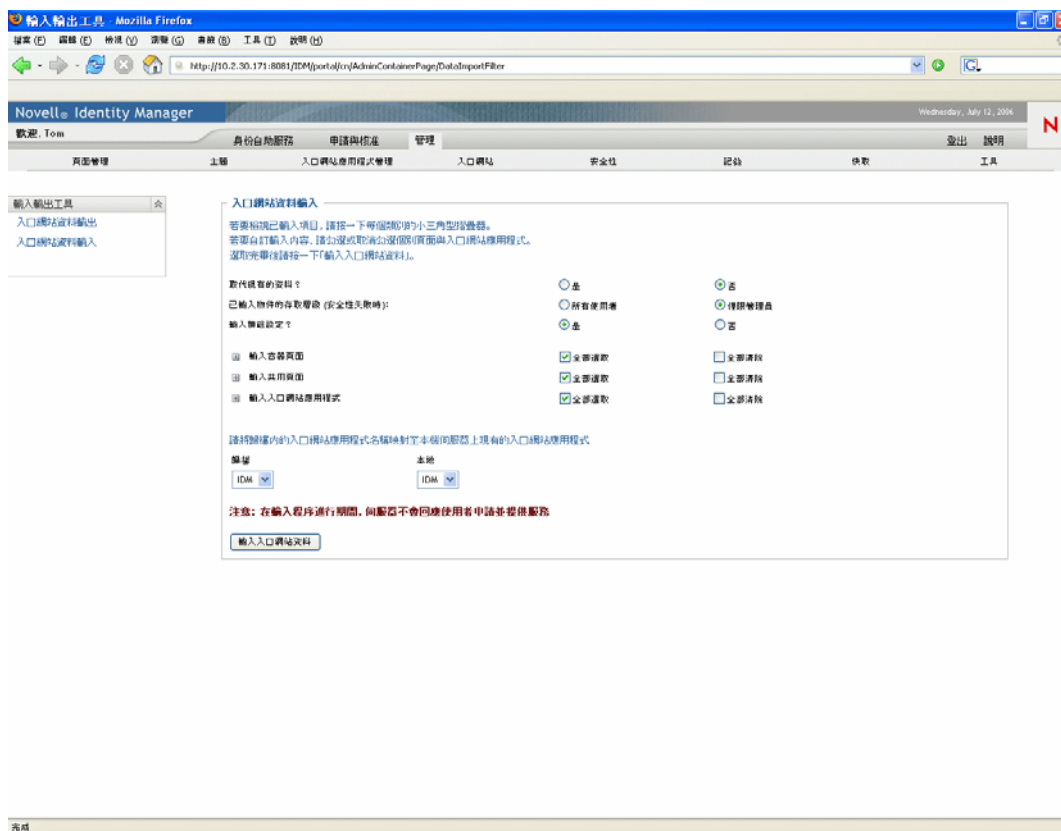


2 指定下列一般輸入設定：

設定	操作
歸檔	<p>按一下「瀏覽」按鈕以選取要輸入的「入口網站資料輸出」ZIP 檔。例如：</p> <p style="text-align: center;">PortalData.21-Oct-05.09.12.16.zip</p>
輸入安全性設定？	<p>選取下列其中一項：</p> <ul style="list-style-type: none"> ◆ 是：如果您想要輸入許可，而該許可是由「入口網站資料輸出」ZIP 檔指定給使用者、群組和容器用於存取頁面和入口網站應用程式。請確定涉及到的使用者、群組和容器都存在於目標入口網站身份儲存區中，遺失實體的許可便無法輸入。 ◆ 否：如果您想要忽略「入口網站資料輸出」ZIP 檔指定的許可。

3 按一下「檢視輸入歸檔」按鈕。

面板會顯示選定的「入口網站資料輸出」ZIP 檔及其輸入方式的詳細資料：



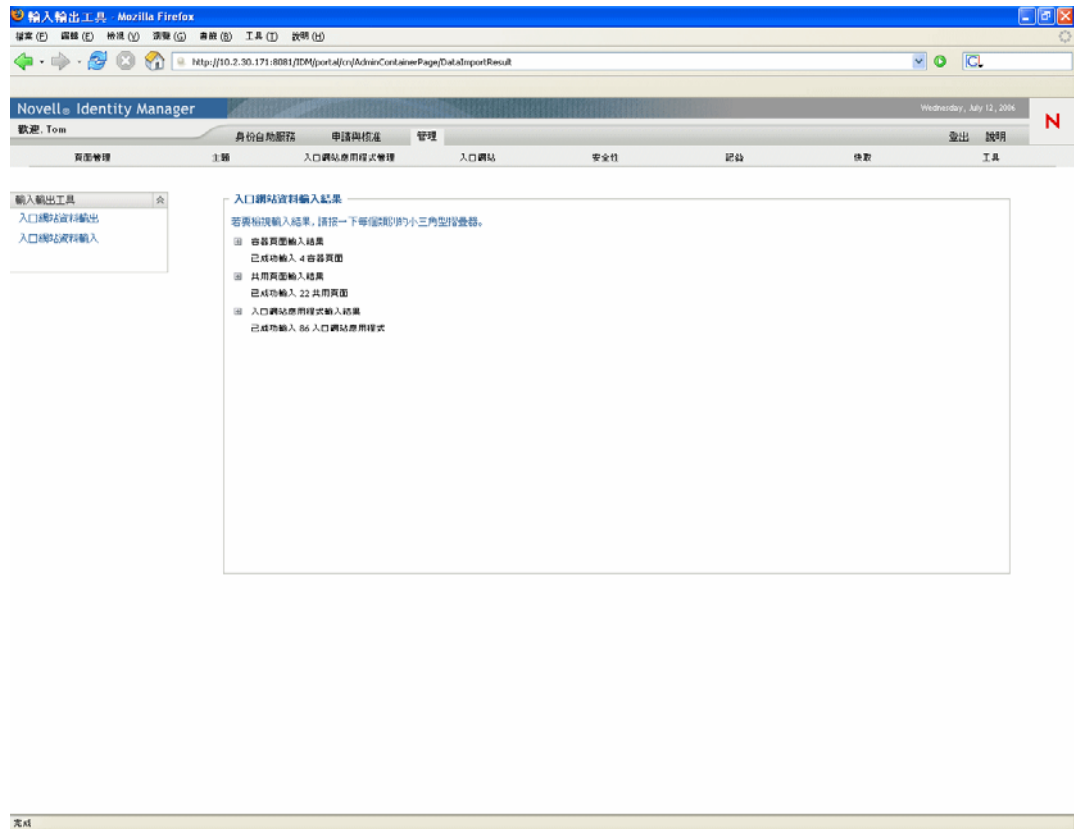
4 指定下列詳細輸入設定：

設定	操作
取代現有的資料？	<p>選取下列其中一項：</p> <ul style="list-style-type: none"> ◆ 是：如果您想要以「入口網站資料輸出」ZIP 檔的內容，覆寫已存在於目標入口網站中相對應的頁面和入口網站應用程式。例如，如果「入口網站資料輸出」ZIP 檔包含名為 MyPage 的共用頁面，目標入口網站也包含名為 MyPage 的共用頁面，則會在目標入口網站中覆寫現有的頁面。 ◆ 否：如果您想要跳過所有現有頁面和入口網站應用程式的輸入。

設定	操作
已輸入物件的存取層級	<p>選取下列其中一項：</p> <ul style="list-style-type: none"> ◆ 所有使用者：適用於無限制存取輸入頁面和入口網站應用程式。 ◆ 僅限管理員：適用於受限的存取，輸入頁面和入口網站應用程式。 <p>如果您選擇輸入安全性設定，則此存取層級僅適用於那些無法輸入安全性設定的輸入頁面和入口網站應用程式（通常是因為目標入口網站身份儲存區中不存在指定的使用者、群組或容器）。</p> <p>如果您選擇不輸入安全性設定，則此存取層級會套用至所有輸入的頁面和入口網站應用程式。</p>
輸入群組設定？	<p>(如果您選擇輸入安全性設定) 選取下列其中一項：</p> <ul style="list-style-type: none"> ◆ 是：如果您想要輸入由「入口網站資料輸出」ZIP 檔指定給群組的預設容器頁面和預設共用頁面指定。請確定涉及到群組存在於目標入口網站身份儲存區中，遺失群組的指定便無法輸入。 ◆ 否：如果您想要忽略由「入口網站資料輸出」ZIP 檔指定給群組的預設頁面指定。
輸入容器頁面	<p>請遵循畫面指示，按照想要從「入口網站資料輸出」ZIP 檔輸入到目標入口網站的項目，選取頁面和入口網站應用程式。</p>
輸入共用頁面	
輸入入口網站應用程式	<p>附註：部份沒有為輸出而選取的入口網站應用程式仍可能會予以輸出。如果您輸入包含入口網站應用程式的頁面，但是未將該入口網站應用程式選為輸入，則仍會輸入該入口網站應用程式（以確保輸入頁面不會發生執行時期錯誤）。</p>
請映射入口網站應用程式名稱 ... 歸檔 / 本地	<p>使用「歸檔」和「本地」下拉式功能表，將歸檔中的入口網站應用程式名稱（「入口網站資料輸出」ZIP 檔案）映射至本地（目標）應用程式伺服器上現有的入口網站應用程式。</p>

5 當您準備好開始輸入時，按一下「輸入入口網站資料」按鈕。

當輸入完成時，「入口網站資料輸入結果」面板即會顯示：



失敗的輸入會以紅色顯示。若要疑難排解輸入（或輸出）問題，請查看您的應用程式伺服器系統主控台或記錄檔案（例如 `jboss/server/IDM/log/server.log`），以取得下列使用者應用程式記錄的訊息：

```
com.novell.afw.portal.util
```

入口網站應用程式參考資訊

IV

下列章節說明如何設定 Identity Manager 使用者介面中使用的身份和系統入口網站應用程式的組態。

- ◆ 第 15 章 「關於入口網站應用程式」, 第 215 頁
- ◆ 第 16 章 「建立入口網站應用程式參考資訊」, 第 219 頁
- ◆ 第 17 章 「詳細資料入口網站應用程式參考資訊」, 第 225 頁
- ◆ 第 18 章 「組織圖入口網站應用程式參考資訊」, 第 239 頁
- ◆ 第 19 章 「密碼管理入口網站應用程式參考資訊」, 第 253 頁
- ◆ 第 20 章 「搜尋清單入口網站應用程式參考資訊」, 第 265 頁

關於入口網站應用程式

本章提供 Identity Manager 使用者應用程式中使用之入口網站應用程式的相關資訊。主題包含：

- 「附屬入口網站應用程式」，第 215 頁
- 「管理入口網站應用程式」，第 215 頁
- 「身份入口網站應用程式」，第 216 頁
- 「密碼入口網站應用程式」，第 216 頁
- 「系統入口網站應用程式」，第 217 頁

如需管理入口網站應用程式的相關資訊，請參閱第 9 章「入口網站應用程式管理」，第 161 頁。

15.1 附屬入口網站應用程式

附屬入口網站應用程式提供一組不同的功能，您可將其新增至 Identity Manager 使用者應用程式。附屬入口網站應用程式提供電子郵件、檔案系統和其他功能。如需相關資訊：

入口網站應用程式類別	相關資訊
電子郵件	請參閱《Identity Manager 附屬入口網站應用程式管理指南》
檔案系統	
其他	

15.2 管理入口網站應用程式

「管理」類別中的入口網站應用程式用於控制使用者介面的配置和內容。

附註：建議您不使用或修改這些入口網站應用程式。它們會為使用者應用程式提供架構服務。

「管理」入口網站應用程式包含：

入口網站應用程式名稱	描述
標題入口網站應用程式	顯示使用者介面的頂層索引標籤控制項和標題資訊。 此入口網站應用程式沒有優先設定。
共用頁面導覽	顯示包含 Identity Manager 使用者應用程式共用頁面的功能表。 優先設定會定義顯示內容和顯示方式。 請參閱「共用頁面導覽入口網站應用程式」，第 216 頁。

15.2.1 共用頁面導覽入口網站應用程式

「共用頁面導覽」入口網站應用程式會產生 Identity Manager 使用者應用程式共用頁面的連結。優先設定會定義顯示的共用頁面連結。優先設定包含：

優先設定	指定內容
sharedpages-sorting	共用頁面在類別內顯示的順序：遞增 / 遞減。
sharedpages-sortmode	如何排序共用頁面：「字母順序」還是「優先程度」。
sharedpages-category	指定一或多個共用頁面類別。 類別名稱顯示為標題，在該類別內的所有共用頁面都顯示為連結。如果類別不包含任何共用頁面，則不會顯示該類別。如果共用頁面不在類別中，則其顯示為未分類。
guest-category	指定要在入口網站著陸頁面顯示其入口網站應用程式的類別。它必須是預先存在的類別，並且此類別中包含的頁面不能具有任何 ACL 讀取條件約束。

15.3 身份入口網站應用程式

「身份」入口網站應用程式用於 Identity Manager 使用者應用程式的「身份自助服務」索引標籤。它們包含：

入口網站應用程式名稱	描述
建立	提供可讓使用者在身份儲存區中建立物件的精靈介面。 請參閱第 16 章「建立入口網站應用程式參考資訊」，第 219 頁。
詳細資料	可讓使用者顯示和處理實體的屬性資料。 請參閱第 17 章「詳細資料入口網站應用程式參考資訊」，第 225 頁。
組織圖	可讓使用者檢視和瀏覽身份儲存區中物件之間的階層式關係。 請參閱第 18 章「組織圖入口網站應用程式參考資訊」，第 239 頁。
搜尋清單	允許使用者搜尋身份儲存區中的物件。 請參閱第 20 章「搜尋清單入口網站應用程式參考資訊」，第 265 頁。

15.4 密碼入口網站應用程式

密碼入口網站應用程式針對 Identity Manager 使用者應用程式提供密碼自助服務功能。它們包含：

入口網站應用程式名稱	相關資訊
IDM 處理安全回應	請參閱第 19 章 「密碼管理入口網站應用程式參考資訊」，第 253 頁
IDM 變更密碼	
IDM 忘記密碼	
IDM 提示定義	
IDM 登入	

15.5 系統入口網站應用程式

系統入口網站應用程式會針對 Identity Manager 使用者應用程式提供服務。

附註：建議您不使用或修改此類別的入口網站應用程式。

系統入口網站應用程式包含：

入口網站應用程式名稱	描述
入口網站頁面控制器	顯示使用者目前已透過「共用頁面導覽」入口網站應用程式選取的共用頁面。 此入口網站應用程式沒有優先設定。

建立入口網站應用程式參考資訊

本章說明如何在 Identity Manager 使用者應用程式中使用「建立」入口網站應用程式。主題包含：

- ◆ 「關於建立入口網站應用程式」，第 219 頁
- ◆ 「設定建立入口網站應用程式的組態」，第 220 頁
- ◆ 「設定建立優先設定」，第 222 頁

16.1 關於建立入口網站應用程式

「建立」入口網站應用程式提供容易使用的精靈，可讓使用者建立不同類型的身份儲存區物件。入口網站應用程式優先設定會控制：

- ◆ 使用者可以建立的物件類型。
- ◆ 使用者可以提供的屬性。

如需相關資訊，請參閱「設定建立優先設定」，第 222 頁。

「建立」入口網站應用程式的預設組態（透過 Identity Manager 使用者應用程式的「建立使用者或群組」動作存取）可讓使用者建立「使用者」、「群組」或「任務群組」。在預設狀態下，此入口網站應用程式限制為「使用者應用程式管理員」。下列範例顯示預設的「建立」入口網站應用程式精靈如何提示使用者進行下列操作：

- ◆ 選取要建立的物件類型：



- ◆ 填入物件的屬性：

The screenshot shows the 'Novell Identity Manager' interface. The main window is titled '建立' (Build) and contains the following sections:

- 基本參數 (Basic Parameters):**
 - 物件 ID:* (Object ID): [Text input field]
 - 容器:* (Container): [Text input field with dropdown arrow]
- 物件屬性 (Object Properties):**
 - 隱蔽 (Hidden):
 - 名:* (Name): [Text input field]
 - 姓:* (Surname): [Text input field]
 - 職稱 (Title): [Text input field with dropdown arrow and icons]
 - 部門 (Department): [Text input field with dropdown arrow and icons]
 - 區域 (Region): [Text input field with dropdown arrow and icons]

- ◆ 提示輸入密碼 (物件類型需要時)：

The screenshot shows the 'Novell Identity Manager' interface. The main window is titled '建立' (Build) and contains the following sections:

- 建立密碼 (Create Password):**
 - 密碼 (Password): [Text input field]
 - 確認密碼 (Confirm Password): [Text input field]
- Navigation: [Return arrow] 返回 (Return) and 繼續 (Continue) [Continue arrow]

如果已指定密碼規則，則此入口網站應用程式會顯示所有的自定規則訊息。

- ◆ 在成功建立物件之後提供資訊訊息，以連結至該物件的「詳細資料」入口網站應用程式 (假設以同樣的方式設定「詳細資料」入口網站應用程式的組態)，進一步編輯。

16.2 設定建立入口網站應用程式的組態

若要設定「建立」入口網站應用程式的組態，您需要進行下列操作：

步驟	任務	描述
1	判定預設的「建立使用者或群組」功能是否符合您的需求	如果符合，則您無需再執行任何動作。 如果不符合，則您需要完成其餘的步驟。

步驟	任務	描述
2	定義您允許使用者建立的物件類型	將物件和屬性新增至目錄抽象層。 如需相關資訊，請參閱第 4 章「設定目錄抽象層的組態」，第 65 頁。
3	決定您要讓使用者存取此新入口網站應用程式的方式	您要讓使用者從現有頁面還是新的頁面啟動此入口網站應用程式？哪些使用者可以存取入口網站應用程式和頁面？ 如需頁面的相關資訊，請參閱第 7 章「頁面管理」，第 121 頁。
4	指定可以存取頁面和入口網站應用程式例項的使用者	編輯頁面安全性並將使用者新增至清單。如需限制使用者存取頁面的相關資訊，請參閱第 7 章「頁面管理」，第 121 頁。 編輯入口網站應用程式例項，以變更安全性。如需限制使用者存取入口網站應用程式的相關資訊，請參閱第 9 章「入口網站應用程式管理」，第 161 頁。
5	設定入口網站應用程式的優先設定	優先設定可讓您定義： <ul style="list-style-type: none"> ◆ 使用者可以建立的物件。 ◆ 建立期間要提供的屬性。 如需相關資訊，請參閱「設定建立優先設定」，第 222 頁。
6	測試	驗證是否已建立物件並已正確填入屬性。
7	在 eDirectory 中針對一般使用者建立正確有效的權限	若要建立物件，使用者需要是建立物件之組織和組織單位的託管者。

16.2.1 目錄抽象層設定

「建立」入口網站應用程式之使用者可以填入的屬性和可以建立的物件必須在目錄抽象層中定義，如下所示：

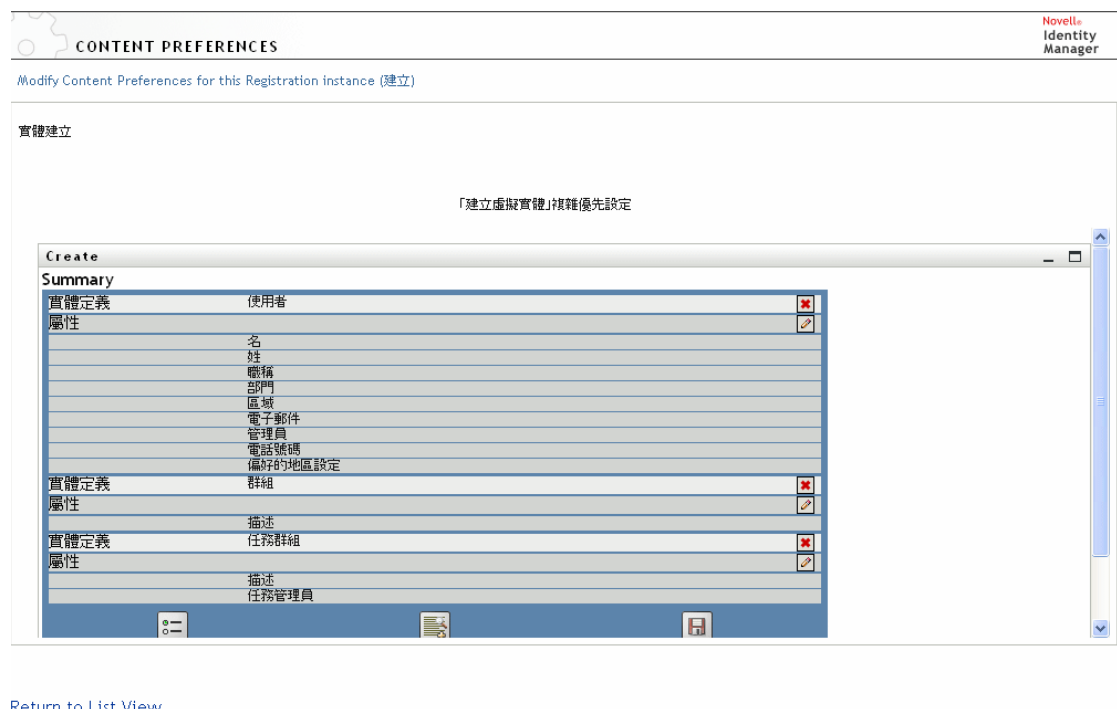
定義類型	內容	值
entity	create	選取
	view	選取 如果未選取，則實體不會顯示在可以建立的實體清單中。
	Container for Create	指定有效的身份儲存區容器。 如果未提供有效的容器，則會使用在使用者應用程式安裝期間指定的根容器。
	Password	如果實體類型在建立時需要密碼，則選取。 具有「建立」存取權和 OU「託管者」權限的任何人員都可以建立使用者並指定 啓始密碼 。新的使用者首次登入時，會重新導向至要修改啓始密碼的「IDM 變更密碼」入口網站應用程式。 如需「IDM 變更密碼」入口網站應用程式的相關資訊，請參閱第 19 章「密碼管理入口網站應用程式參考資訊」，第 253 頁。
attribute	enabled	選取
	viewable	如果將 enabled 或 viewable 設為不選取 (false)，則入口網站應用程式無法使用該屬性。

如需設定抽象層的相關資訊，請參閱第 4 章「設定目錄抽象層的組態」，第 65 頁。

16.3 設定建立優先設定


藉由設定優先設定，您可以設定使用者能建立的物件類型之組態，和設定允許提供或需要提供的屬性之組態。

「建立」入口網站應用程式的優先設定包含在單一自定優先設定頁面中。開啓它時，即會顯示個別的「建立」優先設定：



優先設定如下所示 (或者您可以按一下「描述」按鈕，以顯示此入口網站應用程式的線上說明)。

優先設定	描述
實體定義	<p>要建立之物件類型的名稱。</p> <p>它代表實體定義區塊的開始處，您可在此定義入口網站應用程式處理建立操作的方式。</p> <p>限制物件：</p> <p>在複雜優先設定中列出的物件會在下拉式功能表中顯示給使用者。若要限制使用者可以建立的物件，請透過刪除按鈕從此優先設定表中移除它們。</p> <p>新增其他實體：</p> <p>按一下「新增實體定義」，完成精靈。</p>

優先設定	描述
屬性	<p data-bbox="610 260 1401 344">控制提示使用者填入的屬性。您必須併入所有物件的必要屬性，否則實際的物件建立會失敗。此外，如果您遺失必要的屬性，則不會適當地儲存優先設定。</p> <p data-bbox="610 369 773 394">新增或移除屬性：</p> <ul data-bbox="638 420 951 445" style="list-style-type: none">◆ 按一下「修改屬性」按鈕。 <div data-bbox="667 478 704 516" style="text-align: center;"></div> <ul data-bbox="638 562 1401 726" style="list-style-type: none">◆ 若要新增屬性，請從「可用」屬性清單中選取它。您可以使用 CTRL 或 Shift 鍵選取多個屬性。◆ 按一下箭頭，以將其移至「選定」清單中。進行反向操作以移除屬性。◆ 若要將清單中的屬性重新排列，請按一下「選定」清單右側的向上或向下箭頭。按一下「提交」。 <p data-bbox="610 751 773 777">屬性和資料類型：</p> <p data-bbox="610 802 1385 856">屬性的資料類型會影響其顯示方式。例如，如果將屬性定義為「本地」或「全域」清單次類型，則它會顯示在清單方塊中。</p> <p data-bbox="610 882 1195 907">如需相關資訊，請參閱「使用實體和屬性」，第 76 頁。</p>

完成優先設定面板 若要驗證是否已提交有效的項目，請按一下「提交」。如果有無效的項目，您就會看到錯誤訊息顯示在優先設定頁面的頂端。若在按一下「提交」之後沒有發生錯誤，請按一下「返回清單檢視」。返回「清單檢視」之後，您必須按一下「儲存優先設定」。

本章說明可讓使用者顯示和處理實體屬性資料的「詳細資料」入口網站應用程式。它是 Identity Manager 使用者應用程式「身份自助服務」索引標籤中「我的設定檔」動作的基礎。主題包含：

- ◆ 「關於詳細資料入口網站應用程式」，第 225 頁
- ◆ 「先決條件」，第 233 頁
- ◆ 「設定優先設定」，第 236 頁

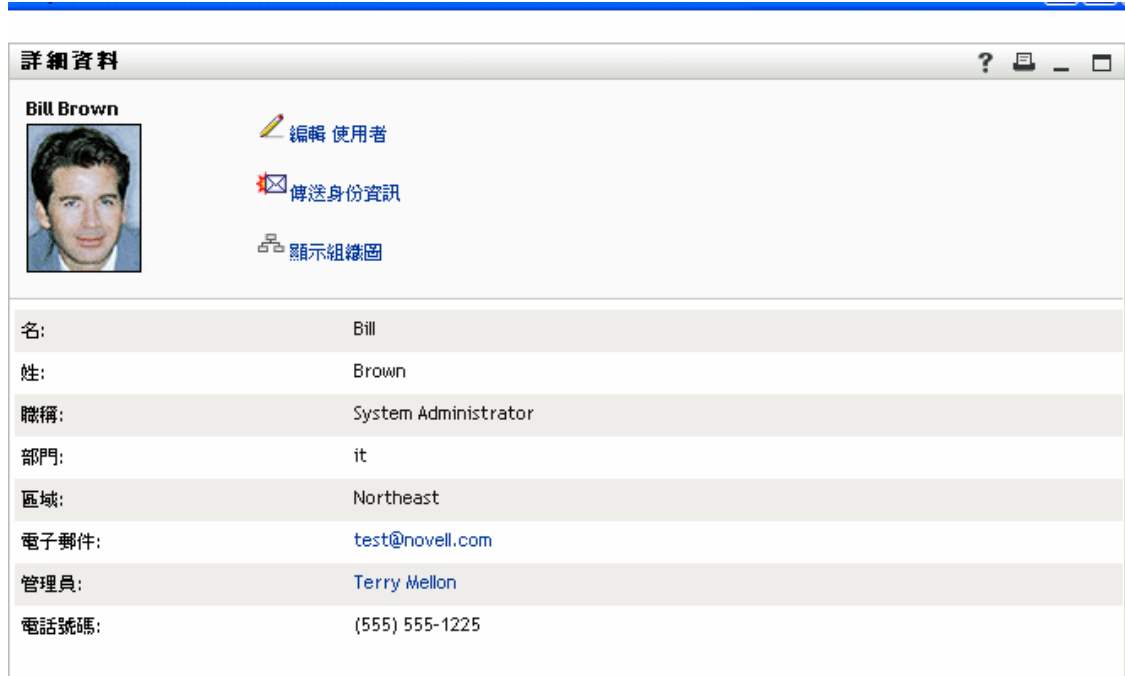
17.1 關於詳細資料入口網站應用程式

「詳細資料」入口網站應用程式會為使用者提供實體屬性及其值的詳細檢視窗。入口網站應用程式具有兩種模式：顯示和編輯。存取「詳細資料」入口網站應用程式時，使用者可以利用其內建功能來處理此資訊，包含：

- ◆ 「顯示實體資料」，第 226 頁
- ◆ 「編輯實體資料」，第 229 頁
- ◆ 「以電子郵件傳送實體資料」，第 231 頁 (僅限顯示模式)
- ◆ 「連結至組織圖」，第 232 頁
- ◆ 「連結至其他實體的詳細資料」，第 232 頁 (僅限顯示模式)
- ◆ 「列印實體資料」，第 233 頁 (僅限顯示模式)

17.1.1 顯示實體資料

存取它時，「詳細資料」入口網站應用程式會顯示選定實體的屬性資料，例如使用者或群組。例如，下面是使用者 Bill Brown 檢視自己的資訊時，「詳細資料」入口網站應用程式可能會顯示的內容：



使用者影像 在預設狀態下，「詳細資料」入口網站應用程式的組態會設定為包含「使用者照片」屬性。然而，如果您的身份儲存區不包含或未填入此屬性，則在執行時期會顯示預設的影像。如果您將使用者影像儲存在不同的位置，則可以將入口網站應用程式的組態設定為顯示這些影像。

如需相關資訊，請參閱「動態載入影像」，第 229 頁。

決定要顯示的屬性

「詳細資料」入口網站應用程式僅顯示符合下列條件的屬性：

- ◆ 目錄抽象層資料定義可以檢視的屬性
如需 VDD 組態的相關資訊，請參閱第 4 章「設定目錄抽象層的組態」，第 65 頁。
- ◆ 在「詳細資料」優先設定中指定的屬性
若要瞭解指定「詳細資料」入口網站應用程式中顯示的屬性，請參閱「設定優先設定」，第 236 頁。
- ◆ 目前使用者具有檢視權限的屬性
例如，具有薪水屬性檢視權限的管理員可以查看薪水資料，但是其他使用者無法查看。
如需相關資訊，請參閱「指定實體的權限」，第 234 頁。
- ◆ 目前已填入值的屬性

決定屬性的顯示方式

顯示屬性時，「詳細資料」會將資料格式化為文字，但是在下列情況中例外：

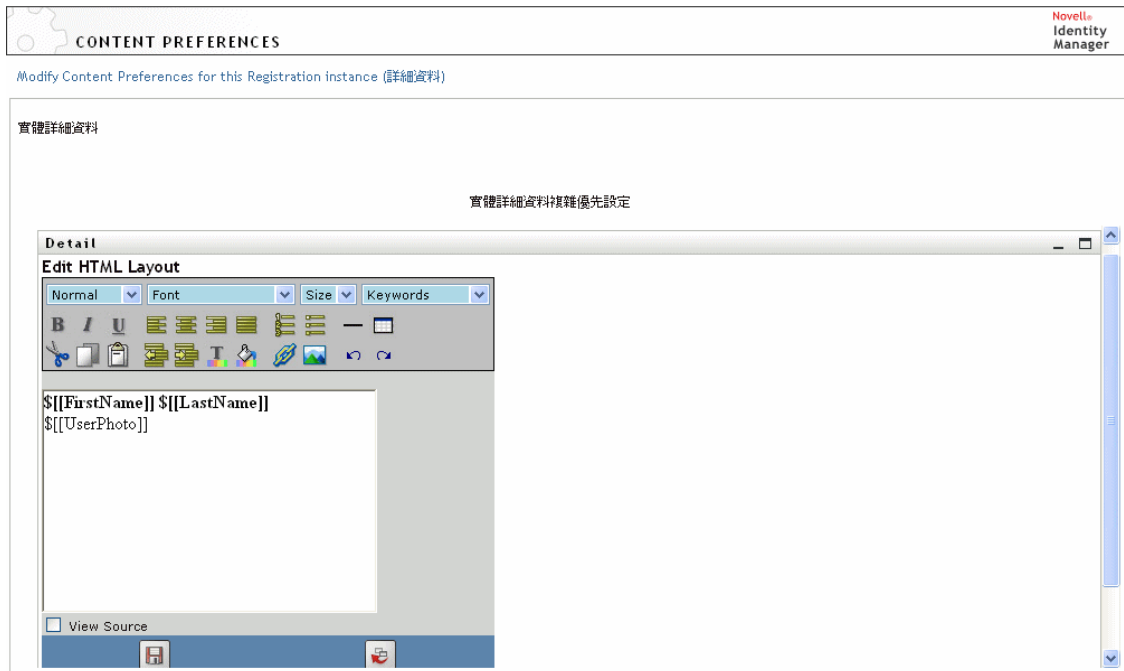
抽象層定義中的格式規格	顯示方式
格式：電子郵件	顯示為 <code>mailto</code> 連結
格式： <ul style="list-style-type: none">◆ groupwise-im◆ aol-im◆ yahoo-im	顯示為啓始聊天並新增該使用者的圖示
資料類型：二進位	顯示為檢視影像的按鈕和連結
格式：影像	
資料類型：布林值	顯示為指出 <code>true</code> 或 <code>false</code> 的已停用選項圓鈕 按鈕會顯示，但不會指出預設值，這是由於在指定值之前沒有為使用者實際建立屬性。
多值：選取	顯示為用於編輯、新增和移除個別屬性值的一組重複控制項 (以逗號分隔的清單格式)
控制項類型：DNLookup	顯示為連結 在上述範例中，會顯示可存取 Bill Brown 管理員「詳細資料」的連結 (Terry Mellon)。
控制項類型： <ul style="list-style-type: none">◆ 本地清單◆ 全域清單	顯示為顯示標籤而不是實際的 (鍵) 值 例如， <code>EmployeeType</code> 屬性會顯示全職而不是實際的值 <code>ft</code> 。

