Novell Identity Manager Driver for Active Directory*

3.1

www.novell.com

實作指南

2006 年 4 月 28 日

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。

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或其他國家的額外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：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

ConsoleOne 是 Novell, Inc. 在美國與其他國家的註冊商標。
DirXML 是 Novell, Inc. 在美國與其他國家的註冊商標。
eDirectory 是 Novell, Inc. 的商標。
NCP 及 NetWare Core Protocol 均爲 Novell, Inc. 的註冊商標。
NDS 和 Novell Directory Services 均爲 Novell, Inc. 在美國與其他國家的註冊商標。
NetWare 是 Novell, Inc. 在美國與其他國家的註冊商標。
Novell 是 Novell, Inc. 在美國與其他國家的註冊商標。
Novell Certificate Server 是 Novell, Inc. 的商標。
Novell Client 是 Novell, Inc. 的註冊商標。

協力廠商資料

所有的協力廠商商標均爲其個別擁有廠商的財產。

目錄

關於本指南

本指南說明如何安裝、設定組態及管理 Identity Manager Driver for Active Directory。

使用對象

本指南適用於實作 Identity Manager Driver for NT Domains 的 Active Directory 管理員、Novell® eDirectory™ 管理員及其他人員。

意見反應

我們想知道您對於本手冊與其他本產品隨附之文件的意見與建議。請使用線上文件中每頁底下的「使用者意見」功能，或請造訪 www.novell.com/documentation/feedback.html，然後寫下您的意見。

文件更新

如需本文件的最新版本，請造訪驅動程式文件網站 (http://www.novell.com/documentation/lg/dirxmldrivers)。

其他文件

如需使用 Identiy Manager 和其他 Identity Manager 驅動程式的相關文件，請參閱 Identity Manager 文件網站 (http://www.novell.com/documentation/lg/dirxml20)。

文件慣例

在 Novell 文件中，大於符號 (>) 是用以分隔步驟中的各個動作，以及前後參照路徑中的數個項目。

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

綜覽

1

1.1 關鍵詞彙

1.1.1 Identity Manager

Novell® Identity Manager 是一種服務，利用一套功能強大的可設定組態規則，對一組已連接系統中之數台伺服器間的資料進行同步化。Identity Manager 使用 Identity Vault 儲存共享資訊，並在 Identity Vault 或已連接系統上的資訊發生變更時，使用 Metadirectory 引擎以規則爲基礎管理這些資訊。Identity Manager 可以在 Identity Vault 和 Metadirectory 引擎所在的伺服器上執行。

1.1.2 已連接系統

已連接系統可以是任何透過驅動程式就能與 Identity Manager 共享資料的系統。Active Directory 就是一種已連接系統。

1.1.3 Identity Vault

Identity Vault 是由 eDirectory™ 提供的持續資料庫，Identity Manager 使用它來儲存要與已連接系統保持同步的資料。從狹義上講，可以將此 Identity Vault 當做 Identity Manager 的私人資料儲存區，而從廣義上考慮，還可以將其充當儲存企業全面性資料的 Metadirectory。所有 eDirectory 支援的通訊協定都可使用該 Identity Vault 中的資料，這類通訊協定包括 NCP™ (ConsoleOne® 和 iManager 之類的公用程式所使用的傳統通訊協定)、LDAP 和 DSML。

因爲此 Identity Vault 由 eDirectory 提供，所以透過將現有的目錄樹當做 Identity Vault 使用，就可以輕鬆地將 Identity Manager 整合到貴公司的目錄基礎結構中。

1.1.4 Metadirectory 引擎

Metadirectory 引擎是實作事件管理和 Identity Manager 規則的核心伺服器。該引擎會在 eDirectory 中的 Java* 虛擬機器上執行。

1.1.5 Active Directory 驅動程式

驅動程式會爲已連接系統實作資料共享規則。您可以使用 iManager 定義過濾器和規則，透過這種方式來控制驅動程式的動作。對於 Active Directory 而言，驅動程式會爲單一領域實作規則。

1.1.6 驅動程式 Shim

驅動程式 Shim 是驅動程式的元件，用於將基於 XML 的 Identity Manager 指令和事件語言 (XDS) 轉換成與已連接系統進行互動所需的通訊協定和應用程式介面 (API) 呼叫。執行完「輸出轉換」後，會呼叫 Shim 以執行已連接系統上的指令。指令通常會在「訂閱者」通道上產生，但是也可以由「發行者」通道上的指令寫回產生。

該 Shim 也可以從「輸入轉換」規則的已連接系統產生事件。驅動程式 Shim 可以在 Java 類別中實作，也可以做爲原始 Windows DLL 檔案來實作。適用於 Active Directory 的 Shim 是 ADDriver.dll。

ADDriver.dll 可以做爲原始 Windows DLL 檔案來實作。ADDriver 會使用多種 Windows 應用程式介面 (API) 來整合 Active Directory。通常，這些應用程式介面 (API) 需要進行某種類型的登入和驗證才能運作。同時，這些應用程式介面 (API) 可能還需要登入帳戶在 Active Directory 中及執行 ADDriver.dll 所在的機器上具備一定的權限。

如果使用「遠端載入器」，會在執行「遠端載入器」所在的伺服器上執行 ADDriver.dll。否則就會在執行 Metadirectory 引擎所在的伺服器上執行。

1.1.7 遠端載入器

「遠端載入器」可讓驅動程式 Shim 於 Metadirectory 引擎之外執行 (可能是在另一部機器上遠端執行)。通常，會在 Identity Manager 伺服器不符合驅動程式 Shim 要求的情況下使用「遠端載入器」。例如，如果於 Linux* 之上執行 Metadirectory 引擎，則會在 Windows 伺服器上使用「遠端載入器」來執行 Active Directory 驅動程式 Shim。

「遠端載入器」是用於執行驅動程式 Shim 和在 Shim 與 Metadirectory 引擎之間傳遞資訊的一種服務。使用「遠端載入器」時，請在執行「遠端載入器」(而不是執行 Metadirectory 引擎) 的伺服器上安裝驅動程式 Shim。您可以選擇使用保全插槽層 (SSL) 加密 Metadirectory 引擎和「遠端載入器」之間的連接。

搭配使用「遠端載入器」和 Active Directory 驅動程式 Shim 時，有兩種網路連接方式：

- 連接領域控制器和「遠端載入器」
- 連接 Active Directory 和 Active Directory 驅動程式 Shim

1.2 新功能

- 「驅動程式功能」，第 9 頁
- 「Identity Manager 功能」，第 9 頁

1.2.1 驅動程式功能

- 「平台登入」是驅動程式 Shim 組態參數。它可以讓 Shim 本地登入。啓用本地登入時，「訂閱者」通道密碼的設定和修改會使用應用程式介面 (API) 的平台密碼管理，此平台密碼管理不需要保全插槽層 (SSL) 加密的輕量目錄存取協定 (LDAP) 會期。

  利用 CDOEXM 進行的交換操作會使用線串身份進行驗證和授權，以減少在輕量目錄存取協定 (LDAP) 通道以外操作失敗的可能性。如需詳細資訊，請參閱第 4 章 「設定 Active Directory 驅動程式」, 第 35 頁。
- 驅動程式 Shim 組態參數已更新。這些驅動程式參數使用靈活提示，使得參數分類更趨合理並能夠更好地控制放置在參數中的值。限制參數爲一組已知的值，由下拉式清單進行控制，並且檢查需要整數值的參數以找出無效字元。
- 新增了兩種驅動程式 Shim 組態參數用以控制 Microsoft Exchange 信箱的移動和刪除。如果啓用 CDOEXM 和「Exchange 信箱移動」，那麼一旦爲擁有 Exchange 信箱的使用者物件設定了 homeMDB 屬性值，信箱就會被移動到新的「Exchange 訊息資料庫」。Shim 僅在下列情況下支援領域內的移動：存放新訊息資料庫的 Exchange 伺服器必須置於 Shim 所管理的領域內。
- 透過「使用者應用程式」或透過規則可增強對「角色授權」的支援。請參閱《*Novell Identity Manager 3.0* 管理指南》中的「建立並使用授權」。
- 驅動程式 Shim 包括對延伸查詢 (query-ex) 的支援。延伸查詢在輕量目錄存取協定 (LDAP) 搜尋中啓用分頁顯示結果功能。此功能可讓 Shim 將較大資料集從 Active Directory 移轉至 Identity Vault。如需從 Active Directory 移轉資料集的相關資訊，請參閱第 8 章 「疑難排解」, 第 79 頁。

1.2.2 Identity Manager 功能

如需 Identiy Manager 新功能的相關資訊，請參閱《*Identity Manager 3.0* 安裝指南》中的「Identity Manager 3 的新功能」。

1.3 在系統之間傳送資料

本節說明資料在 Active Directory 和 Identity Vault 之間的流動方式。

1.3.1 發行者和訂閱者通道

Active Directory 驅動程式支援「發行者」和「訂閱者」通道。

「發行者」通道負責處理下列事項：

- 從與驅動程式 Shim 連接之伺服器上所代管之領域的 Active Directory 中讀取事件。
- 將該資訊提交給 Identity Vault。

「訂閱者」通道負責處理下列事項：

- 監視對 Identity Vault 物件所進行的新增和修改操作。
- 對反映這些變更的 Active Directory 進行變更。

您可以設定驅動程式的組態，以同時允許 Active Directory 和 Identity Vault 更新特定的屬性。在此組態設定中，除非是由過濾器和合併權限控制合併操作的情況，否則屬性值由最近發生的變更決定。

1.4 預設的驅動程式組態

Active Directory 驅動程式隨附於名爲 ActiveDirectory.xml 的預設組態檔案中。當隨 Designer 或 iManager 一起輸入時，此組態檔案會建立一個驅動程式，此驅動程式具有一組適合用於與 Active Directory 進行同步化的規則。如果驅動程式預設的規則與您的要求不同，請變更這些規則使您所需要的規則生效。請特別留意預設的「相符」規則。因爲您相信會符合使用者的資料常常是與預設不同。規則本身已加了備註，因此您可以透過輸入測試驅動程式並利用 Designer 或 iManager 檢視這些規則，進一步了解它們的功能。

1.4.1 使用者物件名稱映射

通常，Identity Vault 的管理公用程式 (如 iManager 和 ConsoleOne) 對使用者物件的命名與 Microsoft* Management Console (MMC) 的使用者和電腦嵌入式管理單元不同。請確定您清楚了解這類不同，以便讓您擁有的「相符」規則和任何「轉換」規則都能正常運作。

1.4.2 資料流程

資料可以在 Active Directory 與 Identity Vault 之間流動。資料流程由 Active Directory 驅動程式中現有的規則進行控制。

規則

規則會控制 Active Directory 與 Identity Vault 之間的資料同步化。

在驅動程式組態設定期間，Active Directory 組態檔案可讓您選取會影響所建立之預設規則和過濾器的數個選項。表格 1-1 頁上 10 會列出這些選項以及它們如何影響所建立的規則和過濾器：

表格 ***1-1*** 資料流程選項

選項	描述
AD 至 Vau	「設定資料流程的組態」會建立啓始驅動程式過濾器，此過濾器可用來控制要進行同步化處理的類別和屬性。此選項的目的在於設定驅動程式的組態，以最適當的方式表示一般資料流程的規則。輸入後就可以對其進行變更以反映特定要求。 「*雙向*」會將類別和屬性設定成可同時在「發行者」和「訂閱者」通道上進行同步化。不論是在 Identity Vault 上還是 Active Directory 上發生的變更，都會在另一方獲得反映。如果您想讓雙方都做爲資料的授權來源，請使用此選項。 「*AD 至 Vault*」會將類別和屬性設定成僅可在「發行者」通道上進行同步化。在 Active Directory 上發生的變更會反映在 Identity Vault 上，但反之發生在 Identity Vault 上的變更則會被忽略。如果您想讓 Active Directory 做爲資料的授權來源，請使用此選項。 「*Vault 至 AD*」會將類別和屬性設定成僅可在「訂閱者」通道上進行同步化。在 Identity Vault 上發生的變更會反映在 Active Directory 上，但反之發生在 Active Directory 上的變更則會被忽略。如果您想讓 Identity Vault 做爲資料的授權來源，請使用此選項。

選項	描述
[illegible]	「發行者佈置」用於控制在 Identity Vault 中建立物件的位置。 「*鏡像複製*」會根據物件在 Active Directory 中的階層將其放置在 Identity Vault 中的同一階層。 「*平面*」會將所有物件都放置在組態設定期間所指定之 Identity Vault 的基本容器中。
[illegible]	「訂閱者佈置」用於控制物件在 Active Directory 中的放置方式。 「*鏡像複製*」會根據物件在 Identity Vault 中的階層將其放置在 Active Directory 中的同一階層。 「*平面*」會將所有物件都放置在組態設定期間所指定之 Active Directory 的基本容器中。

表格 1-2 頁上 11 會列出預設規則，並說明組態設定期間所選取的選項會如何影響規則：

表格 ***1-2*** 預設規則

規則	描述
建立	不論是鏡像複製還是平面階層，您都必須定義「全名」，使用此名稱建立的 Active Directory 使用者要與 Identity Vault 中的使用者相同。
相符	在鏡像複製階層中，「相符」規則會嘗試比對位於該階層之相同位置的物件。
佈置	在平面階層中，「相符」規則會嘗試比對與所指定基本容器中之物件「全名」相同的使用者。 在鏡像複製階層中，「佈置」規則會將所有物件都放置在與傳送操作的資料儲存區階層形成鏡像的階層中。 在平面階層中，「佈置」規則會將所有物件都放置在您所指定的基本容器中。

綱要映射

會將下列 Identity Vault 使用者、群組和「組織單位」屬性映射到 Active Directory 使用者和群組屬性。

表格中所列出的映射都是預設映射。您可以重新映射相同類型的屬性。

表格 ***1-3*** 所有類別的映射屬性

eDirectory	Active Directory
CN	cn
Description	description
Facsimile Telephone Number	facsimiletelephoneNumber
Full name	displayName
Given Name	givenName

eDirectory	Active Directory
Initials	initials
Internet EMail Address	mail
L	physicalDeliveryOfficeName
Locality	locality
Login Disabled	dirxml-uACAccountDisabled
Login Expiration Time	accountExpires
Physical Delivery Office Name	l
Postal Code	PostalCode
Postal Office Box	postOfficeBox
S	st
SA	streetAddress
See Also	seeAlso
Surname	sn
Telephone Number	telephoneNumber
Title	title

eDirectory 的 L 屬性會映射到 Active Directory 的 physicalDeliveryOfficeName 屬性，而 eDirectory 的 Physical Delivery Office Name 屬性會映射到 Active Directory 的 L 屬性。由於相似的具名欄位具有相同的值，所以根據此方式映射屬性可讓屬性在 ConsoleOne 和 Microsoft Management Console (MMC) 中都能正常運作。

表格 ***1-4*** 使用者的映射屬性

eDirectory	Active Directory
CN	userPrincipalName
DirXML-ADAliasName	sAMAccountName
Login Allowed Time Map	logonHours

表格 ***1-5*** 映射的組織單位屬性

eDirectory	Active Directory
Organizational Unit	organizationalUnit
OU	ou

名稱映射規則

預設組態包括兩種名稱映射規則，您可以搭配使用這兩種規則來協助協調 Identity Vault 和 Active Directory 之間不同的命名規則。使用「Active Directory 使用者和電腦」工具 (一種 Microsoft Management Console 的嵌入式管理單元，本文件中縮寫爲 MMC) 建立使用者時，您會發現使用者全名會做爲它的物件名稱。使用者物件的屬性會定義 Windows 2000 以前的登入名稱 (也稱爲 NT 登入名稱或 sAMAccountName) 以及 Windows 2000 登入名稱 (也稱爲 userPrincipalName)。使用 iManager 或 ConsoleOne 在 Identity Vault 中建立使用者時，其物件名稱和使用者登入名稱是相同的。

如果您使用 MMC 於 Active Directory 中建立一些使用者，而在 Identity Vault 或其他與 Identity Vault 同步化的已連接系統中建立另一些物件，則在相對的主控台上的這個物件會被視爲異常，因此可能無法在相對的系統上建立這個物件。

「全名映射規則」用於管理 Active Directory 中使用 Microsoft Management Console (MMC) 慣例的物件。啓用此規則，Identity Vault 中的「全名」屬性就會與 Active Directory 中的物件名稱同步化。

「NT 登入名稱映射規則」用於管理 Active Directory 中使用 Identity Vault 慣例的物件。啓用此規則，就會使用 Identity Vault 物件名稱對 Active Directory 中的物件名稱以及「NT 登入名稱」進行同步化。Active Directory 中的物件與 Identity Vault 中的物件同名，「NT 登入名稱」與 Identity Vault 登入名稱相符。

如果同時啓用兩種規則，則 Active Directory 物件名稱就是「Identity Vault 全名」，同時「NT 登入名稱」也符合 Identity Vault 登入名稱。

如果兩種規則皆被停用，則不會建立特殊映射。會同步化物件名稱，而且沒有任何特殊規則可用於建立「NT 登入名稱」。但是因爲「NT 登入名稱」是 Active Directory 中的強制屬性，所以您需要在新增操作期間使用某些方法產生一個這樣的名稱。「NT 登入名稱」(sAMAccountName) 會映射到 Identity Vault 中的 DirMXL-ADAliassName。因此，您可以使用該屬性控制 Active Directory 中的「NT 登入名稱」，或在「訂閱者建立」規則中建立自己的規則來產生一個名稱。利用此規則選項，使用 MMC 建立的使用者可使用由 MMC 產生的物件名稱做爲 Identity Vault 中的物件名稱。使用此名稱登入 Identity Vault 可能會不方便。

Windows 2000 登入名稱規則

Windows 2000 登入名稱 (也稱爲 userPrincipalName 或 UPN) 在 Identity Vault 中沒有直接對應的名稱。UPN 與電子郵件地址 (user@mycompany.com) 相似，而且實際上可能就是使用者的電子郵件名稱。在使用 UPN 時需要注意的重點就是，必須使用爲領域設定的領域名稱 (@ 符號後面的部份)，才能順利使用 UPN。新增 UPN 時，您可以透過使用 MMC 建立使用者，以及檢查領域名稱下拉式方塊，找出可用的領域名稱。

預設組態提供了幾種管理 userPrincipalName 的方法。如果已設定領域，以便使用者的電子郵件地址可用來做爲 userPrincipalName，那麼追蹤使用者電子郵件地址的這個方法就是適當的。您可以根據擁有電子郵件授權的那一方，將 userPrincipalName 放在 Identity Vault 或 Active Directory 電子郵件地址的後面。如果使用者電子郵件地址不適當，您可以選擇以使用者登入名稱加上一個既定的領域名稱來建構 userPrincipalName。如果有多個名稱可供使用，則在輸入後要更新規則才能完成選擇。如果沒有適當的選項，您可以停用預設的規則，然後寫入自己的規則。

授權

使用授權可以輕鬆整合 Identity Manager 與「Identity Manager 使用者應用程式」以及 eDirectory 中的「角色服務」。使用「使用者應用程式」時，在完成適當的核准以前，於

Active Directory 中提供帳戶的這類動作會延遲。使用「角色服務」時，會根據使用者物件的屬性而不是由一般群組成員來決定權限指定。這兩種服務都爲 Identity Manager 帶來了挑戰，因爲從物件屬性並不能清楚看出是否已授予核准或使用者是否符合角色。

授權將 Identity Vault 物件上記錄此資訊的方法加以標準化。從驅動程式角度考慮，授權會授予或撤銷 Active Directory 中的某些權限。您可以使用授權來授予 Active Directory 中的帳戶權限、控制群組成員並提供 Exchange 信箱。驅動程式無法識別「使用者應用程式」或「角色授權」。全憑「使用者應用程式」伺服器或「授權」驅動程式，根據自己的規則授予或撤銷對使用者的授權。

所以，您應該只有在想要搭配使用驅動程式與「使用者應用程式」或「角色授權」時，才啓用驅動程式的授權。

準備 Active Directory

2

本節內容：

2.1 Active Directory 先決條件

- ❑ 如需 Novell® Identity Manager 3.0 及其先決條件的清單，請參見《*Identity Manager 3.0 安裝指南*》中的「安裝 Identity Manager」一節。
- ❑ Windows 2003 Server 或 Windows 2000 Server (含 Service Pack 2 或更新版本)。
- ❑ 在執行 Active Directory (AD) 驅動程式的伺服器和目標領域控制器上，使用 Internet Explorer 5.5 或更新版本。
- ❑ 由驗證方法決定採用 Active Directory 領域控制器 DNS 名稱還是 IP 位址。

同時，我們建議代管 Active Directory 驅動程式的伺服器應是 Active Directory 領域的成員。若要提供 Exchange 信箱和同步化密碼，則這就是必要條件。如果您不需要這些功能，則只要使用「簡易」(簡易結合) 驗證模式，伺服器所在的領域可以不限。若要具有雙向密碼同步化功能，必須選取「交涉」驗證選項。

2.2 規劃安裝

您可以將 Active Directory 驅動程式安裝在領域控制器上也可以安裝在成員伺服器上。開始安裝驅動程式前，請確定以下各項：

- Active Directory 驅動程式 Shim 的安裝位置
- 如何解決安全性事宜

2.2.1 Active Directory 驅動程式和 Shim 的安裝位置

Active Directory 驅動程式 Shim 必須在其中一種受支援的 Windows 平台上執行。但是您並不需要在相同機器上安裝 Metadirectory 引擎。使用「遠端載入器」，您可以將引擎和驅動程式 Shim 分開，如此能平衡不同機器的負載或配合公司指令。

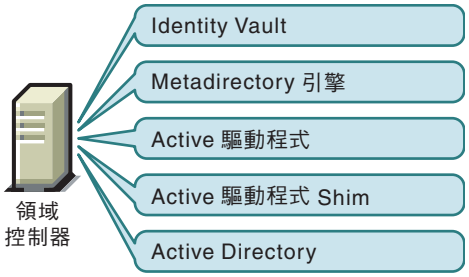
您選取的安裝案例決定了驅動程式 Shim 的安裝方式。如果您選擇在 Identity Manager 所在的機器 (Metadirectory 引擎和 Identity Vault 都位於此位置) 上安裝驅動程式 Shim，則 Identity Manager 會直接呼叫驅動程式 Shim。如果您選擇在另一台機器上安裝驅動程式 Shim，則必須使用「遠端載入器」。

驅動程式本身的安裝方式在每個案例中都是相同的。請參閱第 4 章 「設定 Active Directory 驅動程式」, 第 35 頁。

本地安裝

單一 Windows 領域控制器可以代管 Identity Vault、Metadirectory 引擎和驅動程式。

特性 **2-1** 案例 *1* - 所有元件都在一台伺服器上



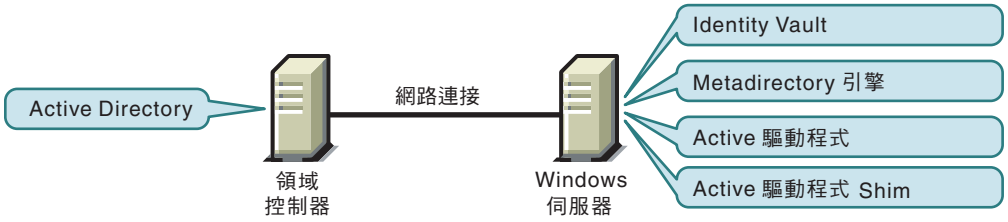
此組態適用於希望節省硬體成本的組織。同時由於 Identity Manager 和 Active Directory 之間沒有網路流量，因此它也是具有最高效能的組態。

但是，在領域控制器上代管 Identity Vault 和 Metadirectory 引擎會增加控制器上的總負載，從而增加了控制器失敗的風險。在 Microsoft 網路中領域控制器扮演著重要的角色，因此和額外硬體成本相比，很多組織更加關注的是領域驗證的速度以及領域控制器失敗的風險。

僅在 **Windows** 伺服器上進行遠端安裝

您可以將 Identity Vault、Metadirectory 引擎和驅動程式安裝在與 Active Directory 領域控制器不同的電腦上。此組態使得領域控制器可不受 Identity Manager 軟體的限制。

特性 **2-2** 案例 *2* - *Active Directory* 和驅動程式 *Shim* 位於不同伺服器

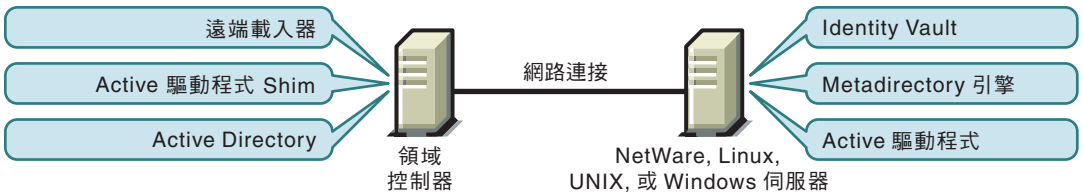


此組態適用於公司規則不允許在您的領域控制器上執行驅動程式的情況。

在 **Windows** 和其他平台上進行遠端安裝

您可以在 Active Directory 領域控制器上安裝「遠端載入器」和驅動程式 Shim，而將 Identity Vault 和 Metadirectory 引擎安裝在另一台伺服器上。

