綜覽指南

Novell® Identity Manager

4.0.1

2011 年 04 月 15 日

www.novell.com

法律聲明

Novell, Inc. 對本文件的內容與使用不做任何陳述或保證，對本產品在任何特定用途的適銷性與適用性上，亦不做任何明示或默示的保證。此外，Novell, Inc. 保留隨時修改本出版品及其內容的權利，進行此類修正或更動時，亦毋需另行通知任何人士或公司組織。

此外，Novell, Inc. 對軟體不做任何陳述或保證，對本產品在任何特定用途的適銷性與適用性上，亦不做任何明示或默示的保證。此外，Novell, Inc. 保留隨時修改任何或全部 Novell 軟體的權利，進行此類更動時，亦毋需通知任何人士或公司。

此合約下提到的任何產品或技術資訊可能受美國出口管制法與其他國家 / 地區的貿易法的限制。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之實體，或是任何美國出口法所指定之禁運或恐怖主義國家。您同意不將交付產品用在禁止的核武、飛彈或生化武器等用途上。如需輸出 Novell 軟體的相關資訊，請參閱國際貿易服務 (http://www.novell.com/company/policies/trade_services)。Novell 無需承擔您無法取得任何必要的出口核准之責任。

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 產品的最新線上文件，請參閱 Novell 文件網頁 (http://www.novell.com/documentation)。

Novell 商標

若要查看 Novell 商標，請參閱 Novell 商標和服務標誌清單 (http://www.novell.com/company/legal/trademarks/tmlist.html)。

協力廠商資料

所有的協力廠商商標均爲其各別擁有廠商的財產。

目錄

關於本指南

本指南介紹一款智能型工作負載產品： Novell Identity Manager，它可以管理實體、虛擬及雲端環境中的身分與存取權限。本指南將說明 Identity Manager 可在降低成本並確保法規遵循的同時，還能協助您解決的企業問題。此外，它還提供了可用於建立 Identity Manager 解決方案之 Identity Manager 元件與工具的技術綜覽。本指南是以下列方式進行編排：

適用對象

本指南適用於需要深入瞭解 Identity Manager 企業解決方案、技術和工具的管理員、顧問和網路工程師。

文件更新

如需本文件的最新版本，請參閱 Identity Manager 文件網站 (http://www.novell.com/documentation/idm401/index.html)。

其他文件

如需 Identity Manager 驅動程式的相關文件，請參閱 Identity Manager 驅動程式網站 (http://www.novell.com/documentation/idm401drivers/index.html)。

1 Identity Manager 與企業流程自動化

本章中的資訊說明您可以透過實作 Novell Identity Manager 系統而得以自動化的一些企業流程。如果您已清楚 Identity Manager 所提供的企業自動化解決方案，您可以直接跳到第 4 章「Identity Manager 架構」(第 21 頁) 中的技術介紹。

管理身分識別需求是大多數企業的一項核心任務。比方說，想像一下現在是星期一的一大早。您開始瀏覽待辦的申請清單：

- Jim Taylor 的行動電話號碼已經改了。您必須在 HR 資料庫和其他四個獨立系統中更新這項資料。
- 剛休完長假回來的 Karen Hansen 忘了她的電子郵件密碼。您必須幫她取回密碼，或是重設密碼。
- Jose Altimira 剛雇用了一位新員工。您必須給這位員工網路存取權和電子郵件帳戶。
- Ida McNamee 想要存取 Oracle 財務資料庫，所以您需要向三位不同的主管取得核准。
- John Harris 剛從應付帳款部門調到法務部門。您必須讓他可以存取法務部門其他同事可存取的相同資源，並讓他無法存取應付帳款的資源。
- 您的上司 Karl Jones 看到了這份關於 Ida McNamee 想要存取 Oracle 財務資料庫的申請，很擔心是否太多人有存取權。您需要替他產生一份報告，列出有權存取資料庫的每一個人。

在深呼吸之後，您便開始處理第一件申請。您知道要處理完所有的申請，恐怕得花不少時間，更何況自己也有其他待處理的專案在手上。

如果這就是您或組織裡某人的日常工作，那麼，Identity Manager 將會是您的得力助手。事實上，下圖所介紹的 Identity Manager 核心功能可以幫您將以上所有的任務 (以及更多任務) 自動化。以下功能 (工作流程、角色、證明、自助服務、稽核及報告) 使用企業規則所驅動的多重系統資料同步化，來實現使用者佈建與密碼管理這兩項 IT 組織中最困難、最耗時的任務所涉及之程序的自動化。

圖 1-1 Identity Manager 核心功能

後續幾節會介紹這些 Identity Manager 功能，及其如何協助您順利達成組織的身分識別管理需求：

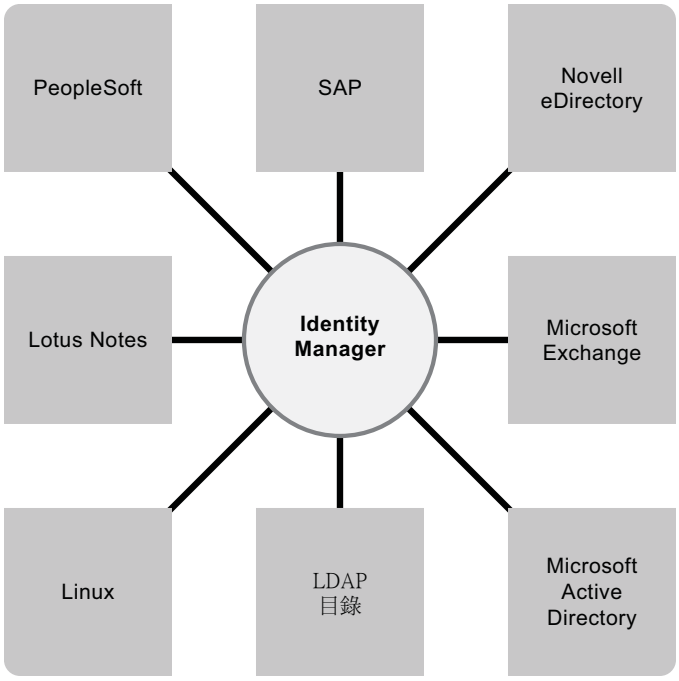
- 第 1.1 節「資料同步」(第 8 頁)
- 第 1.2 節「工作流程」(第 11 頁)
- 第 1.3 節「角色與證明」(第 12 頁)
- 第 1.4 節「自助服務」(第 13 頁)
- 第 1.5 節「稽核、報告及法規遵循」(第 14 頁)

1.1 資料同步

如果您的組織和大多數的組織一樣，則身分識別資料應該是儲存在多個系統中。亦或是會將身分識別資料儲存在您實際上會在另一個系統中使用的一個系統中。無論是何種方式，您都需要能夠在各系統之間輕鬆共享和同步資料。

Identity Manager 可讓您在多種應用程式、資料庫、作業系統及目錄 (例如 SAP、PeopleSoft、Salesforce、Microsoft SharePoint、Lotus Notes、Microsoft Exchange、Microsoft Active Directory、Novell eDirectory、Linux 與 UNIX、LDAP 目錄) 之間同步、轉換及配送資訊。

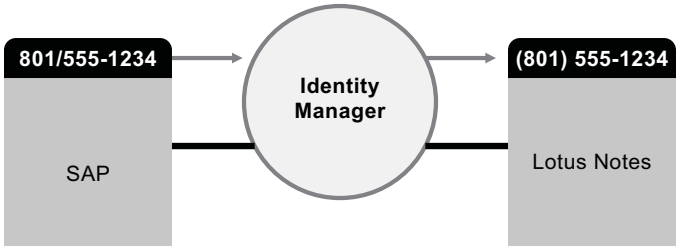
圖 1-2 連接多種系統的 Identity Manager



您可以控制連接的系統之間的資料流程。此外，您還可以決定要共享的資料、某項資料管理來源的系統，以及如何解譯和轉換資料才能符合其他系統的需求。

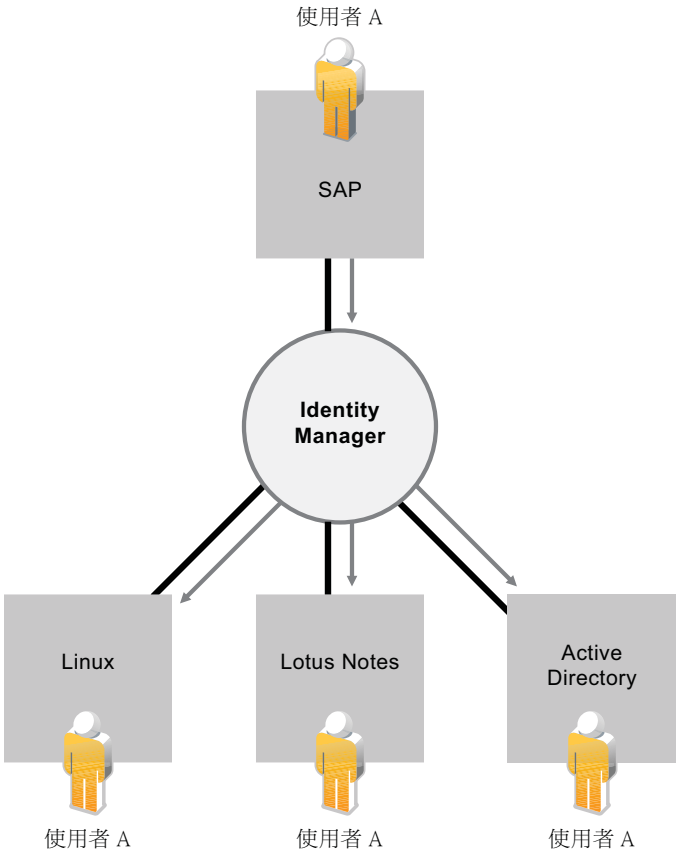
在下圖中，SAP HR 資料庫是使用者電話號碼的管理來源。因爲 Lotus Notes 系統也使用電話號碼，所以 Identity Manager 會將號碼轉換成必要的格式，再分享給 Lotus Notes 系統使用。每當電話號碼在 SAP HR 系統中一有變動，就會同步至 Lotus Notes 系統。

圖 1-3 連接的系統之間的資料同步



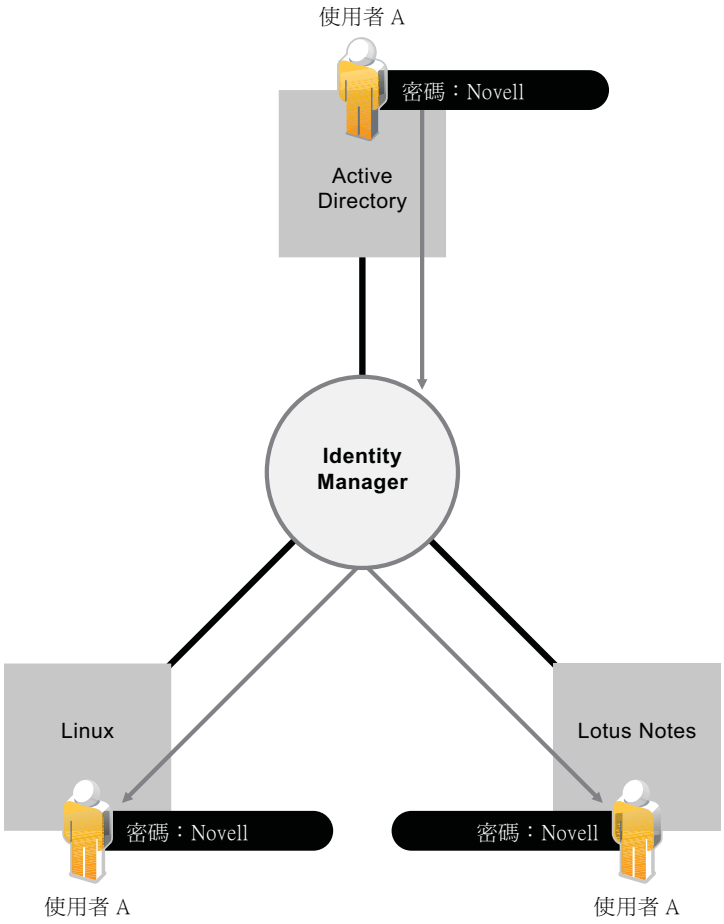
管理現有使用者的資料只是 Identity Manager 資料同步功能的開端。除此之外，Identity Manager 還可以在如 Active Directory 的目錄、PeopleSoft 和 Lotus Notes 的系統及 UNIX 與 Linux 作業系統中，建立新的使用者帳戶和移除現有的帳戶。例如，當您將新員工新增至 SAP HR 系統時，Identity Manager 可以自動在 Active Directory 中建立新的使用者帳戶、在 Lotus Notes 中建立新帳戶，以及在 Linux NIS 帳戶管理系統中建立新帳戶。