決定標題區域顯示的內容

您可以使用標準的 HTML 功能，配置「詳細資料」入口網站應用程式的標題區域：



「詳細資料」優先設定會提供 *HTML* 配置編輯器，您可以使用它來建立想要的外觀和內容：



[Return to List View](#)

使用 HTML 配置編輯器

「HTML 配置編輯器」會提供定義文字格式和清單，以及指定錨點和影像等 HTML 編輯器的一般功能。

關鍵字 設計配置時，您可以使用「關鍵字」下拉式功能表，將變數插入至「詳細資料」入口網站應用程式的標題區域內，這些變數會在執行時期由特定的屬性值取代。您還可以使用下列語法進行輸入：

```
$[[keyword]]
```

其中，*keyword* 是屬性 (例如 LastName) 的值。

您可以使用此語法來串連屬性：

```
$[[keyword+keyword]]
```

例如：

```
$[[FirstName+LastName]]
```

您可以視需要串連多個屬性，也可以併入用引號括住的字串，如下所示：

```
$[[keyword+"sample text"+keyword]]
```

這樣會轉換用引號括住的文字和關鍵字值。

附註：如果配置中的關鍵字輸入錯誤，則會在執行時期按原樣轉換 (包含 `${[]}`)。

動態載入影像 若要顯示影像，例如顯示身份儲存區中儲存的使用者照片，您可以使用「HTML 配置編輯器」新增屬性名稱。例如，新增「使用者照片」屬性會顯示使用者的照片。如果您將影像儲存在身份儲存區外部，則需要使用 `IMG:` 標籤 (在「HTML 編輯器」的「檢視來源」模式中)，如下所示：

- 1 移至入口網站應用程式的優先設定，並存取「HTML 編輯器」。
- 2 按一下「檢視來源」。
- 3 使用 `IMG:` 標籤利用下列語法結合位置、屬性鍵和副檔名，如下所示：

```
${[IMG:"URL" + attribute-key-name + "fileextension"]}
```

如果您將員工照片做為 `JPG` 影像按照「姓」儲存在應用程式伺服器的 `/images` 子目錄中，則下列範例會顯示您所使用的語法：

```
${[IMG:"http://myhost:8080/images/"+LastName+".jpg"]}
```

在執行時期，入口網站應用程式會串連 `URL` 與 `LastName` 屬性和副檔名 `.jpg`。

請注意，「HTML 編輯器」支援靈活的語法。它支援文字和屬性的任何組合，因此語法可以是：

```
${[IMG:"some text" + attribute-key-name + ...]}
```

17.1.2 編輯實體資料

「詳細資料」入口網站應用程式會自動提供「編輯」連結 (例如「編輯您的資訊」或「編輯使用者」或「編輯設備」)，以從顯示模式切換至編輯模式。這可讓具有目前實體適當權限的使用者變更其屬性值並儲存這些變更。

例如，下面是使用者 Bill Brown (具有必要的權限) 編輯自己的資訊時，「詳細資料」可能會顯示的內容：

隱藏	屬性	值
<input type="checkbox"/>	名:*	Bill
<input type="checkbox"/>	姓:*	Brown
<input type="checkbox"/>	職稱:	System Administrator
<input type="checkbox"/>	部門:	it
<input type="checkbox"/>	區域:	Northeast
<input type="checkbox"/>	電子郵件:	test@novell.com
<input type="checkbox"/>	管理員:	Terry Mellon
<input type="checkbox"/>	群組:	
<input type="checkbox"/>	電話號碼:	[555] 555-1225
<input type="checkbox"/>	偏好的地區設定:	(未選取)
<input type="checkbox"/>	使用者照片:	新增影像
<input type="checkbox"/>	行政管理員:	<input type="radio"/> true <input type="radio"/> false
<input type="checkbox"/>	任務群組管理員:	<input type="radio"/> true <input type="radio"/> false
<input type="checkbox"/>	受管理的任務群組:	

附註：若為布林值屬性，同時不選這兩個選項圓鈕表示使用者的屬性不存在。核取 *true* 或 *false* 選項圓鈕都會針對使用者建立屬性並設定其值。

決定會顯示的屬性

在編輯模式中，「詳細資料」入口網站應用程式僅顯示符合下列條件的那些屬性：

- ◆ 目錄抽象層資料定義使屬性可以檢視
如需資料定義的相關資訊，請參閱第 4 章 「設定目錄抽象層的組態」，第 65 頁。
- ◆ 目前使用者具有檢視屬性的權限
例如，具有薪水屬性檢視權限的經理可以查看資料，但是其他使用者無法查看。
如需相關資訊，請參閱 「指定實體的權限」，第 234 頁。

屬性必須滿足上述全部的條件，才能以編輯模式顯示。

決定屬性的顯示方式

在編輯模式中，「詳細資料」會將每個可編輯的屬性格式化為文字方塊，但是在下列情況中例外：

屬性類型規格 (在 VDD 檔案中)	顯示方式
資料類型：二進位 格式：影像	顯示為「實體影像上載」入口網站應用程式的按鈕和連結，以檢視、更新或新增影像
資料類型：布林值 hide：選取	顯示為指出 true 或 false 的選項圓鈕 顯示為標示成「隱藏」的核取方塊
multivalued= 選取	顯示為編輯、新增和移除屬性值的一組控制項
控制項類型：DNLookup	顯示為啟動「參數清單」入口網站應用程式以搜尋和選取 DN 的按鈕
控制項類型： <ul style="list-style-type: none">◆ 本地清單◆ 全域清單	顯示為下拉式清單 (適合的話，允許多重選取)

無法編輯 (依定義或由於使用者權限不足) 的屬性會顯示為已停用或唯讀。

驗證變更

在編輯期間，系統會針對下列屬性類型規格自動執行資料驗證：

- ◆ 格式：電子郵件
- ◆ 資料類型：整數
- ◆ 控制項類型：範圍

使用本地或全域清單的控制項類型時，顯示的清單可能包含屬性指定邊界之外的值。但是此類值會設旗標為超出範圍，且驗證會阻止提交這些值。

定義預設我的設定檔實體

在目錄抽象層定義實體時，您可以指定「預設我的設定檔實體」(在目錄抽象層編輯器的「組態」元素中) 的值，以指定要使用其他實體定義進行編輯。從顯示模式切換至編輯模式時，「詳細資料」入口網站應用程式會一直檢查是否已指定此元素，然後使用適當的實體定義呈現屬性。

例如，假設「學生」的實體定義包含 *user* 做為「預設我的設定檔實體」的值。在此情況下，顯示模式會使用「學生」實體定義，但是編輯模式會使用使用者實體定義。

17.1.3 以電子郵件傳送實體資料

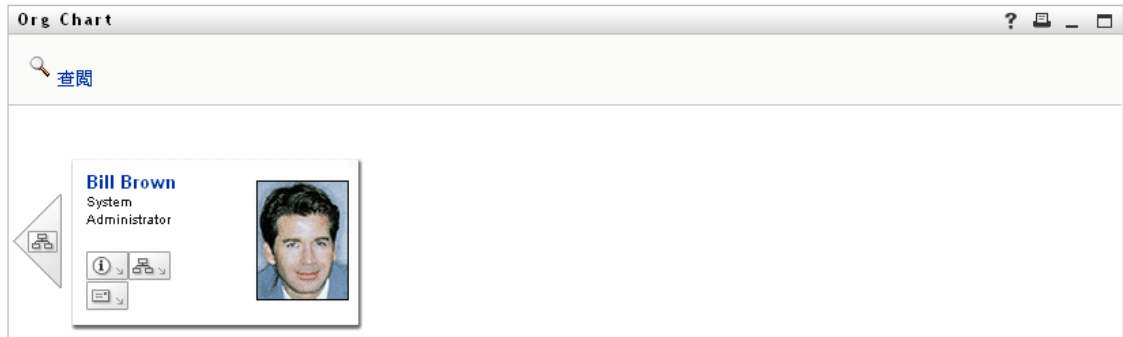
「詳細資料」入口網站應用程式會自動提供名稱為「傳送身份資訊」的連結。使用者可以按一下該連結，將目前實體「詳細資料」的 URL 以電子郵件傳送給一或多個其他使用者。因

為電子郵件傳送的是「詳細資料」URL 而不是實際的資訊，所以可以維護安全性（因為收到 URL 的人員需要適當的權限才能使用它）。

17.1.4 連結至組織圖

「詳細資料」入口網站應用程式會自動提供名稱為「顯示組織圖」的連結。使用者可以按一下此連結，以顯示目前實體的「組織圖」入口網站應用程式。

例如，如果您檢視使用者 Bill Brown 的「詳細資料」，按一下此連結即會顯示：



如需「組織圖」入口網站應用程式的相關資訊，請參閱第 18 章「組織圖入口網站應用程式參考資訊」，第 239 頁。

17.1.5 連結至其他實體的詳細資料

設定「詳細資料」入口網站應用程式的組態時，建議您讓使用者從目前的實體連結至相關實體。您可以藉由併入以控制項類型 *DNLookup* 定義（在目錄抽象層中）的屬性，來執行此操作。

當「管理員」屬性顯示在使用者的「詳細資料」中時，它會顯示為連結。按一下該連結，即會顯示「管理員」的「詳細資料」。



如需目錄抽象層的相關資訊，請參閱第 4 章「設定目錄抽象層的組態」，第 65 頁。

若要瞭解指定「詳細資料」入口網站應用程式中顯示的屬性，請參閱「設定優先設定」，第 236 頁。

17.1.6 列印實體資料

在預設狀態下，「詳細資料」入口網站應用程式的顯示設定會啓用入口網站應用程式標題列上的「列印」選項。如果保持「列印」為啓用狀態，使用者可以按一下該項，以顯示「詳細資料」內容的友善列印格式版本：

若要變更「詳細資料」入口網站應用程式的此設定或其他設定，請使用「管理員」索引標籤更新 *DetailPortlet* (在「入口網站應用程式管理」頁面上) 的「入口網站應用程式註冊」。

如需相關資訊，請參閱第 9 章「入口網站應用程式管理」，第 161 頁。

17.2 先決條件

在開始使用「詳細資料」入口網站應用程式之前，您需要瞭解：

- ◆ 「設定目錄抽象層的組態」，第 234 頁
- ◆ 「指定實體的權限」，第 234 頁

17.2.1 設定目錄抽象層的組態

「詳細資料」入口網站應用程式在許多方面都取決於目錄抽象層定義。本章中的下列各節會提供如何設定抽象層資料定義以支援特定「詳細資料」入口網站應用程式功能的相關指示：

- ◆ 「顯示實體資料」，第 226 頁
- ◆ 「編輯實體資料」，第 229 頁
- ◆ 「在頁面上使用詳細資料」，第 236 頁

如需組態的相關資訊，請參閱第 4 章「設定目錄抽象層的組態」，第 65 頁。

17.2.2 指定實體的權限

若要在「詳細資料」入口網站應用程式中存取實體及其屬性，使用者必須在 *eDirectory* 中指定適當的權限：

執行的操作	使用者需要的權限
顯示屬性	讀取
編輯屬性	寫入

您可以藉由將使用者指定為物件（實體）的託管者來分派權限。然後，您可以針對屬性指定權限。

17.3 從其他入口網站應用程式啟動詳細資料

通常會在從其中一個其他身份入口網站應用程式選取實體之後啟動「詳細資料」入口網站應用程式。您可以採用下列方式啟動「詳細資料」：

- ◆ 「從搜尋清單入口網站應用程式」，第 235 頁
- ◆ 「從組織圖入口網站應用程式」，第 235 頁

17.3.1 從搜尋清單入口網站應用程式

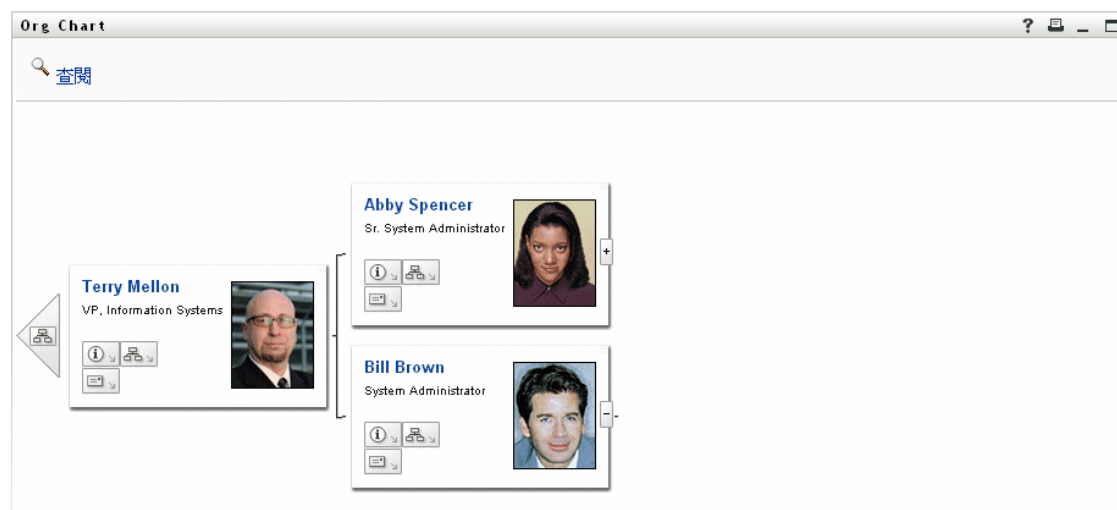
在「搜尋清單」入口網站應用程式中，使用者可以在搜尋結果中按一下實體列，以顯示該實體的「詳細資料」。例如，按一下下列清單中的 **Bill Brown** 列，即會顯示「詳細資料」入口網站應用程式與他的屬性資料：



如需「搜尋清單」入口網站應用程式的相關資訊，請參閱第 20 章「搜尋清單入口網站應用程式參考資訊」，第 265 頁。

17.3.2 從組織圖入口網站應用程式

在「組織圖」入口網站應用程式中，使用者可以按一下實體的「身份動作」圖示，然後選取「顯示資訊」，以顯示該實體的詳細資料。例如，在下列組織圖中，按一下 **Bill Brown** 的「顯示資訊」，即會顯示「詳細資料」入口網站應用程式和他的屬性資料：



如需「組織圖」入口網站應用程式的相關資訊，請參閱第 18 章「組織圖入口網站應用程式參考資訊」，第 239 頁。

17.4 在頁面上使用詳細資料

如果您想要為使用者提供自助服務，以顯示或編輯他們自己的屬性資料，您可以將「詳細資料」入口網站應用程式新增至共用頁面。在共用頁面上使用時，「詳細資料」入口網站應用程式會自動存取目前使用者（或其他預設實體）的資料。

例如，使用者 **Bill Brown** 可以登入並移至下列個人頁面，以透過「詳細資料」入口網站應用程式維護自己的資訊：



The screenshot shows the Novell Identity Manager interface. The top navigation bar includes 'Novell Identity Manager', '歡迎, Bill', and the date 'Sexta-feira, 14 de Julho de 2006'. The main content area is titled '詳細資料' (Detailed Information) and features a user profile for Bill Brown. The profile includes a photo, a '編輯您的資訊' (Edit your information) button, and a '顯示組建圖' (Show organization) button. Below the profile is a table of user attributes:

名:	Bill
姓:	Brown
職稱:	System Administrator
部門:	it
區域:	Northeast
電子郵件:	test@novell.com
管理員:	Terry Mellon
電話號碼:	(555) 555-1225

若要判定「詳細資料」入口網站應用程式在此案例中使用哪個實體定義（在此案例中，實體定義是在頁面上存取，而不是由另一個入口網站應用程式啟動），請指定目錄抽象層「組態」元素中的「預設「我的設定檔」實體」設定。

17.5 設定優先設定

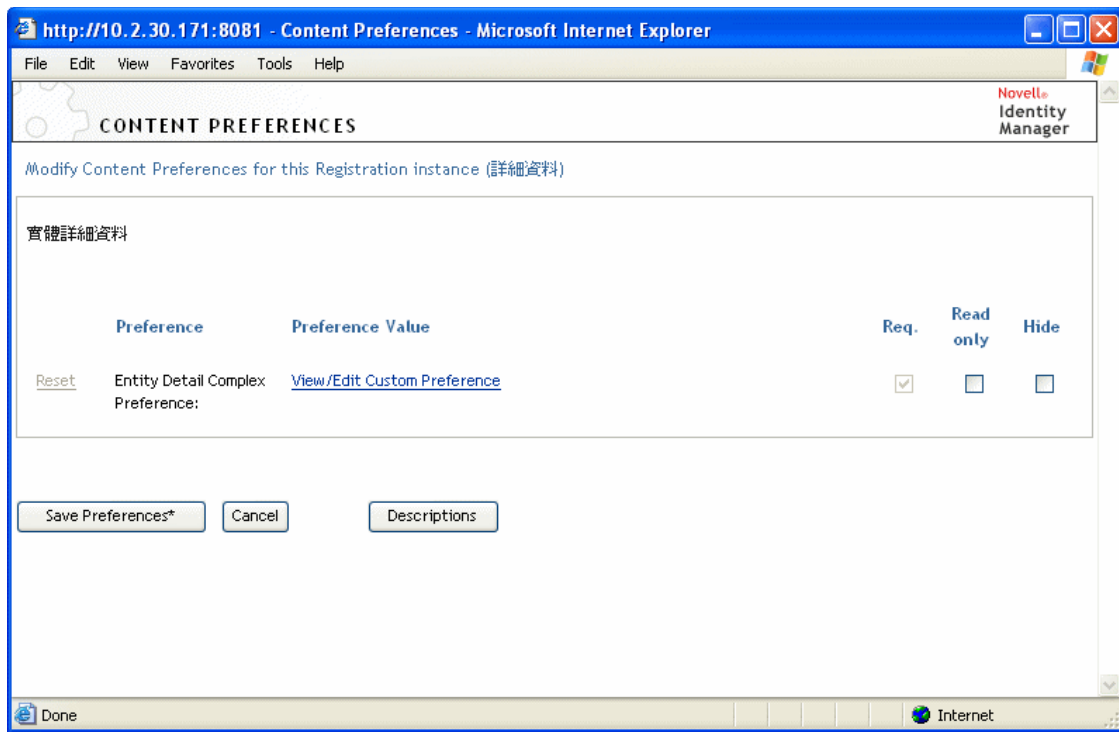
設定優先設定以定義「詳細資料」入口網站應用程式的內容和外觀。您使用「詳細資料」入口網站應用程式的方式會決定設定優先設定的位置：

若要瞭解從共享或容器頁面存取入口網站應用程式優先設定的相關資訊，請參閱第 7 章「頁面管理」，第 121 頁。

若要瞭解針對入口網站應用程式註冊存取入口網站應用程式優先設定的相關資訊，請參閱第 9 章「入口網站應用程式管理」，第 161 頁。

17.5.1 關於優先設定

「詳細資料」優先設定都包含在單一「詳細資料複雜優先設定」下：



當您開啓此複雜優先設定時，會呈現個別「詳細資料」優先設定：



[返回到列表视图](#)

這些優先設定僅適用於顯示模式（而不是編輯模式）。它們包含下列項目：

優先設定	詳細資料
實體定義	指定當「詳細資料」用於特定實體類型（例如「使用者」、「設備」或「群組」）時，要顯示的屬性清單和 HTML 配置。 您可以按一下「 新增實體定義 」，以指定其他實體類型的「詳細資料」支援。
要以清單顯示的屬性	指定您想要入口網站應用程式顯示的選定實體屬性。這些屬性會以您選擇的順序列出。 所提供的按鈕可讓您視需要新增或移除屬性。
HTML 配置	為您提供一個按鈕，以開啓「 HTML 配置編輯器 」，您可以在其中設計「詳細資料」入口網站應用程式要針對選定實體顯示的標題區域。 如需詳細資料，請參閱「 決定標題區域顯示的內容 」，第 227 頁。

本章說明如何修改現有的組織圖功能或新增組織圖功能至 Identity Manager 使用者應用程式。包含下列主題：

- ◆ 「關於組織圖」，第 239 頁
- ◆ 「設定組織圖入口網站應用程式的組態」，第 241 頁
- ◆ 「設定組織圖優先設定」，第 242 頁

18.1 關於組織圖

「組織圖」入口網站應用程式可讓一般使用者檢視並瀏覽身份儲存區中物件之間階層式關係的圖形化表示。例如，您可以定義「組織圖」入口網站應用程式，顯示下列階層：

- ◆ 組織（例如員工和經理）
- ◆ 群組成員（例如群組中的所有員工）
- ◆ 指定給使用者的設備（例如行動電話和筆記型電腦）

Identity Manager 使用者應用程式「身份自助服務」索引標籤的預設組態包含「組織圖」動作。此動作是「組織圖」入口網站應用程式，對其設定組態以顯示身份儲存區中使用者物件之間的關係。下列範例顯示預設「組織圖」入口網站應用程式如何轉換此關係（使用範例資料）。

The screenshot displays the 'Novell Identity Manager' interface. The top navigation bar includes '歡迎, Admin', '身份自助服務', '申請與核准', '管理', '登出', and '說明'. The left sidebar lists various management functions such as '資訊管理', '組織圖', '我的設定檔', '目錄搜尋', '密碼管理', '密碼處理安全回應', '密碼提示定義', '變更密碼', '目錄管理', and '建立使用者或群組'. The main content area, titled 'Org Chart', shows a search bar and a list of organizational members. The members listed are: Jack Miller (President, CEO), Chip Nano (Chief Information Officer), Anthony Palani (Chief Operating Officer), and Timothy Swan (Director, Marketing, Vice President). Each member card includes a photo, name, title, and icons for information, search, and email.

內建連結「組織圖」入口網站應用程式包含下列內建連結。

連結	描述
	可讓使用者導覽至上一層。僅當檢視的關係中父代與子代實體相同時才可用。
	<p>啓動「詳細資料」入口網站應用程式。</p> <p>此內建連結可透過「組織圖配置優先設定」，第 246 頁中描述的組織圖配置優先設定來設定組態。</p>
	<p>顯示組織圖清單。可讓使用者選擇要檢視的組織圖。</p> <p>此組織圖清單是動態的。它會顯示共享相同父代實體類型的其他組織圖。例如，如果您正在檢視經理 / 員工組織圖（父代實體是使用者），並按一下此圖示，則您可以檢視的組織圖清單將僅包含父代實體也是使用者的關係。</p> <p>此內建連結可透過「組織圖配置優先設定」，第 246 頁中描述的組織圖配置優先設定來設定組態。</p>
	<p>啓動電子郵件工具以：</p> <ul style="list-style-type: none"> ◆ 傳送目前選定使用者的身份詳細資料 ◆ 撰寫電子郵件 <p>此內建連結可透過「組織圖配置優先設定」，第 246 頁中描述的組織圖配置優先設定來設定組態。</p>
 查閱	「查閱連結」可讓使用者執行實體搜尋。搜尋會讓找到的實體成爲所顯示之圖表的頂端節點。
	讓使用者向下切入至下一層級。

如需在組織圖上新增和限制內建連結的相關資訊，請參閱「組織圖配置優先設定」，第 246 頁。

18.1.1 關於組織圖關係

「組織圖」入口網站應用程式顯示目錄抽象層中定義的關係。下列關係在安裝 Identity Manager 使用者應用程式之後可用。

- ◆ 群組成員
- ◆ 經理 - 員工
- ◆ 使用者群組

若要瞭解建立或修改「組織圖」關係的相關資訊，請參閱第 4 章「設定目錄抽象層的組態」，第 65 頁。

附註：組織圖入口網站應用程式不完全支援動態群組。您無法將動態群組定義爲關係的「父代實體」，但是可以將動態群組定義爲關係中的子代實體。

18.1.2 關於組織圖顯示

在預設狀態下，組織圖會顯示在入口網站應用程式的框架內，其顯示區域是由「入口網站應用程式寬度」和「入口網站應用程式高度」定義。如果內容需要更大的定義區域，則入口網站應用程式會延伸框線，同時會延伸頁面高度和寬度。使用者可以藉由按一下入口網站應用程式標題列上的最大化圖示，取得完整顯示的組織圖（組織圖從「詳細資料」入口網站應用程式啟動時，會以完整最大化模式顯示）。

使用者影像 在預設狀態下，「使用者」物件的組織圖配置包含「使用者照片」屬性。然而，如果身份儲存區不包含或未填入此屬性，則組織圖在執行時期會忽略此屬性。如果您將照片儲存在不同的位置，則可以設定組織圖的組態，以改為顯示那些影像。

如需相關資訊，請參閱「動態載入影像」，第 251 頁。

18.2 設定組織圖入口網站應用程式的組態

若要設定組織圖入口網站應用程式的組態，您需要：

步驟	任務	描述
1	定義您要顯示的關係	您可以使用與 Identity Manager 使用者應用程式一起安裝之其中一個預先定義的關係，也可以建立您自己的關係。 如需定義關係的相關資訊，請參閱第 4 章「設定目錄抽象層的組態」，第 65 頁。
2	驗證您要在關係中使用的實體和屬性在目錄抽象層中是否可用	如需定義關係的相關資訊，請參閱「目錄抽象層設定」，第 242 頁。
3	決定您要顯示此關係的位置	要建立新頁面以啟動組織圖嗎？或者，要從「詳細資料」入口網站應用程式或從其他組織圖啟動它嗎？ 如需建立頁面和將入口網站應用程式新增至那些頁面的相關資訊，請參閱第 7 章「頁面管理」，第 121 頁。
4	設定入口網站應用程式的優先設定	優先設定可讓您定義： <ul style="list-style-type: none">◆ 要顯示的屬性◆ 如何顯示它們（它們的 HTML 配置） 如需相關資訊，請參閱「設定組織圖優先設定」，第 242 頁。
5	測試	測試關係定義和配置
6	設定 eDirectory 權限並建立增強效能所需的任何索引	有效權限： 顯示入口網站應用程式定義的屬性，使用者必須具有對這些屬性的「讀取」權限。 效能增強： 因為子代屬性用來執行 LDAP 搜尋，所以組織圖顯示效能可以藉由將 eDirectory 值索引新增至關係的子代屬性得到增強。

18.2.1 目錄抽象層設定

「組織圖」內顯示的實體和屬性都必須在目錄抽象層中定義。下表顯示您必須針對「組織圖」中顯示之每個實體和屬性設定的屬性和內容。

定義類型	設定	值
entity	view	選取 (true)
attribute	read	選取 (true)
	search	選取 (true)

查閱連結要求「查閱連結」可讓使用者藉由執行搜尋與「父代實體」鍵相同類型的其他物件，來導覽組織圖。它需要父代實體鍵至少有一個屬性的「需要」和「搜尋」存取內容設為 true (在目錄抽象層編輯器中選取)。如果不是這樣，則無法填入「查閱連結」的「物件查閱」對話方塊，並且它會顯示空的對話方塊。

如需實體和屬性組態的相關資訊，請參閱第 4 章「設定目錄抽象層的組態」，第 65 頁。

18.2.2 設定組織圖優先設定

您可定義兩種類型的優先設定：

- ◆ 「組織圖關係優先設定」，第 243 頁
- ◆ 「組織圖配置優先設定」，第 246 頁

組織圖關係優先設定

「組織圖」關係優先設定包含在單一優先設定頁面中。

此標籤讓您可以修改此「內容例項」所定義的任何預設優先設定。對優先設定所做的任何變更僅會對此特定「內容例項」生效。

優先設定	優先值	申請	唯讀	隱藏
重設 簡報配置	檢視/編輯自定優先設定	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
重設 關係鍵	<input type="text" value="user2users"/>	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>
重設 父代實體鍵	<input type="text" value="{User/id}"/>	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>
重設 預設深度	<input type="text" value="1"/>	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>
重設 最大深度	<input type="text" value="10"/>	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>
重設 入口網站應用程式寬度	<input type="text" value="700"/>	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>
重設 入口網站應用程式高度	<input type="text" value="400"/>	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>
重設 顯示捲軸	<input type="radio"/> True <input checked="" type="radio"/> False	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>
重設 OrgChart 表層	<input type="text" value="Business Card"/>	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>

選擇

值	顯示	
Card	Business Ca	Ins 刪除

NewBleu | True Blue | Ins 刪除
新增

重設	將纜線連接至項目	<input checked="" type="radio"/> True <input type="radio"/> False	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																					
重設	功能表逾時	<input type="text" value="4000"/>	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																					
重設	顯示樹狀目錄	<input type="text" value="4"/> 插入 刪除 新增 	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																					
重設	葉簡報	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> Vertical List of Lines </div> <div style="border: 1px solid #ccc; padding: 5px;"> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="3" style="text-align: center;">選擇</th> </tr> <tr> <th style="width: 20%;">值</th> <th style="width: 50%;">顯示</th> <th style="width: 30%;"></th> </tr> </thead> <tbody> <tr> <td><input type="text" value="0"/></td> <td>Vertical List</td> <td style="text-align: right;">Ins 刪除</td> </tr> <tr> <td><input type="text" value="1"/></td> <td>Vertical List</td> <td style="text-align: right;">Ins 刪除</td> </tr> <tr> <td><input type="text" value="2"/></td> <td>Horizontal L</td> <td style="text-align: right;">Ins 刪除</td> </tr> <tr> <td><input type="text" value="3"/></td> <td>Horizontal L</td> <td style="text-align: right;">Ins 刪除</td> </tr> <tr> <td colspan="3" style="text-align: center;">新增</td> </tr> </tbody> </table> </div>	選擇			值	顯示		<input type="text" value="0"/>	Vertical List	Ins 刪除	<input type="text" value="1"/>	Vertical List	Ins 刪除	<input type="text" value="2"/>	Horizontal L	Ins 刪除	<input type="text" value="3"/>	Horizontal L	Ins 刪除	新增			詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
選擇																											
值	顯示																										
<input type="text" value="0"/>	Vertical List	Ins 刪除																									
<input type="text" value="1"/>	Vertical List	Ins 刪除																									
<input type="text" value="2"/>	Horizontal L	Ins 刪除																									
<input type="text" value="3"/>	Horizontal L	Ins 刪除																									
新增																											
重設	最小項目寬度	<input type="text" value="220"/>	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																					
重設	最小項目高度	<input type="text" value="100"/>	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																					
重設	多值的分隔符號	<input type="text" value=","/>	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																					

儲存優先設定
取消
全部重設
描述

優先設定	操作
簡報配置	按一下「檢視 / 編輯自定優先設定」，以存取配置優先設定。在「組織圖配置優先設定」，第 246 頁中有所描述。
關係鍵	輸入關係鍵。此值必須對應於目錄抽象層中指定的其中一個關係鍵。

優先設定	操作
父代實體鍵	<p>輸入代表您要顯示之組織圖根部節點的實體 DN，或者輸入 <code>\${User/id}</code> 以顯示目前使用者的組織圖 (<code>\${User/id}</code> 參數會解析目前使用者的 DN)。</p> <p>這個值必須存在目錄抽象層內 <code>search-root</code> 內容所指定的節點中，否則 LDAP 搜尋將失敗。</p> <p>以下是一些有效 DN 的範例 (使用範例資料)：</p> <ul style="list-style-type: none"> ◆ 若要以名為 Jack Miller 的員工做為組織圖的根部，來顯示 <code>user2users</code> 的「關係鍵」，則可以指定： <pre>cn=jmiller,ou=users,ou=sample,o=novell</pre> <ul style="list-style-type: none"> ◆ 若要以「會計部門」群組做為根部節點，來顯示 <code>group2users</code> 的「關係鍵」，則可以指定： <pre>cn=Accounting,ou=groups,ou=sample,o=novell</pre>
預設深度	<p>指定第一次顯示時組織圖的深度。</p> <ul style="list-style-type: none"> ◆ 0：僅顯示根部 ◆ 1：顯示根部及其子代 ◆ 2：顯示根部、其子代和子代的子代 <p>依此類推。如果此值增加到高於「最大深度」(下面)的值，則會優先採用「最大深度」值。</p>
最大深度	<p>定義使用者可以在組織圖中向下切入的最大深度。這與導覽受有效權限制之組織圖的能力不相同。</p>
組織圖表層	<p>名片</p> <p>eGuide</p> <p>Novell.com</p> <p>有線</p> <p>真實的藍色</p>
將纜線連接至項目	<p>指定是否由纜線連接組織圖卡。False 表示未連接。</p>
功能表逾時	<p>在目前顯示的功能表 (用於內建連結) 消失之前的毫秒數。</p>