特性 **2-3** 案例 *3* - *Active Directory*、遠端載入器和驅動程式 *Shim* 在一台伺服器上



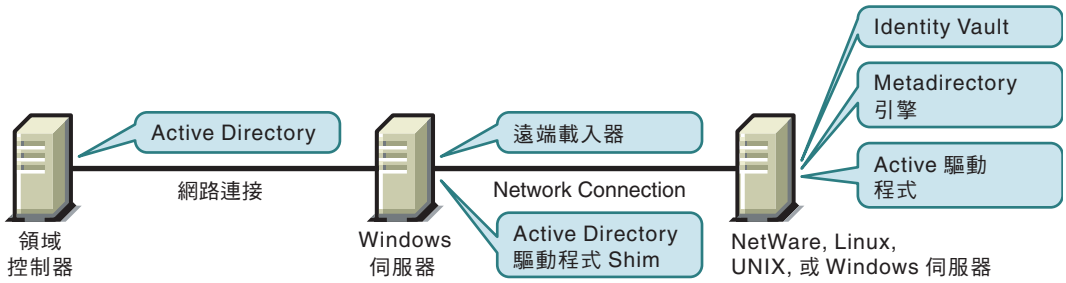
如果您將 Identity Vault 和 Metadirectory 引擎 (Identity Manager) 安裝在受支援的 Windows 版本之外的平台，則適用此組態。

案例 2 和案例 3 的組態都能消除在領域控制器上代管 Identity Vault 和 Metadirectory 引擎所造成的效能影響。

在 **Windows** 成員伺服器上進行遠端安裝

如果您有特殊的平台需求及領域控制器的限制，則可以使用三台伺服器的組態。

特性 ***2-4*** 案例 *4* - 三台伺服器組態



此組態設定起來比較複雜，但是它能適應某些組織的限制。在此圖中，兩台 Windows 伺服器都是領域的成員伺服器。

2.3 解決安全性事宜

要考量的主要安全性事宜是驗證、加密和「遠端載入器」的使用。如果您使用 Windows 2003 或 Windows 2000 SP3 或更新版本，請考量名爲簽章的安全性選項。請參閱「安全性參數」，第 53 頁中的「使用簽章」。

因爲從 Windows 獲取的安全性設定檔會因 Service Pack、DNS 伺服器基礎結構、領域規則和伺服器上之本地規則設定的不同而有所不同，所以管理安全性的方法通常比較複雜。以下章節說明安全性選擇並提供了建議的組態。在實作驅動程式以及升級元件時，須特別留意安全性事宜。

2.3.1 驗證方法

驗證可識別出 Active Directory (很可能還包括本地機器) 的驅動程式 Shim。若要驗證 Active Directory，您可以使用「交涉」方法或「簡易」(簡易結合) 方法。

表格 ***2-1*** 驗證方法

驗證方法	描述	優點	缺點
交涉	偏好的方法。 請使用 Kerberos*、NTLM 或可外掛式驗證綱要 (如果安裝了其中一種)。	驅動程式可以安裝到領域中的任何伺服器上。	代管驅動程式的伺服器必須是領域的成員。

驗證方法	描述	優點	缺點
簡易	適用於代管驅動程式 Shim 之伺服器不是領域成員的情況。	驅動程式可以安裝到領域成員之外的伺服器上。	有些提供的服務不可用，例如 Exchange 信箱提供和密碼同步化。

2.3.2 加密

保全插槽層 (SSL) 加密資料。根據您的組態，可以在兩個地方使用保全插槽層 (SSL)：

- 在 Active Directory 驅動程式和領域控制器之間
- 在 Identity Vault 和執行 Active Directory 驅動程式的「遠端載入器」之間

密碼同步化發生於 Active Directory 與 Identity Vault (eDirectory) 之間。您需要確保所有透過網路進行的通訊都使用保全插槽層 (SSL)。

如果 Metadirectory 引擎、Identity Vault、Active Directory 驅動程式和 Active Directory 位於同一台機器上，則無需使用保全插槽層 (SSL)。因爲不需要透過網路通訊。

但是，如果您使用成員伺服器上的 Active Directory 驅動程式 Shim 來遠端存取 Active Directory，則需要在 Active Directory 驅動程式 Shim 和 Active Directory 之間設定保全插槽層 (SSL)。若要設定 SSL，請在驅動程式組態上將保全插槽層 (SSL) 參數設定爲「是」。請參閱「遠端載入器和 Identity Manager 之間的保全插槽層 (SSL) 連接」，第 21 頁中的步驟 5, 第 20 頁。

如果您使用「領域控制器」上的「遠端載入器」，則可以在 Metadirectory 引擎和「遠端載入器」之間設定保全插槽層 (SSL)。如需保全插槽層 (SSL) 和「遠端載入器」的其他資訊，請參閱《*Novell Identity Manager 3.0* 管理指南》中的「設定已連接系統」。

下表概述「規劃安裝」，第 15 頁所討論之每個案例中使用保全插槽層 (SSL) 連接的位置。

表格 ***2-2*** *SSL* 連接

組態	可用的保全插槽層 (SSL) 連接
單一伺服器	不需要保全插槽層 (SSL) 連接。
兩台伺服器：Identity Manager 和 Active Directory 驅動程式在同一台伺服器上	可以在 Active Directory 驅動程式和領域控制器之間建立保全插槽層 (SSL) 連接。
雙伺服器：Identity Manager 在一台伺服器上，而 Active Directory 驅動程式在另一台伺服器上	可以在 Identity Manager 和執行 Active Directory 驅動程式的「遠端載入器」之間建立保全插槽層 (SSL) 連接。
三台伺服器	可以在 Active Directory 驅動程式和領域控制器之間建立保全插槽層 (SSL) 連接。 也可以在 Identity Manager 和執行 Active Directory 驅動程式的「遠端載入器」之間建立保全插槽層 (SSL) 連接。

Active Directory 驅動程式和「領域控制器」之間的保全插槽層 (SSL) 連接

若要建立與 Active Directory 領域控制器的保全插槽層 (SSL) 連接，必須設定爲使用保全插槽層 (SSL)。這包括設定證書權限以及建立、輸出和輸入必要的證書。

設定證書權限

大多數組織都擁有證書權限。在這種情況下，您需要輸出一個有效證書，然後將其輸入至您領域控制器上的證書儲存區。代管驅動程式 Shim 的伺服器必須託管此證書之發出證書權限所鏈結的根部證書權限。

如果您的組織沒有證書權限，則必須先建立一個。Novell、Microsoft 及其他一些協力廠商均會提供建立證書權限的必要工具。建立證書權限不在本指南的說明範圍。如需相關資訊，請參閱

- 《Novell Certificate Server™ 2.5 管理指南 (http://www.novell.com/documentation/lg/crt252/index.html)》
- 《Microsoft 逐步設定證書權限指南 (http://www.microsoft.com/windows2000/techinfo/planning/security/casetupsteps.asp)》

建立、輸出和輸入證書

具備證書權限後，要想讓輕量目錄存取協定 (LDAP) 保全插槽層 (SSL) 正常運作，輕量目錄存取協定 (LDAP) 伺服器還必須安裝適當的伺服器權限證書。同時，代管驅動程式 Shim 的伺服器必須託管發出那些證書的權限。伺服器和用戶端都必須支援 128 位元加密。

1 產生符合下列 Active Directory 輕量目錄存取協定 (LDAP) 服務要求的證書：

- 輕量目錄存取協定 (LDAP) 證書位於「本機電腦」的「個人」證書儲存區 (在程式上稱爲電腦的 「我的」證書儲存區)。
- 「本機電腦」的儲存區中必須具備與證書相符的私密金鑰，而且該金鑰必須與證書正確關聯。

  請勿對私密金鑰啓用增強式私密金鑰保護。
- 「增強金鑰使用方法」延伸包含「伺服器驗證」(1.3.6.1.5.5.7.3.1) 物件識別碼 (也稱爲 OID)。
- 領域控制器之 Active Directory 完全合法的領域名稱 (例如 DC01.DOMAIN.COM) 會出現於下列其中一個位置：
  - 「標題」欄位中的「公用名稱」 (CN)。
  - 「標題替換名稱」延伸的 DNS 項目。
- 由領域控制器和輕量目錄存取協定 (LDAP) 用戶端託管的證書權限 (CA) 發出證書。

  可以透過設定用戶端和伺服器的組態來建立託管，託管發出證書權限 (CA) 所鏈結到的根部證書權限 (CA)。

此證書允許領域控制器上的輕量目錄存取協定 (LDAP) 服務，監聽並自動接受輕量目錄存取協定 (LDAP) 和全域目錄流量的保全插槽層 (SSL) 連接。

附註：此資訊出現於 Microsoft 知識庫的文章 321051，How to Enable LDAP over SSL with a Third-Party Certificate Authority (http://support.microsoft.com/default.aspx?scid=kb;en-us;321051)。請參閱本文件以取得最新的要求和其他資訊。

---

2 以 Windows 2000 支援的下列其中一個標準證書檔案格式輸出此證書：

- 個人資訊交換 (PFX，也稱爲 PKCS #12)
- 加密訊息語法標準 (PKCS #7)
- 可辨識編碼規則 (DER) 編碼的二進位 X.509
- Base64 編碼的 X.509

3 將此證書安裝到領域控制器。

下列連結包含適用於每個支援平台的指示：

- 如何：Install Imported Certificates on a Web Server in Windows Server 2003 (http://support.microsoft.com/default.aspx?scid=kb;en-us;816794)
- HOW TO: Install Imported Certificates on a Web Server in Windows 2000 (http://support.microsoft.com/default.aspx?scid=kb;EN-US;310178)

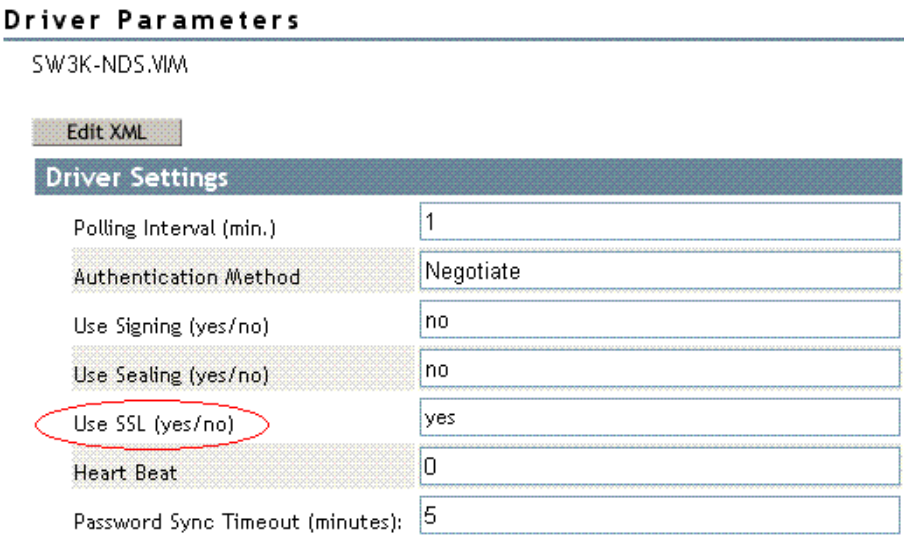
請遵循「將證書輸入至本機電腦儲存區」列出的指示。

4 請確保代管驅動程式 Shim 的伺服器和發出證書的根部證書權限之間建立有託管關係。

代管驅動程式 Shim 的伺服器必須託管發出證書權限所鏈結到的根部證書權限。

如需建立證書託管的相關資訊，請參閱「*Windows 2000 Server* 說明」中的「建立根部證書權限託管的規則」主題。

5 在 iManager 中，編輯驅動程式內容並將「使用 *SSL (是 / 否)*」選項變更爲「是」。



6 重新啓動驅動程式。

重新啓動驅動程式時，在領域控制器和執行 Active Directory 驅動程式 Shim 的伺服器之間允許使用保全插槽層 (SSL) 連接。

驗證證書

若要驗證證書，可以透過保全插槽層 (SSL) 驗證 AD。使用 Windows 伺服器上的 ldifde 指令行公用程式。若要使用 ldifde 指令：

1 開啓指令行提示

2 輸入 ldifde -f output/input file -t 636 -b administrator domain password -s computerFullName

如果是針對連接埠 636 設定您的伺服器組態，以下是可輸入之內容的範例。

ldife -f out.txt -t 636 -b administrator dxad.novell.com novell -s parent1.dxad3.lab.novell

會將輸出傳送到 out.txt 檔案。如果您開啓檔案並找到 Active Directory 中列出的物件，表示成功建立了到 Active Directory 的保全插槽層 (SSL) 連接而且證書是有效的。

2.3.3 遠端載入器和 Identity Manager 之間的保全插槽層 (SSL) 連接

如果您使用的是「遠端載入器」，則需要設定 Metadirectory 引擎和「遠端載入器」之間的保全插槽層 (SSL) 連接，還要設定驅動程式和 Active Directory 之間的設定組態。

如需建立遠端載入器和 Identity Manager 之間保全插槽層 (SSL) 連接的相關資訊，請參閱《*Novell Identity Manager 3.0* 管理指南》中的「設定遠端載入器」。

2.4 建立管理帳戶

於測試環境中，在 Active Directory 驅動程式運作之前，請先使用「管理員」帳戶。然後建立具有適當權限 (包括受限權限) 的管理帳戶，Active Directory 驅動程式可以獨佔性地使用該帳戶驗證 Active Directory。

這樣做可以讓 Identity Manager 管理帳戶不受其他管理帳戶變更的影響。此設計的優點在於：

- 您可以使用 Active Directory 稽核來追蹤 Active Directory 驅動程式的活動。
- 您可以如同使用其他帳戶一樣實作密碼變更規則，然後對驅動程式組態進行必要的更新。

此帳戶名稱和密碼儲存在驅動程式組態中。因此，一旦帳戶密碼發生變更就必須變更此密碼。如果您只變更帳戶密碼而不更新驅動程式組態，則在下一次重新啓動驅動程式時驗證會失敗。

要使「發行者」通道可以操作，此帳戶至少要具備根部領域下的「讀取」和「複製目錄變更」權限。您還需要具備對「訂閱者」通道所修改之任何物件的「寫入」權限。可將「寫入」權限限制在由「訂閱者」通道寫入的容器和屬性範圍內。

若要使用 Exchange 信箱，您的 Identity Manager 帳戶必須具備登入帳戶的「如作業系統的一部份般地執行」權限。

若要查看刪除的物件，Windows 2003 還需要您的帳戶具備其他權限。請參閱附錄 A 「變更 CN=Deleted Objects 容器的許可」，第 85 頁。

2.5 熟悉驅動程式功能

本節討論部署 Active Directory 驅動程式之前，應先熟悉的驅動程式功能：

2.5.1 多值屬性

從版本 2 開始，Active Directory 驅動程式處理多值屬性的方法發生了變更。

透過在「新增」或「修改」操作中，忽略第一次變更值之外的所有值，版本 2 將多值屬性當做「訂閱者」通道上的單一值屬性。Active Directory 驅動程式的版本 3 完全支援多值屬性。

但是，當 Active Directory 驅動程式同步化多值屬性與單一值屬性時，多值屬性會被當做單一值屬性來處理。例如，「電話號碼」屬性在 Active Directory 中是單一值屬性，但是在 Identity Vault 中是多值屬性。當從 Active Directory 同步化此屬性時，只會將單一值儲存到 Identity Vault 中。

這會在兩種屬性之間建立實質的同步化和映射，只不過在將具有多值的屬性映射成具有單一值的屬性時，可能會導致資料遺失。在大部份情況下，如果環境需要，可以透過實作規則將額外值存放在另一個位置。

2.5.2 使用自定布林值屬性管理帳戶設定

Active Directory 屬性 userAccountControl 是一個整數，其位元控制登入帳戶內容，例如是否允許登入、是否需要密碼或帳戶是否被鎖定。因爲每個布林值內容內嵌於其整數值中，所以無法個別同步化布林值內容。

在第 2 版中，Active Directory 驅動程式提供了一種捷徑，可讓您將 userAccountControl 映射至 eDirectory Login Disabled 屬性，但是不允許映射該屬性中的其他內容位元。

在第 3 版中，可以將 userAccountControl 屬性中的每個位元做爲布林值個別參考，也可以將 userAccountControl 做爲一個整數整個來管理。驅動程式會辨識 userAccountControl 中每個位元的布林值別名。這些別名包含在所有含有 userAccountControl 之類別的綱要中。別名值是在「訂閱者」通道上被接受，而在「發行者」通道上顯示出來。

此功能的優點是每個位元都可做爲布林值使用，因此位元可以在「發行者」過濾器中個別地啓用且便於存取。您也可以將 userAccountControl 放入「發行者」過濾器中，以做爲一個整數接收變更通知。

在單一組態中不可混合 userAccountControl 的整數和別名版本。

下表列出可用的別名和十六進位值。不可在「訂閱者」通道上設定唯讀屬性。

表格 ***2-3*** 別名和十六進位值

別名	十六進位	備註
dirxml-uACDontExpirePassword	0x10000	讀寫
dirxml-uACHomedirRequired	0x0008	讀寫
dirxml-uACInterdomainTrustAccount	0x0800	唯讀
dirxml-uACNormalAccount	0x0200	唯讀
dirxml-uACServerTrustAccount	0x2000	唯讀
dirxml-uACWorkstationTrustAccount	0x1000	唯讀
dirxml-uACAccountDisable	0x0002	讀寫
dirxml-uACPasswordNotRequired	0x0020	讀寫

如需 userAccountControl 屬性相關的疑難排解秘訣，請參閱 「Active Directory 帳戶在使用者新增到「訂閱者」通道後關閉」，第 82 頁。

2.5.3 使用 homeMDB 屬性提供 Exchange 信箱

從第 2 版開始，用於提供 Exchange 2000 和 Exchange 2003 信箱的選項已經有所變更。

在第 2 版中，透過設定「使用者」物件上的屬性來完成 Exchange 提供。Microsoft 程式 (收件者更新服務) 使用本資訊提供 Exchange 資料庫。

此方法在 Active Directory 驅動程式的第 3 版中仍可使用，但新增了一種新的方法 (CDOEXM)。啓用了 CDOEXM，就可以透過設定 homeMDB 屬性來提供 Exchange 信箱。設定 homeMDB 屬性時，驅動程式會自動設定所有必要的屬性。

homeMDB 屬性是在啓始組態設定期間設定的，不過，您可以透過修改驅動程式規則來變更此設定。如需此參數的相關討論，請參閱 「組態參數」，第 36 頁。

2.5.4 Active Directory 中的過期帳戶

如果將 Login Expiration Time 的 eDirectory 屬性映射到 accountExpires 的 Active Directory 屬性，Active Directory 中的帳戶會在比 eDirectory 中設定的過期時間早一天過期。

發生此狀況是因爲 Active Directory 設定的 accountExpires 屬性值是以一天爲單位遞增。Login Expiration Time 的 eDirectory 屬性是使用特定的帳戶過期日期與時間。

例如，如果 eDirectory 中帳戶的過期日期設定爲 2006 年 7 月 15 日下午 5:00，則在 Active Directory 中此帳戶最後一天的有效日期是 7 月 14 日。

如果將 Microsoft Management Console (MMC) 中的帳戶過期時間設定爲 2006 年 7 月 15 日，則 Login Expiration Time 的 eDirectory 屬性會設定爲在 2006 年 7 月 16 日上午 12:00 過期。因爲 Microsoft Management Console (MMC) 不允許設定時間值，其預設值是上午 12:00。

驅動程式會使用最受限制的設定。您可以根據要求將 Microsoft 中的過期時間延長一天。

2.5.5 在還原 Active Directory 物件時保留 eDirectory 物件

透過 Active Directory 工具還原的任何 Active Directory 物件會在進行同步化時，刪除相關聯的 eDirectory 物件。Active Directory 驅動程式會尋找 Active Directory 物件之 isDeleted 屬性中的變更。當驅動程式偵測到此屬性中的變更時，會透過與 Active Directory 物件相關聯之物件的驅動程式發出刪除事件。

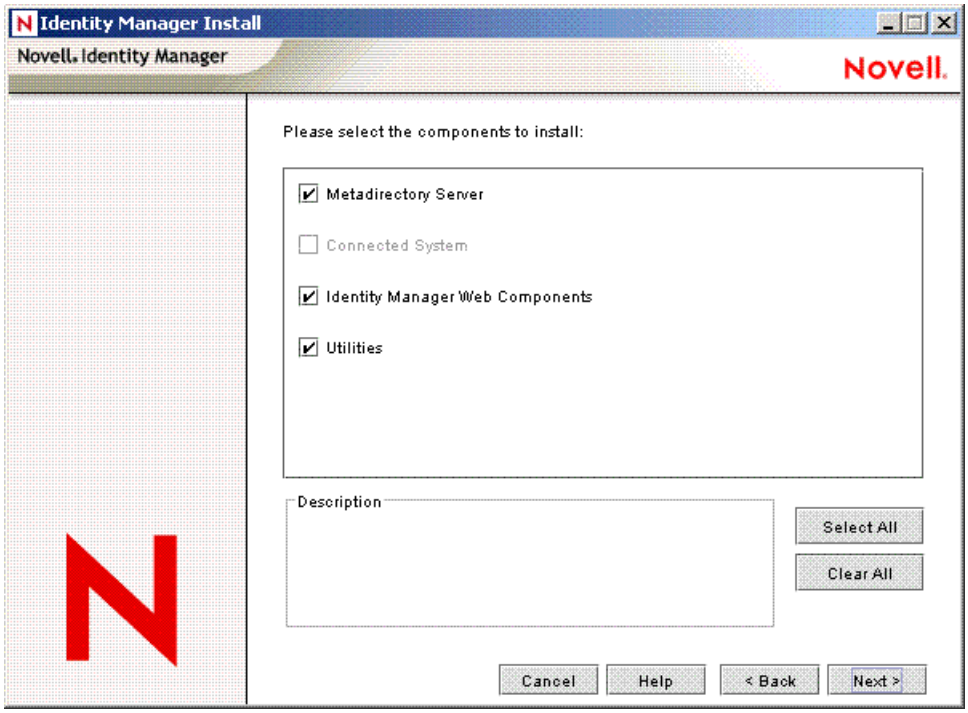
如果您不想刪除 eDirectory 物件，必須爲 Active Directory 驅動程式新增其他規則。Identity Manager 3.0 附有預先定義的規則，此規則會將所有的「刪除」事件變更爲「移除關聯」事件。如需相關資訊，請參閱《規則產生器和驅動程式自訂指南》中的「指令轉換：要停用的發行者刪除」。

安裝 Active Directory 驅動程式 3

3.1 基本步驟

下圖說明安裝 Identity Manager 時可選取的選項。

特性 ***3-1*** *Identity Manager* 安裝選項



表格 ***3-1*** *Identity Manager* 安裝選項

選項	描述
Metadirectory 伺服器	安裝 Metadirectory 引擎和 Identity Manager。
已連接系統	安裝遠端載入器
Identity Manager Web 元件	安裝預先設定的 (範例) 驅動程式組態檔案
公用程式	安裝 Active Directory 探查工具

安裝 Active Directory 驅動程式 Shim 需要三個基本步驟：

表格 *3-2* 安裝步驟

步驟	安裝時選取的內容
1. 在 Metadirectory 引擎伺服器或「遠端載入器」伺服器上安裝 Active Directory 驅動程式 Shim。	選取「Metadirectory 伺服器」或「Identity Manager 已連接系統」選項。請參閱「安裝 Active Directory 驅動程式 Shim」，第 26 頁。
2. 在 iManager 伺服器上安裝預先設定的 Active Directory 輸入檔案。	選取「Identity Manager Web 元件」選項。請參閱「安裝預先設定的輸入檔案」，第 31 頁。
3. 在用來設定 Identity Manager 的工作站上安裝「Active Directory 探查工具」。	選取「公用程式」選項。請參閱「安裝 Active Directory 探查工具」，第 32 頁。

通常，在安裝 Metadirectory 伺服器 (或「遠端載入器」) 和 Web 元件時，可一併安裝 Active Directory 驅動程式元件。不過，您也可以稍後再安裝它們。

