綜覽

Novell®
Identity Manager

3.6.1

2009 年 5 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。

本文件所述產品所使用技術的智慧財產權屬於 Novell, Inc. 所有。特別是 (但不限於) 這些智慧財產權可能包含 Novell 法律專利網頁 (http://www.novell.com/company/legal/patents/) 中所列的一或多項美國專利，以及在美國與其他國家 / 地區的一或多項其他專利或申請中的專利。

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

*線上文件：*如需 Novell 此產品及其他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 Novell® Identity Manager 能夠協助您解決的企業問題，並提供可在您的解決方案中使用的 Identity Manager 軟體元件和工具的綜覽。本指南是以下列方式進行編排：

- 第 1 章 「Identity Manager 與企業流程自動化」(第 9 頁)
- 第 2 章 「Identity Manager 架構」(第 17 頁)
- 第 3 章 「Identity Manager 工具」(第 25 頁)

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/idm36/index.html)。

其他文件

如需其他 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/idm36drivers/index.html)。

文件慣例

在 Novell 文件中，大於符號 (>) 是用來分隔步驟中的動作，以及交互參照路徑中的項目。

商標符號 (®、™ 等) 表示 Novell 的商標。星號 (*) 則代表協力廠商的商標。

雖然在書寫單一路徑名稱時，有些平台採用反斜線，其他平台採用正斜線，但在本文中，路徑名稱一律使用反斜線。使用者若使用要求正斜線的平台 (如 Linux* 或 UNIX*)，則應遵守軟體要求使用正斜線。

Identity Manager 與企業流程自動化

1

下列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 2 章「Identity Manager 架構」(第 17 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。專注於因企業規則所驅動的多系統資料同步需求，結合了工作流程、角色、證明、自助服務、稽核和報告等功能，即可將 IT 組織裡最重要且又費時的兩項任務 (即提供使用者權限與管理密碼) 的相關程序自動化。

圖 1-1 *Identity Manager 核心功能*

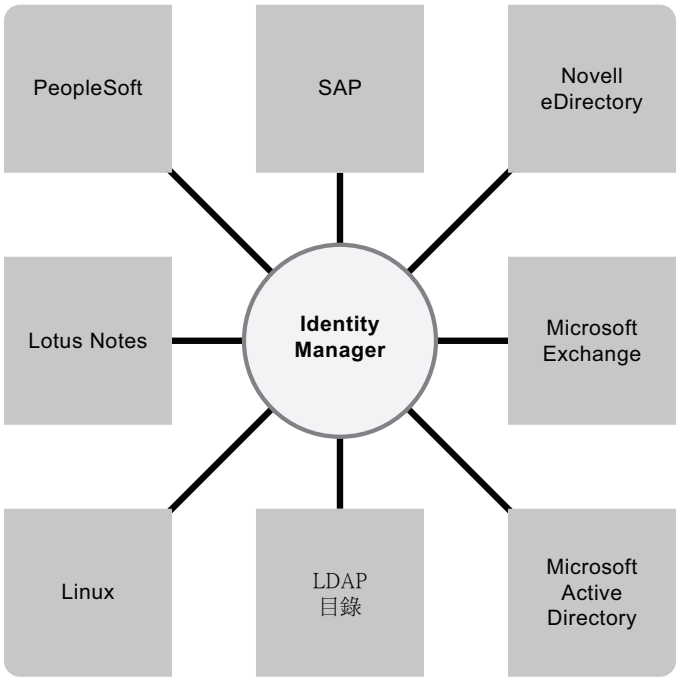
後續幾節會介紹這些 Identity Manager 功能，及其如何協助您順利達成組織的身分識別管理需求：

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。抑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 可讓您在廣泛的應用程式、資料、作業系統及目錄 (例如 SAP*、PeopleSoft*、Lotus Notes*、Microsoft* Exchange、Microsoft Active Directory*、Novell eDirectory™、Linux 與 UNIX 及 LDAP 目錄) 之間同步、轉換及配送資訊。