優先設定	操作
顯示樹狀目錄	<p>定義每個深度層級的組織圖走向、分佈和外觀。</p> <p>前 n 個值將定義從 0 到 $n-1$ 層級的走向、分佈和外觀。最後一個值將會反覆用於 $n-1$ 以上的深度層級。值必須介於 0 到 5 之間。</p> <p>這些值為：</p> <ul style="list-style-type: none"> 0：將名片放置在項目垂直清單上方 1：水平置於項目垂直清單上方 2：將名片放置在項目水平清單上方 3：水平置於項目水平清單上方 4：將名片放置在項目垂直清單前 5：水平置於項目垂直清單前
葉簡報	定義組織圖分支之最大深度層級的組織圖走向、分佈和外觀。
最小項目寬度	此值應該等於 (「項目最小高度」 * 1.618) 的四捨五入值
最小項目高度	此值應該等於 (「項目最小寬度」 / 1.618) 的四捨五入值
多值屬性的分隔符號	用來當作具有多個值之屬性分隔符號的字元。

組織圖配置優先設定

「組織圖配置」優先設定可讓您定義組織圖實體顯示的 HTML 配置。您可以使用偏好的 HTML 編輯器，以更精確地進行編輯。請參閱「[使用外部編輯器](#)」，第 251 頁。



入口網站應用程式註冊：OrgChartPortlet

一般 類別 設定 優先設定 安全性

簡報配置

Org Chart

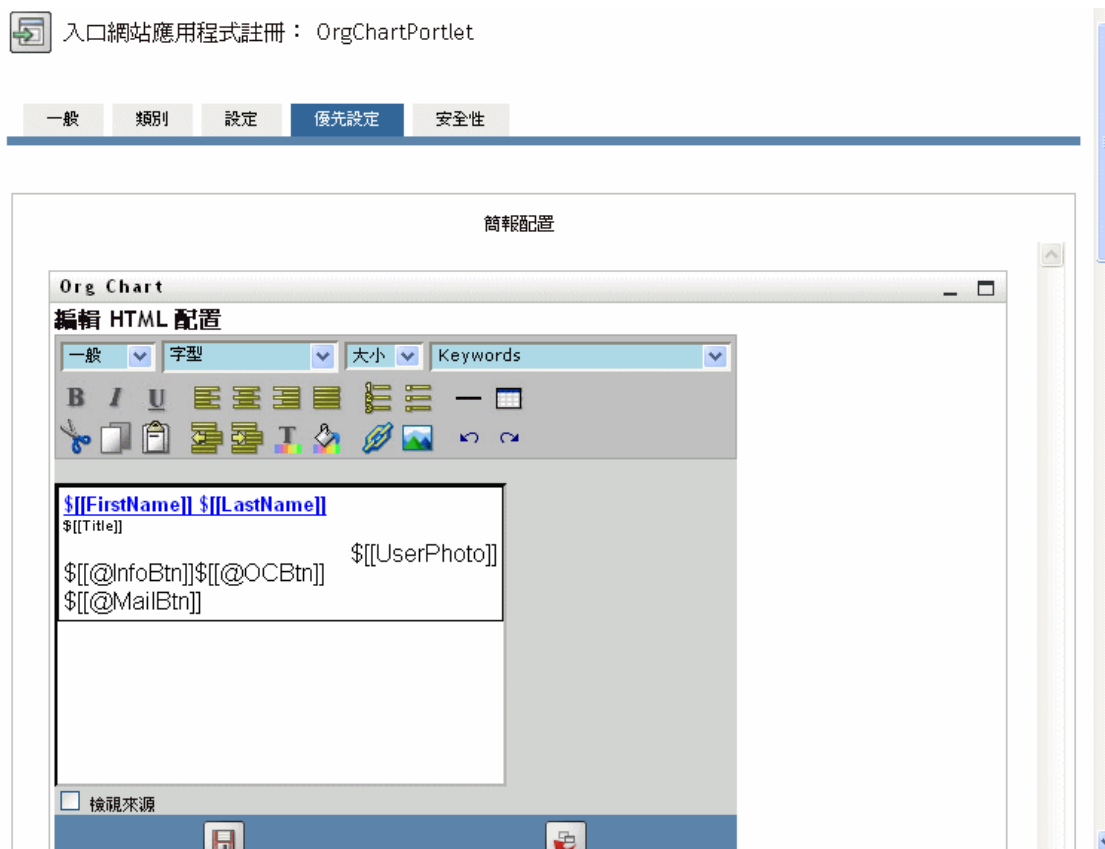
摘要

實體定義	使用者
名片的 HTML 配置	<pre> \$[[FirstName]] \$[[LastName]] \$[[Title]] \$[[UserPhoto]] \$[[@InfoBtn]]\$[[@OCBtn]] \$[[@MailBtn]] </pre>
簡易顯示的 HTML 配置	<pre> \$[[FirstName]] \$[[LastName]] - \$[[Title]] </pre>

名片的 HTML 配置：預設配置。

簡易顯示的 HTML 配置：顯示樹狀目錄優先設定設為 1 時顯示的配置。

HTML 編輯器 您可以按一下編輯按鈕，以存取 HTML 編輯器。HTML 編輯器的外觀如下：



使用 HTML 編輯器

「HTML 編輯器」會提供所見即所得 (What You See Is What You Get, WYSIWYG) 介面，以定義組織圖葉的配置。它會提供定義文字格式和清單、指定錨點和影像等 HTML 編輯器具有的一般功能。使用「關鍵字」下拉式功能表，以將屬性、指令和導覽 URL 置於配置區域內。從下拉式功能表選擇關鍵字時，會插入適當的語法，但您也可以在此配置區域中新增 HTML。

關鍵字設計配置時，您可以使用「關鍵字」下拉式功能表，以插入執行時間由特定屬性值取代的變數。或者您可以使用此語法輸入它們的參考：

```
$[[keyword]]
```

其中，*keyword* 是實體屬性的值，例如 LastName。

您可以使用此語法串連屬性：

`$$[[keyword+keyword]]`

例如：

`$$[[FirstName+LastName]]`

您可以視需要串連多個屬性，也可以包含如下用引號括住的字串：

`$$[[keyword+"sample text"+keyword]]`

這樣會轉換用引號括住的文字和關鍵字值。

附註：如果配置中的關鍵字輸入錯誤，則會在組織圖中按原樣轉換（包含 \$\$[[]]）。

HTML 編輯器功能和關鍵字用法 若要使用「HTML 編輯器」功能和「關鍵字」下拉式清單，請執行下列動作：

功能	秘訣
「插入連結」按鈕	若要插入連結，請執行下列動作： 在 Mozilla 中： <ol style="list-style-type: none">1. 反白您想要超連結的文字，然後按一下「插入連結」。2. 輸入 URL，然後按一下「建立連結」。3. 儲存優先設定。 在 IE 中： <ol style="list-style-type: none">1. 按一下「插入連結」。2. 在快顯視窗中輸入 URL。3. 反白您想要超連結的文字，然後按一下「建立連結」（在快顯視窗中）。4. 儲存優先設定。

附註：如果您的影像或 URL 位於「HTML 編輯器」的左上角，則快顯視窗會遮到它。因為快顯無法移動，所有您必須在編輯器中的其他位置建立文字，然後剪下並貼上至正確位置。

功能	秘訣
「新增影像」按鈕	<p>在 Mozilla 中：</p> <ol style="list-style-type: none"> 1. 將滑鼠焦點置於要插入影像的位置，然後按一下「新增影像」。 2. 輸入 URL 和文字，然後在快顯視窗中按一下「建立影像」。 3. 儲存優先設定。 <p>在 IE 中：</p> <ol style="list-style-type: none"> 1. 按一下「新增影像」。 2. 在快顯視窗中輸入 URL 和文字，並將滑鼠焦點置於要插入影像的位置，然後在快顯視窗中按一下「建立影像」。 3. 儲存優先設定。 <hr/> <p>附註：如果您的影像或 URL 位於「HTML 編輯器」的左上角，則快顯視窗會遮到它。因為快顯無法移動，所有您必須在編輯器中的其他位置建立文字，然後剪下並貼上至正確位置。</p> <hr/>
關鍵字下拉式功能表：屬性	這些是此實體可用的一組屬性。
關鍵字下拉式功能表：指令	<p>這些指令可讓「組織圖」入口網站應用程式啟動其他身份入口網站應用程式或內建功能，例如 IM 或電子郵件工具。</p> <ul style="list-style-type: none"> ◆ 「IM 動作」按鈕：建立傳送 IM 的按鈕。 ◆ 「郵件動作」按鈕：建立傳送電子郵件的按鈕。 ◆ 「組織圖動作」按鈕：建立切換至另一個關係的按鈕，其中選定實體例項是父代 ◆ 「資訊動作」按鈕：啟動「詳細資料」入口網站應用程式 <p>如需產生之按鈕的範例，請參閱「內建連結」，第 239 頁。</p>

功能

秘訣

URL

組織圖導覽 URL 連結：可讓您指定要做為連結顯示的 URL 或實體屬性。當使用者按一下連結時，「組織圖」入口網站應用程式會重新顯示，其中按下的實體成為根部節點。

限制：

僅當關係中的「父代」和「子代」實體屬於相同物件類型時才可用。例如，在「經理 - 員工」關係中，兩者都是使用者。

使用秘訣：

若要使用此關鍵字，您必須執行下列動作：

1. 按一下「檢視來源」。
2. 使用下列語法輸入 `@NavUrl` 關鍵字：

```
<a href="javascript:$[[@NavUrl]]">someText</a>
```

其中 *someText* 是要在執行時間顯示的連結，或實體屬性。在下列範例中，**Click here** 成為可點選的連結。

```
<a href="javascript:$[[@NavUrl]]">Click here</a>
```

在下列範例中，`FirstName` 屬性成為可點選的連結：

```
<a href="javascript:$[[@NavUrl]]">$[[FirstName]]</a>
[XXX]
```

使用限制：

對於 Internet Explorer，您不可使用下列語法。

```
<a href="$[[@NavUrl]]">someText</a>
```

在儲存操作期間，Internet Explorer 會新增下列項目：

```
http://context before $[[@NavUrl]]
```

這表示

```
<a href="$[[@NavUrl]]">someText</a>
```

成為

```
<a href="http://localhost/.../
$[[@NavUrl]]">someText</a>
```


功能	秘訣
	<p>組織圖導覽點選連結：將此關鍵字用於 <code>onClick</code> 事件 (僅啓用要重新整理的組織圖入口網站應用程式區域，而不是整個頁面)。</p> <p>使用秘訣：</p> <p>若要使用此關鍵字，您必須執行下列動作：</p> <ol style="list-style-type: none"> 按一下「檢視來源」。 使用下列語法輸入 <code>@NavClick</code> 關鍵字： <pre>`\${SomeAttribute}`</pre> <p>其中 <i>SomeAttribute</i> 是成爲可點選連結的實體屬性。</p> <p>需要 <code>"javascript:return false;"</code>。省略它會導致錯誤。</p>

若要儲存您定義的配置，請按一下「提交」。

使用外部編輯器 您可以使用 HTML 外部編輯器執行下列動作：

- 1 使用優先設定中可用的「HTML 配置編輯器」，建立實體屬性、指令和關鍵字的 HTML 原始碼。
- 2 將 HTML 原始碼複製到您選擇的編輯器。
- 3 進行想要的變更。
- 4 完成編輯時，將 HTML 原始碼複製回「HTML 配置編輯器」優先設定。

18.2.3 動態載入影像

若要顯示儲存在身份儲存區中的影像 (例如使用者照片)，您可以將屬性名稱新增至名片。例如，新增「使用者照片」屬性至名片配置，以顯示使用者的照片。

如果您將影像儲存在身份儲存區外部，則需要在「HTML 編輯器」的「檢視來源」模式內使用 `IMG:` 標籤，如下所示：

- 1 前往「組織圖」入口網站應用程式的優先設定，並存取「HTML 編輯器」。
- 2 按一下「檢視來源」。
- 3 使用 `IMG:` 標籤利用下列語法結合位置、屬性鍵和副檔名，如下所示：

```
`${IMG:"URL" + attribute-key-name + "fileextension"}`
```

如果您將員工照片做爲 `JPG` 影像按照「姓」儲存在應用程式伺服器的 `/images` 子目錄中，則下列範例會顯示您所使用的語法：

```
`${IMG:"http://myhost:8080/images/"+LastName+".jpg"}`
```

在執行時期，組織圖會串連 URL 與 LastName 屬性和副檔名 .jpg。

請注意，「HTML 編輯器」支援靈活的語法。其支援文字和屬性的任何組合，因此語法可以如下所示：

```
$$[[IMG:"some text" + attribute-key-name + ...]]
```

本章說明如何將密碼自助服務和使用者驗證功能新增至 Identity Manager 使用者應用程式。包含下列主題：

- ◆ 「準備密碼管理」，第 253 頁
- ◆ 「關於密碼入口網站應用程式」，第 255 頁
- ◆ 「IDM 登入入口網站應用程式」，第 257 頁
- ◆ 「IDM 處理安全回應入口網站應用程式」，第 258 頁
- ◆ 「IDM 提示定義入口網站應用程式」，第 259 頁
- ◆ 「IDM 變更密碼入口網站應用程式」，第 260 頁
- ◆ 「IDM 忘記密碼入口網站應用程式」，第 262 頁

19.1 準備密碼管理

若要在 Identity Manager 使用者應用程式中準備支援密碼自助服務和使用者驗證，您需要瞭解下列資訊：

- ◆ 「關於密碼管理功能」，第 253 頁
- ◆ 「eDirectory 中所需的設定」，第 253 頁

19.1.1 關於密碼管理功能

Identity Manager 使用者應用程式支援的密碼管理功能包含「使用者驗證」和「密碼自助服務」。使用這些功能時，它們可讓您的應用程式：

- ◆ 提示「登入」資訊(使用者名稱和密碼)，以驗證 Novell eDirectory
- ◆ 為使用者提供「密碼變更」自助服務
- ◆ 為使用者提供「忘記密碼」自助服務(根據需要包含提示處理安全回應、顯示密碼提示或允許密碼變更)
- ◆ 為使用者提供「處理安全問題」自助服務
- ◆ 為使用者提供「密碼提示」自助服務

19.1.2 eDirectory 中所需的設定

在您可以使用大部份密碼自助服務和使用者驗證功能之前，需要在 eDirectory 中執行下列動作：

- ◆ 啟用「通用密碼」
- ◆ 建立一或多個「密碼規則」
- ◆ 將適當的密碼規則指定給「使用者」

密碼規則 (Policy) 是指定建立和取代使用者密碼準則之管理員定義的規則 (Rule) 集合。Novell Identity Manager 會使用 Novell 模組化驗證服務 (Novell Modular Authentication Service, *NMAS*)，以強制執行在 eDirectory 中指定給使用者的密碼規則。

您可以使用 *Novell iManager*，來執行所需的設定步驟。例如，下列是某使用者如何在 *iManager* 中定義「DocumentationPassword 規則」的範例。



此密碼規則會指定下列項目：

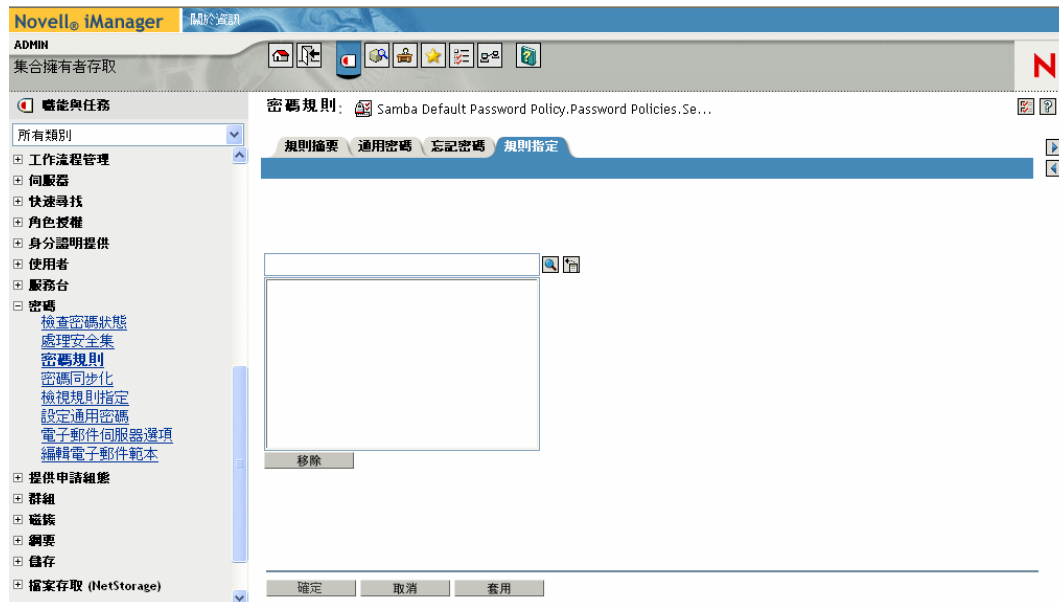
- ◆ 「通用密碼」設定



- ◆ 處理「忘記密碼」情況的設定



- ◆ 將規則套用至特定使用者的指定



如需在 eDirectory 中設定「通用密碼」和密碼規則的相關資訊，請參閱《Novell Identity Manager 管理指南 (<http://www.novell.com/documentation/dirxml20/index.html>)》。

19.2 關於密碼入口網站應用程式

若要在 Identity Manager 使用者應用程式中實作密碼自助服務和使用者驗證功能，請使用下列入口網站應用程式：

入口網站應用程式	描述
「IDM 登入入口網站應用程式」，第 257 頁	「IDM 登入」提供由 Identity Manager 支援的有力使用者驗證 (透過「通用密碼」、密碼規則和 Novell 模組化驗證服務 (NMAS))。「IDM 登入」入口網站應用程式會在登入程序期間，視需要重新導向至其他密碼入口網站應用程式。
「IDM 處理安全回應入口網站應用程式」，第 258 頁	此自助服務入口網站應用程式可讓使用者執行下列動作： <ul style="list-style-type: none"> ◆ 設定管理員定義之處理安全問題的有效回應，並設定使用者定義的處理安全問題和回應 ◆ 變更管理員定義之處理安全問題的有效回應，並變更使用者定義的處理安全問題和回應
「IDM 提示定義入口網站應用程式」，第 259 頁	此自助服務入口網站應用程式可讓使用者設定或變更其密碼提示 (在忘記密碼的情況下可能會做為線索顯示或以電子郵件傳送)。
「IDM 變更密碼入口網站應用程式」，第 260 頁	此自助服務入口網站應用程式可讓使用者根據指定的密碼規則，變更 (重設) 其「通用密碼」。它會使用該規則 (Policy) 來顯示新密碼必須符合的規則 (Rule)。 <p>如果未啟用「通用密碼」，則此入口網站應用程式會根據使用者「密碼限制」中所允許的條件，變更使用者的 eDirectory (簡易) 密碼。</p>
「IDM 忘記密碼入口網站應用程式」，第 262 頁	此自助服務入口網站應用程式使用處理安全回應驗證，讓使用者取得其密碼的相關資訊 (從 Novell 模組化驗證服務 (NMAS))。視指定的密碼規則，結果可能包含下列項目： <ul style="list-style-type: none"> ◆ 在螢幕上顯示使用者的密碼提示 ◆ 以電子郵件將提示傳送給使用者 ◆ 以電子郵件將密碼傳送給使用者 ◆ 提示使用者重設 (變更) 密碼

19.2.1 密碼自助服務入口網站應用程式模式

密碼自助服務入口網站應用程式 (「IDM 處理安全回應」、「IDM 提示定義」和「IDM 變更密碼」) 以兩種模式運作：

模式	描述	執行時期行爲
獨立模式	在共享的頁面上獨立執行入口網站應用程式。	<ul style="list-style-type: none"> ◆ 如果入口網站應用程式順利執行，則會顯示成功訊息，並帶有連結以再次執行操作。 ◆ 如果入口網站應用程式未順利執行，則會在現有表單中顯示錯誤訊息。
委託模式	登入期間驗證檢查之後，會在頁面上顯示入口網站應用程式。	<ul style="list-style-type: none"> ◆ 如果入口網站應用程式順利執行，則會將使用者重新導向至新的入口網站應用程式或使用者應用程式主頁。不會顯示任何成功訊息。 ◆ 如果入口網站應用程式未順利執行，則會在現有表單中顯示錯誤訊息。

19.3 IDM 登入入口網站應用程式

「IDM 登入」入口網站應用程式執行由 Identity Manager 支援之非常有力的使用者驗證 (透過「通用密碼」、密碼規則和 Novell 模組化驗證服務 (NMAS))。「IDM 登入」入口網站應用程式會在登入程序期間，視需要重新導向至其他密碼入口網站應用程式。



19.3.1 要求

「IDM 登入」入口網站應用程式有下列要求：

主題	要求
密碼規則	除非您要使用進階密碼規則 (Rule) 或讓使用者按一下「忘記密碼」連結，否則此入口網站應用程式不需要密碼規則 (Policy)。
通用密碼	除非您要使用具有進階密碼規則 (Rule) 的密碼規則 (Policy)，否則此入口網站應用程式不需要啟用「通用密碼」。
SSL	因為此入口網站應用程式使用保全插槽層 (SSL)，所以請確定您的應用程式伺服器已適當設定組態，以支援到 LDAP 領域的 SSL 連接。

19.3.2 用法

若要使用「IDM 登入」入口網站應用程式，您需要瞭解下列內容：

- ◆ [「IDM 登入如何重新導向至其他入口網站應用程式」](#)，第 257 頁
- ◆ [「使用寬限登入」](#)，第 258 頁

IDM 登入如何重新導向至其他入口網站應用程式

在執行時期，「IDM 登入」入口網站應用程式會根據要完成登入程序所需要的條件，重新導向至其他密碼入口網站應用程式。例如：

如果使用者	「IDM 登入」重新導向至
按一下「忘記密碼」連結	「IDM 忘記密碼入口網站應用程式」，第 262 頁

如果使用者	「IDM 登入」重新導向至
需要設定處理安全問題和回應	「IDM 處理安全回應入口網站應用程式」，第 258 頁
需要設定其密碼提示	「IDM 提示定義入口網站應用程式」，第 259 頁
需要重設無效的密碼	「IDM 變更密碼入口網站應用程式」，第 260 頁

使用寬限登入

如果您使用寬限登入，則「IDM 登入」入口網站應用程式會顯示一則警告訊息，要求您變更密碼並指出剩下的寬限登入次數。如果您是最後一次登入，則「IDM 登入」入口網站應用程式會將您重新導向至「IDM 變更密碼」入口網站應用程式。

19.4 IDM 處理安全回應入口網站應用程式

此自助服務入口網站應用程式可讓使用者執行下列動作：

- ◆ 設定管理員定義之處理安全問題的有效回應，並設定使用者定義的處理安全問題和回應
- ◆ 變更管理員定義之處理安全問題的有效回應，並變更使用者定義的處理安全問題和回應

19.4.1 要求

「IDM 處理安全回應」入口網站應用程式有下列要求：

主題	要求
密碼規則	此入口網站應用程式需要已啟用忘記密碼並具有處理安全集的密碼規則。
通用密碼	此入口網站應用程式不需要啟用「通用密碼」。

主題	要求
eDirectory 組態	<p>此入口網站應用程式要求將監督者權限授予登入使用者所在之容器的「使用者應用程式管理員」。授予這些權根可讓使用者將處理安全回應寫入機密儲存。</p> <p>例如，假設 LDAP 領域管理員為 <code>cn=admin、ou=sample、n=novell</code>，且您以 <code>cn=user1、ou=testou、o=novell</code> 身份登入。則您需要將 <code>cn=admin、ou=sample、n=novell</code> 指定為 <code>testou</code> 託管者，並在 [所有屬性權限] 上授予監督者權限。</p>

19.4.2 用法

若要使用「IDM 處理安全回應」入口網站應用程式，您需要瞭解下列內容：

- ◆ 「在登入期間如何使用 IDM 處理安全回應」，第 259 頁
- ◆ 「在使用者應用程式中如何使用 IDM 處理安全回應」，第 259 頁

在登入期間如何使用 IDM 處理安全回應

在登入程序期間，每當使用者需要設定處理安全問題和回應時，[IDM 登入入口網站應用程式 \(第 257 頁\)](#) 會自動重新導向至「IDM 處理安全回應」入口網站應用程式 (例如，管理員在 iManager 中將使用者指定至密碼規則之後，使用者第一次嘗試登入應用程式時。密碼規則必須啟用忘記密碼並包含處理安全集)。

在使用者應用程式中如何使用 IDM 處理安全回應

在預設狀態下，使用者應用程式會為使用者提供變更處理安全問題和回應的自助服務。

19.5 IDM 提示定義入口網站應用程式

此自助服務入口網站應用程式可讓使用者設定或變更其密碼提示 (在忘記密碼的情況下可能會做為線索顯示或以電子郵件傳送)。

19.5.1 要求

「IDM 提示定義」入口網站應用程式有下列要求：

主題	要求
密碼規則	此入口網站應用程式需要已啓用忘記密碼並具有處理安全集的密碼規則。
通用密碼	此入口網站應用程式不需要啓用「通用密碼」。

19.5.2 用法

若要使用「IDM 提示定義」入口網站應用程式，您需要瞭解下列內容：

- ◆ 「在登入期間如何使用 IDM 提示定義」，第 260 頁
- ◆ 「在使用者應用程式頁面中使用 IDM 提示定義」，第 260 頁

在登入期間如何使用 **IDM** 提示定義

在登入程序期間，每當使用者需要設定其密碼提示時，**IDM 登入入口網站應用程式** (第 257 頁) 會自動重新導向至「IDM 提示定義」入口網站應用程式 (例如，管理員在 iManager 中將使用者指定至密碼規則之後，使用者第一次嘗試登入應用程式時。密碼規則必須啓用忘記密碼並將動作設為「將提示以電子郵件傳送至使用者」或「在頁面上顯示提示」)。

在使用者應用程式頁面中使用 **IDM** 提示定義

在預設狀態下，使用者應用程式會為使用者提供變更其密碼提示的自助服務。

19.6 IDM 變更密碼入口網站應用程式

此自助服務入口網站應用程式可讓使用者根據指定的密碼規則，變更 (重設) 其「通用密碼」。它會使用該規則 (Policy) 來顯示新密碼必須符合的規則 (Rule)。

如果未啟用「通用密碼」，則此入口網站應用程式會根據使用者「密碼限制」中所允許的條件，變更使用者的 eDirectory (簡易) 密碼。

身份自助服務 申請與核准 管理 登出 說明

IDM 變更密碼

變更密碼

請在下面輸入新密碼：

您的密碼必須具備下列內容：

- 密碼中的字元最小個數：4
- 密碼中的字元最大個數：12

您可以在密碼中使用數字。

密碼有大小寫之分。

您可以在密碼中使用特殊字元。

舊密碼:

新密碼:

重新輸入密碼:

提交

19.6.1 要求

「IDM 變更密碼」入口網站應用程式有下列要求：

主題	要求	
「目錄抽象層」組態	此入口網站應用程式不需要任何目錄抽象層組態。	
密碼規則	除非您要使用進階密碼規則 (Rule) (已啟用「通用密碼」)，否則此入口網站應用程式不需要密碼規則 (Policy)。	
通用密碼	若要將此入口網站應用程式用於「通用密碼」，則必須在使用者所指定密碼規則 (Policy) 的「進階密碼規則 (Rule)」中啟用設定「允許使用者啓始密碼變更」。	若要將此入口網站應用程式用於 eDirectory (簡易) 密碼，則必須在使用者的「密碼限制」中啟用「允許使用者變更密碼」。

19.6.2 用法

若要使用「IDM 變更密碼」入口網站應用程式，您需要瞭解下列內容：

- ◆ 「在登入期間如何使用 IDM 變更密碼」，第 262 頁
- ◆ 「在使用者應用程式中使用 IDM 變更密碼」，第 262 頁

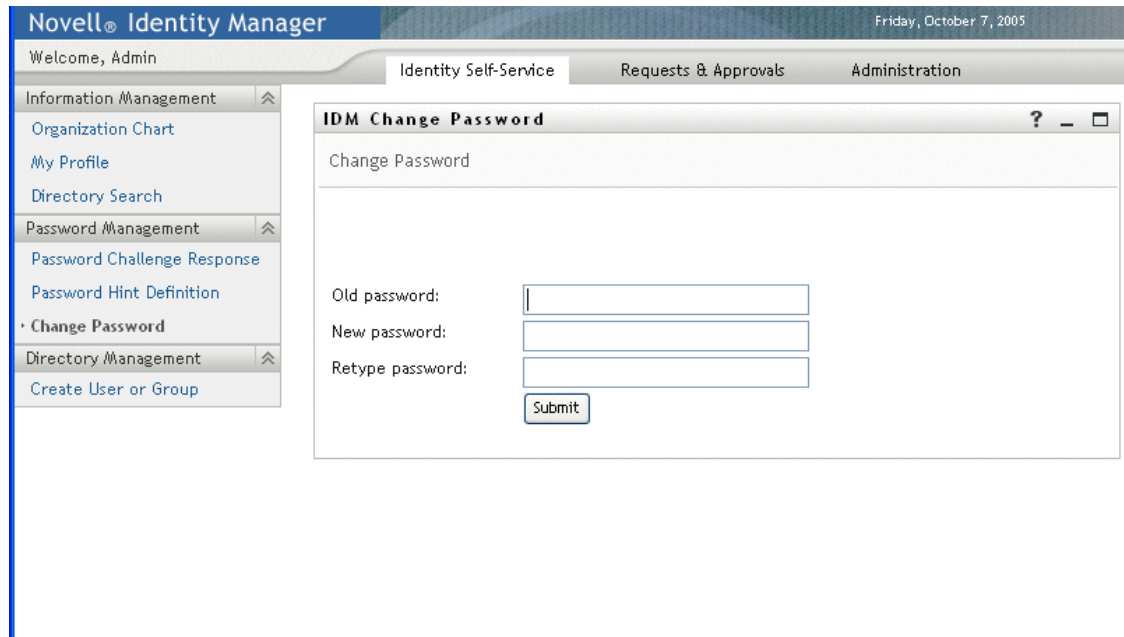
在登入期間如何使用 **IDM** 變更密碼

在登入程序期間，每當使用者需要重設無效的密碼時，**IDM 登入入口網站應用程式 (第 257 頁)** 會自動重新導向至「**IDM 變更密碼**」入口網站應用程式 (例如，管理員在實作要求使用者重設其密碼的密碼規則之後，使用者第一次嘗試登入應用程式時)。

如果使用者所指定密碼規則將重設密碼指定為忘記密碼情況時的動作，則 **IDM 忘記密碼入口網站應用程式 (第 262 頁)** 也會自動重新導向至「**IDM 變更密碼**」。

在使用者應用程式中使用 **IDM** 變更密碼

在預設狀態下，使用者應用程式會為使用者提供使用「**IDM 變更密碼**」入口網站應用程式的密碼變更自助服務。例如：



The screenshot displays the Novell Identity Manager web interface. The top navigation bar includes 'Welcome, Admin', 'Identity Self-Service', 'Requests & Approvals', and 'Administration'. The left sidebar lists various management options, with 'Change Password' highlighted under the 'Password Management' section. The main content area shows the 'IDM Change Password' form, which includes three input fields for 'Old password:', 'New password:', and 'Retype password:', along with a 'Submit' button. The date 'Friday, October 7, 2005' is visible in the top right corner.