3.2 安裝 Active Directory 驅動程式 Shim

3.2.1 在 Metadirectory 伺服器上安裝 Shim

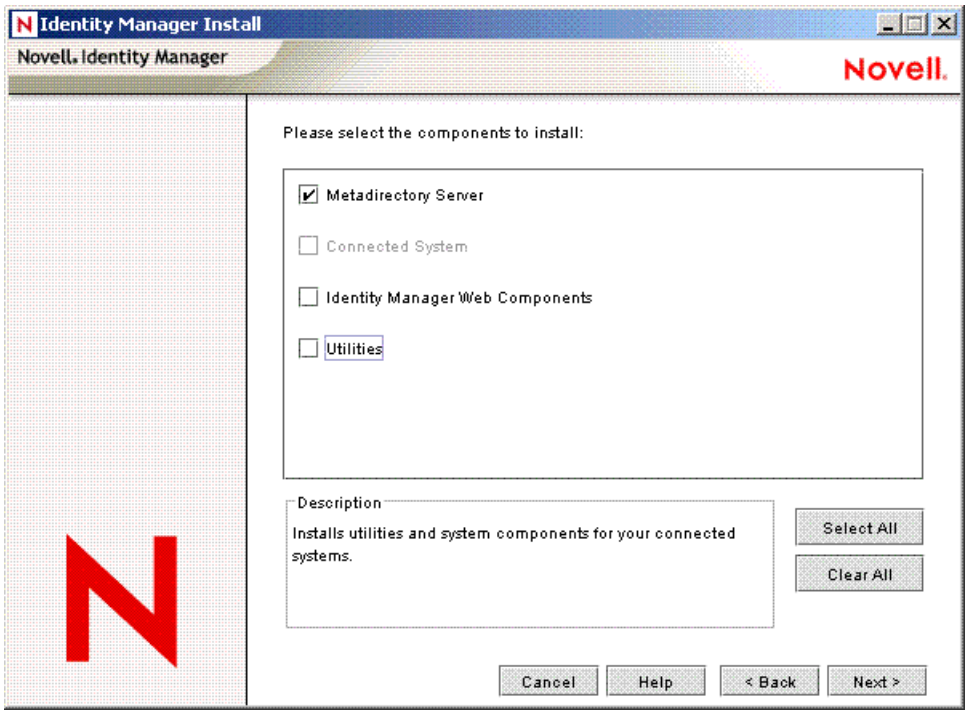
1. 在執行 Identity Vault 和 Metadirectory 引擎的伺服器上，啓動 Identity Manager 安裝。

   從 Identity Manager CD 或下載的影像檔執行安裝程式。
2. 在「歡迎」對話方塊中，按「下一步」，然後接受授權合約。
3. 在第一個「Identity Manager 概觀」對話方塊中，檢視資訊，然後按「下一步」。

   對話方塊會提供下列資訊：
   - Metadirectory 伺服器
   - 已連接系統伺服器
4. 在第二個「Identity Manager 概觀」對話方塊中，檢視資訊，然後按「下一步」。

   對話方塊會提供下列資訊：
   - Web 型態的管理伺服器
   - 公用程式

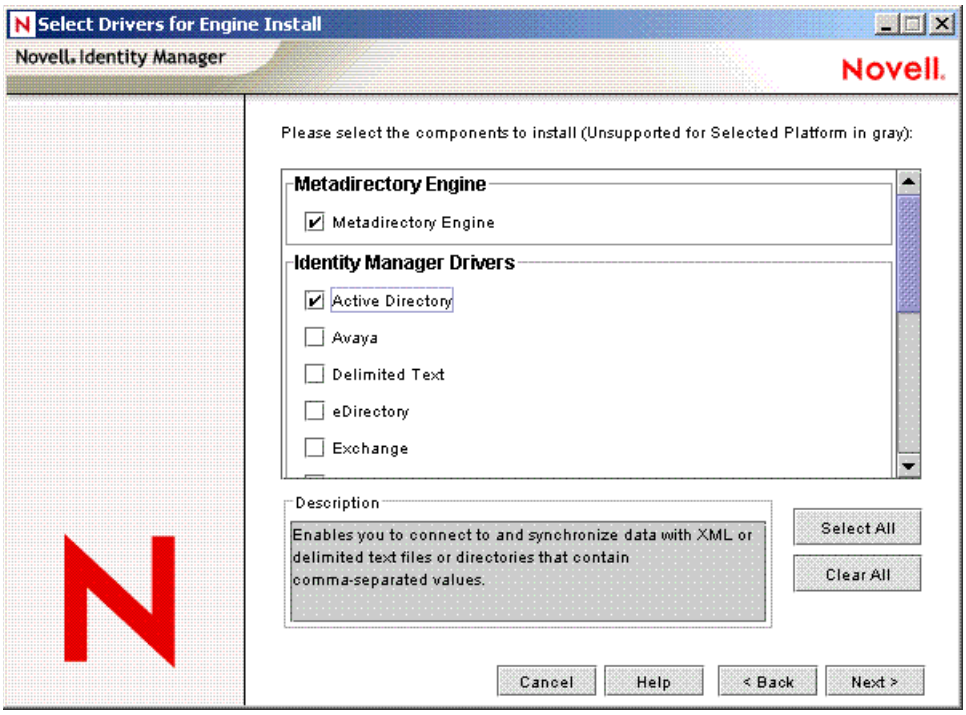
5 在「請選取要安裝的元件」對話方塊中，選取「*Metadirectory* 伺服器」，然後按「下一步」。



如果在此機器上已經安裝了 iManager，且您想在此時安裝 iManager 外掛程式和組態檔案，則也應選取「*Identity Manager Web* 元件」。

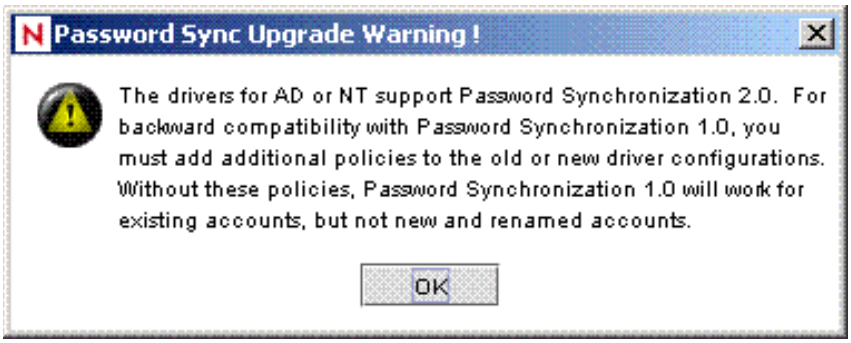
如果您想在此時安裝「Active Directory 管理」工具，則也應選取「公用程式」。

6 在「選取要安裝的引擎驅動程式」對話方塊中，選取「*Metadirectory* 引擎」，然後選取「*Active Directory*」，再按「下一步」。



7 在「Identity Manager 升級警告」對話方塊中，按一下「確定」。

8 在「密碼同步化升級警告」對話方塊中，按一下「確定」。



9 在「綱要延伸」對話方塊中，輸入使用者名稱和密碼，然後按「下一步」。

10 檢視所選取的選項，然後按一下「完成」。

3.2.2 在「遠端載入器」上安裝 Shim

此選項可讓您安裝 Active Directory 驅動程式 Shim，以便在執行 Metadirectory 引擎以外的伺服器上執行。

1 在執行「遠端載入器」的伺服器上，啓動 Identity Manager 安裝。

從 Identity Manager CD 或下載的影像檔執行安裝程式。

2 在「歡迎」對話方塊中，按「下一步」，然後接受授權合約。

3 在第一個「Identity Manager 概觀」對話方塊中，檢視資訊，然後按「下一步」。

對話方塊會提供下列資訊：

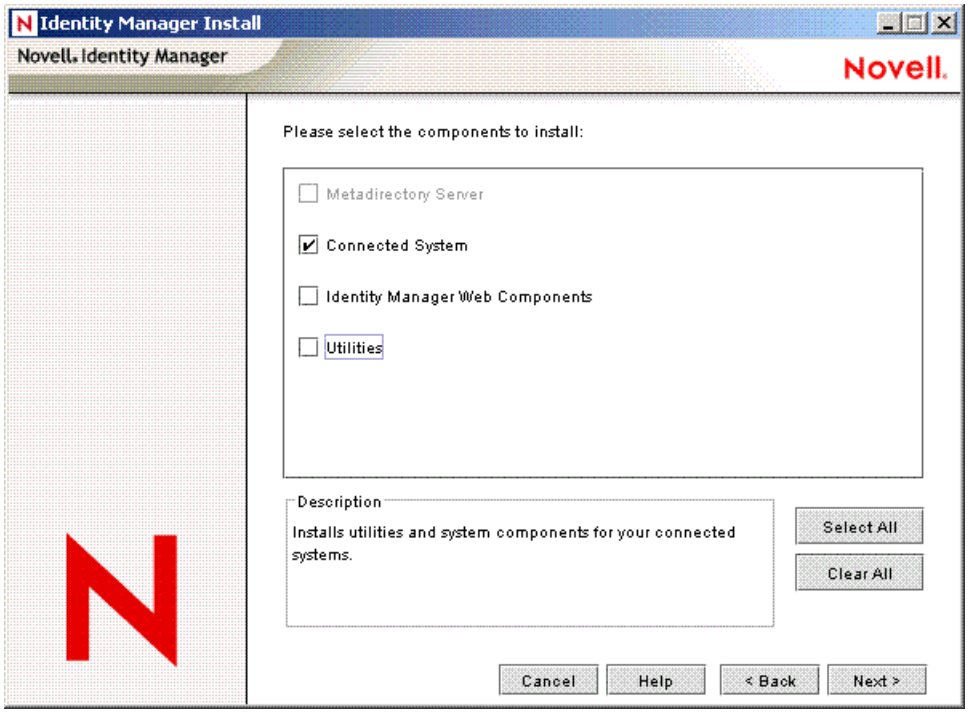
- Metadirectory 伺服器
- 已連接系統伺服器

4 在第二個「Identity Manager 概觀」對話方塊中，檢視資訊，然後按「下一步」。

對話方塊會提供下列資訊：

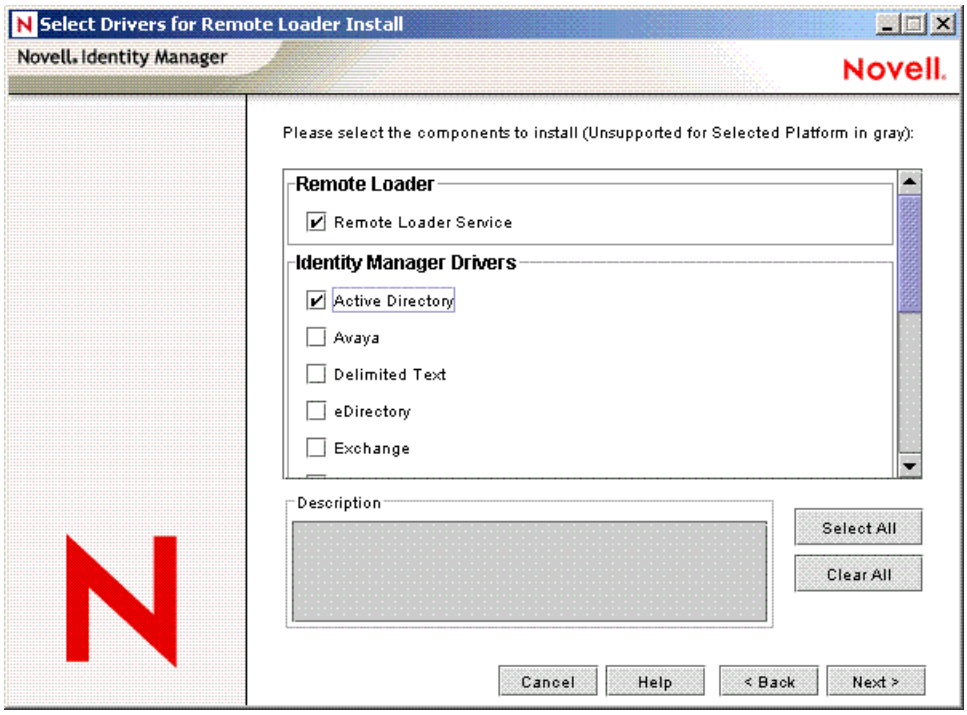
- Web 型態的管理伺服器
- 公用程式

5 在「請選取要安裝的元件」對話方塊中，取消選取「*Metadirectory* 伺服器」和其他選項，選取「*Identity Manager* 已連接系統」，然後按「下一步」。

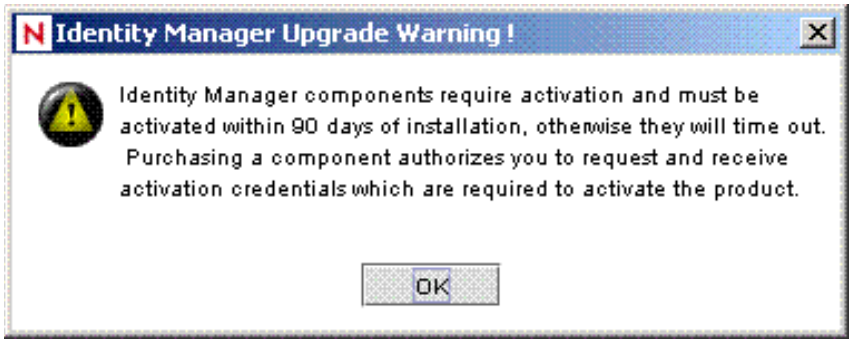


6 指定安裝路徑，然後按「下一步」。

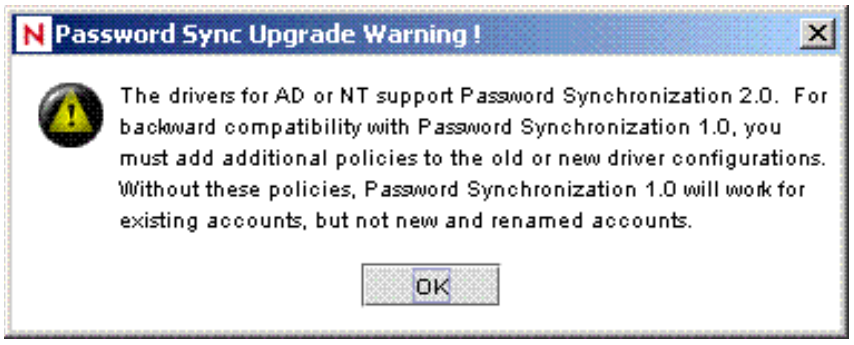
7 在「選取要安裝的引擎驅動程式」對話方塊中，選取「遠端載入器服務」，然後選取「*Active Directory*」，再按「下一步」。



8 在「Identity Manager 升級警告」對話方塊中，按一下「確定」。



9 在「密碼同步化升級警告」對話方塊中，按一下「確定」。



10 檢視所選取的選項，然後按一下 「完成」。

3.3 安裝預先設定的輸入檔案

此選項會安裝 Identity Manager 外掛程式和預先設定的 (範例) 驅動程式組態。安裝完這些檔案後，就可以使用 iManager 將 Active Directory 預先設定的檔案輸入至驅動程式集並設定驅動程式。

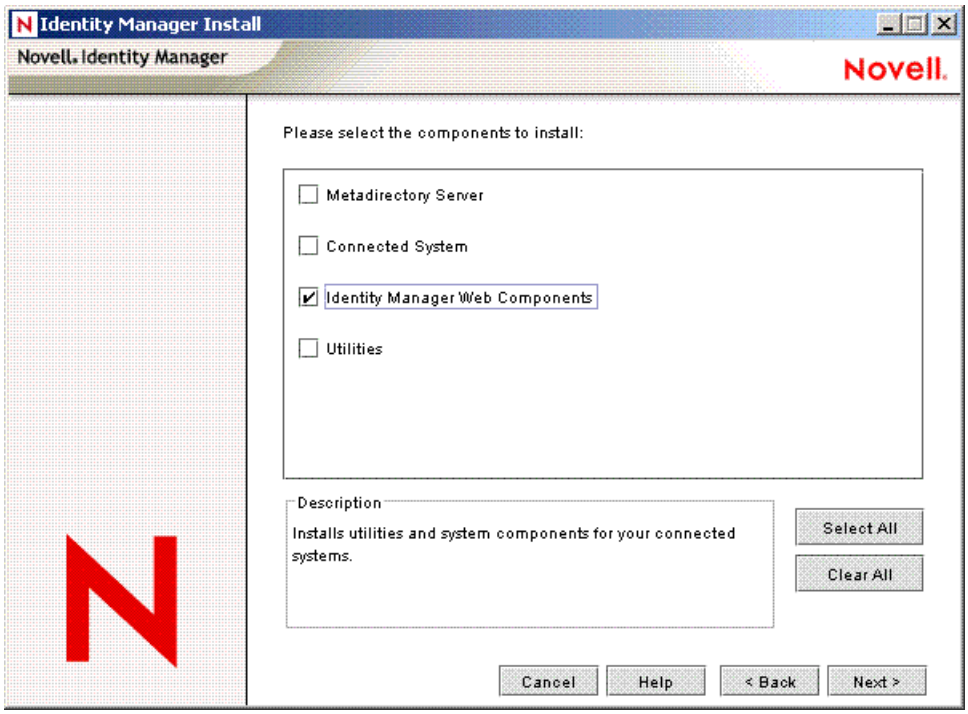
在安裝 Metadirectory 引擎或 「遠端載入器」時，您可能已經安裝了這些檔案。若要個別安裝這些檔案：

1 請在安裝有 iManager 的伺服器上，啓動 Identity Manager 安裝。

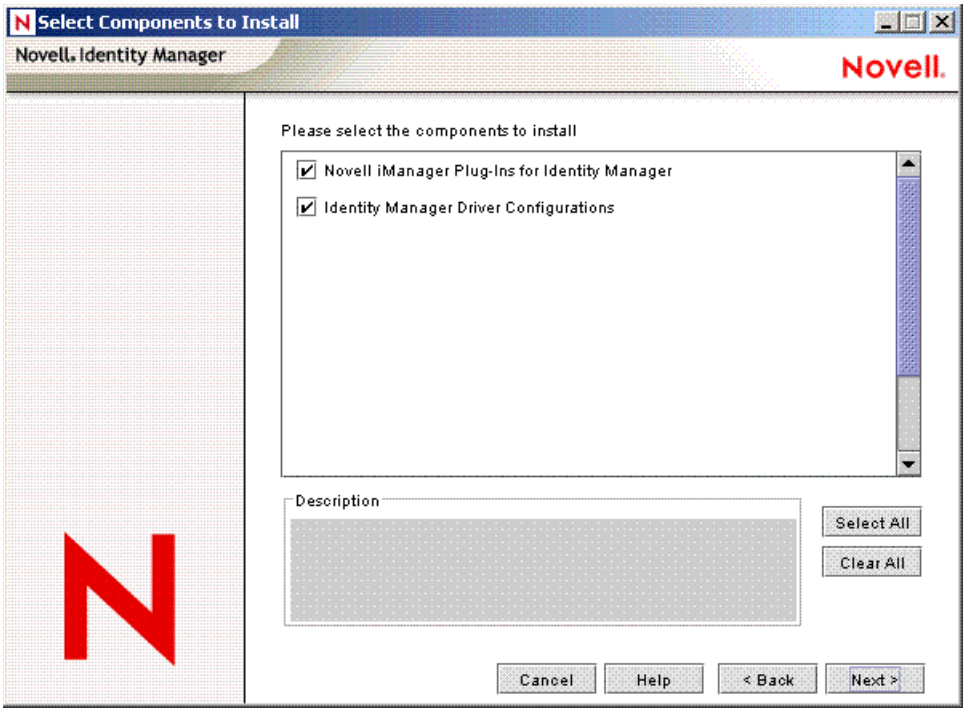
2 在 「歡迎」對話方塊中，按 「下一步」，然後接受授權合約。

3 在第二個 「Identity Manager 概觀」對話方塊中，檢視資訊，然後按 「下一步」。

4 在 「請選取要安裝的元件」對話方塊中，取消選取除了 「*Identity Manager Web* 元件」之外的所有選項，然後按 「下一步」。



5 選取「 *Identity Manager* 驅動程式組態」，然後按「下一步」。



在安裝 Novell iManager 外掛程式時，您可以一併安裝驅動程式組態檔案，或者個別安裝這些檔案。

6 檢視所選取的選項，然後按一下「完成」。

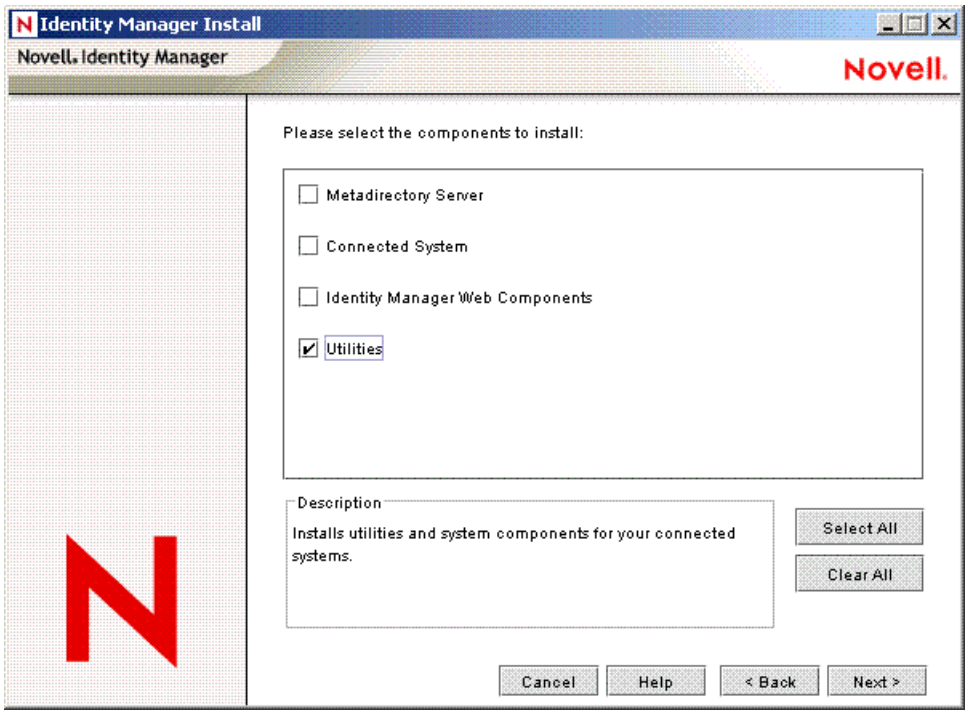
3.4 安裝 Active Directory 探查工具

1 在您用來設定 Active Directory 的工作站上，啓動 Identity Manager 安裝。

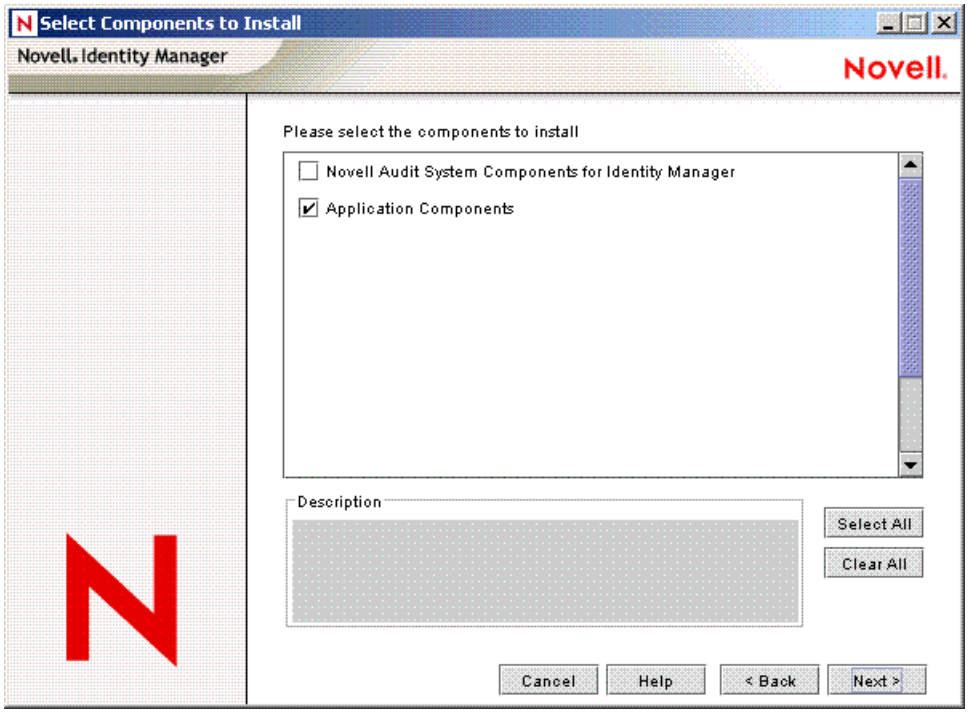
2 在「歡迎」對話方塊中，按「下一步」，然後接受授權合約。

3 在第二個「Identity Manager 概觀」對話方塊中，檢視資訊，然後按「下一步」。

4 在「請選取要安裝的元件」對話方塊中，取消選取除了「公用程式」之外的所有選項，然後按「下一步」。



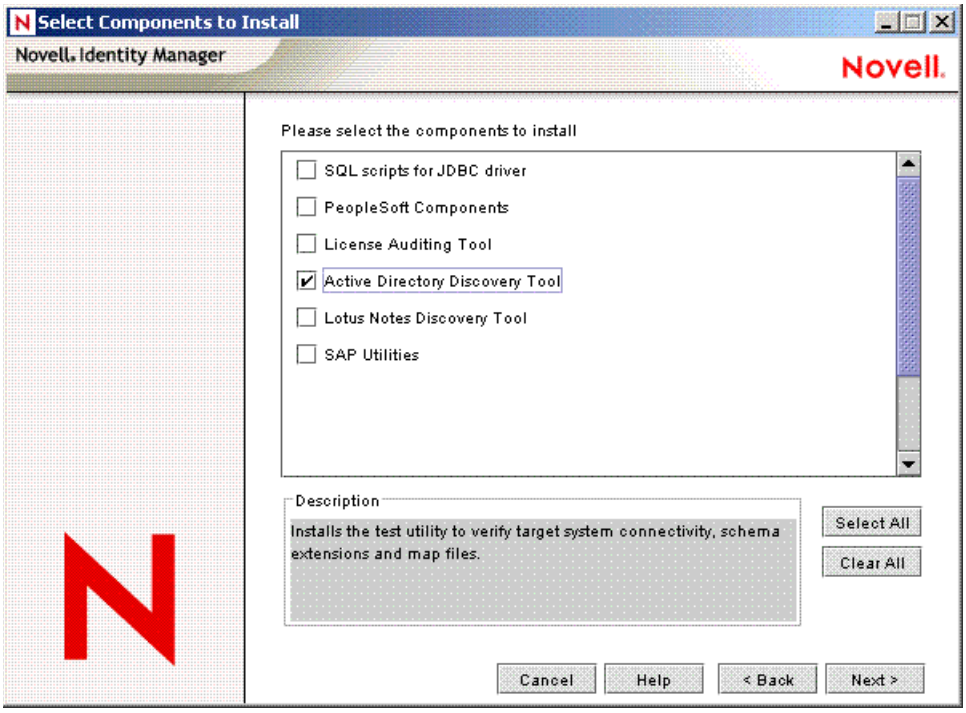
5 選取「應用程式元件」，然後按「下一步」。



取消選取 Identity Manager 的「Novell Audit 系統元件」。

6 指定安裝路徑，然後按「下一步」。

7 僅選取「*Active Directory* 探查工具」，然後按「下一步」。



8 檢視所選取的選項，然後按一下「完成」。

4 設定 Active Directory 驅動程式

在 Novell® iManager 中，您可以使用 「建立驅動程式精靈」協助輸入 Active Directory 的基本驅動程式組態。此精靈會建立並設定使驅動程式正常運作所需的物件。如需使用此精靈的詳細資訊，請參閱 《*Novell Identity Manager 3.0* 管理指南》中的 「建立並設定驅動程式」。