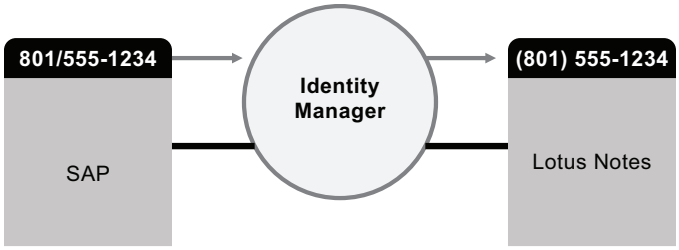
圖 1-2 *連接多種系統的 Identity Manager*



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。

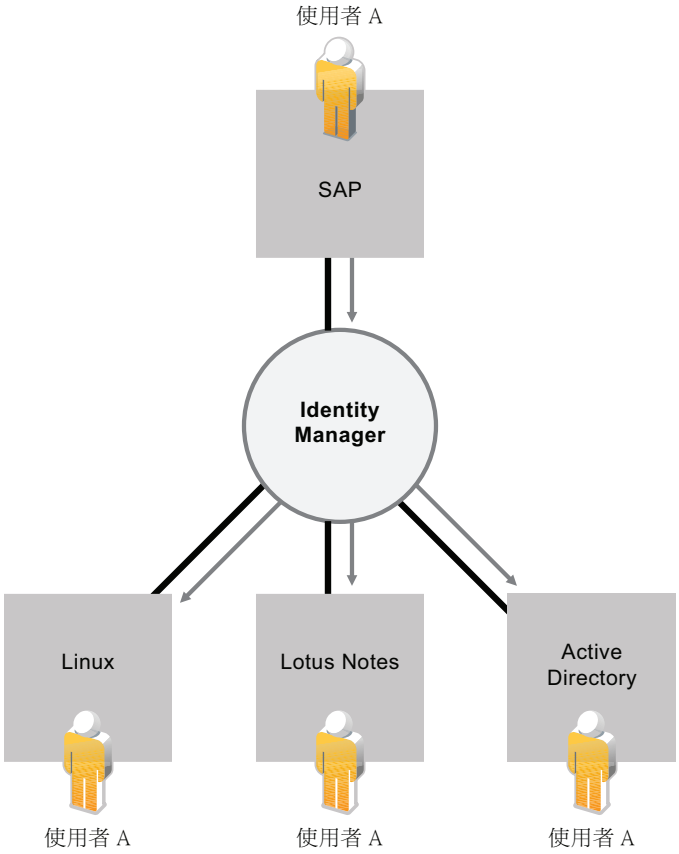
在下圖中，SAP HR 資料庫是使用者電話號碼的管理來源。因爲 Lotus Notes 系統也使用電話號碼，所以 Identity Manager 會將號碼轉換成必要的格式，再分享給 Lotus Notes 系統使用。每當電話號碼在 SAP HR 系統中一有變動，就會同步至 Lotus Notes 系統。

圖 1-3 連接的系統之間的資料同步



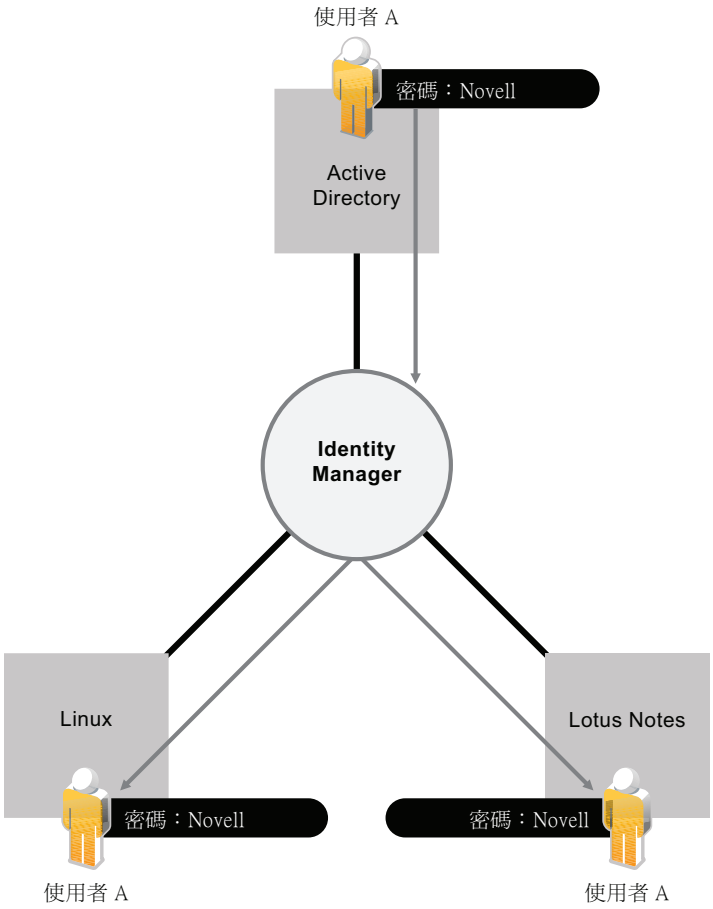
管理現有使用者的資料只是 Identity Manager 資料同步功能的開端。除此之外，Identity Manager 還可以在如 Active Directory 的目錄、PeopleSoft 和 Lotus Notes 的系統及 UNIX 與 Linux 作業系統中，建立新的使用者帳戶和移除現有的帳戶。例如，當您將新員工新增至 SAP HR 系統時，Identity Manager 可以自動在 Active Directory 中建立新的使用者帳戶、在 Lotus Notes 中建立新帳戶，以及在 Linux NIS 帳戶管理系統中建立新帳戶。