19.7 IDM 忘記密碼入口網站應用程式

此自助服務入口網站應用程式使用處理安全 / 回應驗證，讓使用者取得其密碼的相關資訊。視指定的密碼規則，結果可能包含下列項目：

- ◆ 在螢幕上顯示使用者的密碼提示
- ◆ 以電子郵件將提示傳送給使用者
- ◆ 以電子郵件將密碼傳送給使用者
- ◆ 提示使用者重設 (變更) 密碼

IDM 忘記密碼

忘記密碼

您必須指定您的使用者名稱才能登入。

使用者名稱:

提交

19.7.1 要求

「IDM 忘記密碼」入口網站應用程式有下列要求：

主題	要求
密碼規則	此入口網站應用程式需要已啓用忘記密碼並具有處理安全集的密碼規則。
通用密碼	此入口網站應用程式不需要啓用「通用密碼」(除非您要支援下列忘記密碼動作：重設密碼或將密碼以電子郵件傳送給使用者)。

19.7.2 用法

若要使用「IDM 忘記密碼」入口網站應用程式，您需要瞭解下列內容：

- ◆ 「在登入期間如何使用 IDM 忘記密碼」，第 263 頁
- ◆ 「針對電子郵件動作設定環境組態」，第 264 頁
- ◆ 「IDM 忘記密碼的優先設定」，第 264 頁

在登入期間如何使用 **IDM** 忘記密碼

在登入程序期間，如果使用者按一下「忘記密碼」連結，則 **IDM 登入入口網站應用程式 (第 257 頁)** 會重新導向至「IDM 忘記密碼」入口網站應用程式。當顯示「IDM 忘記密碼」時，會進行下列操作：

- 1 提示「使用者名稱」。
- 2 重新導向至 **IDM 登入入口網站應用程式 (第 257 頁)**，以對該使用者執行「處理安全/回應驗證」。
- 3 執行在已驗證之使用者指定密碼規則中指定的「忘記密碼動作」。會進行下列其中一項操作：
 - ◆ 重新導向至 **IDM 變更密碼入口網站應用程式 (第 260 頁)**，以便使用者可以重設其密碼
 - ◆ 以電子郵件將密碼或提示傳送至使用者
 - ◆ 顯示提示

附註：「IDM 忘記密碼」入口網站應用程式將不會獨立使用。這表示您不應將其新增至使用者應用程式中的共用頁面。將此入口網站應用程式置於頁面上可能會產生安全性風險，讓其他人可以在使用者不瞭解或不允許的情況下，變更無人管理之機器上的密碼。

針對電子郵件動作設定環境組態

如果您要支援忘記密碼電子郵件動作，則需要確定已適當設定「電子郵件通知伺服器」：

- 1 在 eDirectory 伺服器上，使用 Web 瀏覽器存取 *iManager*，並以「管理員」身份登入。
- 2 移至「角色和任務 > 密碼」，並選取「電子郵件伺服器選項」。
- 3 指定適當的設定，然後按一下「確定」。

「IDM 忘記密碼」入口網站應用程式使用兩種電子郵件範本。在 *iManager* 中，您可在「角色和任務 > 密碼 > 編輯電子郵件範本」中找到它們。它們的名稱為：

- ◆ 密碼提示申請
- ◆ 您的密碼申請

您可以視應用程式的需要變更這些範本的內容（但不要變更結構）。

IDM 忘記密碼的優先設定

「IDM 忘記密碼」入口網站應用程式提供下列優先設定：

優先設定	詳細資料
login-sequence	要使用的 Novell 模組化驗證服務 (NMAS) 登入程序。在此版本中，入口網站應用程式僅支援「處理安全回應」。
ldap-sslport	要使用的安全 LDAP 連接埠。預設值為 636 。
allow-wildcard	使用者是否可以在輸入使用者名稱時輸入萬用字元。預設值為 false 。
encoding	要使用的字元編碼。預設值為 utf-8 。

本章描述如何設定和自定「搜尋清單」入口網站應用程式，以與 Identity Manager 使用者應用程式搭配使用。包含下列主題：

- ◆ 「關於搜尋清單」，第 265 頁
- ◆ 「設定搜尋清單入口網站應用程式的組態」，第 270 頁

20.1 關於搜尋清單

「搜尋清單」入口網站應用程式可讓使用者搜尋並顯示身份儲存區的內容。它是 Identity Manager 使用者應用程式「身份自助服務」索引標籤之「目錄搜尋」動作的基礎。將「目錄搜尋」動作的組態設定為可讓使用者搜尋使用者、群組和任務群組，但您可以進行修改以變更可搜尋物件和屬性的範圍。

下列範例顯示「目錄搜尋」動作如何讓使用者定義搜尋準則。



使用者介面元素	描述
搜尋	使用者選取要搜尋的物件類型。 如需定義此清單內容的相關資訊，請參閱「設定搜尋清單優先設定」，第 271 頁。

使用者介面元素

描述

使用此準則

使用者可藉由從下拉式功能表選取屬性和搜尋運算子來定義搜尋準則。
當使用者選取「進階搜尋」時，可以指定可內含 (AND) 或排除 (OR) 之搜尋準則群組的多個列和多個區塊。

如需定義可搜尋屬性的相關資訊，請參閱「設定搜尋清單優先設定」，第 271 頁。

搜尋

執行特定的搜尋準則。

如需定義預設搜尋的相關資訊，請參閱「設定搜尋清單優先設定」，第 271 頁。

我已儲存的搜尋

可讓使用者執行、編輯或刪除選定之先前儲存的搜尋。



進階搜尋

與「搜尋」按鈕類似，它可讓使用者新增搜尋準則的列或區塊，但在進階搜尋中，可以指定可內含 (AND) 或排除 (OR) 之搜尋準則群組的多個列和多個區塊。



如需定義可搜尋屬性的相關資訊，請參閱「設定搜尋清單優先設定」，第 271 頁。

此範例顯示在輸入搜尋準則「名字開頭為 A」之後，入口網站應用程式如何顯示：

Novell Identity Manager 搜尋清單截圖。顯示了搜尋結果，包括使用者名稱、位置、組織、職稱、電子郵件和電話號碼。

身份	位置	組織	職稱	電子郵件	電話號碼
Alison	Chester		Manager		
Admin	Idmsample				
Admin	WacKenzie		Director, Marketing		(555) 555-1220
Alison	Quinn				
Alison	Ryan				
Alison	Siggins		MS		

您可以設定「搜尋清單」入口網站應用程式的組態，以使用下列任何功能：

使用者介面元素	描述
「身份」、「位置」、「組織」索引標籤	使用者按一下其中一個索引標籤，來查看以不同方式顯示的結果清單。 如需格式的相關資訊，請參閱「 關於結果清單顯示格式 」，第 268 頁。
我已儲存的搜尋 	可讓使用者選取先前儲存的搜尋。
儲存搜尋 	可讓使用者儲存搜尋準則並視需要重新執行儲存的搜尋。這些搜尋儲存在目前登入之使用者的 <code>srprvQueryList</code> 屬性中。
輸出結果 	可讓使用者以不同格式輸出搜尋結果。
修訂搜尋 	可讓使用者變更搜尋準則。
新搜尋 	可讓使用者定義新的搜尋。

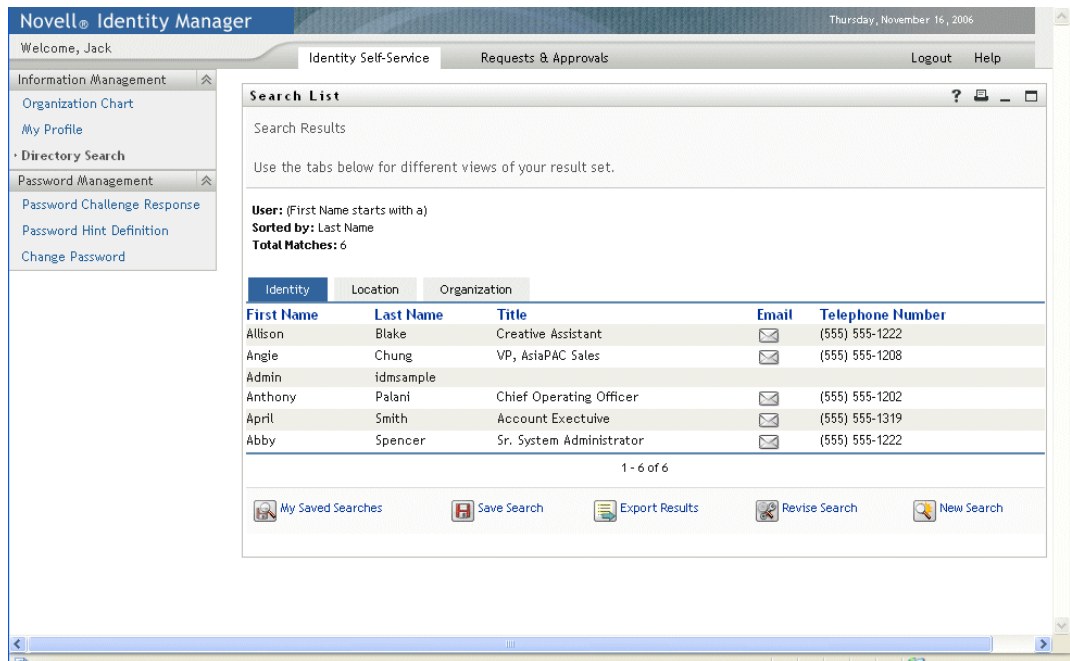
在預設狀態下，「搜尋清單」還可讓一般使用者執行下列動作：

- ◆ 列印搜尋結果
- ◆ 從結果清單啟動電子郵件
- ◆ 從結果清單啟動「詳細資料」入口網站應用程式

20.1.1 關於結果清單顯示格式

您可以定義如何將從身份儲存區搜尋傳回的資料顯示給一般使用者。可在下列一或多個頁面類型中組織資料：

- ◆ 身份頁面：通常包含聯絡人資訊，如下所示：



The screenshot displays the Novell Identity Manager interface. The main content area shows a search results page titled "Search List". The search criteria are "User: (First Name starts with a)", sorted by "Last Name", with a total of 6 matches. The results are presented in a table with columns for First Name, Last Name, Title, Email, and Telephone Number. The table lists six users: Allison Blake, Angie Chung, Admin idmsample, Anthony Palani, April Smith, and Abby Spencer. Below the table, there are navigation options: My Saved Searches, Save Search, Export Results, Revise Search, and New Search.

Identity	Location	Organization		
First Name	Last Name	Title	Email	Telephone Number
Allison	Blake	Creative Assistant	✉ (555) 555-1222	
Angie	Chung	VP, AsiaPAC Sales	✉ (555) 555-1208	
Admin	idmsample			
Anthony	Palani	Chief Operating Officer	✉ (555) 555-1202	
April	Smith	Account Executive	✉ (555) 555-1319	
Abby	Spencer	Sr. System Administrator	✉ (555) 555-1222	

- ◆ 位置頁面：通常包含位置資訊，如下所示：



- ◆ 組織頁面：通常包含組織階層資訊，如下所示：



您可以使用入口網站應用程式的複雜優先設定來定義其他結果清單格式。例如，如果您的身份儲存區網要包含員工技能或驗證的相關資訊，則可以設定結果清單以顯示此資訊。

根據設定入口網站應用程式組態的方式而定，一般使用者可以執行下列動作：

- ◆ 選擇要搜尋的身份儲存區物件類型（例如，使用者和群組）
- ◆ 指定他們要搜尋的「準則」（例如，「名字開頭為」、「姓氏包含」等等）
- ◆ 選擇他們要檢視搜尋結果的「顯示格式」
- ◆ 變更「排序順序」

20.2 設定搜尋清單入口網站應用程式的組態

若要設定「搜尋清單」入口網站應用程式的組態，請遵循下列一組步驟：

步驟	任務	描述
1	定義： <ul style="list-style-type: none">◆ 將允許使用者搜尋的實體和屬性◆ 要如何顯示結果清單	<p>您可以使用與目前 Identity Manager 使用者應用程式一起安裝的預先定義「目錄搜尋」動作。您可以修改它，或建立您自己的「目錄搜尋」動作。</p> <p>如需相關資訊，請參閱「設定搜尋清單優先設定」，第 271 頁。</p>
2	驗證用於搜尋的實體和屬性集是否在目錄抽象層中定義。	如需相關資訊，請參閱第 4 章「設定目錄抽象層的組態」，第 65 頁。
3	決定您要使用者存取入口網站應用程式的方式。	<p>要使用者從現有或新的頁面啟動此入口網站應用程式？</p> <p>如需頁面的相關資訊，請參閱第 7 章「頁面管理」，第 121 頁。</p>
4	設定入口網站應用程式的優先設定	<p>搜尋清單入口網站應用程式的優先設定可讓您定義下列項目：</p> <ul style="list-style-type: none">◆ 針對每個結果清單格式顯示的屬性◆ 搜尋將會產生的結果清單顯示格式◆ 結果清單格式的預設排序順序 <p>如需相關資訊，請參閱「設定搜尋清單優先設定」，第 271 頁。</p>
5	測試設定	驗證結果清單是否顯示所需屬性。
6	設定 eDirectory 權限並建立增強效能所需的任何索引	<p>eDirectory 權限：</p> <p>執行搜尋</p> <ul style="list-style-type: none">◆ 執行搜尋的使用者需要對要搜尋之所有使用者或物件的「瀏覽」權限。 <p>儲存搜尋（針對非「管理」使用者）：</p> <ul style="list-style-type: none">◆ 使用者執行搜尋所在組織單位和組織的「託管者」。◆ 「使用者」需要寫入、個別和監督者權限。 <p>效能增強：將 eDirectory 值索引新增至搜尋所依據的屬性，可增進搜尋的效能。</p>

如需定義不同結果清單顯示格式的相關資訊，請參閱「設定搜尋清單優先設定」，第 271 頁。

20.2.1 目錄抽象層設定

必須在目錄抽象層中定義可從搜尋準則下拉式功能表選取的實體和屬性，以及從身份儲存區搜尋傳回的資料。下表顯示您應針對搜尋清單使用之實體和屬性設定的內容。

定義類型	設定	目錄抽象層值
entity	view	選取 (true)
attribute	enable	選取 (true)
	search	選取 (true) 當為 false 時，您無法在此屬性上定義搜尋，或將其包含在結果清單格式中
	hide	不選 (false) 因為在搜尋期間，「搜尋清單」入口網站應用程式不會檢查 hide 屬性的值 (這樣會降低效能)，所以 search 為選取 (true) 的屬性必須同時將 hide 設為不選 (false)。 假設 User1 將 HomePhone 屬性設為 hide=true (在 eDirectory 中)。因為 HomePhone 是可搜尋的，所以「搜尋清單」會取回記錄，但「搜尋清單」不會檢查其他屬性的值 (因為這會影響效能)。如果另一個使用者已搜尋到 HomePhone 屬性的完全相符項目，則隱藏的記錄會在結果清單中顯示。

其他目錄抽象層設定 目錄抽象層資料類型、格式類型、過濾器 and 搜尋範圍也會影響「搜尋清單」入口網站應用程式。資料類型和格式類型會影響外觀，而過濾器和搜尋範圍會影響傳回的資料數目。

如需相關資訊，請參閱「使用實體和屬性」，第 76 頁。

20.2.2 設定搜尋清單優先設定

您可定義兩種類型的優先設定：

- ◆ 「搜尋優先設定」，第 272 頁
- ◆ 「結果清單格式優先設定」，第 274 頁

搜尋優先設定

搜尋優先設定內含於單一優先設定頁面中：

[修改此註冊例項的內容優先設定 \(搜尋清單\)](#)

搜尋清單

優先設定	優先值	申請	唯讀	隱蔽																				
重設 預設模式:	<input type="text" value="My Saved Searches"/>	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>																				
<table border="1"><thead><tr><th>選擇</th><th>值</th><th>顯示</th><th></th></tr></thead><tbody><tr><td></td><td>MODE_SIMP</td><td>Basic Search</td><td>Ins 刪除</td></tr><tr><td></td><td>MODE_ADVA</td><td>Advanced Se</td><td>Ins 刪除</td></tr><tr><td></td><td>MODE_SAVE</td><td>My Saved Se</td><td>Ins 刪除</td></tr><tr><td colspan="4" style="text-align: center;">新增</td></tr></tbody></table>					選擇	值	顯示			MODE_SIMP	Basic Search	Ins 刪除		MODE_ADVA	Advanced Se	Ins 刪除		MODE_SAVE	My Saved Se	Ins 刪除	新增			
選擇	值	顯示																						
	MODE_SIMP	Basic Search	Ins 刪除																					
	MODE_ADVA	Advanced Se	Ins 刪除																					
	MODE_SAVE	My Saved Se	Ins 刪除																					
新增																								
重設 頁碼:	<input type="text" value="10"/>	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>																				
<table border="1"><thead><tr><th>範圍</th><th>分鐘</th><th>上限</th></tr></thead><tbody><tr><td></td><td><input type="text"/></td><td><input type="text"/></td></tr></tbody></table>					範圍	分鐘	上限		<input type="text"/>	<input type="text"/>														
範圍	分鐘	上限																						
	<input type="text"/>	<input type="text"/>																						
重設 結果限制:	<input type="text" value="0"/>	詳細資料	<input checked="" type="checkbox"/>	<input type="checkbox"/>																				
<table border="1"><thead><tr><th>範圍</th><th>分鐘</th><th>上限</th></tr></thead><tbody><tr><td></td><td><input type="text"/></td><td><input type="text"/></td></tr></tbody></table>					範圍	分鐘	上限		<input type="text"/>	<input type="text"/>														
範圍	分鐘	上限																						
	<input type="text"/>	<input type="text"/>																						
重設 搜尋及清單複雜優先設定:	檢視/編輯自定優先設定	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																				

搜尋優先設定定義如下：

優先設定	操作
預設模式	<p>指定當使用者首次存取入口網站應用程式時，您想讓其顯示的方式。值為：</p> <p>基本搜尋：允許使用者輸入單一搜尋準則。例如：</p> <p>First Name starts with A</p> <p>進階搜尋：允許使用者在一或多個搜尋區塊中定義多個搜尋準則。使用者可以在搜尋準則內或搜尋區塊之間使用 and/or 邏輯運算子。例如，使用者可以建立如下所示的搜尋：</p> <p>(First Name starts with A or First Name starts with B) and (Region = Northeast or Region = Southeast)</p> <p>或</p> <p>(First Name starts with A and Last Name starts with B) or (First Name starts with B and Last Name starts with A)</p> <p>我已儲存的搜尋：顯示由目前登入使用者儲存的搜尋清單。這些搜尋儲存在使用者的 <code>srvprvQueryList</code> 屬性中。</p> <hr/> <p>附註：藉由執行或編輯搜尋，或按一下入口網站應用程式底部的按鈕，使用者可以在執行時期存取任一模式。</p>
頁碼	一次顯示的最大列數。
結果限制	搜尋傳回的最大符合項目數。如果設為 0，則該最大值會遵循目錄抽象層設定。
搜尋和清單複雜優先設定	<p>按一下以修改下列項目：</p> <ul style="list-style-type: none"> ◆ 要搜尋的實體 ◆ 結果集類型 ◆ 包含於頁面中的屬性和它們出現的順序 <p>在預設狀態下，在目錄抽象層中列出之屬性 <code>view=true</code> 的任何物件都包含於搜尋中。實體的屬性清單衍生自目錄抽象層中列出的屬性，且其屬性定義為 <code>enable=true</code>。</p>

結果清單格式優先設定

複雜優先設定頁面可讓您定義要包含於搜尋中的實體，以及格式化結果清單的方式。預設的優先設定頁面如下所示：

Novell Identity Manager

內容優先設定

[修改此註冊例項的內容優先設定 \(搜尋清單\)](#)

搜尋清單

搜尋及清單複雜優先設定

搜尋清單

摘要

實體定義	使用者	
將電子郵件顯示為圖示	<input checked="" type="radio"/> true <input type="radio"/> false	<input type="checkbox"/>
結果清單類型	預設值	<input type="checkbox"/>
身份	<input checked="" type="radio"/>	排序 <input type="checkbox"/>
屬性名	<input type="radio"/>	<input type="checkbox"/>
姓	<input checked="" type="radio"/>	<input type="checkbox"/>
職稱	<input type="radio"/>	<input type="checkbox"/>
電子郵件	<input type="radio"/>	<input type="checkbox"/>
電話號碼	<input type="radio"/>	<input type="checkbox"/>
位置	<input type="radio"/>	排序 <input type="checkbox"/>
屬性名	<input type="radio"/>	<input type="checkbox"/>
姓	<input type="radio"/>	<input type="checkbox"/>
區域	<input checked="" type="radio"/>	<input type="checkbox"/>
電子郵件	<input type="radio"/>	<input type="checkbox"/>
電話號碼	<input type="radio"/>	<input type="checkbox"/>
組織	<input type="radio"/>	排序 <input type="checkbox"/>
屬性名	<input type="radio"/>	<input type="checkbox"/>
姓	<input type="radio"/>	<input type="checkbox"/>
職稱	<input type="radio"/>	<input type="checkbox"/>

[返回清單檢視](#)

複雜優先設定包含下列項目：

優先設定	操作
實體定義	<p>對搜尋有效的每個物件 (view=true) 在此優先設定頁面上都具有對應的「實體定義」區塊。使用這些優先設定，來執行下列動作：</p> <ul style="list-style-type: none"> ◆ 定義包含於搜尋中的物件。 ◆ 修改結果清單格式定義 (例如新增和移除顯示的屬性以及其預設的排序順序)。 ◆ 藉由按一下「實體定義」行上顯示的刪除按鈕，移除您不想包含於搜尋中的任何物件。這會刪除整個實體定義區塊。 <p>稍後，您可以藉由按一下「新增實體定義」(位於頁面的底部)，並完成精靈選項面板，來將物件新增回搜尋。</p> <hr/> <p>提示：如果物件未在此清單中列出，而是在目錄抽象層中列出，請核取「檢視」修改元 (在實體物件上)。如果設為 false，則身份入口網站應用程式無法使用實體。</p>
將電子郵件顯示為圖示	<p>當為 true 且已在結果清單中指定「電子郵件」屬性時，它將顯示為圖示。當為 false 時，「電子郵件」屬性會顯示完整的電子郵件地址。電子郵件屬性 (無論是文字或圖示) 是可點選的 mailto: 連結。</p>
結果清單類型 (預設值)	<p>指定目前實體的結果清單預設格式。僅當目前使用者未選取其他格式時，才會使用預設值。</p>
結果清單顯示格式區塊	<p>指定顯示格式 (例如「身份」、「位置」或「組織」頁面)，並包含類型要包含的屬性集。</p> <p>若要移除「結果清單類型」，請執行下列動作：</p> <ul style="list-style-type: none"> ◆ 按一下「結果清單類型」旁的刪除按鈕。 <p>即會從搜尋中刪除頁面類型及其所有相關聯的屬性。</p> <p>若要新增結果集頁面，請執行下列動作：</p> <ul style="list-style-type: none"> ◆ 按一下展開按鈕，並從選項清單中選取結果集格式。

優先設定	操作
屬性	<p>指定針對特定顯示格式顯示的屬性集。</p> <p>若要新增或移除屬性，請執行下列動作：</p> <ul style="list-style-type: none"> ◆ 按一下修改屬性按鈕。 ◆ 若要新增屬性，請從「可用」屬性清單中選取它。 ◆ 按一下箭頭，以將其移至「選定」清單中。執行相反的动作，以從「結果清單」中移除屬性。 ◆ 若要重排屬性清單，請按一下選定清單右側的向上和向下箭頭。 ◆ 按一下「提交」。 <p>屬性和資料類型：屬性的資料類型會影響其顯示的方式。例如，如果將屬性定義為本地清單或全域清單的子類型，則可能的值會顯示在「基本搜尋準則」或「進階搜尋準則」螢幕的下拉式清單方塊中。如果類型是 DN，則會顯示搜尋和歷程按鈕，以讓使用者在「基本搜尋準則」或「進階搜尋準則」螢幕中選取值，且 DN 將會在結果清單中解析成使用者易讀的顯示名稱。資料類型和子類型還會限制針對使用者顯示的比較運算子，以確保只建構有效的比較。</p> <p>如需相關資訊，請參閱第 4 章「設定目錄抽象層的組態」，第 65 頁。</p>
結果清單顯示格式區塊排序	<p>「結果清單」的排序順序以此屬性為基礎。僅當「結果集類型」不是目前使用者會期的顯示格式時，預設的排序順序才會生效。</p> <p>多值屬性和單一值屬性：在結果清單中顯示的記錄數目根據排序屬性是單一還是多值而定。雖然符合項目的總數保持不變，但是排序多值屬性通常會產生更多記錄。這是因為多值屬性的每個值都會單獨顯示為一行。</p>

完成優先設定面板

若要驗證您已提交有效的項目，請按一下「提交」。如果項目無效，則您會看到一則錯誤訊息，顯示在優先設定頁面的頂端。一旦您可以解決所有的錯誤，就按一下「返回清單檢視」，然後按一下「儲存優先設定」。

設計和管理提供申請



下列章節說明如何使用「Identity Manager 提供模組」的功能。

- ◆ 第 21 章 「工作流程提供簡介」, 第 279 頁
- ◆ 第 22 章 「設定提供申請定義的組態」, 第 291 頁
- ◆ 第 23 章 「管理提供工作流程」, 第 313 頁

工作流程提供簡介

本章提供工作流程提供的綜覽。包含下列主題：

- ◆ 「關於工作流程提供」，第 279 頁
- ◆ 「提供組態和管理」，第 287 頁
- ◆ 「提供安全性」，第 287 頁

21.1 關於工作流程提供

Identity Manager 的主要功能就是工作流程提供，它是管理使用者存取組織中安全資源的程序。這些資源可能包含數位實體，例如使用者帳戶、電腦和資料庫。在本版次中，提供的資源會映射至 Identity Manager 授權。

Identity Manager 可以為多種「提供申請」提供服務。提供申請是用於授予或撤銷對組織資源之存取權的使用者或系統動作。它們可以由一般使用者透過 Identity Manager 使用者應用程式直接啓始，或間接回應在身份儲存區 (eDirectory) 中發生的事件。

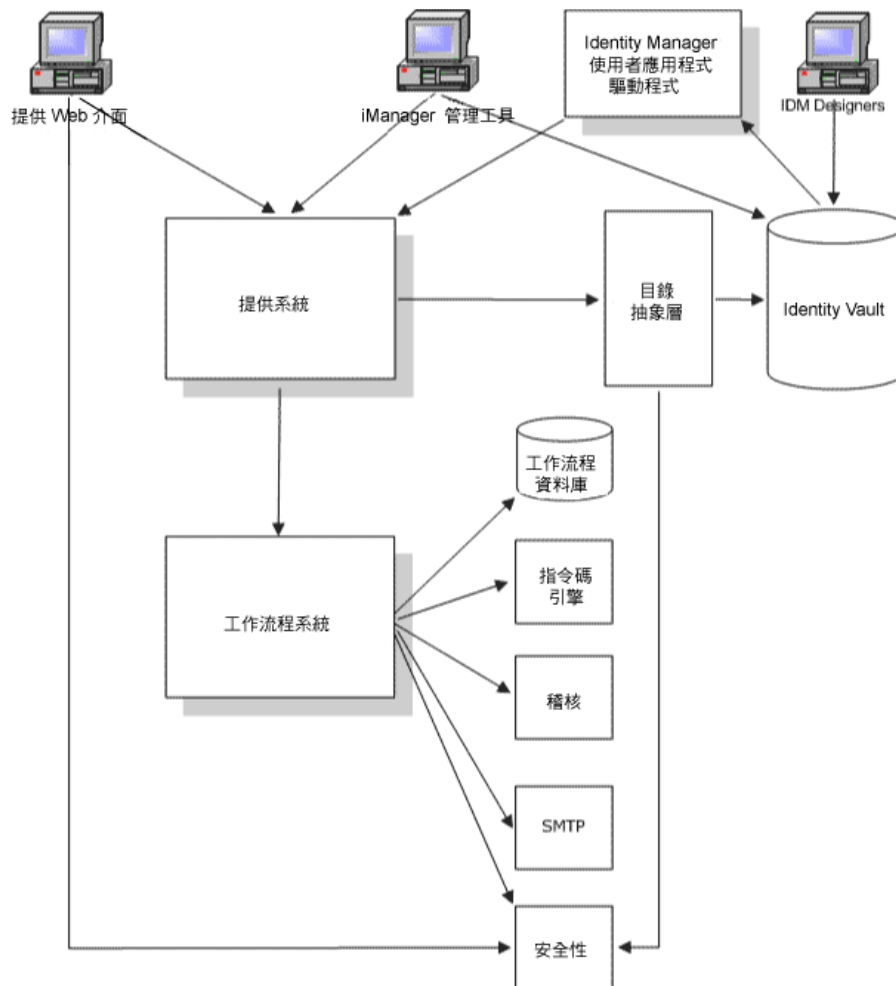
當提供申請需要組織中一或多個人員的許可時，申請便會啓動工作流程。工作流程會協調完成申請所需的核准。一些提供申請需要單個人員的核准；而其他提供申請則需要數個人員的核准。在某些例項中，無需任何核准即可完成申請。

部份工作流程需要處理以循序方式繼續，且要循序執行每個核准步驟。其他工作流程會提供對平行處理的支援。定義提供申請時，您要指定讓工作流程支援循序處理還是平行處理。

Identity Manager 會提供一組 Web 型態的工具，管理員可以使用這些工具在使用者應用程式中建立提供功能。這些工具可讓您設定提供申請的組態，並管理正在進行中的工作流程。若要設定提供申請的組態，管理員需要建立提供申請定義，將資源結合至工作流程。

21.1.1 高層級結構

下圖顯示 Identity Manager 中包含的工作流程提供系統高層級結構：



下列各節描述此結構的每個元件。

提供 **Web** 介面

Identity Manager 使用者應用程式會提供 Web 介面，一般使用者可透過該介面提交提供申請，並在提交申請之後對這些申請進行管理。使用者應用程式還會提供能夠指定提供工作流程之委託和代理的「組織管理員」或「使用者應用程式管理員」。

提示：您可以在 Identity Manager 使用者應用程式的「申請與核准」索引標籤上找到提供和工作流程動作。

如需委託和代理的相關資訊，請參閱「提供安全性」，第 287 頁。如需使用使用者應用程式的完整詳細資料，請參閱《Identity Manager 使用者應用程式：使用者指南》。

iManager 管理工具

iManager 會提供您可用於設定和管理提供申請及其相關工作流程的外掛程式。

若要設定提供申請的組態，請將其結合至提供的資源，指定相關工作流程的執行時期特性，然後啓用它以供使用。在啓始提供申請之後，您可以使用 **iManager** 來檢視執行中工作流程程序的狀態，重新指定工作流程內的活動，或者在工作流程阻塞時終止該工作流程。

Identity Manager 使用者應用程式驅動程式

除了支援提供資源的一般使用者申請之外，**Identity Manager** 還可讓您啓始提供申請，以回應在 **eDirectory** 中發生的事件。**Identity Manager** 的「使用者應用程式驅動程式」會監聽事件，並藉由啓始對應的提供申請進行回應。之後，這些申請可能會啓始工作流程來處理核准程序。例如，如果設定為執行此動作，則 **Identity Manager** 將支援下列情況：在 **eDirectory** 中新增使用者會自動執行預先指定的提供申請和工作流程。

提供系統

「提供系統」會執行啓始和完成提供申請所需的所有處理。如果申請需要一或多個核准，則「提供系統」隨後會呼叫「工作流程」系統，以啓動工作流程程序。提供必要的核准之後，「提供系統」就會供應申請的資源。

「提供系統」會維護在身份儲存區 (**eDirectory**) 中可用而未解決之提供申請的相關資訊。

若要啓始申請或執行完成申請所需的處理，系統會透過「目錄抽象層」來存取身份儲存區。

如需「目錄抽象層」的詳細資料，請參閱第 4 章「設定目錄抽象層的組態」，第 65 頁。

工作流程系統

當提供申請需要一或多個核准時，「工作流程系統」會協調核准程序。在處理的過程中，它會與下列元件互動：

- ◆ 工作流程資料庫
- ◆ 指令碼引擎
- ◆ Audit
- ◆ SMTP
- ◆ 安全性系統

工作流程資料庫

爲了追蹤進行中的工作流程狀態，「工作流程系統」會將資訊儲存在資料庫中。此資料庫會維護工作流程程序例項、工作清單(佇列)和工作流程收件人的相關資訊。此外，它還會儲存在執行工作流程程序期間新增的任何備註。

指令碼引擎

每當工作流程包含必須評估的動態運算式時，「工作流程系統」就會呼叫「指令碼引擎」。動態運算式可以包含變數、函數和運算子，以及「目錄抽象層」中實體的參考。

Novell Audit

若要記錄工作流程程序狀態的相關資訊，「工作流程系統」會與 **Novell Audit** 互動。在處理過程中，工作流程可能會記錄已發生之各種事件的相關資訊。然後，使用者可以使用 **Novell Audit** 報告工具來查看記錄資料。

如需設定記錄的詳細資料，請參閱第 5 章「設定記錄」，第 105 頁。如需控制想要 Identity Manager 使用者應用程式產生之記錄訊息層級的詳細資料，請參閱第 12 章「記錄組態」，第 191 頁。

SMTP

工作流程程序經常會在執行過程中的不同時機傳送電子郵件通知。例如，當使用者將工作流程活動指定給新收件人時，可能就會傳送電子郵件。

管理員可以在 iManager 中編輯電子郵件範本，然後將此範本用於工作流程程序中。在執行時期，「工作流程系統」會從 eDirectory 中取回它，並以適用於通知的動態文字取代標籤。

電子郵件通知透過「簡易郵件傳輸協定 (Simple Mail Transfer Protocol, SMTP)」進行處理。

如需電子郵件通知所需的基本設定步驟，請參閱「設定電子郵件伺服器的組態」，第 321 頁和「使用已安裝的電子郵件範本」，第 322 頁。如需設定工作流程之電子郵件通知組態的詳細資料，請參閱「設定工作流程活動的組態」，第 303 頁。

安全性

「安全性」系統會處理工作流程提供應用程式之安全性的所有方面。

如需工作流程安全性的相關資訊，請參閱「提供安全性」，第 287 頁。

21.1.2 提供和工作流程範例

假設使用者在 IT 系統上需要帳戶。若要設定帳戶，使用者會透過 Identity Manager 使用者應用程式啓始申請。此申請會啓動工作流程，以協調核准程序。在授予必要的核准之後，便會完成申請。在此程序中有三個基本步驟，概述如下。

步驟 1：啓始申請

在 Identity Manager 使用者應用程式中，使用者會依類別瀏覽資源清單，並選取要提供的一種資源。在身份儲存區中，選取的提供資源與提供申請定義相關聯。提供申請定義是提供系統中最重要物件。它將提供資源結合至工作流程，並做為工作流程程序向一般使用者公開的方法。提供申請定義會提供所有必要的資訊，以向使用者顯示啓始申請表單，並啓動啓始申請之後的流程。

在此範例中，使用者會選取「新帳戶」資源。當使用者啓始申請時，Web 應用程式會從「提供系統」（從提供申請定義取得這些物件）取回啓始申請表單，以及相關聯之啓始申請資料的描述。