本節內容：

4.1 在 Designer 中輸入驅動程式組態檔案

Designer 可以讓您輸入 Active Directory 的基本驅動程式組態檔案。此檔案會建立並設定使驅動程式正常運作所需的物件和規則。下列指示說明建立驅動程式和輸入驅動程式組態的方法。

輸入驅動程式組態檔案的方法有很多種。此程序僅記錄其中一種方法。

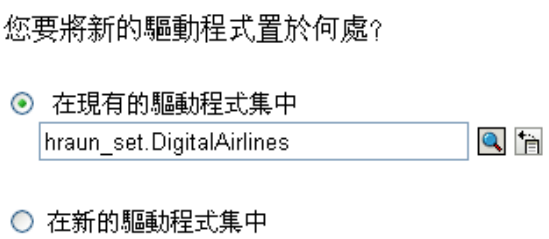
1. 在 Designer 中開啓專案，並以滑鼠右鍵按一下模擬器中的 「驅動程式集」物件，並選取 「新增已連接的應用程式」。
2. 從下拉式清單中選取 「*ActiveDirectory.xml*」，然後按一下 「執行」。
3. 在 「執行提示驗證」視窗中，按一下 「是」。它會要您填入所有的欄位以正確設定 Active Directory 驅動程式。
4. 利用填入欄位來設定驅動程式。請指定您環境的特定資訊。如需這些設定的相關資訊，請參閱 「組態參數」，第 36 頁。
5. 指定參數後，按一下 「確定」以輸入驅動程式。
6. 輸入驅動程式後，自定並測試該驅動程式。
7. 驅動程式測試全部完成之後，再將驅動程式部署到 Identity Vault。請參閱 《*Designer for Identity Manager 3*：管理指南》中的 「部署驅動程式至 Identity Vault」。

4.2 在 iManager 中輸入驅動程式組態檔案

Active Directory 預先設定檔案是一個範例組態檔案。當您在 iManager 伺服器上安裝 Identity Manager Web 元件時就會安裝此檔案。可將該預先設定檔案當做針對您的環境進行輸入、自定或設定的範本。

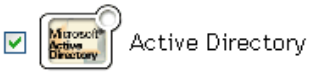
1. 在 iManager 中，選取 「*Identity Manager* 公用程式」 > 「輸入驅動程式」。

2 選取驅動程式集，然後按 「下一步」。



如果您將此驅動程式置於新的驅動程式集中，則必須指定驅動程式集名稱、網路位置和相關聯的伺服器。

3 選取 「*Active Directory*」驅動程式，然後按 「下一步」。



4 利用填入組態參數來設定驅動程式。如需這些設定的相關資訊，請參閱 「組態參數」，第 36 頁。

5 用使用者物件來定義安全性等值，而該物件擁有驅動程式在伺服器上所需具備的權限。

此任務通常是使用 「管理員」使用者物件。不過，您可能要建立 DriversUser (舉例來說)，並將安全性等值指定給該使用者。不管驅動程式在伺服器上所需具備的權限爲何，DriversUser 物件都必須具有相同的安全性權限。

6 識別所有代表管理角色的物件，並將它們從複製中排除。

排除在步驟 2 中所指定的安全性等值物件 (例如，DriversUser)。如果您刪除該安全性等值物件，即表示您已從驅動程式中移除權限。因此，驅動程式無法對 Identity Manager 進行變更。

7 按一下 「完成」。

4.3 組態參數

下表說明在啓始驅動程式組態期間必須提供的參數。

附註：這些參數會顯示在數個畫面上，而某些參數則只會在先前提示的回答需要更多資訊才能正確設定規則的組態時顯示。

表格 ***4-1*** 組態參數

欄位	描述
驅動程式名稱	指定給此驅動程式的 eDirectory™ 物件名稱。 由於每個 Active Directory 領域需要個別的驅動程式，所以驅動程式名稱中應包含領域名稱。這樣當您查看驅動程式時，便知道與之關聯的是哪個領域。

欄位	描述
驗證方法	使用 Active Directory 進行驗證的方法。 偏好的方法是「*交涉*」。選取「交涉」以使用 Microsoft 安全性套件進行驗證的交涉。若要使用「交涉」，裝載驅動程式的伺服器必須是領域的成員。 如果您規劃使用密碼同步化並且要在成員伺服器上執行，則需要 SSL。 「*簡易*」使用 LDAP 簡易結合。如果您選取「簡易」，建議使用 SSL。 重要：簡易結合不支援密碼同步化或 Exchange 提供。
驗證 ID	Identity Manager 所使用之具有管理特權的 Active Directory 帳戶。使用的名稱格式由所選取的驗證機制而定。 如果是「交涉」，請提供 Active Directory 驗證機制所需的名稱格式。例如： ◆ 管理員：AD 登入名稱 ◆ 領域 / 管理員：領域合法的 AD 登入名稱 如果是「簡易」，請提供 LDAP ID。例如： ◆ cn=DirXML,cn=Users,DC=domain,dc=com
驗證密碼	在驗證 ID 中指定之使用者帳戶的密碼。
驗證網路位置	用於同步化之 Active Directory 領域控制器的名稱。 例如，如果是「交涉」驗證法，請使用 DNS 名稱 mycontroller.domain.com。如果是「簡易」驗證法，可以使用伺服器的 IP 位址 (例如，10.10.128.23 或 DNS 名稱)。 如果未指定值，則會使用本地主機。 附註：此值儲存在「驗證網路位置」屬性中。若要在啓始組態設定後變更此值，請遵循「安全性參數」，第 53 頁中的說明修改此屬性。
領域名稱	由此驅動程式管理的 Active Directory 領域。 驅動程式需要 LDAP 格式的領域名稱 dc=domain,dc=com
領域 DNS 名稱	由此驅動程式管理之 Active Directory 領域的 DNS 名稱。 驅動程式需要 DNS 格式的領域名稱 domain.com
驅動程式輪詢間隔	Identity Vault 會在發生變更時立即將變更傳送至 Active Directory。但是，Active Directory 的變更只會按照設定的輪詢間隔傳送至 Identity Vault。預設值是 1 分鐘。 重要：輪詢間隔會影響系統效能。輪詢間隔越小，則搜尋越頻繁，資料更新也就越快。而較大的輪詢間隔會產生週期性的流量湧進。雖然輪詢間隔越小整體成本越高，但是成本按時間分攤會更平均。 如果設定間隔爲 0 (零)，則輪詢會每十秒進行一次。

欄位	描述
密碼同步化逾時 (分)	驅動程式嘗試同步化密碼所需花費的分鐘數。 要將此值設定得夠大，才足以處理任何已存在密碼的暫時積存。如果要進行大量變更，請將逾時設定得夠大以處理所有的變更。一般規則是允許一秒鐘處理一個密碼。例如，同步化 18,000 個密碼允許花費的時間爲 300 分鐘 (18,000 個密碼除以 60 秒)。 如果設定值爲 -1，表示時間無限。此設定雖然可以處理大量變更，但可能會導致問題。例如，某個密碼可能會因爲帳戶未關聯，而永遠無法同步化。此密碼就會永遠保留在系統中。許多類似情況都可能導致系統中儲存大量的未同步化密碼。 密碼同步化逾時必須設定爲至少是輪詢間隔的三倍。
驅動程式爲本地 / 遠端	選取「*遠端*」以設定與「遠端載入器」服務一起使用的驅動程式，或選取「*本地*」以設定供本地使用的驅動程式。
遠端主機名稱和連接埠	僅限「遠端」選項。 安裝有「遠端載入器服務」並爲此驅動程式執行的主機名稱或 IP 位址和連接埠號碼。預設的連接埠爲 8090。 只有將「驅動程式爲本地 / 遠端」設定爲「遠端」時，才會顯示此設定。
驅動程式密碼	僅限「遠端」選項。 「遠端載入器」使用「驅動程式物件密碼」向 Identity Manager 伺服器執行自我驗證。此密碼必須與「遠端載入器」上指定的「驅動程式」物件密碼相同。 只有將「驅動程式爲本地 / 遠端」設定爲「遠端」時，才會顯示此設定。
遠端密碼	僅限「遠端」選項。 「遠端載入器」密碼是用於控制對「遠端載入器」例項的存取。此密碼必須與「遠端載入器」上指定的「遠端載入器」密碼相同。 只有將「驅動程式爲本地 / 遠端」設定爲「遠端」時，才會顯示此設定。
輸入將繼續沿用驅動程式規則的選取	僅限「遠端」選項。 *確定*，如果您按一下該按鈕，驅動程式精靈會繼續進行伺服器規則的組態設定。
eDirectory 中的基本容器	指定 Identity Vault 中用於同步化的基本容器。此容器在「訂閱者相符」規則中是用來限制要同步化的 Identity Vault 物件，而在「發行者佈置」規則中的使用時機則是在將物件新增到 Identity Vault 時。 根據預設，新使用者是放置在此容器中。使用點格式。例如， users.myorg 如果該容器不存在，則必須先予以建立並確保其與 Active Directory 基本容器相關聯，然後再嘗試將使用者新增到此容器。

欄位	描述
發行者佈置	「*鏡像複製*」會將物件按階層放置於基本容器中。 「*平面*」會嚴密地將物件放置於基本容器中。 此選項會建立預設的「發行者佈置」規則。 附註：如果選取「*鏡像複製*」，驅動程式會假設 eDirectory 資料庫的結構與 eDirectory 基本容器中之 Active Directory 資料庫的結構相同。如果兩者的結構不同，便無法正確放置物件。請在 Active Directory 中建立與 eDirectory 中已存在之資料庫結構相同的結構，或者在移轉「使用者」物件前先移轉 eDirectory 容器。
Active Directory 中的基本容器	以 LDAP 格式指定 Active Directory 中的基本容器。根據預設，新使用者是放置在此容器中。例如， CN=Users,DC=MyDomain,DC=com 如果目標容器不存在，則必須先予以建立並確保其與 eDirectory 基本容器相關聯，然後再嘗試將使用者新增到此容器。 如果您使用或建立的是 Active Directory「使用者」以外的容器，則容器會是 OU 而不是 CN。例如， OU=Sales,OU=South,DC=MyDomain,DC=com
Active Directory 佈置	「*鏡像複製*」會將物件按階層放置於基本容器中。 「*平面*」會嚴密地將物件放置於基本容器中。 此選項會建立預設的「訂閱者佈置」規則。 附註：如果選取「*鏡像複製*」，驅動程式會假設 Active Directory 中資料庫的結構與 Active Directory 基本容器中之 eDirectory 資料庫的結構相同。如果兩者的結構不同，便無法正確放置物件。請在 eDirectory 中建立與 Active Directory 中已存在之資料庫結構相同的結構，或者在移轉「使用者」物件前先移轉 Active Directory 容器。

欄位	描述
設定資料流程	「設定資料流程」會建立啓始驅動程式過濾器，此過濾器可用來控制要進行同步化處理的類別和屬性。此選項的目的在於設定驅動程式的組態，以最適當的方式表示一般資料流程的規則。輸入後就可以對其進行變更以反映特定要求。 「*雙向*」選項會將類別和屬性設定成可同時在「發行者」和「訂閱者」通道上進行同步化。變更不論是發生在 Identity Vault 上還是 Active Directory 上，都會反映在另一方。如果您想讓雙方都做爲資料的授權來源，請使用此選項。 「*AD 至 Vault*」選項會將類別和屬性設定成僅可在「發行者」通道上進行同步化。在 Active Directory 上發生的變更會反映在 Identity Vault 上，但反之發生在 Identity Vault 上的變更則會被忽略。如果您想讓 Active Directory 做爲資料的授權來源，請使用此選項。 「*Vault 至 AD*」選項會將類別和屬性設定成僅可在「訂閱者」通道上進行同步化。在 Identity Vault 上發生的變更會反映在 Active Directory 上，但反之發生在 Active Directory 上的變更則會被忽略。如果您想讓 Identity Vault 做爲資料的授權來源，請使用此選項。 警告：刪除。「移動」和「重新命名」事件與過濾器無關。選取哪個選項並不重要，因爲這些事件由驅動程式處理。如果不想同步化這些事件，則必須變更驅動程式的預設組態。 您可以使用 Identity Manager 3.0 隨附的其中一個預先定義規則，將「刪除」事件變更爲「移除關聯」事件。如需相關資訊，請參閱《*規則產生器和驅動程式自訂指南*》中的「指令轉換：要停用的發行者刪除」。 若要阻止「移動」和「重新命名」事件，則必須自定驅動程式。
密碼失敗通知使用者	將密碼同步化規則設定爲密碼更新失敗時以電子郵件通知相關使用者。您也可以選擇將通知電子郵件的副本傳送給其他使用者，例如安全管理員。如果想要傳送副本，請輸入或瀏覽該使用者的 DN。否則，請將此欄位保留空白。
設定授權	可以將驅動程式設定爲使用「授權」來管理 Active Directory 中的使用者帳戶和群組成員，並提供 Exchange 信箱。使用「授權」時，驅動程式要搭配使用外部服務 (如 Identity Manager 「使用者應用程式」或「角色授權」)，以控制 Active Directory 中提供或取消提供這些功能的條件。如需相關資訊，請參閱 「授權」，第 13 頁。 如果您規劃使用這些外部服務的其中一項來控制對 Active Directory 的提供，請選取「*是*」。 如果您沒有規劃使用 Identity Manager「使用者應用程式」或提供 Exchange 信箱，請選取「*否*」，。
使用者帳戶規則	僅限「設定元素」選項。 可以透過同步化或搭配使用「授權」與「工作流程」服務或「角色授權」，來控制 Active Directory 中的使用者帳戶。 「*授權*」讓 Identity Vault 中的「授權」可以在 Active Directory 中控制帳戶的啓用。 「*規則實作*」使用的是驅動程式中的規則而不是「授權」。

欄位	描述
Exchange 規則	僅限「設定元素」選項。 可由驅動程式規則和「授權」來處理 Exchange 提供，或者完全忽略。可以爲使用者指定 Exchange 信箱 (使用者擁有信箱功能)，或者將外部信箱的相關資訊儲存在 Identity Vault 記錄中 (使用者擁有郵件功能)。使用驅動程式規則時，完全由規則來控制是採用信箱啓用使用者還是郵件啓用使用者，以及儲存帳戶的 Exchange 訊息資料庫。 使用「*授權*」時，外部服務 (如「工作流程」服務或「角色授權」) 會做出這些決定，而驅動程式規則只需套用它們。 「*規則實作*」使用驅動程式中的規則 (而不是「授權」) 來指定 Exchange 信箱。 如果選取「*無*」，則預設組態不會建立 Exchange 信箱，但是會同步化 Identity Vault 網際網路電子郵件地址與 Active Directory 郵件屬性。
群組成員規則	僅限「設定元素」選項。 可以透過同步化成員清單或使用「授權」來控制 Active Directory 中的群組成員。 「*授權*」使用「工作流程」服務或「角色授權」來指定群組成員。 「*同步化*」使用規則來同步化群組成員清單。 「*無*」不會同步化群組成員資訊。
將 CDOEXM 用於 Exchange (是 / 否)	僅限「Exchange 規則」選項。 可以透過呼叫 Microsoft Exchange 管理系統 (而不是一般的屬性同步) 來控制 Exchange 信箱。啓用此選項後，驅動程式 Shim 會攔截對 Active Directory homeMDB 屬性的變更，並呼叫 CDOEXM (Collaboration Data Objects for Exchange Management) 子系統。 您在此處選擇的值會被記錄到驅動程式 Shim 組態中。 「*是*」同步化 Exchange 信箱。 「*否*」不同步化 Exchange 信箱。
允許移動 CDOEXM Exchange 信箱 (是 / 否)	僅限「Exchange 規則」選項。 啓用此選項後，驅動程式 Shim 會攔截對 Active Directory homeMDB 屬性的修改，並呼叫 CDOEXM 將信箱移至新的訊息資料儲存庫。 「*是*」移動 Exchange 信箱。 「*否*」不移動 Exchange 信箱。
允許刪除 CDOEXM Exchange 信箱 (是 / 否)	僅限「Exchange 規則」選項。 啓用此選項後，驅動程式 Shim 會攔截對 Active Directory homeMDB 屬性的移除，並呼叫 CDOEXM 刪除信箱。 「*是*」允許刪除 Exchange 信箱。 「*否*」不允許刪除 Exchange 信箱。

欄位	描述
預設 Exchange MDB	僅限規則選項中的「Exchange 規則」>「實作」。 輸入預設 Exchange 訊息資料庫 (MDB)。例如， [CN=Mailbox Store (CONTROLLER),CN=First Storage Group,CN=InformationStore,CN=CONTROLLER,CN=Servers,CN=First Administrative Group,CN=Administrative Groups,CN=Domain,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=Domain,DC=com] 完成輸入後，驅動程式即會進行更新，以管理其他 MDB。
當帳戶授權撤銷時	僅限「Exchange 規則」選項。 允許您在「授權」移除「使用者」帳戶時，選擇要執行的動作。 *關閉帳戶* *刪除帳戶*
名稱映射規則選取	驅動程式會將 Identity Vault Full Name 屬性映射至 Active Directory 物件名稱，並將 Windows 2000 以前的 Active Directory 登入名稱映射至 Identity Vault 使用者名稱。 您可以接受全部規則，也可以手動選取部份規則。如果規則不符合您的需求，則可以在輸入後修改規則，只要在完成輸入之後，對「訂閱者和發行者指令轉換」規則中的 NameMap 規則進行編輯即可。 「*接受*」使用全部規則。 「*手動*」可以使用部份規則。
全名映射	僅限「名稱映射規則選取」>「手動」選項。 「*是*」允許驅動程式將 Identity Vault Full Name 屬性與 Active Directory 物件名稱和顯示名稱保持同步。 「*否*」不會將 Identity Vault Full Name 屬性與 Active Directory 物件名稱和顯示名稱保持同步。 在 Active Directory 中使用「Microsoft Management Console 使用者與電腦」嵌入程式建立使用者帳戶時，可以使用此規則。
登入名稱映射	僅限「名稱映射規則選取」>「手動」選項。 「*是*」允許驅動程式將 Identity Vault 物件名稱與 Windows 2000 以前的 Active Directory 登入名稱 (也稱爲「NT 登入名稱」或 sAMAccountName) 保持同步。 「*否*」不會將 Identity Vault 物件名稱與 Windows 2000 以前的 Active Directory 登入名稱保持同步。
輸入將繼續沿用 Windows 2000 登入名稱規則選取	僅限「名稱映射規則選取」>「手動」選項。 *確定*

欄位	描述
使用者主體名稱映射	允許您選擇一種方法，以便管理 Active Directory Windows 2000 登入名稱 (也稱爲 userPrincipalName)。userPrincipalName 會採用電子郵件地址的格式，如 usere@domain.com。雖然 Shim 可以將任意值放入 userPrincipalName，但它不能充當登入名稱，除非將領域設定爲允許領域名稱使用該名稱。 「*遵循 Active Directory 電子郵件地址*」會將 userPrincipalName 設定爲 Active Directory 郵件屬性的值。如果您要將使用者的電子郵件地址用於驗證，並且 Active Directory 可以爲電子郵件地址授權，則可以使用此選項。 「*遵循 Identity Vault 電子郵件地址*」會將 userPrincipalName 設定爲 Identity Vault 電子郵件地址屬性的值。如果您要將使用者的電子郵件地址用於驗證，並且 Identity Vault 可以爲電子郵件地址授權，則可以使用此選項。 如果您要從使用者登入名稱 (加上在規則中定義的硬式編碼字串) 產生 userPrincipalName，則可以使用「*遵循 Identity Vault 名稱*」。 如果您不想控制 userPrincipalName 或不想實作自己的規則，則可以使用「*無*」。

升級 Active Directory 驅動程式 5

5.1 升級所用的核對清單

若要升級 Active Directory 驅動程式，請使用下列核對清單。如果您不熟悉 Identity Manager，則可能要聘請一位合格的顧問。

- ❑ 若要使用「密碼同步化 2.0」，則新增驅動程式資訊清單和密碼規則。

  請參閱「升級現有的驅動程式組態以支援 Identity Manager 密碼同步化 (http://www.novell.com/documentation/dirxml20/index.html?page=/documentation/dirxml20/admin/data/bo16oyy.html)」。

- ❑ 若要繼續使用「密碼同步化 1.0」，請新增舊規則至現有的驅動程式組態。

  請參閱「將密碼同步化 1.0 升級至 Identity Manager 提供的密碼同步化 (http://www.novell.com/documentation/dirxmldrivers/index.html?page=/documentation/dirxmldrivers/ad/data/bnwjt02.html)」。

- ❑ 在現有驅動程式的樣式表中，移除 sAMAccountName 的結構化格式。

  在 DirXML® 1.1a Active Directory 2.0 驅動程式中，sAMAccountName 爲結構化的屬性。在新的 Active Directory 3.0 驅動程式中，它則是字串。

  舊格式：

  ```
  <value type="structured"> <component name="nameSpace">0</
  component> <component association-
  ref="XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX" name="volume"/> <component
  name="path">jsmith</component> </value>
  ```

  新格式：

  ```
  <add-attr attr-name="sAMAccountName"> <value
  type="string">jsmith</value> </add-attr>
  ```

- ❑ 升級驅動程式的組態參數。

  建議您使用下列預設設定：

  ```
  <?xml version="1.0"?> <driver-config name="Active Directory
  Driver"> <driver-options> <pollingInterval display-name="Polling
  Interval (min.)"> 1</pollingInterval> <auth-method display-
  name="Authentication Method"> Negotiate</auth-method> <signing
  display-name="Use Signing (yes/no)" id="> no</signing> <sealing
  display-name="Use Sealing (yes/no)"> no</sealing> <use-ssl display-
  name="Use SSL (yes/no)"> no</use-ssl> <pub-heartbeat-interval
  display-name="Heart Beat"> 0</pub-heartbeat-interval> <pub-
  password-expire-time display-name="Password Sync Timeout
  ```

```
(minutes):">60</pub-password-expire-time> <use-CDOEXM display-
name="Use CDOEXM for Exchange (yes/no)"> no</use-CDOEXM> <cdoexm-
move display-name="Allow CDOEXM Exchange mailbox move (yes/
no)">yes</cdoexm-move> <cdoexm-delete display-name="Allow CDOEXM
Exchange mailbox delete (yes/no)">yes</cdoexm-delete> </driver-
options> </driver-config>
```

- 將驗證 ID 轉換成 Sam 帳戶名稱 (例如，jsmith) 或領域名稱 / 帳戶名格式 (例如 *domain*/jsmith)。
- 將 Login Disabled 屬性的映射從 userAccountControl 變更爲 dirxml-uACAccountDisable。
- 如果您是提供 Exchange 帳戶，則將 CDOEXM 的驅動程式參數變更爲「是」，然後從現有驅動程式組態的樣式表中移除下列四項硬式編碼屬性：
  - msExchHomeServerName
  - legacyExchangeDN
  - homeMTA
  - msExchMailboxSecurityDescriptor
- 如果您從 Identity Manager 2.x 進行升級，並且啓用了 Exchange 提供，則驅動程式會套用重疊。Identity Manager 3.0 會控制 Exchange 信箱的移動和刪除。因爲這功能要在升級的驅動程式上運作，所以必須套用重疊。如需如何套用重疊的相關資訊，請參閱「對 Exchange 信箱套用重疊」，第 47 頁。