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

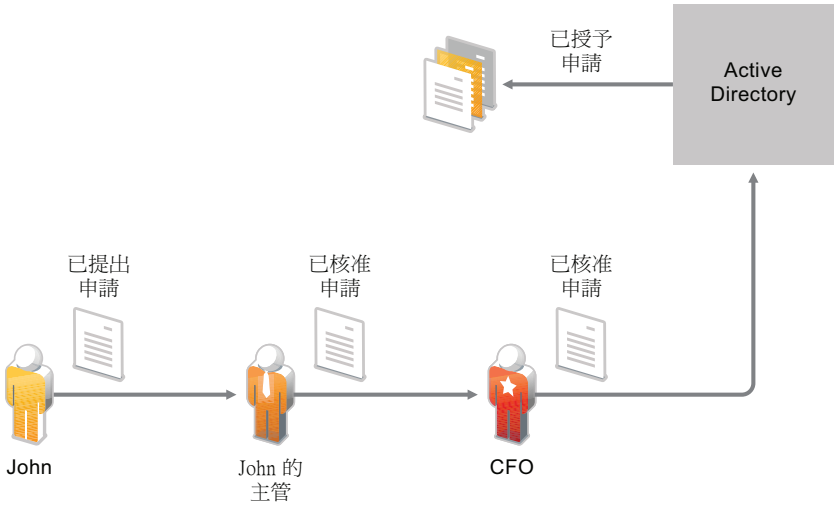


1.2 工作流程

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



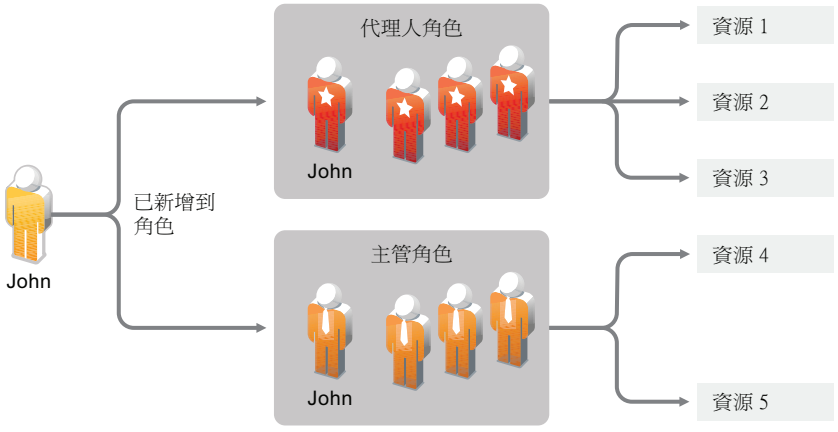
您可以在每當有某事件發生時 (例如，有新的使用者新增至您的 HR 系統) 就自動啓始工作流程，或是透過使用者申請來手動啓始。爲了確保適時進行核准，您可以設定代理核准人和核准小組。

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而要求存取資源。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。如果指定多個角色給一位使用者，該使用者就會獲得這些角色相關的資源存取權，如下圖所示。