圖 1-4 在連接的系統中建立使用者帳戶



Identity Manager 功能之一的資料同步也可以協助您在系統之間同步密碼。例如，如果使用者在 Active Directory 中變更自己的密碼，Identity Manager 可以將這個密碼同步至 Lotus Notes 和 Linux。

圖 1-5 連接的系統之間的密碼同步

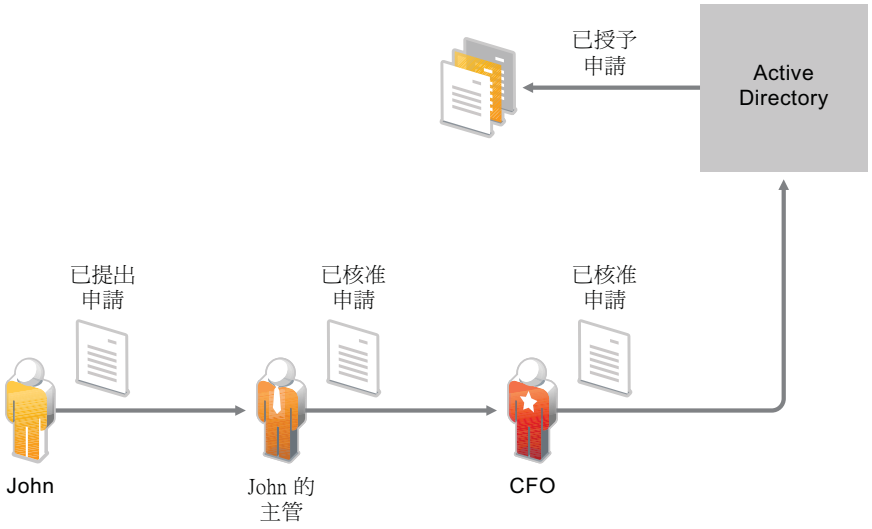


1.2 工作流程

使用者多半不須經過任何人的核准，就能存取組織中的許多資源。不過，存取其他資源可能會受到限制，需要經過一或多人的核准。

Identity Manager 提供工作流程功能，以確保您的提供程序有適當的資源核准人在把關。例如，假設已提供 John Active Directory 帳戶，他必須透過 Active Directory 來存取一些財務報告。這需要取得 John 的直屬主管和財務長的核准。幸好，您已經設好核准工作流程，可以將 John 的申請呈報給他的主管，等到主管核准之後，再呈報給財務長。財務長的核准會促成自動提供 John 存取和檢視財務文件所需的 Active Directory 權限。

圖 1-6 使用者提供的核准工作流程



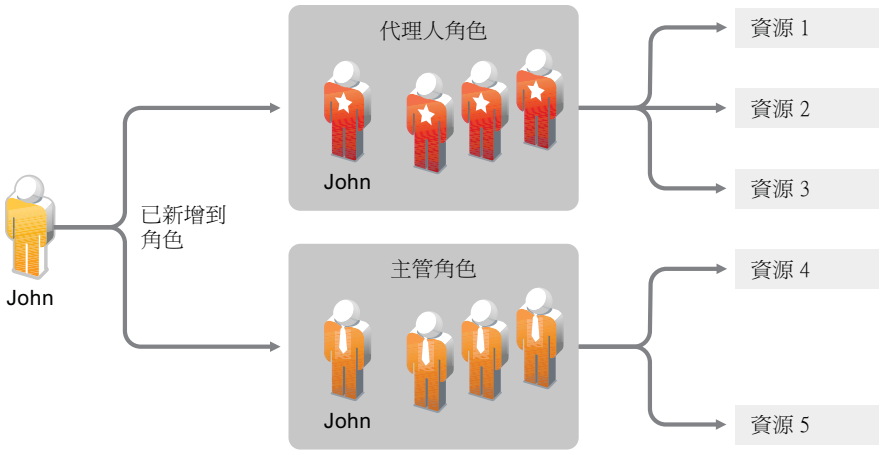
您可以在每當有某事件發生時 (例如，有新的使用者新增至您的 HR 系統) 就自動啓始工作流程，或是透過使用者申請來手動啓始。爲了確保適時進行核准，您可以設定代理核准人和核准小組。

1.3 角色與證明

使用者通常會根據自己在組織裡所扮演的角色來要求存取資源。例如，法律事務所的律師需要存取的資源，可能就與助理不一樣。

Identity Manager 可讓您根據使用者在組織裡的角色來提供使用者。您應該根據組織的需求來定義角色和進行指定。指定角色給使用者時，Identity Manager 就會將此角色關聯的資源存取權提供給使用者。如果爲一位使用者指定多個角色，該使用者就會獲得這些角色相關的資源存取權限，如下圖所示：

圖 1-7 資源的角色佈建



您可以透過組織中發生的事件讓使用者自動新增至角色中 (例如，職稱爲「代理人」的新使用者新增至 SAP HR 資料庫中)。如果需要核准才能將使用者新增至某個角色，您可以建立工作流程，將角色申請呈報給適當的核准人。您也可以手動指定使用者的角色。

在某些情況下，不應該將某些角色指定給同一人，因爲這些角色會發生衝突。Identity Manager 提供「職務分離」功能，可避免指定衝突的角色給使用者，除非組織中有人對衝突設定例外條件。

因爲角色指定可決定使用者在組織內對資源的存取，確保正確指定相當重要。不正確的指定會造成違背公司與政府法規的規定。Identity Manager 可透過證明程序，協助您驗證角色指定的正確性。組織裡的負責人員可以透過這個程序來證明與角色關聯的資料：

- **使用者設定檔證明：**選定的使用者證明自己的設定檔資訊 (名字、姓氏、職稱、部門、電子郵件等等)，並更正任何不正確的資訊。正確的角色指定需要有正確的設定檔資訊。
- **「職務分離」違規證明：**負責人員檢閱「職務分離」違規報告，並證明報告的正確性。報告中列出允許指定衝突角色給使用者的任何例外。
- **角色指定證明：**負責人員檢閱的報告中列出選定的角色及指定到每個角色的使用者、群組及角色。然後，負責人員必須證明資訊的正確性。
- **使用者指定證明：**負責人員檢閱一份列出選定的使用者和對這些使用者所指定角色的報告。然後，負責人員必須證明資訊的正確性。

這些證明報告主要是協助您確保角色指定正確，以及允許衝突角色的例外有明確的理由。

1.4 自助服務

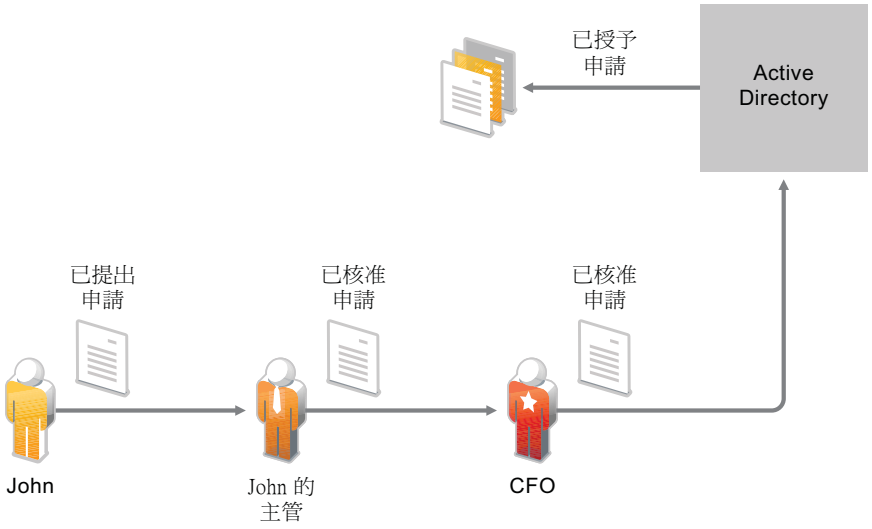
企業主管和部門可能想要自行管理使用者資訊和存取需求，而不想依賴您或您的幹部來管理。您一定常常聽到：「我爲什麼不能在公司目錄裡更改自己的手機號碼？」或是「我是行銷部門的人，爲什麼要打電話給服務台才能存取行銷資訊資料庫？」

透過 Identity Manager，您可以將管理職務委託給應負責的人。例如，您可以讓使用者個人：

- 管理自己在企業目錄中的個人資料。他們可以先在一個地方變更手機號碼，然後將此資料在您已透過 Identity Manager 同步的所有系統上進行變更，而不需由您來進行。
- 變更密碼、設定忘記密碼時的提示，以及設定忘記密碼時的安全問題和回應。他們可以在收到提示或回應安全密碼問題後自行重設，而不會因爲忘了密碼來要求您重設密碼。
- 要求存取資料庫、系統及目錄等資源。他們可以從可用的資源清單中選取應用程式，而不需打電話給您，申請應用程式的存取權。

除了使用者個人的自助服務以外，對於負責輔助、監看和核准使用者申請的職掌工作 (管理、「服務台」等等)，Identity Manager 還提供自助服務管理。例如，我們以第 1.2 節「工作流程」(第 11 頁) 中的情況爲例，如下所示。

圖 1-8 以自助服務提供工作流程



不只是 John 會使用 Identity Manager 自助服務功能來申請存取他所需的文件，John 的主管和財務長也會使用自助服務功能來核准申請。已建立的核准工作流程可讓 John 啓始並監看他的申請進度，也可讓 John 的主管和財務長回應他的申請。當 John 的主管和財務長核准申請時，就會促成提供 John 存取和檢視財務文件所需的 Active Directory 權限。

1.5 稽核、報告及法規遵循

如果沒有 Identity Manager，提供使用者就會變成一項繁重、費時又浪費成本的工作。但相較於驗證您的提供活動是否符合組織的政策、需求和法規，這項工作所花費的力氣還算是小事。每個人是否都適得其所，能夠存取正確的資源嗎？有沒有把不對的人擋在這些相同的資源之外？昨天到職的員工能夠存取網路、他的電子郵件及他的工作所需的其他六個系統嗎？是否已把上星期離職員工的存取取消？

有了 Identity Manager，您就輕鬆多了，因爲您的所有使用者佈建活動 (過去與現在的) 都會被追蹤並記錄下來，以備隨時稽核。Identity Manager 提供了一套智慧型資訊儲存機制，用於儲存組織中 Identity Vault 及受管理系統的實際狀態與希望的狀態。透過查詢倉儲，您可以擷取需要的所有資訊，以確保您所在組織完全遵守商業法律與法規。

該倉儲可讓您從各個角度檢視您的企業授權，並提供必要的知識供您查看授權過去的與現在的狀態，以及授予組織中各身分的許可。具備了這些知識，您甚至可以回答最爲複雜的組織治理、風險管理及法規遵循 (GRC) 方面的查詢。

Identity Manager 預先定義了一些報告，可讓您對身分資訊倉儲進行查詢，以瞭解業務、IT 及企業規則的法規遵循程度。如果預先定義的報告不符合您的需求，您也可以建立自定報告。

Identity Manager 4.0.1 的功能 2

Novell Identity Manger 4.0.1 提供了智慧型身分架構，它將您現有的 IT 資產與軟體即服務 (SaaS) 這樣的新運算模型完美融合，降低了成本並確保了實體、虛擬及雲端環境中的法規遵循。有了 Novell Identity Manager 解決方案，您就可以確保企業擁有最新的使用者身分資訊。您可以透過在防火牆內管理、佈建及取消佈建身分並延伸至雲端，掌握企業層級的控制權。Identity Manager 還可協助您將法規遵循管理延伸至雲端。

Identity Manager 4.0.1 提供了整合式身分管理、角色管理、報告及套件管理功能，可讓您預先設定和自定 Identity Manager 驅動程式規則。您還可以在各個系統網域中套用安全性規則。Identity Manager 可讓您管理不斷增加的法規要求中的使用者生命週期，並透過更具策略性的使用者佈建施加更細化的保護，以滿足防火牆內或雲端環境中日益增長的安全性需求。智慧型身分架構可協助您在現有的基礎架構上使用 SaaS 這類新運算模型。

