



NetIQ® Identity Manager 安裝和升級指南 - Windows

2024 年 5 月

法律聲明

Copyright 2009 - 2024 Open Text 版權所有。

Open Text 及其關係企業和授權者 (統稱為「Open Text」) 之產品與服務的保固，依約僅載於該項產品與服務隨附的明確保固聲明中。本文中任何內容不得解釋為構成其他保固。對於本文中之技術或編輯錯誤或疏漏，Open Text 不負任何責任。此處包含的資訊如有變更，恕不另行通知。如需其他資訊 (如與認證相關的聲明和商標)，請造訪 <http://www.microfocus.com/about/legal/> (<http://www.microfocus.com/about/legal/>)。

目錄

關於本書和文件庫	11
I Identity Manager 環境綜覽	13
1 Identity Manager 元件簡介	15
Identity Manager 伺服器元件	16
Identity Manager 伺服器	17
遠端載入器	17
擴送代理程式	18
Identity Console	18
Identity Applications 元件	18
使用者應用程式	19
驗證服務	19
Self-Service Password Reset	19
Web 應用程式伺服器	19
Identity Applications 資料庫	20
Identity Applications 的驅動程式	20
Identity Reporting 元件	21
Identity Reporting	21
驗證服務	21
Self-Service Password Reset	21
Identity Reporting 資料庫	21
Web 應用程式伺服器	22
Identity Reporting 的驅動程式	22
Sentinel Log Management for Identity Governance and Administration	23
Identity Manager 工具	23
Designer for Identity Manager	23
Analyzer for Identity Manager	24
功能架構	25
Identity Manager 的部署選項	26
範例 Identity Manager 部署	27
範例進階版部署	28
範例標準版部署	30
II 規劃 Identity Manager 安裝	33
2 規劃安裝	35
確定硬體要求	35
部署規劃工作表	36
架構工作表	36
系統要求工作表	37
查看 Identity Manager 元件使用的連接埠	37

III 安裝和設定 Identity Manager 元件	39
3 安裝和組態程序綜覽	41
安裝順序	41
瞭解 Identity Manager 伺服器、Identity Applications 及 Identity Reporting 元件的安裝和組態程序	41
安裝方式類型	42
安裝選項	42
組態模式類型	42
在組態期間使用不可猜出的密碼	43
瞭解 Designer 和 Analyzer 的安裝程序	43
安裝程序	43
Identity Manager 伺服器、Identity Applications 和 Identity Reporting 的安裝程序	43
安裝遠端載入器	45
安裝 Java 遠端載入器	46
安裝 .NET 遠端載入器	48
安裝 SSPR	48
瞭解組態設定	49
Identity Manager 引擎的組態工作表	49
Identity Applications 的組態工作表	50
Identity Reporting 的組態工作表	52
Self-Service Password Reset 的組態工作表	54
安裝後步驟	55
將 preferIPv4Stack 內容傳遞至 JVM	55
檢查伺服器的狀態	56
監控狀態統計資料	56
建立複合索引	57
設定 Identity Application 以拒絕用戶端發起的 SSL 重新交涉	57
4 完成安裝的最後步驟	59
設定 Identity Vault 的組態	59
手動將 Identity Applications 和 Identity Reporting 證書輸入至 Identity Vault 中	59
設定遠端載入器和驅動程式	60
設定忘記密碼管理功能	60
使用 Self Service Password Reset 進行忘記密碼管理	60
使用外部系統進行忘記密碼管理	62
針對分散式環境或叢集環境更新儀表板中的 SSPR 連結	63
設定 Identity Applications 的資料庫	64
設定 Oracle 資料庫	64
設定 SQL Server 資料庫	65
設定 Identity Applications	66
完成 Identity Applications 的設定	66
部署適用於 Identity Applications 的 REST API	88
使用 Oracle 服務名稱存取 Oracle 資料庫	88
手動建立資料庫綱要	88
組態 Identity Applications 的單一登入設定	90
啟動 Identity Applications	90
Identity Applications 的組態和使用考量	91
設定資料收集的執行時期環境	91
將資料收集服務驅動程式設定為從 Identity Applications 收集資料	92
移轉資料收集服務驅動程式	93
新增對自訂屬性和物件的支援	95

新增多個驅動程式集支援	97
將驅動程式設定為使用 SSL 在遠端模式下執行	99
設定 Identity Reporting	100
在「身分資料收集服務」頁面中手動新增資料來源	100
對 Oracle 資料庫執行報告	101
手動產生資料庫綱要	101
部署 Identity Reporting 的 REST API	105
連接遠端 Remote PostgreSQL 資料庫	105
Identity Reporting 的安裝後步驟	106
啟用 Identity Manager	106
查看 Identity Manager 元件使用的連接埠	106
 IV 在 FIPS 模式下設定 Identity Manager	 109
 5 為 FIPS 設定 JRE	 111
 6 在 FIPS 模式下設定 Identity Manager 引擎	 113
程序	113
 7 在 FIPS 模式下設定擴送代理程式	 115
程序	115
 8 在 FIPS 模式下設定 Identity Applications 和 Identity Reporting	 117
程序	117
 9 在 FIPS 模式下設定遠端載入器	 123
 V 安裝 Designer	 125
 10 規劃 Designer 安裝	 127
Designer 安裝核對清單	127
 11 安裝 Designer	 129
執行 Windows 可執行檔	129
使用靜默安裝程序	129
在除系統地區設定以外的地區設定中安裝 Designer	130
修改包含空格字元的安裝路徑	131
 VI 安裝 Analyzer	 133
 12 規劃 Analyzer 安裝	 135
Analyzer 的安裝核對清單	135

13 安裝 Analyzer	137
執行 Windows 可執行檔	137
使用靜默安裝程序	137
14 安裝後任務	139
設定已連接系統	139
建立和設定驅動程式集	139
建立驅動程式集	140
將預設密碼規則指定給驅動程式集	140
在 Identity Vault 中建立密碼規則物件	140
建立自訂密碼規則	141
在 Identity Vault 中建立預設通知集合物件	141
建立驅動程式	142
定義規則	142
管理驅動程式活動	143
啟用 Identity Manager	143
VII 升級 Identity Manager	145
15 升級 Identity Manager 的準備工作	147
Identity Manager 的升級核對清單	147
瞭解升級和移轉	148
支援的升級路徑	150
從 Identity Manager 4.7.5 版本升級	150
從 Identity Manager 4.8.x 版本升級	151
備份目前組態	153
輸出 Designer 專案	153
輸出驅動程式的組態	154
16 升級 Identity Manager 的元件	157
升級注意事項	157
升級順序	157
升級 Designer	158
升級 Identity Manager 引擎元件	159
升級 Identity Vault	159
升級 Identity Manager 引擎	160
升級遠端載入器	162
升級 Java 遠端載入器	163
升級擴送代理程式	163
升級 Identity Applications	164
瞭解升級程式	165
升級先決條件	165
系統要求	165
升級 PostgreSQL 資料庫	165
升級 Identity Applications 的驅動程式套件	167
升級 Identity Applications	167
升級後任務	169
升級 Identity Reporting	173
升級先決條件	173

升級 Identity Reporting	173
Reporting 的升級後步驟	174
變更對資料庫中 reportRunner 的參考	175
驗證 Identity Reporting 的升級	176
升級 Analyzer	176
停止和啟動 Identity Manager 驅動程式	176
停止驅動程式	176
啟動驅動程式	177
升級 Identity Manager 驅動程式	178
建立新驅動程式	179
以套件中的內容取代現有內容	179
保留目前內容並透過套件新增新內容	179
將新伺服器新增至驅動程式集	180
將新伺服器新增至驅動程式集	180
從驅動程式集移除舊的伺服器	180
將自訂規則還原至驅動程式	181
使用 Designer 將自訂規則還原至驅動程式	182
使用 Identity Console 將自訂規則和規則還原至驅動程式	182
 17 從進階版切換到標準版	183
 VIII 將 Identity Manager 資料移轉至新安裝中	185
 18 移轉 Identity Manager 的準備工作	187
用於執行移轉的核對清單	187
 19 將 Identity Manager 移轉至新伺服器	189
Identity Manager 的移轉核對清單	189
準備用於移轉的 Designer 專案	190
複製驅動程式集的伺服器特定資訊	190
在 Designer 中複製伺服器特定資訊	191
在 Identity Console 中變更伺服器特定的資訊	192
變更使用者應用程式的伺服器特定資訊	192
將 Identity Manager 引擎移轉至新伺服器	192
移轉使用者應用程式驅動程式	192
輸入新的基礎套件	193
升級現有的基礎套件	193
部署移轉的驅動程式	193
升級 Identity Applications	194
移轉 Identity Applications	194
將資料庫移轉至新伺服器	194
在新伺服器上安裝 Identity Applications	195
完成 Identity Applications 的移轉	196
準備 Oracle 資料庫以執行 SQL 檔案	196
衝洗瀏覽器快取	197
更新 SharedPagePortlet 的最大逾時設定	197
停用群組的自動查詢設定	197

IX 在 Microsoft Azure 上部署 Identity Manager	199
20 在 Microsoft Azure 上規劃和實作 Identity Manager	201
先決條件	201
部署程序	201
建立資源群組	203
建立虛擬網路和子網路	203
建立應用程式閘道	204
建立虛擬機器例項	205
更新 VM 中的主機項目	206
安裝 Designer	207
設定應用程式閘道	208
21 範例混合式 Identity Manager 方案	211
使用多伺服器驅動程式集連接	211
使用 eDirectory 驅動程式連接	212
X 部署 Identity Manager 以實現高可用性	213
22 在叢集環境中安裝 Identity Manager 的準備工作	215
先決條件	215
Identity Vault	215
Identity Applications	216
Identity Applications 的資料庫	216
為 Identity Applications 準備叢集	217
瞭解 Tomcat 環境中的叢集群組	217
設定工作流程引擎 ID 的系統內容	217
為叢集中的每個使用者應用程式使用相同的萬能金鑰	217
23 Identity Manager 叢集部署解決方案範例	219
先決條件	219
在 eDirectory 叢集上設定 NetIQ Identity Manager	219
遠端載入器叢集化	219
24 範例 Identity Applications 叢集部署解決方案	221
先決條件	222
安裝程序	223
為叢集啟用許可權索引	228
25 解除安裝 Identity Manager 的元件	229
解除安裝 Identity Vault	229
從 Identity Vault 中移除物件	230
解除安裝 Identity Manager 引擎	230
解除安裝遠端載入器	230
解除安裝 Identity Applications	231
刪除 Roles Based Provisioning Module 的驅動程式	231

解除安裝 Identity Applications	231
解除安裝 Identity Reporting 元件	232
刪除報告驅動程式	232
解除安裝 Identity Reporting	232
解除安裝 Analyzer	233
解除安裝 Designer	233

26 疑難排解 235

Identity Manager 引擎疑難排解	235
對 Identity Applications 和 RBPM 安裝進行疑難排解	236
安裝和解除安裝疑難排解	238
登入疑難排解	242
SSPR 頁面申請錯誤疑難排解	244
對在 Windows 2016 上無法啟動 .NET 遠端載入器的問題進行疑難排解	245
在 Azure 部署中載入表單時出現「502 錯誤的閘道」疑難排解	245

關於本書和文件庫

本《安裝和升級指南》提供關於安裝或更新 NetIQ Identity Manager (簡稱 Identity Manager) 產品的說明。其中介紹了在分散式環境中安裝和設定各個元件的過程。

適用對象

本書提供的資訊適用於負責為其組織建立身分管理解決方案的身分架構師和身管理員，協助他們安裝所需元件。

文件庫中的其他資訊

如需 Identity Manager 文件庫的詳細資訊，請造訪 Identity Manager 文件網站 (<https://www.netiq.com/documentation/identity-manager-49/>)。

Identity Manager 環境綜覽

本指南重點說明要安裝和設定 Identity Manager 所必須完成的任務。

如果您是 NetIQ Identity Manager 的新使用者，以下章節中的資訊將協助您熟悉該解決方案及其包括的元件。您可下載和安裝的元件取決於您的 Identity Manager 版本。

- ◆ [Identity Manager 元件簡介](#)
- ◆ [功能架構](#)

1 Identity Manager 元件簡介

我們提供了進階版和標準版 Identity Manager，以符合客戶的各種需求。每個版本包括一組特定的功能，而每項功能由多個元件處理。因此，您的 Identity Manager 實作可能包含下列一個或所有元件，具體取決於您的要求：

- ◆ Identity Manager 伺服器
- ◆ Identity Applications
- ◆ Identity Reporting
- ◆ Identity Manager 工具

圖 1-1 列出了 Identity Manager Advanced Edition 環境中部署的元件。

圖 1-1 Identity Manager Advanced Edition 的元件

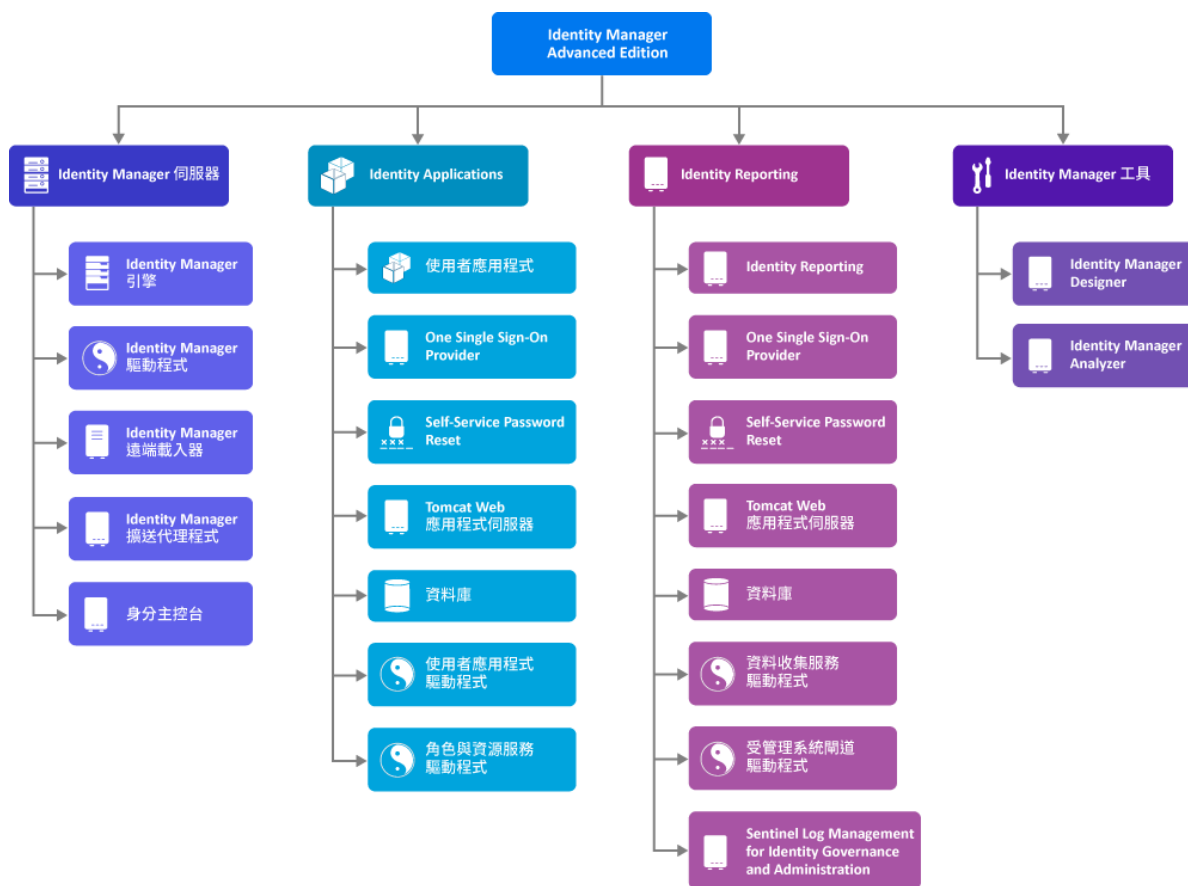
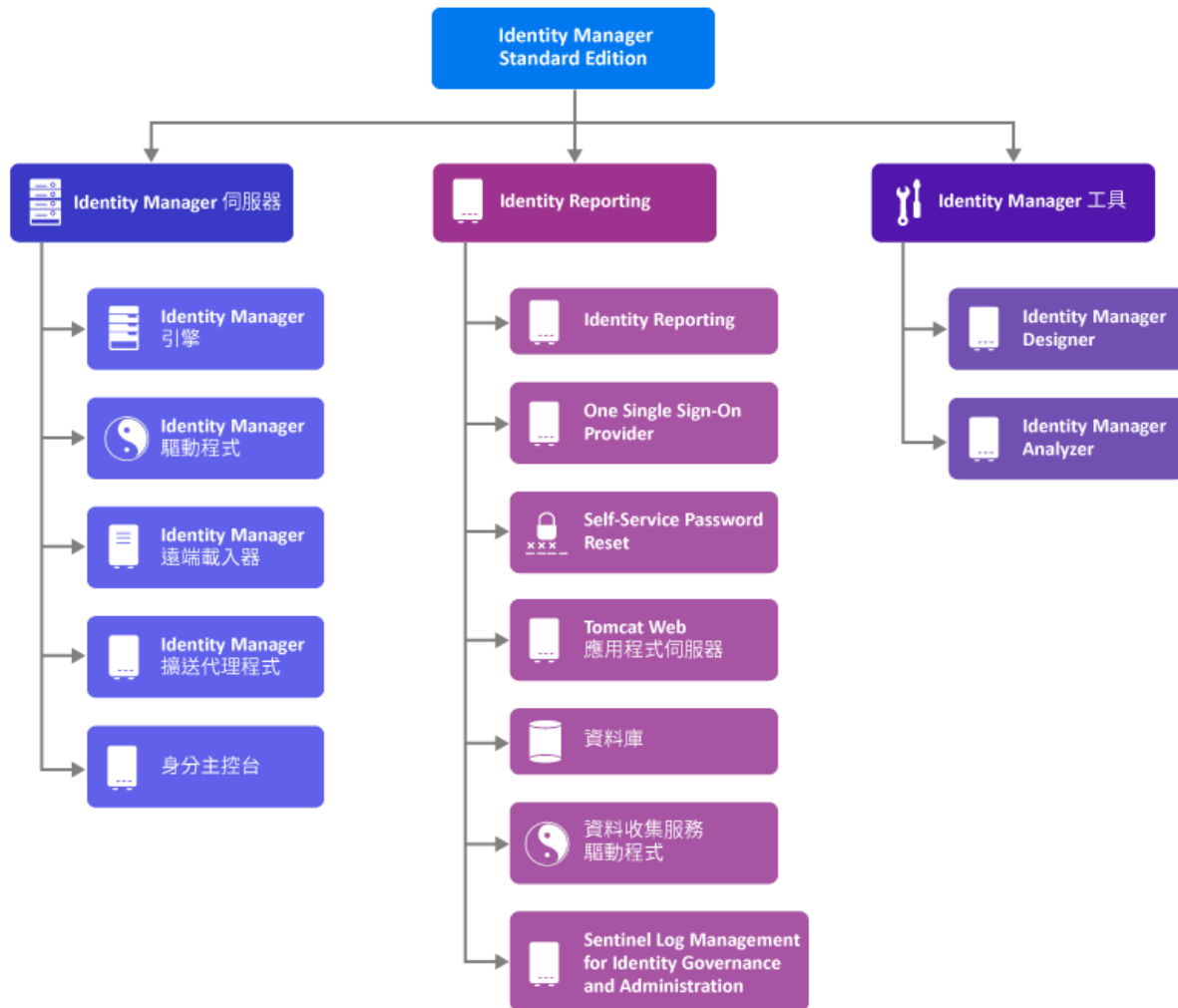


圖 1-2 列出了 Identity Manager Standard Edition 環境中部署的元件。

圖 1-2 Identity Manager Standard Edition 的元件



依據元件之間的互動模式，在邏輯上會將某些元件以一組元件的形式加以安裝。為了簡化安裝體驗，會將某些元件做為獨立的元件進行安裝。如需元件之間互動模式的資訊，請參閱《[NetIQ Identity Manager Overview and Planning Guide](#)》(NetIQ Identity Manager 綜覽和規劃指南)。

請查看後續章節中的資訊，以瞭解元件的分組方式，以及每個元件或一組元件的安裝方式。

Identity Manager 伺服器元件

所有安裝必需的元件

Identity Manager 伺服器安裝包括以下元件。

Identity Manager 伺服器

Identity Manager 伺服器負責執行 Identity Manager 內的任務。它由 Identity Vault、Identity Manager 引擎和 Identity Manager 驅動程式構成。

為了支援 Identity Manager 伺服器運作，安裝程式將安裝受支援版本的 Oracle Java Runtime Environment (JRE)。若要安裝 Identity Manager 伺服器元件，請使用安裝程式的 **Identity Manager 引擎安裝選項**。

Identity Vault

當您安裝 Identity Manager 引擎時，安裝程序會建立並設定與 Identity Vault 的連接。Identity Manager 使用 Identity Vault 做為所有身分資料的預設儲存庫。身分資料包括受管理身分 (包括使用者帳戶和組織資料) 的目前狀態。

Identity Manager 引擎

Identity Manager 引擎負責處理 Identity Vault 或連接的應用程式中發生的所有資料變更。用來執行 Identity Manager 引擎的伺服器稱為 Identity Manager 伺服器。

Identity Manager 驅動程式

Identity Manager 伺服器處理使用者的佈建，並透過驅動程式管理已連接系統的帳戶和群組。驅動程式是已連接系統的軟體介面。

Identity Manager 驅動程式做為 Identity Manager 伺服器架構的一部分執行。驅動程式充當原生端點類型系統技術的閘道。例如，僅當已在 Identity Manager 伺服器或者可與 Identity Manager 伺服器通訊的目標應用程式伺服器上安裝了 Active Directory 驅動程式時，才能管理執行 Active Directory 服務的電腦。驅動程式會管理位於已連接系統上的物件。受管理物件包括帳戶、群組和特定於端點類型的物件 (選擇性)。

驅動程式會將 Identity Manager 引擎動作轉譯為已連接系統上的變更，例如「在 Microsoft Exchange 已連接系統上建立新電子郵件帳戶」。在 Identity Manager 中設定的每個驅動程式都有一個關聯的事件快取檔案 (TAO 檔案)。在驅動程式處理事件之前，系統會在該快取檔案中快取這些事件。快取檔案預設存放在 Identity Vault 的 DIB (資料資訊庫) 目錄中。

Identity Manager 提供數個內建驅動程式 (Java、原生、.NET) 來管理與不同類型的已連接系統之間的連接。Identity Manager 還提供開發自訂驅動程式的功能，以使資料能夠同步到其他各種系統，例如，組織內部開發的應用程式，或者沒有技術介面，因而無法利用現成驅動程式的儲存庫。

遠端載入器

可以在 Identity Manager 伺服器本地安裝驅動程式，也可以使用遠端載入器來安裝。遠端載入器可載入驅動程式，並代表遠端伺服器上安裝的驅動程式與 Identity Manager 引擎通訊。如果應用程式與 Identity Manager 引擎在同一個伺服器上執行，您便可以將驅動程式安裝在該伺服器上。但是，如果應用程式與 Identity Manager 引擎不在同一個伺服器上執行，您必須將驅動

程式安裝在應用程式所在的伺服器上。若要改善您環境的工作負載或組態，可以將遠端載入器安裝在單獨的伺服器上，不要將其與 Tomcat 和 Identity Manager 伺服器安裝在同一部伺服器上。如需遠端載入器的詳細資訊，請參閱《[NetIQ Identity Manager Driver Administration Guide](#)》(NetIQ Identity Manager 驅動程式管理指南) 中的「[Determining When to Use the Remote Loader](#)」(確定何時使用遠端載入器)。

使用 Identity Manager 遠端載入器伺服器安裝選項可在遠端載入器中安裝遠端載入器服務和驅動程式例項。

擴送代理程式

Identity Manager 擴送代理程式是 Java Database Connectivity (JDBC) 擴送驅動程式用來建立多個 JDBC 擴送驅動程式例項的安裝元件。使用擴送驅動程式可以十分輕鬆地為多個資料庫佈建使用者、群組和密碼。有了此驅動程式，Identity Manager 管理員就不必再使用相同的規則設定多個 JDBC 驅動程式來佈建多個相同類型的資料庫。您可以集中管理使用者帳戶，並在適當的情況下自動建立、設定、維護和移除這些帳戶。如需詳細資訊，請參閱《[NetIQ Identity Manager Driver for JDBC Fanout Implementation Guide](#)》(NetIQ Identity Manager Driver for JDBC FanOut 實作指南) (https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/netiq-identity-manager-for-jdbc-fan-out-driver-implementation-guide.html)。

若要安裝擴送代理程式，請使用安裝程式的 Identity Manager 擴送代理程式安裝選項。

Identity Console

Identity Console 取代了 iManager。

NetIQ Identity Console 是 Web 式管理主控台，有了它，使用者可隨時隨地透過網際網路和網頁瀏覽器，以虛擬、安全的自訂方式存取網路管理公用程式。Identity Console 可讓系統管理任務的分權化更為容易。

使用 Identity Console，您可以執行使用 Designer 可執行的類似任務，還可以監控系統的狀態。NetIQ 建議您使用 Identity Console 來執行管理任務。請使用 Designer 來執行需要對套件進行變更的組態任務、塑模和部署前測試。

如需 Identity Console 的詳細資訊，請參閱《[Identity Console Administration Guide](#)》(Identity Console 管理指南)。

Identity Applications 元件

進階版安裝必需的元件

Identity Applications 指一組基於瀏覽器的互連 Web 應用程式。它們可讓貴組織管理使用者帳戶以及與提供給使用者的各種角色和資源關聯的許可權。您可以設定 Identity Applications，以便為您的使用者提供自助服務支援，例如申請角色或變更他們的密碼。您還可以設定工作流程，以提高管理和指定角色與資源的效率。Identity Applications 由可協助您執行這些任務的管理主控台 (用於執行管理任務)、使用者主控台 (儀表板) 和 REST 服務組成。

附註：只有在安裝 Identity Manager 引擎之後，才能安裝 Identity Applications。

若要安裝 Identity Applications 元件，請使用安裝程式的 **Identity Applications** 安裝選項。

Identity Applications 安裝包括以下元件：

使用者應用程式

使用者應用程式是基於瀏覽器的 Web 應用程式，可讓使用者執行各種身分自助服務和角色佈建任務。在本產品的舊版本中使用使用者應用程式介面執行的部分任務已轉移至新使用者介面，新介面包括管理主控台和使用者主控台。使用者應用程式將繼續提供新使用者介面中尚不存在的一些功能。如需詳細資訊，請參閱《[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)》(NetIQ Identity Manager - Identity Applications 管理員指南)。

驗證服務

驗證服務提供了存取 Identity Applications 功能的通道。如需在 Identity Manager 中使用單一登入存取的詳細資訊，請參閱《[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)》(NetIQ Identity Manager - Identity Applications 管理員指南)。

NetIQ One Single Sign-On Provider (OSP) 元件會提供驗證服務。Identity Applications 要求在本機安裝 OSP。OSP 將隨 Identity Applications 一併自動安裝。

Self-Service Password Reset

自助密碼管理服務可讓使用者存取自助密碼管理功能。Identity Applications 中包含 NetIQ Self Service Password Reset (SSPR)，可協助能夠存取 Identity Applications 的使用者重設其密碼，而無需管理人員介入。

Identity Applications 安裝程序預設會啟用 SSPR。但是，如果您的部署需要 SSPR，或者您要安裝標準版，您可以選擇在單獨的電腦上安裝 SSPR。如果在進階版中將 SSPR 安裝到單獨的電腦上，您必須在完成這兩個元件的安裝之後，以手動方式或使用 ConfigUpdate 公用程式在 Identity Applications 組態檔案 (ism-configuration.properties) 中定義密碼管理設定。

Web 應用程式伺服器

該應用程式伺服器提供用於執行 Identity Applications 元件的執行時期架構。Identity Applications 會封裝成 WAR (Web 應用程式資源或 Web 應用程式歸檔) 檔案。安裝程序允許您將 WAR 檔案部署到應用程式伺服器。應用程式伺服器執行 Java™ 虛擬機器，用於為應用程式程式碼提供執行時期環境。以下 WAR 檔案適用於 Identity Applications 元件的 URL：

- ◆ **IDMProv** (用於使用者應用程式介面)
- ◆ **idmdash** (用於儀表板)
- ◆ **idmadmin** (用於 Identity Applications 管理介面)

當某個使用者與 `idmdash` 或 `idmadmin` 應用程式互動時，這些應用程式將查詢基礎 `IDMProv.war` 檔案，並擷取該使用者的資訊。`IDMProv.war` 會公開 REST 和 SOAP API，這些 API 的 `idmdash` 和 `idmadmin` 包含提供使用者介面的資訊。

Identity Applications 在安裝套件中隨附的 **Apache Tomcat** 應用程式伺服器上執行。為支援 **Tomcat** 應用程式伺服器，安裝程式將安裝受支援版本的 **JRE** 和 **Apache ActiveMQ**。

Identity Applications 資料庫

Identity Applications 資料庫會維護 **Identity Applications** 的組態資料，例如當地語系化的標籤、授權值和電子郵件伺服器組態。它還會儲存工作流程引擎所需的工作流程狀態資料。**Identity Applications** 支援的資料庫包括 **PostgreSQL**、**Oracle** 和 **Microsoft SQL Server**。

Identity Applications 安裝程式會自動安裝受支援版本的 **PostgreSQL** 資料庫，該資料庫做為 **Identity Applications** 的預設資料庫。如果您不想使用 **PostgreSQL** 資料庫，可以為 **Identity Applications** 設定受支援版本的 **Oracle** 或 **MS SQL** 資料庫。**Identity Applications** 需要使用 **Java Database Connectivity** 驅動程式 (**JDBC** 類型 4 驅動程式) 來與資料庫通訊。安裝程式會提示您提供資料庫 **JDBC** 驅動程式的位置和名稱。因此，在開始安裝 **Identity Applications** 之前，必須從資料庫安裝目錄獲取此 **JDBC** 驅動程式。

- 對於 **PostgreSQL** 資料庫，**Identity Manager** 安裝程式中已隨附該驅動程式。
- 對於 **Oracle** 資料庫，您可以從 [Oracle 網站](#) 下載該驅動程式。
- 對於 **Microsoft SQL Server** 資料庫，可以從 [Microsoft 網站](#) 下載該驅動程式。

資料庫可以位於 **Identity Applications** 伺服器本地，也可以位於遠端電腦上。使用遠端資料庫時，必須設定與該資料庫的連接。

Identity Applications 的驅動程式

Identity Applications 元件需要以下驅動程式：

使用者應用程式驅動程式

儲存組態資訊，並在 **Identity Vault** 中發生變更時立即通知 **Identity Applications**。您可以設定驅動程式，以允許 **Identity Vault** 中的事件觸發工作流程。該驅動程式還可以向使用者應用程式報告工作流程的佈建活動是成功還是失敗，以便使用者可以檢視其申請的最終狀態。

角色與資源服務驅動程式

管理所有角色指定、為需要核准的角色指定申請啟動相應工作流程，以及依據群組和容器成員資格維護間接角色指定。該驅動程式會依據使用者的角色成員資格為其授予和撤銷授權，以及執行已完成申請的清理程序。該驅動程式除了維護角色申請外，還可維護資源申請。

安裝程式的 **Identity Applications** 安裝選項會將使用者應用程式驅動程式以及角色與資源服務驅動程式部署到 **Identity Vault**。

Identity Reporting 元件

(選擇性) 僅當您計畫實作報告功能時，才需安裝此元件

Identity Reporting 可讓您全面瞭解使用者的授權，並會提供所需資訊供您瞭解授予組織中各身分的授權和許可權的過去和目前狀態。Identity Manager 提供了預先定義的報告，供您監控 Identity Manager 環境的狀態，包括從 Identity Vault 和已連接系統收集的資訊。若要將提供的報告與 Identity Manager 配合使用，需安裝 Identity Manager 隨附的 Identity Reporting。Identity Reporting 還提供了一個報告封裝工具，可簡化自訂報告的建立過程。Identity Reporting 的使用者介面便於您將報告排程在非高峰時間執行，從而實現效能最佳化。如需 Identity Reporting 的詳細資訊，請參閱《[Administrator Guide to NetIQ Identity Reporting](#)》(NetIQ Identity Reporting 管理員指南)。

附註：在進階版中安裝 Identity Reporting 之前，必須先安裝 Identity Applications。

Identity Reporting 安裝包括以下元件：

Identity Reporting

基於瀏覽器的應用程式，用於透過呼叫報告服務來產生報告。報告服務將從 Identity Reporting 儲存庫 (身分資訊倉儲) 中擷取產生報告所需的資料。Identity Reporting 儲存庫中包含所有報告管理資訊 (例如報告定義和排程)、資料庫檢視及報告所需的組態資訊。

驗證服務

OSP 元件負責提供驗證服務。如需詳細資訊，請參閱「[驗證服務](#)」(第 19 頁)。

附註：OSP 將隨 Identity Reporting 一併自動安裝。但是，在進階版安裝中，Identity Reporting 可以使用隨 Identity Applications 一併安裝的同一驗證服務。使用同一驗證服務時，必須在 Identity Reporting 組態期間指定驗證設定。

Self-Service Password Reset

自助密碼管理服務可讓使用者存取自助密碼管理功能。如需詳細資訊，請參閱「[Self-Service Password Reset](#)」(第 19 頁)。

Identity Reporting 資料庫

Identity Reporting 資料庫 (身分資訊倉儲) 用於儲存組織中 Identity Vault 與已連接系統的實際和預期狀態相關資訊。您可以依據這些資訊產生報告，以檢視使用者和角色等物件之間的關係。該資料庫可以位於 Identity Reporting 伺服器本地，也可以位於遠端電腦上。Identity Manager 使用資料來源連接至資料庫。Identity Reporting 需要使用 Java Database Connectivity

驅動程式 (JDBC 類型 4 驅動程式) 來與資料庫通訊。JDBC 驅動程式使 Identity Reporting 伺服器能夠與資料來源通訊。Identity Reporting 支援的資料庫有 PostgreSQL、Oracle 和 Microsoft SQL。

- 對於 PostgreSQL 資料庫，Identity Manager 安裝程式中已隨附此驅動程式。
- 對於 Oracle 資料庫，您可以從 [Oracle 網站](#) 下載該驅動程式。
- 對於 Microsoft SQL Server 資料庫，可以從 [Microsoft 網站](#) 下載該驅動程式。

附註：只有在安裝 Identity Manager 伺服器之後，才能安裝 Identity Reporting 元件。

Web 應用程式伺服器

該應用程式伺服器提供用於執行 Identity Reporting 元件的執行時期架構。以下 WAR 檔案適用於 Identity Reporting 元件的 URL：

- **IDMRPT** (用於 Identity Reporting 應用程式 / 介面)
- **idmdcs** (用於 Identity Manager 資料收集服務)

當某個使用者與 IDMRPT 或 idmdcs 應用程式互動時，這些應用程式將查詢報告服務，並擷取該使用者的資訊。報告服務會公開 REST API，這些 API 中的 IDMRPT 和 idmdcs 包含提供使用者介面的資訊。

如需 Web 應用程式伺服器的詳細資訊，請參閱「[Web 應用程式伺服器](#)」(第 19 頁)。

Identity Reporting 的驅動程式

Identity Reporting 元件需要以下驅動程式：

受管理系統閘道驅動程式

可查詢 Identity Vault 以從受管理系統收集下列類型的資訊：

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

資料收集服務驅動程式

資料收集服務使用資料收集服務驅動程式來擷取對儲存在 Identity Vault 中的物件 (例如帳戶、角色、資源、群組和團隊成員資格) 所做的變更。驅動程式會向該服務註冊自身，並將變更事件 (例如資料同步、新增、修改及刪除事件) 推送至該服務。

該服務包括三個子服務：

- **報告資料收集器：**使用提取設計模型從一或多個 Identity Vault 資料來源擷取資料。收集動作會定期執行，具體時間由一組組態參數決定。為了擷取資料，收集器會呼叫受管理系統閘道驅動程式。