圖 1-7 資源的角色提供模組



您可以根據組織中發生的事件，自動將使用者新增至某個角色 (例如，將職稱爲 「律師」 的新使用者新增至 SAP HR 資料庫)。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，可能會由於角色發生衝突，而不應該將有些角色指定給同一人。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

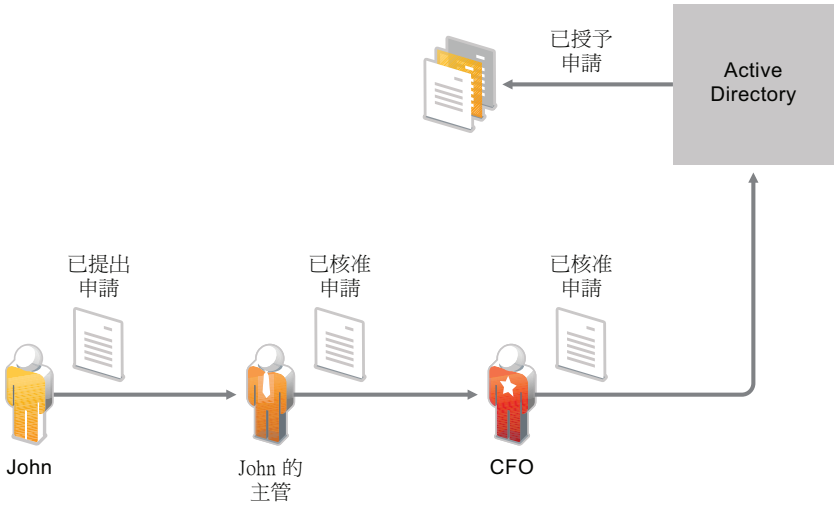
企業主管和部門可能想要自行管理使用者資訊和存取需求，而不想依賴您或您的幹部來管理。您一定常常聽到：「我爲什麼不能在公司目錄裡更改自己的手機號碼？」或是「我是行銷部門的人，爲什麼要打電話給服務台才能存取行銷資訊資料庫？」

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 12 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 稽核與報告

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提供活動都會經過追蹤並記錄下來，以備隨時稽核。Identity Manager 會對所有發生的活動發出事件訊息。您可以使用 Novell Sentinel™ 來收集這些訊息，以製作下列類型的報告：

- 一段特定期間的所有核准工作流程，並記錄每一個工作流程的動作 (已啓動、轉遞、拒絕、核准等等)。
- 一段特定期間提供的所有資源，並記錄每一項資源的動作 (已提交、授予、撤銷、成功等等)。
- 一位使用者在一段特定期間的所有工作流程狀態、密碼變更及管理變更。
- 一段特定期間提供給一位使用者的所有資源。
- 一段特定期間提供給所有使用者的所有資源。

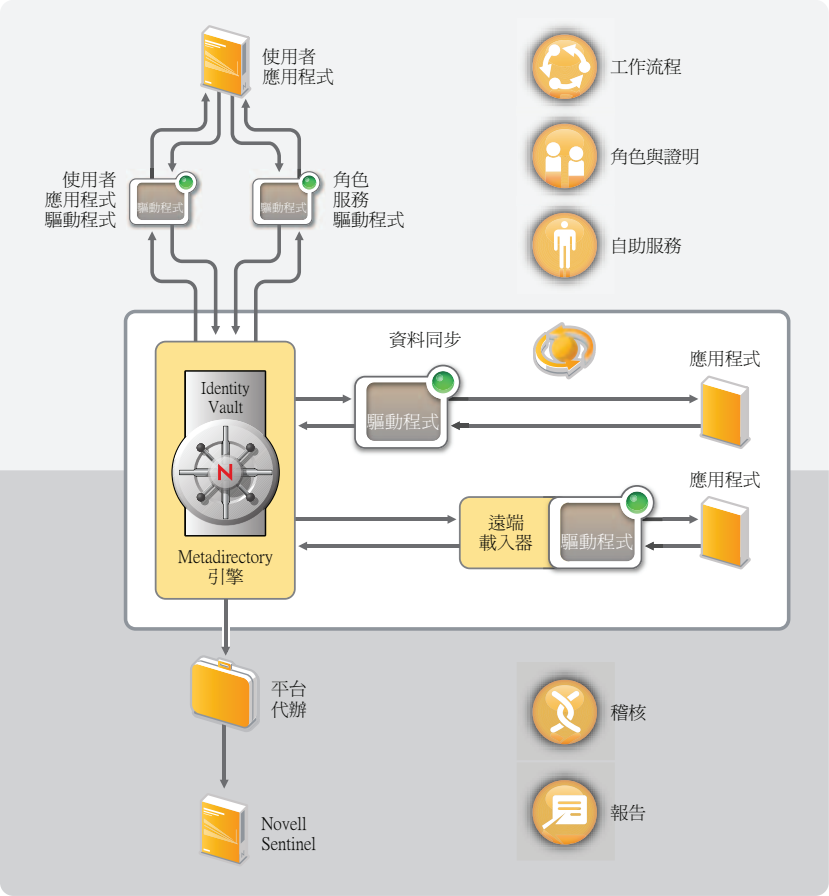
Novell Sentinel 與 Identity Manager 分開銷售。