2.1 Identity Manager 4.0.1 的新功能

- **資源申請活動：** 資源申請活動可讓您自動對使用者授予或撤銷資源。例如，您可以撰寫一個佈建申請定義，佈建新員工第一天工作所需的全部資源。使用資源申請活動，您便可以自動核准員工使用指定資源。如需資源申請活動的詳細資料，請參閱 *《User Application: Design Guide》*(使用者應用程式：設計指南) 中的 *「Resource Request Activity」*(資源申請活動)。
- **遙測：** Identity Manager 遙測是 Identity Manager 4.0.1 引入的一種全新工作。該工作可做爲使用量計數工具或授權監控工具，向 Identity Manager 客戶提供相關值，這樣他們便可新增更多授權或淘汰未使用的授權。客戶還可以使用像是未啓用使用者定價的有用功能。

  遙測工作用於收集所安裝的 Identity Manager 軟體與硬體的相關詳細資料，以及客戶環境中 Identity Manager 驅動程式的使用情況。客戶註冊 Novell Customer Center 後，該資訊就會傳送給 Novell。此資訊可讓 Novell 爲客戶提供更完善的支援，開發和測試 Identity Manager 時更有效率，並在未來制定重要決策。如需詳細資訊，請參閱 *《Identity Manager 4.0.1 Jobs Guide》*(Identity Manager 4.0.1 工作指南)。
- **報告：** Identity Reporting 模組中新增了以下報告：
  - **Identity Vault 中的使用者狀態變更：** 顯示與 Identity Vault 使用者相關的重要事件。
  - **Identity Vault 中的使用者密碼變更：** 顯示 Identity Vault 中的所有使用者密碼變更。
  - **按接收者列出的存取申請：** 按接收者分組顯示資源指定工作流程程序。
  - **按申請者列出的存取申請：** 按申請者分組顯示資源指定工作流程程序。
  - **按資源列出的存取申請：** 按資源分組顯示資源指定工作流程程序。

2.2 Identity Manager 4.0 的功能

除本節之前列出的新增功能之外，Identity Manager 4.0.1 還提供了以下 Identity Manager 4.0 中引入的功能。

- **全面的立即可用報告：** Novell Identity Manager 4.x 產品套裝的整合式報告模組提升了內部及雲端部署中法規遵循的可見度。該報告功能可讓您檢視使用者的身分狀態與存取權限，或有關使用者的動作與佈建歷程的報告。如需詳細資訊，請參閱 *《Identity Reporting Module Guide》*(Identity Reporting 模組指南)。
- **增強型整合：** 爲建立讓所有元件均位於同一部伺服器上的新 Identity Manager 解決方案，Novell Identity Manager 4.x 提供了一個整合式安裝程式，它可簡化安裝程序，讓您更快地設定系統。您無需分別安裝各個 Identity Manager 元件，只需使用整合式安裝程式，便可一次安裝所有元件。如需詳細資訊，請參閱 *《Identity Manager 4.0.1 整合式安裝指南》*。
- **套件管理：** Identity Manager 4.x 引入了一個新概念：套件管理。這是一個用於建立、配送及使用 Identity Manager 規則內容之高質量建置區塊的系統。如需 Identity Manager 套件的詳細資訊，請參閱 *《Designer 4.0.1 for Identity Manager 4.0.1 Administration Guide》*(Designer 4.0.1 for Identity Manager 4.0.1 管理指南) 中的 *「Configuring Packages」*(設定套件)。
- **雲端就緒的驅動程式：** 爲了與 SaaS 立即整合，Identity Manager 4.x 提供了數個驅動程式。這些驅動程式透過提供佈建、取消佈建、申請 / 核准程序、密碼變更、身分設定檔更新及報告等功能，實現與 SaaS 及代管解決方案的緊密整合。全新的 SharePoint 與 Salesforce.com 驅動程式可協助將企業身分整合至雲端應用程式。如需雲端就緒驅動程式的詳細資訊，請參閱 *《Identity Manager 4.0.1 Driver for Salesforce.com Implementation Guide》*(Identity Manager 4.0.1 Driver for Salesforce.com 實作指南) 與 *《Identity Manager 4.0.1 Driver for SharePoint Implementation Guide》*(Identity Manager 4.0.1 Driver for SharePoint 實作指南)。
- **內嵌式 Identity Vault ：** Novell Identity Manager 4.x 產品的架構包含一個選擇性的內建 Identity Vault，這樣您就不需要爲身分識別目的而單獨建立並管理一個目錄結構。此外，Novell Identity Manager 4.x 產品系列還提供了一些驅動程式，可將 Identity Vault 與您企業中的其他身分資訊儲存機制輕鬆整合，這些機制包括 Active Directory 或各種資料庫等。如需詳細資訊，請參閱 *《Identity Manager 4.0.1 整合式安裝指南》*。
- **簡化的身分與角色管理：** Novell Identity Manager 4.x 產品系列將不同角色儲存機制的整合簡化至一個統一位置，如此您就不需要分開管理身分資訊的來源。透過全新的直觀介面使用角色對應管理員，您甚至可以將協力廠商角色與設定檔對應到 Novell Identity Manager 4.x。如需詳細資訊，請參閱 *《Novell Identity Manager Role Mapping Administrator 4.0.1 User Guide》*(Novell Identity Manager 角色對應管理員 4.0.1 使用者指南)。
- **增強型工具：** Designer 是一項重要工具，它可提供商務與技術資訊，用於建立滿足您需求的 Identity Manager 解決方案。Designer 4.x 中有數個功能得到了增強。請參閱 *「新功能」*(http://www.novell.com/documentation/designer401/resources/whatsnew/index.html) 中的 Designer 增強功能清單。如需 Designer 功能與管理的資訊，請參閱 *《Designer 4.0.1 for Identity Manager 4.0.1 Administration Guide》*(Designer 4.0.1 for Identity Manager 4.0.1 管理指南)。此外，Identity Manager 還提供了一個可協助您簡化分析和清理資料程序的工具。如需詳細資訊，請參閱 *《Analyzer 4.0.1 for Identity Manager Administration Guide》*(Analyzer 1.2 for Identity Manager 管理指南)。

Identity Manager 系列

3

爲滿足不同的客戶需求，Identity Manager 系列劃分成以下三個不同的產品群組：

- Identity Manager Advanced Edition
- Identity Manager Standard Edition
- Compliance Management Platform

在 Identity Manager Advanced Edition 中，除了會提供 Identity Manager Standard Edition 中具備的 Identity Manager 功能外，還會提供一些其他功能。在 Compliance Management Platform 中，除了會提供 Identity Manager Advanced 與 Standard Edition 中具備的功能外，還會提供一些其他工具。

圖 3-1 *Identity Manager 產品群組*

若要比較 Advanced Edition 與 Standard Edition 中提供的 Identity Manager 功能，請參閱 Identity Manager 版本比較 (http://www.novell.com/products/identitymanager/features/identitymanager-version-comparison.html)。

- 第 3.1 節 「Identity Manager Advanced Edition」 (第 18 頁)
- 第 3.2 節 「Identity Manager Standard Edition」 (第 18 頁)
- 第 3.3 節 「Compliance Management Platform」 (第 20 頁)
- 第 3.4 節 「啓用 Identity Manager Standard Edition 與 Advanced Edition」 (第 20 頁)

3.1 Identity Manager Advanced Edition

Identity Manager 4.0.1 Advanced Edition 包含本產品的整套功能，主要用於企業級使用者佈建。它提供 Standard Edition 的身分自助服務功能，以及所有基於工作流程的佈建功能。Advanced Edition 可讓您啓始化工作流程核准程序、佈建角色與資源，以及使用法規遵循功能。Advanced Edition 還提供了工作儀表板。

Identity Manager 4.0.1 Advanced Edition 以單獨的 ISO 提供。

附註：Identity Manager 4.0.1 Advanced Edition 有一個 90 天的試用版套件。

3.2 Identity Manager Standard Edition

爲滿足不同的客戶需求，Novell 引入了 Identity Manager 4.0.1 Standard Edition。Standard Edition 包含 Identity Manager Advanced Edition 中提供的一部分功能。

Standard Edition 仍會提供舊版 Identity Manager 中的所有功能：

- 身分同步化
- 基於角色的自動化佈建
- 密碼管理與密碼自助服務
- 具有現有白頁和組織圖功能的身分自助服務

附註：Identity Manager Advanced Edition 與 Standard Edition 的整合模組均保持不變。

除前面的清單之外，Standard Edition 還包含 Advanced Edition 中提供的以下功能：

- 使用者介面的外觀與操作
- 報告模組
- 內容封裝架構
- 支援 REST API 和單一簽入 (SSO)
- 用於資料重整的 Analyzer 工具

Identity Manager 4.0.1 Standard Edition 以單獨的可下載 ISO 提供。若要從 Standard Edition 升級至 Advanced Edition，請使用 Identity Manager Advanced Edition ISO。您需要套用正確的啓用碼才能升級至 Advanced Edition。如需從 Standard Edition 升級至 Advanced Edition 的詳細資訊，請參閱 *《Identity Manager 4.0.1 Upgrade and Migration Guide》*(Identity Manager 4.0.1 升級與移轉指南)。

使用 Identity Manager Standard Edition ISO 無法從現有的 Identity Manager Advanced Edition 切換。若要從 Identity Manager Advanced Edition 切換至 Standard Edition，請先解除安裝伺服器上的 Advanced Edition，然後安裝 Identity Manager 媒體中的 Standard Edition ISO。

Identity Manager Standard Edition 中未提供以下功能：

- 未提供角色對應管理員 (RMA)。

- 以下限制適用於使用者應用程式：
  - **「身分自助服務」索引標籤是業務使用者唯一可以使用的索引標籤：** 在 Standard Edition 中，如果以業務使用者身分登入使用者應用程式，則「*身分自助服務*」索引標籤是您唯一可見的索引標籤。如果以使用者應用程式管理員身分登入，您還會看到「*管理*」索引標籤。
  - **不支援角色與資源：** 要使用角色與資源，則需要安裝 Advanced Edition。Standard Edition 中未提供「*角色與資源*」索引標籤。
  - **不支援「法規遵循」索引標籤：**「*法規遵循*」索引標籤需要安裝 Identity Manager 4.0.1 Advanced Edition 才能使用。Standard Edition 中未提供「*法規遵循*」索引標籤。
  - **未提供「工作儀表板」：** Standard Edition 中未提供「*工作儀表板*」索引標籤。
  - **不支援自定角色：** 未提供定義自定角色功能。Standard Edition 僅支援系統角色。
  - **不支援工作流程：** 不支援啓始化核准工作流程的功能。
  - **REST API ：** 未提供與角色、資源、工作流程等相關的 REST API。
  - **簡化了安全性模型：** Standard Edition 以細化層級提供安全性模型，以免意外使用 Advanced Edition 中提供的功能。您只需要指定以下管理員角色：
    - **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。這包括存取 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。
    - **報告管理員：** 此使用者擁有報告網域內的所有功能。報告管理員可以對報告網域內的所有物件執行所有動作。
    - **安全性管理員：**此角色爲成員賦予安全性網域內的所有功能。安全性管理員可以對安全性網域內的所有物件執行所有允許的動作。此角色可以委託並授予使用者存取所有 Identity Manager Advanced Edition 功能的權限，因此，該角色有別於使用者應用程式管理與報告管理角色。

    附註：出於測試目的，Novell 不會在 Standard Edition 中鎖定安全性模型。因此，安全性管理員可以指定所有網域管理員、委託管理員及其他安全性管理員。不過，線上環境中不支援使用這些進階功能，如一般使用者授權合約中所述。在線上環境中，所有管理員指定均受授權限制。Novell 可以將監控資料收集到稽核資料庫中，以確保線上環境遵循法規。此外，Novell 還建議只對一位使用者授予安全性管理員許可權。

    如需使用者應用程式功能的詳細資訊，請參閱 *《Identity Manager Roles Based Provisioning Module 4.0 User Application: Administration Guide》* (Identity Manager Roles Based Provisioning Module 4.0 使用者應用程式：管理指南)。
- 以下限制適用於 Identity Reporting 模組：
  - **受管理系統閘道驅動程式會禁用：** 受管理系統閘道驅動程式可在 Identity Manager 4.0.1 中從已啓用資料收集的任何受管理系統提取資訊，只要該系統支援授權。