啓始提供申請時，「提供系統」會追蹤啓始者與收件者。啓始者是建立申請的人員。而收件者又是為之建立申請的人員。在某些情況下，啓始者和收件者可能是相同的人員。

每個提供申請都具有與其相關聯的操作。該操作指定使用者是要授予還是要撤銷資源。

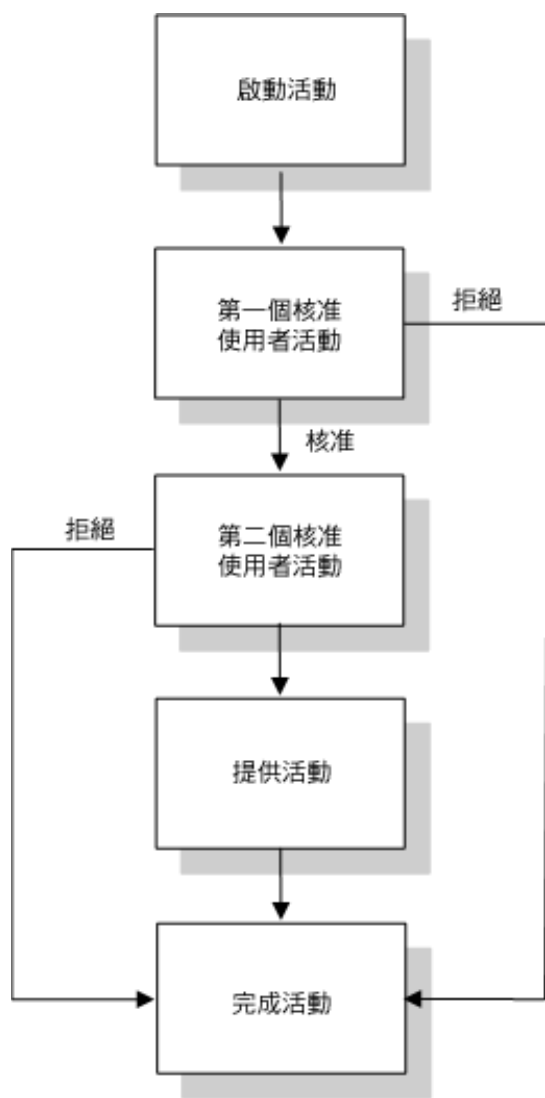
步驟 2：核准申請

在使用者啓始申請之後，「提供系統」會啓動工作流程程序。工作流程程序會協調核准。在此範例中，需要兩個層級的核准，一個來自於使用者的管理員，而另一個來自於管理員的監督者。如果工作流程中的任何使用者拒絕核准，則流程都會終止且申請會被拒。

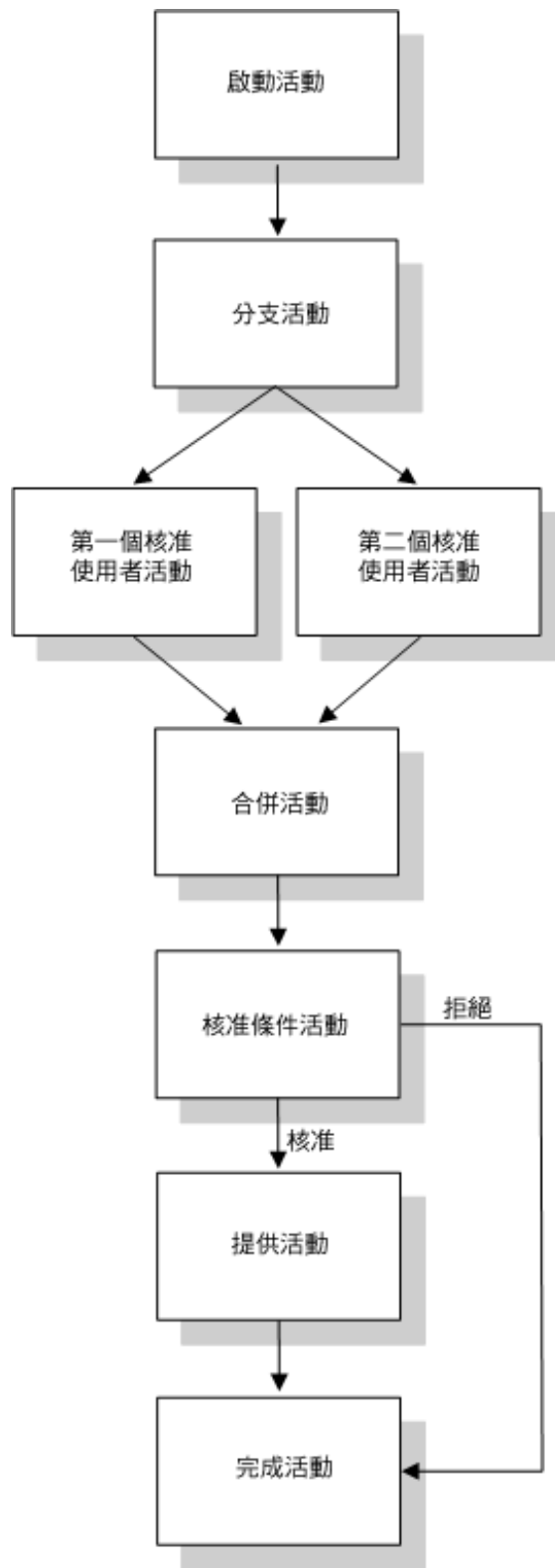
附註：Identity Manager 隨附一組提供申請範本，最高可支援五個層級的工作流程核准。在 Identity Manager 的後續版本中，基於 Eclipse 之設計環境提供的工具可讓您建立自己的自定工作流程程序。如需此版次隨附之範本的相關資訊，請參閱「[使用已安裝的範本](#)」，第 291 頁。

工作流程可以循序方式或平行方式來處理核准。在循序工作流程中，必須先處理目前的核准任務，然後才能開始下一個核准任務。在平行工作流程中，使用者可以同時處理核准任務。

循序流程 下列為具有兩個核准之循序工作流程的基本設計模式：



平行流程 下列為具有兩個核准之平行工作流程的基本設計模式：



附註：您可以輕鬆變更顯示標籤（「第一個」核准、「第二個」核准等）來滿足應用程式要求。針對平行流程，建議您指定不表示循序處理的標籤。例如，建議您指定像是「平行核准三段之一」、「平行核准三段之二」等等的標籤。

工作流程定義由下列元件組成

程序元件	描述
活動	<p>活動是代表任務的物件。活動可以向使用者呈現資訊，並回應使用者互動，或執行使用者看不見的背景函數。</p> <p>在上面顯示的工作流程範例中，活動以方塊表示。</p> <p>在 Identity Manager 使用者應用程式中，處理核准程序的使用者活動稱為任務。一般使用者可以藉由按一下動作群組「我的工作」中的「我的任務」，查看其佇列中的任務清單。若要查看已針對特定任務處理的工作流程活動，使用者可以選取任務，並按一下「任務詳細資料」表單上的「檢視備註歷程」按鈕。</p> <p>若要查看已針對特定提供申請處理的工作流程活動，使用者可以按一下「我的申請」，選取申請，然後按一下「申請詳細資料」表單上的「檢視備註與流程歷程」按鈕。</p> <p>如需「我的任務」和「我的申請」動作的相關資訊，請參閱《Identity Manager 使用者應用程式：使用者指南》。</p>
連結	<p>連結是將工作流程中的活動結合在一起的項目。連結代表在兩個活動之間所遵循的路徑。</p> <p>活動可以具有多個內送連結和多個外送連結。當活動具有多個外送連結時，選取的連結視活動的結果而定。該結果是活動執行之處理的最終結果。例如，「使用者」活動可能具有已核准或被拒的結果，根據使用者採取的動作而定。</p> <p>在上面顯示的工作流程範例中，連結以箭頭代表。</p>

啟動活動 工作流程序以執行啟動活動開始。此活動會使用啓始申請資料啓始化工作文件。它也會結合數個系統值（例如啓始者和接收者），以便可以將這些系統值用於程序檔運算式中。

使用者活動「啟動」活動執行完成之後，「工作流程系統」會將處理轉遞至流程中的第一個「使用者」活動。「使用者」活動是支援使用者互動的活動。若要處理這些互動，活動會顯示表單，以讓使用者處理申請。在上面顯示的工作流程範例中，「第一個」核准和「第二個」核准是「使用者」活動的範例。可以當地語系化「使用者」活動的顯示標籤，以滿足國際要求。

「使用者」活動可以支援下列一或多個動作：

- ◆ 要求
- ◆ 核准
- ◆ 拒絕 (Deny)
- ◆ 拒絕 (Refuse)
- ◆ 重新指定（僅限「組織管理員」和「使用者應用程式管理員」使用）

附註：表單上的欄位和按鈕會根據所申請之資源和設定工作流程組態之方式而定。例如，產品隨附的許多範本都不支援拒絕 (*Refuse*) 動作。

「使用者」活動具有五個可能的結果：

- ◆ 已核准
- ◆ 被拒 (Denied)
- ◆ 被拒 (Refused)
- ◆ 錯誤
- ◆ 逾時

附註：如果使用者未採取任何動作，則可能會發生「錯誤」和「逾時」結果。

如果使用者核准申請，則工作流程會將控制轉遞至流程中的下一個活動。如果無需任何的進一步核准，則會提供資源。如果使用者拒絕申請，則工作項目會轉遞給工作流程中的下一個活動，且申請會被拒。或者，使用者可以重新指定任務（如果該使用者是「組織管理員」或「使用者應用程式管理員」），這會將工作項目置於另一個使用者的佇列中。

附註：已設定產品隨附之提供申請範本的組態，以在申請被拒時終止工作流程程序。在申請被拒時，工作項目會轉遞給「完成」活動，以終止流程。

已被指定「使用者」活動的使用者稱為收件人。活動的收件人可能會透過電子郵件得到指定的任務通知。若要執行與活動相關聯的工作，收件人可以按一下電子郵件中的 URL，在工作清單（佇列）中找到任務，然後要求該任務。

收件人必須在指定的一段時間內回應「使用者」活動，否則該活動會逾時。一般而言，逾時間隔以小時或天為單位表示，以允許使用者有足夠的時間來回應。

當活動逾時時，工作流程程序可能會嘗試重新完成活動，根據針對活動指定的重試計數而定。在某些情況下，可能會設定工作流程程序的組態，以將已逾時的活動提升到另一個使用者。在此情況下，要將活動重新指定給新的收件人（例如，使用者的管理員），讓這位使用者有機會完成活動的工作。如果上次重試逾時，則該活動會標示為已核准或被拒，根據設定工作流程組態的方式而定。

條件式活動 在執行的過程中，工作流程程序可能會執行測試，並檢查結果，以查看下一步的操作。「條件式」活動提供此功能。「條件式」活動會使用指令碼運算式，來定義要評估的條件。在上面顯示的工作流程範例中，「核准條件」是「條件式」活動的範例。

「條件式」活動支援三個可能的結果：

- ◆ True
- ◆ False
- ◆ 錯誤

分支和合併活動 在支援平行處理的工作流程中，「分支」活動可讓兩個使用者平行處理工作項目的不同區域。在使用者完成工作之後，「合併」活動會同步化流程中的內送分支。

提供活動 「提供」活動會完成提供申請。僅當所有必要的核准都提供時，才會執行此活動。

如需提供步驟的詳細資料，請參閱「[步驟 3：完成申請](#)」，第 287 頁。

完成活動「完成」活動是工作流程中的最後一個活動。當流程中的所有活動都已完成，且流程的最終結果可用時，才可以執行「完成」活動。「工作流程系統」可以藉由檢查「完成」活動的連結，判定程序的最終狀態。整體流程狀態在核准連結到達「完成」活動時為「已核准」。如果任何其他結果（拒絕、逾時或錯誤）導致「完成」活動，則整體流程狀態為「被拒」。

當工作流程程序到達「完成」活動，且狀態為已核准時，則核准程序完成，且提供申請可以完成。

步驟 3：完成申請

當已核准提供申請時，「工作流程系統」可以開始提供步驟。此時，控制會傳遞回到「提供系統」。

為了完成提供申請，「提供系統」可能會執行 Identity Manager 授權，或者直接處理 eDirectory 物件和它的屬性。在提供步驟期間，它會建立所有相關的物件，並且在收件者上記錄提供動作的結果，如提供資料定義中所述。根據使用者是否申請授權或撤銷操作而定，這可能會涉及設定或移除收件者上屬性的值，或者新增或移除收件者上多值屬性的項目。涉及的屬性是 eDirectory 屬性（可能藉由將輔助類別新增至收件者以使其可用）。屬性值本身可能會很簡易，或者可能會是允許「提供系統」指定內部子屬性值的複雜類型。

21.2 提供組態和管理

若要設定提供申請定義的組態，請使用 iManager 將其結合到提供的資源，指定相關工作流程的執行時期特性，然後啓用它以供使用。Identity Manager 會隨附一組預先部署的提供申請定義和工作流程。您可以將這些做為範本使用，以建立您自己的提供系統。安裝的範本易於使用，並且還很靈活，可以滿足多種業務環境的要求。若要設定您的系統，可根據已安裝的範本定義新物件，並且自定這些物件以符合組織的需求。

在設定提供申請定義的組態之後，您可以使用 iManager 來檢視執行中工作流程程序的狀態，重新指定工作流程內的活動，或者在工作流程阻塞時終止該工作流程。

如需將 iManager 用於提供組態和管理的相關資訊，請參閱第 22 章「設定提供申請定義的組態」，第 291 頁和第 23 章「管理提供工作流程」，第 313 頁。

21.3 提供安全性

當使用者登入 Identity Manager 使用者應用程式時，「安全性」系統會驗證該使用者，並且設定存取控制以防止未經授權使用提供和工作流程物件。這會確保使用者僅可以查看已授予存取權限的那些提供申請定義。除了針對使用者應用程式執行驗證和授權服務之外，「安全性」系統還會管理代理和委託指定。

- ◆ 委託是獲得授權以執行其他使用者之工作的使用者。委託指定適用於特定提供申請定義。
- ◆ 代理是獲得授權以執行一或多個使用者、群組或容器之任一或所有工作的使用者。與委託指定不同，代理指定不相依於提供申請定義，因此適用於所有工作和設定。

如果已啓用記錄，則會記錄代理或委託所採取的所有動作，以及其他使用者所採取的動作。當代理或委託採取動作時，記錄訊息會清楚地指出該動作是由其他使用者的代理或委託所執行。此外，每次定義新的代理或委託指定時，同樣會記錄此事件。

如果提供申請定義已設為產生電子郵件通知，則代理和收件人會收到電子郵件通知。委託不會收到電子郵件通知。

工作流程安全性角色「安全性」系統會辨識下列安全性角色：

角色	描述	權限
使用者應用程式管理員	具有完整管理權限的 locksmith 使用者。	<p>「使用者應用程式管理員」允許在 iManager 中執行這些任務：</p> <ul style="list-style-type: none"> ◆ 設定提供申請的組態 ◆ 管理已處於程序中的工作流程 <p>「使用者應用程式管理員」允許在使用者應用程式內執行這些任務：</p> <ul style="list-style-type: none"> ◆ 檢視與編輯所有工作流程佇列中的所有任務。 ◆ 定義系統中任何使用者的代理和委託指定。 ◆ 檢視系統中任何使用者的隱藏資訊 (隱藏的屬性)。 ◆ 建立「任務群組管理員」, 並且將它們指定給群組。「使用者應用程式管理員」是唯一可以建立並指定「任務群組管理員」的使用者。
		<p>附註：Identity Manager 使用者應用程式的「管理」索引標籤會提供工具, 以指定管理使用者應用程式的權限。若要使用此索引標籤, 您必須先以安裝期間被指定為「使用者應用程式管理員」的使用者身份登入。</p>
組織管理員	<p>員工的直接報告監督者。每個使用者僅具有一個「組織管理員」。</p> <hr/> <p>提示：「組織管理員」還可以視為行政管理者。</p>	<p>「組織管理員」允許：</p> <ul style="list-style-type: none"> ◆ 檢視他 / 她小組工作流程佇列中的所有任務。此功能適用於管理階層中的單一層級, 因此, 「組織管理員」監督者無法查看「組織管理員」直接報告的任務。 ◆ 編輯直接報告的任務, 但是以下情況例外：當直接報告中的任務指定給某群組, 但該群組的「任務群組管理員」不是「組織管理員」。在此情況下, 「組織管理員」可以檢視任務, 但不可以執行任何編輯。擴大時, 任務會移至「任務群組管理員」, 而不是「組織管理員」。 ◆ 要求任務和未要求任務, 以及將任務重新指定給他 / 她的小組成員。 ◆ 定義他或她自己, 以及他 / 她的小組成員的代理和委託關係。 ◆ 檢視他 / 她小組成員的隱藏屬性。

角色	描述	權限
任務群組管理員	<p>被授予任務群組相關任務職責的使用者。任務群組是「LDAP 群組」物件的延伸。每個任務群組僅可以具有一個「任務群組管理員」。</p> <p>「任務群組管理員」由「使用者應用程式管理員」指定。</p> <p>當任務指定給群組時，群組的 srvprvTaskManager 屬性會包含使用者 (指定的「任務群組管理員」) 的 DN。針對改進的效能，使用者物件上的屬性也會識別「任務群組管理員」。srvprvIsTaskManager 屬性會針對指定的「任務群組管理員」使用者設為 true。</p>	<p>「任務群組管理員」允許：</p> <ul style="list-style-type: none"> ◆ 檢視與編輯指定給群組 (他 / 她是該群組的指定領導) 的所有任務。 <p>「任務群組管理員」不允許：</p> <ul style="list-style-type: none"> ◆ 建立資源或收回申請。 ◆ 定義代理或委託關係。 ◆ 檢視他 / 她小組成員的隱藏屬性。

附註：所有使用者都可以檢視與自己身份相關的隱藏屬性。

定義代理和委託關係 若要定義使用者的代理指定，請使用 Identity Manager 使用者介面之「申請與核准」索引標籤上的「小組代理指定」頁。若要定義使用者的委託指定，請使用在「申請與核准」索引標籤上也可用的「小組委託指定」頁。

建立任務群組管理員 若要定義任務群組的「任務群組管理員」，請使用 Identity Manager 使用者介面之「身份自助服務」索引標籤上的「建立使用者或群組」頁。

如需定義「任務群組管理員」、代理和委託的完整詳細資料，請參閱《Identity Manager 使用者應用程式：使用者指南》。

設定提供申請定義的組態

本章提供設定提供申請定義之組態的指示。主題包含：

- ◆ 「關於提供申請組態外掛程式」，第 291 頁
- ◆ 「使用已安裝的範本」，第 291 頁
- ◆ 「設定提供申請定義的組態」，第 294 頁

22.1 關於提供申請組態外掛程式

若要設定提供申請定義的組態，您需要使用 iManager 的「提供申請組態」外掛程式。此外掛程式可讓您將提供申請定義結合到提供的資源，指定相關工作流程的執行時期特性，以及啓用它以供使用。在本版本中，提供的資源會映射到 Identity Manager 授權。

附註：您還可以執行直接映射至身份儲存區中屬性的提供申請定義。然而，因為安裝的範本基於授權，所以它們不支援此類型的資源。

您可以在 iManager 的 *Identity Manager* 類別中尋找「提供申請組態」外掛程式。外掛程式會在「提供申請組態」角色中包含「提供申請」任務。「提供申請」任務由這些面板組成：

面板	描述
提供驅動程式選取	提供您選取 Identity Manager 使用者應用程式驅動程式的機會。驅動程式包含一組預先部署的提供申請定義，所以您需要在開始設定提供申請組態之前選擇驅動程式。
提供申請組態	提供的工具可讓您： <ul style="list-style-type: none"> ◆ 瀏覽可用的提供申請定義，並且選擇一個以設定組態 ◆ 根據現有的定義建立新的提供申請定義 ◆ 設定提供申請定義的內容 ◆ 將提供申請定義指定至提供的資源 ◆ 針對相關聯工作流程中的每個活動，編輯收件人和逾時設定 當選擇建立新的提供申請或編輯現有的提供申請時，外掛程式會執行「提供申請組態精靈」。

22.2 使用已安裝的範本

Identity Manager 會隨附一組預先部署的提供申請定義和工作流程。您可以使用它們做為範本，以建立您自己的提供系統。若要設定您的系統，可根據已安裝的範本定義新物件，並且自定這些物件以符合組織的需求。

已安裝的範本可讓您判定要完成之申請需要的核准步驟數目。您可以設定提供申請的組態，它需要：

- ◆ 無核准

- ◆ 一個核准步驟
- ◆ 兩個核准步驟
- ◆ 三個核准步驟
- ◆ 四個核准步驟
- ◆ 五個核准步驟

您還可以指定想要支援循序處理還是平行處理，以及如果在處理期間工作流程逾時，想要核准還是拒絕申請。

如需工作流程設計模式的相關資訊，請參閱「[提供和工作流程範例](#)」，第 282 頁。

Identity Manager 會隨附下列範本：

範本	描述
自行提供核准	允許完成提供申請，而無任何核准。
一個步驟核准 (逾時核准)	需要單一核准，以完成提供申請。如果活動逾時，則活動會核准申請，並且工作項目會轉遞到下一個活動。
兩個步驟循序核准 (逾時核准)	需要兩個核准，以完成提供申請。如果活動逾時，則活動會核准申請，並且工作項目會轉遞到下一個活動。 此範本支援循序處理。
三個步驟循序核准 (逾時核准)	需要三個核准，以完成提供申請。如果活動逾時，則活動會核准申請，並且工作項目會轉遞到下一個活動。 此範本支援循序處理。
四個步驟循序核准 (逾時核准)	需要四個核准，以完成提供申請。如果活動逾時，則活動會核准申請，並且工作項目會轉遞到下一個活動。 此範本支援循序處理。
五個步驟循序核准 (逾時核准)	需要五個核准，以完成提供申請。如果活動逾時，則活動會核准申請，並且工作項目會轉遞到下一個活動。 此範本支援循序處理。
一個步驟核准 (逾時拒絕)	需要單一核准，以完成提供申請。如果活動逾時，則工作流程會拒絕申請。 此範本支援循序處理。
兩個步驟循序核准 (逾時拒絕)	需要兩個核准，以完成提供申請。如果活動逾時，則工作流程會拒絕申請。 此範本支援循序處理。
三個步驟循序核准 (逾時拒絕)	需要三個核准，以完成提供申請。如果活動逾時，則工作流程會拒絕申請。 此範本支援循序處理。
四個步驟循序核准 (逾時拒絕)	需要四個核准，以完成提供申請。如果活動逾時，則工作流程會拒絕申請。 此範本支援循序處理。

範本	描述
五個步驟循序核准 (逾時拒絕)	需要五個核准，以完成提供申請。如果活動逾時，則工作流程會拒絕申請。 此範本支援循序處理。
兩個步驟平行核准 (逾時核准)	需要兩個核准，以完成提供申請。如果活動逾時，則活動會核准申請，並且工作項目會轉遞到下一個活動。 此範本支援平行處理。
三個步驟平行核准 (逾時核准)	需要三個核准，以完成提供申請。如果活動逾時，則活動會核准申請，並且工作項目會轉遞到下一個活動。 此範本支援平行處理。
四個步驟平行核准 (逾時核准)	需要四個核准，以完成提供申請。如果活動逾時，則活動會核准申請，並且工作項目會轉遞到下一個活動。 此範本支援平行處理。
五個步驟平行核准 (逾時核准)	需要五個核准，以完成提供申請。如果活動逾時，則活動會核准申請，並且工作項目會轉遞到下一個活動。 此範本支援平行處理。
兩個步驟平行核准 (逾時拒絕)	需要兩個核准，以完成提供申請。如果活動逾時，則工作流程會拒絕申請。 此範本支援平行處理。
三個步驟平行核准 (逾時拒絕)	需要三個核准，以完成提供申請。如果活動逾時，則工作流程會拒絕申請。 此範本支援平行處理。
四個步驟平行核准 (逾時拒絕)	需要四個核准，以完成提供申請。如果活動逾時，則工作流程會拒絕申請。 此範本支援平行處理。
五個步驟平行核准 (逾時拒絕)	需要五個核准，以完成提供申請。如果活動逾時，則工作流程會拒絕申請。 此範本支援平行處理。

工作流程和提供資源 每個提供申請定義都具有與提供資源和工作流程之預先設定組態的結合。您可以變更與申請定義相關的提供資源，但不可以變更工作流程或它的拓樸。

提供申請的類別 每個提供申請範本也都會結合至類別。類別會提供方便的方式，以組織一般使用者的提供申請。所有提供申請範本的預設類別是「授權」。類別鍵 (即 `srvprvCategoryKey` 屬性的值) 是 *entitlements* (小寫)。

您可以藉由使用目錄抽象層編輯器來建立您自己的類別。當建立新類別時，請確保類別鍵 (`srvprvCategoryKey` 的值) 是小寫。對於確保類別在 Identity Manager 使用者應用程式中正常工作而言，這是很必要的。

如需建立提供類別的詳細資料，請參閱「[使用清單](#)」，第 91 頁。

22.3 設定提供申請定義的組態

在設定提供申請定義的組態之前，您需要選取包含定義的 Identity Manager 使用者應用程式驅動程式。選取驅動程式之後，您可以建立新的提供申請定義，或者編輯現有的定義。您還可以刪除提供申請定義，變更申請定義的狀態，或者定義申請定義的權限。

22.3.1 選取驅動程式

若要選取 Identity Manager 使用者應用程式驅動程式，請執行下列動作：

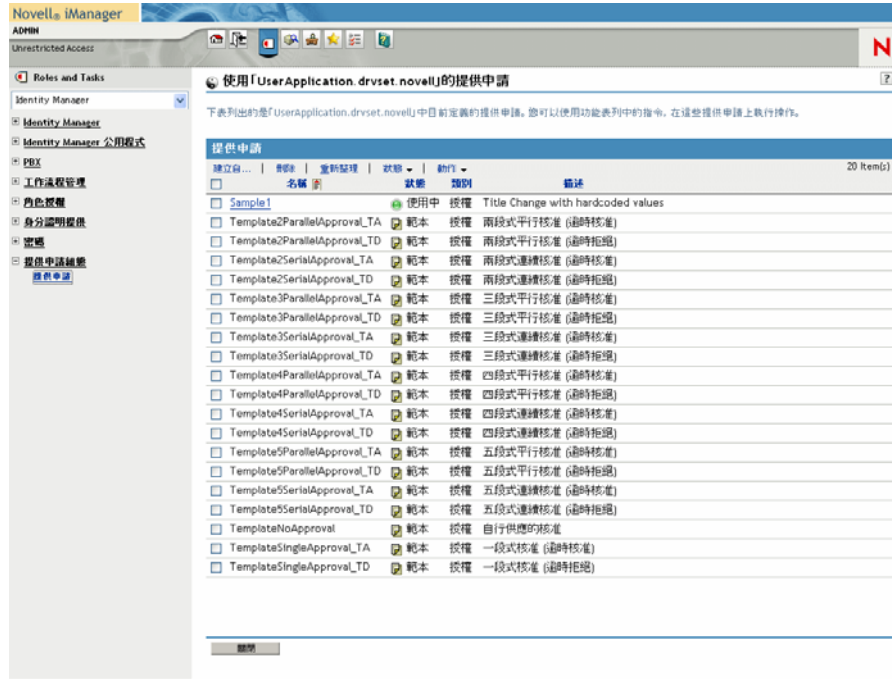
- 1 在 iManager 中選取「Identity Manager」類別。
- 2 開啓「提供申請組態」角色。
- 3 按一下「提供申請」任務。

iManager 即會顯示「使用者應用程式驅動程式」螢幕。



- 4 在「使用者應用程式驅動程式」欄位中指定驅動程式名稱，然後按一下「確定」。

iManager 即會顯示「提供申請組態」面板。「提供申請組態」面板會顯示可用提供申請定義的清單。



安裝的範本會顯示為深色文字，其狀態為範本。因為做為範本的申請定義是唯讀的，所以它們不會顯示超文件連結。

附註：如果申請定義的組態設為使用當地語系化的文字，則這些定義的名稱和描述會顯示符合目前地區設定的文字。

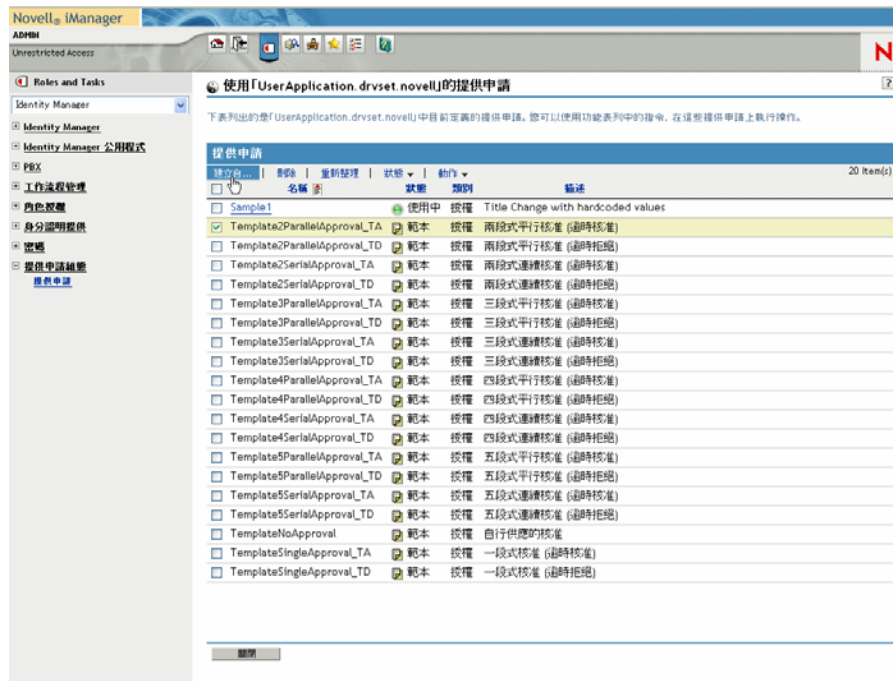
變更驅動程式 選取驅動程式之後，除非您選取新的驅動程式，否則驅動程式選項會在您的 iManager 會期期間一直起作用。若要選取新的驅動程式，請按一下「動作」指令，並從「動作」功能表中選擇「選取使用者應用程式驅動程式」。

22.3.2 建立或編輯提供申請

若要建立新的提供申請，請執行下列動作：

- 1 按一下「提供申請組態」面板中您要做為範本使用之提供申請的名稱。

2 按一下「提供申請組態」面板中的「建立自」指令。



「設定新提供申請的組態」精靈的第一個頁面即會顯示。



- 3 在「名稱」欄位中輸入新物件的公用名稱。
- 4 針對每種您要在應用程式中支援的語言，在「提供申請當地語系化字串」下的「顯示名稱」和「描述」欄位中輸入當地語系化的文字。此文字將用於識別使用者應用程式的提供申請。
- 5 若要將新語言新增至清單，請按一下「新增」，然後選取所需的語言。

附註：在預設狀態下，新建立的提供申請僅支援英文。

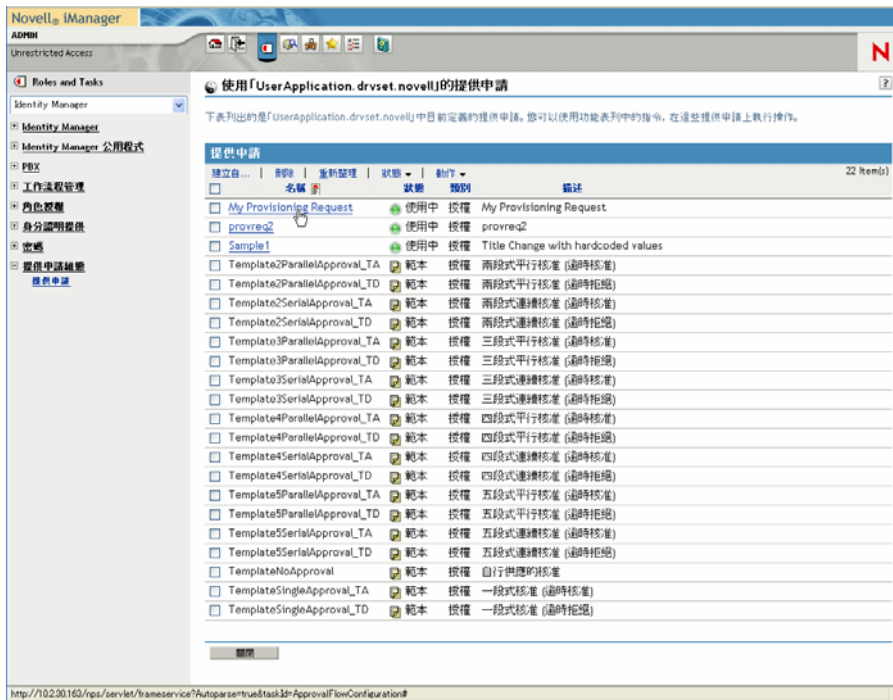
- 6 按「下一步」。
- 7 指定申請定義的提供資源，如「指定提供資源」，第 299 頁中所述。
- 8 設定與申請定義相關之工作流程的動作組態，如「設定工作流程活動的組態」，第 303 頁中所述。
- 9 指定申請定義的存取權限，如「指定提供申請的存取權限」，第 307 頁中所述。
- 10 指定申請定義的起始狀態，如「指定提供申請的啓始狀態」，第 307 頁中所述。