Identity Manager 架構

2

下圖顯示高階架構元件，這些元件提供第 1 章 「Identity Manager 與企業流程自動化」(第 9 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 2-1 *Identity Manager 高階架構*



下列幾節介紹其中每一個元件：

- 第 2.1 節 「資料同步」(第 17 頁)
- 第 2.2 節 「工作流程、角色、證明與自助服務」(第 21 頁)
- 第 2.3 節 「稽核與報告」(第 22 頁)

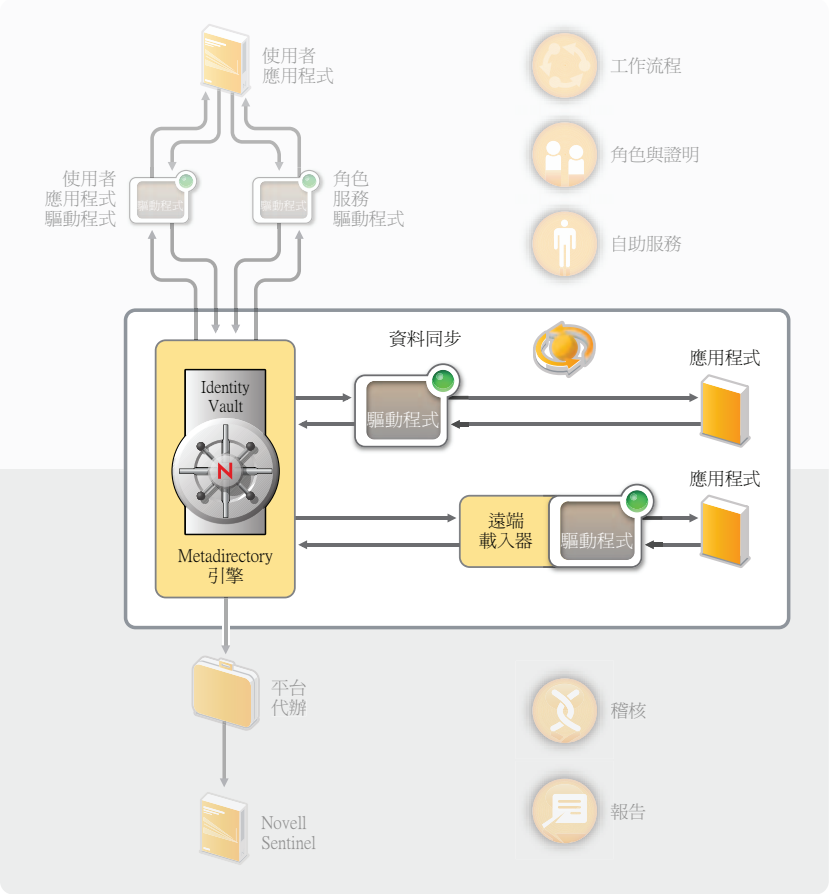
2.1 資料同步

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，應該會自動反映變更。

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、Metadirectory 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 2-2 *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：

- 第 2.1.1 節 「元件」(第 18 頁)
- 第 2.1.2 節 「重要概念」(第 19 頁)

2.1.1 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。

Metadirectory 引擎：當 Identity Vault 或連接的應用程式中有資料變更時，Metadirectory 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。Metadirectory 引擎又稱爲「*Identity Manager 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的責任：1) 將應用程式中的資料變更 (事件) 回報給 Metadirectory 引擎，2) 將 Metadirectory 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 Metadirectory 引擎位於相同的伺服器上，則您只要在這部伺服器上安裝驅動程式即可。然而，如果應用程式和 Metadirectory 引擎不在相同的伺服器上 (換言之，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 Metadirectory 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*」。