    Identity Manager Standard Edition 中禁用了受管理系統閘道驅動程式。
  - **報告僅顯示 Identity Vault 資料：** Identity Manager Standard Edition 產生的報告僅顯示 Identity Vault 資料，不顯示受管理 (已連接) 系統的相關資料。
  - **報告不顯示歷史資料：** Standard Edition 未對報告提供收集歷史狀態資料的功能。使用 Standard Edition 只能檢視目前的狀態資料。
  - **未提供部分報告：** Identity Manager 4.0 與 4.0.1 中新增了數個新報告。Standard Edition 未提供適用於連接的系統與歷史資料的報告。

- **部分報告不含資料：** 僅當您購買了 Identity Manager Advanced Edition，有些報告才能正常運作，因爲這些報告使用的是 Standard Edition 中未提供的資料，例如角色、資源及工作流程程序。

3.3 Compliance Management Platform

Novell Compliance Management Platform 透過一套可簡化解決方案實作與管理程序的可靠工具，將 Novell 身分識別、存取和安全性管理產品集於一體。本平台將身分識別與存取資訊以及安全性資訊和事件管理技術加以整合，針對企業上下的所有網路事件提供即時而全面的檢視。這樣緊密的整合提供了強大的風險管理能力，確保企業規則能轉化爲自動的 IT 實務。如需詳細資訊，請造訪 Comliance Management Platform 網站 (http://www.novell.com/documentation/ncmp10/)。

3.4 啓用 Identity Manager Standard Edition 與 Advanced Edition

您必須在安裝 Identity Manager Advanced Edition 與 Standard Edition 後的 90 天內啓用產品，否則它們將會停用。Identity Manager Advanced Edition 與 Standard Edition ISO 在 90 天內會正常運作。您可在 90 天內的任意時間或在 90 天內之後，選擇啓用 Identity Manager 產品。如需詳細資訊，請參閱 *《Identity Manager 4.0.1 架構安裝指南》*中的「啓用 Novell Identity Manager 產品」。

若將 Standard Edition 啓用碼套用至未啓用的現有 Advanced Edition 系統，Metadirectory 伺服器與驅動程式會停止運作。

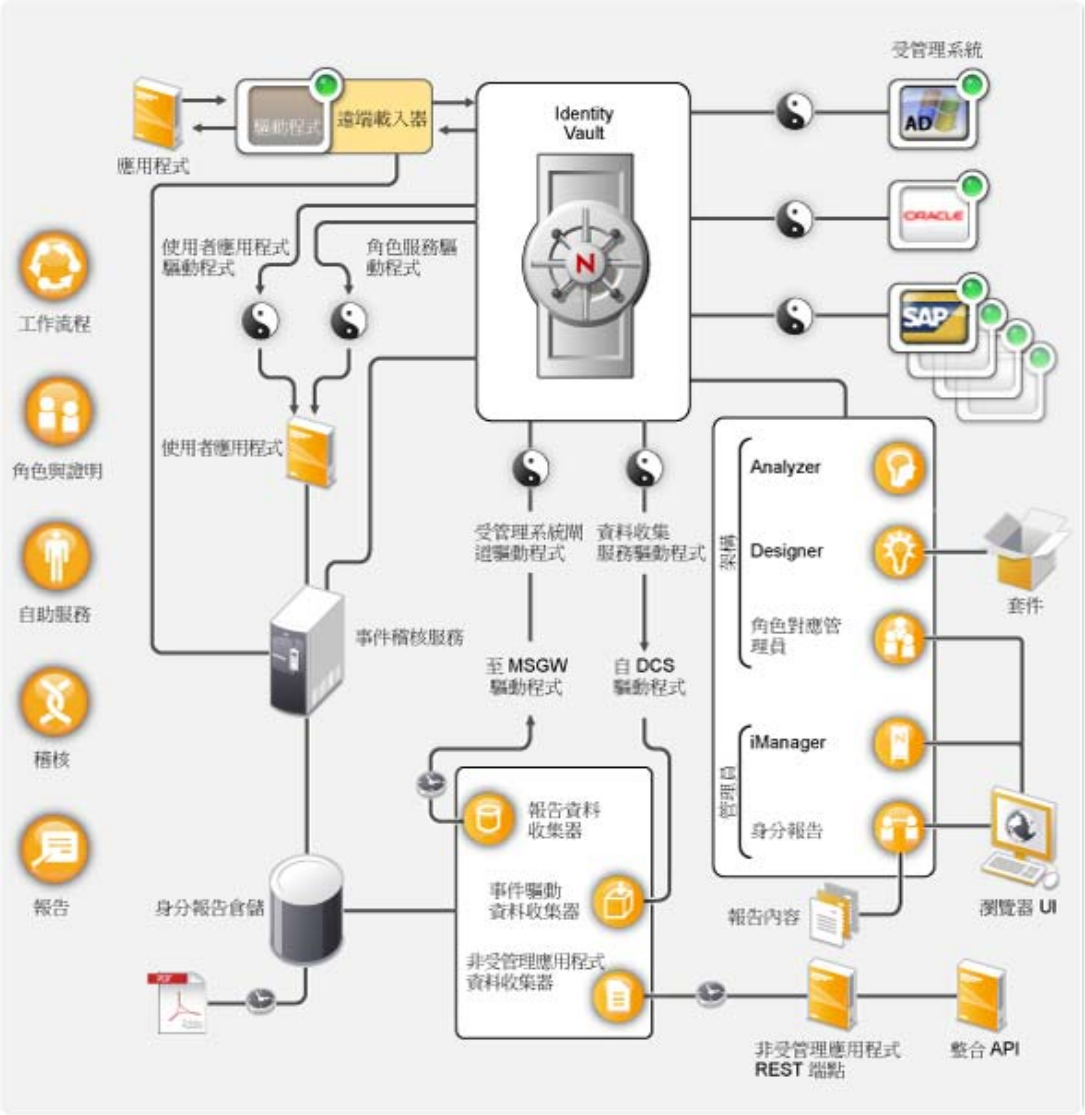
附註：如果既安裝了 Identity Manager Advanced Edition，又安裝了 Identity Manager Standard Edition，請確保在正確的伺服器上使用正確的啓用碼。

Identity Manager 架構

4

下圖顯示了高階架構元件，這些元件提供第 1 章 「Identity Manager 與企業流程自動化」 (第 7 頁) 中介紹的 Novell Identity Manager 功能：資料同步、工作流程、角色、證明、自助服務及稽核 / 報告。

圖 4-1 *Identity Manager 高階架構*



下列幾節介紹其中每一個元件：

- 第 4.1 節 「資料同步」 (第 22 頁)
- 第 4.2 節 「工作流程、角色、證明與自助服務」 (第 25 頁)
- 第 4.3 節 「稽核與報告」 (第 27 頁)

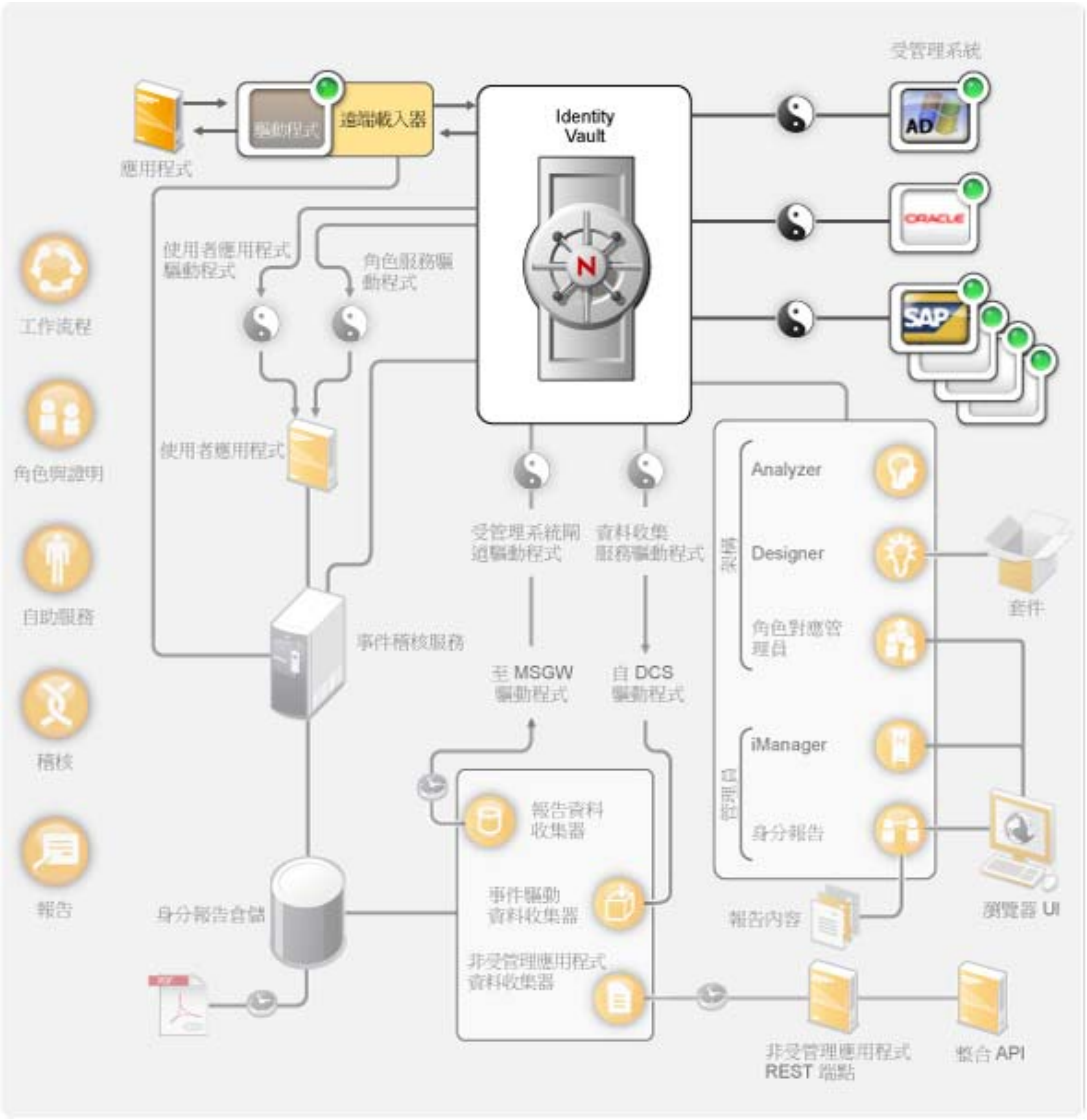
4.1 資料同步

資料同步提供自動化企業流程的基礎。以最簡單的形式來說，資料同步是指資料從已變更資料項目的位置移動到需要資料項目的其他位置。例如，假設在公司的人力資源系統中，員工的電話號碼有所變動，則在儲存員工電話號碼的所有其他系統上，會自動反映這一變更。

Identity Manager 不只是會同步身分識別資料，Identity Manager 還能同步儲存在連接的應用程式或 Identity Vault 中任何類型的資料。

資料同步 (包括密碼同步) 是由 Identity Manager 解決方案的五個基本元件所提供：Identity Vault、Identity Manager 引擎、驅動程式、遠端載入器及連接的應用程式。下圖顯示這些元件。

圖 4-2 *Identity Manager 架構元件*



下列幾節說明每一個元件，並爲您解說在組織裡的各系統之間有效地同步資料所應該瞭解的概念：

4.1.1 元件

Identity Vault：Identity Vault 可做爲您在應用程式之間要同步的資料的 Metadirectory。例如，從 PeopleSoft 系統同步至 Lotus Notes 的資料會先新增至 Identity Vault，然後再傳送至 Lotus Notes 系統。此外，Identity Vault 還會儲存 Identity Manager 的特定資訊，例如驅動程式組態、參數和規則。Novell eDirectory 用於 Identity Vault。

Identity Manager 引擎 : 當 Identity Vault 或連接的應用程式中的資料發生變更時，Identity Manager 引擎會負責處理變更。對於 Identity Vault 中發生的事件，引擎會處理變更，並透過驅動程式發出指令給應用程式。對於應用程式中發生的事件，引擎會接收驅動程式送來的變更、處理變更，然後發出指令給 Identity Vault。Identity Manager 引擎也稱爲 Metadirectory 引擎。