11 檢視您的設定，然後按一下「完成」。



若要編輯現有的提供申請，請執行下列動作：

1 按一下「提供申請組態」面板中提供申請的名稱。



您不允許編輯做為範本的提供申請。因為狀態為「範本」的申請定義是唯讀的，所以它們不會顯示超文件連結。

附註：如果您具有大量的申請定義，則可能要依特定欄（例如，「名稱」或「描述」）排序清單。若要依特定欄排序，只需按一下欄標題。

- 2 針對每種您要在應用程式中支援的語言，按一下「提供申請當地語系化字串」下清單中語言旁邊的核取方塊，然後在「顯示名稱」和「描述」欄位中輸入當地語系化的文字。此文字將用於識別使用者應用程式的提供申請。
- 3 若要將語言新增至清單，請按一下「新增」，並選取所需的語言。

附註：在預設狀態下，新建立的提供申請僅支援英文。

- 4 按「下一步」。
- 5 指定申請定義的提供資源，如「指定提供資源」，第 299 頁中所述。
- 6 設定與申請定義相關之工作流程的動作組態，如「設定工作流程活動的組態」，第 303 頁中所述。
- 7 指定申請定義的存取權限，如「指定提供申請的存取權限」，第 307 頁中所述。
- 8 指定申請定義的起始狀態，如「指定提供申請的啓始狀態」，第 307 頁中所述。
- 9 檢視您的設定，然後按一下「完成」。

指定提供資源

本節提供指定基於授權之提供資源的指示。它不會提供建立和使用授權之指示或授權的相關概念資訊。

如需授權的完整詳細資料，請參閱《<z-DocTitleInVariable>Novell Identity Manager：管理指南》。

若要指定提供資源，請執行下列動作：

- 1 若要使用目前與申請定義相關的目標，請選取「提供資源」選項圓鈕。

如果您正在編輯參考有效資源的申請定義，則預設會選取「提供資源」選項圓鈕。如果定義新的提供申請，則不會選取此選項圓鈕。

- 2 若要將申請定義結合到先前在目前選取之驅動程式內定義的另一個資源，則選取「可用的提供資源」選項圓鈕，然後從下拉式清單中選取目標。



附註：如果申請定義已結合到不是授權的資源，則您不允許變更資源。

- 3 選取「類別」下拉式清單中提供資源定義的類別。
類別預設為目前已選取之提供資源的類別。變更提供資源時，申請定義的類別也會變更，以符合資源的類別。如果想要將不同的類別指定給申請定義，則在「類別」下拉式清單中選取該類別。
- 4 若要根據 Identity Manager 授權建立新資源，請按一下「+」按鈕。



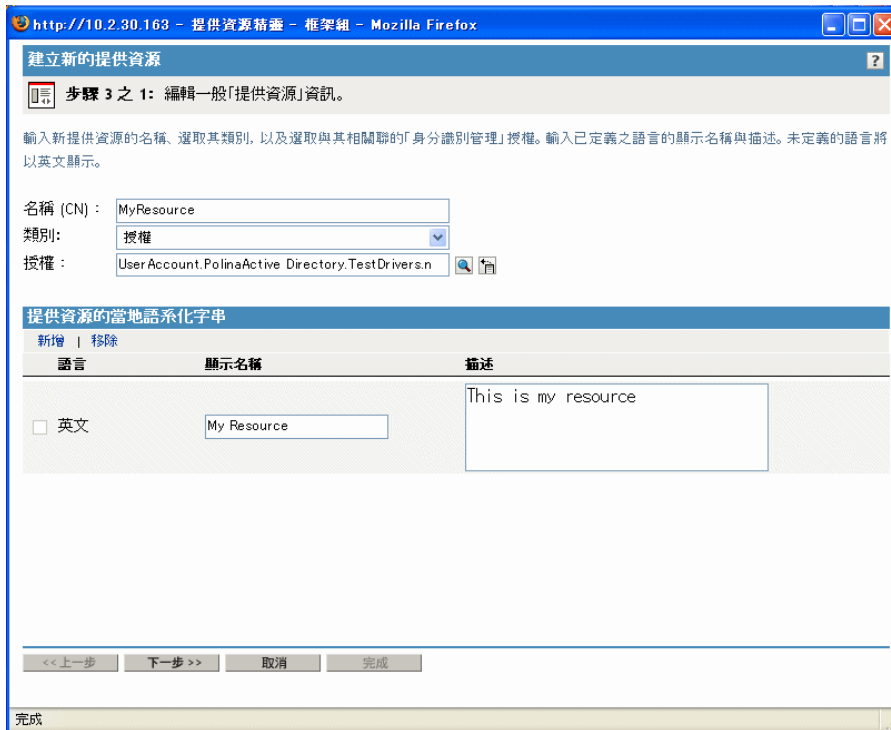
若要編輯現有的資源，則按一下畫筆按鈕。



若要定義資源的特性，請遵循下列步驟：

- 4a 在「名稱 (CN)」欄位中指定資源的名稱。
- 4b 在「類別」下拉式功能表中選取資源的類別。
- 4c 在「授權」欄位中指定授權。
- 4d 針對每種您要在應用程式中支援的語言，按一下「提供資源當地語系化字串」下拉清單中語言旁邊的核取方塊，然後在「顯示名稱」和「描述」欄位中輸入當地語系化的文字。此文字將用於識別使用者應用程式的提供資源。
- 4e 若要將語言新增至清單，請按一下「新增」，並選取所需的語言。

附註：在預設狀態下，新建立的提供資源僅支援英文。



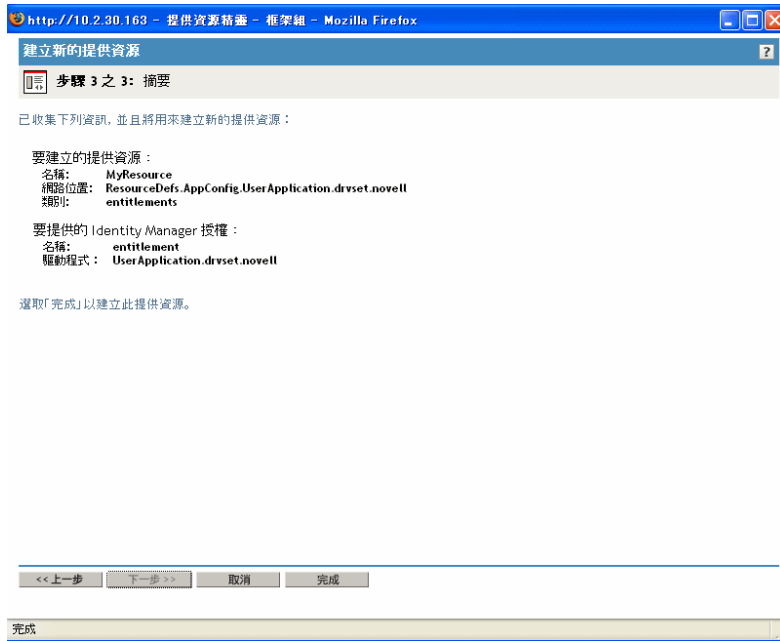
5 按「下一步」。

「提供資源」精靈即會顯示螢幕，以讓您提供授權所需之任何參數的資料。



6 如果授權不需要任何授權參數，請按「下一步」。

「建立新的提供資源」精靈會顯示「摘要」頁，它會提供您所定義之資源的相關資訊。



7 按一下「完成」。

設定工作流程活動的組態

若要設定相關工作流程之活動的組態，請執行下列動作：

- 1 藉由選取或不選「以電子郵件通知參與者」核取方塊，指定您是否想透過電子郵件通知每個活動的收件人。

http://10.2.30.163 - 提供申請組態精靈 - 框架組 - Mozilla Firefox

編輯現有的提供申請

步驟 6 之 3: 請提供設定提供申請的必要資料。

啟用或停用電子郵件通知，定義提供申請內每項活動的收件人、逾時及重試資訊。逾時指的是分配給收件人執行活動的一段時間。

以電子郵件通知參與者

第一次核准

收件人：

運算式： 收件者 管理员

DN: (例如 CN=Admin, O=Novell)

逾時： 48 小時 (沒有值：使用系統預設值)

重試：

嘗試次數： 3 (沒有值：沒有項目)

收件人：

運算式： 「第一次核准」的收件人 管理员

DN: (例如 CN=Admin, O=Novell)

<< 上一步 下一步 >> 取消 完成

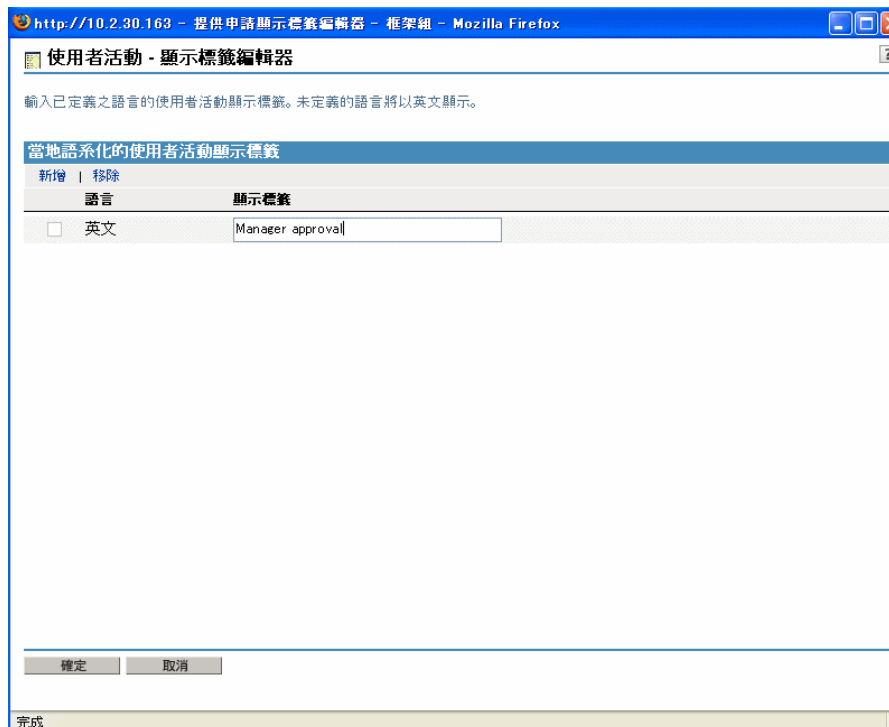
完成

附註：如果您選取「以電子郵件通知參與者」核取方塊，且收件人已指定代理，則電子郵件也會通知該代理。委託不會收到電子郵件通知。

- 2 針對每個工作流程活動，藉由按一下活動（在此情況下，為「第一個核准」）名稱旁邊的圖示，選擇性地變更顯示標籤。



在「顯示標籤」欄位中輸入顯示標籤，並按一下「確定」。



附註：預設的顯示標籤（「第一個」核准、「第二個」核准等）表示會循序處理核准。針對平行流程，建議您指定不表示循序處理的標籤。例如，建議您指定像是「平行核准三段之一」、「平行核准三段之二」等等的標籤。

3 針對每個工作流程活動，也會提供下列資訊：

欄位	描述
收件人運算式	<p>指定識別活動之收件人的動態運算式。該收件人是根據評估運算式的方式在執行時期決定的。</p> <p>收件人運算式的第一個詞彙可以是下列其中任何一個值：</p> <ul style="list-style-type: none">◆ Initiator◆ Recipient◆ Addressee of <i>activity-name</i> <p>工作流程中每個活動（除了您目前設定組態的活動之外）的「運算式」下拉式功能表中會列出單獨的 Addressee of <i>activity-name</i> 詞彙。<i>activity-name</i> 是為活動指定的顯示標籤，或是預設名稱（如果您未指定顯示標籤）。</p> <p>收件人運算式的第二個詞彙可以是下列其中任何一個值：</p> <ul style="list-style-type: none">◆ Manager◆ <No attribute> <hr/> <p>附註：因為 Manager 屬性之前已經在抽象層中的「使用者」實體上定義，所以它自動可供使用。如果其他屬性（除了 Manager 之外）滿足下列要求，則可以選擇它們：</p> <ul style="list-style-type: none">◆ 必須在抽象層中的「使用者」實體上定義◆ 必須是單一值◆ 必須具有 DN 資料類型
收件人 DN	<p>指定使用者、群組或任務群組的可辨識名稱。</p> <hr/> <p>附註：如果想要「任務群組管理員」可以依任務群組（在使用者應用程式的「我的小組任務」動作中）搜尋任務，則您需要將任務群組指定為收件人。</p> <hr/>
逾時	<p>指定分配給收件人完成任務的時間期間。每次收件人執行活動時，都會套用逾時間隔。</p> <p>指定以秒、分鐘、小時或天為單位的值。</p>

欄位	描述
重試收件人運算式	<p>指定在已達到逾時限制的情況下，識別應該取得此任務之使用者的動態運算式。</p> <p>重試收件人是根據評估運算式的方式在執行時期決定的。</p> <p>收件人運算式的第一個詞彙可以是下列其中任何一個值：</p> <ul style="list-style-type: none"> ◆ approval.getAddressee() ◆ Initiator ◆ Recipient ◆ Addressee of <i>activity-name</i> <p>approval.getAddressee() 選項會取得目前的收件人。</p> <p>工作流程中每個活動 (除了您目前設定組態的活動之外) 的「運算式」下拉式功能表中會列出單獨的 Addressee of <i>activity-name</i> 詞彙。<i>activity-name</i> 是為活動指定的顯示標籤，或是預設名稱 (如果您未指定顯示標籤)。</p> <p>收件人運算式的第二個詞彙可以是下列其中任何一個值：</p> <ul style="list-style-type: none"> ◆ Manager ◆ <No attribute> <hr/> <p>附註：因為 Manager 屬性之前已經在抽象層中的「使用者」實體上定義，所以它自動可供使用。如果其他屬性 (除了 Manager 之外) 滿足下列要求，則可以選擇它們：</p> <ul style="list-style-type: none"> ◆ 必須在抽象層中的「使用者」實體上定義 ◆ 必須是單一值 ◆ 必須具有 DN 資料類型
重試次數	<p>指定在逾時的情況下重試活動的次數。</p> <p>當活動逾時時，根據為活動指定的重試計數而定，工作流程程序可能會嘗試重新完成活動。在每次重試時，工作流程程序都可能將活動提升到另一個使用者。在此情況下，活動會重新指定給另一個收件人 (例如，使用者的管理員)，以讓此使用者有機會完成活動的工作。如果上次重試逾時，根據設定工作流程組態的方式而定，該活動會標示為已核准或被拒。</p>
重試收件人 DN	<p>指定在已達到重試限制的情況下，應該取得此任務之使用者或群組的可辨識名稱。</p>

4 當您完成設定活動的組態時，需要向下捲動以查看流程的其他活動。

5 按「下一步」。

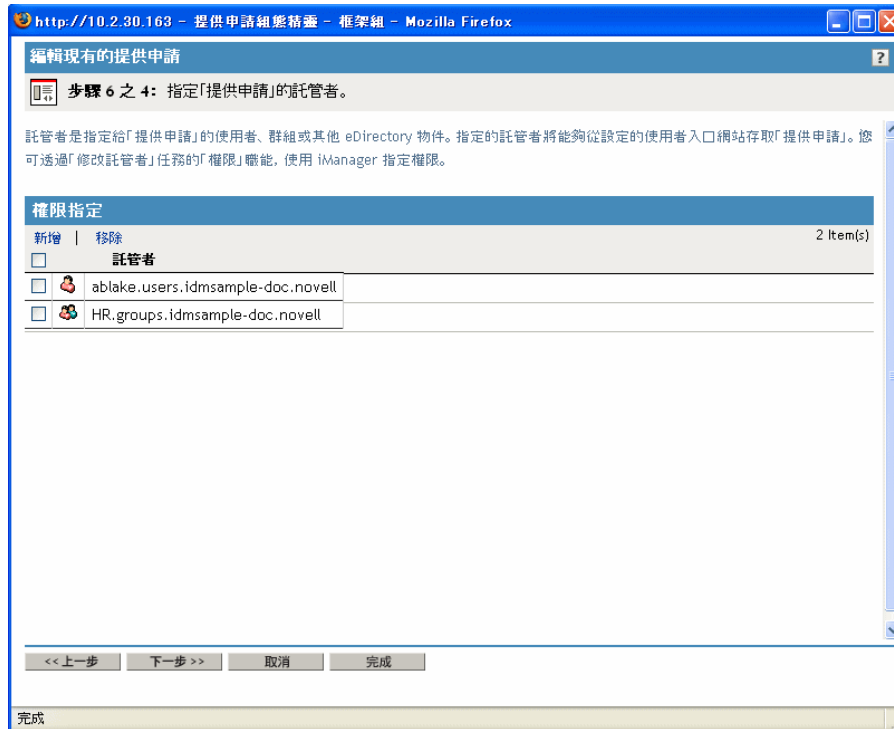
附註：根據結合至申請定義的工作流程範本而定，您可以設定組態的活動數目會不同。根據與申請相關聯的提供資源而定，授權參數的數目和類型會不同。

指定提供申請的存取權限

若要指定提供申請的存取權限，請執行下列動作：

- 1 若要將使用者、群組或其他 eDirectory 物件新增至此申請定義的託管者清單，請按一下「新增」，並選取物件。

在您新增物件之後，它會包含在託管者清單中。



- 2 若要移除使用者、群組或其他物件，請選取「託管者」清單中的項目，然後按一下「移除」。
- 3 按「下一步」。

指定提供申請的啓始狀態

若要設定提供申請的啓始狀態，請執行下列動作：

- 1 按一下想要之狀態的選項圓鈕：

狀態	描述
使用中	可供使用。
未啓用	暫時無法使用。此為預設。
已淘汰	永久停用。



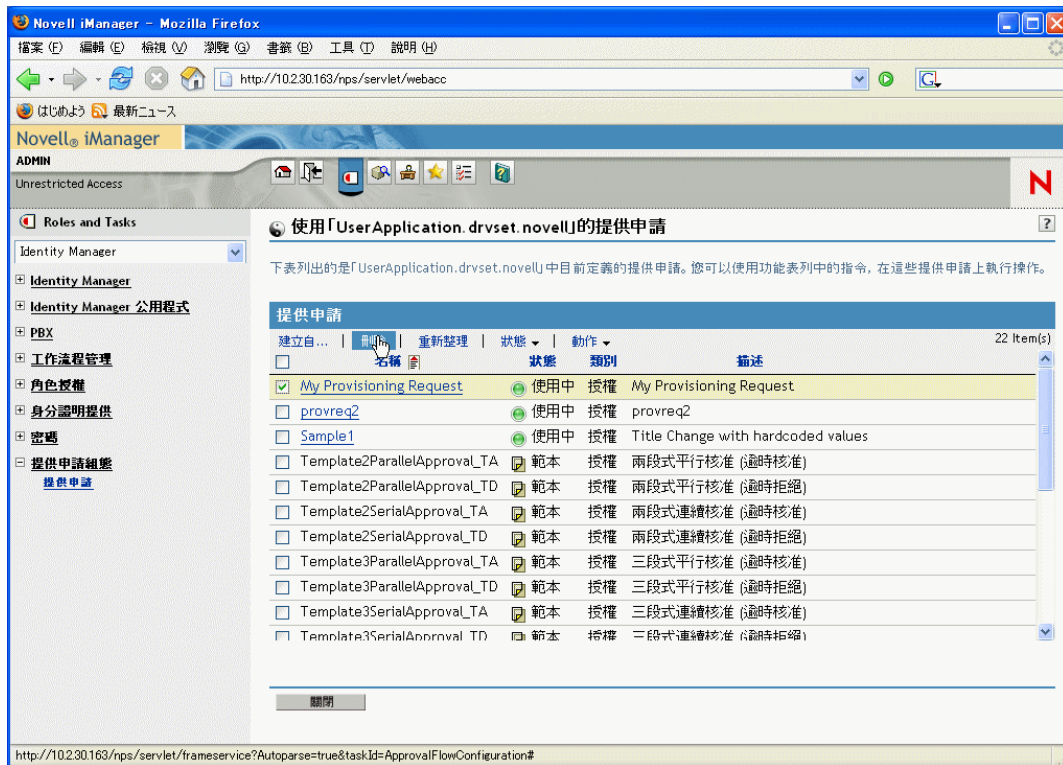
- 2 按一下正確動作（「授予」或「撤銷」）的選項圓鈕。
- 3 按「下一步」。

22.3.3 刪除提供申請

若要刪除提供申請，請執行下列動作：

- 1 藉由按一下名稱旁邊的核取方塊，選取您要刪除的提供申請。
您不允許刪除做為範本的提供申請。

2 按一下「提供申請組態」面板中的「刪除」指令。

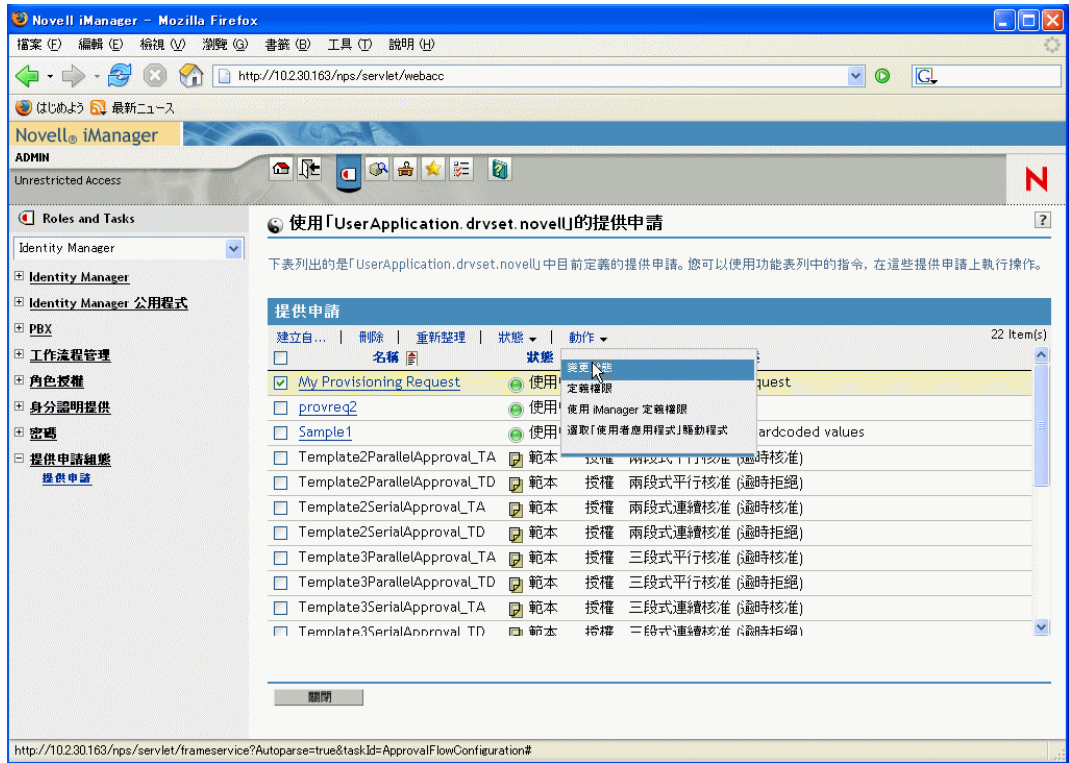


22.3.4 變更現有提供申請的狀態

若要變更現有提供申請的狀態，請執行下列動作：

1 藉由按一下名稱旁邊的核取方塊，選取您想要變更其狀態的提供申請。

2 按一下「提供申請組態」面板中的「變更狀態」指令。



3 按一下「狀態」功能表中的狀態：

狀態	描述
使用中	可供使用。
未啓用	暫時無法使用。
已淘汰	永久停用。

4 按一下正確動作（「授予」或「撤銷」）的選項圓鈕。

5 按一下「完成」。

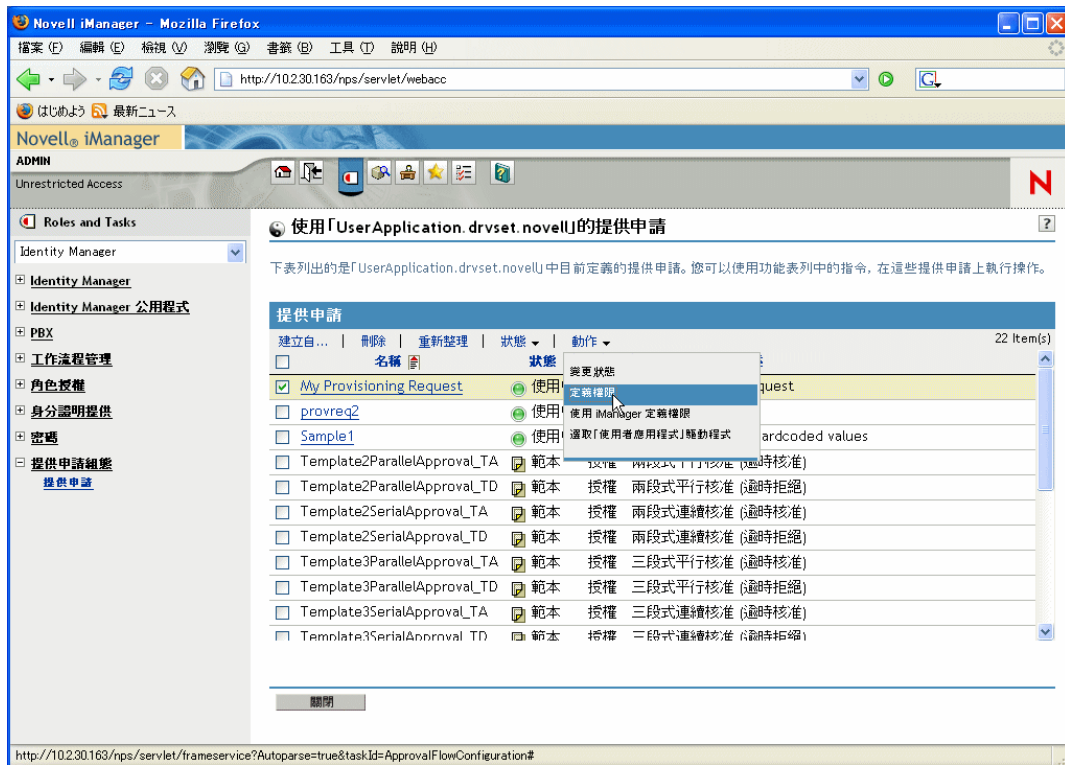
22.3.5 定義現有提供申請的權限

若要定義現有提供申請的權限，請執行下列動作：

1 藉由按一下名稱旁邊的核取方塊，選取您定義其權限的提供申請。

2 按一下「提供申請組態」面板中的「動作」指令。

3 按一下「動作」功能表上的「定義權限」指令。



4 遵循在「指定提供申請的存取權限」，第 307 頁下給出的步驟。

若要使用 iManager 定義提供申請的權限，請執行下列動作：

- 1 藉由按一下名稱旁邊的核取方塊，選取您想要定義其權限的提供申請。
- 2 按一下「提供申請組態」面板中的「動作」指令。
- 3 按一下「動作」功能表上的「使用 iManager 定義權限」指令。

管理提供工作流程

本章提供在執行時期管理提供工作流程的指示，並會提供設定提供工作流程之電子郵件通知組態的指示。

主題包含：

- ◆ 「關於工作流程管理外掛程式」，第 313 頁
- ◆ 「管理工作流程」，第 313 頁
- ◆ 「設定電子郵件伺服器的組態」，第 321 頁
- ◆ 「使用已安裝的電子郵件範本」，第 322 頁

23.1 關於工作流程管理外掛程式

iManager 的「工作流程管理」外掛程式會提供瀏覽器為主的介面，可讓您檢視工作流程程序的狀態，重新指定工作流程中的活動，或者在工作流程阻塞的情況下終止它。

您可以在 iManager 的 *Identity Manager* 類別中找到「工作流程管理」外掛程式。外掛程式包含「工作流程管理」角色中的「工作流程」任務。

「工作流程管理」角色還包含「電子郵件範本」和「電子郵件伺服器選項」任務。這些任務是「密碼」角色下列出之其他任務的捷徑。

關於工作流程任務「工作流程」任務包含下列面板：

面板	描述
工作流程	<p>提供主要使用者介面，以管理提供工作流程。該介面會列出目前正在處理的工作流程，並可讓您在這些工作流程上執行各種動作。</p> <p>當您首次啟動「工作流程」任務時，「工作流程」面板會要您選取 Identity Manager 使用者應用程式驅動程式。該驅動程式會指向工作流程伺服器。您需要先選取驅動程式，然後才能登入伺服器，並開始工作流程管理。</p> <p>在選取驅動程式之後，您可以指定搜尋準則，以選取要管理的工作流程。</p>
工作流程詳細資料	提供唯讀使用者介面，以檢視特定工作流程的詳細資料。

23.2 管理工作流程

本節包含使用「工作流程管理」外掛程式管理提供工作流程的程序。

23.2.1 連接至工作流程伺服器

您需要先連接至工作流程伺服器，然後才可以開始管理工作流程。如果使用者應用程式驅動程式結合至單一工作流程伺服器，則您只需指定要使用的驅動程式名稱。如果驅動程式與多個工作流程伺服器相關聯，則您需要選取目標工作流程伺服器。