- ◆ **事件驅動的資料收集器**：使用提取設計模型收集資料收集服務驅動程式擷取的事件資料。
- ◆ **非受管理應用程式資料收集器**：透過呼叫專為每個應用程式撰寫的 REST 端點，從一或多個非受管理應用程式擷取資料。非受管理應用程式是指企業內未連接至 Identity Vault 的應用程式。

安裝程序的 **Identity Reporting** 安裝選項會將受管理系統閘道驅動程式和資料收集服務驅動程式部署到 Identity Vault。

Sentinel Log Management for Identity Governance and Administration

Sentinel Log Management for Identity Governance and Administration (IGA) 是安全性資訊與事件管理 (SIEM) 系統，可接收來自整個企業中眾多來源的資訊，並將這些資訊標準化、設定它們的優先程度，然後將其提供給您以便制定與威脅、風險和規則相關的決策。Sentinel Log Management for IGA 可擷取與數個 NetIQ 產品 (包括 Identity Reporting、Identity Applications 和 Identity Vault) 中執行的動作關聯的記錄事件。這些事件儲存在 Identity Reporting 儲存庫 (身分資訊倉儲) 內的公用綱要中。

Identity Manager 提供單獨的 Sentinel Log Management for IGA 安裝程式 (SentinelLogManagementForIGA8.2.2.0.tar.gz)。

Identity Manager 工具

所有安裝必需的元件

Identity Manager 中包含一組用於簡化解決方案實作、自訂和維護的管理工具。其中的一些工具將隨 Identity Manager 一併安裝，而有些則需要單獨安裝。

Designer for Identity Manager

Designer for Identity Manager (Designer) 可協助您在網路或測試環境中設計、測試、記錄和部署 Identity Manager 解決方案。您可以在離線環境中設定 Identity Manager 專案，然後再將其部署到線上系統。從設計角度而言，Designer 可協助執行下列工作：

- ◆ 以圖形方式檢視構成 Identity Manager 解決方案的所有元件，並觀察它們如何互動。
- ◆ 修改並測試 Identity Manager 環境，確保它的表現符合預期，然後再將部分或整個測試解決方案部署到線上環境。

Designer 會追蹤設計及配置資訊。您只需按一下按鈕，即可用選定的格式列印該資訊。Designer 還允許團隊共享針對企業層級專案執行的工作。

Identity Manager 提供單獨的 Designer 安裝程式。

Analyzer for Identity Manager

Analyzer for Identity Manager (Analyzer) 提供資料分析、清理、重整和報告，以協助您遵守內部資料品質規則。Analyzer 可讓您分析、增強及控制企業中的所有資料儲存。Analyzer 包含下列功能：

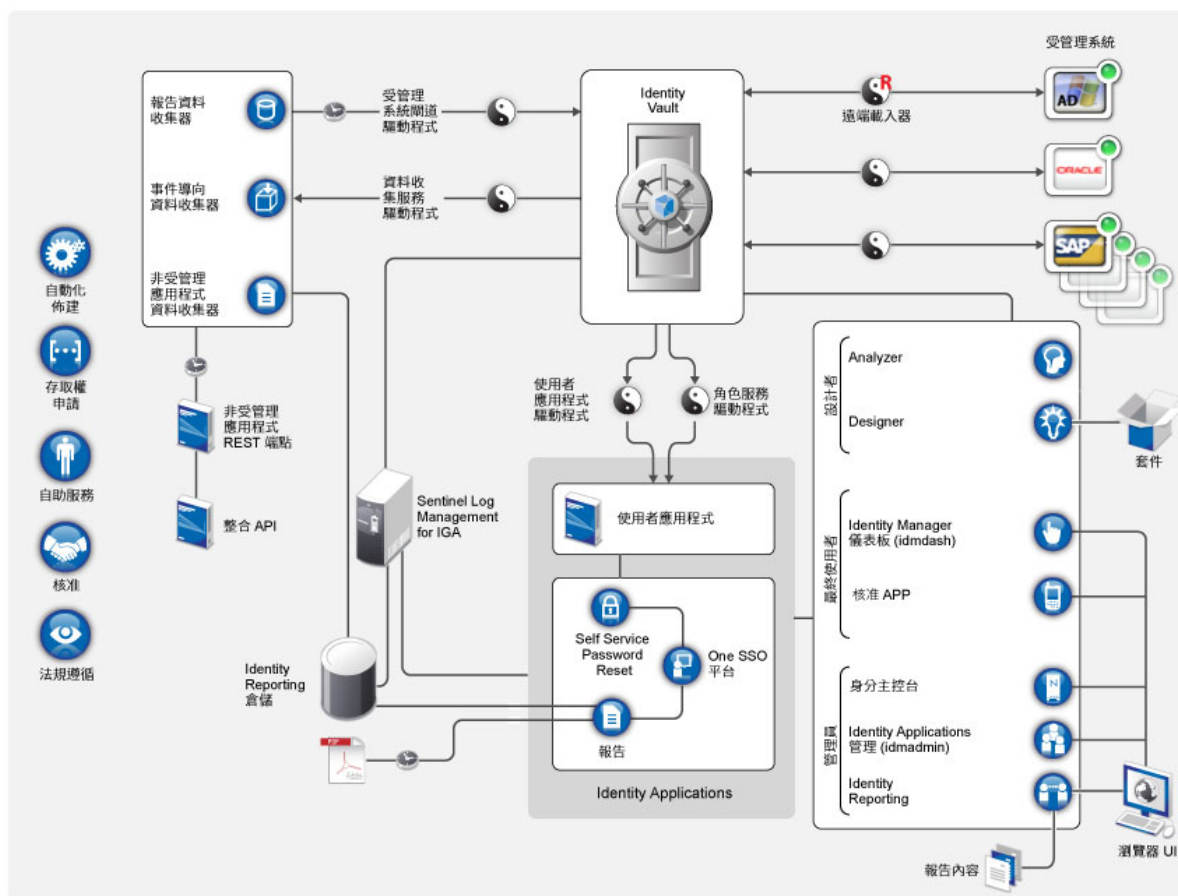
- ◆ Analyzer 的綱要對應可使應用程式的綱要屬性與 Analyzer 基礎綱要中的對應綱要屬性相關聯。這可讓您確保您的資料分析和清理操作在不同系統之間正確關聯類似的值。為此，Analyzer 利用了 Designer 中的綱要對應功能。
- ◆ 分析設定檔編輯器可讓您設定用於分析一或多個資料集例項的設定檔。每個分析設定檔包含一或多個測量標準，您可以依據這些測量標準來評估屬性值，以確定資料符合您所定義之資料格式標準的程度。
- ◆ 比對設定檔編輯器可讓您比較一或多個資料集中的值。您可以檢查指定的資料集中是否有重複的值，以及兩個資料集之間是否有相符的值。

Identity Manager 提供單獨的 Analyzer 安裝程式。

重要：Identity Manager 4.9 ISO 中不包含 Analyzer 工具。如果已安裝 Analyzer，請務必將其更新至版本 4.8.5，並與 Identity Manager 4.9 配合使用。

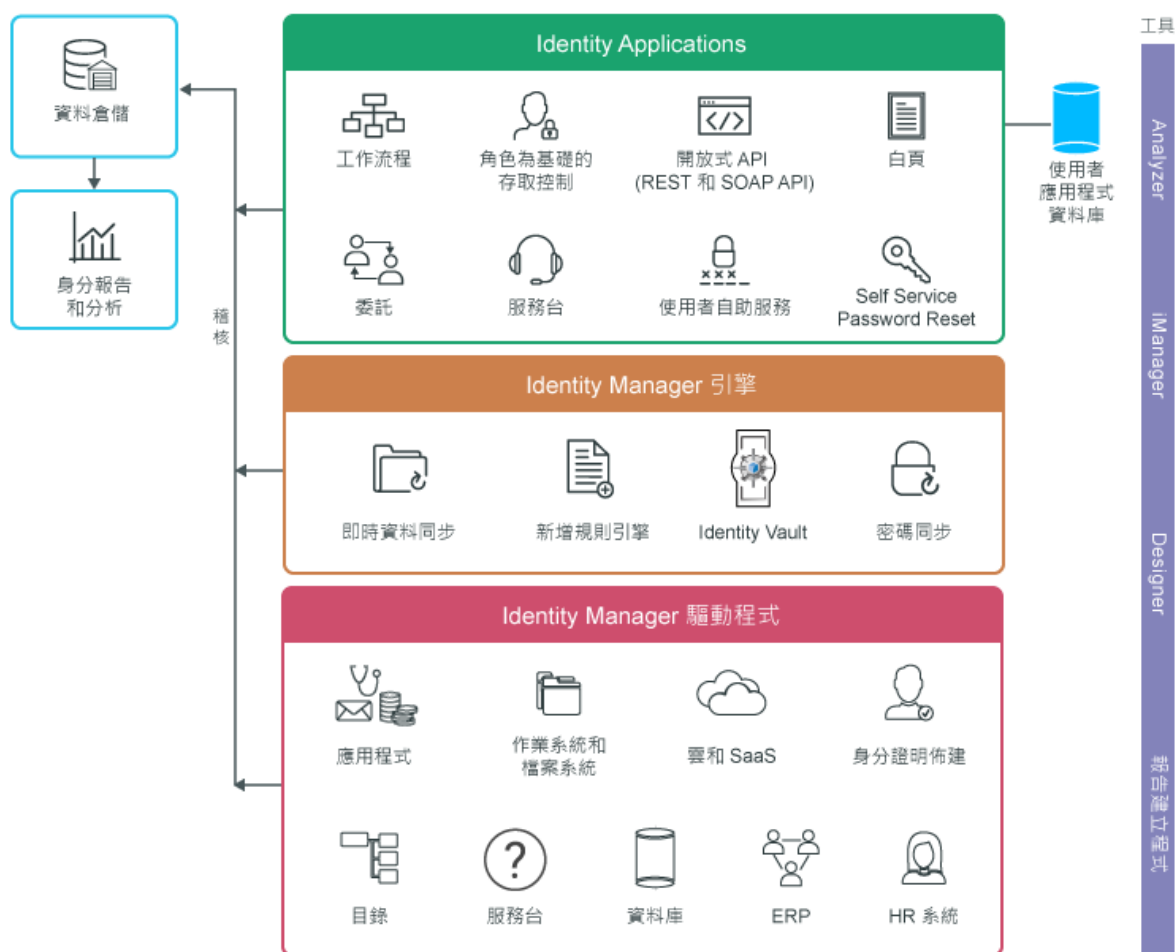
瞭解 Identity Manager 不同元件的用途及安裝方式後，請參閱圖 1-3 以瞭解元件之間的互動模式。

圖 1-3 Identity Manager 元件之間的互動



功能架構

下圖顯示了 Identity Manager 元件的基本功能架構。此插圖並未涵蓋所有可能的整合。



如需可能的部署案例資訊，請參閱 [Identity Manager 的部署選項](#)。

Identity Manager 的部署選項

請查閱下表來規劃 Identity Manager 解決方案的實體環境。這些部署使用案例概述了 Identity Management 實體架構，以及元件產品的連接方式、互相通訊及與其他產品通訊的方式。如需 Identity Management 功能架構和元件的簡要綜覽，請參閱「[功能架構](#)」(第 25 頁)。

部署選項	總結
一部電腦上的單伺服器組態	最基本的部署組態包括在一部電腦上安裝的 Identity Manager 伺服器以及其他必需的應用程式。您必須確定該電腦具有所需的記憶體、速度和可用磁碟空間，以符合工作負載的要求。這是基本的部署使用案例，基本上只適合用於概念證明 (POC) 和演示目的，可能不適合用於生產環境。

部署選項	總結
分散式伺服器組態	這種部署包括在一部電腦上安裝的 Identity Manager 伺服器，以及在其其他一或多部電腦上安裝的所有其他必需的應用程式。例如， Identity Applications 、 OSP 和 SSPR 等元件可在單獨的電腦上執行。您可以提供一部額外的電腦來代管報告服務的元件，以符合執行 Sentinel Log Management for IGA 元件的系統要求。
高可用性部署	高可用性是一種備援運作模式。當主要伺服器發生故障或者需要維護而暫時關閉時，高可用性功能可以自動切換到待命伺服器。Identity Manager 支援在高可用性環境中安裝以下元件： ◆ Identity Vault ◆ Identity Manager 引擎 ◆ 遠端載入器 ◆ Identity Applications，不包括 Identity Reporting 一般的叢集組態包含代管 Identity Applications 以便實現負載平衡和容錯的 Tomcat 應用程式伺服器節點。所有通訊都透過負載平衡器路由。所有節點均與同一個 Identity Vault 和 Identity Applications 資料庫例項通訊。此組態可擴充。您可以輕鬆增加節點來處理負載。

範例 Identity Manager 部署

Identity Manager 允許您控制使用者身分以及他們對已連接系統上的應用程式和帳戶的存取權。請依據所需的功能，選取要安裝的 **Identity Manager** 版本，而這又決定了要安裝的元件。下表列出了 **Identity Manager Advanced Edition** 和 **Identity Manager Standard Edition** 提供的功能。

特性	進階版	標準版	要安裝的元件
基於規則的自動化使用者佈建	✓	✓	Identity Manager 引擎 和 Designer
即時身分同步	✓	✓	Identity Manager 引擎 和 Designer
密碼管理與密碼自助服務	✓	✓	Identity Manager 引擎 和 SSPR
統一身分資訊工具 (Analyzer)	✓	✓	Analyzer
REST API 和單一登入支援	✓	✓ (僅提供受限制的支援)	Identity Manager 引擎 、 OSP 和 Identity Reporting
目前狀態報告	✓	✓	Identity Manager 引擎 和 Identity Reporting

特性	進階版	標準版	要安裝的元件
基於角色的企業級佈建	✓	✗	Identity Manager 引擎和 Identity Applications
業務規則執行的自動化核准工作流程	✓	✗	Identity Manager 引擎、Designer 和 Identity Applications
Identity Applications 中的進階自助服務	✓	✗	Identity Manager 引擎和 Identity Applications
資源模型和目錄方便資源佈建	✓	✗	Identity Manager 引擎和 Identity Applications
歷程狀態報告	✓	✗	Identity Manager 引擎和 Identity Reporting
已連接系統報告	✓	✗	Identity Manager 引擎和 Identity Reporting
角色和資源管理	✓	✗	Identity Manager 引擎和 Identity Applications

附註：在所有 Identity Manager 安裝中，Identity Manager 伺服器是一個中心元件。根據所選的 Identity Manager 版本，將會在 Tomcat 應用程式伺服器上僅安裝 Identity Reporting，或同時安裝 Identity Reporting 和 Identity Applications。請視需要使用 Identity Manager 元件的專用安裝程式來安裝其他元件。例如，安裝 Designer、Analyzer 或 Sentinel Log Management for Identity Governance and Administration。

此外，在安裝 Identity Manager 之前，請查看實作的目標，並注意實體拓撲選項，例如高可用性和延展性。這有助於確定與貴組織要求相符的組態。

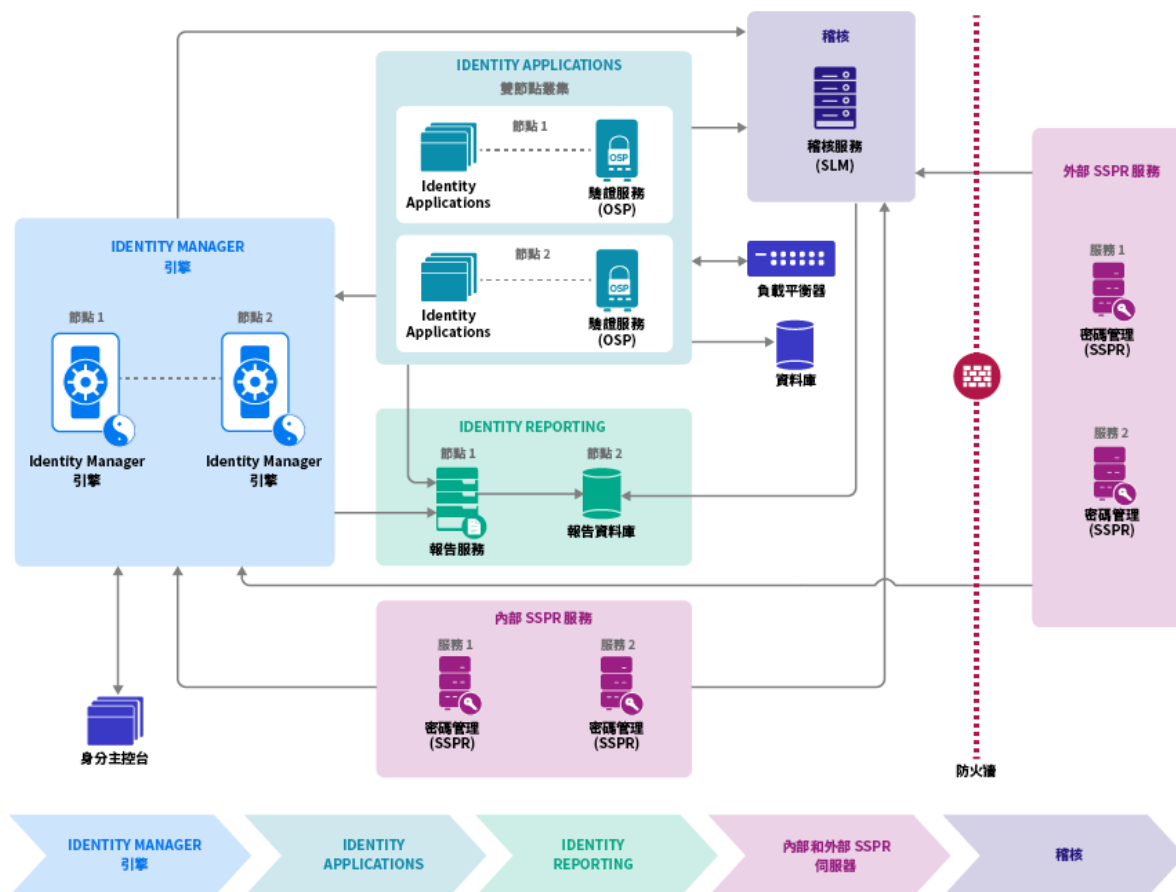
高可用性可確保關鍵網路資源 (包括資料、應用程式和服務) 的高效可管理性。您可以透過減少任何單一故障點及使用備援元件來實作高可用性。同樣地，將 Identity Management 元件的多個例項連接至負載平衡器也可以提供高度可用的環境。

本節透過兩個範例概要說明進階版和標準版的實作。您可以參考這些範例來設計實作的部署圖。

範例進階版部署

圖 1-4 顯示了 Identity Manager Advanced Edition 安裝的高階部署拓撲。

圖 1-4 範例進階版部署



- Identity Manager 伺服器元件及其基礎儲存庫 (Identity Vault) 和支援 Web 的元件 (Identity Applications 和 Identity Reporting) 安裝在內部網路區域中。負載平衡器將流量路由到 Identity Applications 元件。這種部署可提供增強的安全性，因為防火牆會將這些元件與國際網路流量隔離。
- Identity Manager 伺服器元件設定為使用雙伺服器 (主要 / 次要) 組態。做為主要節點 (使用中) 的主要伺服器上有一個使用中的虛擬邏輯 IP 位址，另一部伺服器做為次要節點。如果主要伺服器發生故障，該邏輯 IP 位址將轉移到次要伺服器。然後，所有程序都將在次要伺服器上啟動。轉移邏輯 IP 位址後，存取次要伺服器的應用程式程序可能會遇到暫時性的服務中斷，而所有其他程序都會啟動。在任意時間點，所有元件都使用同一部 Identity Vault 伺服器。
- 防火牆的內部和外部都會提供 SSPR 服務，用於解決組織的本地和行動使用者的密碼管理需求。在防火牆內部安裝的服務可解決本地密碼管理需求。如果忘記了密碼，行動工作人員將無法存取 VPN，這可以防止他們存取在內部部署的 SSPR 服務。他們可以直接存取防火牆外部部署的 SSPR 服務來管理自己的密碼。
- 使用者應用程式和驗證服務 (OSP) 部署在叢集中，用於處理負載和支援 Identity Applications 的容錯移轉程序。叢集節點連接至在單獨的電腦上安裝的同一個 Identity Applications 資料庫。這種部署允許您將更多節點新增至叢集，因而提供了更高的延展性。叢集組態會立即傳送到新增的節點。負載平衡器通常是叢集的一部分。它瞭解叢集組態及容錯移轉規則。在此組態中，所有叢集節點在任意時間點均處於使用中狀態。負

載平衡器會將負載分散到各個節點，以確保每個節點的工作負載大致相同。如果某個節點失敗，對該節點發出的申請將轉移到叢集中倖存的節點。由於此安裝是一種站點內高可用性解決方案，因此可在發生本地硬體和軟體故障時提供保護，並使用基於雙節點硬體的叢集來實現 Identity Applications 元件的高可用性。

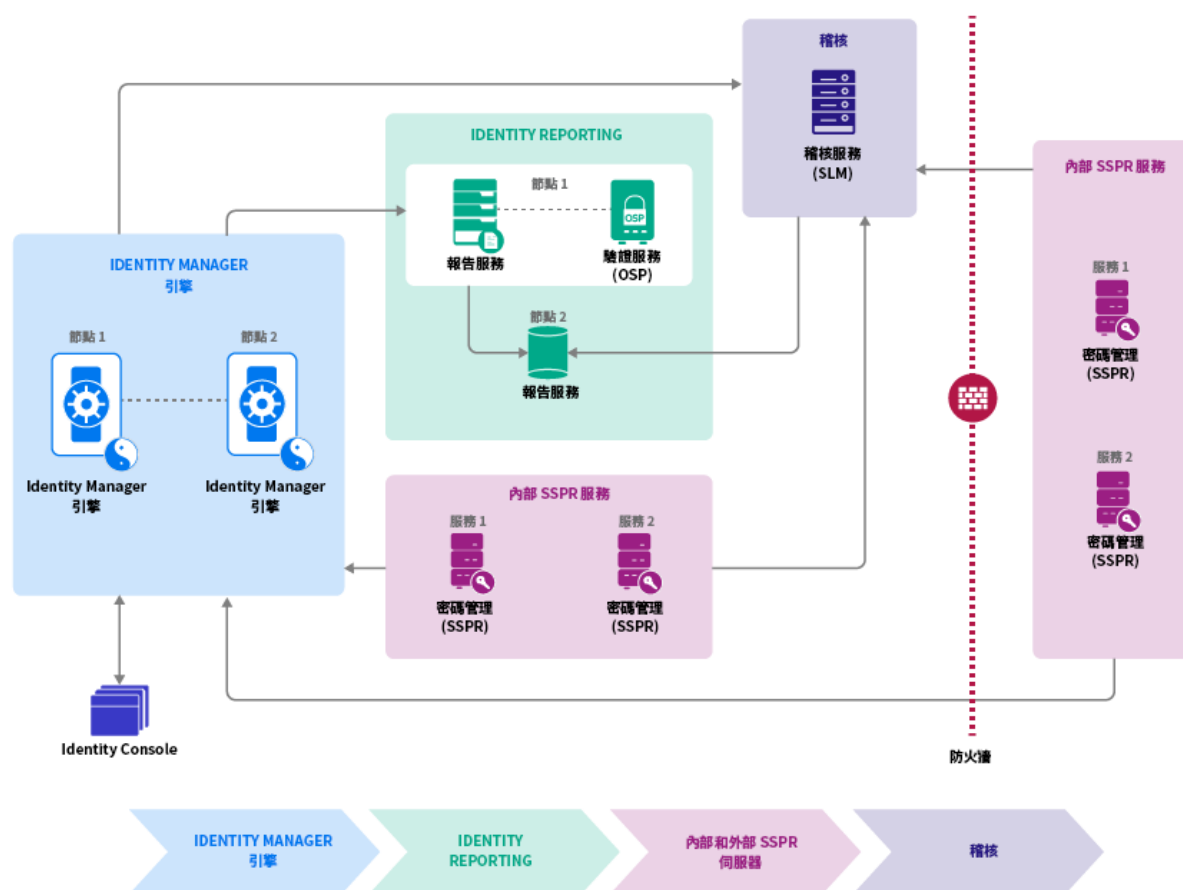
NetIQ 已對此組態進行測試，並建議使用此組態。

附註：Identity Manager 不支援將 Identity Manager 元件叢集化。

範例標準版部署

在生產部署中，安全性規則可能會規定不能向公用網路公開用於為您的環境提供進階驗證和保護的驗證服務。圖 1-5 顯示了 Identity Manager Standard Edition 安裝的高階部署拓撲。

圖 1-5 範例標準版部署



- Identity Manager 伺服器元件及其基礎儲存庫 (Identity Vault) 和 Identity Reporting 元件安裝在內部網路區域中。網際網路 Web 流量透過在防火牆後面安裝的 Web 伺服器路由到 Identity Reporting 元件，以增強保護。這種部署可提供增強的安全性，因為防火牆會將這些元件與網際網路流量隔離。

- ◆ **Identity Manager** 伺服器元件設定為使用雙伺服器 (主要 / 次要) 組態。做為使用中節點的主要伺服器上有一個使用中的虛擬邏輯 IP 位址，另一部伺服器做為次要節點。如果主要伺服器發生故障，該邏輯 IP 位址將轉移到次要伺服器。然後，所有程序都將在次要伺服器上啟動。轉移邏輯 IP 位址後，存取次要伺服器的應用程式程序可能會遇到暫時性的服務中斷，而所有其他程序都會啟動。在任意時間點，所有元件都使用同一部 **Identity Vault** 伺服器。
- ◆ 防火牆的內部和外部都會提供 **SSPR** 服務，用於解決組織的本地和行動使用者的密碼管理需求。在防火牆內部安裝的服務可解決本地密碼管理需求。如果忘記了密碼，行動工作人員將無法存取 **VPN**，這可以防止他們存取在內部部署的 **SSPR** 服務。他們可以直接存取防火牆外部部署的 **SSPR** 服務來管理自己的密碼。

NetIQ 已對此組態進行測試，並建議使用此組態。

附註：Identity Manager 不支援將 Identity Manager 元件叢集化。



規劃 Identity Manager 安裝

依據您希望 Identity Manager 如何管理使用者，以及您需要使用哪些功能來實現業務目標，對您的 Identity Manager 實作進行規劃。考慮以下要點可協助您做出決策：

- ◆ 我要如何管理身分。
- ◆ 我是否需要自動佈建。
- ◆ 我應使用工作流程實作哪些業務要求。

您做出的決策將會確定依您的要求實作 Identity Manager 的最佳方式。

在大型企業中部署 Identity Manager 之前，需要規劃一些額外的任務。如需詳細資訊，請參閱《[NetIQ Identity Manager Overview and Planning Guide](#)》(NetIQ Identity Manager 綜覽和規劃指南) 中的「[Planning](#)」(規劃)一節。

2 規劃安裝

下表列出了要支援您要實作的功能所需安裝的元件。如需安裝這些元件的說明，請參閱「安裝」一節。

功能	要安裝的元件
管理企業目錄中的使用者身分	Identity Manager 伺服器
佈建已連接系統中的帳戶	Identity Manager 伺服器 Identity Applications 使用者應用程式驅動程式 角色與資源服務驅動程式 Designer
驗證	附註：如需安裝 Identity Manager 驅動程式的說明，請參閱 Identity Manager 驅動程式文件 網站上適用於您要安裝的驅動程式類型的驅動程式實作指南。 Identity Manager 伺服器
密碼管理	One Single Sign-On Provider Identity Manager 伺服器 Self Service Password Management
產生有關 Identity Manager 活動的報告	Identity Manager 伺服器 Identity Reporting One Single Sign-On Provider

確定硬體要求

Identity Manager 安裝所需的硬體取決於兩個因素：

- ◆ 要實作的功能
- ◆ 部署規模

以下部署類型可協助您預估部署的規模。

部署類型	硬體要求
概念證明 (演示)	單伺服器部署，用於在開發環境中進行演示或基本測試。

部署類型	硬體要求
基本	適合中小規模實作的多伺服器實作。 此類實作需要使用一部伺服器來執行 Identity Manager 伺服器及其元件，並使用另外兩部伺服器來執行 Identity Applications 和 Identity Reporting 元件。
中介	適合中等規模實作的高可用性實作。
大型企業	高可用性實作，包括用於提供容錯移轉功能的 Identity Manager 引擎叢集，以及用於支援單一登入存取 (Windows 上的 OSP)、負載平衡和容錯的另一個 Identity Applications 與驗證服務叢集。

部署規劃工作表

使用本主題中的資訊可瞭解新的 **Identity Manager** 實作的詳細資料。

表格 2-1 規劃工作表

規劃活動	工作表
設計部署架構。列出支援環境所需的實體電腦 / 伺服器和其他系統的數量	架構工作表
確定您的系統符合系統要求	系統要求工作表
查看網路連接埠，以確定預設連接埠是否與使用中的連接埠相衝突	查看 Identity Manager 元件使用的連接埠

架構工作表

確定部署規模後，選取適當的部署，並記錄支援該部署所需的實體電腦 / 伺服器數量。

表格 2-2 架構工作表

部署使用案例
包含所有驅動程式的 Identity Manager 伺服器容錯移轉部署
執行的驅動程式數量
Identity Applications 高可用性部署

系統要求工作表

如需建議的硬體、受支援作業系統和虛擬環境的詳細資訊，請參閱《[System Requirements for Identity Manager 4.9](#)》(Identity Manager 4.8 系統要求)。

如需某個特定版本的系統要求資訊，請參閱 [Identity Manager 文件網站](#) 上提供的該版本的版本說明。Identity Manager 實作可能會因您的 IT 環境需求而有所不同，因此您應在最終確定適用於您環境的 Identity Manager 架構之前聯絡 [NetIQ 諮詢服務部門](#) 或任何 NetIQ Identity Manager 合作夥伴。

查看 Identity Manager 元件使用的連接埠

各 Identity Manager 元件使用不同的連接埠來保持相互之間的正常通訊。

附註：如果某個預設連接埠已在使用中，請務必為 Identity Manager 的元件指定另一個連接埠。

連接埠號碼	元件	連接埠用途
389	Identity Vault	用於以純文字方式與 Identity Manager 的元件進行 LDAP 通訊
465	Identity Reporting	用於與 SMTP 郵件伺服器進行通訊
524	Identity Vault	用於 NetWare 核心協定 (NCP) 通訊
636	Identity Vault	用於透過 TLS/SSL 與 Identity Manager 的元件進行 LDAP 通訊
5432	Identity Applications	用於與 Identity Applications 資料庫進行通訊
7707	Identity Reporting	受管理系統閘道驅動程式使用該連接埠來與 Identity Vault 通訊
8000	遠端載入器	驅動程式例項使用該連接埠進行 TCP/IP 通訊 附註： 應該為每個遠端載入器例項指定唯一的連接埠。
8005	Identity Applications	Tomcat 使用該連接埠來監聽關閉指令
8009	Identity Applications	Tomcat 使用該連接埠透過 AJP 通訊協定 (而不是 HTTP) 來與 Web 連接器通訊
8028	Identity Vault	用於進行 HTTP 純文字通訊和 NCP 通訊
8030	Identity Vault	用於進行 HTTPS 通訊和 NCP 通訊
8080	Identity Applications	Tomcat 使用該連接埠進行 HTTP 純文字通訊
8090	遠端載入器	遠端載入器使用該連接埠監聽來自遠端介面 shim 的 TCP/IP 連接 附註： 應該為每個 Remote Loader 例項指定唯一的連接埠。

連接埠號碼	元件	連接埠用途
8109	Identity Applications	僅適用於使用整合式安裝程序的情況 Tomcat 使用該連接埠透過 AJP 通訊協定 (而不是 HTTP) 來與 Web 連接器通訊
8180	Identity Applications	執行 Identity Applications 的 Tomcat 應用程式伺服器使用該連接埠進行 HTTP 通訊
8443	Identity Applications	Tomcat 使用該連接埠進行 HTTPS (SSL) 通訊，或者重新導向 SSL 通訊的申請
8543	Identity Applications	<i>預設不監聽</i> 當您未使用 TLS/SSL 通訊協定時，Tomcat 使用該連接埠來重新導向需要 SSL 傳輸的申請
5432	Identity Reporting	用於 PostgreSQL 資料庫 Sentinel
45654	使用者應用程式	將 Tomcat 與叢集群組配合執行時，安裝 Identity Applications 資料庫的伺服器使用該連接埠來監聽通訊



安裝和設定 Identity Manager 元件

此部分將引導您完成安裝和設定 Identity Manager 元件的過程。如需安裝說明，請參閱「[安裝程序](#)」(第 43 頁)。

安裝 Identity Manager 元件並完成基本組態後，必須執行一些額外的組態步驟，才能讓元件完全正常運作。如需詳細資訊，請參閱第 4 章「[完成安裝的最後步驟](#)」(第 59 頁)。

3 安裝和組態程序綜覽

本章介紹安裝和設定 Identity Manager 元件的程序。在開始組態過程前，必須查看每個元件的組態選項。如需詳細資訊，請參閱[瞭解組態設定](#)。

某些元件 (例如 Designer 和 Analyzer) 可能不需要進行設定。

安裝順序

必須依以下順序安裝元件，因為一些元件的安裝程式需要之前所安裝元件的相關資訊：

- ◆ Sentinel Log Management for Identity Governance and Administration (IGA) (只能在 Linux 電腦上安裝)
- ◆ Identity Manager 伺服器元件
- ◆ Identity Applications 元件 (僅適用於 Advanced Edition)
- ◆ Identity Reporting 元件
- ◆ Designer for Identity Manager
- ◆ Analyzer for Identity Manager

在安裝每個元件之前，必須查看該元件的安裝先決條件和注意事項。

瞭解 Identity Manager 伺服器、Identity Applications 及 Identity Reporting 元件的安裝和組態程序

Identity Manager 提供基於精靈的安裝方式來安裝和設定 Identity Manager 的下列元件：

- ◆ Identity Manager 伺服器
- ◆ Identity Applications
- ◆ Identity Reporting

安裝程式允許您以互動或靜默方式來安裝和設定元件。安裝程序允許您指定所安裝元件的值。

安裝程序還會在您的檔案系統上建立 JRE、Apache Tomcat、PostgreSQL、ActiveMQ 和 OpenSSL 等相依元件的儲存庫。如果您將多個 Identity Manager 元件安裝在同一部電腦上，安裝程序會參考此儲存庫，而不是為每個需要這些相依元件的 Identity Manager 元件建立它們的多個副本。例如，如果將 Identity Applications 和 Identity Reporting 安裝在同一部電腦上，它們會使用同一個 Tomcat。

安裝方式類型

Identity Manager 支援互動和靜默安裝方式。靜默 (非互動式) 安裝不顯示使用者介面，也不向使用者提出任何問題。

互動模式

您需要選取要安裝的元件。安裝程式會依據您的選擇安裝元件。

靜默方式

您需要在內容檔案中指定要安裝的元件的值。當您呼叫安裝程式時，它會從內容檔案中讀取這些值。您可以使用同一個內容檔案在環境中的不同電腦上執行靜默安裝。

安裝選項

下表說明了使用安裝程式提供的安裝選項將會安裝的元件：

表格 3-1 安裝選項

安裝選項	安裝的元件
Identity Manager 引擎	安裝 Identity Vault、Identity Manager 引擎、遠端載入器服務和 Identity 外掛程式、擴送代理程式以及驅動程式。
Identity Applications	安裝 Identity Applications、One SSO Provider (OSP)、使用者應用程式驅動程式、角色與資源服務驅動程式 (RRSD)、PostgreSQL 和 Self Service Password Reset (SSPR)。 附註： 如果您要在未安裝 Identity Applications 的其他伺服器上安裝 SSPR，請使用 <iso 掛接位置>\common\sspr\ 目錄中的 install.exe。
Identity Reporting	安裝 Identity Reporting、OSP、PostgreSQL、資料收集服務驅動程式 (DCS) 和受管理系統閘道 (MSG) 驅動程式。

組態模式類型

您可以使用以下方式設定 Identity Manager 元件：

- ◆ 一般
- ◆ 自訂

一般組態對於大部分組態選項都採用預設設定。在自訂組態中，您可以根據自己的要求指定自訂值。您可以使用此選項來組態大部分設定。

在組態期間使用不可猜出的密碼

許多 Identity Manager 元件都要求您在組態階段指定密碼。為了更快地完成組態，您可以指示安裝程序對所有組態參數套用相同的密碼。

該密碼必須至少包含六個字元。請不要使用字典中可以找到的單字。免費的密碼破解工具使用隨附的字典清單很容易就能猜出字典中的單字。如果您必須使用字典中的單字，請嘗試將它們與數字和標點符號結合使用。