驅動程式：驅動程式會連接至您要管理身分識別資訊的應用程式。驅動程式有兩項基本責任：將應用程式中的資料變更 (事件) 回報給 Identity Manager 引擎；將 Identity Manager 引擎所提交的資料變更 (指令) 貫徹到應用程式。

遠端載入器：驅動程式也必須安裝到連接的應用程式所在的相同伺服器上，並加以執行。如果應用程式和 Identity Manager 引擎位於同一部伺服器上，則您只要在這部伺服器上安裝驅動程式即可。但如果應用程式和 Identity Manager 引擎不在同一部伺服器上 (換言之，應用程式在引擎伺服器遠端，不在本端)，您必須在應用程式的伺服器上安裝驅動程式和遠端載入器。遠端載入器會載入驅動程式，並代表驅動程式與 Identity Manager 引擎進行通訊。

應用程式：驅動程式所連接的系統、目錄、資料庫或作業系統。應用程式必須提供 API，供驅動程式用來判斷應用程式資料的變更，然後使應用程式資料變更生效。應用程式通常稱爲「*連接的系統*」。

4.1.2 重要概念

通道：在 Identity Vault 與連接的系統之間，資料會沿著兩條不同的「*通道*」流動。「*訂閱者通道*」提供從 Identity Vault 至連接的系統之間的資料流程，換言之，連接的系統會訂閱 Identity Vault 中的資料。「*發行者通道*」提供從連接的系統至 Identity Vault 之間的資料流程，換言之，連接的系統會將資料發行至 Identity Vault。

資料表示法：資料是以「*XML 文件*」的形式在通道中流動。當 Identity Vault 或連接的系統中發生變更時會建立 XML 文件。XML 文件會傳送至 Identity Manager 引擎，該引擎會根據與驅動程式通道關聯的一組過濾器和規則來處理文件。完成對 XML 文件的所有處理後，Identity Manager 引擎會利用文件來對 Identity Vault (發行者通道) 啓始化適當的變更，或是驅動程式會利用文件，在連接的系統 (訂閱者通道) 中啓始化適當的變更。

資料管理：當 XML 文件流經驅動程式通道時，文件資料會受到與通道關聯「*規則*」的影響。

原則可用在許多方面，包括變更資料格式、在 Identity Vault 與連接的系統之間對應屬性、根據條件封鎖資料流程、產生電子郵件通知，以及修改資料變更的類型。

資料流程控制：*過濾器* (或稱爲「*過濾器規則*」) 可控制資料流程。過濾器會指定在 Identity Vault 與連接的系統之間要同步的資料項目。例如，系統之間通常會同步使用者資料。因此，大多數連接的系統的過濾器中會列出使用者資料。不過，對大多數應用程式而言，印表機通常不是很重要，因此在大多數連接的系統的過濾器中，並不會出現印表機資料。

在 Identity Vault 與連接的系統之間，每一種關係都有兩個過濾器：「訂閱者」通道上的過濾器可控制從 Identity Vault 至連接的系統之間的資料流程，以及「發行者」通道上的過濾器則可控制從連接的系統至 Identity Vault 之間的資料流程。

管理來源：與身分識別關聯的大多數資料項目都有一個概念擁有者。資料項目的擁有者就是該項目的「*管理來源*」。一般而言，只有資料項目的管理來源才能變更資料項目。

例如，企業電子郵件系統通常就是員工電子郵件地址的管理來源。如果企業白頁目錄的管理員變更該系統某位員工的電子郵件地址，則此變更對於員工是否實際上收到已變更之地址的電子郵件並不會有影響，因爲必須在電子郵件系統中進行變更才有效。

Identity Manager 使用過濾器來指定項目的管理來源。例如，如果在 PBX 系統與 Identity Vault 之間的關係過濾器允許員工的電話號碼從 PBX 系統流入 Identity Vault，但不允許從 Identity Vault 流入 PBX 系統，則 PBX 系統就是電話號碼的管理來源。如果其他所有連接的系統關係只允許電話號碼從 Identity Vault 流至連接的系統，但反向則不允許，實際結果爲 PBX 系統在企業中是員工電話號碼的唯一管理來源。

自動化佈建：自動化佈建是指 Identity Manager 產生使用者佈建動作的能力，而不僅僅是簡單的資料項目的同步而已。

例如，在一般的 Identity Manager 系統中，人力資源資料庫是大部分員工資料的管理來源，將員工新增至 HR 資料庫會促成在 Identity Vault 中自動建立對應的帳戶。建立 Identity Vault 帳戶又進而促成在電子郵件系統中自動建立員工的電子郵件帳戶。用來提供電子郵件系統帳戶的資料取自於 Identity Vault，並且可能包含員工姓名、所在位置、電話號碼等等。

您有許多方法可以控制帳戶、存取和資料的自動提供，包括：

- **資料項目值：** 例如，各大樓的存取資料庫帳戶的自動建立，可利用員工所在位置屬性的值加以控制。
- **核准工作流程：**例如，在財務部門建立員工會促成自動傳送電子郵件給財務部門主管，要求核准在財務系統中建立新的員工帳戶。接著從電子郵件中引導財務部門主管開啓可讓其核准或拒絕申請的網頁。如果核准，則會促成在財務系統中自動建立員工的帳戶。
- **角色指定：** 例如，授予員工「會計」角色。Identity Manager 會透過系統工作流程 (沒有人工介入) 或人工核准流程 (或是雙管齊下)，提供員工指定給「會計」角色的所有帳戶、存取和資料。

授權：授權代表連接的系統中的某項資源，例如帳戶或群組成員資格。當使用者符合在連接的系統的授權所建立的準則時，Identity Manager 就會處理使用者的事件，結果就會授予使用者資源的存取。當然，所有的規則都必須完備，才能啓用資源的存取。例如，如果使用者符合 Active Directory 中 Exchange 帳戶的準則，則 Identity Manager 引擎會透過一組提供 Exchange 帳戶的 Active Directory 驅動程式規則來處理使用者。

授權的主要好處在於，您只需要在一個授權中定義存取資源的商業邏輯，而不需在多個驅動程式規則中定義。例如，您可以定義一個「帳戶」授權，在四個連接的系統中給予使用者帳戶。是否提供帳戶給使用者取決於授權，這意味著這四個驅動程式的規則都不需要包含業務邏輯。相反地，規則只需要提供授予帳戶的機制。如果您需要變更商業邏輯，則只要在授權中變更即可，不需在每一個驅動程式中變更。

工作：在大多數情況下，Identity Manager 會因應資料變更或使用者申請來採取動作。例如，當一個系統中有某一項資料變更時，Identity Manager 會在另一個系統中變更對應的資料。或者，當使用者申請存取系統時，Identity Manager 會啓始適當的程序 (工作流程、資源提供等等) 來提供存取。

「工作」可讓 Identity Manager 執行不是由資料變更或使用者申請所啓始的動作。工作是由儲存在 Identity Vault 中的組態資料及一段對應的實作程式碼組成。Identity Manager 包含一些預先定義的工作，這些工作可執行的動作包括啓動或停止驅動程式、傳送密碼過期電子郵件通知，以及檢查驅動程式的狀態等。您也可以實作自定工作來執行其他動作；在自定工作中，您 (或開發人員 / 顧問) 需要建立必要的程式碼來執行所要的動作。

工作順序：只要 Identity Vault 或連接的應用程式中的資料一有變動，通常就會馬上處理。工作順序可讓您排定要在特定日期與時間執行的任務。例如，已雇用一位新員工，但排定在一個月後才上班。需要將這位員工新增至 HR 資料庫，但在到職日之前，不應授予任何企業資源 (電子郵件、伺服器等等) 的存取權。如果沒有工作順序，就會立即授予員工存取。只要實作工作順序，就會建立一個只有在到職日才會啓始帳戶提供的工作順序。

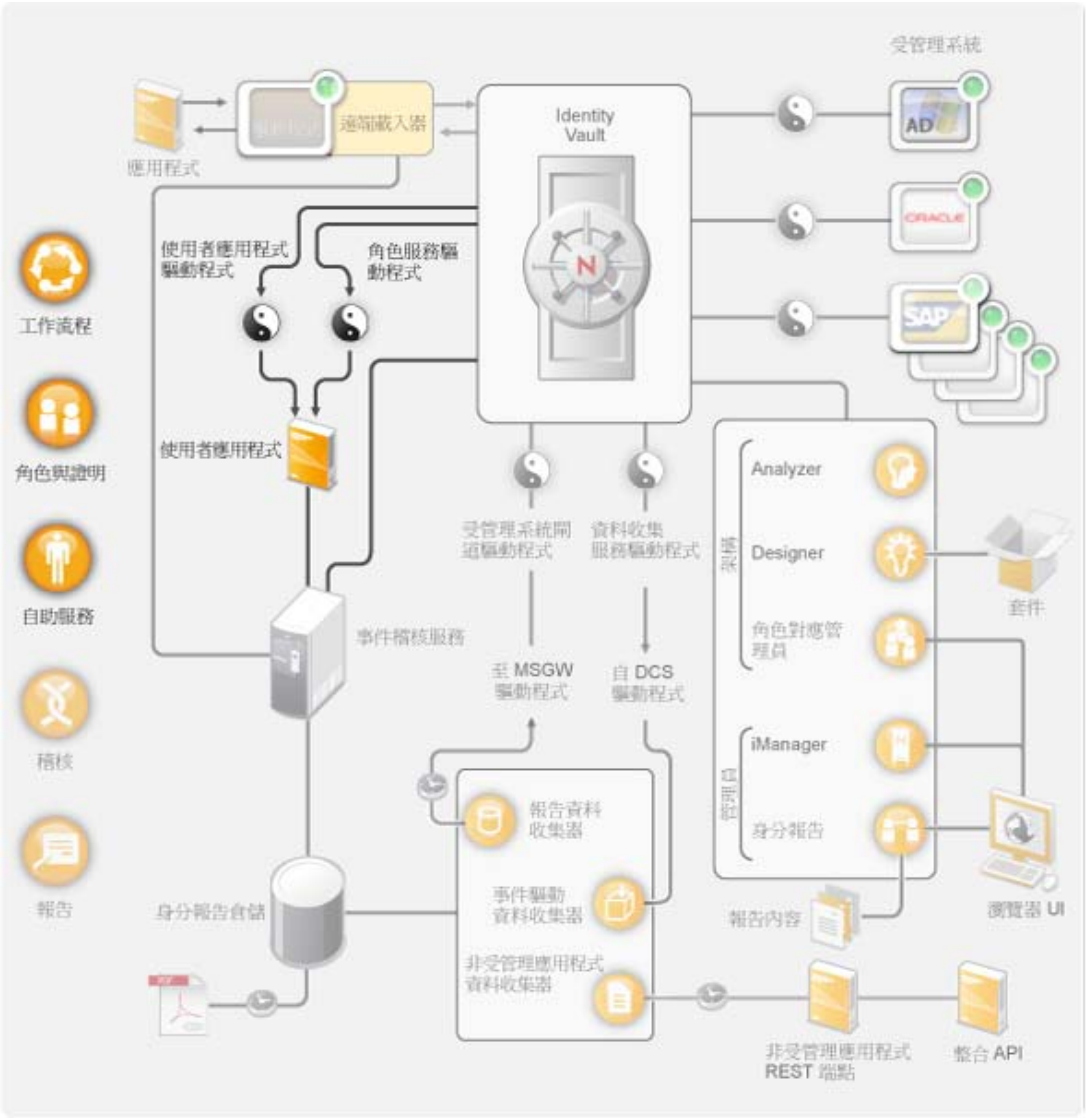
4.2 工作流程、角色、證明與自助服務

Identity Manager 提供一個專業的應用程式，即「使用者應用程式」，它提供了核准工作流程、角色指定、證明和身分自助服務。

標準的「使用者應用程式」隨附於 Identity Manager 中。標準版提供密碼自助服務 (幫助使用者記住密碼或重設忘記的密碼)、組織圖 (管理使用者目錄資訊)、使用者管理功能 (允許在 Identity Vault 中建立使用者)，以及基本的身分自助服務 (例如管理使用者設定檔資訊)。