2.1.2 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 Metadirectory 引擎，該引擎會根據與驅動程式通道的關聯的一組過濾器和規則來處理文件。在 XML 文件上完成所有處理時，Metadirectory 引擎會利用文件來啓始適當的變更給 Identity Vault (發行者通道)，或是驅動程式會利用文件，在連接的系統中啓始適當的變更 (訂閱者通道)。

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。

自動化提供：自動化提供是指 Identity Manager 產生使用者提供動作的能力，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 中所建立 Exchange 帳戶的準則，則 Metadirectory 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商業邏輯。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。

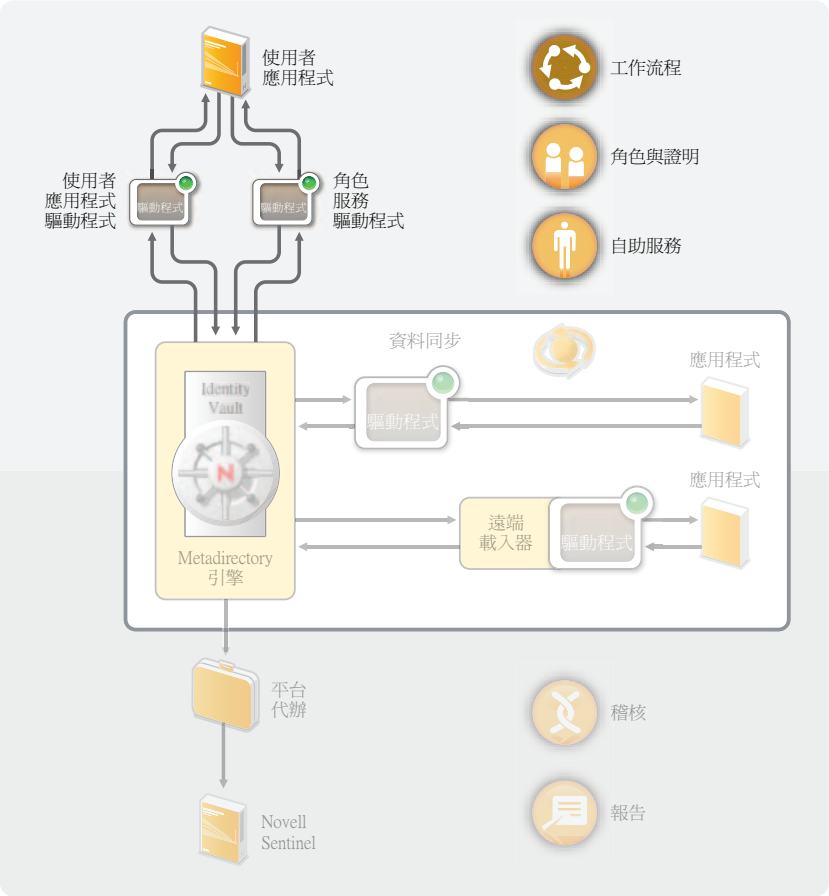
2.2 工作流程、角色、證明與自助服務

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)。

「使用者應用程式角色提供模組」是另外銷售的 Identity Manager 附加產品。當您新增「角色提供模組」時，標準的「使用者應用程式」功能會擴充爲包含進階自助服務、核准工作流程、角色型提供、「職務分離」條件約束，以及證明。

圖 2-3 *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 2.2.1 節 「元件」(第 22 頁)
- 第 2.2.2 節 「重要概念」(第 22 頁)

2.2.1 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。

角色服務驅動程式：「角色服務」驅動程式可管理所有角色指定、啓動工作流程來處理需要核准的角色指定申請，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。

2.2.2 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。

角色提供：「角色提供」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。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，「使用者應用程式角色提供模組」提供一項「職務分離」功能。您可以建立定義處於衝突之角色狀態的職務分離「*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：必須由已指定到「*角色模組管理員*」和「*角色管理員*」系統角色的人來管理角色。