5.2 處理 Login Disabled 值

在沒有 Login Disabled = true 的情況下，eDirectory™ 會將其當成 Login Disabled = false 來處理。因此，如果您是透過第一次安裝而不是升級取得 Active Directory 驅動程式第 3 版，並且 Login Disabled = false 值不存在，則「建立規則」中的預設規則會建立此值。

依預設，驅動程式從第 2 版升級成第 3 版時，不會套用此規則。

5.3 從 DirXML 1.1a 升級驅動程式 Shim

此項升級操作會以新的驅動程式 Shim 取代先前的驅動程式 Shim，但會保留先前驅動程式的組態。新的驅動程式 Shim 可以執行 DirXML 1.1a 組態，而不會對其進行變更 (除非您正在使用「密碼同步化 1.0」)。

如果您繼續使用「密碼同步化 1.0」，則不需要升級驅動程式 Shim。DirXML 1.1a 驅動程式 Shim 會在 Identity Manager 3.0 引擎上執行，但 Identity Manager 3.0 驅動程式 Shim 卻不能在 DirXML 1.1a 引擎上執行。

如果您選擇不升級驅動程式 Shim，則在安裝 Identity Manager 3.0 引擎時，請務必取消選取 Active Directory 驅動程式。如果選取此選項，就會升級驅動程式 Shim。

若要升級驅動程式 Shim：

1. 請確定已使用目前所執行之版本的所有修補程式更新驅動程式。

   建議在所有驅動程式上執行此步驟，這有助於將升級問題減至最少。
2. 安裝 Identity Manager 3.0 驅動程式 Shim。您可以在安裝 Identity Manager 3.0 引擎的同時執行此步驟。

請遵循《*Identity Manager 3.0* 安裝指南》之「安裝 Identity Manager」一節中的指示。

警告：如果您已在使用「密碼同步化 1.0」，請先閱讀「將密碼同步化 1.0 升級至 Identity Manager 提供的密碼同步化」，第 61 頁，並準備新增規則至驅動程式組態，爲「密碼同步化 1.0」提供反向相容性後，再安裝升級後的 Identity Manager Driver for Active Directory。

不支援將 Identity Manager 2.0 或 3.0 驅動程式 Shim 或組態與 DirXML 1.1a 引擎一起執行。

3 安裝 Shim 後，需要重新啓動 Novell eDirectory 和驅動程式。

3a 在 iManager 中，按一下「*Identity Manager* > *Identity Manager* 概觀」。

3b 瀏覽至驅動程式所在的「驅動程式集」，然後按一下「搜尋」。

3c 按一下驅動程式圖示的右上角，然後按一下「重新啓動驅動程式」。

4 使用 Identity Manager 啓用身分證明來啓用驅動程式 Shim。

請參閱「啓用驅動程式」，第 57 頁。

安裝驅動程式 Shim 之後，請繼續參閱第 4 章 「設定 Active Directory 驅動程式」, 第 35 頁。

5.4 從 IDM 2.*x* 升級驅動程式 Shim

1 請確定已使用目前所執行之版本的所有修補程式更新驅動程式。

建議在所有驅動程式上執行此步驟，這有助於將升級問題減至最少。

2 安裝 Identity Manager 3.0 驅動程式 Shim。您可以在安裝 Identity Manager 3.0 引擎的同時執行此步驟。

請遵循《*Identity Manager 3.0* 安裝指南》之「安裝 Identity Manager」一節中的指示。

警告：如果您已在使用「密碼同步化 1.0」，請先閱讀「將密碼同步化 1.0 升級至 Identity Manager 提供的密碼同步化」，第 61 頁，並準備新增規則至驅動程式組態，爲「密碼同步化 1.0」提供反向相容性後，再安裝升級後的 Identity Manager Driver for Active Directory。

不支援將 Identity Manager 驅動程式 Shim 或組態與 DirXML 1.1a 引擎一起執行。

3 安裝 Shim 後，需要重新啓動 Novell eDirectory 和驅動程式。請遵循《*Novell Identity Manager 3.0* 管理指南》之「啓動、停止或重新啓動驅動程式」中的指示。

4 使用 Identity Manager 啓用身分證明來啓用驅動程式 Shim。

請參閱「啓用驅動程式」，第 57 頁。

安裝驅動程式 Shim 之後，請繼續參閱第 4 章 「設定 Active Directory 驅動程式」, 第 35 頁。

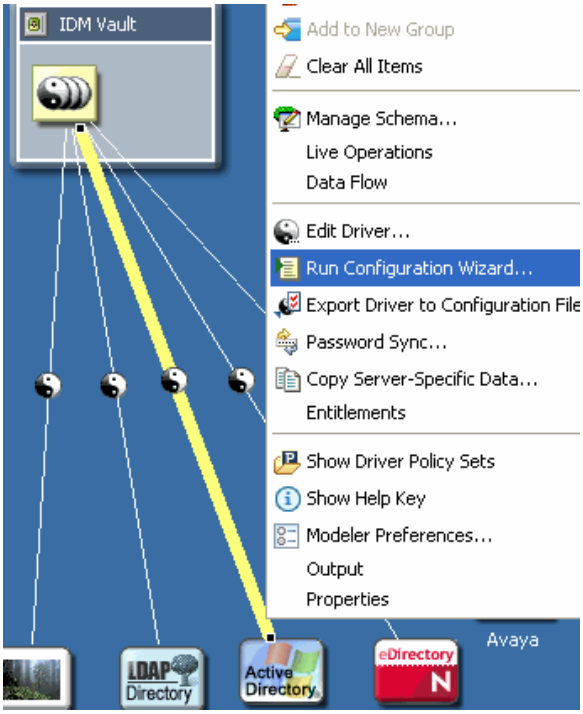
5.5 對 Exchange 信箱套用重疊

如果您已從 Identity Manager 2.x 升級到 Identity Manager 3.0，並且在驅動程式上啓用了 Exchange 提供，則需要套用 AD 驅動程式重疊。重疊可以讓驅動程式對 Exchange 信箱的刪除和移動操作進行控制。

- 「在 Designer 中套用重疊」，第 48 頁
- 「在 iManager 中套用重疊」，第 51 頁

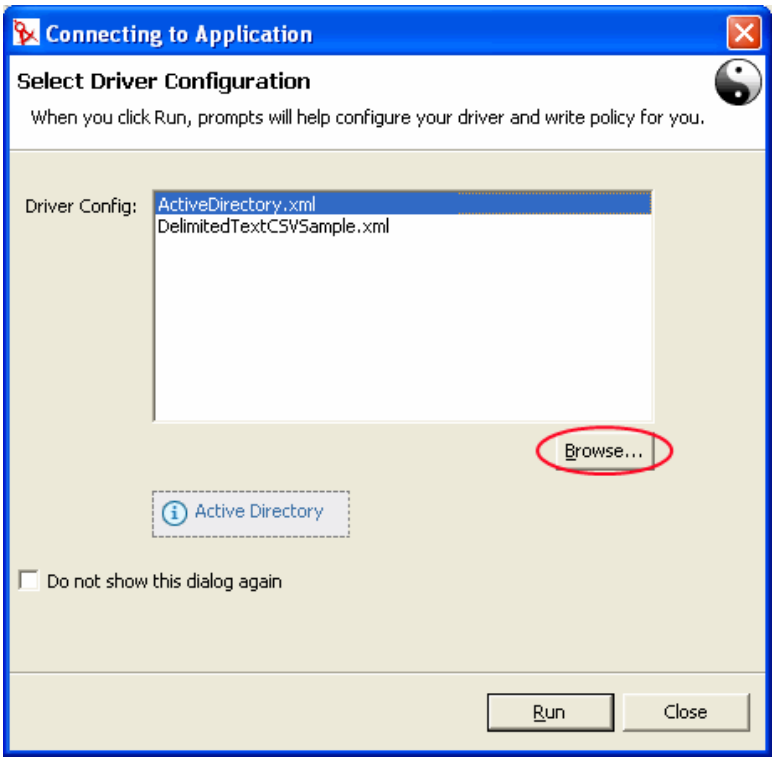
5.5.1 在 Designer 中套用重疊

1 在模擬器中，在 AD 驅動程式連接器圖示上按一下滑鼠右鍵，然後按一下「執行組態精靈」。



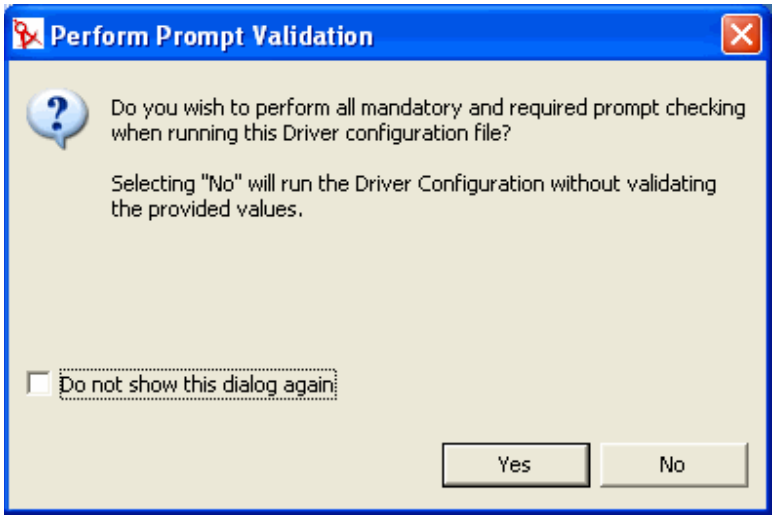
2 選取「瀏覽」，並瀏覽至檔案 ActiveDirectoryUpdate.xml，然後按一下「開啓」。

此檔案位於外掛程式
eclipse\plugins\com.novell.designer.idm_*x.x.x*\defs\ActiveDirectoryUpdate.xml 中。



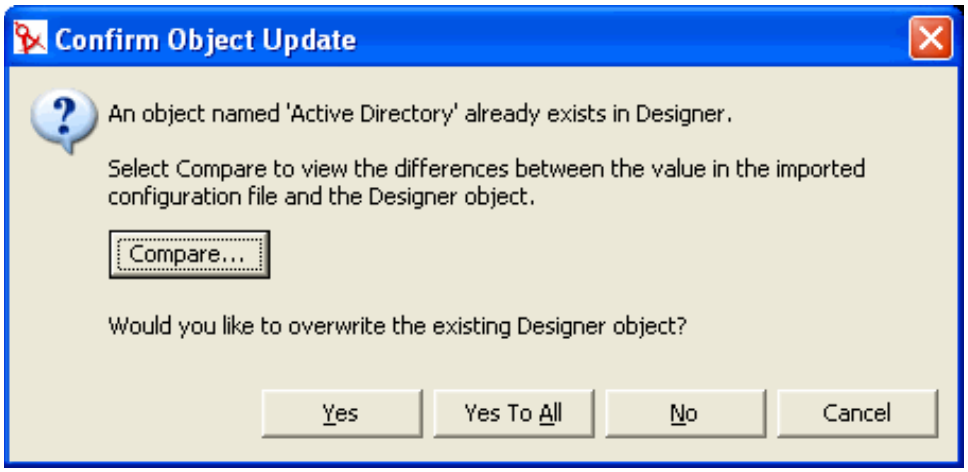
3 選取「*ActiveDirectoryUpdate.xml*」，然後按一下「執行」。

4 根據您是否希望 Designer 對提示符中輸入的資訊進行驗證，來選取「是」或「否」。



5 輸入環境特定的資訊，然後按一下「確定」。如需此欄位的描述，請參閱表格 5-1 頁上 50。

6 在「確認物件更新」視窗中，選取「比較」以檢視輸入之組態檔案與 Designer 物件中的值有何不同，然後按一下「關閉」。



7 如果變更正確，則選取「是」以覆寫現有的 Designer 物件。如果您不想更新驅動程式，則選取「否」。

表格 ***5-1*** 在 *Designer* 中重疊組態參數

參數	描述
驅動程式名稱	這是需要更新爲新參數的驅動程式。輸入驅動程式名稱，或者瀏覽至驅動程式，然後選取該驅動程式。
更新驅動程式	它會更新驅動程式的參數。如果要更新驅動程式，請選取「*是*」。. 如果不要更新驅動程式，則選取「*否*」。
homeMDB 控制 Exchange 的移動	允許變更使用者 HomeMDB 屬性，以便在使用 CDOEXM 時移動使用者的 Exchange 信箱。使用者的信箱要移往的 Exchange 訊息資料庫，必須與先前的 Exchange 訊息資料庫處於同一個領域中。 如果選取了「*是*」，則當「使用者」物件移到 eDirectory 中時，該移動會同時反映在 Active Directory 和 Exchange 中。 如果選取了「*否*」，則當 eDirectory 中的「使用者」物件移動時，該移動會反映在 Active Directory 中，而不會反映在 Exchange 中。
homeMDB 控制 Exchange 的刪除	允許移除使用者 homeMDB 屬性，以便在使用 CDOEXM 時刪除使用者的 Exchange 信箱。 如果選取了「*是*」，則當刪除「eDirectory 使用者」物件時，相關的「Active Directory 使用者」物件和 Exchange 帳戶都會一併刪除。 如果選取了「*否*」，則當刪除「eDirectory 使用者」物件時，相關的「Active Directory 使用者」物件也會一併刪除，而 Exchange 帳戶則保留不動。

參數	描述
登入和身分	允許 CDOEXM 和「密碼設定」支援的驅動程式驗證帳戶以不同的方式登入。 如果選取了「*否*」，則驅動程式只執行網路登入。 如果選取了「*是*」，則驅動程式會執行本地登入。驗證帳戶必須是具有管理特權的 Active Directory 帳戶。

5.5.2 在 iManager 中套用重疊

使用 iManager 更新驅動程式的方法有兩種。一種是在「Identity Manager 概觀」中進行更新，另一種是使用「Identity Manager 公用程式」進行更新。

Identity Manager 概觀

1. 在 iManager 中，選取「*Identity Manager* > *Identity Manager* 概觀」。
2. 選取「搜尋」，以尋找儲存 Active Director 驅動程式的「驅動程式集」物件。
3. 在「Identity Manager 概觀」螢幕中選取「新增驅動程式」。
4. 瀏覽至儲存 Active Director 驅動程式的「驅動程式集」物件，並將其選取，然後按「下一步」。
5. 選取「從伺服器 *(.XML* 檔案 *)* 輸入驅動程式組態」。
6. 從下拉式功能表中選取「*ActiveDirectoryUpdate.xml*」，然後按「下一步」。
7. 輸入環境特定的資訊，然後按「下一步」。如需這些欄位的描述，請參閱表格 5-2 頁上 51。
8. 選取「更新驅動程式 *(* 包括驅動程式的影像 *)*」以更新此驅動程式，或是選取「選取不同的驅動程式」，然後按「下一步」。
9. 檢視變更的摘要，然後按一下「完成」。

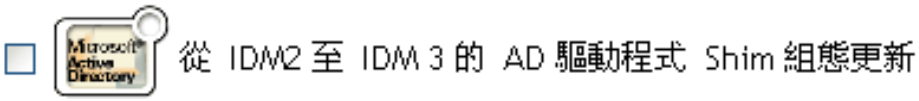
表格 ***5-2*** 在 *iManager* 中重疊組態參數

參數	描述
驅動程式名稱	這是需要更新爲新參數的驅動程式。
現有的驅動程式	從下拉式功能表中，選取啓用 Exchange 提供之更新的 AD 驅動程式名稱。一旦選取了驅動程式名稱，「驅動程式」名稱欄位就會自動填入。
更新驅動程式	它會更新驅動程式的參數。如果要更新驅動程式，請選取「*是*」。. 如果不要更新驅動程式，則選取「*否*」。
homeMDB 控制 Exchange 的移動	允許變更使用者 HomeMDB 屬性，以便在使用 CDOEXM 時移動使用者的 Exchange 信箱。使用者之信箱要移往的 Exchange 訊息資料庫，必須與先前的 Exchange 訊息資料庫處於同一個領域中。 如果選取了「*是*」，則當 eDirectory 中的「使用者」物件移動時，該移動會同時反映在 Active Directory 和 Exchange 中。 如果選取了「*否*」，則當「使用者」物件移動到 eDirectory 中時，該移動會反映在 Active Directory 中，而不會反映在 Exchange 中。

參數	描述
homeMDB 控制 Exchange 的刪除	允許移除使用者 homeMDB 屬性，以便在使用 CDOEXM 時刪除使用者的 Exchange 信箱。 如果選取了「*是*」，則當刪除「eDirectory 使用者」物件時，相關的「Active Directory 使用者」物件和 Exchange 帳戶都會一併刪除。 如果選取了「*否*」，則當刪除「eDirectory 使用者」物件時，相關的「Active Directory 使用者」物件也會一併刪除，而 Exchange 帳戶則保留不動。
登入和身分	允許 CDOEXM 和「密碼設定」支援的驅動程式驗證帳戶以不同的方式登入。 如果選取「*否*」，則驅動程式只執行網路登入。 如果選取「*是*」，則驅動程式會執行本地登入。驗證帳戶必須是具有管理特權的 Active Directory 帳戶。

Identity Manager 公用程式

1. 在 iManager 中，選取「*Identity Manager* 公用程式 > 輸入驅動程式」。
2. 瀏覽至儲存 Active Director 驅動程式的「驅動程式集」物件，並選取該物件，然後按「下一步」。
3. 在「其他規則」下，選取「*AD* 驅動程式 *Shim* 組態從 *IDM2* 更新至 *IDM 3*」，然後按「下一步」。



4. 輸入環境特定的資訊，然後按「下一步」。如需這些欄位的描述，請參閱表格 5-2 頁上 51。
5. 選取「更新驅動程式 *(* 包括驅動程式的影像 *)*」以更新此驅動程式，或是選取「選取不同的驅動程式」，然後按「下一步」。
6. 檢視變更的摘要，然後按一下「完成」。

管理 Active Directory 驅動程式 6

6.1 安全性參數

在安裝期間，驅動程式會蒐集必要的資訊，並建立預設安全性規則和參數。在開始自定 Active Directory 驅動程式之前，應先熟悉下列內容：

- 預設規則和參數
- 本主題在第 8 章 「疑難排解」, 第 79 頁中有描述，您可以據此判斷這些問題是否適用於您的環境。

了解參數之間的合作方式及參數在作業系統中的運作方式，有助於您爲 Identity Manager 資料同步化定義安全性方法。

- 驗證 **ID**：驅動程式用於存取領域資料的帳戶。

表格 ***6-1*** 驗證 *ID*

格式	使用者名稱	方法
領域名稱	使用者	交涉
完全合法的領域名稱	領域 \ 使用者	交涉
可辨識名稱	cn=DirXML,cn=Users,DC=domain,dc=com	簡易

- 驗證網路位置：用於存取領域資料的網路位置。

表格 ***6-2*** 驗證網路位置

格式	範例	方法
Active Domain 控制器的 DNS 名稱	mycontroller.mydomain.com	交涉
Active Domain 控制器的 DNS 名稱，或 LDAP 伺服器的 IP 位址	mycontroller.mydomain.com 137.65.134.83	簡易

- 應用程式密碼： 驗證 ID 帳戶的密碼。
- 使用簽章：此參數是用於 Active Directory 驅動程式和 Active Directory 之間，而不是用於 Metadirectory 引擎與「遠端載入器」之間。簽章可確保不讓惡意電腦攔截資料。如果您沒有使用 LDAP SSL 連接埠，此旗標會啓用 Active Directory 連接的簽章。

此設定需要 Windows 2003 或附有最新支援套件的 Windows 2000，而且兩種伺服器都必須有 Internet Explorer 5.5 SP2 或更新版本。這會啓用 Kerberos 或 NTLM v2 驗證連線上的簽章。

與 SSL 一樣，在啓始輸入中無法使用此參數。您要在安裝完成後，透過「驅動程式參數」頁面對其進行設定。

- 使用密封：此參數是用於 Active Directory 驅動程式和 Active Directory 之間，而不是用於 Metadirectory 引擎與「遠端載入器」之間。密封會加密資料，使網路監視器無法對其進行檢視。如果您沒有使用 LDAP SSL 連接埠，此旗標會啓用 Active Directory 連接的密封。

  此設定需要 Windows 2003 或附有最新支援套件的 Windows 2000，而且兩種伺服器都必須有 Internet Explorer 5.5 SP2 或更新版本。此設定會啓用 Kerberos 或 NTLM v2 驗證連線上的加密。

  與 SSL 一樣，在啓始輸入中無法使用此參數。您要在安裝完成後，透過「驅動程式參數」頁面對其進行設定。

- 使用 **SSL**：此參數是用於 Active Directory 驅動程式和 Active Directory 之間。如果您使用 LDAP SSL 連接埠連接至 Active Directory，此參數就會控制加密。此參數對「交涉」和「簡易」驗證方法均適用。

  依預設此參數是設定爲「否」。如果您將該值設定爲「是」，整個交流的 SSL 管線就會加密。一般偏好使用加密管線，因爲驅動程式通常會對機密資訊進行同步化。不過，加密會降低伺服器的一般效能。

  在輸入驅動程式後，此參數可以透過「驅動程式參數」頁面進行設定。

6.1.1 建議的安全性組態

使用 **Identity Manager** 遠端載入器

表格 ***6-3*** 建議的設定

參數	描述
驗證 ID	領域登入名稱，例如 Administrator。
驗證網路位置	領域控制器的 DNS 名稱。 如果不想在 Active Directory 領域控制器上執行驅動程式，則在「交涉」方法中使用 ***hostname***，但在「簡易」方法中使用 ***hostname*** 或 IP 位址。
應用程式密碼	用於驗證帳戶的密碼。
遠端載入器密碼	用於「遠端載入器」服務的密碼。
驗證方法	交涉。
使用簽章	否。需要 Windows 2003 或附有最新支援套件的 Windows 2000，而且兩種伺服器都必須有 Internet Explorer 5.5 SP2 或更新版本。
使用密封	否。需要 Windows 2003 或帶有最新支援套件的 Windows 2000，而且兩種伺服器都必須有 Internet Explorer 5.5 SP2 或更新版本。
使用 SSL	是。當驅動程式 Shim 沒有在領域控制器上執行時，需要有 SSL 才能執行「訂閱者」密碼的檢查、設定和修改操作。

使用 **SSL**

如果選取了 「簡易」驗證機制，則建議使用 SSL，因爲 「簡易」驗證會以純文字傳遞密碼。

表格 ***6-4*** *SSL* 參數

參數	描述
驗證 ID	LDAP 格式驗證 ID
驗證網路位置	領域控制器的 IP 位址
密碼	指定之驗證 ID 的密碼
使用簽章	否
使用密封	否
使用 SSL	是

6.2 管理群組

Active Directory 群組類別會定義兩種群組類型，並定義三種群組成員資格的範圍。類型和範圍是由 groupType 屬性 (可以在 Active Director 中建立群組後，透過 Identity Manager 規則設定該屬性) 控制，並可透過修改該屬性加以變更。

群組包含物件參考的集合。「配送群組」類型不會向其成員授予特殊的權限或特權，因此通常用做 Exchange 的配送清單。「安全性群組」類型是安全性主體，其成員具有該群組的權限和特權。「安全性群組」具備 Windows 2000 以前的登入名稱 (samAccountName) 和安全性識別碼 (SID)，該識別碼可用於其他物件上的安全性描述詞 (SD) 存取控制清單 (ACL)，以便向其成員授予或拒絕權限及特權。

「群組」範圍會控制來自域外領域的物件能否成爲群組的成員，以及群組本身能否成爲另一個群組的成員。三個範圍分別是 「領域本地」、「全域」和 「通用」。這些範圍的運作方法及範圍是否完全有效，均取決於 Active Directory 是在 「Windows 2000 混合」、「Windows 2000 原始」還是 Windows 2003 模式中。

一般而言，「領域本地」群組可以保留對樹系中任意位置之物件的參考，但是只能獲得該領域內的許可。「全域」群組則恰好相反。它們只能保留對領域內部物件的參考，但可以獲得整個樹系內的許可。「通用」群組可以保留參考，並可以獲得整個樹系的許可。但是，「通用」群組還帶有其自身的限制和效能問題。應當遵照 Microsoft 的建議來建立和使用群組。

groupType 屬性是一個 32 位元的整數，其位元會定義類型和範圍。在任一指定的時間，群組的範圍必須是單一的。

表格 ***6-5*** *GroupType* 屬性

GroupType 屬性	範圍	定義類型和範圍的位元
GROUP_TYPE_GLOBAL_GROUP	配送	0x00000002
GROUP_TYPE_DOMAIN_LOCAL_GROUP	配送	0x00000004

GroupType 屬性	範圍	定義類型和範圍的位元
GROUP_TYPE_UNIVERSAL_GROUP	配送	0x00000008
GROUP_TYPE_SECURITY_ENABLED	安全性	0x80000000