瞭解 Designer 和 Analyzer 的安裝程序

對於 Designer 和 Analyzer，Identity Manager 提供了不同的 Windows 安裝程式。您可在[產品下載網站](#)獲取 Designer 和 Analyzer 的安裝程式。

Designer

您可以使用 Identity_Manager_4.9.0_Designer_Windows.zip 檔案安裝 Designer。若要進行靜默安裝，請在 designerInstaller.properties 檔案中為安裝指定相應的值。否則，安裝程式將假定使用預設參數值進行安裝。

Designer 不需要任何組態。

Analyzer

重要：Identity Manager 4.9 ISO 中不包含 Analyzer 工具。如果已安裝 Analyzer，請務必將其更新至版本 4.8.5，並與 Identity Manager 4.9 配合使用。

您可以使用 Identity_Manager_4.8.5_Windows_Analyzer.zip 檔案安裝 Analyzer。若要進行靜默安裝，請在 designerInstaller.properties 檔案中為安裝指定相應的值。否則，安裝程式將假定使用預設參數值進行安裝。

Analyzer 不需要任何組態。

安裝程序

透過閱讀此主題，您可瞭解 Identity Manager 元件的安裝方式。

Identity Manager 伺服器、Identity Applications 和 Identity Reporting 的安裝程序

本節將引導您透過互動或靜默方式完成安裝 Identity Manager 伺服器、Identity Applications 和 Identity Reporting 元件的整個過程。安裝程式中的 **Identity Manager 伺服器** 選項允許您安裝 32 位元、64 位元和 .NET 遠端載入器。

附註：安裝 Identity Manager 引擎之前，請確定已使用最新的 Windows 修補程式更新您的 Windows 伺服器，並已重新啟動 Windows 伺服器。

附註：如果您要在多伺服器環境中部署次要伺服器，必須指定主要伺服器 Identity Vault 的 IP 位址。

互動安裝

- 1 從軟體和授權頁面 (<https://sld.microfocus.com/>) 下載 Identity_Manager_4.9.0_Windows.iso。
- 2 掛接下載的 iso。
- 3 依據要安裝的元件，執行位於下列位置的 install.exe：
 - ◆ **Identity Manager 伺服器：**<iso 掛接位置>\IdentityManagerServer
 - ◆ **Identity Applications：**<iso 掛接位置>\IdentityApplications
 - ◆ **Identity Reporting：**<iso 掛接位置>\IdentityReporting
- 4 選取安裝時要使用的語言，然後按一下**確定**。
簡介螢幕會顯示可供安裝的元件。
- 5 按**下一步**。
- 6 閱讀並接受授權合約。
- 7 選取要安裝的元件，然後按**下一步**。
- 8 指定安裝資料夾，然後按**下一步**。

附註：自訂安裝資料夾不得包含特殊字元，例如 . 和 _

- 9 請選取安裝類型：
 - ◆ 典型安裝
 - ◆ 自訂安裝
- 10 安裝參數將因您選取的安裝模式而異。請指定所需的詳細資料。如需組態參數的資訊，請參閱下列表格：
 - ◆ [Identity Manager 引擎設定](#)
 - ◆ [Identity Applications 設定](#)
 - ◆ [Identity Reporting 設定](#)
- 11 查看「安裝前摘要」頁面上的詳細資料，然後按一下**安裝**。

靜默安裝

若要以靜默方式安裝 Identity Manager 元件，請使用 .iso 中相應元件的內容檔案。Identity Manager 媒體中包含一個範例內容檔案，位於 <iso 下載位置>\<Identity Manager 元件>\response-files 位置。

若要使用靜默方式安裝元件，請執行以下動作：

- 1 從 NetIQ 下載網站下載 Identity_Manager_4.9.0_Windows.iso。
- 2 掛接下載的 .iso。

- 3 依據要用來安裝元件的安裝模式，使用位於以下位置的 `typical_install.properties` 或 `custom_install.properties` 檔案：
 - ◆ **Identity Manager 伺服器**：<iso 掛接位置>\IdentityManagerServer\response-files
 - ◆ **Identity Applications**：<iso 掛接位置>\IdentityApplications\response-files
 - ◆ **Identity Reporting**：<iso 掛接位置>\IdentityReporting\response-files
- 4 依據需要修改安裝參數。如需組態參數的資訊，請參閱下列表格：
 - ◆ [Identity Manager 引擎設定](#)
 - ◆ [Identity Applications 設定](#)
 - ◆ [Identity Reporting 設定](#)
- 5 若要執行靜默安裝，請從元件的目標安裝目錄執行以下指令：

```
.\install.exe -i silent -f <path to typical or custom install properties file>
```

例如：

```
.\install.exe -i silent -f C:\Users\Administrator\Desktop  
typical_install_idmengine.properties
```
- 6 (選擇性) 關於預設安裝位置，請參閱安裝記錄。例如，您可以查看以下檔案：

```
C:\Program Files\NetIQ\IDM\Install\logs
```

安裝遠端載入器

Identity Manager 提供了在獨立伺服器上安裝遠端載入器的選項。如果您要將 Identity Manager 引擎和遠端載入器安裝到不同的電腦上，請使用此選項。

附註：您可以使用此選項安裝 64 位元遠端載入器和 .NET 遠端載入器。若要安裝 32 位元遠端載入器，請參閱 [Identity Manager 伺服器](#)、[Identity Applications](#) 和 [Identity Reporting](#) 的安裝程序。

互動安裝

- 1 從 NetIQ 下載網站下載 `Identity_Manager_4.9.0_RL_Windows.iso`。
- 2 掛接下載的 `.iso`。
- 3 從掛接位置執行 `install.exe` 檔案。
- 4 選取安裝時要使用的語言，然後按一下**確定**。
- 5 按**下一步**。
- 6 閱讀並接受授權合約。
- 7 按**下一步**。
- 8 指定安裝資料夾，然後按**下一步**。
- 9 按一下「**安裝**」。

靜默安裝

- 1 從 NetIQ 下載網站下載 Identity_Manager_4.9.0_RL_Windows.iso。
- 2 掛接下載的 .iso。
- 3 導覽至 <ISO 掛接位置>\response-files。
- 4 若要進行靜默安裝，請從內容檔案所在的目錄執行以下指令：

```
install.exe -i silent -f install.properties
```

安裝 Java 遠端載入器

Identity Manager 會使用 Java 遠端載入器，在一部伺服器上執行的 Identity Manager 引擎與其他位置 (該位置未執行 rdxml) 執行的 Identity Manager 驅動程式之間交換資料。您可以在裝有相容 JRE 和 Java 通訊端的任何受支援 Windows 平台上安裝 Java 遠端載入器 - dirxml_jremote。

- 1 在代管 Identity Manager 引擎的伺服器上，複製位於預設位置的應用程式 Shim .iso 或 .jar 檔案。例如，C:\NetIQ\idm\NDS\lib 目錄。
- 2 登入您要安裝 Java 遠端載入器的電腦 (目標電腦)。
- 3 驗證目標電腦是否裝有受支援版本的 JRE。
- 4 從 NetIQ 下載網站下載 Identity_Manager_4.9.0_Windows.iso。
- 5 掛接下載的 .iso。
- 6 導覽至 <iso 掛接位置>\IdentityManagerServer\products\IDM\java_remoteloader 目錄。
- 7 將 dirxml_jremote_dev.tar.gz 檔案複製到目標電腦上的所需位置。例如，將該檔案複製到 C:\NetIQ\idm。
- 8 將下列其中一個檔案複製到目標電腦上的所需位置：
 - ◆ dirxml_jremote.tar.gz
 - ◆ dirxml_jremote_mvs.tar如需 mvs 的資訊，請將 dirxml_jremote_mvs.tar 檔案解包，然後參閱 usage.html 文件。
- 9 在目標電腦上，解壓縮並擷取 .tar.gz 檔案。
例如，使用 7-Zip 或受支援的軟體解壓縮 .tar.gz 檔案。
- 10 將 CLASSPATH 環境變數設定至存在於 lib 資料夾中的所有 jar。如果您有特定於任何驅動程式的相依 jar，請將這些 jar 檔案複製到 lib 資料夾，然後也將 CLASSPATH 環境變數設定至這些 jar。
例如，進行如下設定：

```
CLASSPATH=E:\RL\JAVARL\lib\activation.jar;E:\RL\JAVARL\lib\comondrive  
rshim.jar;E:\RL\JAVARL\lib\delimitedtextshim.jar;E:\RL\JAVARL\lib\deli  
mitedtextutil.jar;E:\RL\JAVARL\lib\dirxml.jar;E:\RL\JAVARL\lib\dirxml_  
misc.jar;E:\RL\JAVARL\lib\dirxml_remote.jar;E:\RL\JAVARL\lib\jco3envir  
onment.jar;E:\RL\JAVARL\lib\mail.jar;E:\RL\JAVARL\lib\mapdb.jar;E:\RL\  
JAVARL\lib\nxsl.jar;E:\RL\JAVARL\lib\shimwrapper.jar;E:\RL\JAVARL\lib\  
xds.jar;E:\RL\JAVARL\lib\xp.jar
```

- 11** 將 PATH 環境變數設定為 Java.exe 的 JDK 或 JRE 對應的 bin 資料夾。

- 12** 必須在 dirxml_jremote 程序檔中指定 jar 檔案的位置。這些檔案位於 dirxml_jremote.tar.gz 解壓縮目錄的 lib 子目錄中。例如 \lib*.jar。

- 13** 設定範例組態檔案 config8000.txt，使其可用於您的應用程式 shim。

dirxml_jremote.tar.gz jar 檔案包含此檔案。如需詳細資訊，請參閱《[NetIQ Identity Manager Driver Administration Guide](#)》(NetIQ Identity Manager 驅動程式管理指南) 中的「[Configuring the Remote Loader and Drivers](#)」(設定遠端載入器和驅動程式)。

- 14** 使用以下指令啟動遠端載入器：

- 14a** 若要指定遠端載入器密碼：

```
java.exe -classpath %CLASSPATH%  
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config  
file name> -sp <Remote Loader Password> <Object Driver Password>
```

例如：

```
java.exe -classpath %CLASSPATH%  
com.novell.nds.dirxml.remote.loader.RemoteLoader -config  
e:\RL\JAVARL\config8000.txt -sp novell novell
```

- 14b** 若要啟動遠端載入器：

```
java.exe -classpath %CLASSPATH%  
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config  
file name>
```

例如：

```
java.exe -classpath %CLASSPATH%  
com.novell.nds.dirxml.remote.loader.RemoteLoader -config  
e:\RL\JAVARL\config8000.txt
```

- 14c** 若要停止遠端載入器：

```
java.exe -classpath %CLASSPATH%  
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config  
file name> -unload
```

例如：

```
java.exe -classpath %CLASSPATH%  
com.novell.nds.dirxml.remote.loader.RemoteLoader -config  
e:\RL\JAVARL\config8000.txt -unload
```

安裝 .NET 遠端載入器

若要管理使用者身分安裝 .NET 遠端載入器：

- 1 以管理員身分登入要安裝 .NET 遠端載入器的電腦。
- 2 若要存取安裝程式，請完成下列其中一個步驟：
 - 2a (視情況而定) 如果您已取得 Identity Manager 安裝套件的 .iso 影像檔，請導覽至包含 .Net 遠端載入器安裝檔案的目錄 (預設為 \products\idm\windows\setup\ 目錄)。
 - 2b (視情況而定) 如果您已從 NetIQ 下載網站下載了 .NET 遠端載入器安裝檔案，請完成以下步驟：
 - ◆ 導覽至所下載影像的 .tgz 檔案。
 - ◆ 將該檔案的內容擷取到本地電腦上的某個資料夾中。
- 3 執行安裝目錄中的 idm_install.exe 程式。
- 4 接受授權合約，然後按下一步。
- 5 在「選取元件」視窗中，指定「.NET 遠端載入器」。
- 6 (選擇性) 若要為個別元件選取特定的驅動程式，請完成以下步驟：
 - 6a 按一下自訂選定的元件，然後按下一步。
 - 6b 展開要安裝的元件下方的驅動程式。
 - 6c 選取要安裝的驅動程式。
- 7 按一下「下一步」。
- 8 在啟動通知視窗中，按一下確定。
- 9 選取 .NET 遠端載入器在您電腦上的安裝目錄。
- 10 查看「摘要」頁面，然後按一下安裝以完成安裝。

安裝 SSPR

安裝程式將提供用於單獨安裝 SSPR 的選項。如果要將 Identity Applications 和 SSPR 安裝在不同的電腦上，請使用此選項。這是唯一可在標準版中安裝 SSPR 的選項。安裝程式不會在標準版中自動安裝 SSPR。

您可以採用互動或靜默方式安裝 SSPR。

互動安裝

- 1 從 NetIQ 下載網站下載 Identity_Manager_4.9.0_Windows.iso。
- 2 掛接下載的 .iso。
- 3 導覽至 <ISO 掛接位置>\common\sspr 目錄。
- 4 執行 install.exe 檔案。
- 5 選取安裝時要使用的語言，然後按一下確定。
- 6 按下一步。

- 7 閱讀並接受授權合約。
- 8 按下一步。
- 9 指定安裝資料夾，然後按下一步。
- 10 指定 SSPR 的組態設定。如需詳細資訊，請參閱「[Self-Service Password Reset 的組態工作表](#)」(第 54 頁)。
- 11 按下一步。
- 12 按一下「安裝」。

靜默安裝

- 1 從 NetIQ 下載網站下載 Identity_Manager_4.9.0_Windows.iso。
- 2 掛接下載的 .iso。
- 3 導覽至 <ISO 掛接位置>\common\sspr 目錄。
- 4 若要進行靜默安裝，請從內容檔案所在的目錄執行以下指令：

```
install.exe -i silent -f sspr_silentinstall.properties
```

瞭解組態設定

使用下面的工作表有助於收集設定 Identity Manager 元件時需要指定的資訊。

Identity Manager 引擎的組態工作表

使用下面的工作表有助於收集設定 Identity Manager 引擎時需要指定的資訊。

表格 3-2 Identity Manager 引擎設定

參數	描述
Identity Vault IDB 位置	指定 Identity Vault IDB 位置。
建立新樹狀結構	如果要建立新 Identity Vault 樹狀結構，請選取此選項。
樹狀結構名稱	<i>僅當您選取了建立新樹狀結構選項時才適用。</i> 指定 Identity Vault 樹狀結構名稱。
新增至現有樹狀結構	如果要連接至遠端伺服器上現有的 Identity Vault 樹狀結構，請選取此選項。您必須指定 IP 位址，系統不支援主機名稱或 FQDN。
主機	<i>僅當您選取了新增至現有樹狀結構時才適用。</i> 指定 Identity Vault 的 IP 位址。

參數	描述
安全 LDAP 連接埠	僅當您選取了新增至現有樹狀結構時才適用。 指定 Identity Vault 用來監聽使用安全通訊端層 (SSL) 通訊協定之 LDAP 要求的連接埠。預設值為 636。如果在安裝 eDirectory 之前伺服器上已載入的某項服務使用了預設連接埠，則您必須指定其他連接埠。
管理員 DN	指定 Identity Manager 引擎的管理員名稱。預設值為 cn=admin,ou=sa,o=system。
管理員密碼	指定管理員物件的密碼。例如，password。
Identity Vault 伺服器網路位置 (使用 LDAP 格式)	指定伺服器容器的 DN。預設值為 ou=servers,o=system
Identity Vault 驅動程式集 (LDAP 格式)	指定驅動程式集的網路位置 DN。預設值為 cn=DriverSet, o=system。
純文字 LDAP 連接埠	指定 Identity Vault 要用來監聽純文字 LDAP 申請的連接埠。預設值為 389。
安全 LDAP 連接埠	指定 Identity Vault 要用來監聽使用安全通訊端層 (SSL) 通訊協定的 LDAP 申請的連接埠。預設值為 636。如果在安裝 eDirectory 之前伺服器上已載入的某項服務使用了預設連接埠，則您必須指定其他連接埠。
Clear Text HTTP Port	指定 HTTP 堆疊要以純文字格式運作的連接埠。預設值為 8028。
安全 HTTP 連接埠	指定 HTTP 堆疊採用 TLS/SSL 通訊協定運作的連接埠。預設值為 8030。
RSA 金鑰大小	僅當您選取了建立新樹狀結構選項時才適用。 指定 RSA 證書的金鑰大小。允許的值為 2048、4096 和 8192 位元。預設值為 4096。
EC 曲線	僅當您選取了建立新樹狀結構選項時才適用。 指定 EC 證書的橢圓曲線 (EC) 限制。允許的值為 P256、P384 和 P521。預設值為 P384。
證書生命期間	僅當您選取了建立新樹狀結構選項時才適用。 指定證書的有效期 (以年計)。

Identity Applications 的組態工作表

使用下面的工作表有助於收集設定 Identity Applications 時需要指定的資訊。

表格 3-3 Identity Applications 設定

參數	描述
安裝 Self-Service Password Reset	指定是否要安裝 SSPR 元件。
主機	指定安裝了 Identity Vault 的伺服器的 IP 位址。
安全 LDAP 連接埠	指定 Identity Vault 要用來監聽使用安全通訊端層 (SSL) 通訊協定的 LDAP 申請的連接埠。預設值為 636。如果在安裝 eDirectory 之前伺服器上已載入的某項服務使用了預設連接埠，則您必須指定其他連接埠。
管理員 DN	指定 Identity Manager 引擎的管理員名稱。預設值為 <code>cn=admin,ou=sa,o=system</code> 。
管理員密碼	僅在安裝新的驗證伺服器時適用。指定 LDAP 驗證伺服器管理員帳戶的密碼。
根容器 DN	指定根容器。預設值為 <code>o=data</code> 。
使用者容器 DN	<i>僅在安裝新的驗證伺服器時適用。</i> 指定 LDAP 驗證伺服器中用於儲存可登入 Access Review 的使用者帳戶的容器。例如 <code>o=data</code> 。
管理員容器 DN	<i>僅在安裝新的驗證伺服器時適用。</i> 指定 LDAP 驗證伺服器中用於儲存管理員帳戶的容器。
驅動程式集 DN	指定驅動程式集 DN。
部署 Identity Applications 驅動程式	如果要部署使用者應用程式驅動程式及角色與資源服務驅動程式，請選取此選項。
選取 Identity Applications 的資料庫平台	選取要與 Identity Applications 配合使用的資料庫。選項有 PostgreSQL、Oracle 和 Microsoft SQL Server。
新 PostgreSQL 伺服器	如果要安裝新的 PostgreSQL 資料庫例項，請選取此選項。
現有 PostgreSQL 伺服器	如果要連接至現有的 PostgreSQL 資料庫伺服器，請選取此選項。
資料庫主機	指定伺服器的名稱或 IP 位址。
資料庫連接埠	指定伺服器要用來與使用者應用程式通訊的連接埠。該值預設為 5432。
Identity Applications 資料庫名稱	指定 Identity Applications 的資料庫名稱。
工作流程引擎資料庫名稱	指定工作流程引擎的資料庫名稱。
資料庫使用者	指定允許使用者應用程式存取和修改資料庫中資料的帳戶名稱。
資料庫使用者密碼	指定資料庫管理員密碼

參數	描述
資料庫驅動程式 JAR	指定資料庫平台的 JAR 檔案。資料庫廠商會提供驅動程式 JAR 檔案，該檔案代表資料庫伺服器的簡易用戶端 JAR。例如，對於 PostgreSQL，您可以指定預設位於 C:\NetIQ\idm\apps\Postgres 資料夾中的 postgresql-9.4-1212.jdbc42.jar。NetIQ 不支援來自協力廠商的驅動程式 JAR 檔案。
要在何時建立綱要	在安裝過程中，指定要在何時建立資料庫綱要。可用選項有現在、應用程式啟動時和將 SQL 寫入檔案。
應用程式伺服器主機	指定安裝了 Tomcat 的伺服器的 IP 位址。
應用程式伺服器 HTTPS 連接埠	指定安裝了 Tomcat 的伺服器的連接埠。該值預設為 8543。
登入畫面名稱	指定要在使用者登入畫面上顯示的自訂名稱。預設值為 Identity Access。 升級 Identity Applications 時，登入畫面名稱會自動變更為 NetIQ Access。
Identity Applications 管理員	指定 LDAP 驗證伺服器管理員帳戶的 DN。例如，cn=uaadmin,ou=sa,o=data
管理員密碼	指定 Identity Applications 管理員密碼。
將此密碼設為其他設定的通用密碼	如果要設定通用密碼，請選取此選項。 附註： Tomcat 金鑰儲存區的預設密碼為 changeit。
OAuth 金鑰儲存區密碼	<i>僅當您選取了將此密碼設為其他設定的通用密碼核取方塊時才適用。</i> 指定 OAuth 金鑰儲存區密碼。
SSO 用戶端密碼	<i>僅當您選取了將此密碼設為其他設定的通用密碼核取方塊時才適用。</i> 指定 SSO 用戶端密碼。
SSPR 組態密碼	<i>僅當您選取了將此密碼設為其他設定的通用密碼核取方塊時才適用。</i> 指定 SSPR 組態密碼。
表單轉譯器 HTTPS 連接埠	指定表單轉譯器 HTTPS 連接埠。該值預設為 8600。
工作流程引擎 ID	為工作流程引擎 ID 指定唯一的值。

Identity Reporting 的組態工作表

使用下面的工作表有助於收集設定 Identity Reporting 時需要指定的資訊。

表格 3-4 Identity Reporting 設定

參數	描述
主機	指定安裝了 Identity Vault 的伺服器的 IP 位址。
安全 LDAP 連接埠	指定 Identity Vault 要用來監聽使用安全通訊端層 (SSL) 通訊協定的 LDAP 申請的連接埠。預設值為 636。如果在安裝 eDirectory 之前伺服器上已載入的某項服務使用了預設連接埠，則您必須指定其他連接埠。
管理員 DN	指定 Identity Manager 引擎的管理員名稱。預設值為 <code>cn=admin,ou=sa,o=system</code> 。
管理員密碼	指定 LDAP 驗證伺服器管理員帳戶的密碼。
使用者容器 DN	<i>僅在安裝新的驗證伺服器時適用。</i> 指定 LDAP 驗證伺服器中用於儲存可登入 Access Review 的使用者帳戶的容器。例如 <code>o=data</code> 。
管理員容器 DN	<i>僅在安裝新的驗證伺服器時適用。</i> 指定 LDAP 驗證伺服器中用於儲存管理員帳戶的容器。
驅動程式集 DN	指定驅動程式集 DN。
部署 Identity Reporting 驅動程式	如果您要部署資料收集服務驅動程式和受管理系統閘道服務驅動程式，請選取此選項。
選取 Identity Reporting 的資料庫平台	選取要與 Identity Reporting 配合使用的資料庫。選項有 PostgreSQL、Oracle 和 Microsoft SQL Server。
新 PostgreSQL 伺服器	如果要安裝新的 PostgreSQL 資料庫例項，請選取此選項。
現有 PostgreSQL 伺服器	如果要連接至現有的 PostgreSQL 資料庫伺服器，請選取此選項。
資料庫主機	指定伺服器的名稱或 IP 位址。
資料庫連接埠	指定伺服器要用來與 Identity Reporting 通訊的連接埠。該值預設為 5432。
資料庫名稱	指定 Identity Reporting 的資料庫名稱。
資料庫使用者密碼	指定資料庫管理員密碼
資料庫帳戶密碼	指定 Identity Reporting 的資料庫帳戶密碼。
應用程式伺服器主機	指定安裝了 Tomcat 的伺服器的 IP 位址。
應用程式伺服器 HTTPS 連接埠	指定安裝了 Tomcat 的伺服器的連接埠。該值預設為 8543。
外部 OSP 伺服器	如果要連接至外部 OSP 伺服器，請選取此選項。例如，如果要連接至 Identity Applications 使用的遠端 OSP，請使用此選項。

參數	描述
OSP 伺服器主機	僅當您選取了外部 OSP 伺服器 選項時才適用。 指定安裝了 OSP 的伺服器的 IP 位址。
OSP 伺服器連接埠	僅當您選取了外部 OSP 伺服器 選項時才適用。 指定 OSP 伺服器連接埠。
OSP 金鑰儲存區	僅當您選取了外部 OSP 伺服器 選項時才適用。 指定 OSP 金鑰儲存區檔案的位置。
OSP 金鑰儲存區密碼	僅當您選取了外部 OSP 伺服器 選項時才適用。 指定 OSP 金鑰儲存區密碼。
OSP 用戶端密碼	僅當您選取了外部 OSP 伺服器 選項時才適用。 指定 OSP 用戶端密碼。
Identity Reporting 管理員	指定 Identity Reporting 的管理員名稱。預設值為 <code>cn=uaadmin,ou=sa,o=data</code> 。
Identity Reporting 管理員密碼	指定 Identity Reporting 的管理員密碼。
將此密碼設為其他設定的通用密碼	如果要設定通用密碼，請選取此選項。

Self-Service Password Reset 的組態工作表

使用下面的工作表有助於收集設定 Self-Service Password Reset (SSPR) 時需要指定的資訊。

僅當您要將 Identity Applications 和 SSPR 安裝到不同的電腦上時，本節內容才適用。

表格 3-5 SSPR 設定

參數	描述
主機	指定安裝了 Identity Vault 的伺服器的 IP 位址。
安全 LDAP 連接埠	指定 Identity Vault 要用來監聽使用安全通訊端層 (SSL) 通訊協定的 LDAP 申請的連接埠。預設值為 636。如果在安裝 eDirectory 之前伺服器上已載入的某項服務使用了預設連接埠，則您必須指定其他連接埠。
管理員 DN	指定 Identity Manager 引擎的管理員名稱。預設值為 <code>cn=admin,ou=sa,o=system</code> 。
管理員密碼	指定 LDAP 驗證伺服器管理員帳戶的密碼。
使用者容器 DN	僅在安裝新的驗證伺服器時適用。 指定 LDAP 驗證伺服器中用於儲存可登入 Access Review 的使用者帳戶的容器。例如 <code>o=data</code> 。

參數	描述
管理員容器 DN	僅在安裝新的驗證伺服器時適用。 指定 LDAP 驗證伺服器中用於儲存管理員帳戶的容器。
應用程式伺服器主機	指定安裝了 Tomcat 的伺服器的 IP 位址。
應用程式伺服器 HTTPS 連接埠	指定安裝了 Tomcat 的伺服器的連接埠。該值預設為 8543。
Identity Applications 管理員	指定 LDAP 驗證伺服器管理員帳戶的 DN。例如， cn=uaadmin,ou=sa,o=data
管理員密碼	指定 Identity Applications 管理員密碼。
驗證伺服器主機	指定安裝了 OSP 的伺服器的 IP 位址。
驗證伺服器 HTTPS 連接埠	指定 OSP 伺服器 HTTPS 連接埠。
驗證伺服器用戶端密碼	指定 OSP 用戶端密碼。

安裝後步驟

本節提供有關在安裝 Identity Applications 後更新 Tomcat 環境的資訊。

- 「將 [preferIPv4Stack](#) 內容傳遞至 JVM」(第 55 頁)
- 「檢查伺服器的狀態」(第 56 頁)
- 「監控狀態統計資料」(第 56 頁)
- 「建立複合索引」(第 57 頁)
- 「設定 Identity Application 以拒絕用戶端發起的 SSL 重新交涉」(第 57 頁)

將 [preferIPv4Stack](#) 內容傳遞至 JVM

Identity Applications 使用 JGroups 來執行快取。在某些組態中，JGroups 要求您將 [preferIPv4Stack](#) 內容設定為 true，以確保 [mcast_addr](#) 結合成功。

如果不使用此選項，可能會發生以下錯誤：

```
[10/1/09 16:11:22:147 EDT] 0000000d UDP          W org.jgroups.util.Util
createMulticastSocket could not bind to /228.8.8.8 (IPv4 address); make
sure
your mcast_addr is of the same type as the IP stack (IPv4 or IPv6).
```

您還可能會看到此錯誤：

```
[3/21/12 10:04:32:470 EDT] 00000024 UDP          E org.jgroups.protocols.TP
down
failed sending message to null (131 bytes)
    java.lang.Exception: dest=/228.8.8.8:45654 (134 bytes)
        at org.jgroups.protocols.UDP._send(UDP.java:353)
```

參數 `java.net.preferIPv4Stack=true` 是一個系統內容，可以使用與其他系統內容 (例如 `extend.local.config.dir`) 相同的方式進行設定。

檢查伺服器的狀態

大多數負載平衡器都提供狀態檢查功能，以確定 HTTP 伺服器是否已啟動且正在監聽。使用者應用程式包含一個 URL，可用於設定負載平衡器上的 HTTP 狀態檢查。該 URL 為：

`http://<節點 IP>: 連接埠 /IDMProv/jsps/healthcheck.jsp`

監控狀態統計資料

REST API 可讓您擷取有關使用者應用程式狀態的資訊。API 可以存取系統，以獲取目前正在執行的線串、記憶體佔用情況、快取和叢集資訊，並使用 GET 操作傳回資訊。

- ◆ **記憶體資訊 (JVM 與系統記憶體)：**讀取與記憶體相關的資訊，例如系統記憶體和 JVM 佔用的記憶體。

例如：

`http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/memoryinfo`

- ◆ **線串資訊：**讀取大量佔用 CPU 資源的線串的相關資訊，並傳回導致高 CPU 利用率的排名靠前的線串清單。

例如：

`http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/threadinfo`

若要存取 JVM 中線串的堆疊追蹤，請將堆疊參數設定為 **True**。

例如：

`http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/threadinfo?stack=true`

若要指定 JVM 中的線串數，請為 **thread-count** 參數指定值。

例如：

`http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/threadinfo?thread-count=1`

- ◆ **快取資訊：**讀取使用者應用程式的快取資訊。

例如：

`http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/cacheinfo`

- ◆ **叢集資訊：**讀取與叢集相關的資訊。

例如：

`http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/clusterinfo`

附註：您必須是安全性管理員才能使用 REST API 檢視使用者應用程式狀態統計資料。

建立複合索引

安裝或升級 Identity Applications 後，為您要用於在 Identity Manager 儀表中對使用者排序的每個屬性手動建立複合索引。您可以使用位於 eDirectory 安裝路徑中的 ndsindex 公用程式來建立複合索引。可以指定多個屬性並以 \$ 符號分隔來建立複合索引。下面是需要建立複合索引的基本屬性：

- ◆ Surname, Given Name
- ◆ Given Name, Surname
- ◆ cn, Surname
- ◆ Title, Surname
- ◆ Telephone Number, Surname
- ◆ Internet Email Address, Surname
- ◆ L, Surname
- ◆ OU, Surname

以下指令可協助您使用 ndsindex 公用程式來建立複合索引：

```
ndsindex add [-h <hostname>] [-p <port>] -D <admin DN> -W [-w <password>] -s <eDirectory Server DN> [<indexName1>, <indexName2>.....]
```

例如，若要依職位對使用者排序，請執行以下指令：

```
ndsindex add -h <hostname> -p <ldap port> -D <admin DN> -w <admin passwd> -s <eDirectory Server DN> Title-SN;Title$Surname;value
```

您也可以使用轉換輸出公用程式建立複合索引。

必須使用 LDIF 檔案來建立索引。輸入 LDIF 檔案後，請透過觸發 Limber 來啟動索引編制活動。否則，索引編制將在 Limber 自動觸發時才執行。

用於建立複合索引，以依據 **Title** 屬性對使用者排序的範例 LDIF 檔案：

```
dn: cn=osg-nw5-7, o=Novell
changetype: modify
add: indexDefinition
indexDefinition: 0$sntitleindex$0$0$0$1$Title$surname
```

如需 LDIF 檔案的詳細資訊，請參閱《[NetIQ eDirectory Administration Guide](#)》(NetIQ eDirectory 管理指南) 中的「[LDIF Files](#)」(LDIF 檔案)。

設定 Identity Application 以拒絕用戶端發起的 SSL 重新交涉

依預設，Identity Applications 安裝程式會設定一個非安全連接 (http)。在某些情況下，非安全連接會使 Identity Manager 容易受到因用戶端所發起與 Identity Applications 伺服器的 SSL 重新交涉而導致的拒絕服務攻擊。為防止發生此問題，請將以下旗標新增至 <tomcat-install-directory>\bin\setenv.bat 檔案中的 CATALINA_OPTS 項目。

```
"-Djdk.tls.rejectClientInitiatedRenegotiation=true"
```


4 完成安裝的最後步驟

完成 Identity Manager 元件的安裝和組態後，您必須執行特定的任務，以使解決方案可在您的環境中正常運作。例如，依據業務程序定義的規則和要求設定安裝的驅動程式，以及設定 Sentinel Log Management for IGA 以收集稽核事件。

安裝後任務通常包含下列項目：

- 「設定 Identity Vault 的組態」(第 59 頁)
- 「設定遠端載入器和驅動程式」(第 60 頁)
- 「設定忘記密碼管理功能」(第 60 頁)
- 「設定 Identity Applications 的資料庫」(第 64 頁)
- 「設定 Identity Applications」(第 66 頁)
- 「設定資料收集的執行時期環境」(第 91 頁)
- 「設定 Identity Reporting」(第 100 頁)
- 「啟用 Identity Manager」(第 106 頁)
- 「查看 Identity Manager 元件使用的連接埠」(第 106 頁)

設定 Identity Vault 的組態

- 手動將 Identity Applications 和 Identity Reporting 證書輸入至 Identity Vault 中

手動將 Identity Applications 和 Identity Reporting 證書輸入至 Identity Vault 中

- 如果您有 Identity Applications 和 Identity Reporting 元件的自訂證書，請將這些證書輸入至 Identity Vault 中的 cacerts (C:\NetIQ\eDirectory\jre\lib\security\cacerts)。

例如，您可以使用以下 keytool 指令將證書輸入至 Identity Vault 中：

```
keytool -import -trustcacerts -alias <User Application certificate alias name> -keystore <cacerts file> -file <User Application certificate file>
```

- 如果您將 SSPR 安裝在未安裝使用者應用程式的其他伺服器上，請將 SSPR 應用程式證書輸入至使用者應用程式中的 idm.jks (C:\NetIQ\idm\apps\tomcat\conf\idm.jks)。

例如，您可以使用以下 keytool 指令將證書輸入至使用者應用程式中：

```
keytool -import -trustcacerts -alias <SSPR certificate alias name> -keystore <idm.jks> -file <SSPR certificate file>
```

設定遠端載入器和驅動程式

利用遠端載入器，Identity Manager 驅動程式可以存取連接的應用程式，而無需在此應用程式所在的伺服器上安裝 Identity Vault 和 Identity Manager 引擎。若要使用遠端載入器，您需要設定應用程式 shim，以使其能夠安全連接至 Identity Manager 引擎。此外，您還必須設定遠端載入器和 Identity Manager 驅動程式。《[NetIQ Identity Manager Driver Administration Guide](#)》(NetIQ Identity Manager 驅動程式管理指南) 的「[Configuring the Remote Loader and Drivers](#)」(設定遠端載入器和驅動程式) 中提供了相關資訊。

設定忘記密碼管理功能

Identity Manager 安裝程式中包含 Self Service Password Reset，以協助您管理重設忘記的密碼的程序。您也可以使用外部密碼管理系統。

- 「使用 [Self Service Password Reset](#) 進行忘記密碼管理」(第 60 頁)
- 「使用外部系統進行忘記密碼管理」(第 62 頁)
- 「針對分散式環境或叢集環境更新儀表板中的 SSPR 連結」(第 63 頁)

使用 Self Service Password Reset 進行忘記密碼管理

大多數情況下，您可以在安裝 SSPR 和 Identity Applications 時啟用忘記密碼管理功能。但是，您之前可能還未指定密碼變更後，SSPR 應將使用者轉遞到的 Identity Applications 抵達頁面 URL。此時，您可能需要啟用忘記密碼管理。這個單元將提供下列資訊：

- 「將 Identity Manager 設定為使用 Self Service Password Reset」(第 60 頁)
- 「為 Identity Manager 設定 Self Service Password Reset」(第 61 頁)
- 「鎖定 SSPR 組態」(第 61 頁)