使用者應用程式 Roles Based Provisioning Module 是 Identity Manager 4.0.1 Advanced Edition 的一部分。它包含一個標準的使用者應用程式，具有進階自助服務、核准工作流程、角色佈建、職務分離條件約束和證明功能。Identity Manager 4.0.1 Advanced Edition 包含標準功能及角色佈建模組功能。

圖 4-3 Identity Manager 使用者應用程式



下列幾節說明每一個元件，並爲您解說在組織裡的各系統之間有效地實作和管理元件所應該瞭解的概念：

- 第 4.2.1 節「元件」(第 26 頁)
- 第 4.2.2 節「重要概念」(第 27 頁)

4.2.1 元件

使用者應用程式：「使用者應用程式」是在瀏覽器中執行的 Web 應用程式，可讓使用者和企業管理員執行各種身分自助服務和角色提供任務，包括管理密碼和身分識別資料、啓始和監看提供和角色指定申請、管理提供申請的核准程序，以及驗證證明報告。它包含工作流程引擎，可在適當的核准程序中控制申請的呈交。

使用者應用程式驅動程式：「使用者應用程式」驅動程式會儲存組態資訊，且只要 Identity Vault 中一有變動，就會通知「使用者應用程式」。也可以將它設爲允許 Identity Vault 中的事件觸發工作流程，並向「使用者應用程式」回報工作流程的提供活動是成功或失敗，以便使用者檢視其申請的最終狀態。

角色與資源服務驅動程式：「角色與資源服務」驅動程式可管理所有角色與資源指定、啓動工作流程來處理需要核准的角色與資源指定申請，以及根據群組和容器成員資格來維護間接角色指定。該驅動程式還會根據使用者的角色成員資格，向使用者授予和撤銷授權，並對已完成的申請執行清理程序。

4.2.2 重要概念

工作流程爲主的提供：「工作流程爲主的提供」可讓使用者申請對資源的存取。提供申請會經由預先定義的工作流程來呈遞，可能包含需經過一人或多人的核准。只要授予所有核准，使用者就會收到資源的存取。爲因應 Identity Vault 中發生的事件，也可以間接地啓始提供申請。例如，將使用者新增至群組可能會啓始申請，要求將特定資源的存取授予使用者。

角色佈建：「角色佈建」可以根據指定給使用者的角色，讓使用者獲得特定資源的存取權限。可以指定一或多個角色給使用者。如果角色指定需要核准，則指定申請會啓動工作流程。

權限分散：爲了避免將衝突的角色給指定使用者，「使用者應用程式 Roles Based Provisioning Module」提供一項「職務分離」功能。您可以建立用於定義哪些角色將會衝突的職務分離條件約束。當角色發生衝突時，職務分離核准人可以核准或拒絕條件約束的任何例外。核准的例外會記錄成職務分離違規，可透過以下說明的證明程序來檢閱。

角色管理：必須由已指定了「角色模組管理員」和「角色管理員」系統角色的人員來管理角色。

「角色模組管理員」可以建立新的角色、修改現有的角色及移除角色；修改角色之間的關係、授予或撤銷使用者的角色指定；以及建立、修改及移除「職務分離」條件約束。

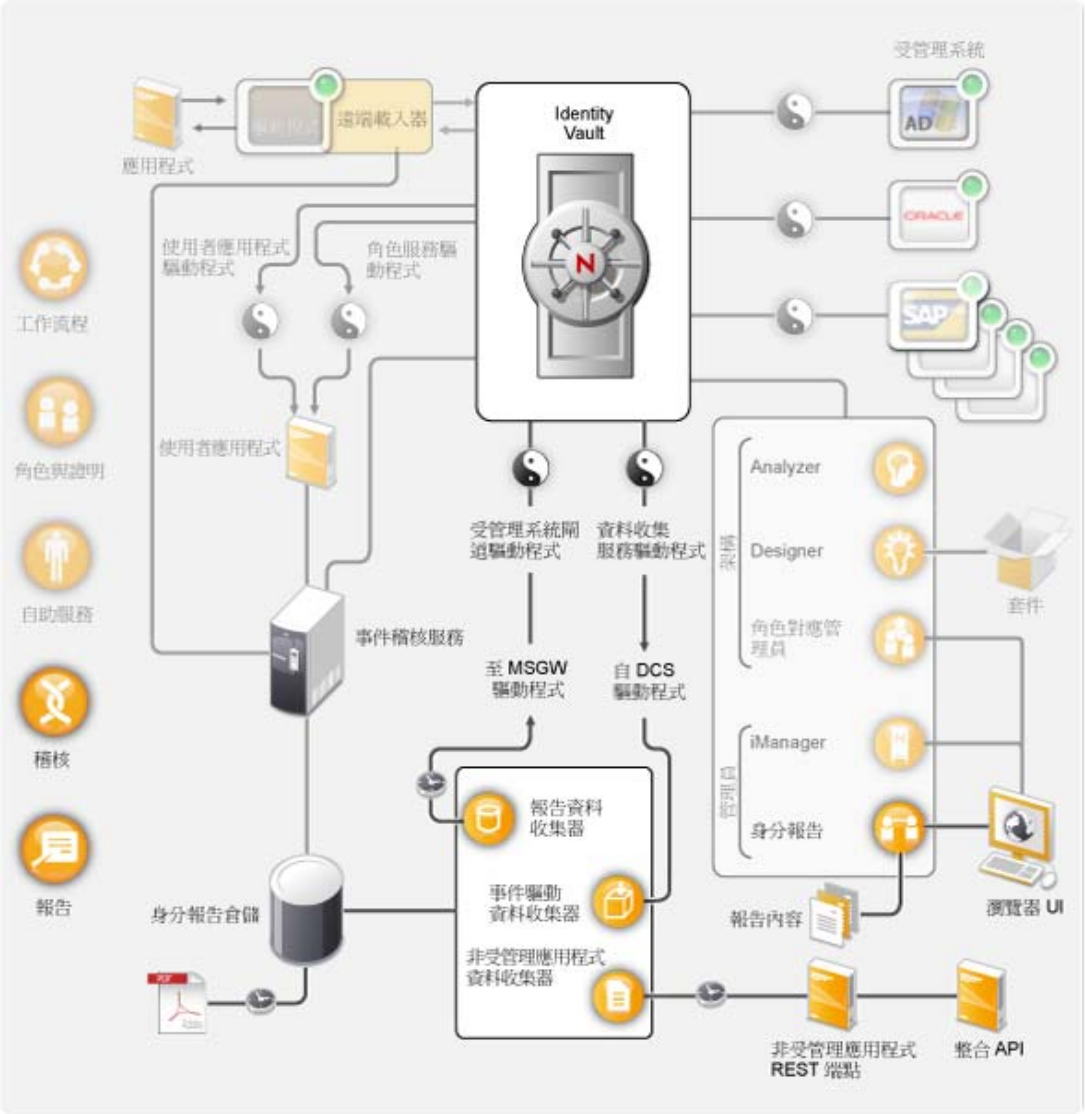
「角色管理員」可以做的事與「角色模組管理員」相同，但無法管理「職務分離」條件約束、設定「角色」系統及執行所有報告。「角色模組管理員」在「角色」系統內的活動範圍不受限制，而「角色管理員」範圍則局限於明確指定的使用者、群組和角色。

證明：角色指定可決定使用者在組織內的資源存取，指定不正確會違反公司和政府的法規。Identity Manager 可透過證明程序，協助您驗證角色指定的正確性。透過這個程序，使用者個人可以驗證自己的設定檔資訊，而「角色管理員」可以驗證角色指定和職務分離違規。

4.3 稽核與報告

Identity Reporting 模組提供了稽核與報告功能，這是 Identity Manager 4.0.1 的一項新功能，如下圖所示。

圖 4-4 Identity Manager 稽核與報告



Identity Reporting 模組可產生顯示關於 Identity Manager 各方面組態之重要企業資訊的報告，包括從 Identity Vault 及受管理系統 (例如 Active Directory 或 SAP) 收集的資訊。Identity Reporting 模組使用以下元件來管理資料：

事件稽核服務： 擷取與報告模組中執行的動作 (例如輸入、修改、刪除或排程報告) 關聯之記錄事件的服務。事件稽核服務 (EAS) 會擷取與 Roles Based Provisioning Module (RBPM) 及角色對應管理員 (RMA) 中執行之動作關聯的記錄事件。

身分資訊倉儲： 以下資訊類型的儲存機制：

- 報告管理資訊 (例如報告定義、報告排程及完成的報告)、用於執行報告的資料庫檢視窗以及組態資訊。
- 報告資料收集器、事件驅動資料收集器及非受管理應用程式資料收集器所收集的身分資料。
- 稽核資料，包括事件稽核服務收集的事件。

身分資訊倉儲將其資料儲存於 Security Information and Event Management (SIEM) 資料庫中。

資料收集服務： 從組織內的各個來源收集資訊的服務。資料收集服務包含以下三項子服務：

- **報告資料收集器：** 使用提取設計模型從一或多個 Identity Vault 資料來源擷取資料。收集動作會定期執行，具體時間由一組組態參數決定。爲了擷取資料，收集器會呼叫受管理系統閘道驅動程式。
- **事件驅動資料收集器：** 使用推送設計模型蒐集資料收集服務驅動程式所擷取的事件資料。
- **非受管理應用程式資料收集器：** 透過呼叫專爲每個非受管理應用程式撰寫的 REST 端點，從一或多個應用程式擷取資料。非受管理應用程式是指企業內未連接至 Identity Vault 的應用程式。如需詳細資訊，請參閱 *Identity Reporting Module Guide*(Identity Reporting 模組指南) 中的「REST Services for Reporting」(用於報告的 REST 服務)。

資料收集服務驅動程式： 擷取儲存於 Identity Vault 中之物件 (例如帳戶、角色、資源、群組及團隊成員) 變更的驅動程式。資料收集服務驅動程式會向資料收集服務自身進行註冊，並將變更事件 (例如資料同步、新增、修改及刪除事件) 推送至資料收集服務。

擷取的資訊記錄了以下物件的變更：

- 使用者帳戶與身分
- 角色與角色層級
- 群組

  附註：報告模組不支援動態群組，僅會產生靜態群組資料的相關報告。

- 群組成員
- 佈建申請定義
- 職務分離定義與違規
- 使用者授權關聯
- 資源定義與資源參數
- 角色與資源指定
- Identity Vault 授權、授權類型及驅動程式

受管理系統閘道驅動程式： 從受管理系統收集資訊的驅動程式。爲了擷取受管理系統資料，驅動程式會查詢 Identity Vault。擷取的資料包括下列內容：

- 所有受管理系統的清單
- 所有受管理系統帳戶的清單
- 受管理系統的授權類型、值、指定及使用者帳戶設定檔

身分報告： 報告模組的使用者介面便於您將報告排程在非高峰時間執行，從而最佳化效能。如需 Identity Reporting 模組的詳細資訊，請參閱 *《Identity Reporting Module Guide》*。

報告：Identity Manager 預先定義了一些報告，能以有效、可用的方式顯示身分資訊倉儲中的資訊。您也可以建立自定報告。如需報告的詳細資訊，請參閱 *《Using Identity Manager 4.0 Reports》*(使用 Identity Manager 4.0 報告)。如需自定報告的相關資訊，請參閱 *《Identity Reporting Module Guide》*(Identity Reporting 模組指南) 中的「Creating Custom Report Definitions」(建立自定報告定義)。

非受管理應用程式 REST 端點： 非受管理應用程式是指未連接至 Identity Vault 但包含您要報告之資料的應用程式。透過爲應用程式定義 REST 端點，報告模組便可從此應用程式收集資料。