6.3 管理 Microsoft Exchange 信箱

Active Directory 驅動程式可以被設定爲在 Active Directory 中建立、移動和刪除使用者的 Microsoft Exchange 信箱。信箱可以透過設定和移除使用者物件上 homeMDB 屬性的值來進行管理。此屬性包含信箱所在之「Exchange 私人訊息資料庫」(MDB) 的「可辨識名稱」。該驅動程式只會管理與其在同一個領域之 Exchange 伺服器上的信箱。

管理 Exchange 信箱的方法有多種。預設組態會藉由在「訂閱者指令轉換」規則中做出的規則決策來管理信箱。使用者符合指定條件時，就會建立、移動或移除信箱。輸入檔案會向您提供三種信箱管理的選項：

- 授權
- 規則
- 不管理 Exchange 信箱

在使用提供的授權方法時，會依據 Identity Vault 中使用者的授權設定來授予或拒絕使用者信箱。授權包含 MDB 的「可辨識名稱」和狀態值，該值會告知驅動程式是授予還是撤銷授權。授權本身則由「使用者應用程式」或「角色授權」驅動程式進行管理。在任何一種情況下，外部工具都會授予 (或撤銷) 對信箱的權限，「訂閱者指令轉換」規則會將該權限轉譯成 homeMDB 屬性上的新增值或移除值，驅動程式 Shim 則將 homeMDB 的變更轉譯成對 Exchange 管理系統的適當呼叫。

如果您正在使用授權，並且在組織中有多個 MDB，則可以使用「使用者應用程式」來決定要將哪個 MDB 指定給特定使用者。《Identity Manager 附屬入口網站應用程式參考指南 (http://www.novell.com/documentation/idm)》包含了有關如何設定多個 MDB 的文件。Identity Manager 驅動程式的作用是要回應位於使用者物件上的授權，而不是爲使用者物件授權。如果您正在使用「使用者應用程式」，則會向您提供一份 Exchange MDB 清單，以便您從中選擇一項做爲貫穿整個核准程序的工作流程項目。如果您正在使用「角色授權」，則會將 MDB 指定給擁有使用者角色的群組。

在使用提供之以規則爲基礎的方法時，「訂閱者指令轉換」規則會使用 Identity Vault 之使用者物件狀態的相關資訊來指定 MDB。驅動程式 Shim 會將此變更轉譯成對 Exchange 管理系統的適當呼叫。預設規則會使用簡易的規則來指定信箱。假設只有一個 MDB，並且所有藉由規則鏈完成操作的使用者都應被指定到該 MDB。因爲用於指定不同 MDB 的規則在不同的公司之間變化也很大，所以預設組態不會嘗試建立「正確」的方式。若要實作自己的規則，只要變更預設的指定規則即可。您可以使用「DirXML 程序檔」的 if 陳述式來定義信箱指定的條件，以及 homeMDB 屬性的 do-set-dest-attribute 指令，使變更生效。您可以使用 ADManager.exe 工具或是用自己的方法來取得 Exchange MDB 清單。

不在管理 Exchange 信箱的時候，驅動程式會對使用者的電子郵件地址和郵件綽號進行同步化。

管理 Exchange 信箱的方法還有其他幾種。例如，您可以延伸 Identity Vault 的網要以包含 homeMDB 資訊，並使用基本的資料同步化來爲 Active Directory 中的使用者指定信箱。在此情況下，您要使用自己的工具在 Identity Vault 中進行指定。

預設規則非常適用於單一 MDB 的簡易信箱指定。若要讓規則能夠反映環境中所需更加複雜的規則 (Rule)，則必須變更規則 (Policy)。

6.4 啓用驅動程式

在安裝後 90 天內啓用驅動程式。90 天的試用期結束後，若沒有正確的啓用身分證明，驅動程式就無法啓動。在未啓用驅動程式期間發生的事件，會在啓用並啓動驅動程式後進行處理。

如需啓用的相關資訊，請參閱《*Identity Manager 3.0* 安裝指南》中的「啓用 Novell Identity Manager 產品」。

密碼同步化

7

本節假設您熟悉《*Novell Identity Manager 3.0* 管理指南》之「已連接系統間的密碼同步化」中的資訊。本節包含該驅動程式特定的資訊。

重要：如果您先前已使用「密碼同步化 1.0」，請先閱讀「將密碼同步化 1.0 升級至 Identity Manager 提供的密碼同步化」，第 61 頁並了解其含義後，再安裝新的驅動程式 Shim。如果您安裝驅動程式 Shim，則即使您不打算立即使用 Identity Manager 提供的「密碼同步化」，還是要在驅動程式規則中新增「密碼同步化 1.0」的反向相容性。

本節內容：

如需疑難排解密碼同步化的相關資訊，請參閱「密碼同步化秘訣」，第 81 頁。

7.1 比較密碼同步化 1.0 與 Identity Manager 提供的密碼同步化

表格 ***7-1*** 密碼同步化之不同版本間的差異

功能	在密碼同步化 1.0 中	在 Identity Manager 提供的密碼同步化中
產品交付方式	與 Identity Manager 分開的單獨產品。	包含在 Identity Manager 中的功能，不做爲單獨產品出售。

功能	在密碼同步化 1.0 中	在 Identity Manager 提供的密碼同步化中
平台	◆ Active Directory ◆ NT 領域	在下列平台上支援完全雙向密碼同步化： ◆ Active Directory ◆ eDirectory™ ◆ NIS ◆ NT 領域 這些已連接系統支援發行 Identity Manager 的使用者密碼。因爲「通用密碼」與「配送密碼」是可回復的，所以 Identity Manager 可以將密碼配送至已連接系統。 所有支援「訂閱者」密碼元素的已連接系統都可以從 Identity Manager 訂閱密碼。 請參閱《*Novell Identity Manager 3.0 管理指南*》中的「已連接系統間的密碼同步化」。
eDirectory 中使用的密碼	eDirectory 密碼 (不可回復)	通用密碼 (可回復) 或配送密碼 (也可回復)。如有必要，eDirectory 密碼還可以保持同步化。如需範例案例，請參閱《*Novell Identity Manager 3.0 管理指南*》中的「實作密碼同步化」。
Windows 已連接系統的主要功能	提供雙向密碼同步化，以使 eDirectory 密碼與 Windows 密碼同步化。不過，每個工作站都需要安裝 Novell® Client™。	提供雙向密碼同步化。因爲「通用密碼」和「配送密碼」是可回復的，所以密碼可以從兩個方向進行同步化，且分別在 Identity Manager 的「發行者」和「訂閱者」通道中完成。
LDAP 密碼變更	不支援。	支援。
Novell Client	必要。	非必要。
nadLoginName 屬性	用於不斷更新密碼。	未使用。
包含密碼同步化功能的元件	包含更新 nadLoginName 功能的 Identity Manager 驅動程式。	驅動程式組態中的規則提供密碼同步化功能。驅動程式只執行由 Metadirectory 引擎提供的任務，而這些任務來自規則中的邏輯。 驅動程式資訊清單、全域組態值和驅動程式過濾器設定也必須支援密碼同步化。它們包含在範例驅動程式組態中，也可新增至現有的驅動程式。請參閱「升級現有的驅動程式組態以支援 Identity Manager 密碼同步化」，第 66 頁。
代辦	軟體的單獨部份。	未安裝任何代辦；現在該功能是驅動程式的一部份。

7.2 將密碼同步化 1.0 升級至 Identity Manager 提供的密碼同步化

如果您目前正在使用「密碼同步化 1.0」，請先完成本節中的指示再進行升級。

重要：請先檢視這些指示，再安裝 Identity Manager 驅動程式 Shim。

若要從「密碼同步化 1.0」升級至 Identity Manager 提供的「密碼同步化」：

1. 確定您的環境已做好使用「通用密碼」的準備。

   請參閱《*Novell Identity Manager 3.0* 管理指南》中的「準備使用 Identity Manager 密碼同步化和通用密碼」。

   啓用「通用密碼」不會自動變更兩個系統中的密碼。只有在使用者變更其密碼後，「通用密碼」同步化才會開始運作。

   案例：通用密碼。在 DigitalAirlines 處，網路管理員 Sandy 啓用了「通用密碼」。使用者 Markus 登入並變更他的密碼。於是兩個系統都設定了 Markus 的「通用密碼」。然而，使用者 Marie 登入後，並沒有變更她的密碼。她繼續使用未變更的密碼進行登入。在她變更密碼之前，系統不會爲她設定「通用密碼」功能。

2. 安裝 Identity Manager 3 驅動程式 Shim，以取代 DirXML® 1.1a 驅動程式 Shim，並立即完成步驟 3。

   附註：如果您正在執行 Identity Manager 2.0，並且使用「通用密碼」，則不必升級「密碼同步化」。

   根據《*Identity Manager 3.0* 安裝指南》之「安裝 Identity Manager」這一章中的描述使用安裝程式，並且只選取「Identity Manager Driver for Active Directory」。

3. 根據「透過新增規則建立與密碼同步化 1.0 的反向相容性」，第 63 頁中的描述新增新的規則至驅動程式組態，以建立「密碼同步化 1.0」的反向相容性。

   DirXML 1.1a 驅動程式 Shim 會更新 nadLoginName 屬性，而 Identity Manager 驅動程式 Shim 則不會。因此，您必須新增規則至驅動程式組態，以更新 nadLoginName。這能讓「密碼同步化 1.0」在您安裝驅動程式 Shim 時正常運作，以便在完成「Identity Manager 密碼同步化」的部署後，不會遺失任何密碼變更。

   重要：如果不建立反向相容性，「密碼同步化 1.0」會繼續更新現有的使用者，但只有在您部署了「Identity Manager 密碼同步化」後，才會對新增或重新命名的使用者進行同步化。

   完成此步驟後，您就有了 Identity Manager 3.0 驅動程式 Shim 和反向相容性的規則。. 因此，驅動程式支援「密碼同步化 1.0」。

   如果您無法立即完成此程序的剩餘部份，在準備完成「Identity Manager 密碼同步化」的部署前，仍然可以繼續使用「密碼同步化 1.0」。

4. 向每個您想讓其參與密碼同步化的驅動程式，新增對「Identity Manager 密碼同步化」的支援。

   升級現有的組態，或取代現有的組態。

升級現有的組態 將現有的 DirXML 1.1a 驅動程式組態轉換成 Identity Manager 格式，並新增 「Identity Manager 密碼同步化」所需的規則，即可升級該組態。

- 使用精靈將驅動程式轉換爲 Identity Manager 格式。請參閱 《*Novell Identity Manager 3.0* 管理指南》中的 「升級現有的驅動程式組態以支援密碼同步化」。
- 新增規則以支援 「Identity Manager 密碼同步化」。您可以使用 「重疊」組態檔案，一次同時新增規則、驅動程式資訊清單和 GCV。您還必須新增屬性至 「過濾器」。如需指示，請參閱 《*Novell Identity Manager 3.0* 管理指南》中的 「升級現有的驅動程式組態以支援密碼同步化」。

以 **Identity Manager** 組態取代現有的組態，並再次新增反向相容性： Identity Manager 範例驅動程式組態包含規則、驅動程式資訊清單、GCV 及過濾器設定，以支援 「Identity Manager 密碼同步化」。如需輸入新驅動程式組態的相關資訊，請參閱此驅動程式指南之第 4 章 「設定 Active Directory 驅動程式」 , 第 35 頁中的指示。

- 如果您選擇取代現有的組態，請確定遵照 「透過新增規則建立與密碼同步化 1.0 的反向相容性」，第 63 頁中的描述，再次新增反向相容性。Identity Manager 範例驅動程式組態不包含那些規則。
- 確定 nadLoginName 屬性是設定爲 「發行者」，因爲它是在先前的驅動程式組態中。

5 如果您要讓已連接系統提供 Identity Manager 的使用者密碼，請安裝新的 「密碼同步化」過濾器並對它們進行設定。

請參閱 「設定密碼同步化過濾器」，第 69 頁。

6 必要時，設定 SSL。

如需指示，請參閱 「解決安全性事宜」，第 17 頁。

驅動程式要能夠設定 Active Directory (「訂閱者」通道) 中的密碼，需要由下列其中一個條件提供安全連接：

- 執行驅動程式的機器也就是領域控制器。
- 執行驅動程式的機器與領域控制器在同一個領域中。
- 在領域外的機器需要使用 「簡易」方法和 SSL 設定來連接領域控制器。只有在使用 「交涉」驗證機制時，才可以使用雙向密碼同步化。

  請參閱 Microsoft 文件以獲取相關指示，例如在領域控制器上設定數位證書 (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp)。

7 建立已啓用 「通用密碼」的 「密碼規則」來開啓 Identity Vault 使用者帳戶的 「通用密碼」。

請參閱 《*Novell Identity Manager 3.0* 管理指南》中的 「管理密碼同步化」。

爲了簡化管理，建議您將 「密碼規則」儘量指定至網路樹中的高層級。

8 使用驅動程式的 「密碼規則」和 「密碼同步化」設定來設定要用於 「密碼同步化」的案例。

請參閱 《*Novell Identity Manager 3.0* 管理指南》中的 「實作密碼同步化」。

9 測試密碼同步化。

10 「Identity Manager 密碼同步化」運作後，移除 「密碼同步化 1.0」。

10a 使用 「新增 / 移除程式」時，可以透過移除代辦來關閉 「密碼同步化 1.0」。

10b 在驅動程式的過濾器中，將 nadLoginName 屬性變更爲 「忽略」。

10c 從驅動程式組態移除會更新 nadLoginName 的反向相容性規則。

10d 如有需要，您還可以在運作 「Identity Manager 密碼同步化」後，從使用者移除 nadLoginName 屬性，因爲該屬性已經不再需要。

7.2.1 透過新增規則建立與密碼同步化 1.0 的反向相容性

「密碼同步化 1.0」依賴於更新名爲 nadLoginName 之屬性的驅動程式 Shim。該屬性會指出使用者的密碼是否需要同步化。如果新增新的使用者或變更使用者的密碼，系統就會新增或更新 nadLoginName 屬性以與之相符。

由於「Identity Manager 密碼同步化」中不需要此屬性，因此 Identity Manager 中的驅動程式 Shim 不再對其進行更新。因此，一旦安裝了新的驅動程式 Shim，就不會更新 nadLoginName 屬性。這說明 「密碼同步化 1.0」將不再接收已新增或重新命名之使用者的通知，除非您爲驅動程式組態新增反向相容性。

爲了從 「密碼同步化 1.0」順利地轉換到 「Identity Manager 密碼同步化」，您需要有 「密碼同步化 1.0」的反向相容性。

如需 「密碼同步化 1.0」的反向相容性，您必須新增會更新 nadLoginName 屬性的規則。

無論是更新現有的驅動程式組態，還是以 Identity Manager 提供的新組態來取代，都必須新增這些規則。依預設，Active Directory 的 Identity Manager 範例驅動程式組態不包含這些規則。

有三個規則是必要的，它們分別用於 「訂閱者輸出轉換」、「發行者輸入轉換」和 「發行者指令轉換」。這些規則會在 Identity Manager 之名爲 「Active Directory 的密碼同步化 1.0 規則」的組態檔案中提供。. 下列程序說明輸入新規則並將其新增至驅動程式組態的方法。

1. 在 iManager 中，按一下 「*Identity Manager* 公用程式」 > 「輸入驅動程式」。

   「輸入驅動程式精靈」隨即開啓。
2. 選取現有 Active Directory 驅動程式所在的驅動程式集，然後按 「下一步」。
3. 在出現的驅動程式組態清單中，捲動至 「其他規則」區段，並選取 「舊密碼同步化 *1.0* 規則：*AD* 和 *NT* 的反向相容性」，然後按 「下一步」。
4. 完成輸入提示：

   4a 選取現有的 Active Directory 驅動程式。

   選取現有的驅動程式可讓您新增必要的三個規則。輸入程序會建立三個新規則物件，之後您必須將這些物件插入到驅動程式組態的適當位置。

   4b 指定驅動程式是否爲 Active Directory 驅動程式。

   根據所選擇的系統，輸入的規則會略有不同。

   4c 瀏覽並選取與所要更新之驅動程式相關聯的 nadDomain 物件。

   此物件一般可以在 「驅動程式」物件下找到。

   4d (僅限 Active Directory) 指定映射到 Active Directory 屬性 AMAccountNam 之 eDirectory™ 屬性的名稱。

   您可以在驅動程式組態的 「網要映射」規則中找到此資訊。

   附註：如果 sAMAccountName 沒有映射到任何 eDirectory 屬性，則將 sAMAccountName 映射到 DirXML-ADAlias 名稱。

   ---
5. 按 「下一步」。

由於您選擇了現有的驅動程式，會出現一個網頁要您決定驅動程式的更新方式。在此情況下，您只需更新選定的規則即可。

6 選取「僅更新驅動程式中選定的規則」，並選取所列之三個規則的核取方塊。

7 按「下一步」，然後按一下「完成」，以完成精靈。

此時，已在「驅動程式」物件下建立三個新的規則做爲「規則」物件，但它們還不是驅動程式組態的一部份。若要連結它們，您必須在「訂閱者」和「發行者」通道上之驅動程式組態中的正確位置，手動插入每個規則。

8 將這三個新規則一一插入現有驅動程式組態上的正確位置中。

如果驅動程式組態的任一部份都有多個規則，請確定這些新的規則是列在最後。

表格 *7-2* 規則

規則物件名稱	插入規則的位置
PassSync(Pub) 指令轉換規則	發行者通道上的指令轉換規則
PassSync(Pub) 輸入轉換規則	發行者通道上的輸入轉換規則
PassSync(Sub) 輸出轉換規則	訂閱者通道上的輸出轉換規則

針對每個規則重複步驟 8a 至 8f。

8a 按一下「*Identity Manager*」>「*Identity Manager* 概觀」。

8b 選取正在更新之驅動程式的驅動程式集。

8c 按一下您剛剛更新的驅動程式。

即會開啓一個頁面，顯示驅動程式組態的圖形化表示。

8d 在要新增三個新規則之一的位置上按一下圖示。

8e 按一下「插入」，以新增新的規則。

在所顯示的「插入」頁面中，按一下「使用現有規則」，瀏覽新的規則物件，然後按一下「確定」。

8f 如果這三個新規則中的任何一個在清單中都有多個規則，則使用箭頭按鈕，將新的規則向下移至清單結尾。

9 針對所有 Active Directory 驅動程式重複步驟 1 至 9。

如果需要在「發行者」通道的「網要映射」規則中，將 sAMAccountName 映射至 DirXML-ADAliasName，則遵循此程序。

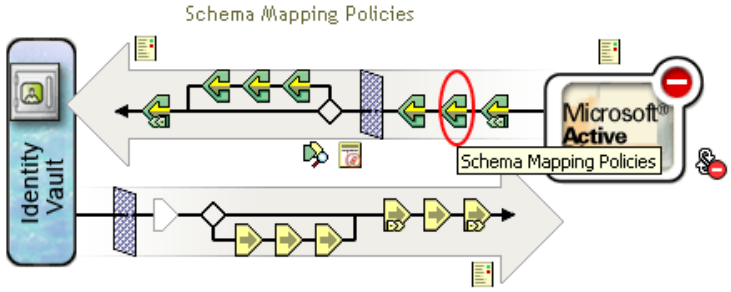
警告：如果 sAMAccountName 映射至另一個屬性，遵循此程序會使規則失效。此規則會停止同步化密碼。確定您在步驟 4d, 第 63 頁中輸入的是正確的屬性。

---

1 在 iManager 中，選取「*Identity Manager* > *Identity Manager* 概觀」。

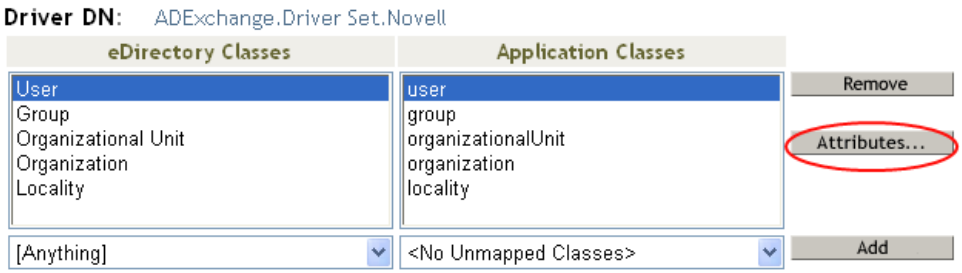
2 瀏覽至包含 Active Director 驅動程式的「驅動程式集」物件，並將其選取，然後按「下一步」。

3 按一下驅動程式圖示，然後按一下 「發行者」通道的 「網要映射規則」圖示。



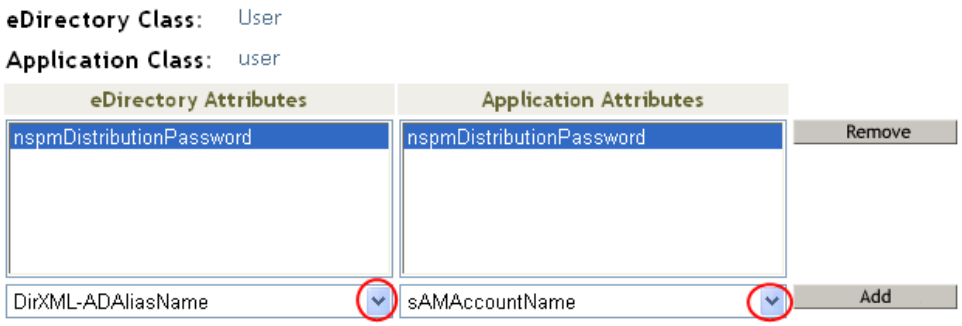
4 按一下 「編輯」。

5 選取 「使用者」類別，然後按一下 「屬性」。



6 按一下 「eDirectory 屬性」下方的下拉式清單，然後瀏覽至 「DirXML-ADAliasName」並將其選取。

7 按一下 「應用程式屬性」下方的下拉式清單，然後瀏覽至 「sAMAccountName」並將其選取。



8 按一下 「新增」，然後按一下 「確定」。

9 選取 「群組」類別，然後按一下 「屬性」。

10 針對 「群組」類別重複步驟 6 至 8。

11 按兩次 「確定」。

在完成此程序後，Active Directory 驅動程式的驅動程式組態會與 「密碼同步化 1.0」反向相容。這表示 「密碼同步化」會繼續如往常一樣運作，可以讓您在方便的時候升級至 「Identity Manager 密碼同步化」。

7.3 新的驅動程式組態與 Identity Manager 密碼同步化

如果您尚未使用「密碼同步化 1.0」，而是建立新的驅動程式或以 Identity Manager 組態取代現有驅動程式的組態，則請遵循《*Novell Identity Manager 3.0* 管理指南》之「設定並同步化新的驅動程式」中的指示。

此外，請執行下列各項：

- 必要時，設定 SSL。請參閱 「解決安全性事宜」，第 17 頁。

  驅動程式要能夠設定 Active Directory (「訂閱者」通道) 中的密碼，需要由下列其中一個條件提供安全連接：

  - 執行驅動程式的機器也就是領域控制器。
  - 執行驅動程式的機器與領域控制器在同一個領域。
  - 領域外的機器需要使用「簡易」方法和 SSL 設定來連接領域控制器。只有在使用「交涉」驗證機制時，才可以使用雙向密碼同步化。

    請參閱 Microsoft 文件以獲取相關指示，例如啓用 SharePoint Portal Server 2003 的安全通訊端層 (http://office.microsoft.com/en-us/assistance/HA011648191033.aspx)。
- 如果您要讓已連接系統提供 Identity Manager 的使用者密碼，請安裝新的「密碼同步化」過濾器並設定它們的組態。請參閱 「設定密碼同步化過濾器」，第 69 頁。
- 使用驅動程式的「密碼規則」和「密碼同步化」設定，來設定所需的「密碼同步化」案例。請參閱《*Novell Identity Manager 3.0* 管理指南》中的「實作密碼同步化」。

7.4 升級現有的驅動程式組態以支援 Identity Manager 密碼同步化

重要：如果驅動程式與「密碼同步化 1.0」搭配使用，則除了完成本節中的步驟外，還需完成 「將密碼同步化 1.0 升級至 Identity Manager 提供的密碼同步化」，第 61 頁中的其他步驟。

以下是使用本節中的程序所必須完成之任務的綜覽：

- 將驅動程式資訊清單、全域組態值和密碼同步化規則新增至驅動程式組態。如需新增之規則的清單，請參閱《*Novell Identity Manager 3.0* 管理指南》中的「驅動程式組態中所需的規則」。
- 變更過濾器，以在 nspmDistributionPassword 屬性上啓用「訂閱者」通知，並將「發行者」設定爲忽略。