將 Identity Manager 設定為使用 Self Service Password Reset

本節提供關於將 Identity Manager 設定為使用 SSPR 的資訊。

- 1 登入安裝了 Identity Applications 的伺服器。
- 2 執行組態更新公用程式。如需詳細資訊，請參閱第 3 節「[安裝和組態程序綜覽](#)」(第 41 頁)。
- 3 在公用程式中，導覽至驗證 > 密碼管理。
- 4 對於密碼管理提供程式，請指定 Self Service Password Reset (SSPR)。
- 5 (選擇性) 若要在 Identity Applications 登入頁面上提供用於重設使用者名或密碼，或者啟用新使用者帳戶的連結，請從使用者介面下拉式清單中選取其他連結，然後選取所需的核取方塊。或者，可以從使用者介面下拉式清單中選取「無法登入？」來提供通用連結。以下連結將顯示在 Identity Applications 登入頁面上：如果您忘記了使用者名稱或密碼，或者需要註冊，請按一下這裡。
- 6 導覽至 IDM SSO 用戶端 > Self Service Password Reset。

- 7 對於 **OAuth 用戶端 ID**，請指定用來供驗證伺服器識別 SSPR 單一登入用戶端的名稱。預設值為 `sspr`。
- 8 對於 **OAuth 用戶端機密**，請指定 SSPR 單一登入用戶端的機密。
- 9 對於 **OAuth 重新導向 URL**，請指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。
使用以下格式：`protocol://server:port/path`。例如，`http://10.10.10.48:8180/sspr/public/oauth`。
- 10 儲存變更，然後關閉公程式。

為 Identity Manager 設定 Self Service Password Reset

本節提供關於設定 SSPR 以與 Identity Manager 配合使用的資訊。例如，您可能想要修改密碼規則和處理安全回應問題。

如果 SSPR 是隨 Identity Manager 一起安裝的，則您已指定管理員可用來設定應用程式的密碼。NetIQ 建議您修改 SSPR 設定，然後指定管理員帳戶或群組可以設定 SSPR。

附註：如果您將 SSPR 安裝在不同於使用者應用程式伺服器的另一部伺服器上，請務必將 SSPR 應用程式證書新增至使用者應用程式 `cacerts`。

- 1 使用您在安裝期間指定的組態密碼登入 SSPR。
- 2 在「設定」頁面中，修改密碼規則和處理安全回應問題的設定。如需設定 SSPR 設定預設值的詳細資訊，請參閱《[NetIQ Self Service Password Reset Administration Guide](#)》(NetIQ Self Service Password Reset 管理指南) 中的「[Configuring Self Service Password Reset](#)」(設定 Self Service Password Reset)。
- 3 鎖定 SSPR 組態檔案 (`SSPRConfiguration.xml`)。如需鎖定組態檔案的詳細資訊，請參閱「[鎖定 SSPR 組態](#)」(第 61 頁)。
- 4 (選擇性) 若要在鎖定組態後修改 SSPR 設定，必須在 `SSPRConfiguration.xml` 檔案中將 `configIsEditable` 設定設為 `true`。
- 5 登出 SSPR。
- 6 為使變更生效，請重新啟動 Tomcat。

鎖定 SSPR 組態

- 1 移至 `http://<IP/DNS 名稱>:<連接埠>/sspr`。此連結可使您進入 SSPR 入口網站。
- 2 使用管理員帳戶或現有的登入身分證明登入 Identity Manager。
- 3 按一下頁面頂部的**組態管理員**，然後指定您在安裝期間指定的組態密碼。
- 4 按一下**組態編輯器**，然後導覽至**設定 > LDAP 設定**。
- 5 鎖定 SSPR 組態檔案 (`SSPRConfiguration.xml`)。
 - 5a 在「管理員許可權」區段下，為對 Identity Vault 中的 SSPR 擁有管理員權限的使用者或群組定義一個 LDAP 格式的過濾器。依預設，該過濾器設定為 `groupMembership=cn=Admins,ou=Groups,o=example`。

例如，對於使用者應用程式管理員，請將它設定為 `uaadmin (cn=uaadmin)`。

這可以防止使用者修改 SSPR 中的組態，但具有修改設定的完整權限的 SSPR 管理員使用者不包括在內。

5b 為確保 LDAP 查詢傳回結果，請按一下 **檢視相符項目**。

如果設定中存在任何錯誤，您將無法繼續設定下一個組態選項。SSPR 會顯示錯誤詳細資料，以協助您對問題進行疑難排解。

5c 按一下 **儲存**。

5d 在確認快顯視窗中，按一下 **確定**。

鎖定 SSPR 後，管理員使用者可以在「管理」使用者介面中查看其他選項，例如「儀表板」、「使用者活動」、「資料分析」等，而在鎖定 SSPR 之前，這些選項不會顯示。

6 (選擇性) 若要在鎖定組態後修改 SSPR 設定，必須在 `SSPRConfiguration.xml` 檔案中將 `configIsEditable` 設定設為 `true`。

7 登出 SSPR。

8 以 **步驟 3** 中定義的管理員使用者身分再次登入 SSPR。

9 按一下 **關閉組態**，然後按一下 **確定** 以確認變更。

10 為使變更生效，請重新啟動 Tomcat。

使用外部系統進行忘記密碼管理

若要使用外部系統，您必須指定包含「忘記密碼」功能之 WAR 檔案的位置。此程序包括以下活動：

- ♦ 「指定外部忘記密碼管理 WAR 檔案」(第 62 頁)
- ♦ 「測試外部忘記密碼組態」(第 63 頁)
- ♦ 「設定應用程式伺服器之間的 SSL 通訊」(第 63 頁)

指定外部忘記密碼管理 WAR 檔案

如果您在安裝期間未指定這些值，現在想要修改設定，可以使用 RBPM 組態公用程式，或者以管理員身分在使用者應用程式中進行變更。

1 (視情況而定) 若要在 RBPM 組態公用程式中修改設定，請完成以下步驟：

1a 登入安裝了 Identity Applications 的伺服器。

1b 執行 RBPM 組態公用程式。如需詳細資訊，請參閱第 3 節「安裝和組態程序綜覽」(第 41 頁)。

1c 在公用程式中，導覽至 **驗證 > 密碼管理**。

1d 對於密碼管理提供程式，請指定使用者應用程式 (舊版)。

2 (視情況而定) 若要在使用者應用程式中修改設定，請完成以下步驟：

2a 以使用者應用程式管理員身分登入。

2b 導覽至 **管理 > 應用程式組態 > 密碼模組設定 > 登入**。

3 對於**忘記密碼**，請指定外部。

4 對於**忘記密碼連結**，請指定當使用者在登入頁面上按一下**忘記密碼**時顯示的連結。當使用者按一下此連結時，應用程式會將其導向至外部密碼管理系統。例如：

```
http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp
```

5 對於**忘記密碼返回連結**，請指定在使用者執行完忘記密碼程序後顯示的連結。使用者按一下此連結會重新導向到指定的連結。例如：

```
http://localhost/IDMProv
```

6 對於**忘記密碼 Web 服務 URL**，請指定外部轉遞密碼 WAR 用來回呼至 Identity Applications 的 Web 服務 URL。請使用以下格式：

```
https://idmhost:sslport/idm/pwdmgt/service
```

返回連結必須使用 SSL，以確保與 Identity Applications 進行安全的 Web 服務通訊。如需詳細資訊，請參閱「[設定應用程式伺服器之間的 SSL 通訊](#)」(第 63 頁)。

7 手動將 ExternalPwd.war 複製到執行外部密碼 WAR 功能的遠端應用程式伺服器部署目錄中。

測試外部忘記密碼組態

如果您擁有外部密碼 WAR 檔案，想要透過存取忘記密碼功能來測試該功能，則可以在以下位置存取該功能：

- 直接在瀏覽器中存取。移至外部密碼 WAR 檔案中的「忘記密碼」頁面。例如 `http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp`。
- 在使用者應用程式登入頁面中，按一下**忘記密碼連結**。

設定應用程式伺服器之間的 SSL 通訊

如果您使用的是外部密碼管理系統，則必須在部署 Identity Applications 與外部忘記密碼管理 WAR 檔案的 Tomcat 例項之間設定 SSL 通訊。如需詳細資訊，請參閱 Tomcat 文件。

針對分散式環境或叢集環境更新儀表板中的 SSPR 連結

安裝程序假設您要將 SSPR 部署在 Identity Applications 和 Identity Reporting 所在的同一個應用程式伺服器上。依預設，儀表板中應用程式頁面上的內建連結會使用指向本地系統上 SSPR 的相對 URL 格式。例如 `\sspr\private\changepassword`。如果在分散式環境或叢集環境中安裝應用程式，則必須更新 SSPR 連結的 URL。

如需詳細資訊，請參閱 *Identity Applications 說明*。

- 1 以管理員身分登入儀表板。例如，以 `uaadmin` 身分登入。
- 2 按一下「**編輯**」。
- 3 在「**編輯首頁項目**」頁面上，將游標停在要更新的項目上，然後按一下編輯圖示。例如，選取**變更我的密碼**。

- 4 對於連結，請指定絕對 URL。例如 `http://10.10.10.48:8180/sspr/changepassword`。
- 5 按一下「儲存」。
- 6 對每個要更新的 SSPR 連結重複上述步驟。
- 7 完成後，按一下我已完成。
- 8 登出系統，然後以一般的使用者身分登入以測試變更。

設定 Identity Applications 的資料庫

Identity Applications 的資料庫支援多種任務，例如，儲存組態資料和工作流程活動的資料。您必須先安裝並設定資料庫，然後才能安裝應用程式。如需受支援資料庫的詳細資訊，請參閱「[NetIQ Identity Manager System requirements](#)」(NetIQ Identity Manager 系統要求) 頁面。

附註：如果要移轉至新版 RBPM 和 Identity Applications，您必須使用先前安裝所用的同一個資料庫。「先前安裝」是指您要從中移轉資料的安裝。

- ◆ 「設定 Oracle 資料庫」(第 64 頁)
- ◆ 「設定 SQL Server 資料庫」(第 65 頁)

設定 Oracle 資料庫

本節介紹為使用者應用程式使用 Oracle 資料庫時可用的組態選項。如需受支援 Oracle 版本的資訊，請參閱 [NetIQ Identity Manager 技術資訊網站](#)。

檢查資料庫的相容性層級

來自不同 Oracle 版本的資料庫相容的前提為，這些資料庫支援相同的功能且這些功能以相同的方式執行。如果它們不相容，則某些功能或操作可能無法依預期運作。例如，建立綱要會失敗，導致您無法部署 Identity Applications。

若要檢查資料庫的相容性層級，請執行以下步驟：

1. 連接至資料庫引擎。
2. 連接至 SQL Server 資料庫引擎的適當例項後，在物件總管中按一下伺服器名稱。
3. 展開資料庫，然後依據資料庫選取使用者資料庫，或者展開系統資料庫並選取一個系統資料庫。
4. 以滑鼠右鍵按一下資料庫，然後按一下內容。
資料庫內容對話方塊隨即開啟。
5. 在選取頁面窗格中，按一下選項。
目前的相容性層級會顯示在相容性層級清單方塊中。
6. 若要檢查相容性層級，請在查詢視窗中輸入以下內容，然後按一下執行。

```
SQL> SELECT name, value FROM v$parameter  
WHERE name = 'compatible';
```

預期輸出為：12.2.0.1

設定字元集

使用者應用程式資料庫必須使用 Unicode 編碼的字元集。在建立資料庫時，請使用 AL32UTF8 指定此字元集。

若要確認是否將 Oracle 12c 資料庫設定為使用 UTF-8，請發出以下指令：

```
select * from nls_database_parameters;
```

如果資料庫未設定為使用 UTF-8，系統將會回應以下資訊：

```
NLS_CHARACTERSET  
WE8MSWIN1252
```

否則，系統會回應以下資訊，確認資料庫已設定為使用 UTF-8：

```
NLS_CHARACTERSET  
AL32UTF8
```

附註：建議使用 JDBC JAR 版本 ojdbc6.jar。

如需設定字元集的詳細資訊，請參閱「[Choosing an Oracle Database Character Set](#)」（選擇 Oracle 資料庫字元集）。

設定管理員使用者帳戶

使用者應用程式要求 Oracle 資料庫使用者帳戶擁有特定的權限。在 SQL Plus 公用程式中輸入以下指令：

```
CREATE USER idmuser IDENTIFIED BY password  
GRANT CONNECT, RESOURCE to idmuser  
ALTER USER idmuser quota 100M on USERS;
```

其中，*idmuser* 代表使用者帳戶。

設定 SQL Server 資料庫

本節介紹為使用者應用程式使用 SQL Server 資料庫時可用的組態選項。如需受支援 SQL Server 版本的資訊，請參閱 [NetIQ Identity Manager 技術資訊網站](#)。

設定字元集

SQL Server 不允許您為資料庫指定字元集。使用者應用程式在支援 UTF-8 的 NCHAR 欄類型中儲存 SQL Server 字元資料。

附註：SQL 僅支援 SQL_Latin1_General_CP1_CI_AS 定序。

設定管理員使用者帳戶

安裝受支援版本的 Microsoft SQL Server 之後，請使用 SQL Server Management Studio 之類的應用程式建立資料庫和資料庫使用者。該資料庫使用者帳戶必須擁有以下權限：

- ◆ CREATE TABLE
- ◆ DELETE
- ◆ INSERT
- ◆ SELECT
- ◆ UPDATE

附註：建議對 Microsoft SQL Server 2014 使用 JDBC JAR 版本 `sqljdbc4.jar`，對 Microsoft SQL Server 2016 使用 `sqljdbc42.jar`。

設定 Identity Applications

- ◆ 「完成 Identity Applications 的設定」 (第 66 頁)
- ◆ 「部署適用於 Identity Applications 的 REST API」 (第 88 頁)
- ◆ 「使用 Oracle 服務名稱存取 Oracle 資料庫」 (第 88 頁)
- ◆ 「手動建立資料庫綱要」 (第 88 頁)
- ◆ 「組態 Identity Applications 的單一登入設定」 (第 90 頁)
- ◆ 「啟動 Identity Applications」 (第 90 頁)
- ◆ 「Identity Applications 的組態和使用考量」 (第 91 頁)

完成 Identity Applications 的設定

Identity Applications 組態公用程式可協助您管理使用者應用程式驅動程式和 Identity Applications 的設定。Identity Applications 的安裝程式將呼叫某版本的此公用程式，以使您能夠更快地設定應用程式。您也可以安裝後修改其中的大部分設定。

依預設，用於執行組態公用程式 (`configupdate.bat`) 的檔案位於 Identity Applications 的某個安裝子目錄 (`C:\NetIQ\idm\apps\UserApplication`) 中。

附註：在叢集中，所有叢集成員的組態設定都必須相同。將主要節點中的 `ism-sensitive.properties`、`ism-configuration.properties` 和 `encrypt-keys.pkcs12` 複製到所有使用者應用程式節點。

本節說明了組態公用程式中的設定。這些設定按索引標籤組織。如果您要安裝 Identity Reporting，安裝程序會將 Reporting 的參數新增至公用程式中。

- ◆ 「執行 Identity Applications 組態公用程式」 (第 67 頁)
- ◆ 「儲存 Configupdate 公用程式密碼 (選擇性)」 (第 67 頁)

- ◆ 「使用者應用程式參數」(第 68 頁)
- ◆ 「Reporting 參數」(第 78 頁)
- ◆ 「驗證參數」(第 80 頁)
- ◆ 「SSO 用戶端參數」(第 83 頁)
- ◆ 「CEF 稽核參數」(第 87 頁)

執行 Identity Applications 組態公用程式

- 1 在文字編輯器中開啟 configupdate.properties 檔案，並驗證是否已設定以下選項：

```
edit_admin="true"
use_console="false"
```

- 2 在指令提示符處，執行組態公用程式 (configupdate.bat)。

附註：您可能需要花幾分鐘時間等待公用程式啟動。

附註：由於 Identity Manager 不支援 NAM OAuth，因此請不要在組態公用程式的「驗證伺服器」索引標籤中使用 **Access Manager 是 OAuth 提供者** 選項。

儲存 Configupdate 公用程式密碼 (選擇性)

Configupdate 公用程式的預設密碼為 changeit，該密碼儲存在

C:\NetIQ\IDM\apps\tomcat\conf 下的主金鑰儲存區 (encrypt-keys.pkcs12) 密碼中。此密碼的加密值儲存在 C:\NetIQ\IDM\apps\tomcat\conf 下的 ism-sensitive.properties 檔案中。如果您要使用 keytool 指令變更主金鑰儲存區的密碼，需要在 ism-sensitive.properties 中加密並更新此密碼。

執行以下步驟來變更並加密密碼：

1. 在指令提示符處執行以下指令，以變更您的 Configupdate 公用程式密碼：

```
keytool -storepasswd -new <new master keystore password> -keystore
C:\NetIQ\IDM\apps\tomcat\conf\encrypt-keys.pkcs12 -storepass changeit -
storetype PKCS12
```

2. 若要加密新密碼，請執行以下指令：

```
C:\NetIQ\Common\JRE\bin\java -cp
C:\NetIQ\IDM\apps\tomcat\lib\obscurity-<version>-uber.jar
com.netiq.ism.obfuscate.server.util.PasswordObfuscator <new master
keystore password>
```

3. 請務必透過變更 C:\NetIQ\IDM\apps\tomcat\conf 下 ism-sensitive.properties 檔案中的 com.microfocus.ism.master-storepass 值，來儲存已加密的密碼

使用者應用程式參數

在設定 Identity Applications 時，此索引標籤用於定義應用程式在與 Identity Vault 通訊時使用的值。有些設定對於完成安裝程序必不可少。

該索引標籤預設會顯示基本選項。若要查看所有設定，請按一下顯示進階選項。此索引標籤包含以下幾組設定：

- ◆ 「Identity Vault 設定」 (第 68 頁)
- ◆ 「Identity Vault DN」 (第 69 頁)
- ◆ 「Identity Vault 使用者身分」 (第 71 頁)
- ◆ 「Identity Vault 使用者群組」 (第 72 頁)
- ◆ 「Identity Vault 證書」 (第 73 頁)
- ◆ 「電子郵件伺服器組態」 (第 73 頁)
- ◆ 「可信金鑰儲存區」 (第 75 頁)
- ◆ 「NetIQ Sentinel 數位簽名證書與金鑰」 (第 76 頁)
- ◆ 「其他」 (第 76 頁)
- ◆ 「容器物件」 (第 77 頁)

Identity Vault 設定

本節定義可讓 Identity Applications 存取 Identity Vault 中的使用者身分和角色的設定。有些設定對於完成安裝程序必不可少。

Identity Vault 伺服器

必需

指定 LDAP 伺服器的主機名稱或 IP 位址。例如 myLDAPhost。

LDAP 連接埠

指定 Identity Vault 要用來監聽純文字格式 LDAP 要求的連接埠。預設值為 389。

LDAP 安全連接埠

指定 Identity Vault 用來監聽使用安全通訊端層 (SSL) 通訊協定之 LDAP 要求的連接埠。預設值為 636。

如果在安裝 eDirectory 之前伺服器上已載入的某項服務使用了預設連接埠，則您必須指定其他連接埠。

Identity Vault 管理員

必需

指定 LDAP 管理員的身分證明。例如，cn=admin。Identity Vault 中必須已存在此使用者。

Identity Applications 將使用此帳戶來與 Identity Vault 建立管理連接。這個值會根據萬能金鑰進行加密。

Identity Vault 管理員密碼

必需

指定與 LDAP 管理員關聯的密碼。這個密碼會根據萬能金鑰進行加密。

使用公用匿名帳戶

指定未登入的使用者是否能夠存取 LDAP 公用匿名帳戶。

安全管理員連接

指定 RBPM 是否使用 SSL 通訊協定來進行與管理員帳戶相關的所有通訊。如果指定此設定，則無需 SSL 的其他操作可以在不使用 SSL 的情況下執行。

附註：此選項可能會對效能造成負面影響。

安全使用者連接

指定 RBPM 是否使用 TLS/SSL 通訊協定來進行與已登入使用者帳戶相關的所有通訊。如果指定此設定，則無需 TLS/SSL 的其他操作可以在不使用該通訊協定的情況下執行。

附註：此選項可能會對效能造成負面影響。

Identity Vault DN

本節定義可在 Identity Applications 與其他 Identity Manager 元件之間進行通訊的容器和使用者帳戶的可辨識名稱。有些設定對於完成安裝程序必不可少。

根容器 DN

必需

指定根容器的 LDAP 可辨識名稱。當在目錄抽象層中沒有指定任何搜尋根部時，會將它用作預設實體定義搜尋根部。例如 `o=mycompany`。

使用者容器 DN

必需

在顯示進階選項的情況下，公用程式會在「Identity Vault 使用者身分」下顯示此參數。

指定使用者容器的 LDAP 可辨識名稱 (DN) 或完全合格的 LDAP 名稱。對於此項設定，請注意以下事項：

- ◆ 允許此容器 (及其下層) 中的使用者登入 Identity Applications。
- ◆ 如果您已啟動代管 Identity Applications 的 Tomcat，則無法使用 `configupdate.bat` 檔案變更此設定。
- ◆ 此容器必須包含您在安裝使用者應用程式驅動程式時指定的使用者應用程式管理員。否則，指定的帳戶將無法執行工作流程。

群組容器 DN

必需

在顯示進階選項的情況下，公用程式會在「*Identity Vault* 使用者群組」下顯示此參數。

指定群組容器的 LDAP 可辨識名稱 (DN) 或完全合格的 LDAP 名稱。對於此項設定，請注意以下事項：

- ◆ 目錄抽象層中的實體定義使用此 DN。
- ◆ 如果您已啟動代管 *Identity Applications* 的 Tomcat，則無法使用 `configupdate.bat` 檔案變更此設定。

使用者應用程式驅動程式

必需

指定使用者應用程式驅動程式的可辨識名稱。

例如，如果驅動程式為 `UserApplicationDriver`，驅動程式集名為 `MyDriverSet`，並且驅動程式集位於網路位置 `o=myCompany` 中，請指定 `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`。

使用者應用程式管理員

必需

指定 *Identity Vault* 中有權對使用者應用程式的指定使用者容器執行管理任務的現有使用者帳戶。對於此項設定，請注意以下事項：

- ◆ 如果您已啟動代管使用者應用程式的 Tomcat，則無法使用 `configupdate.bat` 檔案變更此設定。
- ◆ 若要在部署使用者應用程式後變更此指定，請在使用者應用程式的**管理 > 安全性**頁面中進行變更。
- ◆ 此使用者帳戶有權使用使用者應用程式的**管理索引標籤**來管理入口網站。
- ◆ 如果使用者應用程式管理員參與 **Designer** 或使用者應用程式 (**申請和核准索引標籤**) 中公開的工作流程管理任務，則您必須為此管理員授予適當的託管者權限，使其能夠存取使用者應用程式驅動程式中包含的物件例項。如需詳細資訊，請參閱《*User Application Administration Guide*》(使用者應用程式管理指南)。

佈建管理員

指定 *Identity Vault* 中的一個現有使用者帳戶，該帳戶將負責管理可在整個使用者應用程式中使用的「佈建工作流程」功能。

若要在部署使用者應用程式之後變更此指定，請使用使用者應用程式中的「**管理**」>「**管理員指定**」頁面。

法規遵循管理員

指定 *Identity Vault* 中的一個現有帳戶，該帳戶可執行某個系統角色，以允許成員執行法規遵循索引標籤上的所有功能。對於此項設定，請注意以下事項：

- ◆ 若要在部署 *Identity Applications* 後變更此項指定，請在使用者應用程式的**管理 > 管理員指定**頁面中進行變更。
- ◆ 在組態更新期間，只有在未指定有效的法規遵循管理員時，對此值的變更才會生效。如果已存在有效的法規遵循管理員，則不會儲存所做的變更。

角色管理員

指定一個角色，該角色允許成員建立、移除或修改所有角色，以及授予或撤銷對任何使用者、群組或容器的任何角色指定。它還允許其角色成員為任一使用者執行報告。對於此項設定，請注意以下事項：

- ◆ 依預設，「使用者應用程式」管理員會指定為此角色。
- ◆ 若要在部署 Identity Applications 後變更此項指定，請在使用者應用程式的**管理 > 管理員指定**頁面中進行變更。
- ◆ 在組態更新期間，只有在未指定有效的角色管理員時，對此值的變更才會生效。如果有有效的「角色管理員」已存在，則不會儲存您所做的變更。

安全性管理員

指定一個為成員提供安全性網域內所有功能的角色。對於此項設定，請注意以下事項：

- ◆ 安全性管理員可以對安全性網域內的所有物件執行所有允許的動作。安全性網域允許安全性管理員為 RBPM 中所有網域內的所有物件設定存取許可權。安全性管理員可以設定團隊，還可以指定網域管理員、委託管理員及其他安全性管理員。
- ◆ 若要在部署 Identity Applications 後變更此項指定，請在使用者應用程式的**管理 > 管理員指定**頁面中進行變更。

資源管理員

指定一個為成員提供資源網域內所有功能的角色。對於此項設定，請注意以下事項：

- ◆ 資源管理員可以對資源網域內的所有物件執行所有允許的動作。
- ◆ 若要在部署 Identity Applications 後變更此項指定，請在使用者應用程式的**管理 > 管理員指定**頁面中進行變更。

RBPM 組態管理員

指定一個為成員提供組態網域內所有功能的角色。對於此項設定，請注意以下事項：

- ◆ RBPM 組態管理員可以對組態網域內的所有物件執行所有允許的動作。RBPM 組態管理員控制對 RBPM 中導覽項目的存取權。此外，RBPM 組態管理員還可以設定委託與代理服務、佈建用者介面及工作流程引擎。
- ◆ 若要在部署 Identity Applications 後變更此項指定，請在使用者應用程式的**管理 > 管理員指定**頁面中進行變更。

RBPM 報告管理員

指定報告管理員。依預設，安裝程式列出的該值與其餘安全性欄位中的使用者相同。

Identity Vault 使用者身分

本節定義可讓 Identity Applications 與 Identity Vault 中的使用者容器通訊的值。有些設定對於完成安裝程序必不可少。

僅當您選取了**顯示進階選項**時，公用程式才會顯示這些設定。

使用者容器 DN

必需

在不顯示進階選項的情況下，公用程式會在「*Identity Vault DN*」下顯示此參數。

指定使用者容器的 LDAP 可辨識名稱 (DN) 或完全合格的 LDAP 名稱。對於此項設定，請注意以下事項：

- ♦ 允許此容器 (及其下層) 中的使用者登入 Identity Applications 。
- ♦ 如果您已啟動代管 Identity Applications 的 Tomcat，則無法使用 configupdate.bat 檔案變更此設定。
- ♦ 此容器必須包含您在安裝使用者應用程式驅動程式時指定的使用者應用程式管理員。否則，指定的帳戶將無法執行工作流程。

使用者搜尋範圍

指定 Identity Vault 使用者在搜尋容器時可以探查的範圍深度。

使用者物件類別

指定 LDAP 使用者的物件類別。通常，該類別為 inetOrgPerson。

登入屬性

指定代表使用者登入名稱的 LDAP 屬性。例如，cn。

命名屬性

指定在查閱使用者或群組時做為識別碼的 LDAP 屬性。這與登入屬性不同，後者僅在登入期間使用。例如，cn。

使用者成員資格屬性

(選擇性) 指定代表使用者群組成員資格的 LDAP 屬性。指定名稱時請不要使用空格。

Identity Vault 使用者群組

本節定義可讓 Identity Applications 與 Identity Vault 中的群組容器通訊的值。有些設定對於完成安裝程序必不可少。

僅當您選取了顯示進階選項時，公用程式才會顯示這些設定。

群組容器 DN

必需

在不顯示進階選項的情況下，公用程式會在「*Identity Vault DN*」下顯示此參數。

指定群組容器的 LDAP 可辨識名稱 (DN) 或完全合格的 LDAP 名稱。對於此項設定，請注意以下事項：

- ♦ 目錄抽象層中的實體定義使用此 DN。
- ♦ 如果您已啟動代管 Identity Applications 的 Tomcat，則無法使用 configupdate.bat 檔案變更此設定。

群組容器範圍

指定 Identity Vault 使用者在搜尋群組容器時可以探查的範圍深度。

群組物件類別

指定 LDAP 群組的物件類別。通常，該類別為 `groupofNames`。

群組成員資格屬性

(選擇性) 指定使用者的群組成員資格。請勿在此名稱中使用空格。

使用動態群組

指定是否要使用動態群組。

您還必須指定動態群組物件類別的值。

動態群組物件類別

僅當您選取了使用動態群組時才適用。

指定 LDAP 動態群組的物件類別。通常，該類別為 `dynamicGroup`。

Identity Vault 證書

本節定義 JRE 金鑰儲存區的路徑和密碼。有些設定對於完成安裝程序必不可少。

金鑰儲存區路徑

必需

指定 Tomcat 在執行時所用 JRE 金鑰儲存區 (`cacerts`) 檔案的完整路徑。您可以手動輸入路徑，也可以瀏覽至 `cacerts` 檔案。對於此項設定，請注意以下事項：

- 在環境中，您必須指定 RBPM 的安裝目錄。預設值會設定為正確的位置。
- Identity Applications 的安裝程式將會修改金鑰儲存區檔案。

金鑰儲存區密碼

必需

指定金鑰儲存區檔案的密碼。預設值為「`changeit`」。

電子郵件伺服器組態

本節定義用於啟用電子郵件通知的值，您可以使用電子郵件通知來進行基於電子郵件的核准。如需詳細資訊，請參閱《[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)》(NetIQ Identity Manager - Identity Applications 管理員指南)。

通知樣板主機

指定代管 Identity Applications 的 Tomcat 的名稱或 IP 位址。例如 `myapplication serverServer`。

此值會取代電子郵件範本中的 `$HOST$` 記號。安裝程式將使用此資訊來建立佈建申請任務和核准通知的 URL。

通知樣板連接埠

指定代管 Identity Applications 的 Tomcat 的連接埠號碼。

此值將取代佈建申請任務和核准通知中所用電子郵件樣板內的 `$PORT$` 記號。

通知樣板安全連接埠

指定代管 Identity Applications 的 Tomcat 的安全連接埠號碼。

此值將取代佈建申請任務和核准通知中所用電子郵件樣板內的 `$SECURE_PORT$` 記號。

通知樣板通訊協定

指定在傳送使用者電子郵件時要包含在 URL 中的非安全通訊協定。例如 `http`。

此值將取代佈建申請任務和核准通知中所用電子郵件樣板內的 `$PROTOCOL$` 記號。

通知樣板安全通訊協定

指定在傳送使用者電子郵件時要包含在 URL 中的安全通訊協定。例如：`https`。

此值將取代佈建申請任務和核准通知中所用電子郵件樣板內的 `$SECURE_PROTOCOL$` 記號。

SMTP 電子郵件通知寄件者

指定 Identity Applications 用來傳送電子郵件通知的電子郵件帳戶。

SMTP 伺服器名稱

指定 Identity Applications 為佈建電子郵件使用之 SMTP 電子郵件主機的 IP 位址或 DNS 名稱。請不要使用 `localhost`。

伺服器需要驗證

指定伺服器是否需要驗證。

您還必須指定電子郵件伺服器的身分證明。

使用者名稱

僅當您啟用了伺服器需要驗證時才適用。

指定電子郵件伺服器的登入帳戶名稱。

密碼

僅當您啟用了伺服器需要驗證時才適用。

指定郵件伺服器的登入帳戶密碼。

使用 SMTP TLS

指定在郵件伺服器之間進行傳輸期間，是否要保護電子郵件內容的安全。

電子郵件通知影像位置

指定要在電子郵件通知中包含的影像所在的路徑。

當 Identity Applications 伺服器和電子郵件伺服器均設定為使用安全連接時，請確定滿足以下條件：

- ◆ 用於在 Identity Applications 伺服器與電子郵件伺服器之間建立安全連接的證書是可信的 CA 證書
- ◆ 在影像路徑中使用 `https`。例如 `https://localhost:8543/IDMProv/images`

如果 Identity Applications 在使用 `http` 進行純文字通訊的伺服器上運作，請在影像路徑中用 `http` 取代 `https`。影像路徑的範例：`http://localhost:8080/IDMProv/images`

對電子郵件簽名

指定是否要將數位簽名新增至外送郵件。

如果啟用此選項，則還必須指定金鑰儲存區和簽名金鑰的設定。

金鑰儲存區路徑

僅當您啟用了對電子郵件簽名時才適用。

指定要用於對電子郵件數位簽名的金鑰儲存區 (cacerts) 檔案的完整路徑。您可以手動輸入路徑，也可以瀏覽至 cacerts 檔案。

例如，C:\NetIQ\idm\apps\jre\lib\security\cacerts。

金鑰儲存區密碼

僅當您啟用了對電子郵件簽名時才適用。

指定金鑰儲存區檔案的密碼。例如，changeit。

簽名金鑰的別名

僅當您啟用了對電子郵件簽名時才適用。

指定簽章金鑰在金鑰儲存區中的別名。例如，idmapptest。

簽名金鑰密碼

僅當您啟用了對電子郵件簽名時才適用。

指定用於保護包含簽名金鑰的檔案的密碼。例如，changeit。

可信金鑰儲存區

本節定義 Identity Applications 的可信金鑰儲存區的值。僅當您選取了顯示進階選項時，公用程式才會顯示這些設定。

可信儲存區路徑

指定包含所有可信簽名者證書之可信金鑰儲存區的路徑。如果此路徑為空，Identity Applications 將會從系統內容 javax.net.ssl.trustStore 中取得路徑。如果該系統內容無法提供路徑，安裝程式預設使用 jre/lib/security/cacerts。

可信儲存區密碼

指定可信金鑰儲存區的密碼。如果您將此欄位保留空白，Identity Applications 將會從系統內容 javax.net.ssl.trustStorePassword 中取得密碼。如果該系統內容無法提供密碼，安裝程式會使用預設值 changeit。

這個密碼會根據萬能金鑰進行加密。

可信證書儲存區類型

指定可信證書儲存區路徑應使用 Java 金鑰儲存區 (JKS) 還是 PKCS12 進行數位簽章。

NetIQ Sentinel 數位簽名證書與金鑰

本節定義可讓 Identity Manager 與 Sentinel 通訊以進行事件稽核的值。僅當您選取了顯示進階選項時，公用程式才會顯示這些設定。

Sentinel 數位簽名證書

列出您希望 OAuth 伺服器用來驗證傳送至 Sentinel 之稽核訊息的自訂公用金鑰證書。

Sentinel 數位簽名私密金鑰

指定您希望 OAuth 伺服器用來驗證傳送至 Sentinel 之稽核訊息的自訂私密金鑰檔案所在的路徑。

其他

僅當您選取了顯示進階選項時，公用程式才會顯示這些設定。

OCSP URI

指定當用戶端安裝使用線上證書狀態通訊協定 (OCSP) 時要使用的資源識別字串 (URI)。例如 `http://host:port/ocspLocal`。

OCSP URI 會在線上更新可信證書的狀態。

授權組態路徑

指定授權組態檔案的完全合格名稱。

Identity Vault 索引

在安裝期間，指定是否希望安裝程式建立 `manager` 和 `srvprvUUID` 屬性的索引。安裝後，您可以修改設定，以指向索引的新位置。對於此項設定，請注意以下事項：

- ◆ 如果沒有建立這些屬性的索引，Identity Applications 使用者可能會遇到 Identity Applications 效能不佳的問題。
- ◆ 您可以在安裝 Identity Applications 後使用 Identity Console 來手動建立這些索引。
- ◆ 為取得最佳效能，您應該在安裝期間建立索引。
- ◆ 僅當索引處於線上模式時，您才可將 Identity Applications 提供給使用者使用。
- ◆ 若要建立或刪除索引，您還必須指定伺服器 DN 的值。