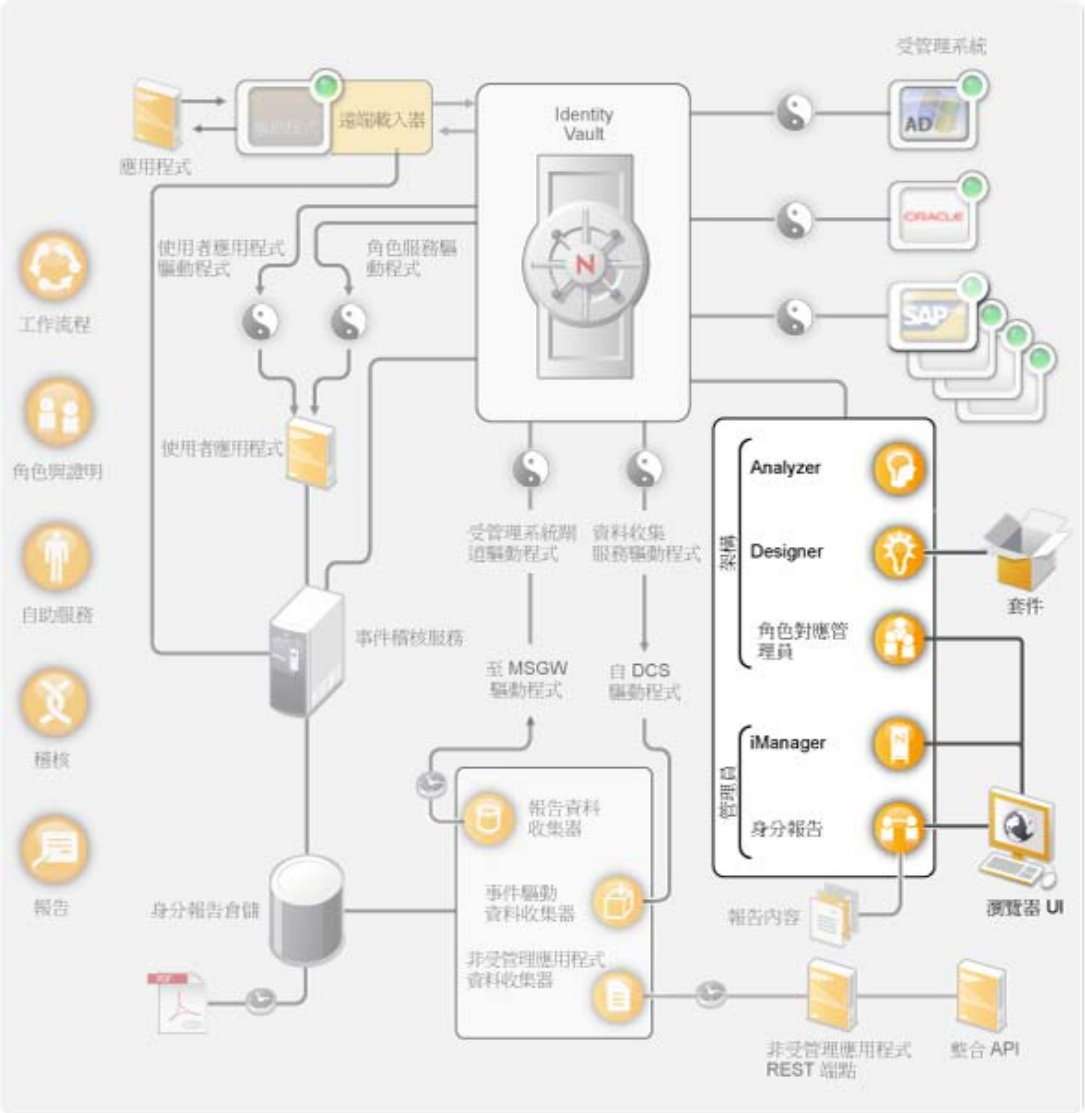
整合 API ： Identity Reporting 模組提供一組 REST API，用於爲非受管理應用程式實作 REST 端點，此外還能撰寫自定報告應用程式。

Identity Manager 工具

5

Identity Manager 提供了一些工具，可協助您建立並維護 Identity Manager 解決方案。每個工具都有其特定的功能。

圖 5-1 *Identity Manager 工具*



您可以使用 Designer 在離線環境下設計、建立並設定 Identity Manager 系統，然後再將所做的變更部署至線上系統。Designer 還爲您提供套件管理功能，可讓您預先設定和自定 Identity Manager 驅動程式規則。建立 Identity Manager 解決方案時則可使用 Analyzer 來分析、清理並準備要同步的資料。

角色對應管理員可用於建立和管理整個 Identity Manager 解決方案中的各個角色。

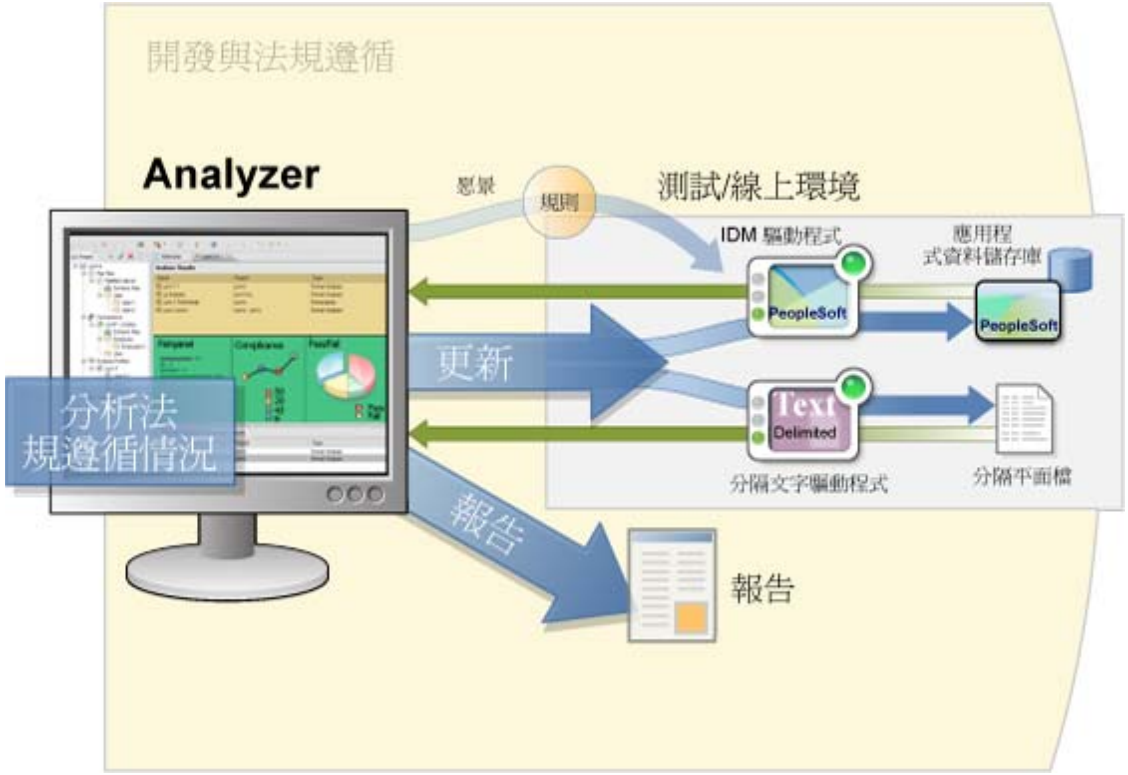
您可以使用 iManager 執行與 Designer 類似的任務並監控系統的狀態，不過，iManager 不支援套件管理。建議您使用 iManager 來執行管理任務，使用 Designer 執行部署之前需要對套件、模型及測試進行變更的組態任務。

下列幾節提供每一種工具的詳細資訊：

5.1 Analyzer

Analyzer 是基於 Eclipse 的身分管理工具集，可提供資料分析、資料清理、資料重整及資料監控與報告，協助您確保內部資料品質規則得以遵循。Analyzer 可讓您分析、增強及控制企業中的所有資料儲存。

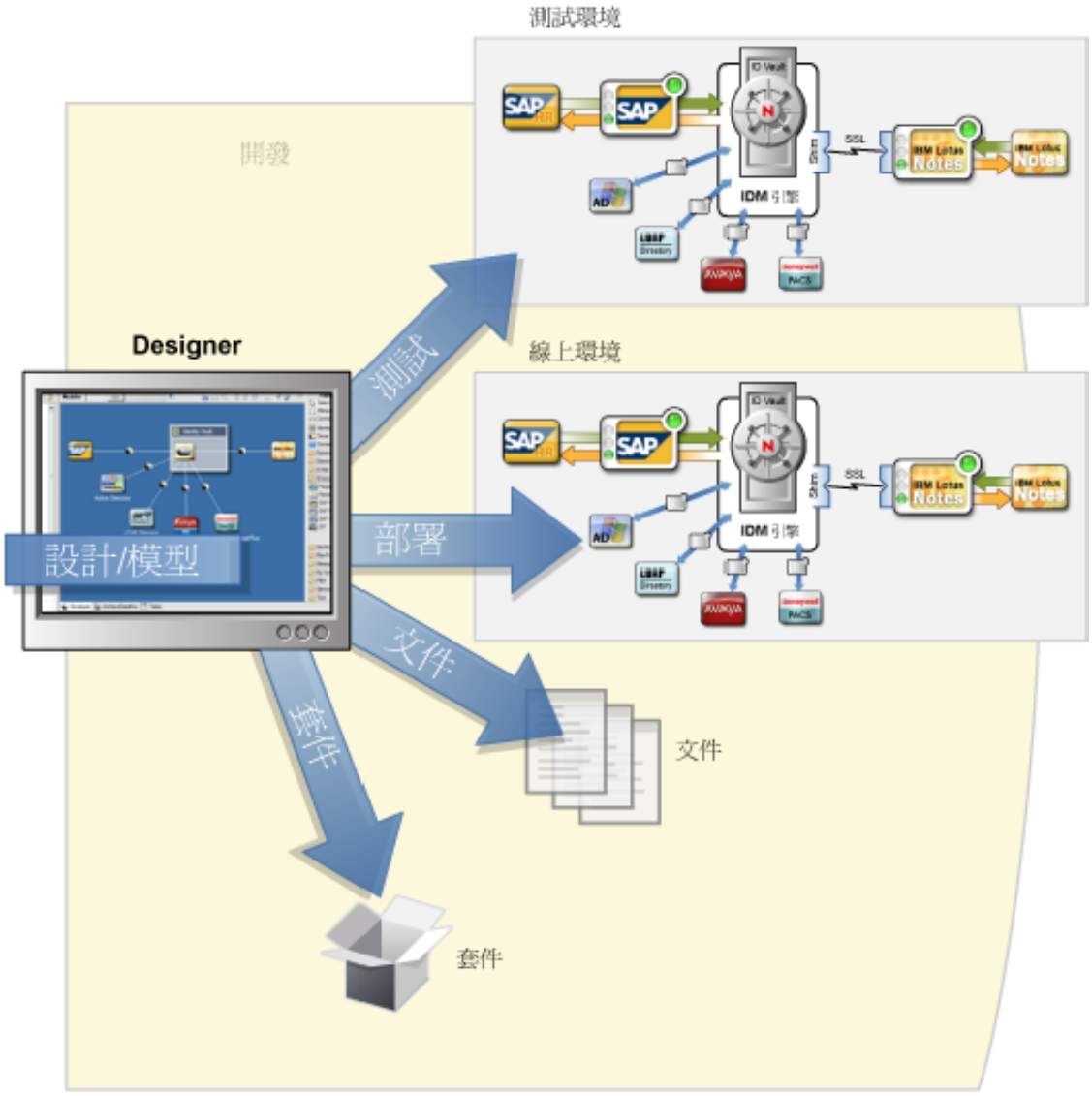
圖 5-2 *Analyzer for Identity Manager*



5.2 Designer

Designer 是基於 Eclipse 的工具，可協助您設計、部署和記載 Identity Manager 系統。在 Designer 的圖形介面中，您可以在離線環境下設計和測試您的系統、將系統部署至生產環境，以及記載下所部署系統的詳細資料。

圖 5-3 Identity Manager 適用的 Designer



設計：您可以透過 Designer 提供的圖形介面來模擬您的系統。這包括讓您建立和控制 Identity Manager 與應用程式之間的連接、設定規則，以及管理資料在連接的應用程式之間如何流動的檢視。