先決條件

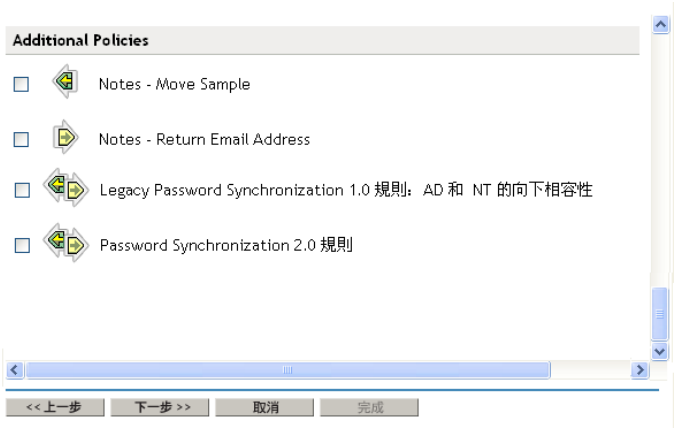
- ❑ 確定已將現有的驅動程式轉換成 Identity Manager 格式，如《*Novell Identity Manager 3.0* 管理指南》中的「將驅動程式組態從 DirXML 1.1a 升級至 Identity Manager 格式」所述。
- ❑ 使用「匯出驅動程式精靈」建立現有驅動程式的備份。
- ❑ 確定您已安裝新的驅動程式 Shim。如果沒有 Identity Manager 驅動程式 Shim，部份密碼同步化功能 (例如，「檢查密碼狀態」) 將無法運作。

程序

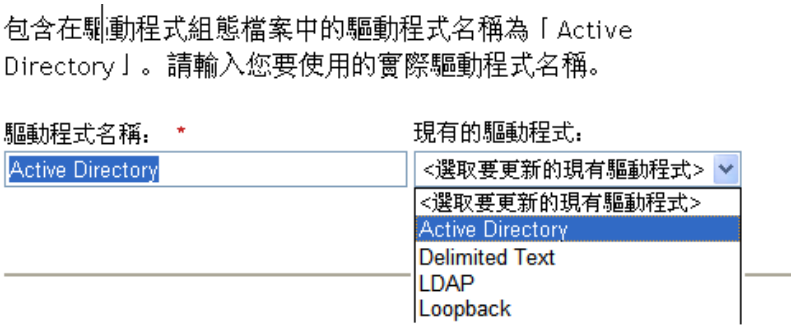
1 在 iManager 中，按一下「*Identity Manager* 公用程式」>「輸入驅動程式」。

「輸入驅動程式精靈」隨即開啓。

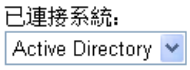
2 選取您現有驅動程式所在的驅動程式集，然後按「下一步」。



3 在出現的驅動程式組態清單中，選取「密碼同步化 *2.0* 規則」，然後按「下一步」。



4 從下拉式清單中選取「*Active Directory*」。



5 選取「*Active Directory*」做爲已連接系統，然後按「下一步」。

6 有關驅動程式和已連接系統之功能的三個提示，請回答「是」。

- 已連接系統是否可以提供 Identity Manager 的密碼。
- 已連接系統是否可以接受來自 Identity Manager 的密碼
- 已連接系統是否可以檢查密碼，以查看它是否與 Identity Manager 中的密碼相符。

7 按「下一步」，然後選取更新驅動程式的所有相關項目。

此選項會提供給您密碼同步化所需的驅動程式資訊清單、全域組態值 (GCV) 和密碼規則。

驅動程式資訊清單和 GCV 會覆寫已經存在的任何值，但由於這些類型的驅動程式參數是在 Identity Manager 中新增的，因此不應有任何要覆寫的現有值。

密碼規則不會覆寫任何現有的規則物件，而只是將它們新增至「驅動程式」物件。

如果您有想要儲存的驅動程式資訊清單或 GCV 值，則爲該驅動程式選擇名稱爲「僅更新選定的規則」的選項，並選取所有規則的核取方塊。此選項會輸入密碼規則，但不會變更驅動程式資訊清單或 GCV。

8 按「下一步」，然後按一下「完成」，以完成精靈。

此時，雖然這些新規則已做爲規則物件建立在驅動程式物件下，但它們還不是驅動程式組態的一部份。若要連結它們，您必須在「訂閱者」和「發行者」通道上之驅動程式組態中的正確位置，手動插入每個規則。

9 將每個新規則插入現有驅動程式組態上的正確位置。

如果規則集有多個規則，請確定這些密碼同步化規則列在最後。

如需規則及其插入位置的清單，請參閱《*Novell Identity Manager 3.0* 管理指南》中的「驅動程式組態中所需的規則」。

針對每個規則重複步驟 9a 至 9e。

9a 按一下「*Identity Manager*」>「*Identity Manager* 概觀」，然後選取所更新之驅動程式的驅動程式集。

9b 按一下您剛剛更新的驅動程式。

即會開啓一個頁面，顯示驅動程式組態的圖形化表示。

9c 在需要新增其中一個新規則的位置按一下圖示。

9d 按一下「插入」，以新增新的規則。

在所顯示的「插入」頁面中，按一下「使用現有規則」，瀏覽新的規則物件，然後按一下「確定」。

9e 如果任何一個新規則在清單中都有多個規則，則使用箭頭按鈕，將新的規則移至清單中的正確位置。

確定會依照《*Novell Identity Manager 3.0* 管理指南》中之「驅動程式組態中所需的規則」的列出順序顯示這些規則。

10 變更驅動程式的過濾器，以允許同步化 nspmDistributionPassword 屬性。

僅啓用「訂閱者」通道上的「通知」功能。將「發行者」通道設定爲「忽略」。

11 必要時，設定 SSL。

相關指示包含在「解決安全性事宜」，第 17 頁中。

驅動程式要能夠設定 Active Directory (訂閱者通道) 中的密碼，需要由下列其中一個條件提供安全連接：

- 執行驅動程式的機器也就是領域控制器。
- 執行驅動程式的機器與領域控制器在同一個領域。
- 領域外的機器需要使用「簡易」方法和 SSL 設定來連接領域控制器。只有在使用「交涉」驗證機制時，才可以使用雙向密碼同步化。

  請參閱 Microsoft 文件以獲取相關指示，例如在領域控制器上設定數位證書 (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp)。

12 如果您要讓已連接系統提供 Identity Manager 的使用者密碼，請安裝新的「密碼同步化」過濾器並設定它們的組態。請參閱「設定密碼同步化過濾器」，第 69 頁。

此時，驅動程式具有新的驅動程式 Shim、Identity Manager 格式和支援密碼同步化所需的其他元素：驅動程式資訊清單、GCV、密碼同步化規則和過濾器。現在您可以使用 iManager 中的「密碼同步化」介面，指定密碼流進和流出已連接系統的方式。

13 使用驅動程式的「密碼規則」和「密碼同步化」設定來設定所需的「密碼同步化」案例。

請參閱《*Novell Identity Manager 3.0* 管理指南》中的「實作密碼同步化」。

14 針對需要參與密碼同步化的所有驅動程式，重複步驟 1 至 14。

7.5 設定密碼同步化過濾器

驅動程式需要設定爲僅能在一台 Windows 機器上執行。

但是，安裝並設定好驅動程式後，還需要在其他每個領域控制器上執行下列操作：

1 安裝密碼過濾器 (pwfilter.dll 檔案)。

2 設定登錄以擷取密碼，這樣才能將獲取的密碼傳送至 Identity Manager。

密碼過濾器會隨著領域控制器的啓動而自動開啓。過濾器會擷取使用者使用 Windows 用戶端進行的密碼變更，對其加密，然後將它們傳送到驅動程式以更新 Identity Manager 資料儲存。

附註：如需設定「密碼同步化」的相關資訊，請參閱《*Novell Identity Manager 3.0* 管理指南》中的「實作密碼同步化」。

爲了簡化密碼過濾器的設定和管理，安裝驅動程式時，Identity Manager PassSync 公用程式會新增到「控制台」。依據您是否允許遠端存取領域控制器上的登錄，此公用程式會提供兩種設定密碼過濾器的選項：

- 如果您允許遠端存取登錄： 請使用 Identity Manager PassSync 公用程式，從要執行驅動程式的單一機器，設定所有領域控制器的密碼過濾器組態。

  此方法可讓您從同一位置設定所有領域控制器的組態。

  如果從同一機器設定所有領域控制器的組態，則 Identity Manager PassSync 公用程式會提供下列功能，協助您進行設定：

  - 可讓您指定要參與密碼同步化的領域。
  - 自動探查此領域的所有領域控制器。
  - 可讓您在每個領域控制器上從遠端安裝 pwfilter.dll。
  - 可在驅動程式執行的機器上，以及每個領域控制器上，自動更新登錄。
  - 可讓您檢視每個領域控制器上的過濾器狀態。
  - 可讓您從遠端將領域控制器重新開機。

    在您第一次新增密碼同步化的領域時，有必要將領域控制器重新開機，因爲擷取密碼變更的過濾器是一個 DLL 檔，而此 DLL 檔會在領域控制器啓動時隨之啓動。

  請參閱「從同一台機器設定所有領域控制器的密碼過濾器組態」，第 70 頁。

- 如果您不允許遠端存取登錄： 請分別設定每個領域控制器上的密碼過濾器。若要執行此動作，請在每個領域控制器上安裝驅動程式檔案，以取得 Identity Manager PassSync 公用程式，然後在每台機器上使用此公用程式來安裝密碼過濾器並更新登錄。

  請參閱「請分別設定每個領域控制器上的密碼過濾器」，第 73 頁。

7.5.1 從同一台機器設定所有領域控制器的密碼過濾器組態

此程序會說明如何從執行驅動程式的機器上安裝，以及如何設定所有領域控制器各自的密碼過濾器組態。

如果您允許遠端存取登錄，請使用此方法。

因爲設定過濾器需要重新開機領域控制器，您應該要在數小時之後再執行此程序，或一次只重新開機一個領域控制器。如果領域中有一個以上的領域控制器，請記住，需要執行 「密碼同步化」的每個領域控制器，都必須安裝過濾器，且需要重新開機。

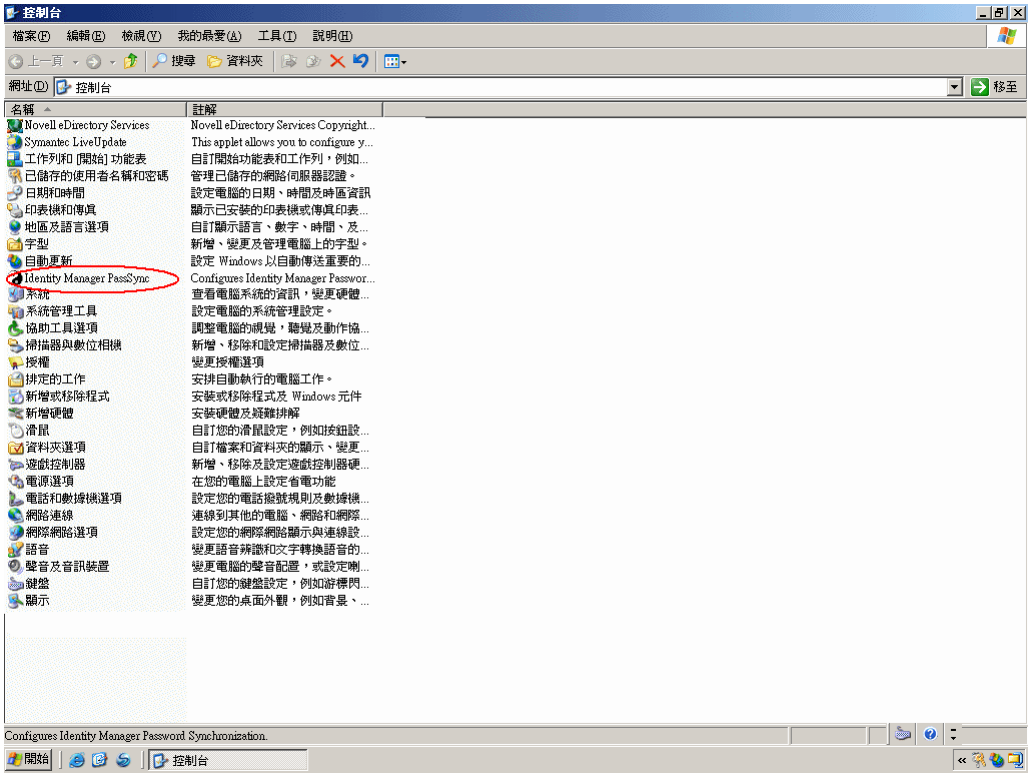
1 請確認在 135 (RPC 端點映射器) 在領域控制器以及設定要執行 Identity Manager Driver for Active Directory 的機器上，均可存取連接埠。

如果是透過 TCP 使用 NetBIOS，則還需要下列連接埠：

- 137: NetBIOS 名稱服務
- 138: NetBIOS 資料包服務
- 139: NetBIOS 會期服務

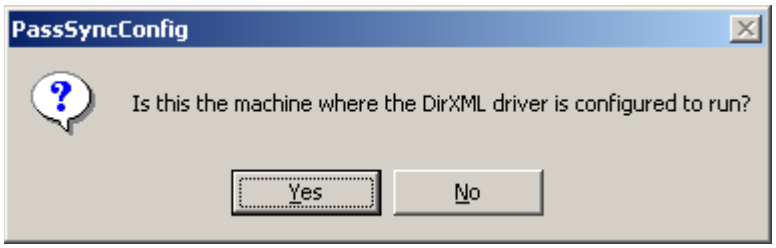
防火牆可以防止對連接埠的遠端存取。

2 在安裝驅動程式的電腦上，按一下 「開始 > 設定 > 控制台」。



3 連按兩下 *Identity Manager PassSync*。

第一次開啓此公用程式時，系統會詢問這是否是安裝 Identity Manager 驅動程式的機器。



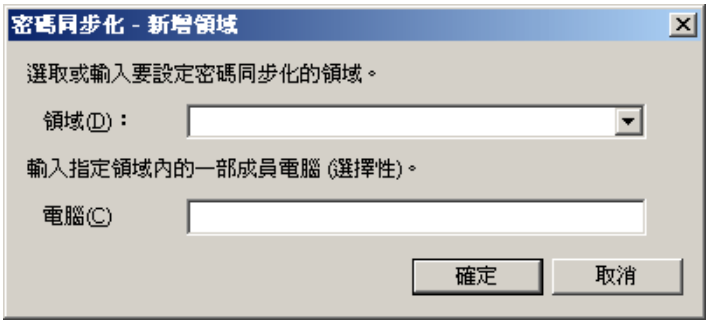
完成組態設定之後，除非從清單中移除此領域，否則系統不會再顯示此提示。

4 按一下「是」。

標示「已同步領域」的清單會隨即顯示。

5 若要新增想要參與密碼同步化的領域，請按一下「新增」。

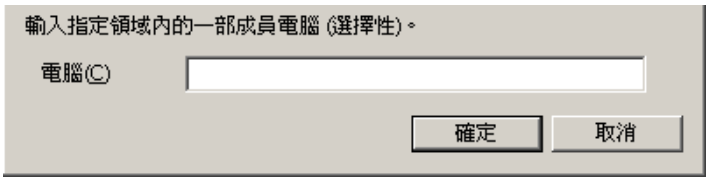
「新增領域」對話方塊會隨即顯示。



6 指定或選取您想新增的領域名稱。

下拉式清單會顯示已知的領域。

7 (選擇性) 指定領域中的電腦。



如果「電腦」編輯方塊保留空白，PassSync 會查詢本地機器。因此，如果是在領域控制器上執行 PassSync，就不需要輸入名稱。PassSync 會查詢本地機器 (此案例中指領域控制器)，並從資料庫內取得此領域中所有領域控制器的清單。

如果不是在領域控制器上進行安裝，則需要輸入領域內可以取得領域控制器的電腦名稱。

如果收到一條錯誤訊息指出 PassSync 無法找到領域，請輸入其他名稱。

8 決定是否使用領域的 DNS 名稱。

DNS 名稱提供了更多的進階驗證，可以在更大的安裝範圍內更可靠地尋找領域。不過，所能做出的選擇會由您的環境決定。

9 以管理員身份登入。

Identity Manager PassSync 公用程式會找到此領域內的所有領域控制器，並在每個領域控制器上安裝 pwfilter.dll。同時會在執行驅動程式的電腦以及每個領域控制器上更新登錄。這可能需費時數分鐘。

在重新開機領域控制器之後，pwfilter.dll 才會擷取密碼變更。Identity Manager PassSync 公用程式可讓您查看所有領域控制器的清單，以及領域控制器上過濾器的狀態。這也可以讓您從公用程式內部重新開機領域控制器。

10 按一下清單中的領域名稱，然後按一下「過濾器」。

公用程式會顯示所有領域控制器的名稱，以及每個領域控制器上過濾器的狀態。

每個領域控制器的狀態都會表示爲需要重新開機。但是，公用程式可能需要費時數分鐘來完成自動執行的任務，此時其狀態可能顯示爲「不明」。

11 重新開機每個領域控制器。

您可以根據自己的環境，選擇合適的時間執行重新開機。但是請記住，只有重新開機所有領域控制器之後，密碼同步化功能才會起作用。

12 當所有領域控制器的狀態都顯示爲「執行中」時，請測試密碼同步化功能確認其是否有效。

13 若要新增更多領域，請按一下「確定」回到領域清單，然後重複步驟 6 至步驟 12。

7.5.2 請分別設定每個領域控制器上的密碼過濾器

本節中描述的程序會說明如何分別安裝並設定 (一次一個) 每個領域控制器上的密碼過濾器。

如果您不允許遠端存取登錄，請使用此方法。

在此程序中，您會安裝此驅動程式，以取得 Identity Manager PassSync 公用程式。然後，您就可以使用此公用程式安裝 pwfilter.dll 檔案，指定要使用的連接埠，並指定執行 Identity Manager Driver for Active Directory 的主機機器。

因爲設定過濾器需要重新開機領域控制器，您應該要在數小時之後再執行此程序，或一次只重新開機一個領域控制器。如果領域中有一個以上的領域控制器，請記住，需要執行「密碼同步化」的每個領域控制器，都必須安裝過濾器，且需要重新開機。

1 請確認下列連接埠可供領域控制器以及設定要執行 Identity Manager Driver for Active Directory 的機器使用。

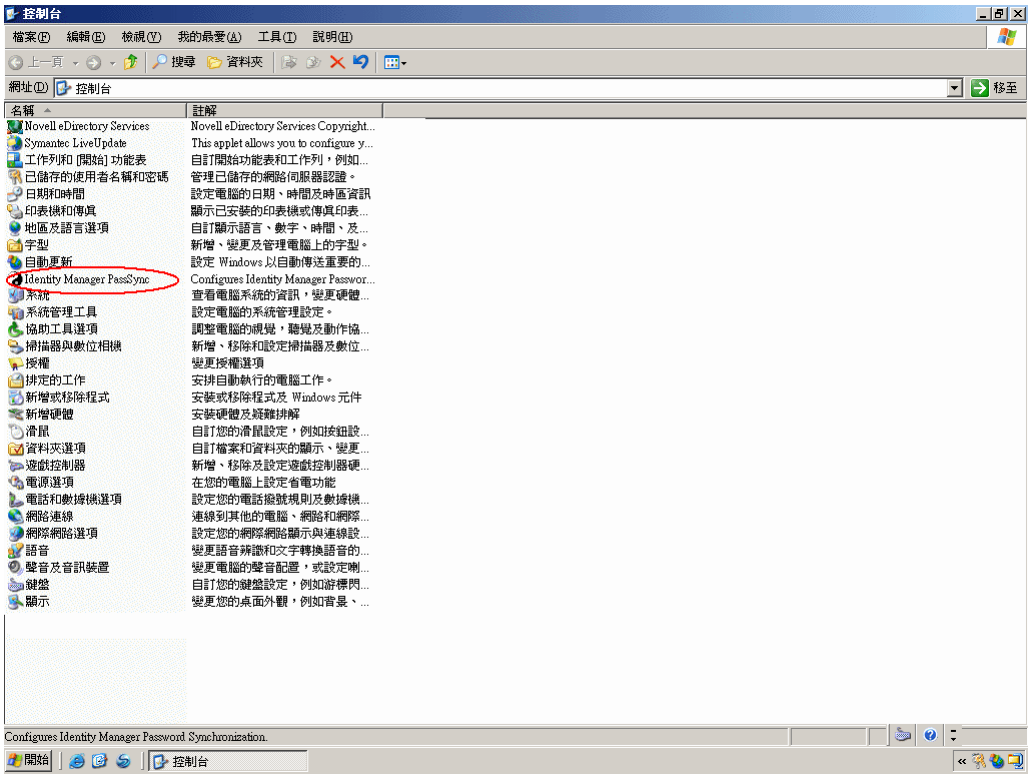
- 135: RPC 端點映射器

- 137: NetBIOS 名稱服務
- 138: NetBIOS 資料包服務
- 139: NetBIOS 會期服務

2 在領域控制器上，可以使用「Identity Manager 安裝」只安裝 Identity Manager Driver for Active Directory。

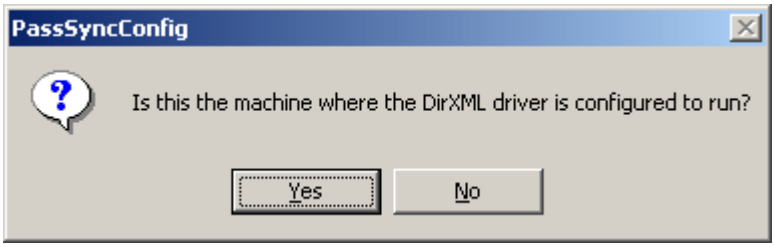
安裝此驅動程式時，會安裝 Identity Manager PassSync 公用程式。

3 按一下「開始 > 設定 > 控制台」，然後找到 Identity Manager PassSync 公用程式。



4 連按兩下 *Identity Manager PassSync*。

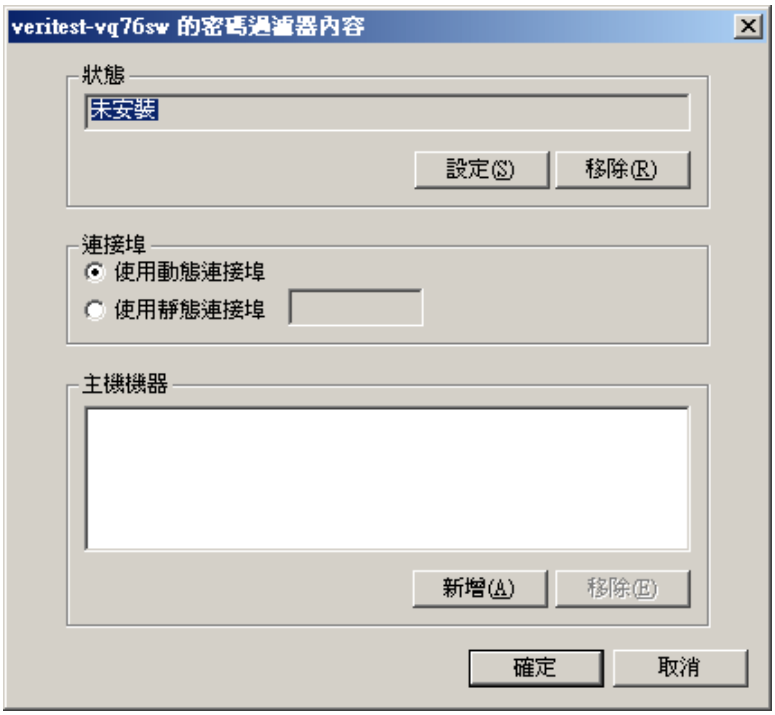
第一次開啓此公用程式時，系統會詢問這是否是安裝 Identity Manager 驅動程式的機器。



5 按一下「否」。

完成組態設定之後，除非使用「密碼過濾器內容」對話方塊中的「移除」按鈕移除密碼過濾器，否則系統不會再顯示此提示。

按一下「否」，會隨即顯示「密碼過濾器內容」對話方塊，其中的狀態訊息會指出此領域控制器上尚未設定密碼過濾器。



6 按一下「設定」按鈕，安裝密碼過濾器 (pwfilter.dll)。

7 在「連接埠」設定中，指定是否使用動態連接埠或靜態連接埠。

只有在決定設定自己的領域控制器遠端程序呼叫 (RPC) 組態而不使用預設值之後，您才可以選擇使用靜態連接埠。

8 指定 Identity Manager 驅動程式的位置，按一下「新增」按鈕，在「密碼同步化過濾器 - 新增主機」對話方塊中，指定執行 Identity Manager 驅動程式的機器「主機名稱」，然後按一下「確定」。

此步驟必須執行，密碼過濾器才會知道要將密碼變更傳送至何處。密碼過濾器會擷取密碼變更，然後必須將它們傳送到 Identity Manager 驅動程式，這樣才能更新 Identity Manager 資料儲存。

9 在「密碼過濾器內容」對話方塊中，按一下「確定」。

10 重新開機領域控制器，以完成密碼過濾器的安裝。

您可以根據自己的環境，選擇合適的時間執行重新開機。但是，請記住，只有所有領域控制器都安裝密碼過濾器且執行了重新開機之後，密碼同步化功能才會完全發生作用。

完成安裝並重新開機領域控制器之後，無論何時開啓領域控制器，都會自動載入密碼過濾器。

11 按一下「開始 > 設定 > 控制台」，然後連按兩下 Identity Manager PassSync 公用程式，再次查看密碼過濾器的狀態。

請確認狀態顯示爲「執行中」。

12 對於要參與「密碼同步化」的每個領域控制器，重複步驟 2 至步驟 11。

13 當所有領域控制器的狀態都顯示爲「執行中」時，請測試「密碼同步化」功能，以確認是否有效。

7.6 如果「同步化」失敗，請重試。

驅動程式和密碼過濾器的功能已提升，改進了密碼同步化失敗之後的重試方式。

7.6.1 「新增」或「修改」事件之後重試

如果未能成功從 Active Directory 將密碼變更傳送到 Identity Vault，驅動程式會快取密碼。只有擁有密碼的使用者發生「新增」或「修改」事件時，才會再次重試 (在之前版本中，每發生一次輪詢就會重試一次這些已儲存密碼)。