伺服器 DN

僅當您要建立或刪除 Identity Vault 索引時才適用。

指定要在其中建立或移除索引的 eDirectory 伺服器。

一次只能指定一個伺服器。若要在多個 eDirectory 伺服器上設定索引，必須執行 RBPM 組態公用程式多次。

重新啟始化 RBPM 安全性

指定是否要在安裝程序完成時重設 RBPM 安全性。您還必須重新部署 Identity Applications。

IDMReport URL

指定 Identity Manager Reporting Module 的 URL。例如 `http://hostname:port/IDMRPT`。

自訂主題網路位置名稱

指定要用於在瀏覽器中顯示 Identity Applications 的自訂主題名稱。

記錄訊息識別碼字首

指定要在 idmuserapp_logging.xml 檔案內 CONSOLE 和 FILE 附加器的配置模式中使用的值。預設值為 RBPM。

變更 RBPM 網路位置名稱

指定是否要變更 RBPM 的網路位置名稱。

您還必須指定角色與資源驅動程式的新名稱和 DN。

RBPM 網路位置名稱

僅當您選取了變更 RBPM 網路位置名稱時才適用。

指定 RBPM 的新網路位置名稱。

角色驅動程式 DN

僅當您選取了變更 RBPM 網路位置名稱時才適用。

指定角色與資源驅動程式的 DN。

容器物件

這些參數僅在安裝期間適用。

此區段可協助您定義容器物件的值，或建立新的容器物件。

已選定

指定您要使用的容器物件類型。

容器物件類型

指定容器：地域性、國家 / 地區、組織單位、組織或網域。

您也可以在 Identity Console 中定義自己的容器，然後在新增容器物件下新增該容器。

容器屬性名稱

設定與指定容器物件類型關聯之屬性類型的名稱。

新增新容器物件：容器物件類型

指定 Identity Vault 中可用做新容器之物件類別的 LDAP 名稱。

新增新容器物件：容器屬性名稱

指定與新容器物件類型關聯之屬性類型的名稱。

Reporting 參數

在設定 Identity Applications 時，此索引標籤定義用於管理 Identity Reporting 的值。當您安裝 Identity Reporting 時，公用程式會新增此索引標籤。

該索引標籤預設會顯示基本選項。若要查看所有設定，請按一下顯示進階選項。此索引標籤包含以下幾組設定：

- ◆ 「電子郵件傳送組態」(第 78 頁)
- ◆ 「報告保留值」(第 79 頁)
- ◆ 「修改地區設定」(第 79 頁)
- ◆ 「職能組態」(第 79 頁)
- ◆ 「傳出代理」(第 79 頁)

電子郵件傳送組態

本節定義用於傳送通知的值。

SMTP 伺服器主機名稱

指定您希望 Identity Reporting 在傳送通知時應使用之電子郵件伺服器的 DNS 名稱或 IP 位址。請不要使用 localhost。

SMTP 伺服器連接埠

指定 SMTP 伺服器的連接埠號。

SMTP 使用 SSL

指定是否要使用 TLS/SSL 通訊協定來與電子郵件伺服器通訊。

伺服器需要驗證

指定是否要對電子郵件伺服器通訊使用驗證。

SMTP 使用者名稱

指定要用來進行驗證的電子郵件地址。

您必須指定一個值。如果伺服器不需要驗證，則可指定無效的位址。

SMTP 使用者密碼

僅當您指定了伺服器需要驗證時才適用。

指定 SMTP 使用者帳戶的密碼。

預設電子郵件地址

指定您希望 Identity Reporting 用做電子郵件通知來源的電子郵件地址。

報告保留值

本節定義用於儲存已完成報告的值。

報告單位，報告生命期間

指定 Identity Reporting 在刪除已完成報告之前應保留這些報告的時間。例如，若要指定六個月，請在**報告生命期間**欄位中輸入 6，然後在**報告單位**欄位中選取月。

報告的位置

指定要用來儲存報告定義的路徑。例如，C:\NetIQ\idm\apps\IdentityReporting。

修改地區設定

本節定義您希望 Identity Reporting 使用的語言值。Identity Reporting 在搜尋中會使用特定的地區設定。如需詳細資訊，請參閱《[Administrator Guide to NetIQ Identity Reporting](#)》(NetIQ Identity Reporting 管理員指南)。

職能組態

本節定義 Identity Reporting 用來產生報告之驗證來源的值。

新增驗證來源

指定您要為報告功能新增的驗證來源類型。驗證來源可以是

- ◆ 預設值
- ◆ LDAP 目錄
- ◆ 檔案

傳出代理

本節定義了要使用供 Identity Reporting 用來下載報告的反向代理伺服器所需指定的值。

使用代理

指定該選項會為報告功能使用反向代理伺服器。

- ◆ 主機名稱或 IP 位址
- ◆ Port (連接埠)
- ◆ 使用 TLS

僅當您要使用 TCP 做為網路通訊協定時適用。

驗證參數

在設定 Identity Applications 時，此索引標籤定義 Tomcat 用於將使用者導向至 Identity Applications 和密碼管理頁面的值。

該索引標籤預設會顯示基本選項。若要查看所有設定，請按一下顯示進階選項。此索引標籤包含以下幾組設定：

- ◆ 「驗證伺服器」(第 80 頁)
- ◆ 「驗證組態」(第 81 頁)
- ◆ 「驗證方法」(第 81 頁)
- ◆ 「密碼管理」(第 82 頁)
- ◆ 「Sentinel 數位簽名證書和金鑰」(第 83 頁)

驗證伺服器

本節定義 Identity Applications 用於連接驗證伺服器的設定。

OAuth 伺服器主機識別碼

必需

指定向 OSP 發出記號之驗證伺服器的相對 URL。例如 192.168.0.1。

OAuth 伺服器 TCP 連接埠

指定驗證伺服器的連接埠。

Access Manager 是 OAuth 提供者

不支援透過組態更新公用程式的「驗證」索引標籤將 OAuth 從 OSP 轉換為 NAM。若要隱藏此選項，請在 configupdate.sh.properties 檔案中將 no_nam_oauth 的值設定為 "true"。

OAuth 伺服器正在使用 TLS/SSL

指定驗證伺服器是否使用 TLS/SSL 通訊協定進行通訊。

選擇性 TLS/SSL 可信證書儲存區檔案

僅當您選取了 OAuth 伺服器正在使用 TLS/SSL，並且公用程式顯示了進階選項時才適用。

選擇性 TLS/SSL 可信證書儲存區密碼

僅當您選取了 OAuth 伺服器正在使用 TLS/SSL，並且公用程式顯示了進階選項時才適用。

指定用於載入 TLS/SSL 驗證伺服器之金鑰儲存區檔案的密碼。

附註：如果您未指定金鑰儲存區路徑和密碼，並且驗證伺服器的信任證書不在 JRE 可信證書儲存區 (cacerts) 中，則 Identity Applications 無法連接到使用 TLS/SSL 通訊協定的驗證服務。

驗證組態

本節定義驗證伺服器的設定。

管理員容器的 LDAP DN

必需

指定 Identity Vault 中包含 OSP 必須驗證之任何管理員使用者物件的容器可辨識名稱。例如 `ou=sa,o=data`。

重複的解析命名屬性

指定用於區分 `cn` 值相同的多個 eDirectory 使用者物件的 LDAP 屬性名稱。預設值為 `mail`。

將驗證來源限制為網路位置

指定是要將 Identity Vault 中使用者和管理員容器內進行的搜尋限制為僅涵蓋這些容器中的使用者物件，還是讓搜尋範圍也涵蓋子容器。

工作階段逾時 (分鐘)

指定當使用者的工作階段處於非使用中狀態多少分鐘後，伺服器應使該工作階段逾時。其預設值為 20 分鐘。

存取記號生命期間 (秒)

指定 OSP 存取記號保持有效的秒數。預設值是 60 秒。

重新整理記號生命期間 (小時)

指定 OSP 重新整理記號保持有效的秒數。重新整理記號供 OSP 內部使用。預設值為 48 小時。

驗證方法

本節定義可讓 OSP 對登入 Identity Manager 瀏覽器元件的使用者進行驗證的值。

方法：

指定您希望 Identity Manager 在使用者登入時使用的驗證類型。

- ◆ **名稱與密碼**：OSP 向 Identity Vault 驗證的資訊。
- ◆ **Kerberos**：OSP 接受來自 Kerberos 票證伺服器和 Identity Vault 的驗證。您還必須指定對應屬性名稱的值。
- ◆ **SAML 2.0**：OSP 接受來自 SAML 身分提供者和 Identity Vault 的驗證。您還必須指定對應屬性名稱和中繼資料 URL 的值。

對應屬性名稱

僅當您指定了 Kerberos 或 SAML 時才適用。

指定要對應到 Kerberos 票證伺服器或身分提供程式中 SAML 表示的屬性名稱。

中繼資料 URL

僅當您指定了 SAML 時才適用。

指定 OSP 用來將驗證要求重新導向至 SAML 的 URL。

密碼管理

本節定義可讓使用者透過自助操作形式修改其密碼的值。

密碼管理提供程式

指定要使用的密碼管理系統類型。

使用者應用程式 (舊版)：使用 Identity Manager 慣常所用的密碼管理程式。此選項還允許您使用外部密碼管理程式。

Self Service Password Reset (SSPR)：使用 Identity Applications 隨附的 NetIQ Self Service Password Reset 服務，該服務可協助使用者重設其密碼，而無需管理人員介入。您可以選取要在 Identity Applications 儀表板登入頁面上顯示的連結，讓使用者能夠根據要求選取用於重設登入存取方式的適當動作。如需詳細資訊，請參閱「[使用者介面](#)」(第 82 頁)。

SSPR 是密碼管理提供程式欄位中的預設選項。

忘記密碼

僅當您選取了使用者應用程式 (舊版) 時，此功能表清單才適用。

指定您要使用使用者應用程式中整合的密碼管理系統，還是要使用外部系統。

- ◆ **內部：**使用預設的內部密碼管理功能。/jsps/pwdmgt/ForgotPassword.jsp (開頭不加 http(s) 通訊協定)。這會將使用者重新導向至「使用者應用程式」內建的「忘記密碼」功能，而不是外部 WAR。
- ◆ **外部：**使用外部忘記密碼 WAR 透過 Web 服務回呼使用者應用程式。您還必須指定外部系統的設定。

忘記密碼連結

僅當您要使用外部密碼管理系統時才適用。

指定指向「忘記密碼」功能頁面的 URL。在外部或內部密碼管理 WAR 中指定 ForgotPassword.jsp 檔案。

忘記密碼返回連結

僅當您要使用外部密碼管理系統時才適用。

指定使用者在執行完忘記密碼操作後可以使用的忘記密碼返回連結的 URL。

忘記密碼 Web 服務 URL

僅當您要使用外部密碼管理系統時才適用。

指定外部忘記密碼 WAR 將用來回呼至使用者應用程式，以執行核心忘記密碼功能的 URL。請使用以下格式：

```
https://<idmhost>:<sslport>/<idm>/  
pwdmgt/service
```

使用者介面

僅當您選取了 Self Service Password Reset (SSPR) 時，此功能表清單才適用。

指定要在 Identity Applications 儀表板登入頁面上顯示的連結。預設選項「無法登入？」顯示用於重設使用者名稱或密碼，或者在登入頁面上註冊存取許可權的通用連結。如果您選取無，則使用者無法自行重設密碼。

選取「其他連結」後，可選取以下選項：

- ◆ **忘記密碼**：提供一個連結，當現有使用者忘記其密碼時，可以按一下該連結重設密碼。
- ◆ **忘記使用者名稱**：提供一個連結，當現有使用者忘記其使用者名稱時，可以按一下該連結重設使用者名稱。
- ◆ **啟用帳戶**：提供一個連結，使用者可以按一下該連結建立用於存取 Identity Applications 的新使用者帳戶。

Sentinel 數位簽名證書和金鑰

本節定義可讓 Identity Manager 與 Sentinel 通訊以進行事件稽核的值。

Sentinel 數位簽名證書

指定您希望 OSP 伺服器用來驗證傳送至稽核系統之稽核訊息的自訂公用金鑰證書。

如需為 Novell Audit 設定證書的資訊，請參閱《[Novell Audit Administration Guide](#)》(Novell Audit 管理指南) 中的「[Managing Certificates](#)」(管理證書)。

Sentinel 數位簽名私密金鑰

指定您希望 OSP 伺服器用來驗證傳送至稽核系統之稽核訊息的自訂私密金鑰檔案所在的路徑。

SSO 用戶端參數

在設定 Identity Applications 時，此索引標籤定義用於管理對應用程式進行單一登入存取的值。

該索引標籤預設會顯示基本選項。若要查看所有設定，請按一下顯示進階選項。此索引標籤包含以下幾組設定：

- ◆ 「IDM 儀表板」(第 83 頁)
- ◆ 「IDM 管理員」(第 84 頁)
- ◆ 「RBPM」(第 84 頁)
- ◆ 「報告」(第 85 頁)
- ◆ 「IDM 資料收集服務」(第 86 頁)
- ◆ 「DCS 驅動程式」(第 86 頁)
- ◆ 「Self Service Password Reset」(第 87 頁)

IDM 儀表板

本節定義使用者存取 Identity Manager 儀表板所需的 URL 值，儀表板是 Identity Applications 的初始登入位置。

IDM 儀表板	
OAuth 用戶端 ID	idmdash
OAuth 用戶端機密	*****
OSP OAuth 重新導向 URL	https://192.168.0.1:8543/idmdash/oauth.html

OAuth 用戶端 ID

必需

指定用於供驗證伺服器識別儀表板的單一登入用戶端的名稱。預設值為 idmdash。

OAuth 用戶端密碼

必需

指定儀表板的單一登入用戶端的密碼。

OSP OAuth 重新導向 URL

必需

指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。

請使用以下格式：通訊協定：// 伺服器：連接埠 / 路徑。例如，https://192.168.0.1:8543/idmdash/oauth.html。

IDM 管理員

本節定義使用者存取 Identity Manager 管理員頁面所需 URL 的值。

OAuth 用戶端 ID

必需

指定用於供驗證伺服器識別 Identity Manager 管理員單一登入用戶端的名稱。預設值為 idmadmin。

OAuth 用戶端密碼

必需

指定 Identity Manager 管理員單一登入用戶端的密碼。

OSP OAuth 重新導向 URL

必需

指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。

請使用以下格式：通訊協定：// 伺服器：連接埠 / 路徑。例如，https://192.168.0.1:8543/idmadmin/oauth.html。

RBPM

本節定義使用者在存取使用者應用程式時需要使用的 URL 值。

RBPM	
OAuth 用戶端 ID	rbpm
OAuth 用戶端機密	*****
抵達頁面的 URL 連結	/idmdash/#/landing
OSP OAuth 重新導向 URL	https://192.168.0.1:8543/IDMProv/oauth
RBPM 至 eDirectory SAML 的組態	無變更

OAuth 用戶端 ID

必需

指定用來供驗證伺服器識別使用者應用程式單一登入用戶端的名稱。預設值為 `rbpm`。

OAuth 用戶端密碼

必需

指定使用者應用程式單一登入用戶端的密碼。

抵達頁面的 URL 連結

必需

指定用於從使用者應用程式中存取儀表板的相對 URL。預設值為 `/landing`。

OSP OAuth 重新導向 URL

必需

指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。

請使用以下格式：通訊協定：`://` 伺服器：連接埠 / 路徑。例如，`https://192.168.0.1:8543/IDMProv/oauth`。

RBPM 至 eDirectory SAML 的組態

必需

指定 SSO 驗證所需的 RBPM 至 eDirectory SAML 設定。

報告

本節定義使用者在存取 Identity Reporting 時需要使用的 URL 值。僅當您將 Identity Reporting 新增到了 Identity Manager 解決方案時，公用程式才會顯示這些值。

報告	
OAuth 用戶端 ID	rpt
OAuth 用戶端機密	*****
抵達頁面的 URL 連結	/idmdash/#/landing
Identity Governance 的 URL 連結	
OSP OAuth 重新導向 URL	https://192.168.0.1:8543/IDMRPT/oauth.html

OAuth 用戶端 ID

必需

指定用來供驗證伺服器識別 Identity Reporting 單一登入用戶端的名稱。預設值為 `rpt`。

OAuth 用戶端密碼

必需

指定 Identity Reporting 單一登入用戶端的密碼。

抵達頁面的 URL 連結

必需

指定用於從 Identity Reporting 中存取儀表板的相對 URL。預設值為 /idmdash/#/landing。

如果您將 Identity Reporting 和 Identity Applications 分別安裝到了不同的伺服器上，請指定絕對 URL。請使用以下格式：通訊協定：// 伺服器：連接埠 / 路徑。例如，https://192.168.0.1:8543/IDMRPT/oauth。

OSP OAuth 重新導向 URL

必需

指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。

請使用以下格式：通訊協定：// 伺服器：連接埠 / 路徑。例如，https://192.168.0.1:8543/IDMRPT/oauth。

IDM 資料收集服務

本節定義使用者存取 Identity Manager 資料收集服務所需 URL 的值。

OAuth 用戶端 ID

必需

指定用於供驗證伺服器識別 Identity Manager 資料收集服務單一登入用戶端的名稱。預設值為 idmdcs。

OAuth 用戶端密碼

必需

指定 Identity Manager 資料收集服務單一登入用戶端的密碼。

OSP OAuth 重新導向 URL

必需

指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。

請使用以下格式：通訊協定：// 伺服器：連接埠 / 路徑。例如，https://192.168.0.1:8543/idmdcs/oauth.html。

DCS 驅動程式

本節定義用於管理資料收集服務驅動程式的值。

圖 4-1

DCS 驅動程式	
OAuth 用戶端 ID	dcsdrv
OAuth 用戶端機密	

OAuth 用戶端 ID

指定用來供驗證伺服器識別資料收集服務驅動程式單一登入用戶端的名稱。此參數的預設值為 dcsdrv。

OAuth 用戶端密碼

指定資料收集服務驅動程式單一登入用戶端的密碼。

Self Service Password Reset

本節定義使用者存取 SSPR 所需 URL 的值。

OAuth 用戶端 ID

必需

指定用來供驗證伺服器識別 SSPR 單一登入用戶端的名稱。預設值為 `sspr`。

OAuth 用戶端密碼

必需

指定 SSPR 單一登入用戶端的密碼。

OAuth 重新導向 URL

必需

指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。

請使用以下格式：通訊協定 : // 伺服器 : 連接埠 / 路徑。例如，`https://192.168.0.1:8543/sspr/public/oauth.html`。

CEF 稽核參數

本節定義用於管理 CEF 稽核參數的值。

傳送稽核事件

指定是否要使用 CEF 在 Identity Applications 中稽核事件。

目的地主機

指定稽核伺服器的 DNS 名稱或 IP 位址。

目的地連接埠

指定稽核伺服器的連接埠。

網路協定

指定稽核伺服器用來接收 CEF 事件的網路通訊協定。

使用 TLS

僅當您要使用 TCP 做為網路通訊協定時適用。

指定稽核伺服器是否設定為將 TLS 與 TCP 搭配使用。

中間事件儲存目錄

指定在將 CEF 事件傳送到稽核伺服器之前快取目錄的位置。

附註：請確定針對中繼事件儲存目錄設定了 `novlua` 許可權。否則，您將不能存取 `IDMDash` 和 `IDMProv` 應用程式，並且系統也不會在中繼事件儲存目錄中記錄 `OSP` 事件。例如，您可以使用 `chown novlua:novlua <directorypath>` 指令變更對該目錄的許可權和擁有權，其中，`<directorypath>` 是中繼事件儲存目錄。

部署適用於 Identity Applications 的 REST API

Identity Applications 元件整合了可在 Identity Applications 中啟用不同功能的多個 REST API。REST 服務使用 `OAuth2` 通訊協定來提供驗證。您可以透過瀏覽器或使用程序檔中的 `curl` 指令來呼叫這些 API，以自動執行管理任務。`idmappsdoc.war` 檔案中提供了 REST API 和相應文件。安裝 Identity Applications 時會自動部署該 `war` 檔案。如需詳細資訊，請參閱 REST API 文件。

若要存取安裝了 Identity Applications 的伺服器上的 REST API 文件，請在瀏覽器的網址列中指定 `https://<Identity Applications 伺服器名稱>:<連接埠>/idmappsdoc`。例如 `https://192.168.0.1:8543/idmappsdoc`。

使用 Oracle 服務名稱存取 Oracle 資料庫

您可以使用 Oracle 系統 ID (SID) 或 Oracle 服務名稱連接至 Oracle 資料庫。Identity Applications 安裝程式僅接受 SID。如果要使用服務名稱存取資料庫，請透過 SID 連接將 Identity Applications 安裝到資料庫例項。完成安裝後，請執行以下動作：

- 1 執行以下指令，以在 Oracle 資料庫中建立服務名稱：

```
alter system set service_names='SERVICE1' scope=both sid='*';
```

其中，`SERVICE 1` 是 Oracle 服務的名稱。

附註：您可以使用大寫或小寫指定服務名稱。並不會區分大小寫。

- 2 在 Tomcat 的 `server.xml` 檔案中修改 Oracle 資料來源詳細資料，以定義服務名稱：

```
url="jdbc:oracle:thin:@IP:PORT/service1"
```

- 3 重新啟動 Tomcat。
- 4 驗證 `catalina.out` 記錄檔案中是否包含該服務名稱。
- 5 驗證 Identity Applications 是否已正確連接至資料庫。

手動建立資料庫綱要

安裝 Identity Applications 時，您可以暫不執行連接到資料庫或在資料庫中建立表格的操作。如果您對資料庫沒有相應的許可權，則可能需要選取此選項。安裝程式將會建立一個 SQL 檔案，供您用來建立資料庫綱要。您也可以安裝後重新建立資料庫表，而無需重新安裝。為此，您需要刪除 Identity Applications 的資料庫，然後建立一個新的同名資料庫。

使用 SQL 檔案產生資料庫綱要

本節假設安裝程式已建立了一個可供您執行以產生資料庫綱要的 SQL 檔案。如果您沒有該 SQL 檔案，請參閱「[手動建立用於產生資料庫綱要的 SQL 檔案](#)」(第 89 頁)。

附註：請不要使用 SQL*Plus 來執行該 SQL 檔案。該檔案中的行長度超過了 4000 個字元。

- 1 停止應用程式伺服器。
- 2 登入資料庫伺服器。
- 3 刪除 Identity Applications 使用的資料庫。
- 4 建立一個與步驟 3 中刪除的資料庫同名的新資料庫。
- 5 導覽至安裝程序建立的 SQL 程序檔 (預設位於 / 安裝路徑 /userapp/sql 目錄中)。
- 6 (視情況而定) 對於 Oracle 資料庫，請在函數 CONCAT_BLOB 的定義後面插入一個反斜線 (/)。例如：

```
-- Changeset icfg-data-load.xml::700::IDMRBPM
CREATE OR REPLACE FUNCTION CONCAT_BLOB(A IN BLOB, B IN BLOB) RETURN BLOB
AS
    C BLOB;
BEGIN
    DBMS_LOB.CREATETEMPORARY(C, TRUE);
    DBMS_LOB.APPEND(C, A);
    DBMS_LOB.APPEND(C, B);
    RETURN c;
END;
/
```

- 7 讓資料庫管理員執行該 SQL 程序檔，以建立並設定使用者應用程式資料庫。
- 8 重新啟動 Tomcat。

手動建立用於產生資料庫綱要的 SQL 檔案

您可以在安裝後重新建立資料庫表，而無需重新安裝，也無需使用 SQL 檔案。本節的內容可協助您在沒有 SQL 檔案的情況下建立資料庫綱要。

- 1 停止 Tomcat。
- 2 登入代管 Identity Applications 資料庫的伺服器。
- 3 刪除現有的資料庫。
- 4 建立一個與您在步驟 3 中刪除的資料庫同名的新資料庫。
- 5 在文字編輯器中，開啟 NetIQ-Custom-Install.log 檔案 (預設位於 Identity Applications 的安裝根目錄中)。例如：

```
C:\NetIQ\idm\apps\UserApplication
```

- 6 在 NetIQ-Custom-Install.log 檔案中搜尋並複製以下指令：

```
C:\NetIQ\idm\jre\bin\java -Xms256m -Xmx256m -Dwar.context.name=IDMProv
-Ddriver.dn="cn=User Application Driver,cn=driverset1,o=system" -
Duser.container="o=data" -jar C:\NetIQ\idm\jre\liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase --
driver=org.postgresql.Driver --
classpath=C:\NetIQ\idm\apps\postgresql\postgresql-9.4.1212jdbc42.jar
C:\NetIQ\idm\apps\UserApplication\IDMProv.war --
changeLogFile=DatabaseChangeLog.xml --url="jdbc:postgresql://
localhost:5432/ idmuserappdb" --contexts="prov,newdb" --logLevel=info -
- logFile=C:\NetIQ\idm\apps\UserApplication\db.out --username=*****
-- password=***** update
```

7 登入安裝了 Identity Applications 資料庫的伺服器。

8 在終端機中，貼上您複製的指令字串。

附註：該指令應為 updateSQL。如果指令是 update，請將其變更為 updateSQL。

9 在該指令中，將代表資料庫使用者名稱和密碼的星號 (*) 取代為進行驗證所需的實際值。此外，請確保 SQL 檔案名稱是唯一的。

10 執行指令。

11 (視情況而定) 如果安裝程序產生了一個 SQL 檔案，而不是在資料庫中填入資料，請將該檔案提供給資料庫管理員，讓其將該檔案輸入至資料庫伺服器。如需詳細資訊，請參閱「使用 SQL 檔案產生資料庫綱要」(第 89 頁)。

12 在資料庫管理員輸入該 SQL 檔案後，啟動 Tomcat。

組態 Identity Applications 的單一登入設定

安裝程序會安裝用於在 Identity Manager 中進行單一登入存取的驗證服務 (OSP)。不過，您也可以將 OSP 驗證伺服器設定為接受來自 Kerberos 票證伺服器或 SAML 的驗證。若要在安裝後組態 Identity Applications 的單一登入設定，請參閱《[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)》(NetIQ Identity Manager - Identity Applications 管理員指南) 中的「[Configuring Single Sign-on Access in Identity Manager](#)」(在 Identity Manager 中設定單一登入存取)。

啟動 Identity Applications

設定 Identity Applications 之後，請務必重新啟動 Tomcat 和 ActiveMQ 服務。

```
systemctl restart netiq-tomcat
```

```
systemctl restart netiq-activemq
```

Identity Applications 的組態和使用考量

在設定和初次使用 Identity Applications 時，需注意以下事項。

- 安裝過程中，安裝程式會將記錄檔案寫入安裝目錄。這些檔案包含組態的相關資訊。設定 Identity Applications 環境之後，您應考慮刪除這些記錄檔案，或將其儲存在安全位置。安裝過程中，您可以選擇將資料庫綱要寫入檔案。由於此檔案包含資料庫的描述性資訊，因此安裝程序完成後，您應將其移至安全的位置。
- (視情況而定) 若要稽核 Identity Applications，必須在環境中安裝 Identity Reporting 和稽核服務，並將其設定為擷取事件。此外，您還必須對 Identity Applications 進行設定以支援稽核。
- 只有在您完成以下活動之後，使用者才能存取 Identity Applications：
 - 確保已安裝所有必要的 Identity Manager 驅動程式。
 - 在所有瀏覽器上啟用 Cookie。如果停用 Cookie，應用程式將無法運作。
- 如果您將 Identity Applications 和 SSPR 安裝在不同的伺服器上，則必須將 CN 為 Identity Applications 的 SSPR 可信證書輸入至 Identity Applications 伺服器的 cacerts 中。

設定資料收集的執行時期環境

本節提供為確保執行時期環境正常運作，您應執行的額外組態步驟的相關資訊。此外，本節還提供了一些疑難排解方法，以及關於特定用途資料庫表格的一些資訊。

此程序包括以下活動：

- 「將資料收集服務驅動程式設定為從 Identity Applications 收集資料」(第 92 頁)
- 「移轉資料收集服務驅動程式」(第 93 頁)
- 「新增對自訂屬性和物件的支援」(第 95 頁)
- 「新增多個驅動程式集支援」(第 97 頁)
- 「將驅動程式設定為使用 SSL 在遠端模式下執行」(第 99 頁)

如果一或多個驅動程式出現了難以解釋的問題，請參閱《NetIQ Identity Reporting Module Guide》(NetIQ Identity Reporting Module 指南)中的「[Troubleshooting the Drivers](#)」(驅動程式疑難排解)。

將資料收集服務驅動程式設定為從 Identity Applications 收集資料

若要使 Identity Applications 與 Identity Reporting 正常配合運作，必須將 DCS 驅動程式設定為支援 OAuth 通訊協定。

附註：

- ◆ 僅當在環境中使用了 Identity Reporting 時，才需要安裝並設定 DCS 驅動程式。
 - ◆ 如果在環境中設定了多個 DCS 驅動程式，則必須針對每個驅動程式完成以下步驟。
-

- 1 登入 Designer 。
- 2 在 Designer 中開啟您的專案。
- 3 (視情況而定) 如果您尚未將 DCS 驅動程式升級至支援的修補程式版本，請完成以下步驟：
 - 3a 下載最新的 DCS 驅動程式修補程式檔案。
 - 3b 將該修補程式檔案擷取到伺服器上的某個位置。
 - 3c 在終端機中，導覽至適用於您環境之修補程式 RPM 的擷取位置，然後執行以下指令：

```
rpm -Uvh novell-DXMLdcs.rpm
```
 - 3d 重新啟動 Identity Vault 。
 - 3e 在 Designer 中，確保已安裝受支援版本的資料收集服務基礎套件。如果需要，請安裝最新版本，然後再繼續。
 - 3f 在 Designer 中重新部署並重新啟動 DCS 驅動程式。
- 4 在大綱檢視窗中，於 DCS 驅動程式上按一下滑鼠右鍵，然後選取內容。
- 5 按一下驅動程式組態。
- 6 按一下驅動程式參數索引標籤。
- 7 按一下顯示連接參數，然後選取顯示。
- 8 按一下 SSO 服務支援，然後選取是。
- 9 指定 Identity Reporting 的 IP 位址和連接埠。
- 10 指定 SSO 服務用戶端的密碼。預設密碼為 driver 。
- 11 按一下「套用」，然後按一下「確定」。
- 12 在模型產生器檢視窗中，於 DCS 驅動程式上按一下滑鼠右鍵，然後選取驅動程式 > 部署。
- 13 按一下部署。
- 14 收到重新啟動 DCS 驅動程式的提示時，按一下是。
- 15 按一下「確定」。

移轉資料收集服務驅動程式

若要將物件同步化至身分資訊倉儲中，您必須移轉資料收集服務驅動程式。

- 1 登入 Identity Console。
- 2 在 **IDM 管理磚** 中，選取「資料收集服務驅動程式」並移至**資料轉換和同步**。
- 3 在資料同步檢視中，選取從 **Identity Vault** 移轉。
- 4 選取包含相關資料的組織，然後按一下**啟動**。

附註：移轉程序可能需要花費幾分鐘時間，具體視您的資料量而定。請務必在移轉程序完成後再繼續下一步。

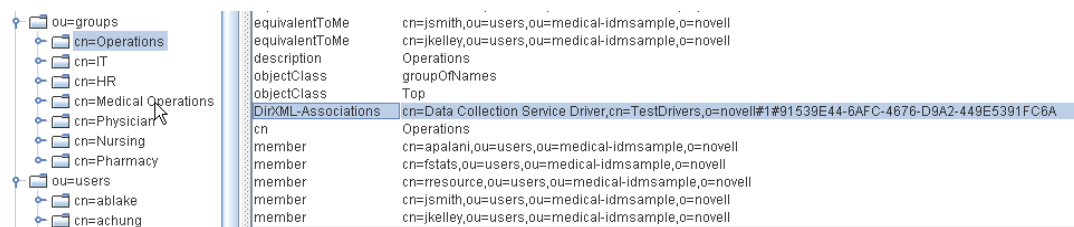
- 5 等待移轉程序完成。
- 6 確保 **idmrpt_identity** 和 **idmrpt_acct** 表格 (提供關於 Identity Vault 中身分和帳戶的資訊) 中包含以下類型的資訊：

	identity_id	first_name	last_name	middle_initial	full_name	job_title	department	location	email_address	office_phone	cell_phone
	[PK] character varying(128)	character varying(12)	character varying(12)	character var	character var	character var	character var	character var	character var	character var	character var
1	6210e8e9b55e4	Allison	Blake			Payroll		Northeast	pfredrickson@n...	(555) 555-1222	
2	05f6a12667734	Ned	North			Senior Physician		Northeast	pfredrickson@n...	(555) 555-1211	
3	1282ce7c69cb4	Fred	Stats			Purchasing Adm		Northeast	pfredrickson@n...	(555) 555-1230	
4	13bd8ba9f0494	Kevin	Chester			Benefits Adminis		Northeast	pfredrickson@n...	(555) 555-1221	
5	13faf90666584	Ken	Carson			Attending Physi		Northeast	pfredrickson@n...	(555) 555-1315	
6	1c886916cfd24	Jane	Smith			Administrative A		Northeast	pfredrickson@n...	(555) 555-1234	
7	1e8e3fcb7364	Application Administrator	Of Sample Data								
8	24fd8b301bce4	Bill	Burke			Administrative A		cn-loc1	pfredrickson@n...	(555) 555-1210	
9	278698aace6b4	April	Smith			Nurse		Northeast	pfredrickson@n...	(555) 555-1319	
10	2d8df9981b1c4	Brad	Jones			Resident Physi		Northeast	pfredrickson@n...	(555) 555-1313	

- 7 在 LDAP 瀏覽器中，驗證移轉程序是否新增了對 DirXML-Associations 的以下參考：
- ◆ 對於每個使用者，驗證以下類型的資訊：

LDAP Browser/Editor v2.8.2	
File	Edit
View	LDIF
Help	
ou=users	Attribute
cn=ablake	employeeType
cn=achung	ACL
cn=apalani	ACL
cn=asmith	6#entry#cn=kcarsen,ou=users,ou=medical-idmsample,o=novell#loginScript
cn=aspencer	6#entry#cn=kcarsen,ou=users,ou=medical-idmsample,o=novell#printJobConfiguration
cn=bbender	DirXML-Associations
cn=bbrown	cn=Data Collection Service Driver,cn=TestDrivers,o=novell#1#C53ADD67-DB19-4DD2-9482-67DD3AC519DB
cn=bburke	givenName
cn=bjenner	photo
cn=bjones	snprvYahoolMAddress
cn=cblack	inetOrgPerson
cn=ccentral	objectClass
cn=cnano	organizationalPerson
cn=eeuro	objectClass
cn=efstats	Person
cn=jbrown	objectClass
cn=jkelly	ndsLoginProperties
cn=jmiller	objectClass
cn=jsmith	Top
cn=kwest	objectClass
cn=kcarsen	snprvUserAux
cn=kchang	objectClass
cn=kcheater	snprvEntityAux
cn=kkeller	homeInfo
	objectClass
	sampleUserDeviceAux
	test
	employeeStatus
	costCenter
	ou
	medical
	securityEquals
	cn=Medical Operations,ou=groups,ou=medical-idmsample,o=novell
	securityEquals
	cn=Physician,ou=groups,ou=medical-idmsample,o=novell
	uid
	kcarsen
	mail
	pfredrickson@novell.com
	cn
	kcarsen
	passwordAllowChange
	TRUE
	sampleDeviceDN
	cn=kcarsen-laptop,ou=devices,ou=medical-idmsample,o=novell

- ◆ 對於每個群組，驗證以下類型的資訊：



- 8 確保 **idmrpt_group** 表格中的資料看上去類似於以下資訊：

group_name	group_desc	dynamic_group	dynamic_rule	nested_group	idmrpt_valid_from	idmrpt_deleted	idmrpt_syn_state
character var	character var	boolean	character var	boolean	timestamp without time zone	boolean	smallint
Pharmacy	Pharmacy	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
IT	Information Tec	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
HR	Human Resources	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Physician	Physician	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Operations	Operations	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Medical Operations	Medical Operations	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Nursing	Nursing	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1

此表格會顯示每個群組的名稱，以及用於指示群組是動態群組還是巢狀群組的旗標。此外，它還會顯示群組是否已移轉。如果某個物件在使用者應用程式中已被修改但尚未移轉，則同步化狀態 (**idmrpt_syn_state**) 可能會設定為 0。例如，如果在群組中新增了使用者，並且尚未移轉驅動程式，那麼，此值可能會設定為 0。

- 9 (選擇性) 驗證以下表格中的資料：

- ◆ **idmrpt_approver**
- ◆ **idmrpt_association**
- ◆ **idmrpt_category**
- ◆ **idmrpt_container**
- ◆ **idmrpt_idv_drivers**
- ◆ **idmrpt_idv_prd**
- ◆ **idmrpt_role**
- ◆ **idmrpt_resource**
- ◆ **idmrpt_sod**