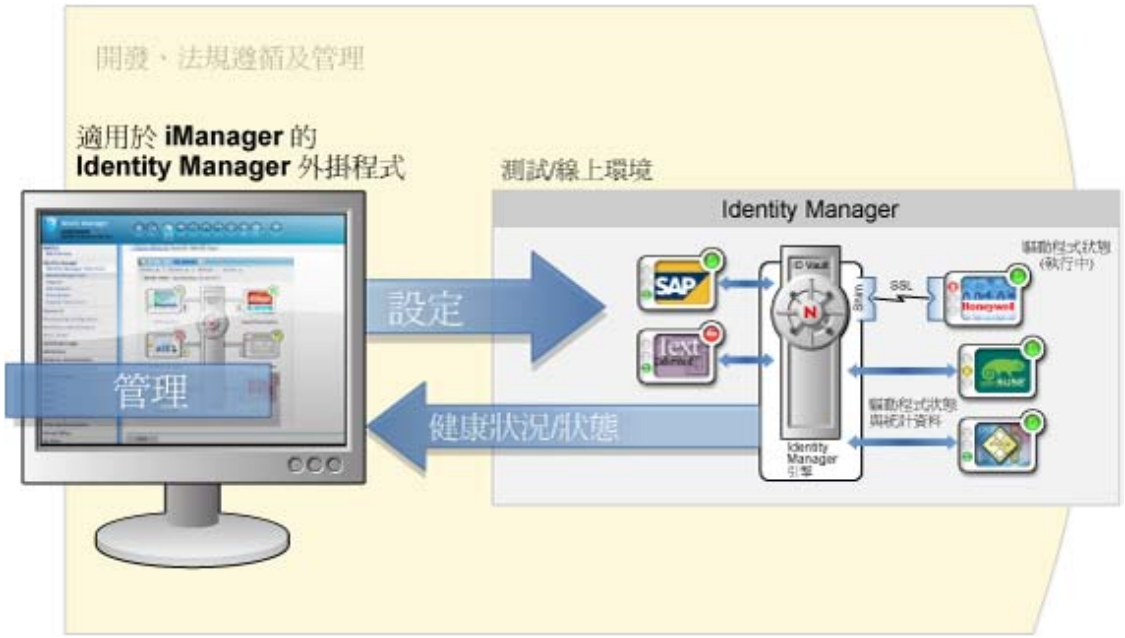
部署：只有在您啓始部署時，您在 Designer 中所做的工作才會部署至生產環境。這樣一來，您便可以在真正進入生產環境之前，放心地實驗、測試結果，並解決任何問題。

文件：您可以產生顯示系統的階層、驅動程式組態、規則組態等等的廣泛文件。基本上會提供讓您瞭解系統的技術層面所需的全部資訊，同時也會協助您驗證是否符合您的企業規則和政策。

5.3 iManager

Novell iManager 是一款基於瀏覽器的工具，提供管理許多 Novell 產品 (包括 Identity Manager) 的中心點。透過 Identity Manager 的 iManager 外掛程式，您可以管理 Identity Manager，並接收 Identity Manager 系統的即時健全和狀態資訊。

圖 5-4 *Novell iManager*



5.4 角色對應管理員

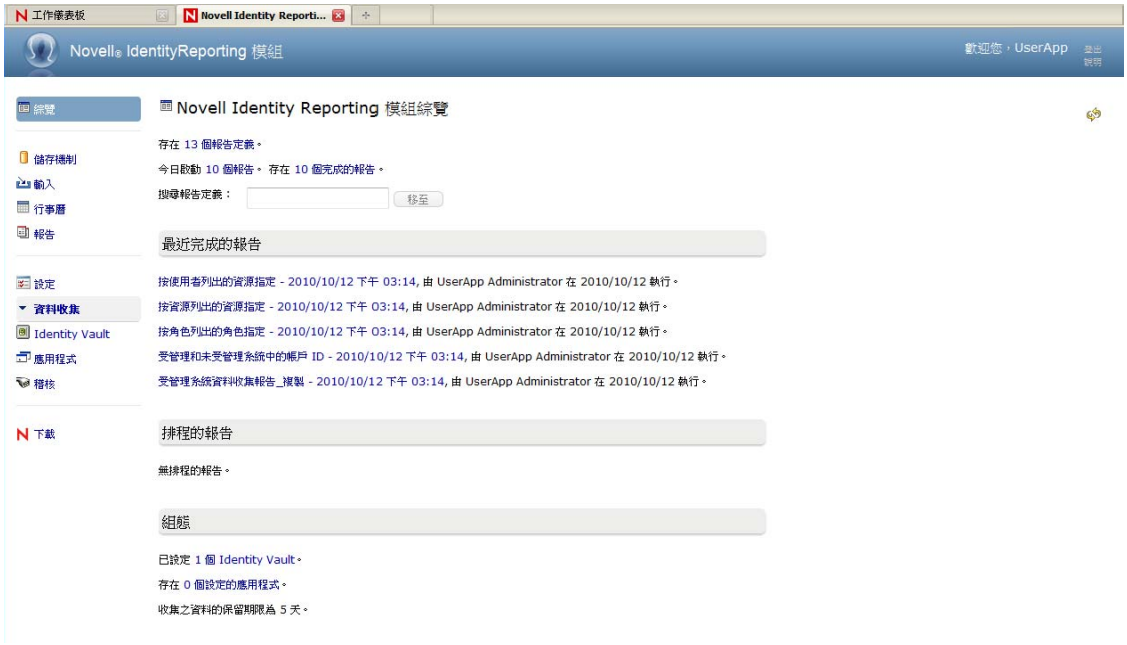
角色對應管理員是一項 Web 服務，可探查主要 IT 系統內可以授予的授權與許可。它可讓商務分析師 (而不僅是 IT 管理員) 定義哪些授權與哪些業務角色相關聯，並對這些關聯進行維護。

圖 5-5 *角色對應管理員*

5.5 身分報告

Identity Reporting 模組可產生顯示關於 Identity Manager 各方面組態之重要企業資訊的報告，包括從 Identity Vault 及受管理系統 (例如 Active Directory 或 SAP) 收集的資訊。該報告模組提供了一組預先定義的報告定義，可用於產生報告。此外，它還提供了輸入協力廠商工具中定義之自定報告的選項。報告模組的使用者介面便於您將報告排程在非高峰時間執行，從而最佳化效能。

圖 5-6 Identity Reporting 模組



該報告模組提供了幾個開放式整合點。例如，若要收集未連接至 Identity Manager 的協力廠商應用程式的資料，您可以實作自定 REST 端點從這些應用程式收集資料。此外，您還可以自定推送至 Identity Vault 的資料。當此資料可用後，您可以寫入自定報告以檢視此資訊。

其他資訊

6

瞭解構成 Identity Manager 4.0.1 的元件後，下一步就是使用相關文件建立 Identity Manager 解決方案。下列幾節說明所列任務相關文件的位置：

6.1 規劃 Identity Manager 解決方案

設計 Identity Manager 解決方案的第一步是決定該解決方案在企業中要執行的操作。請參閱 *《Identity Manager 4.0.1 架構安裝指南》* 中的「規劃」一節，使用 Designer 爲 Identity Manager 解決方案建立規劃。您也可以使用 *《User Application: Design Guide》* (使用者應用程式：設計指南) 來設計使用者應用程式解決方案。

Designer 可讓您將資訊擷取至某個專案，與其他人共享該資訊。您也可以在 Designer 中建立解決方案模型，然後再進行變更。如需 Designer 的詳細資訊，請參閱 *《Understanding Designer for Identity Manager》* (瞭解 Designer for Identity Manager)。

6.2 準備要同步的資料

建立規劃後，需要準備您的環境中要同步的資料。Analyzer 便是用來分析、清理及準備要同步之資料的工具。如需詳細資訊，請參閱 *《Analyzer 4.0.1 for Identity Manager Administration Guide》* (Analyzer 1.2 for Identity Manager 管理指南)。

6.3 安裝或升級 Identity Manager

建立規劃並準備好資料後，您便可以安裝 Identity Manager。如果您的環境是中小型 IT 環境，且之前從未使用過 Identity Manager，最好使用整合式安裝程式。整合式安裝程式會安裝並設定 Identity Manager 提供的所有元件。如需詳細資訊，請參閱 *《Identity Manager 4.0.1 整合式安裝指南》*。

如果您有一個現有的 Identity Manager 系統或大型 IT 環境，請使用 *《Identity Manager 4.0.1 架構安裝指南》* 來安裝或升級不同的 Identity Manager 元件。每個 Identity Manager 管理員元件都是分開安裝和設定的，因此您可以自定您的 Identity Manager 解決方案。

- 如需安裝指示，請參閱 *《Identity Manager 4.0.1 架構安裝指南》* 中的「*安裝*」。
- 如需升級指示，請參閱 *《Identity Manager 4.0.1 Upgrade and Migration Guide》* (Identity Manager 4.0.1 升級與移轉指南) 中的「Performing an Upgrade」(執行升級)。

- 若要將現有系統移轉至新硬體，請參閱 *《Identity Manager 4.0.1 Upgrade and Migration Guide》* (Identity Manager 4.0.1 升級與移轉指南) 中的「Performing an Upgrade」(執行升級)。
- 如果需要移轉 Roles Based Provisioning Module，請參閱 *《Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide》* (Identity Manager Roles Based Provisioning Module 4.0 使用者應用程式：移轉指南)。

6.4 設定 Identity Manager

Identity Manager 安裝好後，您必須設定各元件，以便構建一個可完全正常運作的解決方案。

- 第 6.4.1 節「同步化資料」(第 38 頁)
- 第 6.4.2 節「對應角色」(第 38 頁)
- 第 6.4.3 節「設定使用者應用程式」(第 38 頁)
- 第 6.4.4 節「設定稽核、報告及法規遵循」(第 39 頁)

6.4.1 同步化資料

Identity Manager 使用驅動程式來同步不同應用程式、資料庫、作業系統及目錄之間的資料。Identity Manager 安裝好後，您需要爲要與之同步資料的每個系統建立並設定一或多個驅動程式。

每個驅動程式都有相應的文件指南，說明同步資料所需的要求與組態設定步驟。您可在 Identity Manager 4.0.1 驅動程式文件網站 (http://www.novell.com/documentation/idm401drivers/index.html) 找到這些驅動程式指南。

請參閱每個受管理系統特定的驅動程式指南，建立驅動程式來同步身分資料。

6.4.2 對應角色

如果要在不同系統之間同步資訊，請使用角色對應管理員 (RMA) 來管理不同系統中的角色。如需詳細資訊，請參閱 *《Novell Identity Manager Role Mapping Administrator 4.0.1 User Guide》* (Novell Identity Manager 角色對應管理員 2.0 使用者指南)。

6.4.3 設定使用者應用程式

下一步是透過使用者應用程式爲 Identity Manager 解決方案新增企業展望。使用者應用程式可讓您解決以下企業需求：

- 提供一個執行角色佈建動作的方便途徑。
- 確保爲組織提供一個方法，來驗證其人員是否確知組織規則並按部就班遵守這些規則。
- 爲使用者提供自助服務，允許新使用者自行註冊，並爲匿名或來訪使用者提供存取權。
- 確保企業資源的存取遵循組織規則，並且佈建發生在企業安全性規則限定的範圍內。
- 減輕輸入、更新及刪除企業各系統中的使用者資訊帶來的管理負擔。
- 管理身分、服務、資源及資產的手動與自動佈建。
- 支援複雜的工作流程。

《Identity Manager Roles Based Provisioning Module 4.0 User Application: Administration Guide》(Identity Manager Roles Based Provisioning Module 4.0 使用者應用程式：管理指南) 提供了如何設定這些使用者應用程式功能的資訊。

6.4.4 設定稽核、報告及法規遵循

設定稽核、報告及法規遵循功能是建立 Identity Manager 解決方案的最後一步，也是最重要的一步；設定之後您便可驗證解決方案是否與企業規則相符。請使用以下指南安裝並設定這些功能：

- **稽核：** 請參閱 *《Identity Manager 4.0.1 Reporting Guide for Novell Sentinel》*(適用於 Novell Sentinel 的 Identity Manager 4.0 報告指南)。
- **報告：**請參閱 *《Identity Reporting Module Guide》*(Identity Reporting 模組指南) 與 *《Using Identity Manager 4.0 Reports》*(使用 Identity Manager 4.0 報告)。
- **法規遵循：** 請參閱 *《Identity Manager Roles Based Provisioning Module 4.0 使用者應用程式：使用者指南》*中的「使用法規遵循索引標籤」。

6.5 管理 Identity Manager

完成 Identity Manager 解決方案後，您可以使用許多不同的指南，協助您在業務變更及擴展時管理、維護及變更 Identity Manager 解決方案。這些管理指南位於 Identity Manager 4.0.1 文件網站 (http://www.novell.com/documentation/idm401/index.html) 的「Administration」(管理) 標題下。