「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。

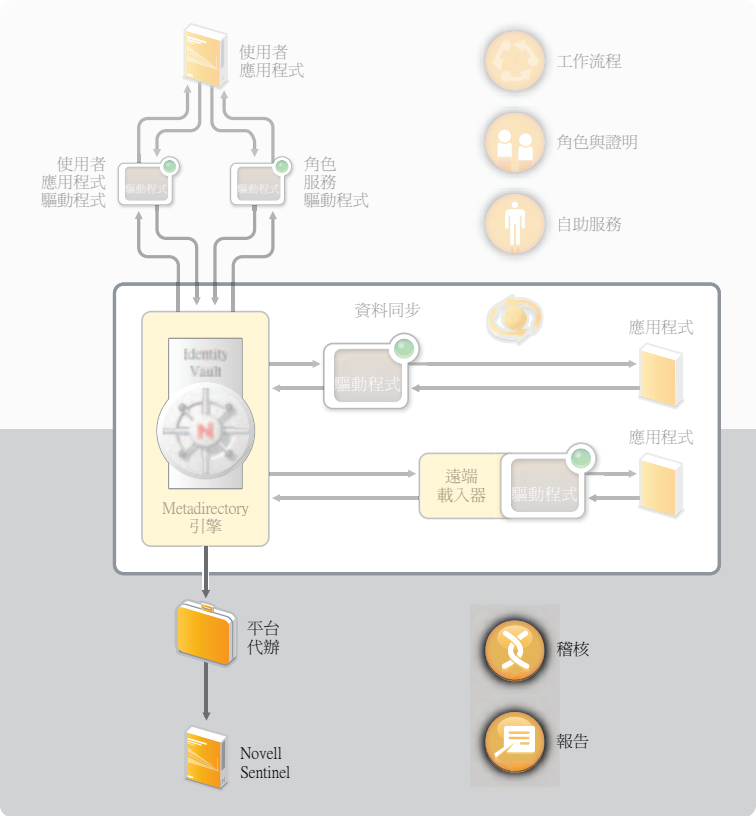
「角色管理員」可以做的事與「角色模組管理員」相同，但無法管理「職務分離」條件約束、設定「角色」系統及執行所有報告。此外，「角色模組管理員」在「角色」系統內的活動範圍不受限制，而「角色管理員」範圍則侷限於明確指定的使用者、群組和角色。

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。

2.3 稽核與報告

如下圖所示，稽核與報告功能是經由與 Novell Sentinel™ 整合來提供。

圖 2-4 *Identity Manager 稽核與報告*



平台代辦：「平台代辦」會擷取來自 Metadirectory 引擎的事件，然後將其傳送至 Novell Sentinel 系統。

Novell Sentinel：Novell Sentinel 是一套安全資訊與事件管理 (SIEM) 解決方案，可將系統網路、應用程式和安全性記錄的收集、分析和報告自動化。Novell Sentinel 是個別販售。

如需 Novell Sentinel 更完整的介紹，包括如何購買產品，請瀏覽 Novell Sentinel 網站 (http://www.novell.com/products/sentinel/)。

Identity Manager 工具

3

Identity Manager 提供三個主要的工具，協助您設定和維護 Identity Manager 系統：Designer、iManager 和「使用者應用程式」管理主控台。

您可以使用 Designer，先在離線環境下建立和設定 Identity Manager 系統，然後才將變更部署至線上系統。iManager 所執行的任務與 Designer 相同，但還可以監看系統的狀態；然而，您在 iManager 中所做的變更會立即部署，因此，建議將 iManager 用在簡單的管理任務上，而將 Designer 用需要在部署進行模擬和測試的複雜組態任務上。

您可以使用「使用者應用程式」管理主控台，透過建立和修改頁面和入口網站應用程式，以管理應用程式的外觀與觀感。您也可以修改應用程式設定，例如快取和記錄設定，並設定「使用者應用程式」的提供功能所需的委託和代理設定。