- 10 (選擇性) 驗證 **idmrpt_ms_collect_state** 表格現在是否包含列。此表格顯示有關受管理系統間道驅動程式的資料收集狀態資訊。

此表格包含針對受管理系統已執行之 REST 端點的相關資料。此時，該表格不包含任何列，因為您尚未啟動此驅動程式的收集程序。

新增對自訂屬性和物件的支援

您可以對資料收集服務驅動程式進行設定，使其收集和保留不屬於預設資料收集規劃之自訂屬性與物件的資料。要進行此設定，您需要修改資料收集服務驅動程式過濾器。修改過濾器不會立即觸發物件同步化，而是會在 Identity Vault 中發生新增、修改或刪除事件時，向資料收集服務傳送新增的屬性和物件。

在新增對自訂屬性和物件的支援時，您需要修改報告，以包括延伸的屬性和物件資訊。以下檢視窗提供有關延伸物件和屬性的目前資料及歷史資料：

- [idm_rpt_cfg.idmrpt_ext_idv_item_v](#)
- [idm_rpt_cfg.idmrpt_ext_item_attr_v](#)

此程序包括以下活動：

- [「將驅動程式設定為使用延伸物件」 \(第 95 頁\)](#)
- [「包含資料庫中的名稱和描述」 \(第 96 頁\)](#)
- [「將延伸屬性新增至已知物件類型」 \(第 96 頁\)](#)

將驅動程式設定為使用延伸物件

您可將任何物件或屬性新增至資料收集服務過濾器規則。在新增新物件或屬性時，請務必依照以下範例所示對應 GUID (subscriber 為 sync) 和物件類別 (subscriber 為 notify)：

```
<filter-class class-name="Device" publisher="ignore" publisher-create-homedir="true" publisher-track-template-member="false" subscriber="sync">
<filter-attr attr-name="CN" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Description" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="GUID" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Object Class" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="notify"/>
<filter-attr attr-name="Owner" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Serial Number" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="sampleDeviceModel" from-all-classes="true" merge-authority="default" publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="sampleDeviceType" from-all-classes="true" merge-authority="default" publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
</filter-class>
```

包含資料庫中的名稱和描述

如果您希望物件包含資料庫中的名稱和描述，則需要為 `_dcsName` 和 `_dcsDescription` 新增一個綱要對應規則。該綱要對應規則會將物件例項的相關屬性值分別與 `idmrpt_ext_idv_item.item_name` 和 `idmrpt_ext_idv_item.item_desc` 欄對應。如果您未新增綱要對應規則，屬性將會填入子表格 `idmrpt_ext_item_attr` 中。

例如：

```
<attr-name class-name="Device">
<nds-name>CN</nds-name>
<app-name>_dcsName</app-name>
</attr-name>
<attr-name class-name="Device">
<nds-name>Description</nds-name>
<app-name>_dcsDescription</app-name>
</attr-name>
```

下面是一個可顯示資料庫中這些物件和屬性值的 SQL 範例：

```
SELECT
    item.item_dn,
    item.item_name,
    item.item_desc,
    attr.attribute_name,
    itemAttr.attribute_value,
    item.idmrpt_deleted as item_deleted,
    itemAttr.idmrpt_deleted as attr_deleted,
    item.item_desc,
    obj.object_class
FROM
    idm_rpt_data.idmrpt_ext_idv_item as item,
    idm_rpt_data.idmrpt_ext_item_attr itemAttr, idm_rpt_data.idmrpt_ext_attr
as attr, idm_rpt_data.idmrpt_ext_obj as obj
WHERE
    item.object_id = obj.object_id and itemAttr.attribute_id =
    attr.attribute_id and itemAttr.cat_item_id = item.item_id
ORDER BY
    item.item_dn, item.item_name
```

將延伸屬性新增至已知物件類型

如果某個屬性已新增至針對資料收集服務驅動程式的過濾器規則中，但未明確與 XML 參考檔案 (`IdmrptIdentity.xml`) 中的報告資料庫對應，系統會在 `idmrpt_ext_item_attr` 表格中填入並維護值，並在 `idmrpt_ext_attr` 表格中新增一個屬性參考。

以下 SQL 範例可顯示這些延伸屬性：

```

SELECT
    acct.idv_acct_dn,
    attrDef.attribute_name,
    attribute_value,
    attrVal.idmrpt_valid_from,
    cat_item_attr_id,
    attrVal.idmrpt_deleted,
    attrVal.idmrpt_syn_state
FROM
    idm_rpt_data.idmrpt_ext_item_attr as attrVal,
    idm_rpt_data.idmrpt_ext_attr as attrDef, idm_rpt_data.idmrpt_identity as
idd, idm_rpt_data.idmrpt_idv_acct as acct
WHERE attrVal.attribute_id = attrDef.attribute_id and idd.identity_id =
acct.identity_id and attrVal.cat_item_id = acct.identity_id and
cat_item_type_id = 'IDENTITY'

```

除了使用者物件以外，您還可將延伸屬性新增至針對以下物件的過濾器規則中，並在資料庫中填入這些屬性：

- ◆ nrfRole
- ◆ nrfResource
- ◆ 容器

附註：安裝的產品會提供對 organizationUnit、Organization 和 Domain 的支援。容器類型在 idmrpt_container_types 表格中維護。

- ◆ 群組
- ◆ nrfSod

您可以查看 idmrpt_cat_item_types.idmrpt_table_name 欄，來瞭解延伸屬性與父表格或父物件之間的關聯。此欄描述如何將 idm_rpt_data.idmrpt_ext_item_attr.cat_item_id 欄聯結到父表格的主鍵。

新增多個驅動程式集支援

資料收集服務範圍套件 (NOVLDCCSSCPNG) 為包含多個驅動程式集和多組資料收集服務驅動程式及受管理系統閘道驅動程式的企業環境提供靜態和動態範圍功能。

在安裝期間或安裝之後，您需要確定要在其上安裝該套件的資料收集服務驅動程式的角色。您需要選取下列其中一個角色：

- ◆ **主要** 驅動程式將會同步化所有資訊，但其他驅動程式集的子網路樹除外。主要資料收集服務驅動程式可以正常為整個 Identity Vault 提供服務，或者可與一或多個次要驅動程式配合運作。
- ◆ **次要** 驅動程式只同步化自身的驅動程式集，不會同步化其他任何資訊。通常，次要資料收集服務驅動程式要求主要驅動程式在不同的驅動程式集中執行，否則，任何本地驅動程式集外部的資料都不會傳送至資料收集服務。
- ◆ **自訂** 允許管理員定義自訂的範圍規則。唯一的隱含範圍是本地驅動程式集，其他任何驅動程式若未明確新增至自訂範圍清單，都會被視為不在範圍內。自訂範圍是 Identity Vault 中應該同步化其從屬或子網路樹之容器的可辨識名稱 (採用斜線格式)。

只有如下所述的某些組態情境中才需要範圍套件：

- ◆ **單個伺服器與具有單個驅動程式集的 Identity Vault**：對於此情境，您不需要定義範圍，因此也就無需安裝範圍套件。
- ◆ **多個伺服器與具有單個驅動程式集的 Identity Vault**：對於此情境，您需要遵循以下指導準則：

- ◆ 確定 Identity Manager 伺服器存有要從中收集資料之所有分割區的複製本。
- ◆ 對於此情境，您不需要定義範圍，因此，請不要安裝範圍套件

- ◆ **多個伺服器與具有多個驅動程式集的 Identity Vault**：此情境中有兩個基本組態：

- ◆ 所有伺服器都存有要從中收集資料之所有分割區的複製本。

對於此組態，您需要遵循以下指導準則：

- ◆ 需要定義範圍，以免有多個 DCS 驅動程式處理同一項變更。
- ◆ 您需要在所有 DCS 驅動程式上安裝範圍套件。
- ◆ 您需要將一個 DCS 驅動程式選做主要驅動程式。
- ◆ 您需要將其他所有 DCS 驅動程式設定為次要驅動程式。

- ◆ 所有伺服器都未存有要從中收集資料之所有分割區的複製本。

此組態存在兩種可能的情況：

- ◆ 應從中收集資料的所有分割區 僅由一個 Identity Manager 伺服器存放

在此情況下，您需要遵循以下指導準則：

- ◆ 需要定義範圍，以免有多個 DCS 驅動程式處理同一項變更。
- ◆ 您需要在所有 DCS 驅動程式上安裝範圍套件。
- ◆ 您需要將所有 DCS 驅動程式都設定為主要驅動程式。

- ◆ 應從中收集資料的所有分割區 不是僅由一個 Identity Manager 伺服器存放 (部分分割區由多個 Identity Manager 伺服器存放) 。

在此情況下，您需要遵循以下指導準則：

- ◆ 需要定義範圍，以免有多個 DCS 驅動程式處理同一項變更。
- ◆ 您需要在所有 DCS 驅動程式上安裝範圍套件。
- ◆ 您需要將所有 DCS 驅動程式都設定為自訂驅動程式。

您需要為每個驅動程式定義自訂的範圍規則，並且務必不要建立任何重疊的範圍。

將驅動程式設定為使用 SSL 在遠端模式下執行

在以遠端模式執行時，您可以將資料收集服務驅動程式和受管理系統閘道驅動程式設定為使用 SSL。本節提供用於將驅動程式設定為使用 SSL 在遠端模式下執行的步驟。

若要使用受管理系統閘道驅動程式的金鑰儲存區設定 SSL：

- 1 在 Identity Console 中建立伺服器證書。
 - 1a 在 **eDirectory** 下，按一下**證書管理 > 伺服器證書管理**。
 - 1b 瀏覽到裝有受管理系統閘道驅動程式的伺服器物件並選取它。
 - 1c 指定證書綽號。
 - 1d 選取**標準建立方法**，然後按**下一步**。
 - 1e 按一下**完成**，然後按一下**關閉**。
- 2 使用 Identity Console 輸出伺服器證書。
 - 2a 在 **eDirectory** 下，按一下**證書管理 > 伺服器證書管理**。
 - 2b 選取**步驟 1 (第 99 頁)** 中建立的證書，然後按一下**輸出**。
 - 2c 在**證書功能表**中，選取該證書的名稱。
 - 2d 確保已核取**輸出私密金鑰**。
 - 2e 輸入密碼，然後按**下一步**。
 - 2f 按一下**儲存輸出的證書**，並儲存輸出的 pfx 證書。
- 3 將**步驟 2 (第 99 頁)** 中輸出的 pfx 證書輸入至 Java 金鑰儲存區。
 - 3a 使用 Java 隨附的 keytool。您必須使用 JDK 6 或更新版本。
 - 3b 在指令提示符處輸入以下指令：

```
keytool -importkeystore -srckeystore pfx certificate -srcstoretype PKCS12 -destkeystore Keystore Name
```

例如：

```
keytool -importkeystore -srckeystore cert.pfx -srcstoretype PKCS12 -destkeystore msgw.jks
```
 - 3c 接著系統會提示您輸入密碼。
- 4 使用 Identity Console 將受管理系統閘道驅動程式組態修改為使用金鑰儲存區。
 - 4a 在 **IDM 管理**中，按一下包含受管理系統閘道驅動程式的驅動程式集。
 - 4b 按一下受管理系統閘道驅動程式圖示並移至組態。
 - 4c 按一下**驅動程式參數**下拉式功能表。
 - 4d 在**驅動程式設定索引標籤**下，設定要顯示的**連接參數**，並將**驅動程式組態模式**設定為「遠端」。
 - 4e 輸入金鑰儲存區檔案的完整路徑和密碼。
 - 4f 儲存驅動程式並將其重新啟動。

- 5 使用 Identity Console 將資料收集服務驅動程式組態修改為使用金鑰儲存區。
 - 5a 在 **IDM** 管理中，按一下包含資料收集服務驅動程式的驅動程式集。
 - 5b 按一下資料收集服務驅動程式圖示並移至驅動程式組態。
 - 5c 按一下驅動程式參數下拉式功能表，並設定要顯示的註冊參數。
 - 5d 在受管理系統閘道註冊標題下，將受管理系統閘道驅動程式組態模式設定為「遠端」。
 - 5e 輸入金鑰儲存區的完整路徑、密碼以及在步驟 1c (第 99 頁) 中指定的別名。
 - 5f 儲存驅動程式並將其重新啟動。

設定 Identity Reporting

安裝 Identity Reporting 後，您仍可以修改許多安裝內容。若要進行變更，請執行組態更新公用程式 (configupdate.sh) 檔案。

如果使用組態工具變更了 Identity Reporting 的任何設定，您必須重新啟動 Tomcat 才能使變更生效。但是，在 Identity Reporting 的 Web 使用者介面中進行變更後，不需要新啟動伺服器。

- ◆ 「在「身分資料收集服務」頁面中手動新增資料來源」(第 100 頁)
- ◆ 「對 Oracle 資料庫執行報告」(第 101 頁)
- ◆ 「手動產生資料庫綱要」(第 101 頁)
- ◆ 「部署 Identity Reporting 的 REST API」(第 105 頁)
- ◆ 「連接遠端 Remote PostgreSQL 資料庫」(第 105 頁)
- ◆ 「Identity Reporting 的安裝後步驟」(第 106 頁)

在「身分資料收集服務」頁面中手動新增資料來源

1. 登入 Identity Reporting 應用程式。
2. 按一下資料來源。
3. 按一下新增。
4. 在新增資料來源對話方塊中，按一下從預定義清單中選取選項圓鈕。
5. 選取 **IDMDCSDataSource**。
6. 按一下儲存。

對 Oracle 資料庫執行報告

Identity Reporting 可讓您針對遠端 Oracle 資料庫執行報告。確定執行 Oracle 資料庫的伺服器上存在 `ojbc8.jar` 檔案。

手動產生資料庫綱要

若要在安裝後手動產生資料庫綱要，請對您的資料庫執行下列程序之一：

- 「針對 PostgreSQL 資料庫設定 `Create_rpt_roles_and_schemas.sql` 綱要」(第 101 頁)
- 「針對 Oracle 資料庫設定 `Create_rpt_roles_and_schemas.sql` 綱要」(第 102 頁)
- 「針對 MS SQL 資料庫設定 `Create_rpt_roles_and_schemas.sql` 綱要」(第 104 頁)
- 「清除資料庫檢查總數」(第 104 頁)

針對 PostgreSQL 資料庫設定 `Create_rpt_roles_and_schemas.sql` 綱要

- 1 使用位於 `C:\NetIQ\idm\apps\IdentityReporting\sql` 中的 `create_dcs_roles_and_schemas.sql` 和 `create_rpt_roles_and_schemas.sql` SQL，將必需的角色新增至資料庫中。
- 2 以 `postgres` 使用者身分登入 `PGAdmin`。
- 3 執行查詢工具。
- 4 若要建立 `Create_rpt_roles_and_schemas` 和 `Create_dcs_roles_and_schemas` 程序，請將這些 SQL 中的內容複製到查詢工具，然後對連接的資料庫執行指令。
- 5 若要建立 `IDM_RPT_DATA`、`IDM_RPT_CFG` 和 `IDMRPTUSER` 角色，請依給定順序執行以下指令：

```
Select CREATE_DCS_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_DATA>', '<Set  
pwd for IDMRPTUSER>');
```

```
Select CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>');
```

例如，如果 `IDM_RPT_DATA`、`IDMRPTUSER` 和 `IDM_RPT_CFG` 的密碼分別是 *password*、*password1* 和 *password2*，則您必須執行以下指令：

```
Select CREATE_DCS_ROLES_AND_SCHEMAS('password', 'password1');
```

```
Select CREATE_RPT_ROLES_AND_SCHEMAS('password2');
```

- 6 將 `C:\NetIQ\idm\apps\IdentityReporting\sql` 中 `get_formatted_user_dn.sql` 的內容複製到查詢工具中，然後對連接的資料庫執行這些指令。

附註：如果針對資料庫綱要建立選項選取檔案，則必須手動新增 `get_formatted_user_dn.sql` 函數。如果針對資料庫綱要建立選項選取現在或啟動，安裝程式會將此函數新增至資料庫。

針對 Oracle 資料庫設定 Create_rpt_roles_and_schemas.sql 綱要

- 1 以資料庫管理員使用者身分登入 SQL Developer。
- 2 建立 Create_rpt_roles_and_schemas，為此，請將以下 SQL 的內容複製到 SQL Developer，並針對連接的資料庫執行這些代碼：

```
alter session set "_ORACLE_SCRIPT"=true;

CREATE OR REPLACE PROCEDURE create_rpt_roles_and_schemas(
    idm_rpt_cfg_password character varying)
AUTHID CURRENT_USER
AS
    cnt number;
BEGIN
    /* Create user IDM_RPT_CFG if it does not exist */
    select count(*) into cnt from ALL_USERS WHERE USERNAME =
    'IDM_RPT_CFG';
    IF cnt = 0 THEN
        execute immediate 'CREATE USER idm_rpt_cfg IDENTIFIED BY ' ||
idm_rpt_cfg_password;
        DBMS_OUTPUT.put_line('Created user idm_rpt_cfg');
    END IF;

    /* Grant rights to the idm_rpt_cfg user */
    execute immediate 'GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW,
CREATE PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, UNLIMITED TABLESPACE
to idm_rpt_cfg';
    DBMS_OUTPUT.put_line('Granted rights to user idm_rpt_cfg');
    execute immediate 'alter session set "_ORACLE_SCRIPT"=true';
    execute immediate 'alter session set "_ORACLE_SCRIPT"=false';
END;
/
exec CREATE_RPT_ROLES_AND_SCHEMAS('Novell123');
/
alter session set "_ORACLE_SCRIPT"=false;
/
```

- 3 以系統使用者的身分登入，然後建立 Create_dcs_roles_and_schemas，為此，請將以下 SQL 的內容複製到 SQL Developer，並針對連接的資料庫執行這些代碼：

```
alter session set "_ORACLE_SCRIPT"=true;

CREATE OR REPLACE PROCEDURE create_dcs_roles_and_schemas(
    idm_rpt_data_password character varying,
    idmrptuser_password character varying)
AUTHID CURRENT_USER
AS
    cnt number;
BEGIN
    /* Create user IDM_RPT_DATA if it does not exist already */
    select count(*) into cnt from ALL_USERS WHERE USERNAME =
    'IDM_RPT_DATA';
    IF cnt = 0 THEN
        execute immediate 'CREATE USER idm_rpt_data IDENTIFIED BY ' ||
```

```

idm_rpt_data_password;
    DBMS_OUTPUT.put_line('Created user idm_rpt_data');
END IF;

/* Grant rights to the idm_rpt_data user */
execute immediate 'GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW,
CREATE PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, UNLIMITED TABLESPACE
to idm_rpt_data';
execute immediate 'GRANT CREATE PUBLIC SYNONYM to IDM_RPT_DATA';
execute immediate 'GRANT SELECT ON DBA_SEGMENTS TO IDM_RPT_DATA';
DBMS_OUTPUT.put_line('Granted rights to user idm_rpt_data');
/* Create user IDMRPTUSER if it does not exist */
select count(*) into cnt from ALL_USERS WHERE USERNAME =
'IDMRPTUSER';
IF cnt = 0 THEN
    execute immediate 'CREATE USER idmrptuser IDENTIFIED BY ' ||
idmrptuser_password;
    DBMS_OUTPUT.put_line('Created user idmrptuser');
END IF;

/* Grant rights to the idmrptuser user */
execute immediate 'GRANT CREATE SESSION to idmrptuser';
execute immediate 'GRANT SELECT ON sys.all_tables TO idmrptuser';
DBMS_OUTPUT.put_line('Granted rights to user idmrptuser');
END;
/

```

- 4 若要建立 IDM_RPT_CFG 角色，請執行以下指令：

```

begin
CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>');
end;

```

例如，如果 IDM_RPT_CFG 的密碼是 *password*，則您必須執行以下指令：

```

begin
CREATE_RPT_ROLES_AND_SCHEMAS('password');
end;

```

- 5 將 C:\NetIQ\idm\apps\IdentityReporting\sql 中 get_formatted_user_dn-oracle.sql 的內容複製到 SQL Developer 中，然後對連接的資料庫執行這些指令。

附註：如果針對資料庫網要建立選項選取檔案，則必須手動將 get_formatted_user_dn-oracle.sql 函數新增至資料庫。如果針對資料庫網要建立選項選取現在或啟動，安裝程式會將此函數新增至資料庫。

針對 MS SQL 資料庫設定 Create_rpt_roles_and_schemas.sql 綱要

- 1 執行 delete_create_dcs_roles_and_schemas-mssql.sql 和 delete_get_formatted_user_dn-mssql.sql。
- 2 使用 C:\NetIQ\idm\apps\IdentityReporting\sql 中的 create_dcs_roles_and_schemas.mssql 和 create_rpt_roles_and_schemas.mssql，將必需的角色新增至資料庫中。
- 3 以資料庫管理員使用者身分登入 SQL Developer。
- 4 若要建立 Create_rpt_roles_and_schemas 和 Create_dcs_roles_and_schemas 程序，請將 create_dcs_roles_and_schemas.mssql 和 create_rpt_roles_and_schemas.mssql 中的內容複製到 SQL Developer，然後對連接的資料庫執行這些指令。
- 5 若要建立 IDM_RPT_DATA、IDM_RPT_CFG 和 IDMRPTUSER 角色，請依給定順序執行以下指令：

```
execute CREATE_DCS_ROLES_AND_SCHEMAS '<設定 IDM_RPT_DATA 的密碼>', '<設定 IDMRPTUSER 的密碼>'
```



```
execute CREATE_DCS_ROLES_AND_SCHEMAS '<設定 IDM_RPT_DATA 的密碼>', '<設定 IDMRPTUSER 的密碼>'
```
- 6 將 C:\NetIQ\idm\apps\IdentityReporting\sql 中 get_formatted_user_dn.sql 的內容複製到 SQL Developer 中，然後對連接的資料庫執行這些指令。

清除資料庫檢查總數

- 1 在 C:\NetIQ\idm\apps\IdentityReporting\sql 中找到下列 .sql 檔案。
 - ◆ DbUpdate-01-run-as-idm_rpt_cfg.sql
 - ◆ DbUpdate-02-run-as-idm_rpt_cfg.sql
 - ◆ DbUpdate-03-run-as-idm_rpt_data.sql
 - ◆ DbUpdate-04-run-as-idm_rpt_data.sql
 - ◆ DbUpdate-05-run-as-idm_rpt_data.sql
 - ◆ DbUpdate-06-run-as-idm_rpt_cfg.sql
- 2 清除資料庫檢查總數
 - 2a 若要使用每個 .sql 執行 clearchsum 指令，請將下行附加到每個檔案的開頭：

```
update DATABASECHANGELOG set MD5SUM = NULL;
```


修改後的內容應該類似如下：

```
--
*****
**
-- Update Database Script
--
*****
**
-- Change Log: IdmDcsDataDropViews.xml
-- Ran at: 2/23/18 5:17 PM
-- Against: IDM_RPT_CFG@jdbc:oracle:thin:@192.99.170.20:1521/orcl
-- Liquibase version: 3.5.1
--
*****
**
update databasechangelog set md5sum = null;
```

2b 以相應的使用者身分執行每個 .sql。

3 將變更提交到資料庫。

部署 Identity Reporting 的 REST API

Identity Reporting 在報告功能中整合了多個用於啟用不同特性的 REST API。這些 REST API 使用 OAuth2 通訊協定進行驗證。

在 Tomcat 上，系統會在安裝 Identity Reporting 時自動部署 rptdoc war 和 dcsdoc war。

連接遠端 Remote PostgreSQL 資料庫

如果您的 PostgreSQL 資料庫安裝在其他伺服器上，則需要在該遠端資料庫的 postgresql.conf 和 pg_hba.conf 檔案中變更預設設定。

1 在 postgresql.conf 檔案中變更監聽位址。

依預設，PostgreSQL 允許監聽 localhost 連接，不允許遠端 TCP/IP 連接。若要允許進行遠端 TCP/IP 連接，請將以下項目新增至

C:\NetIQ\idm\apps\postgres\data\postgresql.conf 檔案中：

```
listen_addresses = '*'
```

如果伺服器上有多個介面，可以指定要監聽的特定介面。

2 將用戶端驗證項目新增至 pg_hba.conf 檔案中。

依預設，PostgreSQL 只接受來自 localhost 的連接。它會拒絕遠端連接。透過套用存取控制規則來控制此行為，該規則允許使用者在提供有效密碼 (md5 關鍵字) 後從某個 IP 位址登入。若要接受遠端連接，請將以下項目新增至

C:\NetIQ\idm\apps\postgres\data\pg_hba.conf 檔案中。

```
host all all 0.0.0.0/0 md5
```

例如，192.168.104.24/26 trust

這僅適用於 IPv4 位址。對於 IPv6 位址，請新增以下項目：

```
host all all ::0/0 md5
```

如果您要允許來自特定網路上多部用戶端電腦的連接，請採用 CIDR 位址格式在此項目中指定網路位址。

pg_hba.conf 檔案支援以下用戶端驗證格式。

- ◆ local database user authentication-method [authentication-option]
- ◆ host database user CIDR-address authentication-method [authentication-option]
- ◆ hostssl database user CIDR-address authentication-method [authentication-option]
- ◆ hostnossl database user CIDR-address authentication-method [authentication-option]

您可以使用以下格式在單獨的欄位中指定 IP 位址和網路遮罩，而不使用 CIDR 位址格式：

- ◆ host database user IP-address IP-mask authentication-method [authentication-option]
- ◆ hostssl database user IP-address IP-mask authentication-method [authentication-option]
- ◆ hostnossl database user IP-address IP-mask authentication-method [authentication-option]

3 測試遠端連接。

3a 重新啟動遠端 PostgreSQL 伺服器。

3b 使用使用者名稱和密碼從遠端登入伺服器。

Identity Reporting 的安裝後步驟

在安裝期間，如果您針對何時建立 Identity Reporting 的綱要提示選取了啟動或檔案選項，則必須從 Identity Reporting 使用者介面手動新增資料來源。若要新增資料來源，請導覽至資料來源選項，按一下新增，然後從清單中選擇 IDMDCSDataSource。

另外，請在啟動一次 Tomcat 後再重新啟動一次，以確定可用資料庫正常執行。

啟用 Identity Manager

您無需提供啟用代碼就能安裝或初次執行 Identity Manager。但是，如果您未提供啟用代碼，Identity Manager 將在安裝 90 天後停止運作。在這 90 天內或者 90 天後，您隨時都可以啟用 Identity Manager。如需詳細資訊，請參閱《[NetIQ Identity Manager Overview and Planning Guide](#)》(NetIQ Identity Manager 綜覽和規劃指南) 中的「[Activating Identity Manager](#)」(啟用 Identity Manager)。

查看 Identity Manager 元件使用的連接埠

Identity Manager 元件使用多個連接埠來相互通訊。防火牆中預設已開啟這些連接埠。若要查看 Identity Manager 元件使用的連接埠，請參閱《[NetIQ Identity Manager Security Guide](#)》(NetIQ Identity Manager 安全性指南) 中的「[Understanding Identity Manager Communication](#)」(瞭解 Identity Manager 通訊)。

```

kind: PersistentVolume
apiVersion: v1
metadata:
  name: task-pv-volume
  labels:
    type: nfs
spec:
  storageClassName: manual
  capacity:
    storage: 3Gi
  accessModes:
    - ReadWriteMany
  hostPath:
    path: '/mnt'
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: task-pv-claim1
spec:
  storageClassName: manual
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
---
apiVersion: v1
kind: Pod
metadata:
  labels:
    name: identity-engine
  name: identity-engine
spec:
  nodeSelector:
    kubernetes.io/hostname:
  hostNetwork: true
  containers:
    -
      image: <image name>
      name: identity-engine-container
      resources:
        limits:
          cpu: "2"
          memory: 4Gi
        requests:
          cpu: "1"
          memory: 1Gi
      volumeMounts:
        - name: data
          mountPath: /config
      env:
        - name: UPGRADE_IDM
          value:
        - name: IS_ADVANCED_EDITION

```

```

    value:
  - name: INSTALL_ENGINE
    value:
  - name: INSTALL_IDVAULT
    value:
  - name: IS_COMMON_PASSWORD
    value:
  - name: COMMON_PASSWORD
    value:
  - name: TREE_CONFIG
    value:
  - name: ID_VAULT_PASSWORD
    value:
  - name: ID_VAULT_EXISTING_SERVER
    value:
  - name: ID_VAULT_EXISTING_NCP_PORT
    value:
  - name: ID_VAULT_EXISTING_LDAPS_PORT
    value:
  - name: ID_VAULT_EXISTING_CONTEXTDN
    value:
  - name: ID_VAULT_TREENAME
    value:
  - name: ID_VAULT_ADMIN_LDAP
    value:
  - name: ID_VAULT_ADMIN
    value:
  - name: ID_VAULT_PASSWORD
    value:
  - name: ID_VAULT_VARDIR
    value:
  - name: ID_VAULT_DIB
    value: '
  - name: ID_VAULT_NCP_PORT
    value:
  - name: ID_VAULT_LDAP_PORT
    value:
  - name: ID_VAULT_LDAPS_PORT
    value:
  - name: ID_VAULT_HTTP_PORT
    value:
  - name: ID_VAULT_HTTPS_PORT
    value:
  - name: ID_VAULT_CONF
    value:
  - name: ID_VAULT_DRIVER_SET
    value:
  - name: ID_VAULT_DEPLOY_CTX
    value:
  - name: ID_VAULT_SERVER_CONTEXT
    value:
volumes:
  - name: data
    persistentVolumeClaim:
      claimName: task-pv-claim1

```

IV

在 FIPS 模式下設定 Identity Manager

Identity Manager 利用遵守聯邦資訊處理標準 (FIPS) 的功能，滿足美國聯邦機關和客戶對高度安全環境的安全性要求。FIPS 140-2 標準用於監管加密軟體的實作與通訊。Bouncy Castle 使用一個通過了 FIPS 140-2 Level 1 認證的開放原始碼 JCA 提供者。該提供者建立在成熟且知名的 Bouncy Castle 開放原始碼加密提供者基礎之上。本章提供關於如何在 FIPS 模式下設定及操作 Identity Manager 的資訊。

附註：

- ◆ SSPR 不支援 FIPS 模式。您必須將非 FIPS SSPR 設定移轉至另一部伺服器。如需詳細資訊，請參閱《[Self Service Password Reset 4.7 Administration Guide](#)》(Self Service Password Reset 4.7 管理指南) 中的「[Backing Up Configuration Information](#)」(備份組態資訊) 和「[Importing Configuration Information](#)」(輸入組態資訊)。
- ◆ 確定主金鑰儲存區密碼與 Tomcat 金鑰儲存區密碼相同。若要變更密碼，請參閱「[儲存 Configupdate 公用程式密碼 \(選擇性\)](#)」(第 67 頁)。

以下章節提供關於在 FIPS 模式下設定和操作 Identity Manager 的資訊。

- ◆ 第 5 章「[為 FIPS 設定 JRE](#)」(第 111 頁)
- ◆ 第 6 章「[在 FIPS 模式下設定 Identity Manager 引擎](#)」(第 113 頁)
- ◆ 第 7 章「[在 FIPS 模式下設定擴送代理程式](#)」(第 115 頁)
- ◆ 第 8 章「[在 FIPS 模式下設定 Identity Applications 和 Identity Reporting](#)」(第 117 頁)
- ◆ 第 9 章「[在 FIPS 模式下設定遠端載入器](#)」(第 123 頁)

5 為 FIPS 設定 JRE

若要為 BCFIPS 僅核准模式設定 JRE，請執行以下操作：

- 1 將 BCFIPS.jar 檔案新增至 Java 類別路徑。

所需的 BCFIPS 檔案如下：

- ◆ bc-fips-1.0.2.4.jar
- ◆ bcpkix-fips-1.0.7.jar
- ◆ bctls-fips-1.0.18.jar

- 2 修改 <jre-root>/lib/security 目錄下的 java.security 檔案，並設定 BCFIPS 定義的 Java 系統內容。

在文字編輯器中，從 <jre-root>/conf/security/java.security 開啟代管 Web 容器的 JRE 的上述檔案。找到安全性提供者清單，註解化所有現有提供者，然後按照以下方式取代檔案中的項目：

- ◆ security.provider.1=BCFIPS
- ◆ security.provider.2=BCJSSE
- ◆ security.provider.3=SunJSSE
- ◆ security.provider.4=SUN
- ◆ security.provider.5=SunJCE

必須指定 SunJSSE 提供者 (Java 11)，因為 OSP 在啟始化其可信證書儲存區時需要特定的 TrustManager 實作。除了對安全性提供者進行變更之外，還必須使用 BCFIPS JSSE KeyManager 實作。這種必要性主要是因為 Sun 實作中存在缺陷，導致無法在一定程度上做到 FIPS 在金鑰方面所需的確定性。為此，請將 java.security 中的以下一行：

```
ssl.KeyManagerFactory.algorithm=SunX509
```

取代為

```
ssl.KeyManagerFactory.algorithm=PKIX
```

另外，最好停用較舊的 SSL 和 TLS 演算法。這是因為，TLS v2.0 之前的 SSL/TLS 版本所需的演算法在 BCFIPS 已核准模式下不可用。若要停用舊演算法，請找到 jdk.tls.disabledAlgorithms 項目。例如：

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 1024, \ EC  
keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
```

將 TLSv1 和 TLSv1.1 新增至清單中：

```
jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, RC4, MD5withRSA, DH  
keySize < 1024, \ EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
```

停用 TLSv1 和 TLSv1.1 不是強制要求，但這樣可以避免在 OSP 嘗試安全連接到僅支援 TLS v1.1 或更舊版本的服務 (例如 LDAP) 時，出現不明所以的錯誤訊息。停用舊版 TLS 後出現的錯誤訊息更容易理解，並且可以直接指明問題所在。

附註：eDirectory 8.8 (或更舊版本) 無法與安全 LDAP 配合使用，因為它僅支援 TLS v1.0。若要用安全 LDAP，則必須使用 eDirectory 9 或更新版本。另一種做法是修改預設的金鑰儲存區類型。找到 `keystore.type=jks` 或 `keystore.type=pkcs12` 行，將其變更為 `keystore.type=bcfks`。

6 在 FIPS 模式下設定 Identity Manager 引擎

在 Identity Manager 引擎上設定 FIPS 模式之前，應考慮先完成以下準備工作：

- ◆ 若要啟用安全性增強，請將以下 jar 檔案放入 C:\NetIQ\Common\JRE\lib 資料夾：
 - ◆ bc-fips-1.0.2.4.jar
 - ◆ bcpkix-fips-1.0.7.jar
 - ◆ bctls-fips-1.0.18.jar

附註：您可以從以下 maven 儲存庫下載上述 jar 檔案：

- ◆ bc-fips (<https://mvnrepository.com/artifact/org.bouncycastle/bc-fips>)
 - ◆ bcpkix-fips (<https://mvnrepository.com/artifact/org.bouncycastle/bcpkix-fips>)
 - ◆ bctls-fips (<https://mvnrepository.com/artifact/org.bouncycastle/bctls-fips>)
-

- ◆ 將以下值新增至環境變數中：

```
IS_FIPS_ENABLED=true
```

```
BC_FIPS_VERSION=1.0.2.4
```

```
JAVA_OPTS =" -Dorg.bouncycastle.fips.approved_only=true -  
Dorg.bouncycastle.rsa.allow_multi_use=true"
```

```
CLASSPATH=C:\NetIQ\Common\JRE\lib\bc-fips-1.0.2.4.jar
```

附註：若要透過連接埠 636 存取 dxcmnd，請在 LDAP 設定中啟用 SSL EC 證書。

程序

- 1 導覽至 C:\NetIQ\Common\JRE\conf\security 資料夾。
- 2 備份 java.security 檔案。
- 3 執行以下步驟來編輯 java.security 檔案：
 - 3a 搜尋字串 List of providers and their preference orders，註解化所有現有提供者，然後新增以下項目：

```
security.provider.1=BCFIPS  
security.provider.2=BCJSSE  
security.provider.3=SunJSSE  
security.provider.4=SUN  
security.provider.5=SunJCE
```
 - 3b 搜尋字串 ssl.KeyManagerFactory.algorithm=SunX509，將其註解化，然後新增以下項目：