若要連接至工作流程伺服器，請執行下列動作：

- 1 選取 iManager 中的 Identity Manager 類別。
- 2 開啓「工作流程管理」角色。
- 3 按一下「工作流程」任務。

iManager 即會顯示「工作流程」螢幕。

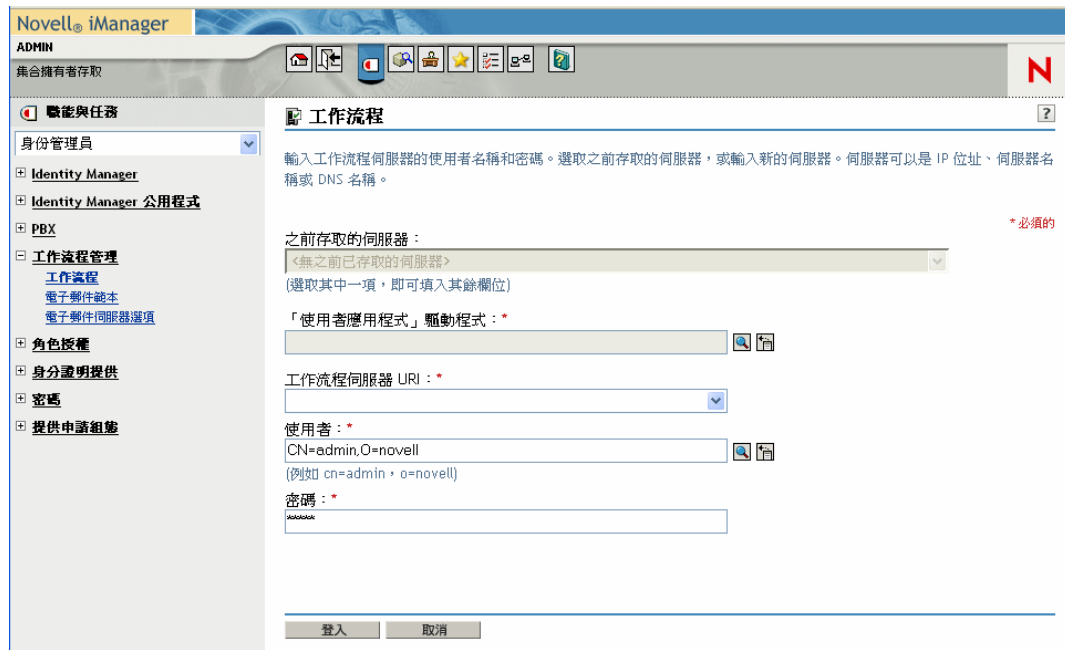


- 4 如果您之前已存取目標工作流程伺服器，則可以從「之前存取的伺服器」下拉式清單中選取伺服器。

iManager 即會為您填入螢幕上的其餘欄位。

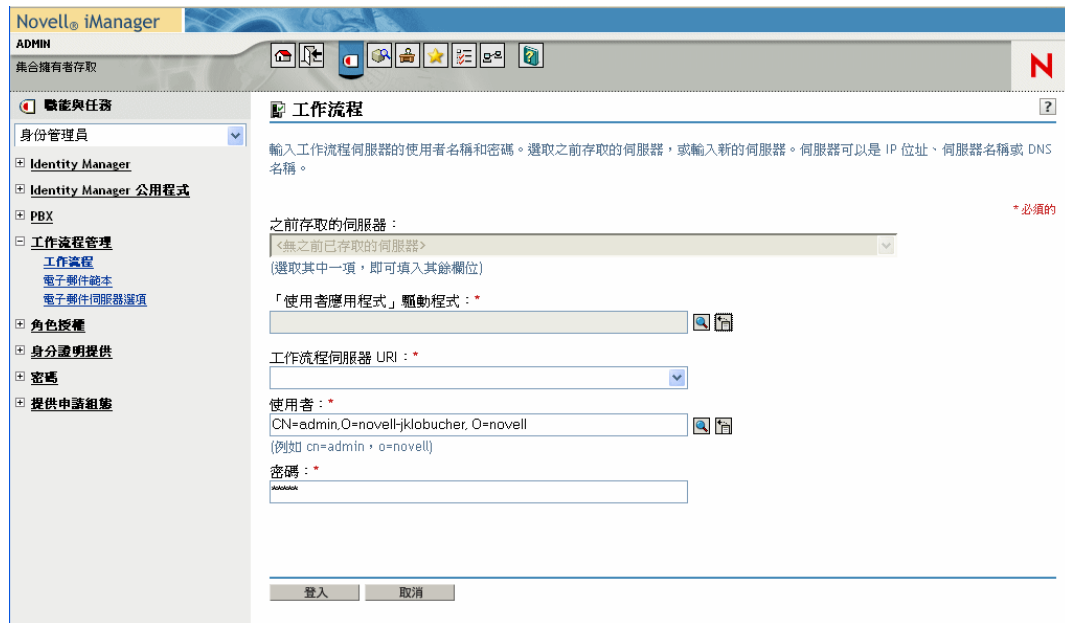
- 5 如果您尚未存取工作流程伺服器，請在「使用者應用程式驅動程式」欄位中指定驅動程式名稱，並按一下「確定」。

iManager 即會為您填入螢幕上的其餘欄位。



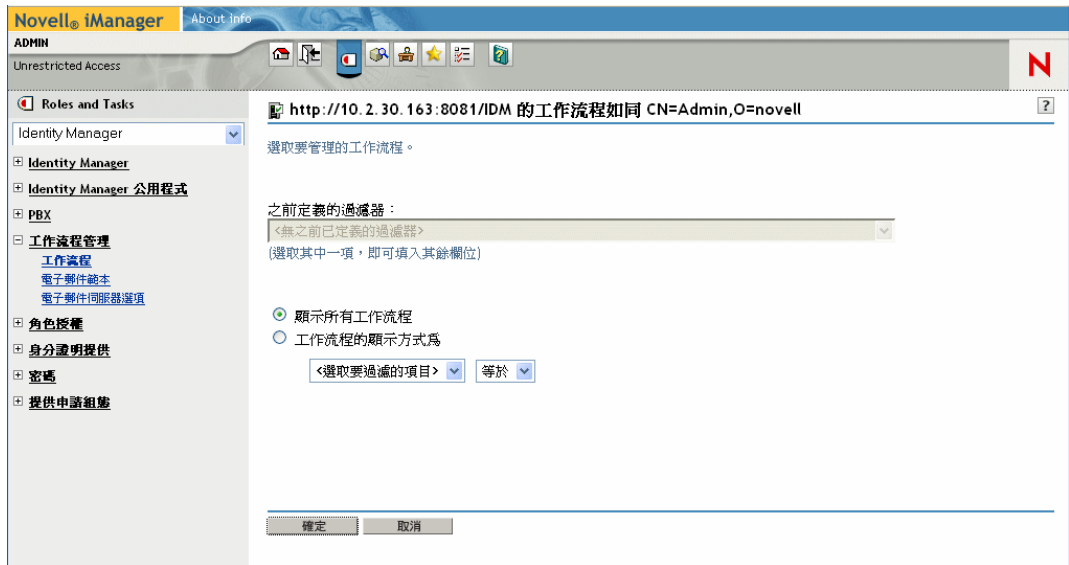
- 6 如果驅動程式與多個工作流程伺服器相關聯，請選取「工作流程伺服器 URI」欄位中的目標伺服器。
- 7 選擇性地置換「使用者」欄位中的使用者名稱和「密碼」欄位中的密碼。

使用者必須是「使用者應用程式管理員」。在預設狀態下，使用者名稱會設為目前登入到 iManager 的使用者。如果此使用者不是管理員，則您需要變更使用者名稱。例如，您應該要修改使用者以指向 idmsample 測試 OU 的「使用者應用程式管理員」，如下所示：



8 按一下「登入」。

「工作流程管理」外掛程式即會顯示可讓您指定尋找工作流程之過濾器的頁面：

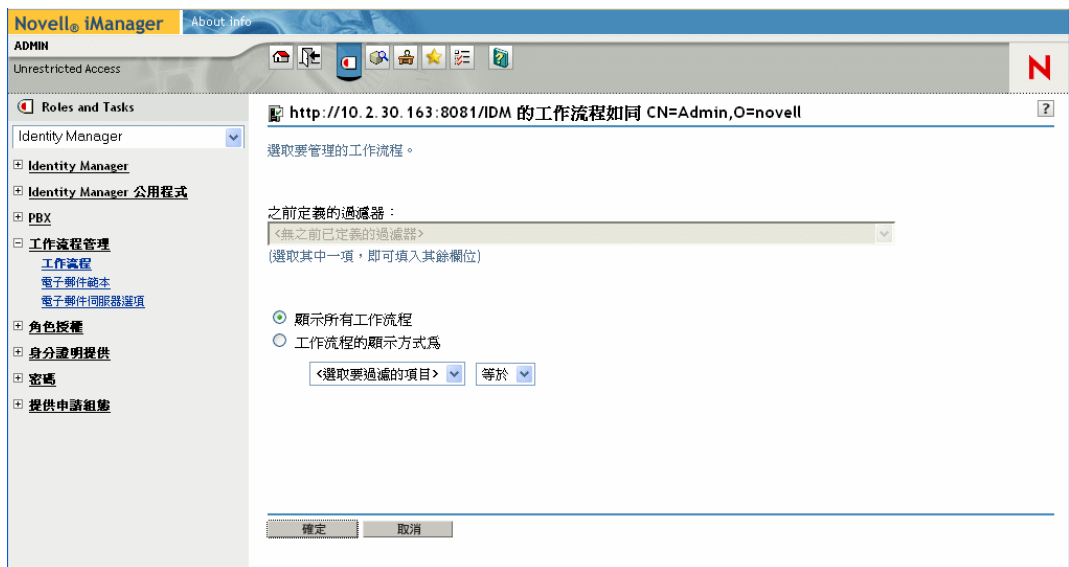


23.2.2 尋找符合搜尋準則的工作流程

如果目標工作流程伺服器正在執行大量的工作流程序，則您應該要過濾在 iManager 中看到的工作流程清單。若要執行此動作，您可以指定搜尋準則。

若要指定過濾工作流程清單的搜尋準則，請執行下列動作：

- 1 選取「工作流程的顯示方式為」選項圓鈕。



附註：在預設狀態下，已選取「顯示所有工作流程」選項圓鈕。如果您想要查看伺服器上工作流程的完整清單，請勿變更預設值。

2 選取您想要指定其準則的屬性。

屬性	描述
建立時間	啓始工作流程的時間。
啓始者	申請者的使用者名稱。
收件者	收件者的使用者名稱。
程序狀態	整個工作流程序的狀態（「已完成」、「執行中」或「已終止」）。
核准狀態	核准程序的狀態（「已核准」、「被拒」或「已取回」）。
授權狀態	由提供申請啓始的授權狀態（「錯誤」、「嚴重錯誤」、「成功」、「不明」或「警告」）。

3 選取運算子：

運算子	備註
等於	支援所有屬性。
之前	僅支援「建立」時間屬性。
之後	僅支援「建立」時間屬性。
之間	僅支援「建立」時間屬性。

4 在屬性和運算子下的欄位中指定值。

針對「建立」時間，您可以使用「日期及時間」控制項來選取值。針對「啓始者」和「收件者」，您可以使用「物件歷程」或「物件選擇器」來指定值。針對所有其他屬性，請從下拉式清單中選取值。

5 按一下「確定」。

iManager 即會顯示您在「工作流程」面板上已選取的工作流程。



變更目標伺服器 and 過濾器 在您選取 workflow 伺服器之後，除非選取新的伺服器，否則此選項會在您的 iManager 會期期間一直起作用。若要選取新的伺服器，請按一下「動作」指令，並從「動作」功能表中選擇「選取伺服器」。



若要指定不同的搜尋準則，請選擇「動作」功能表上的「定義過濾器」。



23.2.3 控制使用中工作流程顯示

「工作流程」面板會列出符合您指定之搜尋準則的工作流程。除了過濾清單之外，您還可以控制顯示。例如，您可以指定重新整理清單和排序特定欄上清單的頻率。

重新整理工作流程的清單

當工作流程伺服器非常忙碌時，使用中工作流程的清單會變更的非常頻繁。在這種情況下，您會想要重新整理正在伺服器上執行之使用中工作流程的清單。

若要重新整理工作流程的清單，請執行下列動作：

- 1 按一下「工作流程」面板中的「重新整理」指令。
- 2 藉由從「重新整理」功能表選取下列其中一個選項，指定您想要使用的重新整理間隔：
 - 2a 關閉重新整理
 - 2b 立即重新整理
 - 2c 10 秒鐘
 - 2d 30 秒鐘
 - 2e 60 秒鐘
 - 2f 5 分鐘

排序工作流程的清單

如果您具有大量的申請定義，則應該要依特定欄（例如，「名稱」或「描述」）排序清單。

若要排序工作流程的清單，請執行下列動作：

- 1 按一下排序欄的標題。

23.2.4 終止工作流程例項

如果您不想要讓工作流程例項繼續其處理，可以終止該工作流程。

若要終止工作流程程序例項，請執行下列動作：

- 1 藉由按一下工作流程名稱旁邊的核取方塊，選取「工作流程」面板中的工作流程。
- 2 按一下「工作流程」面板中的「終止」指令。

23.2.5 檢視工作流程例項的詳細資料

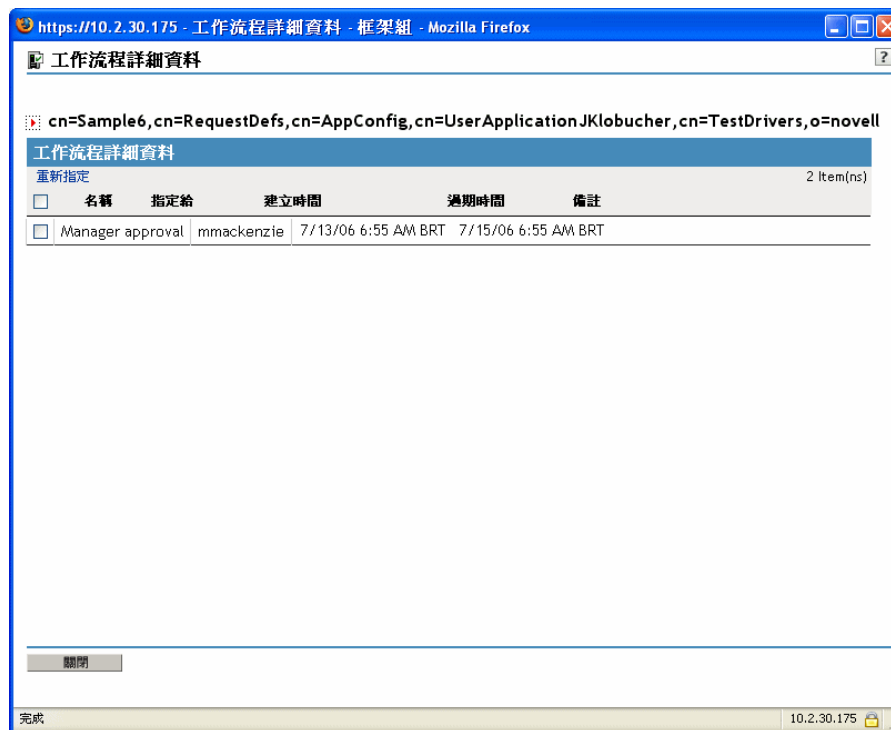
您在特定伺服器上顯示一組執行中工作流程之後，可以選取工作流程例項，以查看執行中程序的相關詳細資料。

附註：如果工作流程例項使用序列處理設計模式，則由於只有一個使用者可以在任何時間點處理工作項目，所以會顯示單一的目前活動。然而，如果工作流程處理平行處理和分支，則工作流程例項可能會有多個目前活動。

若要檢視特定工作流程例項的詳細資料，請執行下列動作：

- 1 按一下「工作流程」面板中工作流程例項的名稱。

iManager 即會顯示「工作流程詳細資料」面板。

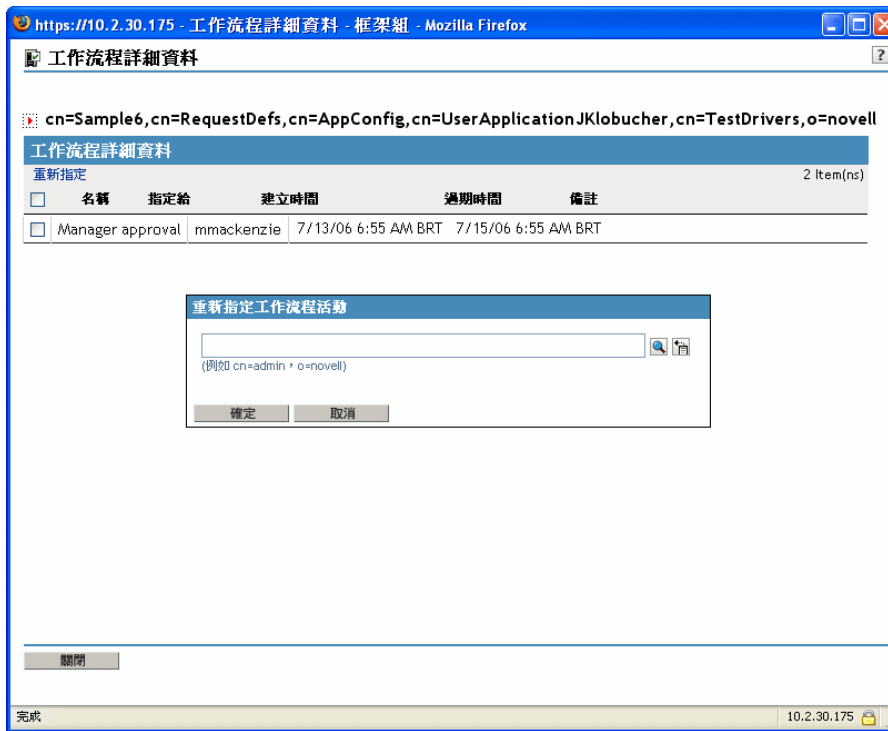


23.2.6 重新指定工作流程例項

如果工作流程例項阻塞，您可以將工作項目重新指定給另一個使用者或群組。

若要重新指定工作流程例項，請執行下列動作：

- 1 藉由按一下「工作流程詳細資料」面板中名稱旁邊的核取方塊，選取與工作流程相關聯的目前活動。
- 2 按一下「工作流程詳細資料」面板中的「重新指定」指令。



- 3 選取您想要重新指定工作項目的使用者或群組。

23.3 設定電子郵件伺服器的組態

工作流程程序經常會在執行過程中的不同時機傳送電子郵件通知。例如，當使用者將工作流程活動指定給新收件人時，電子郵件可能就會傳送。

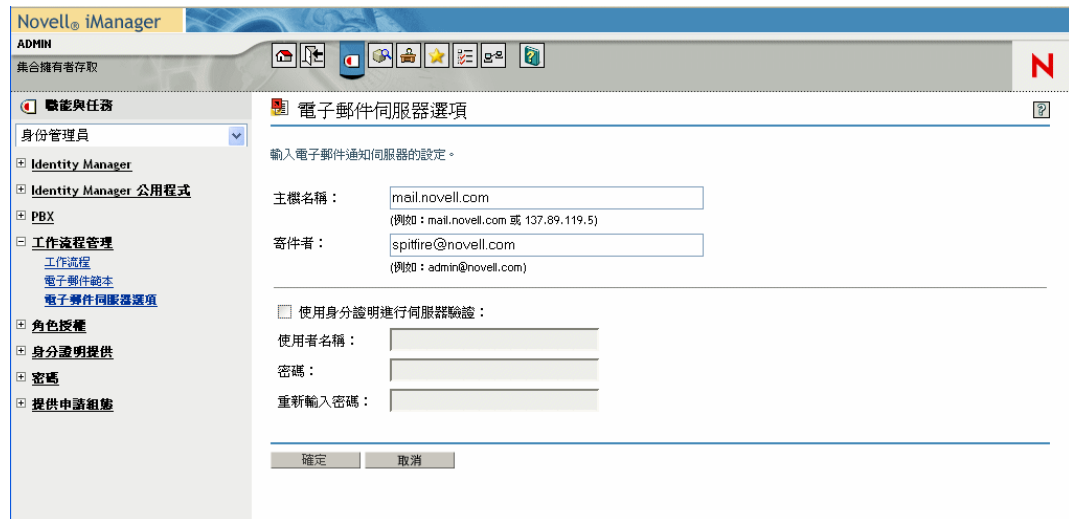
您需要先設定簡易郵件傳輸協定 (SMTP) 電子郵件伺服器的組態，然後才能利用 Identity Manager 的電子郵件通知功能。若要執行此動作，您需要使用 iManager 中「工作流程管理」角色內的「電子郵件伺服器選項」任務。

附註：此任務是「密碼」角色下「電子郵件伺服器選項」任務的捷徑。

若要設定電子郵件伺服器的組態，請執行下列動作：

- 1 選取 iManager 中的 Identity Manager 類別。
- 2 開啓「工作流程管理」角色。
- 3 按一下「電子郵件伺服器選項」任務。

iManager 即會顯示「電子郵件伺服器選項」螢幕。



4 在「主機名稱」欄位中輸入主機伺服器的名稱 (或 IP 位址)。

5 在「寄件者」欄位中輸入寄件者的電子郵件地址。

當收件者開啓電子郵件時，此文字會顯示在電子郵件標題的「寄件者」欄位中。根據您的郵件伺服器設定而定，此欄位中的文字可能需要符合系統中有效的寄件者，以允許郵件伺服器進行反向查詢或驗證。範例是 helpdesk@company.com，而不是描述性文字，例如 The Password Administrator。

6 如果您的伺服器在傳送電子郵件之前需要驗證，請選取「使用身分證明進行伺服器驗證」核取方塊，並指定使用者名稱和密碼。

7 完成後，請按一下「確定」。

23.4 使用已安裝的電子郵件範本

Identity Manager 會隨附特別為工作流程提供而設計的電子郵件範本。此電子郵件範本稱為新的提供申請。產品隨附的所有提供申請範本都與此電子郵件範本相關聯。因此，您建立的任何新申請定義都將使用此電子郵件範本。

雖然您可以編輯「新的提供申請」範本，以變更電子郵件訊息的內容和格式，但是無法建立新的電子郵件範本。

若要編輯「新的提供申請」範本，您需要使用 iManager 中「工作流程管理」角色內的「電子郵件範本」任務。

附註：此任務是「密碼」角色下「編輯電子郵件範本」任務的捷徑。

23.4.1 預設內容和格式

在您安裝產品之後，「新的提供申請」範本如下所示：

Dear \$userFirstName\$, A new provisioning request has been submitted

that requires your approval. Request name: \$requestTitle\$ Submitted by: \$initiatorFullName\$ Recipient: \$recipientFullName\$ Please review the details of this request at \$PROTOCOL\$://\$HOST\$: \$PORT\$/\$TASK_DETAILS\$ to take the appropriate action. You can review a list of all requests pending your approval at \$PROTOCOL\$://\$HOST\$: \$PORT\$/\$TASKLIST_CONTEXT\$.

該範本會識別觸發電子郵件訊息的提供申請定義。此外，它還包含將收件人重新導向至需要核准之任務的 URL，以及顯示該使用者待處理任務之完整清單的 URL。

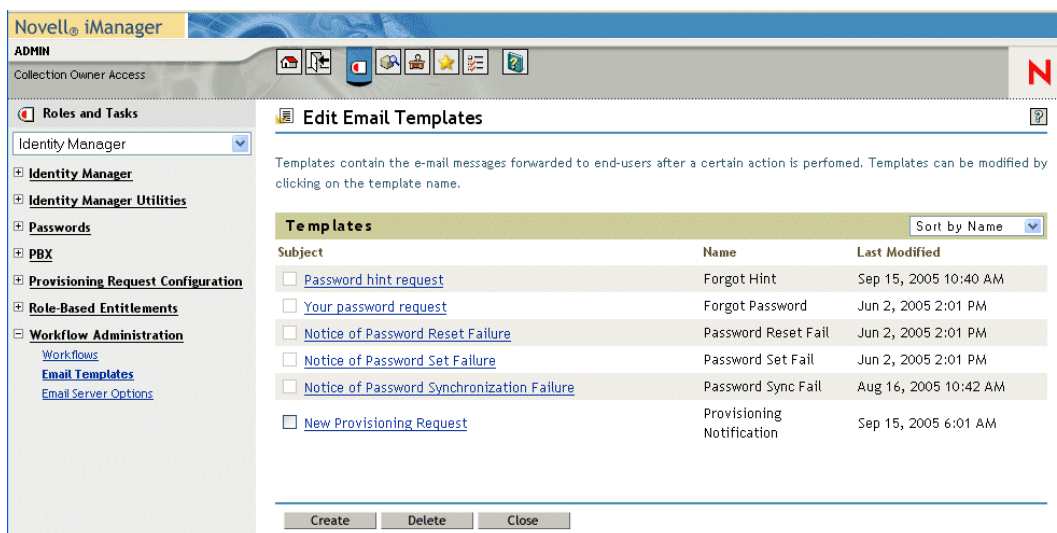
23.4.2 編輯範本

您可以變更「新的提供申請」範本的內容或格式。請注意，該範本會套用至 Identity Manager 使用者應用程式中的所有提供申請，因此請確定您的編輯適用於所有使用者和工作流程任務。

若要編輯範本，請執行下列動作：

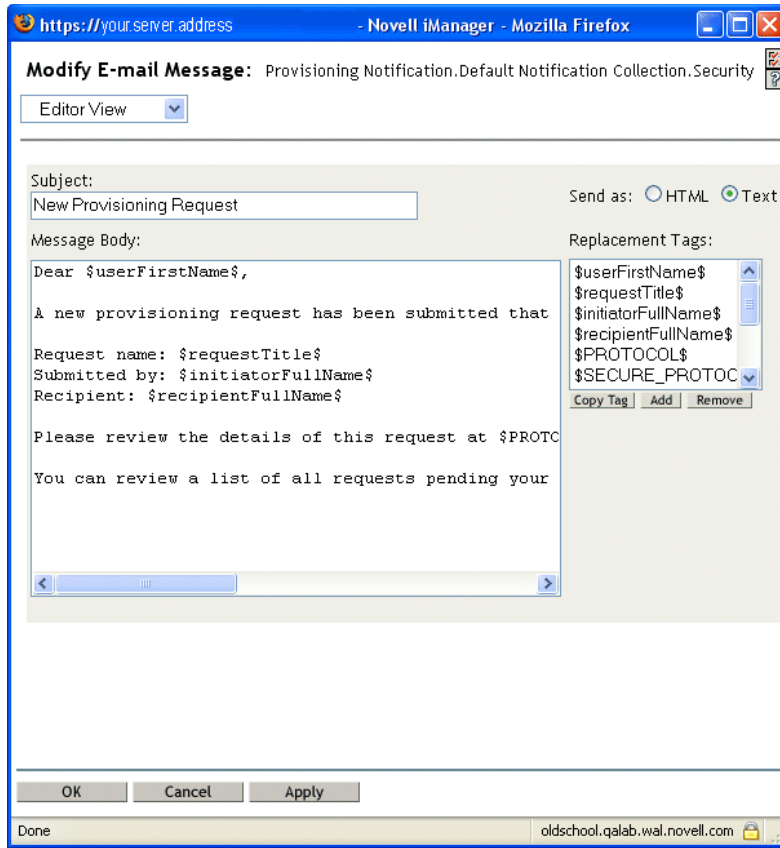
- 1 選取 iManager 中的 Identity Manager 類別。
- 2 開啓「工作流程管理」角色。
- 3 按一下「電子郵件範本」任務。

iManager 即會顯示「編輯電子郵件範本」螢幕。



- 4 按一下範本清單中的「新的提供申請」。

iManager 即會顯示「修改電子郵件訊息」螢幕。



- 5 在「訊息本文」方塊中進行變更。
- 6 必要時，在「取代標籤」清單方塊中複製一或多個提供的標籤，以在訊息本文中併入動態文字。

取代標籤的簡要描述如下所示：

標籤	描述
\$userFirstName\$	收件人的名。
\$requestTitle\$	提供申請定義的顯示名稱。
\$initiatorFullName\$	啓始者的全名。
\$recipientFullName\$	收件者的全名。
\$PROTOCOL\$	電子郵件訊息中包含之 URL 的通訊協定。
\$SECURE_PROTOCOL\$	電子郵件訊息中包含之 URL 的安全通訊協定。
\$HOST\$	執行 Identity Manager 使用者應用程式之 JBoss 應用程式伺服器的主機。
\$PORT\$	Identity Manager 使用者應用程式的連接埠。
\$SECURE_PORT\$	Identity Manager 使用者應用程式的安全連接埠。
\$TASKLIST_CONTEXT\$	顯示收件人所有待處理申請之清單的頁面。

標籤	描述
\$TASK_DETAILS\$	顯示此電子郵件產生所針對之申請詳細資料的頁面。

7 完成後，請按一下「確定」。

23.4.3 修改範本的預設值

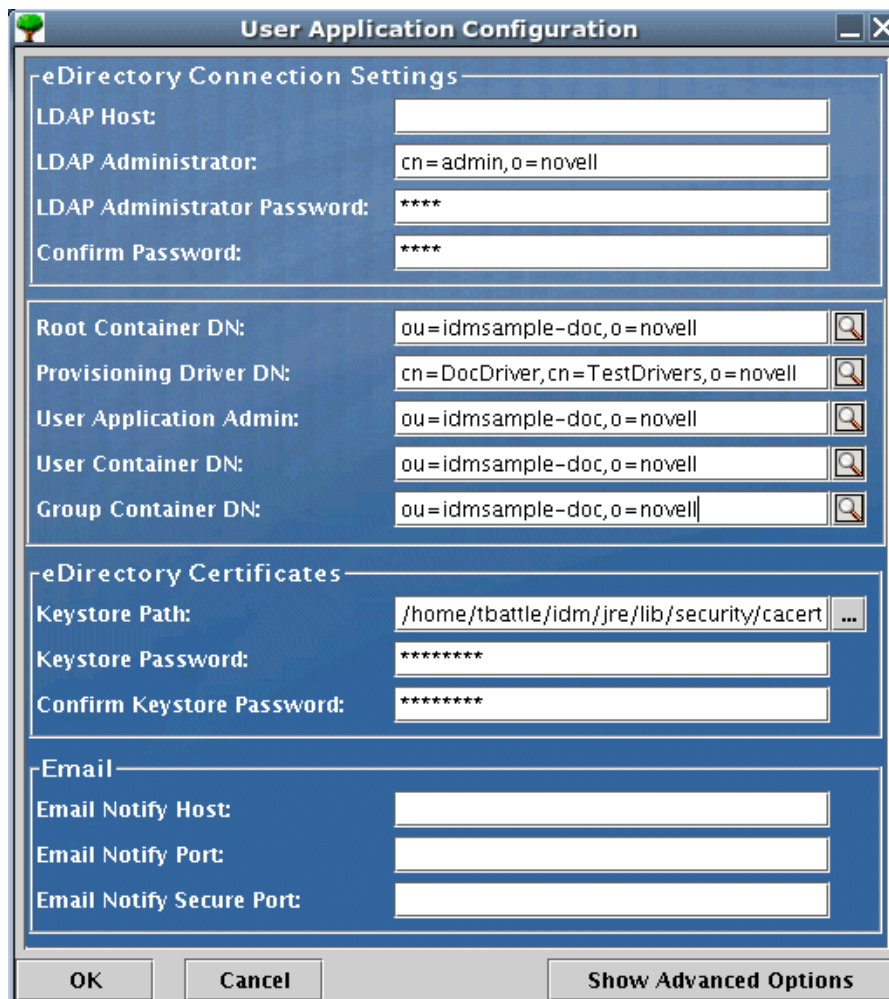
在安裝期間，您可以針對電子郵件範本中使用的數個取代標籤設定預設值。完成安裝之後，您還可以使用「使用者應用程式組態」工具修改這些值。

若要修改安裝設定，請執行下列動作：

- 1 執行 idm 資料夾中的 ldapconfig.sh 程序檔。

```
./configupdate.sh
```

附註：在 Windows 上，要執行的檔案是 configupdate.bat。



2 視需要變更下列任何欄位：

欄位	描述
電子郵件通知主機	用於取代核准流程所使用之電子郵件範本中的 \$HOST\$ 記號。如果保留空白，則會由伺服器進行計算 (此為 JBoss 主機)。
電子郵件通知連接埠	用於取代核准流程所使用之電子郵件範本中的 \$PORT\$ 記號。
電子郵件通知安全連接埠	用於取代核准流程所使用之電子郵件範本中的 \$SECURE_PORT\$ 記號。

3 按一下「確定」以確認變更。

附錄

VI

下列附錄提供 Identity Manager 使用者應用程式的進階主題和其他參考資訊。

- ◆ 附錄 A 「綱要延伸」，第 329 頁
- ◆ 附錄 B 「設定應用程式歸檔的組態」，第 343 頁

綱要延伸

A

A.1 屬性綱要延伸

屬性名稱	描述
srvprvAOLIMAddress	AOL IM 位址
srvprvActiveDelegates	使用者的使用中受託者
srvprvActiveDelegators	使用者的使用中委託者
srvprvAssetRef	具名資產之總資產內容的表示，該具名資產透過 srvprvAssetRecipientAux 類別與使用者相關聯
srvprvAssignExpiration	代理或委託指定過期的時間
srvprvAssignFromContainer	代理或委託指定的容器標題
srvprvAssignFromGroup	代理或委託指定的群組標題
srvprvAssignFromUser	代理或委託指定的使用者標題
srvprvAssignToRelationship	委託指定的目標關係
srvprvAssignToUser	代理或委託指定的「使用者」目標
srvprvCategoryKey	將指定的「提供申請定義」與一組提供類別相關聯。值是 srvprvChoice 例項的鍵
srvprvDefaultTheme	預設主題
srvprvEntitlementRef	「DirXML 授權」的參考
srvprvEntityType	指定「目錄抽象層實體」定義類型
srvprvFlowStrategy	指定要用於「提供申請定義」的流程叫用策略
srvprvGrant	若為 true 時所指定「提供申請定義」支援「授予」操作的旗標
srvprvGroupwiseIMAddress	Groupwise IM 位址
srvprvHeaderFillerFile	標題填充檔案名稱
srvprvHeaderFillerImage	標題填充影像
srvprvHeaderFillerLastMod	標題填充影像的上次修改日期
srvprvHeaderLogo2File	標題標誌的次要影像檔案名稱
srvprvHeaderLogo2Image	標題標誌的次要影像
srvprvHeaderLogo2LastMod	標題標誌次要影像的上次修改日期
srvprvHeaderLogoFile	標題標誌的主要影像檔案名稱
srvprvHeaderLogoImage	標題標誌的主要影像

屬性名稱	描述
srvprvAOLIMAddress	AOL IM 位址
srvprvHeaderLogoLastMod	標題標誌主要影像的上次修改日期
srvprvHeaderTextureFile	標題材質檔案名稱
srvprvHeaderTextureImage	標題材質影像
srvprvHeaderTextureLastMod	標題材質影像的上次修改日期
srvprvIsTaskManager	指出使用者是否為任務群組管理員
srvprvLocalizedDescrs	針對提供 Web 應用程式、 Designer 和 iManager 提供當地語系化描述字串集
srvprvLocalizedNames	針對提供 Web 應用程式、 Designer 和 iManager 提供當地語系化顯示名稱字串集
srvprvLoginFile	登入檔案名稱
srvprvLoginImage	登入影像
srvprvLoginLastMod	登入影像的上次修改日期
srvprvLoginSmallFile	登入的小型影像檔案名稱
srvprvLoginSmallImage	登入的小型影像
srvprvLoginSmallLastMod	登入小型影像的上次修改日期
srvprvModified	指出目錄模型容器中定義物件例項變更的旗標
srvprvNavBckgrColor	導覽背景色彩
srvprvNavBckgrColorLastMod	導覽背景色彩的上次修改日期
srvprvNavColor	導覽色彩
srvprvNavColorLastMod	導覽色彩的上次修改日期
srvprvPreferredLocale	已儲存查詢 / 搜尋準則的清單
srvprvProcessXML	代表「提供」程序定義 (包含「工作流程」和「提供動作」) 的 XML 文件
srvprvRequestDefName	與委託定義相關聯的提供申請定義名稱
srvprvRequestXML	代表啓始申請表單及其資料繫結的 XML 文件
srvprvRevoke	若為 true 時所指定「提供申請定義」支援「撤銷」操作的旗標
srvprvStatus	指出值將包含的「支援的提供物件」狀態
srvprvTaskGroups	其使用者是任務管理員的群組
srvprvUUID	入口網站應用程式的唯一識別碼
srvprvTaskManager	任務群組的任務管理員
srvprvYahooIMAddress	Yahoo IM 位址