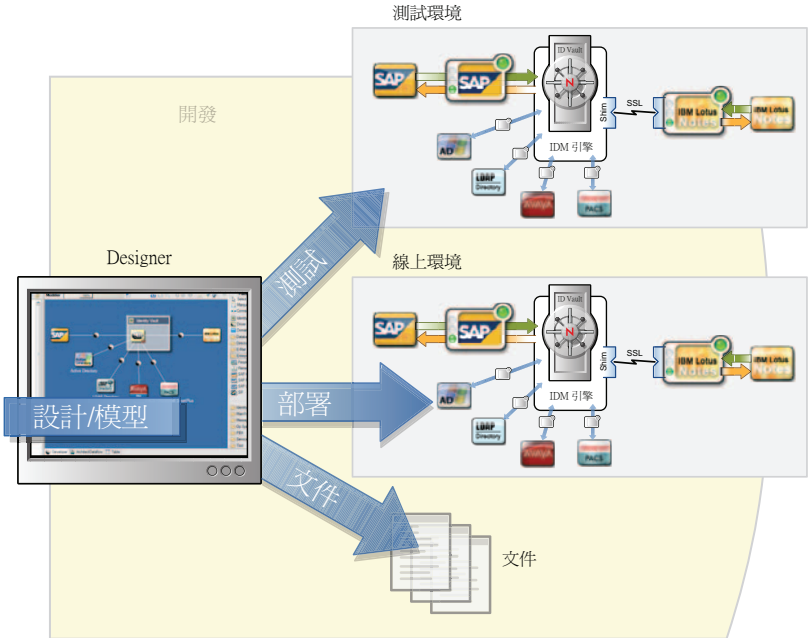
下列幾節提供每一種工具的詳細資訊：

- 第 3.1 節 「Designer」（第 25 頁）
- 第 3.2 節 「iManager」（第 26 頁）
- 第 3.3 節 「使用者應用程式管理主控台」（第 26 頁）

3.1 Designer

Designer 是以 Eclipse* 爲基礎的工具，可協助您設計、部署和記載您的 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 3-1 *Identity Manager 適用的 Designer*



雖然不使用 Designer 也能夠設定 Identity Manager 系統，但會相當困難，並不建議這樣做。

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。

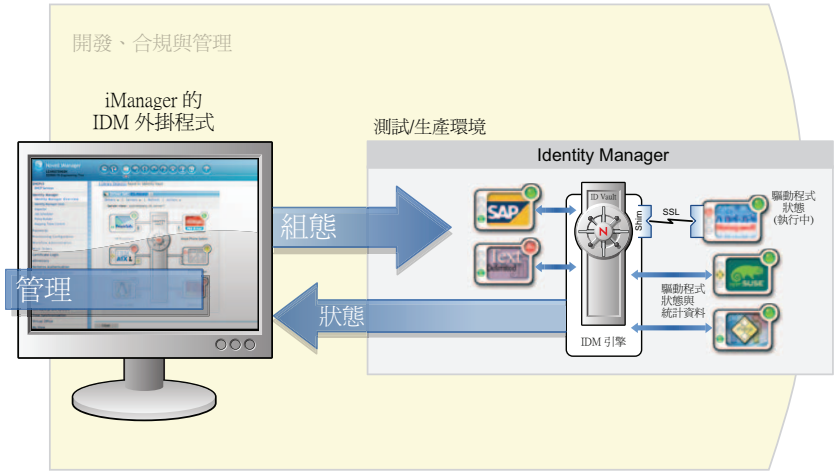
部署：只有在您啓始部署時，您在 Designer 中所做的工作才會部署至生產環境。這樣一來，您便可以在真正進入生產環境之前，放心地實驗、測試結果，並解決任何問題。

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。

3.2 iManager

Novell® iManager 是一個瀏覽器爲主的工具，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 3-2 *Novell iManager*



3.3 使用者應用程式管理主控台

「使用者應用程式」提供 Web 型管理主控台，可讓您設定、管理和自定密碼自助服務、角色和提供。任何人只要獲得管理權限，「使用者應用程式」中就會增加一個 「*管理*」索引標籤，即管理主控台。

圖 3-3 使用者應用程式管理頁面

「使用者應用程式管理」頁面提供下列索引標籤：

- **應用程式組態：**可讓您設定快取、LDAP 參數、記錄、主題和密碼模組安裝。
- **頁面管理：**可讓您建立新的頁面，或自定現有的「身分自助服務」頁面。
- **入口網站管理：**可讓您建立新的入口網站應用程式，或自定在「身分自助服務」頁面上使用的現有的入口網站應用程式。
- **提供：**可讓您設定委託、代理、任務、數位簽名服務，以及引擎和叢集設定。
- **安全性：**可讓您定義具有「提供管理員」和「使用者應用程式管理員」特權的人員。