```
ssl.KeyManagerFactory.algorithm=PKIX
```

- 3c** 搜尋字串 `jdk.tls.disabledAlgorithms`，並將 TLSv1、TLSv1.1 新增至清單中。

例如，`jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, RC4, DES, MD5withRSA, DH keySize < 1024, \EC keySize < 224, 3DES_EDE_CBC, anon, NULL`

- 3d** 搜尋字串 `keystore.type`，將其註解化，然後新增以下項目：

```
keystore.type=bcfks
```

- 4** 導覽至 `C:\NetIQ\Common\JRE\lib\security` 資料夾。

- 5** 備份 `cacerts` 檔案。

- 6** 為了支援安全性增強，請使用以下指令將 `cacerts` 檔案轉換為 `bcfks` 格式：

```
keytool -importkeystore -srckeystore cacerts -srcstorepass changeit -  
srcstoretype JKS -destkeystore cacerts -deststorepass changeit -  
deststoretype BCFKS -providerclass  
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath  
$CLASSPATH
```

產生 `cacerts_bcfks` 檔案後，刪除原來的 `cacerts`，然後將該 `cacerts_bcfks` 重新命名為 `cacerts`。

- 7** 登入 Identity Console。

- 8** 移至 **IDM Administrator**，按一下驅動程式集的  動作功能表。

- 9** 導覽至 **驅動程式集內容 > 驅動程式集組態 > Java 環境參數**。

- 10** 在 **JVM 選項** 中輸入以下內容：

```
Djavax.net.ssl.trustStore=C:\NetIQ\Common\JRE\lib\security\cacerts -  
Djavax.net.ssl.trustStorePassword=changeit -  
Djavax.net.ssl.trustStoreType=BCFKS
```

- 11** 按一下  **儲存** 按鈕。

- 12** 重新啟動 eDirectory。

7 在 FIPS 模式下設定擴送代理程式

在 Identity Manager 擴送代理程式上設定 FIPS 模式之前，應考慮先完成以下準備工作：

- ◆ 在未啟用安全性增強的情況下，啟動擴送代理程式。這會在 config 資料夾中產生一個金鑰儲存區檔案。
- ◆ 將以下 jar 檔案放入 C:\NetIQ\IDM\FanoutAgent\lib 資料夾：
 - ◆ bc-fips-1.0.2.4.jar
 - ◆ bcpkix-fips-1.0.7.jar
 - ◆ bctls-fips-1.0.18.jar
- ◆ 將以下值新增至環境變數中：

```
IS_FIPS_ENABLED=true
```

```
BC_FIPS_VERSION=1.0.2.4
```

```
JAVA_OPTS =" -Dorg.bouncycastle.fips.approved_only=true -  
Dorg.bouncycastle.rsa.allow_multi_use=true"
```

```
CLASSPATH=C:\NetIQ\IDM\FanoutAgent\lib\bc-fips-1.0.2.4.jar
```

程序

- 1 導覽至 C:\NetIQ\Common\JRE\conf\security 資料夾。
- 2 備份 java.security 檔案。
- 3 執行以下步驟來編輯 java.security 檔案：
 - 3a 搜尋字串 List of providers and their preference orders，註解化所有現有提供者，然後新增以下項目：

```
security.provider.1=BCFIPS  
security.provider.2=BCJSSE  
security.provider.3=SunJSSE  
security.provider.4=SUN  
security.provider.5=SunJCE
```
 - 3b 搜尋字串 ssl.KeyManagerFactory.algorithm=SunX509，將其註解化，並新增以下項目：

```
ssl.KeyManagerFactory.algorithm=PKIX
```
 - 3c 搜尋字串 jdk.tls.disabledAlgorithms，並將 TLSv1、TLSv1.1 新增至清單中。
例如，jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, RC4, DES,
MD5withRSA, DH keySize < 1024, \EC keySize < 224, 3DES_EDE_CBC,
anon, NULL

3d 搜尋字串 `keystore.type`，將其註解化，然後新增以下項目：

```
keystore.type=bcfks
```

4 導覽至 `C:\NetIQ\Common\JRE\lib\security` 資料夾。

5 備份 `cacerts` 檔案。

6 若要將金鑰儲存區檔案從 `jks` 格式轉換為 `bcfks` 格式，請執行以下指令：

```
keytool -importkeystore -srckeystore  
C:\NetIQ\IDM\FanoutAgent\config\keystore.jks -srcstorepass changeit -  
srcstoretype PKCS12 -destkeystore  
C:\NetIQ\IDM\FanoutAgent\config\keystore.jks -deststorepass changeit -  
deststoretype BCFKS -providerclass  
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath  
$CLASSPATH
```

7 導覽至 `C:\NetIQ\IDM\FanoutAgent\bin\` 資料夾，並在 `startAgent.bat` 檔案中進行以下變更：

```
"%JAVA%" --add-opens=java.base/sun.security.internal.spec=ALL-UNNAMED -  
Djavax.net.ssl.trustStore=C:\NetIQ\Common\JRE\lib\security\cacerts -  
Djavax.net.ssl.trustStorePassword=changeit -Dkeystore.type=BCFKS -  
Dorg.bouncycastle.fips.approved_only=true -  
Dorg.bouncycastle.rsa.allow_multi_use=true -cp %CLASSPATH%  
com.netiq.idm.fanoutagent.FanoutAgent !FILENAME! !SERVERONLY!.
```

8 啟動擴送代理程式並檢查記錄。

8 在 FIPS 模式下設定 Identity Applications 和 Identity Reporting

在 Identity Manager Reporting 和 Identity Applications 上設定 FIPS 模式之前，應考慮先完成以下準備工作：

- ◆ 在執行 Identity Applications 和 Identity Manager Reporting 元件的伺服器上停止 Tomcat 服務。
- ◆ 驗證管理員是否可以登入 Identity Manager 引擎系統上的 dxcmd 工具。

程序

- 1 為 FIPS 建立一個新資料夾。範例：C:\fips
- 2 在新建立的資料夾中備份以下檔案：

檔案	現有檔案路徑
idm.jks	C:\netiq\idm\apps\tomcat\conf
tomcat.ks	
encrypt-keys.pkcs12	
server.xml	
ism-configuration.properties	
configupdate.sh	C:\netiq\idm\apps\configupdate
configupdate.bat.properties	

- 3 將 osp-tomcat8-pwd-handler-<version>.jar 複製到 C:\netiq\idm\apps\tomcat\lib 資料夾中。
- 4 導覽至 C:\NetIQ\IDM\apps\tomcat\bin\ 資料夾，並按照以下方式編輯 setenv.sh 檔案：
 - ◆ JAVA_OPTS= %JAVA_OPTS% -Dorg.bouncycastle.fips.approved_only=true -Dinternal.osp.framework.fips-password=novell -Dorg.bouncycastle.rsa.allow_multi_use=true -Djavax.net.ssl.keyStoreType=BCFKS -Djavax.net.ssl.trustStoreType=BCFKS -Djavax.net.ssl.trustStore=c:\netiq\idm\apps\tomcat\conf\idm.bcfks -Djavax.net.ssl.trustStorePassword=novell

- ◆ BCFIPS_JARS=c:\netiq\common\jre\lib\bc-fips-1.0.2.4.jar;c:\netiq\common\jre\lib\bcpkix-fips-1.0.7.jar;c:\netiq\common\jre\lib\bctls-fips-1.0.18.jar
- ◆ CLASSPATH=C:\NetIQ\Common\JRE\lib\bc-fips-1.0.2.4.jar;C:\NetIQ\Common\JRE\lib\bcpkix-fips-1.0.7.jar;C:\NetIQ\Common\JRE\lib\bctls-fips-1.0.18.jar;%CLASSPATH%
- ◆ 搜尋 CATALINA_OPTS，將 encrypt-keys.pkcs12 變更為 encrypt-keys.bcfks，並將 storetype 變更為 bcfks

5 在命令提示字元處，導覽至 C:\netiq\idm\commom\jre\bin 並執行以下指令：

```
keytool -importkeystore -srckeystore
C:\NetIQ\IDM\apps\tomcat\conf\idm.jks -srcstorepass novell -
srcstoretype PKCS12 -destkeystore
C:\NetIQ\IDM\apps\tomcat\conf\idm.bcfks -deststorepass novell -
deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

```
keytool -importkeystore -srckeystore
C:\NetIQ\IDM\apps\tomcat\conf\tomcat.ks -srcstorepass changeit -
srcstoretype PKCS12 -destkeystore
C:\NetIQ\IDM\apps\tomcat\conf\tomcat.bcfks -deststorepass changeit -
deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

```
keytool -importkeystore -srckeystore
C:\NetIQ\IDM\apps\tomcat\conf\idm.jks -srcstorepass novell -
srcstoretype PKCS12 -destkeystore C:\NetIQ\IDM\apps\osp\osp.bcfks -
deststorepass novell -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

```
keytool -importkeystore -srckeystore
C:\NetIQ\IDM\apps\tomcat\conf\tomcat.ks -srcstorepass changeit -
srcstoretype PKCS12 -destkeystore C:\NetIQ\IDM\apps\osp\osp.bcfks -
deststorepass novell -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

```
java -jar <mount-location>\common\osp\misc\osp-keymanager-6.7.1.jar -
genkeys -keystore C:\NetIQ\IDM\apps\osp\osp.bcfks -storepass novell -
storetype BCFKS -application idm -providerClass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerPath
C:\NetIQ\Common\JRE\lib\bc-fips-1.0.2.4.jar -keypass novell -use
Encrypting, Signing, TLS
```

```
keytool -importkeystore -srckeystore
C:\NetIQ\IDM\apps\tomcat\conf\encrypt-keys.pkcs12 -srcstorepass
changeit -srcstoretype PKCS12 -destkeystore
C:\NetIQ\IDM\apps\tomcat\conf\encrypt-keys.bcfks -deststorepass
changeit -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

6 按照以下方式編輯 server.xml 檔案：

```
<!--Connector port="8543"
protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="150"
SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
sslProtocol="TLSv1.2" keystoreFile="conf/tomcat.ks"
keystorePass="changeit" maxHttpHeaderSize="65536"
sslEnabledProtocols="TLSv1.2" /-->

<Connector
protocol="com.microfocus.osp.tomcat.http.PasswordHttp11NioProtocol"
port="8543" maxThreads="150" maxHttpHeaderSize="65536"
SSLEnabled="true" scheme="https" secure="true">
<SSLHostConfig protocol="TLS" protocols="TLSv1.2"
ciphers="TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,TLS_DHE_DSS_WITH_AES_256_
GCM_SHA384,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_DHE_DSS_WITH_AES_12
8_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256
_CBC_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_
GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WIT
H_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_EC
DSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECD
HE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_
ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA
_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_CCM,TLS_RSA_WITH_AES_256
_CCM,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_
RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA"
truststoreFile="/opt/netiq/idm/apps/osp/osp.bcfks"
truststorePassword="novell" truststoreType="BCFKS" > <Certificate
certificateKeystoreFile="/opt/netiq/idm/apps/tomcat/conf/tomcat.bcfks"
certificateKeystorePassword="novell" certificateKeyAlias="ssl
certificatedns" certificateKeystoreType="BCFKS" />
</Certificate>
</SSLHostConfig>
</Connector>
```

7 按照以下方式編輯 ism-configuration-properties 檔案：

```
com.netiq.idm.osp.ssl-keystore.file =
C:\\NetIQ\\IDM\\apps\\tomcat\\conf\\tomcat.bcfks

com.netiq.idm.osp.ssl-keystore.type = BCFKS

com.netiq.idm.osp.oauth-keystore.file =
C:\\NetIQ\\IDM\\apps\\osp\\osp.bcfks

com.netiq.idm.osp.oauth-keystore.type = BCFKS

com.netiq.rpt.ssl-keystore.file =
C:\\NetIQ\\IDM\\apps\\tomcat\\conf\\idm.bcfks

com.netiq.rpt.ssl-keystore.type = BCFKS

DirectoryService/realms/jndi/params/KEYSTORE_PATH =
C:\\NetIQ\\IDM\\apps\\tomcat\\conf\\idm.bcfks

com.sssw.fw.security.sigcert.truststore.type = BCFKS
```

```
com.netiq.idm.osp.oauth-truststore.file =
C:\\\\NetIQ\\\\IDM\\\\apps\\\\tomcat\\\\conf\\\\idm.bcfks

com.netiq.idm.ua.ldap.keystore-type = BCFKS

com.netiq.idm.osp.oauth-key-alias = ssl certificatedns
```

- 8 在命令提示字元處，導覽至 C:\netiq\idm\commom\jre\bin 並執行以下指令：

```
keytool -storepasswd -new <new master keystore password> -keystore
C:\NetIQ\IDM\apps\tomcat\conf\encrypt-keys.bcfks -storepass changeit -
storetype BCFKS -providerclass
org.bouncycastle.jcayce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

```
keytool -keypasswd -alias ism.config.encrypt.0 -keypass changeit -new
<new master keystore password> -keystore
C:\NetIQ\IDM\apps\tomcat\conf\encrypt-keys.bcfks -storepass changeit -
storetype BCFKS -providerclass
org.bouncycastle.jcayce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

執行此指令會產生一個 **keystorepass** 值：

```
java -cp C:\NetIQ\IDM\apps\tomcat\lib\obscurity-0.13.2-uber.jar
com.netiq.ism.obfuscate.server.util.PasswordObfuscator novell
```

- 9 取得 **keystorepass** 值後，使用以下行更新 **ism-sensitive.properties** 檔案：

```
com.microfocus.ism.master-keypass = <keystorepass-value>
com.microfocus.ism.master-storepass = <keystorepass-value>
```

- 10 將以下 **jar** 檔案複製到 **configupdate\lib** 資料夾中：

- ◆ bc-fips-1.0.2.4.jar
- ◆ bcpkix-fips-1.0.7.jar
- ◆ bctls-fips-1.0.18.jar

- 11 編輯 **configupdate.bat.properties** 中的以下內容：

```
master_keystore_type=bcfks
master_keystore=C:\NetIQ\IDM\apps\tomcat\conf\encrypt-keys.bcfks
```

- 12 編輯 **configupdate.sh** 中的以下內容：

```
set "JAVA_OPTS= %JAVA_OPTS% -Dorg.bouncycastle.fips.approved_only=true
-Dinternal.osp.framework.fips-password=] -
Dorg.bouncycastle.rsa.allow_multi_use=true -
Djavax.net.ssl.keyStoreType=BCFKS -Djavax.net.ssl.trustStoreType=BCFKS
-Djavax.net.ssl.trustStore=c:\netiq\idm\apps\tomcat\conf\idm.bcfks -
Djavax.net.ssl.trustStorePassword=novell "
```

```
set CLASSPATH=C:\NetIQ\Common\JRE\lib\bc-fips-
1.0.2.4.jar;C:\NetIQ\Common\JRE\lib\bcpkix-fips-
1.0.7.jar;C:\NetIQ\Common\JRE\lib\bctls-fips-1.0.18.jar;%CLASSPATH%
```

13 啟動 configupdate 公用程式。

14 啟動 Tomcat。

9 在 FIPS 模式下設定遠端載入器

若要在遠端載入器上設定 FIPS 模式，請執行以下步驟：

- 1 將以下 jar 檔案放入 C:\NetIQ\IDM\RemoteLoader\lib 資料夾：
 - ◆ bc-fips-1.0.2.4.jar
 - ◆ bcpkix-fips-1.0.7.jar
 - ◆ bctls-fips-1.0.18.jar
- 2 導覽至遠端載入器資料夾，並啟動 rlconsole。
- 3 建立並啟動一個驅動程式。此驅動程式將在資料夾中產生一個 config 檔案。
- 4 在 config 檔案中新增以下一行：

```
is_fips_enabled=true
```
- 5 儲存該檔案並重新啟動 RL 例項。



安裝 Designer

此部分將引導您完成安裝 Designer for Identity Manager 的程序。依預設，安裝程式會在 C:\Netiq 中安裝元件。

重要：請確定包含 Designer 安裝程式的目錄名稱沒有空格。例如，不要將其命名為 Designer Install，但可以命名為 DesignerInstall。

NetIQ 建議您在開始之前檢閱安裝程序。如需詳細資訊，請參閱[第 10 章「規劃 Designer 安裝」](#) (第 127 頁)。

10 規劃 Designer 安裝

本章提供關於安裝 Designer 的先決條件、考量和系統設定。首先，請參閱核對清單，以瞭解安裝程序。

- ◆ 「[Designer 安裝核對清單](#)」(第 127 頁)

Designer 安裝核對清單

NetIQ 建議您在開始安裝前先檢閱以下步驟：

	核對清單項目
☐	1. 查看規劃資訊。如需詳細資訊，請參閱第 II 部分「 規劃 Identity Manager 安裝 」(第 33 頁)。
☐	2. 檢閱關於安裝 Designer 的考量，以確保電腦符合先決條件。
☐	3. 若要安裝 Designer，請參閱下列其中一節： ◆ 「執行 Windows 可執行檔」(第 129 頁) ◆ 「使用靜默安裝程序」(第 129 頁)
☐	4. 安裝其餘的 Identity Manager 元件。
☐	5. (選擇性) 若要啟動 Identity Manager 解決方案的一個專案，請參閱 《NetIQ Designer for Identity Manager Administration Guide》 (NetIQ Designer for Identity Manager 管理指南)。

11 安裝 Designer

您可以根據具體的目標電腦，使用可執行檔、二進位檔案或採用文字模式安裝 Identity Manager Designer。您還可以執行靜默安裝。

Identity Manager 的多個元件都需要 Designer 中的套件。當您安裝 Designer 時，安裝程式會自動將數個套件新增至您的新專案中。

- 「執行 Windows 可執行檔」(第 129 頁)
- 「使用靜默安裝程序」(第 129 頁)
- 「在除系統地區設定以外的地區設定中安裝 Designer」(第 130 頁)
- 「修改包含空格字元的安裝路徑」(第 131 頁)

執行 Windows 可執行檔

- 1 使用管理員帳戶登入要安裝 Designer 的電腦。
- 2 從軟體授權和下載 (<https://sld.microfocus.com/index>) 入口網站下載 Identity_Manager_4.9_Designer_Windows.zip。
- 3 解壓縮 Identity_Manager_4.9_Designer_Windows.zip 檔案。
- 4 導覽至 designer_install 資料夾。
- 5 執行 install.exe 檔案。
- 6 依照精靈中的步驟操作，直到安裝程序完成。

使用靜默安裝程序

您可以使用程序檔以靜默模式執行 Designer，整個過程無需使用者互動。除非您編輯了 designerInstaller.properties 檔案，否則 `-i silent` 選項將會使用預設的參數值進行安裝。

- 1 使用管理員帳戶登入您要安裝 Designer 的電腦。
- 2 導覽至包含安裝程式的目錄。
- 3 (選擇性) 若要設定 Designer 的安裝目錄和語言，請完成以下步驟。
 - 3a 開啟預設位於 `Path_to_unzipped_Designer_file\designer_install` 目錄中的 `designerInstaller.properties` 檔案。
 - 3b 在該 properties 檔案中，修改以下參數的值：
USER_INSTALL_DIR
指定 Designer 安裝位置的路徑。例如：

```
USER_INSTALL_DIR=C:\designer
```

如果指定的路徑不是以 designer 目錄結尾，Designer 安裝程式會自動附加 designer 目錄。

SELECTED_DESIGNER_LOCALE

指定下列其中一種語言，Designer 安裝完成後，啟動時就會使用這個語言：

- ◆ zh_CN - 簡體中文
- ◆ zh_TW - 繁體中文
- ◆ nl - 荷蘭語
- ◆ en - 英語
- ◆ fr - 法語
- ◆ de - 德語
- ◆ it - 義大利語
- ◆ ja - 日語
- ◆ pt_BR - 巴西葡萄牙語
- ◆ es - 西班牙語

3c 儲存並關閉該 properties 檔案。

4 從內容檔案所在目錄執行以下指令：

```
install -i silent -f designerInstaller.properties
```

在除系統地區設定以外的地區設定中安裝 Designer

在除系統地區設定以外的語言中，您可以使用 Windows 可執行檔根據額外提示安裝 Designer。範例情景：您電腦上的系統地區設定為「德文」，但您想要安裝英文版 Designer。

若要安裝，請執行以下操作：

1 下載並解壓縮 Identity_Manager_4.9_Designer_Windows.zip 檔案。

2 導覽至電腦 **Downloads** 資料夾中的 designer_install 資料夾。

例如 C:\Users\< 使用者名稱

>\Downloads\Identity_Manager_4.9_Designer_Windows\designer_install

3 開啟指令提示符並執行以下指令：

```
install.exe -i silent -l en_us
```

此指令將在英文 (美國) 地區設定中以靜默方式安裝 Designer。如需瞭解如何指定 Designer 支援的其他地區設定，請參閱「使用靜默安裝程序」(第 129 頁) 中的步驟 3b。

修改包含空格字元的安裝路徑

您可以將 **Designer** 安裝到目錄名稱中包含空格的位置。但是，在安裝 **Designer** 後，必須修改 `StartDesigner.bat` 和 `Designer.ini` 檔案，以確定 **Designer** 可正常運作。手動以逸出字元 (「\」) 取代空格。例如：

將

`C:\designer installation`

變更為

`C:\designer\ installation`

VI

安裝 Analyzer

此部分將引導您完成安裝 Analyzer for Identity Manager 的程序。Analyzer 是安裝在工作站上的複雜用戶端元件。您可以使用 Analyzer 來檢查和清理要新增至 Identity Manager 解決方案之已連接系統中的資料。在規劃階段，使用 Analyzer 可協助您瞭解需要進行的變更以及最佳的變更方法。

依預設，安裝程式會在 C:\NetIQ\Analyzer 中安裝元件。

重要：Identity Manager 4.9 ISO 中不包含 Analyzer 工具。如果已安裝 Analyzer，請務必將其更新至版本 4.8.5，並與 Identity Manager 4.9 配合使用。

NetIQ 建議您在開始之前檢閱安裝程序。如需詳細資訊，請參閱「[Analyzer 的安裝核對清單](#)」(第 135 頁)。

12 規劃 Analyzer 安裝

本章提供關於準備安裝 Analyzer for Identity Manager 的指導準則。NetIQ 建議您在開始之前檢閱安裝程序。

- ♦ 「Analyzer 的安裝核對清單」(第 135 頁)

Analyzer 的安裝核對清單

NetIQ 建議您在開始安裝程序之前先檢閱以下步驟：

	核對清單項目
☐	1. 查看規劃資訊。如需詳細資訊，請參閱第 II 部分「規劃 Identity Manager 安裝」(第 33 頁)。
☐	2. 查看安裝 Analyzer 的注意事項，以確定電腦符合先決條件。
☐	3. 若要安裝 Analyzer，請參閱以下章節： ♦ 若要使用安裝精靈，請參閱「執行 Windows 可執行檔」(第 137 頁)。 ♦ 若要執行靜默安裝，請參閱「使用靜默安裝程序」(第 137 頁)
☐	4. 若要啟用 Analyzer，請參閱《NetIQ Identity Manager Overview and Planning Guide》(NetIQ Identity Manager 綜覽和規劃指南) 中的「Activating Analyzer」(啟用 Analyzer)。

13 安裝 Analyzer

本章將引導您完成安裝 Analyzer 及設定其環境的程序。

- 「執行 Windows 可執行檔」(第 137 頁)
- 「使用靜默安裝程序」(第 137 頁)

執行 Windows 可執行檔

- 1 使用管理員帳戶登入要安裝 Analyzer 的電腦。
- 2 從 NetIQ 下載網站下載 Identity_Manager_4.9.0_Analyzer_Windows.zip。
- 3 解壓縮 Identity_Manager_4.9.0_Analyzer_Windows.zip 檔案。
- 4 導覽至 analyzer_install 資料夾。
- 5 執行 install.exe 檔案。
- 6 依照精靈中的步驟操作，直到安裝程序完成。

使用靜默安裝程序

您可以使用程序檔以靜默方式安裝 Analyzer，整個過程無需使用者互動。除非您編輯了 analyzerInstaller.properties 檔案，否則指定 `-i silent` 選項將使用預設的參數值進行安裝。

- 1 使用管理員帳戶登入要安裝 Analyzer 的電腦。
- 2 導覽至包含安裝程式的目錄。
- 3 (選擇性) 若要設定 Analyzer 的安裝目錄和語言，請完成以下步驟。
 - 3a 開啟預設位於 `Path_to_unzipped_Analyzer_file\analyzerInstall` 目錄中的 `analyzerInstaller.properties` 檔案。
 - 3b 在該 properties 檔案中，修改以下參數的值：

USER_INSTALL_DIR

指定要安裝 Analyzer 的位置的路徑。例如：

```
USER_INSTALL_DIR=C:\analyzer
```

如果指定的路徑不是以 analyzer 目錄結尾，Analyzer 安裝程式會自動附加 analyzer 目錄。

SELECTED_ANALYZER_LOCALE

指定以下語言之一，做為 Analyzer 在安裝完成後啟動時使用的語言：

- ♦ zh_CN - 簡體中文

- ◆ zh_TW - 繁體中文
- ◆ nl - 荷蘭語
- ◆ en - 英語
- ◆ fr - 法語
- ◆ de - 德語
- ◆ it - 義大利語
- ◆ ja - 日語
- ◆ pt_BR - 巴西葡萄牙語
- ◆ es - 西班牙語

3c 儲存並關閉該 `properties` 檔案。

4 從內容檔案所在目錄執行以下指令：

```
install -i silent -f analyzerInstaller.properties
```

14 安裝後任務

安裝 Identity Manager 之後，應設定安裝的驅動程式，以符合您的商業程序定義的規則及要求。您還需要設定 Sentinel Log Management for IGA 以收集稽核事件。安裝後任務通常包含下列項目：

- 「設定已連接系統」(第 139 頁)
- 「建立和設定驅動程式集」(第 139 頁)
- 「建立驅動程式」(第 142 頁)
- 「定義規則」(第 142 頁)
- 「管理驅動程式活動」(第 143 頁)
- 「啟用 Identity Manager」(第 143 頁)

設定已連接系統

Identity Manager 支援應用程式、目錄和資料庫共享資訊。如需特定於驅動程式的組態說明，請參閱 **Identity Manager 驅動程式文件** (<https://www.netiq.com/documentation/identity-manager-49-drivers/>)。

建立和設定驅動程式集

驅動程式集是一個可容納多個 Identity Manager 驅動程式的容器。一次只能將一個驅動程式集關聯到任一伺服器。您可以使用 Designer 工具來建立驅動程式集。如果已將某部伺服器關聯到某個驅動程式集，然後將該伺服器指定到新的驅動程式集，則會從原始驅動程式集中移除該伺服器。

若要支援將密碼同步到 Identity Vault 的功能，Identity Manager 需要驅動程式集具有密碼規則。您可以使用 Identity Manager 中的預設通用密碼規則套件，也可以依據現有的組織要求建立密碼規則。不過，密碼規則必須包括 DirMXL-PasswordPolicy 物件。如果 Identity Vault 中不存在該規則物件，您可以建立該物件。

- 「建立驅動程式集」(第 140 頁)
- 「將預設密碼規則指定給驅動程式集」(第 140 頁)
- 「在 Identity Vault 中建立密碼規則物件」(第 140 頁)
- 「建立自訂密碼規則」(第 141 頁)
- 「在 Identity Vault 中建立預設通知集合物件」(第 141 頁)

建立驅動程式集

Designer for Identity Manager 提供了許多設定供您建立和設定驅動程式集。這些設定可讓您指定全域組態值、驅動程式集套件、驅動程式集具名密碼、記錄層級、追蹤層級和 Java 環境參數。如需詳細資訊，請參閱《[NetIQ Designer for Identity Manager Administration Guide](#)》(NetIQ Designer for Identity Manager 管理指南) 中的「[Configuring Driver Sets](#)」(設定驅動程式集)。

將預設密碼規則指定給驅動程式集

必須將 DirMXL-PasswordPolicy 物件指定給 Identity Vault 中的每個驅動程式集。Identity Manager 預設通用密碼規則套件包括此規則物件。預設規則會安裝並指定通用密碼規則，以控制 Identity Manager 引擎自動為驅動程式產生隨機密碼的方式。

或者，若要使用自訂密碼規則，您必須建立密碼規則物件和規則。如需詳細資訊，請參閱「[在 Identity Vault 中建立密碼規則物件](#)」(第 140 頁)與「[建立自訂密碼規則](#)」(第 141 頁)。

- 1 在 Designer 中開啟您的專案。
- 2 在「大綱」窗格中，展開您的專案。
- 3 展開**套件目錄 > 通用**以驗證預設通用密碼規則套件是否存在。
- 4 (視情況而定) 如果密碼規則套件尚未在 Designer 中列出，請完成以下步驟：
 - 4a 以滑鼠右鍵按一下**套件目錄**。
 - 4b 選取**輸入套件**。
 - 4c 選取 **Identity Manager 預設通用密碼規則**，然後按一下**確定**。
為了確保表格中顯示所有可用的套件，您可能需要取消選取**僅顯示基礎套件**。
- 5 選取每個驅動程式集並指定密碼規則。

在 Identity Vault 中建立密碼規則物件

如果 Identity Vault 中不存在 DirMXL-PasswordPolicy 物件，您可以使用 Designer 或 ldapmodify 公用程式建立該物件。如需如何在 Designer 中執行此操作的詳細資訊，請參閱《[NetIQ Designer for Identity Manager Administration Guide](#)》(NetIQ Designer for Identity Manager 管理指南) 中的「[Configuring Driver Sets](#)」(設定驅動程式集)。若要使用 ldapmodify 公用程式，請執行以下程序：

- 1 在文字編輯器中建立具有以下屬性的 LDAP 資料交換格式 (LDIF) 檔案：

```

dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: add
nsimPwdRuleEnforcement: FALSE
nspmSpecialAsLastCharacter: TRUE
nspmSpecialAsFirstCharacter: TRUE
nspmSpecialCharactersAllowed: TRUE
nspmNumericAsLastCharacter: TRUE
nspmNumericAsFirstCharacter: TRUE
nspmNumericCharactersAllowed: TRUE
nspmMaximumLength: 64
nspmConfigurationOptions: 596
passwordUniqueRequired: FALSE
passwordMinimumLength: 1
passwordAllowChange: TRUE
objectClass: nspmPasswordPolicy

dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: modify
add: nsimAssignments
nsimAssignments: <driverset LDAP dn>

```

附註：依原樣複製該內容可能會在該檔案中插入隱藏的特殊字元。如果您在將這些屬性新增至 **Identity Vault** 時收到 `ldif_record() = 17` 錯誤訊息，請在兩個 **DN** 之間插入一個額外的空格。

- 2 若要在 **Identity Vault** 中新增 **DirXML-PasswordPolicy** 物件，請從 **Identity Manager** 安裝套件的 `install/utilities` 目錄執行 `ldapmodify.exe`，以從檔案中輸入屬性。

建立自訂密碼規則

您可以不使用 **Identity Manager** 中的預設密碼規則，而是依據組織的要求建立新規則。密碼規則可以指定給整個樹狀結構、分割區根容器、容器或特定的使用者。為簡化管理，**NetIQ** 建議在樹狀結構中盡可能高的層級指定密碼規則。如需詳細資訊，請參閱《[Password Management 3.3.2 Administration Guide](#)》(Password Management 3.3.2 管理指南) 中的「[Creating Password Policies](#)」(建立密碼規則)。

附註：您還必須將 **DirXML-PasswordPolicy** 物件指定給驅動程式集。如需詳細資訊，請參閱「[在 Identity Vault 中建立密碼規則物件](#)」(第 140 頁)。

在 Identity Vault 中建立預設通知集合物件

預設通知集合是一個 **Identity Vault** 物件，它包含一組電子郵件通知樣板，以及一個用於傳送自樣板產生的電子郵件的 **SMTP** 伺服器。如果 **Identity Vault** 中不存在預設通知集合物件，請使用 **Designer** 建立該物件。

- 1 在 **Designer** 中開啟您的專案。
- 2 在「大綱」窗格中，展開您的專案。
- 3 以滑鼠右鍵按一下 **Identity Vault**，然後按一下 **Identity Vault 內容**。
- 4 按一下**套件**，然後按一下**新增套件**圖示。

- 5 選取所有通知樣板套件，然後按一下確定。
- 6 按一下套用以透過安裝操作來安裝套件。
- 7 將通知樣板部署到 Identity Vault。

建立驅動程式

若要建立驅動程式，請使用 Designer 中提供的套件管理功能。對於您打算使用的每個 Identity Manager 驅動程式，建立一個驅動程式物件，並輸入驅動程式組態。驅動程式物件包含該驅動程式的組態參數和規則。在建立驅動程式物件的過程中，安裝驅動程式套件，然後依照您環境的要求修改驅動程式組態。

驅動程式套件包含一組預設的規則。這些規則是為了要在實作資料共享模型時，讓您有一個好的起頭。大部份時候，您可以使用隨附的預設組態設定驅動程式，然後依據環境要求修改驅動程式組態。建立並設定驅動程式後，請將其部署到 Identity Vault 並加以啟動。一般而言，驅動程式建立程序涉及以下動作：

1. 輸入驅動程式套件
2. 安裝驅動程式套件
3. 設定驅動程式物件
4. 部署驅動程式物件
5. 啟動驅動程式物件

如需其他資訊和特定於驅動程式的資訊，請參閱 [Identity Manager 驅動程式網站 \(https://www.netiq.com/documentation/identity-manager-49-drivers/\)](https://www.netiq.com/documentation/identity-manager-49-drivers/) 上的相關驅動程式實作指南。

定義規則

規則可讓您針對特定環境，自訂 Identity Vault 的資訊流入和流出。例如，一個公司可能會使用 inetorgperson 做為主要使用者類別，而另一個公司可能會使用 User。為了處理這種情況，系統會建立規則以告知 Identity Manager 引擎一個使用者在各個系統中的名稱。每次影響使用者的操作在已連接系統之間傳遞時，Identity Manager 都會套用進行此變更的規則。

規則還會建立新的物件、更新屬性值、進行綱要轉換、定義相符準則、維護 Identity Manager 關聯和執行其他作業。

NetIQ 建議您使用 Designer 來定義驅動程式規則，以符合您的業務需求。如需詳細的規則指南，請參閱《[NetIQ Identity Manager - Using Designer to Create Policies](#)》(NetIQ Identity Manager - 使用 Designer 建立規則) 指南和《[NetIQ Identity Manager Understanding Policies Guide](#)》(NetIQ Identity Manager 瞭解規則指南)。如需 Identity Manager 使用的文件類型定義 (DTD) 的資訊，請參閱《[Identity Manager DTD Reference](#)》(Identity Manager DTD 參考)。這些資源包含：

- 每個可用規則的詳細描述。
- 深入的「規則產生器」使用者指南和參考，包含每個條件、動作、名詞和動詞的範例和語法。
- 使用 XSLT 樣式表建立規則的相關討論。

管理驅動程式活動

若要執行 Identity Manager 驅動程式的管理和組態功能，請使用 Designer。《[NetIQ Identity Manager Driver Administration Guide](#)》(NetIQ Identity Manager 驅動程式管理指南) 中詳述了這些功能。

啟用 Identity Manager

您無需提供啟用代碼就能安裝或初次執行 Identity Manager。但是，如果您未提供啟用代碼，Identity Manager 將在安裝 90 天後停止運作。在這 90 天內或者 90 天後，您隨時都可以啟用 Identity Manager。如需詳細資訊，請參閱《[NetIQ Identity Manager Overview and Planning Guide](#)》(NetIQ Identity Manager 綜覽和規劃指南) 中的「[Understanding Licensing and Activation](#)」(瞭解授權和啟用)。

VII 升級 Identity Manager

此部分提供升級 Identity Manager 各元件的資訊。若要將現有資料移轉至新伺服器，請參閱第 VIII 部分「將 Identity Manager 資料移轉至新安裝中」(第 185 頁)。如需升級與移轉之間差異的詳細資訊，請參閱「瞭解升級和移轉」(第 148 頁)。

15 升級 Identity Manager 的準備工作

本章提供的資訊可協助您為將 Identity Manager 解決方案升級至最新版本做好準備。您可以根據具體的目標電腦，使用可執行檔、二進位檔案或文字模式升級 Identity Manager 的大多數元件。若要執行升級，您必須下載並解壓縮或解包 Identity Manager 安裝套件。