A.2 Objectclass 綱要延伸

OBJECTCLASS 名稱	描述
srvprvAppConfig	其「DirXML 驅動程式」父代所連接到之「提供系統」應用程式組態物件的容器
srvprvAppDefs	用於啓始化「提供」執行時期環境(例如「身份入口網站應用程式」的主題)之組態物件的容器。
srvprvAssetRecipientAux	記錄使用者非 IT 資產的提供
srvprvChoice	可以指定給特定屬性、用於查詢等值的列舉，以用於「身份入口網站應用程式」和其他「Web 應用程式」元件
srvprvChoiceDefs	「目錄抽象層選項」定義的容器，將由「身份入口網站應用程式」和「Web 應用程式」公開
srvprvDelegateeAssignment	受託者指定定義
srvprvDelegateeDefs	受託者定義的容器
srvprvDirectoryModel	含有「目錄抽象層」中繼層級物件、「Web 應用程式」和「身份入口網站應用程式」將公開目錄之選定內容的容器
srvprvDirectoryModelConfig	「執行時期目錄抽象層」組態參數
srvprvEntity	定義目錄中已定義類別之選定屬性的檢視窗，用於「身份入口網站應用程式」和其他「Web 應用程式」元件
srvprvEntityAux	標準 ObjectClass
srvprvEntityDefs	「目錄抽象層實體」定義的容器，將由「身份入口網站應用程式」和「Web 應用程式」公開
srvprvProxyAssignment	代理指定定義
srvprvProxyDefs	代理定義的容器
srvprvRelationship	定義目錄中物件之間的關係，用於「身份入口網站應用程式」和其他「Web 應用程式」元件
srvprvRelationshipDefs	「目錄抽象層關係」定義的容器，將由「身份入口網站應用程式」和「Web 應用程式」公開
srvprvRequest	公開要授予或撤銷的一個可提供項目，包含定義「工作流程」和「提供目標」執行時期方面的工作流程程序
srvprvRequestDefs	「提供申請定義」的容器，「Web 應用程式」執行時期的可提供項目集
srvprvResource	定義目錄指定集，針對提供完成操作(「授予」或「撤銷」)來執行
srvprvResourceDefs	「提供目標」定義的容器，包含設計階段描述與任何範本或未使用的目標
srvprvService	描述如何從「工作流程」叫用特定的「Web 服務」，包含輸入和傳回值的規格
srvprvServiceDefs	「服務定義」物件的容器，該物件會包裝由「工作流程」呼叫的「Web 服務」

OBJECTCLASS 名稱	描述
srvprvAppConfig	其「DirXML 驅動程式」父代所連接到之「提供系統」應用程式組態物件的容器
srvprvTaskGroupAux	服務提供任務群組
srvprvTheme	主題物件
srvprvUserAux	服務提供使用者實體
srvprvWebAppConfig	Web 應用程式組態物件
srvprvWorkflow	定義爲了取得提供動作核准而執行之活動 (包含周遊條件) 的網路
srvprvWorkflowDefs	「工作流程」物件的容器，包含設計階段描述與任何範本或未使用的流程
srvprvServiceDefs	「服務定義」物件的容器，該物件會包裝由「工作流程」呼叫的「Web 服務」
srvprvStatus	指出值將包含的「支援的提供物件」狀態
srvprvTaskGroupAux	服務提供任務群組
srvprvTaskGroups	其使用者是任務管理員的群組
srvprvTaskManager	任務群組的任務管理員
srvprvTheme	主題物件
srvprvUserAux	服務提供使用者實體
srvprvWebAppConfig	Web 應用程式組態物件
srvprvWorkflow	定義爲了取得提供動作核准而執行之活動 (包含周遊條件) 的網路
srvprvWorkflowDefs	「工作流程」物件的容器，包含設計階段描述與任何範本或未使用的流程
srvprvYahooIMAddress	Yahoo IM 位址

A.3 LDIF 表示

包含語法、包含規則和上述摘要表格中未顯示之其他資訊的完整綱要資訊如下所示 (LDIF 格式)。此資訊可能會有變更。

```
version: 1 # Copyright (c) 2004-2005 Unpublished Work of Novell, Inc.
All Rights # Reserved. # # THIS WORK IS AN UNPUBLISHED WORK AND
CONTAINS CONFIDENTIAL, # PROPRIETARY AND TRADE SECRET INFORMATION OF
NOVELL, INC. ACCESS TO # THIS WORK IS RESTRICTED TO (I) NOVELL, INC.
EMPLOYEES WHO HAVE A NEED # TO KNOW HOW TO PERFORM TASKS WITHIN THE
SCOPE OF THEIR ASSIGNMENTS AND # (II) ENTITIES OTHER THAN NOVELL, INC.
WHO HAVE ENTERED INTO # APPROPRIATE LICENSE AGREEMENTS. NO PART OF
THIS WORK MAY BE USED, # PRACTICED, PERFORMED, COPIED, DISTRIBUTED,
REVISED, MODIFIED, # TRANSLATED, ABRIDGED, CONDENSED, EXPANDED,
COLLECTED, COMPILED, # LINKED, RECAST, TRANSFORMED OR ADAPTED WITHOUT
```

```

THE PRIOR WRITTEN # CONSENT OF NOVELL, INC. ANY USE OR EXPLOITATION OF
THIS WORK WITHOUT # AUTHORIZATION COULD SUBJECT THE PERPETRATOR TO
CRIMINAL AND CIVIL # LIABILITY. # # Base schema extensions for
SpitFire # # Last Modified: 6/27/05 (ek) # # See rfc2252 for
information on attribute syntax definitions # String =
1.3.6.1.4.1.1466.115.121.1.15 # Boolean =
1.3.6.1.4.1.1466.115.121.1.7 # Octet String =
1.3.6.1.4.1.1466.115.121.1.40 # DN = 1.3.6.1.4.1.1466.115.121.1.12 #
Case Exact String = 1.3.6.1.4.1.1466.115.121.1.26 # Case Ignore List
= 2.16.840.1.113719.1.1.5.1.6 # Case Ignore String =
1.3.6.1.4.1.1466.115.121.1.15 # Stream =
1.3.6.1.4.1.1466.115.121.1.5 # Time = 1.3.6.1.4.1.1466.115.121.1.24
# # OID registered for EPM: # subarc "450" registered at: https://
wiki.innerweb.novell.com/wiki.phtml?title=OID_Registration #
attribute prefix: 2.16.840.1.113719.1.450.4.{3 digit unique per
attribute} # object class prefix: 2.16.840.1.113719.1.450.6.{3 digit
unique number per class} #-----
----- #-- Framework Attributes #-----
----- dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.127 NAME
'srvprvUUID' DESC 'Standard Attribute' SYNTAX
1.3.6.1.4.1.1466.115.121.1.26{64512} SINGLE-VALUE X-NDS_PUBLIC_READ
'1' X-NDS_NOT_SCHED_SYNC_IMMEDIATE '1' ) dn: cn=schema changetype:
modify add: objectClasses objectClasses: (
2.16.840.1.113719.1.450.6.127 NAME 'srvprvEntityAux' DESC 'Standard
ObjectClass' AUXILIARY MAY srvprvUUID X-NDS_NOT_CONTAINER '1' ) #-----
----- #-- User Attributes
#-----
----- dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.60 NAME 'srvprvHideUser' DESC 'Indicates if
a user is hidden during searches' SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.61 NAME
'srvprvHideAttributes' DESC 'List of attributes a user is hiding from
other users' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.62 NAME 'srvprvQueryList' DESC 'List of
saved query/search criteria' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.63 NAME
'srvprvCapabilities1' DESC 'Place holder for classifying skills,
knowledge, references, etc. Classifications are defined in the
application.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.64 NAME 'srvprvCapabilities2' DESC 'Place
holder for classifying skills, knowledge, references, etc.
Classifications are defined in the application.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.65 NAME
'srvprvCapabilities3' DESC 'Place holder for classifying skills,

```

```

knowledge, references, etc. Classifications are defined in the
application.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.66 NAME 'srvprvCapabilities4' DESC 'Place
holder for classifying skills, knowledge, references, etc.
Classifications are defined in the application.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.67 NAME
'srvprvCapabilities5' DESC 'Place holder for classifying skills,
knowledge, references, etc. Classifications are defined in the
application.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.68 NAME 'srvprvIMAddress' DESC 'Key-value
pair of Instant messenger Addresses i.e. groupwise~jsmith' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 ) # This is temporary until we convert
the application to use the multi-value IM address (srvprvIMAddress)
above dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.69 NAME
'srvprvGroupwiseIMAddress' DESC 'Groupwise IM address' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) # This is temporary until
we convert the application to use the multi-value IM address
(srvprvIMAddress) above dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.70 NAME
'srvprvYahooIMAddress' DESC 'Yahoo IM address' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) # This is temporary until
we convert the application to use the multi-value IM address
(srvprvIMAddress) above dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.71 NAME
'srvprvAOLIMAddress' DESC 'AOL IM address' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.72 NAME 'srvprvActiveDelegates' DESC 'The
active delegates of a user' SYNTAX 2.16.840.1.113719.1.1.5.1.6 ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.73 NAME 'srvprvActiveDelegators' DESC 'The
active delegators of a user' SYNTAX 2.16.840.1.113719.1.1.5.1.6 ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.74 NAME 'srvprvIsTaskManager' DESC
'Indicates if user is a task group manager' SYNTAX
1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.75 NAME 'srvprvTaskGroups' DESC 'Groups for
which the user is a task manager' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.77 NAME
'srvprvPreferredLocale' DESC 'List of saved query/search criteria'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.128 NAME 'srvprvUserAux' DESC 'Service
provisioning user entity' AUXILIARY MAY ( srvprvHideUser $
srvprvHideAttributes $ srvprvQueryList $ srvprvCapabilities1 $
srvprvCapabilities2 $ srvprvCapabilities3 $ srvprvCapabilities4 $
srvprvCapabilities5 $ srvprvIMAddress $ srvprvGroupwiseIMAddress $
srvprvYahooIMAddress $ srvprvAOLIMAddress $ srvprvIsTaskManager $

```

```

srvprvTaskGroups $ srvprvActiveDelegates $ srvprvActiveDelegators $
srvprvPreferredLocale) X-NDS_NOT_CONTAINER '1' ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.129 NAME 'srvprvTaskManager' DESC 'Task
manager of the task group' SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.130 NAME 'srvprvTaskGroupAux' DESC 'Service
provisioning task group' AUXILIARY MAY ( srvprvTaskManager ) X-
NDS_NOT_CONTAINER '1' ) #-----
-----
----- #-- Provisioning Attributes #-----
-----
----- dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.100 NAME
'srvprvCategoryKey' DESC 'Associates a given Provisioning Request
Definition to a set of provisioning categories. Values are keys to a
srvprvChoice instance.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.101 NAME 'srvprvGrant' DESC 'Flag which if
true specifies that the Provisioning Request Definition supports a
Grant operation.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )
dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.102 NAME 'srvprvRevoke' DESC 'Flag which if
true specifies that the Provisioning Request Definition supports a
Revoke operation.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )
dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.103 NAME 'srvprvFlowStrategy' DESC
'Specifies the flow invocation strategy to be used for the Provisioning
Request Definition.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
) dn: cn=schema changetype: modify add: attributeTypes attributeTypes:
( 2.16.840.1.113719.1.450.4.104 NAME 'srvprvLocalizedNames' DESC
'Provides set of localized display name strings for the provisioning
web applications, Designers and iManager.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.26 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.105 NAME
'srvprvLocalizedDescrs' DESC 'Provides set of localized description
strings for the provisioning web applications, Designers and
iManager.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.106 NAME 'srvprvStatus' DESC 'Specifies the
status of the Provisioning Object. Supported values will include:
Inactive, Active, Template, and Retired.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.107 NAME 'srvprvProcessXML' DESC 'XML
document representing a Provisioning process definition including
Workflow and Provisioning Action.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.108 NAME 'srvprvEntityType' DESC 'Specifies
Directory Abstraction Layer Entity definition type: P-Public
definitions or S-System definitions.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (

```

```

2.16.840.1.113719.1.450.4.109 NAME 'srvprvRequestXML' DESC 'XML
document representing the initial request form and its data bindings'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.110 NAME 'srvprvModified' DESC 'Flag to
indicate changes to definitions object instances in the directory
model container' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.111 NAME 'srvprvEntitlementRef' DESC
'Reference to a DirXML-Entitlement' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE ) #-----
-----
----- #-- Provisioning Configuration
Containers #-----
----- dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.100 NAME 'srvprvAppConfig' DESC 'Container
for application configuration objects of the Provisioning System to
which its DirXML-Driver parent connects.' SUP top STRUCTURAL MUST ( cn
$ version ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT
( 'DirXML-Driver' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.101 NAME
'srvprvRequestDefs' DESC 'Container for Provisioning Request
Definitions, the set of provisionable items to the Web Application run-
time.' SUP top STRUCTURAL MUST ( cn ) MAY ( description ) X-NDS_NAMING
( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.102 NAME 'srvprvWorkflowDefs' DESC
'Container for Workflow objects, including design-time descriptions
plus any template or unused flows.' SUP top STRUCTURAL MUST ( cn ) MAY
( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvAppConfig' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.103 NAME
'srvprvResourceDefs' DESC 'Container for Provisioning Target
definitions, including design-time descriptions plus any template or
unused targets.' SUP top STRUCTURAL MUST ( cn ) MAY ( description ) X-
NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.104 NAME 'srvprvServiceDefs' DESC 'Container
for Service Definition objects, which wrap Web Services called by
Workflows.' SUP top STRUCTURAL MUST ( cn ) MAY ( description ) X-
NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.105 NAME 'srvprvDirectoryModel' DESC
'Container for Directory Abstraction Layer meta-level objects,
selected contents of the directory to be exposed by the Identity
Portlets and Web Applications.' SUP top STRUCTURAL MUST ( cn ) MAY (
description $ srvprvModified ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT
( 'srvprvAppConfig' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.106 NAME
'srvprvAppDefs' DESC 'Container for configuration objects used to
initialise the Provisioning run-time environment, such as themes for
the Identity Portal.' SUP top STRUCTURAL MUST ( cn ) MAY ( description
) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn:

```

```

cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.111 NAME 'srvprvEntityDefs' DESC 'Container
for Directory Abstraction Layer Entity defintions, to be exposed by the
Identity Portlets and Web Applications.' SUP top STRUCTURAL MUST ( cn )
MAY ( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvDirectoryModel' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.112 NAME
'srvprvRelationshipDefs' DESC 'Container for Directory Abstraction
Layer Relationship definitions, to be exposed by the Identity Portlets
and Web Applications.' SUP top STRUCTURAL MUST ( cn ) MAY ( description
) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvDirectoryModel' ) )
dn: cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.113 NAME 'srvprvChoiceDefs' DESC 'Container
for Directory Abstraction Layer Choice definitions, to be exposed by
the Identity Portlets and Web Applications.' SUP top STRUCTURAL MUST (
cn ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvDirectoryModel' ) ) ##### Provisioning Configuration Object
Classes dn: cn=schema changetype: modify add: objectclasses
objectClasses: ( 2.16.840.1.113719.1.450.6.107 NAME 'srvprvRequest'
DESC 'Exposes one provisionable item to be granted or revoked,
including the workflow process which defines the run-time aspects of
the Workflow and Provisioning Target.' SUP top STRUCTURAL MUST ( cn $
srvprvStatus $ srvprvFlowStrategy $ srvprvGrant $ srvprvRevoke $
srvprvCategoryKey $ srvprvLocalizedNames $ srvprvLocalizedDescrs ) MAY
( description $ srvprvEntitlementRef $ XmlData $ srvprvRequestXML $
srvprvProcessXML ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' ) X-
NDS_CONTAINMENT ( 'srvprvRequestDefs' ) ) dn: cn=schema changetype:
modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.108 NAME 'srvprvWorkflow' DESC 'Defines the
network of activites including traversal conditions to be executed in
order to obtain approval for a provisioning action.' SUP top STRUCTURAL
MUST ( cn $ srvprvLocalizedNames $ srvprvLocalizedDescrs ) MAY (
description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' )
X-NDS_CONTAINMENT ( 'srvprvWorkflowDefs' ) ) dn: cn=schema changetype:
modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.109 NAME 'srvprvResource' DESC 'Defines the
set of directory assignments to execute for a provisioning fulfillment
operation (either Grant or Revoke).' SUP top STRUCTURAL MUST ( cn $
srvprvLocalizedNames $ srvprvLocalizedDescrs ) MAY ( description $
srvprvEntitlementRef $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING
( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvResourceDefs' ) ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.110 NAME 'srvprvService' DESC 'Describes how
to invoke a specific Web Service from an Workflow. This includes
specification of input and return values.' SUP top STRUCTURAL MUST ( cn
) MAY ( description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING (
'cn' ) X-NDS_CONTAINMENT ( 'srvprvServiceDefs' ) ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.114 NAME 'srvprvEntity' DESC 'Defines a view
of selected attributes for defined classes in the directory, used by
the Identity Portlets and other Web Application components.' SUP top
STRUCTURAL MUST ( cn $ srvprvEntityType ) MAY ( description $ XmlData )
X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvEntityDefs' ) ) dn: cn=schema changetype: modify add:

```

```

objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.115 NAME
'srvprvRelationship' DESC 'Defines relationships between objects in
the directory, for use in the Identity Portlets and other Web
Application components.' SUP top STRUCTURAL MUST ( cn ) MAY (
description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' )
X-NDS_CONTAINMENT ( 'srvprvRelationshipDefs' ) ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.116 NAME 'srvprvChoice' DESC 'Enumeration of
values which can be assigned to a particular attribute, used in a
query, etc. for use in the Identity Portlets and other Web Application
components.' SUP top STRUCTURAL MUST ( cn ) MAY ( description $ XmlData
) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvChoiceDefs' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.117 NAME
'srvprvDirectoryModelConfig' DESC 'Runtime Directory Abstraction Layer
configurariion parameters' SUP top STRUCTURAL MUST ( cn ) MAY (
description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' )
X-NDS_CONTAINMENT ( 'srvprvDirectoryModel' ) ) ##### User Aux Classes
and Attributes dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.80 NAME 'srvprvAssetRef'
DESC 'Representation of the aggregate asset properties for a named
asset associated to a user via the srvprvAssetRecipientAux class.'
SYNTAX 2.16.840.1.113719.1.1.5.1.6 ) dn: cn=schema changetype: modify
add: objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.80 NAME
'srvprvAssetRecipientAux' DESC 'Records the provisioning of non-IT
assets on a user' AUXILIARY MAY ( srvprvAssetRef ) ) #-----
-----
----- #-- Web Application Config
Class #-----
----- dn:
cn=schema changetype: modify add: attributeTypes attributeTypes:
(2.16.840.1.113719.1.450.4.20 NAME 'srvprvDefaultTheme' DESC 'The
default theme' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.21 NAME 'srvprvWebAppConfig' DESC 'Web
Application Config Object' SUP top STRUCTURAL MUST (cn) MAY
(description $ srvprvDefaultTheme $ XmlData ) X-NDS_NOT_CONTAINER '1'
X-NDS_NAMING 'cn' X-NDS_CONTAINMENT ( 'srvprvAppDefs' ) ) #-----
-----
----- #-- Theme Branding
Structural Class #-----
-----
-- dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.21 NAME
'srvprvHeaderLogoImage' DESC 'Header Logo Primary Image' SYNTAX
1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.22 NAME 'srvprvHeaderLogoFile' DESC 'Header
Logo Primary Image File Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.23 NAME
'srvprvHeaderLogoLastMod' DESC 'Header Logo Primary Last Modified'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (

```


2.16.840.1.113719.1.450.4.24 NAME 'srvprvHeaderLogo2Image' DESC
 'Header Logo Secondary Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
 SINGLE-VALUE) dn: cn=schema changetype: modify add: attributeTypes
 attributeTypes: (2.16.840.1.113719.1.450.4.25 NAME
 'srvprvHeaderLogo2File' DESC 'Header Logo Secondary Image File Name'
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 | SINGLE-VALUE) dn: cn=schema
 changetype: modify add: attributeTypes attributeTypes: (

2.16.840.1.113719.1.450.4.26 NAME 'srvprvHeaderLogo2LastMod' DESC
 'Header Logo Secondary Last Modified' SYNTAX
 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE) dn: cn=schema changetype:
 modify add: attributeTypes attributeTypes: (

2.16.840.1.113719.1.450.4.27 NAME 'srvprvHeaderTextureImage' DESC
 'Header Texture Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-
 VALUE) dn: cn=schema changetype: modify add: attributeTypes
 attributeTypes: (2.16.840.1.113719.1.450.4.28 NAME
 'srvprvHeaderTextureFile' DESC 'Header Texture File Name' SYNTAX
 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE) dn: cn=schema changetype:
 modify add: attributeTypes attributeTypes: (

2.16.840.1.113719.1.450.4.29 NAME 'srvprvHeaderTextureLastMod' DESC
 'Header Texture Last Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 SINGLE-VALUE) dn: cn=schema changetype: modify add: attributeTypes
 attributeTypes: (2.16.840.1.113719.1.450.4.30 NAME
 'srvprvHeaderFillerImage' DESC 'Header Filler Image' SYNTAX
 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE) dn: cn=schema changetype:
 modify add: attributeTypes attributeTypes: (

2.16.840.1.113719.1.450.4.31 NAME 'srvprvHeaderFillerFile' DESC
 'Header Filler File Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-
 VALUE) dn: cn=schema changetype: modify add: attributeTypes
 attributeTypes: (2.16.840.1.113719.1.450.4.32 NAME
 'srvprvHeaderFillerLastMod' DESC 'Header Filler Last Modified' SYNTAX
 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE) dn: cn=schema changetype:
 modify add: attributeTypes attributeTypes: (

2.16.840.1.113719.1.450.4.33 NAME 'srvprvLoginImage' DESC 'Login
 Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE) dn:
 cn=schema changetype: modify add: attributeTypes attributeTypes: (

2.16.840.1.113719.1.450.4.34 NAME 'srvprvLoginFile' DESC 'Login File
 Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE) dn:
 cn=schema changetype: modify add: attributeTypes attributeTypes: (

2.16.840.1.113719.1.450.4.35 NAME 'srvprvLoginLastMod' DESC 'Login
 Last Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE) dn:
 cn=schema changetype: modify add: attributeTypes attributeTypes: (

2.16.840.1.113719.1.450.4.36 NAME 'srvprvLoginSmallImage' DESC 'Login
 Small Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE) dn:
 cn=schema changetype: modify add: attributeTypes attributeTypes: (

2.16.840.1.113719.1.450.4.37 NAME 'srvprvLoginSmallFile' DESC 'Login
 Small File Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE)
 dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (

2.16.840.1.113719.1.450.4.38 NAME 'srvprvLoginSmallLastMod' DESC
 'Login Small Last Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 SINGLE-VALUE) dn: cn=schema changetype: modify add: attributeTypes
 attributeTypes: (2.16.840.1.113719.1.450.4.39 NAME 'srvprvNavColor'
 DESC 'Navigation Color' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-
 VALUE) dn: cn=schema changetype: modify add: attributeTypes
 attributeTypes: (2.16.840.1.113719.1.450.4.40 NAME

```

'srvprvNavColorLastMod' DESC 'Navigation Color Last Modified' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.41 NAME 'srvprvNavBckgrColor' DESC
'Navigation Background Color' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.42 NAME
'srvprvNavBckgrColorLastMod' DESC 'Navigation Background Color Last
Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.20 NAME 'srvprvTheme' DESC 'Theme Object'
SUP top STRUCTURAL MUST (cn) MAY (description $ srvprvHeaderLogoImage
$ srvprvHeaderLogoFile $ srvprvHeaderLogoLastMod $
srvprvHeaderLogo2Image $ srvprvHeaderLogo2File $
srvprvHeaderLogo2LastMod $ srvprvHeaderTextureImage $
srvprvHeaderTextureFile $ srvprvHeaderTextureLastMod $
srvprvHeaderFillerImage $ srvprvHeaderFillerFile $
srvprvHeaderFillerLastMod $ srvprvLoginImage $ srvprvLoginFile $
srvprvLoginLastMod $ srvprvLoginSmallImage $ srvprvLoginSmallFile $
srvprvLoginSmallLastMod $ srvprvNavColor $ srvprvNavColorLastMod $
srvprvNavBckgrColor $ srvprvNavBckgrColorLastMod ) X-NDS_NOT_CONTAINER
'1' X-NDS_CONTAINMENT ( 'srvprvAppDefs' ) X-NDS_NAMING 'cn' ) #-----
-----
----- #-- Attributes,
objects, and containers for Proxy, Delegatee and User availability, #-
-----
----- dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.120 NAME 'srvprvAssignFromUser' DESC 'User
subjects of a proxy or delegatee assignment' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.121 NAME
'srvprvAssignFromGroup' DESC 'Group subjects of a proxy or delegatee
assignment' SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.122 NAME 'srvprvAssignFromContainer' DESC
'Container subjects of a proxy or delegatee assignment' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.123 NAME
'srvprvAssignToUser' DESC 'The User targets of a proxy or delegatee
assignment' SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.124 NAME 'srvprvAssignToRelationship' DESC
'A target relationship of a delegatee assignment' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.125 NAME 'srvprvAssignExpiration' DESC 'Time
at which a proxy or delegatee assignment expires' SYNTAX
1.3.6.1.4.1.1466.115.121.1.24 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.126 NAME 'srvprvRequestDefName' DESC 'The
provisioning request definition name associated with a delegatee
definition.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (

```

```

2.16.840.1.113719.1.450.6.120 NAME 'srvprvProxyDefs' DESC 'Container
for proxy definitions.' SUP top STRUCTURAL MUST ( cn ) MAY (
description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvAppConfig' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.121 NAME
'srvprvDelegateeDefs' DESC 'Container for delegatee definitions.' SUP
top STRUCTURAL MUST ( cn ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-
NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn: cn=schema changetype:
modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.122 NAME 'srvprvProxyAssignment' DESC 'Proxy
assignment definition' SUP top STRUCTURAL MUST ( cn $
srvprvAssignToUser ) MAY ( description $ srvprvAssignFromUser $
srvprvAssignFromGroup $ srvprvAssignFromContainer $
srvprvAssignExpiration ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvProxyDefs' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.123 NAME
'srvprvDelegateeAssignment' DESC 'Delegatee assignment definition' SUP
top STRUCTURAL MUST cn MAY ( srvprvRequestDefName $ description $
srvprvAssignFromUser $ srvprvAssignFromGroup $
srvprvAssignFromContainer $ srvprvAssignToUser $
srvprvAssignToRelationship $ srvprvAssignExpiration ) X-NDS_NAMING (
'cn' ) X-NDS_CONTAINMENT ( 'srvprvDelegateeDefs' ) ) ##### DO
NOT DELETE THIS LINE #####
#####

```


設定應用程式歸檔的組態

本附錄會描述進階設定，您只需要編輯使用者應用程式的 WAR 檔案，就可以設定這些設定的組態。主題包含：

- 「關於使用者應用程式 WAR」，第 343 頁
- 「設定會期逾時」，第 343 頁

B.1 關於使用者應用程式 WAR

Identity Manager 使用者應用程式會封裝為與 J2EE 相容的 Web 應用程式歸檔 (Web Application Archive, WAR) 檔案。使用者應用程式 WAR 檔案包含 Java 類別和 XML 檔案的集合，它們會控制應用程式的執行時期行為。一般而言，WAR 不應該修改。然而，在少數情況下，您可能需要開啟 WAR 檔案並進行某些變更，以控制應用程式的行為。

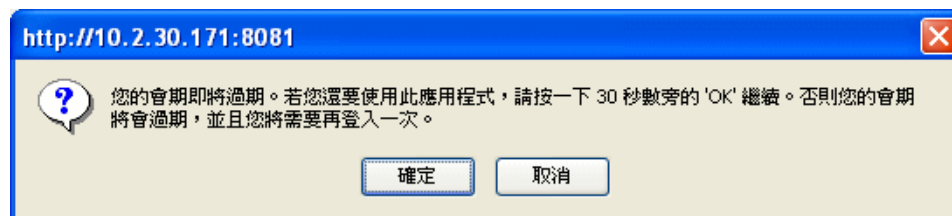
附註：此附錄的其餘部份是假設您已熟悉 J2EE 概念和程序。如果您不確定如何在 WAR 檔案內進行變更，請參閱 J2EE 文件。

B.2 設定會期逾時

為了防止伺服器由於非使用中的會期而多載，Identity Manager 使用者應用程式會讓長期非使用中的使用者會期逾時。預設的逾時間隔為 10 分鐘。您可以編輯使用者應用程式 WAR 檔案之 WEB-INF 資料夾中的 *web.xml* 檔案，以變更該預設。

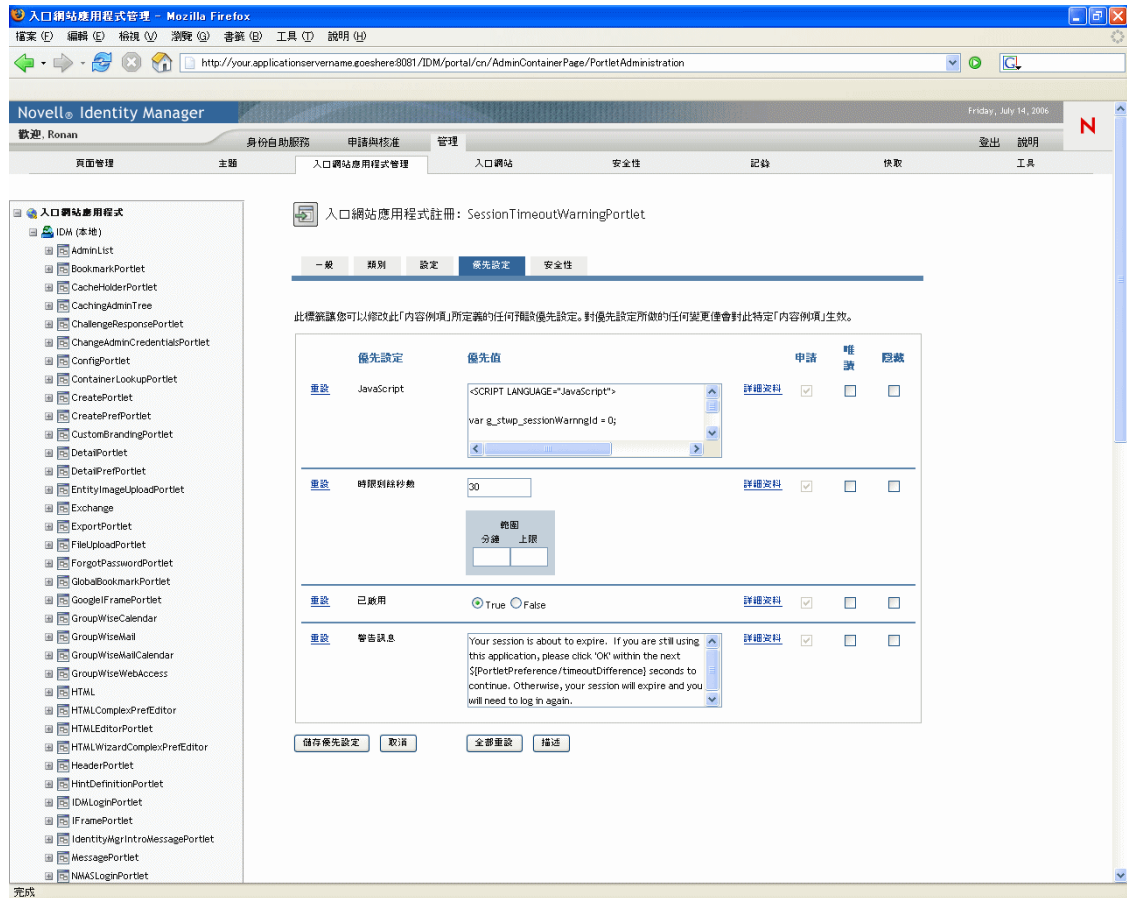
編輯會期逾時間隔 WAR 中的 *web.xml* 檔案具有稱為 `<session-timeout>` 的元素 (它位於 `<session-config>` 元素下面)，該元素會指定會期在逾時前可以為非使用中的時間。若要設定會期逾時間隔，請變更此元素的值。該值必須以分鐘為單位指定。

控制警示訊息的行為在預設狀態下，只要使用者的會期即將逾時，Identity Manager 使用者應用程式即會顯示警示訊息。



如果按一下「確定」後使用者不回應訊息，則會期會逾時。警示訊息預設為已啟用。如果您願意，可以停用它。此外，您還可以指定使用者必須回應警示訊息的時間。

若要控制警示訊息的行為，您需要設定 *SessionTimeoutWarningPortlet* 的組態。若要進行此操作，您需要在入口網站應用程式註冊上編輯入口網站應用程式優先設定，如下所示：



若要指定允許使用者回應警示訊息的時間，請編輯「時限剩餘秒數」值。若要同時停用警示訊息，請按一下「已啟用」旁邊的「*False*」。完成變更之後，按一下「儲存優先設定」。