當驅動程式輪詢 Active Directory 中的變更時，驅動程式會收到使用者的「新增」或「修改」事件。對於每個使用者的「新增」或「修改」事件，驅動程式都會檢查這個新的使用者是否有已儲存的密碼。如果有已儲存的密碼，驅動程式會將此密碼視爲修改使用者事件，傳送至 Identity Vault。

如果「密碼同步化」已設定爲在同步化失敗時向使用者傳送電子郵件訊息，則增強後的方式會將使用者可能收到的電子郵件量減至最少。

7.6.2 密碼過期時間

已新增名爲「密碼過期時間」的參數。此參數可讓您決定第一次同步化失敗時，保留此特定使用者密碼的時間。在 Identity Vault 中的密碼成功變更或超過「密碼過期時間」之前，驅動程式都會保留此密碼。

如果「密碼同步化」已設定爲在同步化失敗時向使用者傳送電子郵件訊息，則增強後的方式會將使用者可能收到的電子郵件量減至最少。

已新增名爲「密碼過期時間」的參數。此參數可讓您決定第一次同步化失敗時，保留此特定使用者密碼的時間。在 Identity Vault 中的密碼成功變更或超過「密碼過期時間」之前，驅動程式都會保留此密碼。

輸入範例驅動程式組態時，系統會提示您指定過期時間。如果不指定，或者時間 (間隔欄位) 包含無效字元，則預設的過期時間爲 60 秒。如果指定的時間小於三倍的指定輪詢間隔時間，則驅動程式會將此時間變更爲三倍的輪詢間隔時間。

請將此值設定得夠大，這樣才能處理任何已存在的密碼暫時積存。如果要進行大量變更，請將逾時設定得足夠大以便處理所有變更。一般規則是允許一秒鐘處理一個密碼。例如，同步化 18,000 個密碼允許花費的時間爲 300 分鐘 (18,000 個密碼除以 60 秒)。

如果設定值爲 -1，表示時間無限。此設定可以處理大量變更，但是會導致問題。例如，由於未關聯帳戶，可能永遠無法同步化密碼。此密碼就會永遠保留在系統中。許多類似情況都可能導致系統中儲存大量的未同步化密碼。

「密碼過期時間」的相關案例

在「發行者」通道上，密碼同步化可能發生在「新增」事件之前。驅動程式會在「新增」事件之後立即重試。

案例：無效

在 Active Directory 中建立具有密碼的新使用者。過濾器會立即將新密碼傳送到驅動程式。但是，由於事件發生在輪詢之間，驅動程式尚未收到使用者「新增」事件。因爲驅動程式尚未在 Identity Vault 中建立此使用者，所以在第一次嘗試密碼同步化時會失敗。驅動程式快取此密碼。

在下一個輪詢期間，驅動程式會收到新使用者的「新增」使用者事件。驅動程式還會檢查是否已快取此新使用者的密碼。驅動程式會將「新增」使用者事件傳送到 Identity Vault，同時也會傳送「修改」使用者事件，以同步化密碼。

在此情況下，密碼同步化只會延遲一個輪詢間隔。

「密碼過期時間」參數在此時是無效的。

案例：增加「過期時間」

在 Active Directory 中建立具有密碼的新使用者。但是，使用者資訊不符合 Active Directory 驅動程式的「建立」規則要求。

例如，「建立」規則可能需要全名，但卻缺少此必要資訊。如同「無效」範例中那樣，過濾器會立即將密碼變更傳送到驅動程式。但是，因爲使用者並不存在，所以 Identity Vault 中的第一次嘗試密碼變更會失敗。驅動程式快取此密碼。

但在此時，因爲使用者資訊不符合「建立」規則的要求，即使驅動程式會輪詢 Active Directory 中的變更且找到了新使用者，它也無法建立新使用者。

建立新使用者和同步化密碼會被延遲，直到所有使用者資訊都新增到 Active Directory 從而符合「建立」規則爲止。然後，驅動程式會將新使用者新增到 Identity Vault，檢查是否已快取此新使用者的密碼，最後傳送「修改」使用者事件以同步化密碼。

只有當時間間隔在 Active Directory 中的使用者資訊符合「建立」規則前即先到期，「密碼過期時間」參數才會影響此案例。如果「新增」事件發生在密碼到期之後，且驅動程式未曾快取使用者的密碼，則不會發生同步化。因爲驅動程式未曾快取密碼，所以會使用密碼規則中的預設密碼。

只有在使用者變更了 Active Directory 或 Identity Vault 中的密碼之後，才會同步化此密碼。

如果「密碼同步化」設定爲雙向密碼流程，則在 Identity Vault 中發生密碼變更時，也可以將密碼從 Identity Vault 同步化到 Active Directory。

如果對「建立」規則有限制，在 Active Directory 中需要花一天多的時間才能完成新使用者資訊，則您可能要相應地增加「密碼過期時間」參數間隔。驅動程式這時可以快取密碼，直到終於在 Identity Vault 中建立使用者爲止。

案例：從未符合要求

在 Active Directory 中建立具有密碼的使用者。不過，此使用者從未符合 Active Directory 驅動程式之「建立」規則的準則。

例如，假設 Active Directory 中的新使用者有「描述」指出此使用者爲約聘，且「建立」規則會阻止建立約聘「使用者」物件，因爲按照業務規則，不希望約聘人員在 Identity Vault 中擁有對應的使用者帳戶。如同上述範例，過濾器會立即傳送密碼變更，但是第一次嘗試密碼同步化時會失敗。驅動程式快取此密碼。

在此情況下，不會在 Identity Vault 中建立對應的使用者帳戶。因此，驅動程式不會同步化已快取的密碼。超過「密碼過期時間」之後，驅動程式會從其快取中移除使用者密碼。

案例：電子郵件通知

Markus 具有 Active Directory 帳戶和對應的 Identity Vault 帳戶。他變更了他的 Active Directory 密碼，其中包含六個字元。但是，此密碼不符合管理員在 eDirectory 中建立的「密碼規則」要求，亦即至少要有八個字元。「密碼同步化」設定爲拒絕不符合規則的密碼，並向 Markus 傳送通知電子郵件，告知密碼同步化失敗。驅動程式只在 Active Directory 中的「使用者」物件發生變更時，才會快取密碼並重試。

在此案例中，變更密碼之後，Markus 會收到說明密碼同步化失敗的電子郵件。每當驅動程式重試密碼時，Markus 都會收到相同的電子郵件訊息。

如果 Markus 在 Active Directory 中將密碼變更爲符合「密碼規則」的密碼，則驅動程式會成功地將新密碼同步化到 Identity Vault。

如果 Markus 變更的密碼不符合規則，則密碼同步化一定會失敗。當超過「密碼過期時間」時，驅動程式會刪除已快取的密碼且以後都不會再重試。

疑難排解

8

8.1 發行者或訂閱者的非同步化變更

若要同步 Active Directory 中的變更，Identity Manager 驅動程式所使用的帳戶必須設定適當的權限。如需必要權限的相關資訊，請參閱 「建立管理帳戶」，第 21 頁。

如果使用預設規則，還必須符合「建立」、「相符」和「佈置」規則的要求。如需預設規則之要求的相關資訊，請參閱 「規則」，第 10 頁。

dirxml-uACLockout 屬性不會在「發行者」通道上同步化。

8.2 使用無效的 NT 登入名稱字元

預設「訂閱者」建立規則會依據 Identity Vault 中帳戶的相對可辨識名稱，產生 NT 登入名稱 (也稱爲 sAMAccountName 和 Windows 2000 以前的登入名稱)。NT 登入名稱使用 ASCII 字元集的子集。在 Active Directory 中建立物件前，預設規則會先去除無效的字元。

如果此規則不符合貴公司的商務規則，可以在輸入規則後再進行變更。Identity Vault 帳戶名稱並非傳統 ASCII 字元集的公司必須特別注意這條規則。

8.3 同步化 c、co 和 countryCode 屬性

使用 Active Directory 管理主控台選取使用者國家時，需要設定三個屬性：

表格 ***8-1*** 國家屬性

屬性	描述
c	包含一個由 ISO 定義的雙字元國家碼。
co	包含一個較長的國家名。
countryCode	包含一個代表國家的數值，此數值也由 ISO 定義。

因爲 ISO 定義的數值國家碼用於無法處理英文字母字元的應用程式，所以在預設情形下，Identity Vault 的綱要包含 c 和 co，但不包含 countryCode。

Identity Manager 能夠映射 c 和 co。如果在 eDirectory™ 綱要中新增一個與 countryCode 類似的屬性，則也能映射 countryCode。

Active Directory 的管理主控台會嘗試讓這三個屬性同步，這樣當您在主控台中設定國家時，三個屬性便都會有適當的值。一些管理員可能希望在透過 Identity Manager 設定屬性時，系統也能執行類似的動作。例如，您應該要設定驅動程式的組態，這樣即使過濾器中只含有 c，當「訂閱者」通道傳送 c 的變更時也會對 co 與 countryCode 進行設定。

8.4 同步化操作屬性

操作屬性是指由包含特殊操作資訊之輕量目錄存取協定 (LDAP) 伺服器所維護的屬性。操作屬性是唯讀的，因此無法同步化或變更。

8.5 Windows 2003 的密碼複雜度

密碼必須符合密碼規則指定的準則。

Windows 2000/2003 密碼規則中的複雜度和要求與 eDirectory 中的不同。

如果您計畫使用「密碼同步化」，則建立和使用的密碼必須同時符合 Active Directory 與 eDirectory™ 的複雜度規則；否則密碼便會失敗。

提示：在制定密碼規則時，應盡可能爲兩個系統制定類似的規則。在實驗室環境中，先停用 Windows 2003 伺服器的加強性密碼功能，然後再安裝 Active Directory 驅動程式。Active Directory 驅動程式正常工作後，確定 eDirectory 和 Active Directory 中使用的密碼同時符合兩個系統的複雜度規則。然後重新啓用 Windows 2003 伺服器的加強性密碼功能。

如需疑難排解秘訣，請參閱 TID 10083320 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10083320.htm)。

8.6 錯誤訊息 LDAP_SERVER_DOWN

錯誤碼 LDAP_SERVER_DOWN 通常表示，驅動程式無法開啓爲同步化所設定之 Active Directory 領域控制器上的輕量目錄存取協定 (LDAP) 連接埠。導致此狀況的原因有多種。

- 驅動程式驗證網路位置中命名的伺服器不正確。驗證網路位置應該包含用於同步化之領域控制器的 DNS 名稱或 IP 位址。如果將參數保留空白，驅動程式會嘗試連接到執行驅動程式 Shim 的機器 (執行 IDM 的伺服器，或「遠端載入器」所在的伺服器)。

- 您正在使用驗證網路位置的 IP 位址，而且停用了 Active Directory 的非 Kerberos 驗證。Kerberos 需要驗證網路位置的 DNS 名稱。

  驅動程式 Shim 只能使用 Windows 2000 之前版本的登入方法或簡易結合來驗證。如果停用網路上的 NTLM、NTLM2 和簡易結合，您可能會收到 LDAP_SERVER_DOWN 的錯誤訊息。
- 您已將驅動程式設定爲使用到 Active Directory 的保全插槽層 (SSL) 連接。此訊息表示您輸入驅動程式 Shim 伺服器的證書出現錯誤，或者根本沒有輸入證書。

8.7 密碼同步化秘訣

我們建議您在同步化密碼時使用安全連接。以下兩者間的連接比較容易遭受攻擊：

- Metadirectory 引擎與 「遠端載入器」
- 「遠端載入器」與 Active Directory

  僅限從所連接的領域控制器遠端執行 「遠端載入器」的情況。
- Metadirectory 引擎與 Active Directory (不使用 「遠端載入器」時)

  僅限領域控制器不在本地機器的情況。

您可以執行下列其中一或多項來建立安全連接：

- 設定 Metadirectory 引擎與 「遠端載入器」之間的保全插槽層 (SSL) 組態
- 在領域控制器上執行 「遠端載入器」
- 設定驅動程式 Shim 和 Active Directory 之間的保全插槽層 (SSL) 組態

  如果是在所連接的領域控制器上執行驅動程式，則不適用。

如果不在領域控制器上執行驅動程式 Shim，則必須先設定保全插槽層 (SSL) 組態才能使密碼同步。

8.7.1 提供啓始密碼

如果在最初建立使用者時，系統顯示密碼不符合規則的錯誤，則需要檢查您的密碼規則。

例如，您希望 Active Directory 驅動程式在 Identity Vault 中建立 「使用者」物件時，能爲使用者提供啓始密碼。建立使用者後，驅動程式 Shim 會建立此使用者並設定密碼。

因爲新增使用者與設定密碼是分別進行的，所以在此情況下，新使用者會收到預設密碼，即使只是暫時性的。因爲 Active Directory 驅動程式會在新增使用者之後立即傳送密碼，所以密碼會很快更新。

如果預設密碼與使用者的 eDirectory 密碼規則不一致，則會顯示錯誤。例如，如果根據使用者的姓所建立的預設密碼太短，不符合密碼規則，您可能就會看到表示密碼太短的 -216 錯誤。然而，如果 Active Directory 驅動程式隨後傳送一致的啓始密碼，則會很快更正此情況。

無論您使用的驅動程式爲何，如果想讓建立 「使用者」物件的已連接系統提供啓始密碼，請考量進行下列其中一項操作：

- 變更 「發行者」通道上建立預設密碼的規則，以使預設密碼符合 Identity Vault 中爲您組織定義的 「密碼規則」(使用 「密碼管理」中的 「管理密碼規則」選項建立)。如果啓始密碼來自授權應用程式，便會取代預設密碼。

  此選項較爲可取。爲了維護系統內的高層次安全性，我們建議使用預設密碼規則。

- 移除「發行者」通道上建立預設密碼的規則。範例組態中，此規則在「指令轉換」規則集內提供。eDirectory 中允許新增沒有密碼的使用者。此選項假設，新建「使用者」物件的密碼最終會經過「發行者」通道，所以「使用者」物件沒有密碼的時間很短。

如果啓始密碼不是源自新增事件，而是源自後續事件，這些方法尤爲重要。

8.8 設定保全插槽層 (SSL) 參數的位置

驅動程式組態中的保全插槽層 (SSL) 參數用於 Active Directory 驅動程式與 Active Directory 之間的 SSL，而非 Metadirectory 引擎與「遠端載入器」之間的保全插槽層 (SSL)。請參閱「加密」，第 18 頁。

8.9 Active Directory 帳戶在使用者新增到「訂閱者」通道後關閉

預設組態是將「Identity Vault 登入關閉」屬性映射到 Active Directory 之 UserAccountControl 屬性的 Dirxml-uACAccountDisable 位元。新增「訂閱者」的操作可能會將「登入關閉」設定爲 false (帳戶啓用)，但是新增操作的「發行者」迴路卻報告「登入關閉」爲 true (帳戶關閉)。

此外，檢查 Active Directory 中的物件時可能會顯示帳戶已關閉。這種狀況有時是因爲驅動程式在 Active Directory 中建立物件的方式所引起的，有時則是因爲驅動程式與 Active Directory 本身之間的規則不符所引起的。

8.9.1 Active Directory 使用者和電腦中的「帳戶關閉」

如果提供週期完成後 Active Directory 中的帳戶仍然關閉，則可能是由於爲驅動程式設定的規則與 Active Directory 強制執行的規則不符。

以「需要密碼」規則爲例。如果使用者新增操作包含無效的密碼 (或根本沒有密碼)，Active Directory 中建立的帳戶便會關閉。但 Active Directory 可能還是會在缺少驅動程式知識的情況下，設定 userAccountControl 中的 dirxml-uACPasswordNotRequired 位元。

有趣的是，如果新增操作不包含 Dirxml-uACPasswordNotRequired 的規則，上述情況就會導致新增操作的「登入啓用」動作失敗。因此，帳戶仍然處於關閉狀態。

驅動程式稍後 (也許很快，如果進行合併操作的話) 可能會將「登入關閉」設定爲 false，以嘗試再次開啓帳戶。如果想要置換 Active Directory 規則，並確保帳戶始終要求密碼，則一旦「訂閱者」通道上的「登入關閉」發生變更，便應該將 Dirxml-uACPasswordNotRequired 設定爲 false。

8.10 將父信箱移至子領域

如果透過變更使用者的 homeMDB 屬性將父信箱移至子領域的信箱儲存，則驅動程式不會執行此移動。傳回的錯誤碼爲 0x80072030。

這種錯誤發生在領域之間的移動。不支援將 Exchange 父信箱移到子領域。

8.11 回存 Active Directory

如果需要回存一些或所有 Active Directory，驅動程式可能會挑出一些過渡事件，並在 Identity Vault 上執行不需要的動作。爲了安全回存，請在執行回存操作期間暫時關閉驅動程式，然後使 Identity Vault 和 Active Directory 再次同步。

1. 關閉驅動程式。
2. 在 Identity Vault 中，刪除驅動程式物件上的 Dirxml-DriverStorage 屬性。
3. 回存 Active Directory。
4. 將 Active Directory 驅動程式設定爲「手動」或「自動」啓動。
5. 啓動驅動程式。
6. 重新移轉以尋找未關聯的物件。

8.12 將驅動程式移動到不同的領域控制器

您可以透過變更驅動程式「驗證網路位置」參數，設定驅動程式與不同的領域控制器同步。重新啓動驅動程式後，驅動程式用來追蹤 Active Directory 變更的狀態資訊無效，Active Directory 可能會重放大量舊事件，讓狀態回到目前時間。

若要避免這種重放，可以在更新「驗證網路位置」時移除驅動程式的狀態資訊：

1. 停止驅動程式。
2. 在 Identity Vault 中，刪除「驅動程式」物件上的 Dirxml-DriverStorage 屬性。
3. 更新「驗證網路位置」參數。
4. 啓動驅動程式。

   這會導致 Identity Vault 中關聯物件的重新同步化。
5. 重新移轉以尋找 Active Directory 中未關聯的物件。

8.13 從 Active Directory 移轉

從 Active Directory 移轉至 Identity Vault 時，需要考慮到 Active Directory 伺服器上的物件內含項目、DN 參考和搜尋限制。處理內含項目的一般策略是先移轉容器，再移轉群組成員物件 (包含使用者物件)，最後移轉群組。如果要移轉的物件很多，則需要調整策略以處理 Active Directory 伺服器上設定的輕量目錄存取協定 (LDAP) 搜尋限制。您可以變更輕量目錄存取協定 (LDAP) 伺服器上的限制，也可以將移轉調整爲每次只取物件的子集 (例如，一次移轉一個容器，或以 酏捸 B 釕 '... 的順序移轉物件)。

8.14 設定輕量目錄存取協定 (LDAP) 伺服器搜尋限制

以下終止會期說明如何使用 NTDSUTIL.EXE 變更領域控制器上的輕量目錄存取協定 (LDAP) 搜尋參數。您只需變更 IDM 同步化在移轉期間使用之領域控制器上的這些設定即可。寫下目前的組態值，並在完成移轉後執行 NTDSUTIL.EXE，還原爲原始值。NTDSUTIL.EXE 可以在任何成員伺服器上執行。

1. 在指令提示符中輸入 ntdsutil。
2. 輸入 LDAP Policies，然後按 Enter。
3. 輸入 Connections，然後按 Enter。

4 輸入 Connect to domain *domain_name*，然後按 Enter。

5 輸入 Connect to server *server_name*，然後按 Enter。

6 輸入 Quit，然後按 Enter。

7 輸入 Show Values，然後按 Enter。

```
C:\>ntdsutil ntdsutil: LDAP Policies ldap policy: Connections server
connections: Connect to domain raptor Binding to \\raptor1.raptor.lab
... Connected to \\raptor1.raptor.lab using credentials of locally
logged on user. server connections: Connect to server raptor1
Disconnecting from \\raptor1.raptor.lab... Binding to raptor1 ...
Connected to raptor1 using credentials of locally logged on user.
server connections: Quit ldap policy: Show Values

Policy                        Current(New) MaxPoolThreads
4 MaxDatagramRecv                   4096 MaxReceiveBuffer
10485760 InitRecvTimeout               120 MaxConnections
5000 MaxConnIdleTime                   900 MaxPageSize
1000 MaxQueryDuration                  120 MaxTempTableSize
10000 MaxResultSetSize                 262144 MaxNotificationPerConn
5 MaxValRange                         1500ldap policy: set MaxQueryDuration
to 1200 ldap policy: set MaxResultSetSize to 6000000 ldap policy:
Commit Changes ldap policy: Quit ntdsutil: Quit Disconnecting from
raptor1...C:\>
```

變更 CN=Deleted Objects 容器的許可

A

Active Directory 物件刪除後，有一小部份物件會保留一段指定的時間，以便正在複製變更的其他領域控制器能注意到此刪除動作。依預設，只有系統帳戶和「管理員」群組成員可以檢視此容器的內容。本節描述如何修改 CN=Deleted Objects 容器的許可。

如果您的企業應用程式或服務以非系統帳戶或非管理員帳戶結合到 Active Directory，並輪詢目錄變更，則可能需要變更 Deleted Objects 容器的許可。

這個程序要求執行 Active Directory Application Mode (ADAM) 套件中的 dscals.exe。此套件是「Windows Server 2003 支援工具」中版本的升級版，支援所有必要的功能。Windows XP Professional、Windows Server 2003 Standard Edition、Windows Server 2003 Enterprise Edition 和 Windows Server 2003 Datacenter Edition 都支援 ADAM 管理工具。

若要取得並安裝 ADAM 管理工具：

1. 從 ADAM 網頁 (http://www.microsoft.com/downloads/details.aspx?FamilyId=9688F8B9-1034-4EF6-A3E5-2A2A57B5C8E4&displaylang=en) 下載 ADAM 零售套件。
2. 連按兩下已下載的檔案，並指定解壓縮歸檔的目的目錄。
3. 連按兩下 adamsetup.exe 啓動「Active Directory Application Mode 設定精靈」，然後按「下一步」。
4. 檢視並接受授權條款，然後按「下一步」。
5. 僅選取 ADAM 管理工具，然後按「下一步」。
6. 檢視選項，然後按「下一步」。
7. 設定結束後，按一下「完成」。

安裝 ADAM 管理工具後，請修改 CN=Deleted Objects 容器的許可：

1. 以「領域管理員」群組成員的使用者帳戶登入。
2. 按一下「開始 > 程式集 > *ADAM* > *ADAM* 工具指令提示符」。
3. 在指令提示符中輸入下列指令：

   ```
   dsacls "CN=Deleted Objects,DC=Contoso,DC=com" /takeownership
   ```

   取代自己領域之 Deleted Objects 容器的可識別名稱。

   樹系中的每一個領域都有自己的 Deleted Objects 容器。

   輸出顯示如下：

   ```
   Owner: Contoso\Domain Admins Group: NT AUTHORITY\SYSTEM Access
   list: {This object is protected from inheriting permissions from
   the parent} Allow BUILTIN\Administrators  SPECIAL ACCESS LIST
   CONTENTS READ PROPERTY Allow NT AUTHORITY\SYSTEM     SPECIAL ACCESS
   DELETE READ PERMISSONS WRITE PERMISSIONS CHANGE OWNERSHIP CREATE
   CHILD DELETE CHILD LIST CONTENTS WRITE SELF WRITE PROPERTY READ
   ```

```
PROPERTY The command completed successfully
```

4 若要授予安全性主體檢視 CN=Deleted Objects 容器中物件的許可，請輸入下列指令：

```
dsacls "CN=Deleted Objects,DC=Contoso,DC=com" /g
CONTOSO\JaneDoe:LCRP
```

在此範例中，授予了使用者 CONTOSO\JaneDoe 對容器的「列出內容」與「讀取內容」許可。使用者擁有這些許可後，已足以檢視 Deleted Objects 容器的內容，但還無法對此容器中的物件做任何變更。這些許可與授予「管理員」群組的預設許可相等。依預設，只有系統帳戶擁有修改 Deleted Objects 容器中物件的許可。

輸出顯示如下：

```
      Owner: CONTOSO\Domain Admins Group: NT AUTHORITY\SYSTEM
Access list: {This object is protected from inheriting permissions
from the parent} Allow BUILTIN\Administrators  SPECIAL ACCESS LIST
CONTENTS READ PROPERTY Allow NT AUTHORITY\SYSTEM    SPECIAL ACCESS
DELETE READ PERMISSONS WRITE PERMISSIONS CHANGE OWNERSHIP CREATE
CHILD DELETE CHILD LIST CONTENTS WRITE SELF WRITE PROPERTY READ
PROPERTY Allow CONTOSO\JaneDoe        SPECIAL ACCESS LIST CONTENTS
READ PROPERTY The command completed successfully.
```

現在，使用者 CONTOSO\JaneDoe 擁有檢視 CONTOSO 領域中已刪除物件的許可。