警告：您必須永遠透過 Identity Manager 修補程式通道來更新隨 Identity Manager 4.9 安裝的元件。否則，您在進行日常的 Identity Manager 修補程式更新期間，可能會遇到嚴重的衝突。

- 「Identity Manager 的升級核對清單」(第 147 頁)
- 「瞭解升級和移轉」(第 148 頁)
- 「支援的升級路徑」(第 150 頁)
- 「備份目前組態」(第 153 頁)

Identity Manager 的升級核對清單

若要執行升級，NetIQ 建議您完成以下核對清單中的步驟：

	核對清單項目
☐	1. 檢閱升級與移轉之間的差異。如需詳細資訊，請參閱「 瞭解升級和移轉 」(第 148 頁)。
☐	2. 升級至 Identity Manager 4.7.5。無法從 4.7.5 之前的版本升級或移轉至版本 4.9。
☐	3. 確保您已取得用於升級 Identity Manager 的最新安裝套件。如需詳細資訊，請參閱《 NetIQ Identity Manager Overview and Planning Guide 》(NetIQ Identity Manager 綜覽和規劃指南)中的「 Where to Get Identity Manager 」(從何處獲取 Identity Manager)。
☐	4. 確保您的電腦符合更新版本 Identity Manager 的硬體和軟體先決條件。
☐	5. 備份目前的專案、驅動程式組態和資料庫。如需詳細資訊，請參閱「 備份目前組態 」(第 153 頁)。
☐	6. 安裝最新版本的 Designer。如需詳細資訊，請參閱「 升級 Designer 」(第 158 頁)。
☐	7. 在執行 Identity Manager 的伺服器上，將 eDirectory 升級至最新的版本和修補程式。
☐	8. 停止與安裝了 Identity Manager 引擎的伺服器相關聯的驅動程式。如需詳細資訊，請參閱「 停止和啟動 Identity Manager 驅動程式 」(第 176 頁)。

	核對清單項目
☐	9. 升級 Identity Manager 引擎。如需詳細資訊，請參閱「升級 Identity Manager 引擎」(第 160 頁)。 附註：若要將 Identity Manager 引擎移轉至新伺服器，可以使用目前 Identity Manager 伺服器上的相同 eDirectory 複製本。如需詳細資訊，請參閱「將 Identity Manager 引擎移轉至新伺服器」(第 192 頁)。
☐	10. (視情況而定) 如果 Identity Manager 引擎的驅動程式集中有任何驅動程式是遠端載入器驅動程式，請升級每個驅動程式的遠端載入器伺服器。如需詳細資訊，請參閱「升級遠端載入器」(第 162 頁)。
☐	11. (視情況而定) 如果使用的是套件，請在現有驅動程式上升級套件以獲取新規則。如需詳細資訊，請參閱「升級 Identity Manager 驅動程式」(第 178 頁)。 僅當套件有更新版本提供，且某個驅動程式規則中包含新的功能，而您想將其新增至現有驅動程式時，才需要執行該操作。
☐	12. (視情況而定) 如果未安裝 SSPR，請加以安裝。如需詳細資訊，請參閱「安裝 SSPR」(第 48 頁)。
☐	13. 升級 Identity Applications。如需詳細資訊，請參閱「升級 Identity Applications」(第 164 頁)。
☐	14. 升級 Identity Reporting。如需詳細資訊，請參閱「升級 Identity Reporting」(第 173 頁)。
☐	15. 啟動與 Identity Applications 和 Identity Manager 引擎關聯的驅動程式。如需詳細資訊，請參閱「停止和啟動 Identity Manager 驅動程式」(第 176 頁)。
☐	16. (視情況而定) 如果您將 Identity Manager 引擎或 Identity Applications 移轉至了某個新伺服器，請將該新伺服器新增至驅動程式集中。如需詳細資訊，請參閱「將新伺服器新增至驅動程式集」(第 180 頁)。
☐	17. (視情況而定) 如果您有自訂的原則和規則，請還原自訂設定。如需詳細資訊，請參閱「將自訂規則還原至驅動程式」(第 181 頁)。
☐	18. 啟用升級後的 Identity Manager 解決方案。如需詳細資訊，請參閱「啟用 Identity Manager」(第 143 頁)。

瞭解升級和移轉

當您要安裝現有 Identity Manager 安裝的更新版本時，通常可以執行**升級**程序。但是，新版 Identity Manager 不提供從現有版本升級的路徑，您需要先升級至可從其升級至 4.9 版的版本。或者，您也可以移轉至新機器。**NetIQ 將移轉**定義為在新伺服器上安裝 Identity Manager，然後將現有資料移轉至此新伺服器的程序。

在產品評估期或者在啟用進階版之後，如果您不想在環境中使用進階版功能，可以**切換**至標準版。Identity Manager 可讓您透過一個簡單的程序從進階版切換至標準版。

升級

一般而言，您可以升級 Identity Manager 4.8 Standard Edition 和 Advanced Edition。

- ♦ **Identity Manager 4.8 Standard Edition**：如果您目前使用的是 Identity Manager 4.8 Standard Edition，則可直接將其升級至 Identity Manager 4.9 Standard Edition。如需詳細資訊，請參閱《[Quick Start Guide for Installing and Upgrading NetIQ Identity Manager 4.9 Standard Edition](#)》(安裝和升級 NetIQ Identity Manager 4.6 Standard Edition 的快速入門指南)。

若要將 Identity Manager 4.8 Standard Edition 升級至 Identity Manager 4.9 Advanced Edition，請選擇以下其中一種方法來完成升級：

- ♦ 將 Identity Manager 4.8 Standard Edition 升級至 Identity Manager 4.9 Standard Edition，然後再升級至 Identity Manager 4.9 Advanced Edition。
- ♦ 將 Identity Manager 4.8 Standard Edition 升級至 Identity Manager 4.8 Advanced Edition，然後再升級至 Identity Manager 4.9 Advanced Edition。
- ♦ **Identity Manager 4.8 Advanced Edition**：如果您目前使用的是 Identity Manager 4.8 Advanced Edition，則可直接將其升級至 Identity Manager 4.9 Advanced Edition。如需詳細資訊，請參閱「[Identity Manager 的升級核對清單](#)」(第 147 頁)。

移轉

在某些情況下，您無法進行直接升級。此時最好採用移轉方式。例如，如果之前裝有 Identity Manager 的伺服器所執行的作業系統不再受支援，則您必須執行移轉，而不是升級。

如果您的多部伺服器都與某個驅動程式集關聯，您可以一次在一部伺服器上執行一個升級或移轉。若您沒有時間同時升級多個伺服器，驅動程式會繼續使用不同版本的 Identity Manager，直到每個伺服器的升級完成。

重要：若您啟用僅受 Identity Manager 4.9 或以上版本支援的驅動程式功能，則在具有混合版本的伺服器上，驅動程式會停止運作。舊版引擎無法處理新功能。因此，在所有伺服器都升級至 Identity Manager 4.9 或以上版本之前，驅動程式將無法運作。

從進階版切換到標準版

Identity Manager 允許您在產品試用期內或啟用進階版後從進階版切換到標準版。

重要：如果您已套用進階版啟用碼，則不需要切換至標準版，因為標準版的所有功能在進階版中都有提供。僅當您不想在環境中使用任何進階版功能，並且要縮減 Identity Manager 部署時，才需要切換至標準版。如需詳細資訊，請參閱第 17 章「[從進階版切換到標準版](#)」(第 183 頁)。

支援的升級路徑

Identity Manager 4.9 支援從 4.7.x 和 4.8.x 版本升級。NetIQ 建議您在開始升級前先查看目前版本的版本說明中的資訊。

- 「從 Identity Manager 4.7.5 版本升級」(第 150 頁)
- 「從 Identity Manager 4.8.x 版本升級」(第 151 頁)

從 Identity Manager 4.7.5 版本升級

如果您已安裝 Identity Manager 4.7.5 http，則必須更新至 Identity Manager 4.7.5 https。確定已提供 tomcat.ks 和 idm.jks，若要建立這些檔案，請參閱《[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)》(NetIQ Identity Manager - Identity Applications 管理員指南) 中的「[Using SSL for Secure Communication](#)」(使用 SSL 進行安全通訊)。

下表列出了 Identity Manager 4.7.5 版本的元件範圍升級路徑：

元件	基礎版本	升級後的版本
Identity Manager 引擎	4.7.5	1. 將作業系統升級至支援的版本。 2. 將 Identity Vault 升級至 9.2.9 3. 將 Identity Manager 引擎升級至 4.9。
遠端載入器 / 擴送代理程式	4.7.5	安裝 4.9 版遠端載入器 / 擴送代理程式。
Designer		安裝 Designer 4.9。
Analyzer		安裝 Analyzer 4.8.5

元件	基礎版本	升級後的版本
Identity Applications	4.7.5	升級 Identity Applications 前，請確定 Identity Vault 和 Identity Manager 引擎已分別升級至 9.2.9 和 4.9。 1. 將作業系統升級至支援的版本。 2. 將資料庫升級至支援的版本。如需受支援的資料庫版本，請參閱 NetIQ Identity Manager 技術資訊網站。 3. (視情況而定) 如果 SSPR 安裝在其他電腦上，請將該元件升級至 4.9 版本。 4. 更新使用者應用程式驅動程式以及角色與資源驅動程式套件。 5. 將 Identity Applications 升級至 4.9。 6. 停止 Tomcat。 附註：升級後，不會將舊的 jre 檔案重新放置到備份目錄，而是將其保留在以下位置：C:\NetIQ\idm\apps\jre
Identity Reporting	4.7.5	1. 將作業系統升級至支援的版本。 2. 將資料庫升級至支援的版本。如需受支援資料庫版本的詳細資訊，請參閱 System Requirements for Identity Manager 4.9 (Identity Manager 4.9 系統要求)。 3. 將 SLM for IGA 升級至支援的版本。 4. 將 Identity Reporting 升級至 4.9。 5. (視情況而定) 從 Identity Manager 的「資料收集服務」頁面建立資料同步規則。

NetIQ 建議開始升級前先在 Identity Manager [文件](#) 頁面您所用版本的版本說明中查看相關資訊。

附註：升級後，確定已提供 tomcat.ks 和 idm.jks，若要建立這些檔案，請參閱《[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)》(NetIQ Identity Manager - Identity Applications 管理員指南) 中的「[Using SSL for Secure Communication](#)」(使用 SSL 進行安全通訊)。

從 Identity Manager 4.8.x 版本升級

下表列出了 Identity Manager 4.8.x 版本的元件範圍升級路徑：

元件	基礎版本	升級後的版本
Identity Manager 引擎	4.8.x	1. 將作業系統升級至支援的版本。 2. 將 Identity Vault 升級至 9.2.9 3. 將 Identity Manager 引擎升級至 4.9。
遠端載入器 / 擴送代理程式	4.8.x	安裝 4.9 版遠端載入器 / 擴送代理程式。
Designer		安裝 Designer 4.9。
Analyzer		安裝 Analyzer 4.8.5。
Identity Applications	4.8.x	升級 Identity Applications 前，請確定 Identity Vault 和 Identity Manager 引擎已分別升級至 9.2.9 和 4.9。 1. 將作業系統升級至支援的版本。 2. 將資料庫升級至支援的版本。如需受支援的資料庫版本，請參閱 NetIQ Identity Manager 技術資訊網站 (https://www.netiq.com/products/identity-manager/advanced/technical-information/)。 3. (視情況而定) 如果 SSPR 安裝在其他電腦上，請將該元件升級至 4.9 版本。 4. 更新使用者應用程式驅動程式以及角色與資源驅動程式套件。 5. 將 Identity Applications 升級至 4.9。 6. 停止 Tomcat。
Identity Reporting	4.8.x	1. 將作業系統升級至支援的版本。 2. 將資料庫升級至支援的版本。如需受支援資料庫版本的詳細資訊，請參閱 System Requirements for Identity Manager 4.9 (Identity Manager 4.9 系統要求)。 3. 將 SLM for IGA 升級至受支援版本 (只能在 Linux 電腦上安裝) 4. 更新資料收集服務和受管理服務閘道驅動程式套件。 5. 升級 Identity Reporting 4.9。 6. (視情況而定) 從 Identity Manager 的「資料收集服務」頁面建立資料同步規則。

NetIQ 建議開始升級前先在 [Identity Manager 文件](#) 頁面您所用版本的版本說明中查看相關資訊。

備份目前組態

NetIQ 建議您在升級之前備份 Identity Manager 解決方案的目前組態。您無需執行額外的步驟即可備份使用者應用程式。所有使用者應用程式組態皆已儲存在使用者應用程式驅動程式中。您可透過以下方法建立備份：

- ◆ 「輸出 Designer 專案」 (第 153 頁)
- ◆ 「輸出驅動程式的組態」 (第 154 頁)

輸出 Designer 專案

Designer 專案包含綱要及所有驅動程式組態資訊。透過建立 Identity Manager 解決方案專案，您可以在一個步驟中輸出所有驅動程式，而無需針對每個驅動程式建立單獨的輸出檔案。

- ◆ 「輸出目前的專案」 (第 153 頁)
- ◆ 「從 Identity Vault 建立新專案」 (第 154 頁)

輸出目前的專案

如果已經有 Designer 專案，請確認專案中的資訊是否與 Identity Vault 中的資訊同步：

- 1 在 Designer 中開啟您的專案。
- 2 在模型產生器中，請在 Identity Vault 上按一下滑鼠右鍵，然後選取即時 > 比較。
- 3 評估專案並調整差異，然後按一下確定。
如需詳細資訊，請參閱《[NetIQ Designer for Identity Manager Administration Guide](#)》(NetIQ Designer for Identity Manager 管理指南) 中的「[Using the Compare Feature When Deploying](#)」(在部署時使用比較功能)。
- 4 在工具列上選取專案 > 輸出。
- 5 按一下全選，以全選所有資源來加以輸出。
- 6 選取專案的儲存位置及儲存格式，然後按一下完成。

將專案儲存在目前工作空間以外的任何位置。升級至 Designer 時，必須建立新的工作空間位置。如需詳細資訊，請參閱《[NetIQ Designer for Identity Manager Administration Guide](#)》(NetIQ Designer for Identity Manager 管理指南) 中的「[Exporting a Project](#)」(輸出專案)。

從 Identity Vault 建立新專案

如果您沒有適合目前 Identity Manager 解決方案的 Designer 專案，則必須建立一個專案，以備份目前的解決方案。

- 1 安裝 Designer。
- 2 啟動 Designer，然後為工作空間指定位置。
- 3 選取是否要檢查線上更新，然後按一下**確定**。
- 4 在「歡迎」頁上，按一下**執行 Designer**。
- 5 在工具列上，選取**專案 > 輸入專案 > Identity Vault**。
- 6 指定專案名稱，然後針對專案使用預設位置或選取不同位置。
- 7 按**下一步**。
- 8 指定以下用於連接 Identity Vault 的值：
 - ◆ **主機名稱**：代表 Identity Vault 伺服器的 IP 位址或 DNS 名稱
 - ◆ **使用者名稱**：代表用於向 Identity Vault 進行驗證的使用者 DN
 - ◆ **密碼**：代表驗證使用者的密碼
- 9 按**下一步**。
- 10 讓 Identity Vault 綱要和「預設通知集合」維持選取狀態。
- 11 展開「預設通知集合」，然後取消選取不需要的語言。
「預設通知集合」會翻譯成多種語言。您可以輸入所有語言或只選取您使用的語言。
- 12 按一下**瀏覽**，然後瀏覽至要輸入的驅動程式集並加以選取。
- 13 針對此 Identity Vault 內的每個驅動程式集重複**步驟 12**，然後按一下**完成**。
- 14 專案輸入後按一下**確定**。
- 15 若您只有一個 Identity Vault，則所有作業已完成。如果您有多個 Identity Vault，請繼續進行**步驟 16**。
- 16 按一下工具列上的**即時 > 輸入**。
- 17 對其他各個 Identity Vault 重複**步驟 8**到**步驟 14**。

輸出驅動程式的組態

建立驅動程式的輸出可以製作目前組態的備份。但是，Designer 目前並不會建立角色授權驅動程式和規則的備份。

使用 Designer 輸出驅動程式組態

- 1 驗證 Designer 中的專案具有最新版本的驅動程式。如需詳細資訊，請參閱《[NetIQ Designer for Identity Manager Administration Guide](#)》(NetIQ Designer for Identity Manager 管理指南) 中的「[Importing a Library, a Driver Set, or a Driver from the Identity Vault](#)」(從 Identity Vault 輸入程式庫、驅動程式集或驅動程式)。
- 2 在「模型產生器」中，於您要升級之驅動程式所在的行上按一下滑鼠右鍵。

- 3 選取「輸出至組態檔案」。
- 4 瀏覽至要儲存組態檔案的位置，然後按一下「儲存」。
- 5 在結果頁面上按一下「確定」。
- 6 對每個驅動程式重複步驟 1 到步驟 5。

16 升級 Identity Manager 的元件

本章提供關於升級 Identity Manager 各個元件的具體資訊。本章還提供了可能需要在升級後執行的步驟。

- ◆ 「升級注意事項」 (第 157 頁)
- ◆ 「升級順序」 (第 157 頁)
- ◆ 「升級 Designer」 (第 158 頁)
- ◆ 「升級 Identity Manager 引擎元件」 (第 159 頁)
- ◆ 「升級 Identity Applications」 (第 164 頁)
- ◆ 「升級 Identity Reporting」 (第 173 頁)
- ◆ 「升級 Analyzer」 (第 176 頁)
- ◆ 「停止和啟動 Identity Manager 驅動程式」 (第 176 頁)
- ◆ 「升級 Identity Manager 驅動程式」 (第 178 頁)
- ◆ 「將新伺服器新增至驅動程式集」 (第 180 頁)
- ◆ 「將自訂規則還原至驅動程式」 (第 181 頁)

升級注意事項

- ◆ 從 Identity Manager 4.9 開始，已棄用對 NetIQ SecretStore 的支援。升級至最新的 UAD 套件並重新啟動 Tomcat 後，NetIQ SecretStore 儲存庫中的所有現有密碼將自動移轉至 `notfSMTPMailPassword` 屬性。此密碼移轉程序由 `ism-configuration.properties` 檔案中的 `com.netiq.idm.migrate.secretstore` 內容控制。依預設，此內容設定為 `true`。移轉完成後，該內容將自動設定回 `false` 並一直保持此狀態。
- ◆ 在將 Identity Applications 元件從 Identity Manager 4.7.5 升級至 4.9 之前，請先使用工作流程移轉工具，將資料從 Identity Applications 資料庫 (`idmuserappdb`) 輸出至工作流程引擎資料庫 (`igaworkflowdb`)。如需詳細資訊，請參閱《[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)》(NetIQ Identity Manager - Identity Applications 管理員指南) 中的「[Migrating Data from Identity Applications Database into Workflow Engine Database](#)」(將資料從 Identity Applications 資料庫移轉至工作流程引擎資料庫)。

升級順序

必須依照以下順序來升級 Identity Manager 的各元件：

1. Designer
2. Sentinel Log Management for IGA (只能在 Linux 電腦上安裝)

3. Identity Vault
4. Identity Manager 引擎
5. 遠端載入器
6. 擴送代理程式
7. Identity Applications (適用於進階版)
8. Identity Reporting
9. Analyzer
10. Self Service Password Reset

升級 Designer

附註：此版本不支援從舊版本升級 **Designer**，因此如果您安裝了舊版本，則需要在安裝 **Designer 4.9** 之前先將其解除安裝。此外，無法使用內建自動更新和離線更新功能升級至 **Designer 4.9**。

- 1 以管理員身分登入安裝了 **Designer** 的伺服器。
- 2 若要建立專案的備份副本，請輸出您的專案。
如需輸出的詳細資訊，請參閱《*NetIQ Designer for Identity Manager Administration Guide*》(NetIQ Designer for Identity Manager 管理指南) 中的「[Exporting a Project](#)」(輸出專案)。
- 3 若要解除安裝 **Designer**，請先將其關閉，然後根據作業系統將其解除安裝：
使用用於新增和移除程式的控制台公用程式。例如，在 **Windows Server 2008** 上，按一下程式和功能。在 **Designer for Identity Manager** 上按一下滑鼠右鍵，然後按一下**解除安裝**。
- 4 啟動 **Identity_Manager_4.9_Designer_Windows.zip** 檔案中的 **Designer** 安裝程式。
(<Designer zip 檔案解壓縮位置>\designer_install\install.exe)
- 5 依照精靈中的步驟操作，直到安裝程序完成。
- 6 安裝 **Designer 4.9** 後，必須輸入舊版本中的所有 **Designer** 專案。當您啟動輸入程序時，**Designer** 會執行專案轉換器精靈，用於將舊專案轉換為目前版本。在精靈中，選取複製專案至工作空間。如需專案轉換器的詳細資訊，請參閱《*NetIQ Designer for Identity Manager Administration Guide*》(NetIQ Designer for Identity Manager 管理指南) 中的「[Converting Earlier Projects](#)」(轉換舊專案)。

升級 Identity Manager 引擎元件

在升級 Identity Manager 引擎前，請務必先升級 Identity Vault。Identity Manager 引擎升級程序會更新主機電腦檔案系統中儲存的驅動程式 shim 檔案。

升級 Identity Vault

- 1 依照《[NetIQ Identity Manager Overview and Planning Guide](#)》(NetIQ Identity Manager 綜覽和規劃指南) 中的「[Where to Get Identity Manager](#)」(從何處獲取 Identity Manager) 所述下載 Identity_Manager_4.9.0_Windows.iso。
- 2 掛接下載的 .iso。
- 3 導覽至 <iso 掛接位置>\IdentityManagerServer\products\eDirectory\x64 目錄。
- 4 執行 eDirectory_929_Windows_x86_x64.exe 檔案。
- 5 在基本索引標籤中指定以下詳細資料：
 - ◆ 如果您選取了新網路樹，請指定以下詳細資料：
 - ◆ 網路樹名稱：指定 Identity Vault 的網路樹名稱。
 - ◆ 伺服器 FDN：指定伺服器 FDN。

附註：雖然 Identity Vault 允許您為 NCP 伺服器物件設定最多包含 256 個字元的 FDN，但 NetIQ 建議您將該變數限制為一個較小的值，因為 Identity Vault 會根據此物件的長度來建立較長的其他物件。

- ◆ 網路樹管理員：指定 Identity Vault 的管理員名稱。
 - ◆ 管理員密碼：指定管理員密碼。
 - ◆ 如果選取了現有網路樹，請指定以下詳細資料：
 - ◆ IP 位址：指定 Identity Vault 現有網路樹的 IP 位址。
 - ◆ 連接埠號碼：指定現有網路樹的連接埠號碼。預設值為 524。
 - ◆ 伺服器 FDN：指定伺服器 FDN。
 - ◆ 網路樹管理員：指定 Identity Vault 的現有管理員名稱。
 - ◆ 管理員密碼：指定管理員密碼。
- 6 (視情況而定) 在進階索引標籤中指定以下詳細資料：
 - ◆ 若要在 Identity Vault 伺服器上使用 IPv6 位址，請選取啟用 IPv6。

附註：NetIQ 建議您啟用此選項。若要在安裝後啟用 IPv6 位址，必須再次執行安裝程式。

- ◆ 若要啟用增強型背景驗證 (EBA)，請選取啟用 EBA。
 - ◆ 指定 HTTP 純文字連接埠和安全連接埠。預設值分別為 8028 和 8030。
 - ◆ 指定 LDAP 純文字連接埠和安全連接埠。預設值分別為 389 和 636。
- 7 在安裝位置欄位中，指定 Identity Vault 的安裝位置。

- 8 在 **DIB 位置欄位** 中，指定 DIB 檔案所在的位置。
- 9 按一下**升級並繼續**進行升級過程。

升級 Identity Manager 引擎

驗證是否已停止驅動程式。如需詳細資訊，請參閱「[停止驅動程式](#)」(第 176 頁)。

升級 Identity Manager 引擎需要執行的步驟如下：

- 1 從 NetIQ 下載網站下載 Identity_Manager_4.9.0_Windows.iso。
- 2 掛接下載的 .iso。
- 3 導覽至 <ISO 安裝位置>\IdentityManagerServer 資料夾，然後執行 install.exe。
- 4 選取安裝時要使用的語言，然後按一下**確定**。
- 5 在「簡介」頁面中按下一步。
- 6 閱讀並接受授權合約，然後按下一步。
安裝的元件及其版本即會顯示。
- 7 選取 **Identity Manager 引擎**，然後按下一步。
- 8 指定以下詳細資料：
Identity Vault 管理員：指定 Identity Vault 管理員名稱。
Identity Vault 管理員密碼：指定 Identity Vault 管理員密碼。
- 9 從以下選項中選取要安裝的 Identity Manager 版本：
 - ◆ 標準版
 - ◆ 進階版

附註：請務必選取與前一發行版 (version) 相同的版本 (edition)。

- 10 指定 Identity Manager 引擎的組態設定。如需詳細資訊，請參閱「[Identity Manager 引擎的組態工作表](#)」(第 49 頁)。
- 11 在「升級前摘要」頁面中查看設定，然後按一下**升級**。

使用 MapDB 3.0.5

MapDB 是 Identity Manager 引擎的附加元件，以下 Identity Manager 驅動程式會使用該元件：

- ◆ 資料收集服務
- ◆ JDBC
- ◆ LDAP
- ◆ 受管理系統閘道
- ◆ Office 365 和 Azure Active Directory
- ◆ Salesforce

如果您使用上述任何驅動程式，在升級驅動程式之前必須先查看以下章節：

- 「[瞭解各驅動程式版本對 Identity Manager 4.9 引擎的支援](#)」(第 161 頁)
- 「[手動移除 MapDB 快取檔案](#)」(第 161 頁)

瞭解各驅動程式版本對 Identity Manager 4.9 引擎的支援

在升級使用 MapDB 的 Identity Manager 驅動程式之前，請先查看以下注意事項：

- Identity Manager 4.9 隨附的驅動程式與 Identity Manager 4.9 引擎或遠端載入器相容。必須遵循特定驅動程式實作指南中的驅動程式升級步驟。
- 早於 Identity Manager 4.9 的版本隨附的驅動程式與 Identity Manager 4.9 引擎或遠端載入器不相容。
- Identity Manager 4.9 隨附的驅動程式與 Identity Manager 4.8.x 引擎或遠端載入器不反向相容。
- Identity Manager 4.9 隨附的驅動程式與 Identity Manager 4.7.x 引擎或遠端載入器不反向相容。

手動移除 MapDB 快取檔案

Identity Manager 引擎升級程序會在 Identity Vault 的 DIB 目錄中保留一些現有的 MapDB 快取檔案(dx*)。升級驅動程式之後，您必須手動移除該驅動程式的這些檔案。此動作可確保您的驅動程式能正常與 Identity Manager 4.9 引擎配合工作。

下表列出了必須移除的 MapDB 快取檔案：

Identity Manager 驅動程式	要移除的 MapDB 狀態快取檔案
資料收集服務	DCSDriver_< 驅動程式例項 GUID>-* < 驅動程式例項 GUID>-*
JDBC	jdbc_< 驅動程式例項 GUID>_*
LDAP	ldap_< 驅動程式例項 GUID>*
受管理系統閘道	MSGW-< 驅動程式例項 GUID>.*
Office 365 和 Azure Active Directory	<Azure 驅動程式名稱>_obj.db.*
Salesforce	<Salesforce 驅動程式名稱>.* <Salesforce 驅動程式名稱>

其中，* 表示 MapDB 狀態快取檔案的名稱。對於 Salesforce 驅動程式，也使用驅動程式名稱來表示 MapDB 狀態快取檔案。下面是這些檔案的一些範例。

- DCSDriver_< 驅動程式例項 GUID>-0.t、< 驅動程式例項 GUID>-1.p
- jdbc_< 驅動程式例項 GUID>_0.t、jdbc_< 驅動程式例項 GUID>_1
- ldap_< 驅動程式例項 GUID>b、ldap_< 驅動程式例項 GUID>b.p

- ◆ MSGW-< 驅動程式例項 GUID>.p、MSGW-< 驅動程式例項 GUID>.t
- ◆ <Azure 驅動程式名稱>_obj.db.t、<Azure 驅動程式名稱>_obj.db.p
- ◆ <Salesforce 驅動程式名稱>.p、<Salesforce 驅動程式名稱>.t、Salesforce driver1

升級遠端載入器

如果您在執行遠端載入器，則需要升級遠端載入器的檔案。

附註：在升級 *.NET* 遠端載入器之前，請確定已在系統上成功安裝所有 Windows 更新。

- 1 建立遠端載入器組態檔案的備份。檔案的預設位置為
C:\...\RemoteLoader\remoteloadername-config.txt。
- 2 驗證是否已停止驅動程式。如需說明，請參閱《[NetIQ Identity Manager Driver Administration Guide](#)》(NetIQ Identity Manager 驅動程式管理指南) 中的「[Stopping, Starting, or Restarting a Driver in Designer](#)」(在 Designer 中停止、啟動或重新啟動驅動程式)。
- 3 停止每一個驅動程式的遠端載入器服務或精靈。
在「遠端載入器主控台」中，選取遠端載入器例項，然後按一下「停止」。
- 4 使用 Windows 工作管理員停止 cache 程序。
- 5 從 NetIQ 下載網站下載 Identity_Manager_4.9.0_Windows.iso。
- 6 掛接下載的 .iso。
- 7 導覽至 <ISO 安裝位置>\IdentityManagerServer 資料夾，然後執行 install.exe。
- 8 選取安裝時要使用的語言，然後按一下**確定**。
- 9 在「簡介」頁面中按下一步。
- 10 閱讀並接受授權合約，然後按下一步。
安裝的元件及其版本即會顯示。
- 11 選取 **遠端載入器服務**並按下一步。
- 12 在「升級前摘要」頁面中按下一步。
- 13 完成升級後，驗證組態檔案是否包含環境的資訊。
- 14 (視情況而定)如果組態檔案有問題，請複製您在步驟 1 中建立的備份檔案。否則，請繼續下一步。
- 15 啟動每一個驅動程式的遠端載入器服務或精靈。

重要：如果您的驅動程式使用 MapDB，請在升級該驅動程式之後，手動移除其現有的 MapDB 狀態快取檔案。之所以需要這樣做，是因為 Identity Manager 引擎升級程序不會從 Identity Vault 的 DIB 目錄中移除所有這些檔案。如需詳細資訊，請參閱「[使用 MapDB 3.0.5](#)」(第 160 頁)。

升級 Java 遠端載入器

- 1 建立遠端載入器組態檔案的備份。檔案的預設位置為
C:\...\RemoteLoader\remoteloadername-config.txt。
- 2 驗證是否已停止驅動程式。如需說明，請參閱《[NetIQ Identity Manager Driver Administration Guide](#)》(NetIQ Identity Manager 驅動程式管理指南) 中的「[Stopping, Starting, or Restarting a Driver in Designer](#)」(在 Designer 中停止、啟動或重新啟動驅動程式)。
- 3 停止每一個驅動程式的遠端載入器服務或精靈。
在「遠端載入器主控台」中，選取遠端載入器例項，然後按一下「停止」。
- 4 使用 Windows 工作管理員停止 lcache 程序。
- 5 從 NetIQ 下載網站下載 Identity_Manager_4.9.0_Windows.iso。
- 6 掛接下載的 .iso。
- 7 導覽至 <ISO 安裝位置
>\IdentityManagerServer\products\IDM\java_remoteloader 資料夾。
- 8 複製並取代現有 Java 遠端載入器安裝目錄中的 dirxml_jremote_dev.tar.gz 檔案。
- 9 依據現有設定中的檔案，複製並取代現有 Java 遠端載入器安裝目錄中的以下檔案之一：
 - ◆ dirxml_jremote.tar.gz
 - ◆ dirxml_jremote_mvs.tar
- 10 將步驟 8 和 9 中複製的檔案解壓縮。
使用 7-zip 或受支援軟體解壓縮 .tar.gz 檔案。
- 11 (視情況而定) 如果組態檔案有問題，請複製您在步驟 1 中建立的備份檔案。否則，請繼續下一步。

附註：請使用 version.txt 檔案來確保 Java 遠端載入器版本是最新的。

- 12 啟動每一個驅動程式的遠端載入器服務或精靈。

升級擴送代理程式

驗證是否已停止驅動程式。如需詳細資訊，請參閱「[停止驅動程式](#)」(第 176 頁)。

升級 Identity Manager 引擎需要執行的步驟如下：

- 1 從 NetIQ 下載網站下載 Identity_Manager_4.9.0_Windows.iso。
- 2 掛接下載的 .iso。
- 3 導覽至 <ISO 安裝位置>\IdentityManagerServer 資料夾，然後執行 install.exe。
- 4 選取安裝時要使用的語言，然後按一下確定。
- 5 在「簡介」頁面中按下一步。
- 6 閱讀並接受授權合約，然後按下一步。
安裝的元件及其版本即會顯示。

- 7 選取擴送代理程式，然後按下一步。
- 8 在「升級前摘要」頁面中查看設定，然後按一下升級。
- 9 啟動擴送代理程式服務。

升級 Identity Applications

本節提供關於升級 Identity Applications 和支援軟體的資訊，其中包括更新以下元件的內容：

- ◆ Identity Manager 使用者應用程式
- ◆ One SSO Provider (OSP)
- ◆ Self-Service Password Reset (SSPR)
- ◆ Tomcat、JDK 和 ActiveMQ

升級後，元件會升級至以下版本：

- ◆ Tomcat – 9.0.85-1
- ◆ ActiveMQ – 5.18.3-1
- ◆ Java 11
- ◆ One SSO Provider – 6.3.4
- ◆ Self-Service Password Reset – 4.4.0.3
- ◆ Identity Applications – 4.9
- ◆ Identity Reporting - 6.5

本節提供關於以下主題的資訊：

- ◆ 「瞭解升級程式」(第 165 頁)
- ◆ 「升級先決條件」(第 165 頁)
- ◆ 「系統要求」(第 165 頁)
- ◆ 「升級 PostgreSQL 資料庫」(第 165 頁)
- ◆ 「升級 Identity Applications 的驅動程式套件」(第 167 頁)
- ◆ 「升級 Identity Applications」(第 167 頁)
- ◆ 「升級後任務」(第 169 頁)

瞭解升級程式

升級程序會從現有元件中讀取組態值。這些資訊包括 `ism-configuration.properties`、`server.xml`、`SSPRConfiguration.xml` 和其他組態檔案。升級程序會使用這些組態檔案在內部叫用各元件的升級程式。此外，此程式還會建立目前安裝的備份。

升級先決條件

如果您的資料庫是透過 SSL 設定的，請在位於 `C:\NetIQ\idm\apps\tomcat\conf` 路徑下的 `server.xml` 檔案中，以 `sslmode=require` 取代 `ssl=true`。

例如，將

```
jdbc:postgresql://<postgres db>:5432/idmuserappdb?ssl=true
```

變更為

```
jdbc:postgresql://<postgres db>:5432/idmuserappdb?sslmode=require
```

系統要求

升級程序會為所安裝元件的目前組態建立備份。確認伺服器具有足夠儲存備份的空間，另外還有可供升級的可用空間。

升級 PostgreSQL 資料庫

重要：升級過程可能需要一段時間，時間長短取決於資料庫大小。因此，請相應規劃您的升級。

- 1 停止伺服器上正在執行的 PostgreSQL 服務。
- 2 重新命名 `C:\Netiq\idm\apps` 中的 `postgres` 目錄。
例如，將 `postgres` 重新命名為 `postgresql_old`。
- 3 執行以下指令以移除舊服務：

```
sc delete <postgres 服務名稱>
```
- 4 安裝作業系統支援的 PostgreSQL 版本。
選擇的位置必須與 PostgreSQL 的目前安裝位置不同。
 - 4a 掛接 `Identity_Manager_4.9.0_Windows.iso` 影像檔，然後導覽至 `\common\postgres_tomcat` 目錄。
 - 4b 執行 `TomcatPostgreSQL.exe` 檔案。
安裝期間，請只選取 **PostgreSQL** 選項。

附註：

- ◆ 不要在 **PostgreSQL** 詳細資料頁面中提供任何資料庫詳細資料。確定取消選取了**建立資料庫登入帳戶**和**建立空資料庫**。
- ◆ 確定您擁有新舊 **PostgreSQL** 安裝目錄的管理員特權。

-
- 5 停止新安裝的 **PostgreSQL** 服務。移至**服務**，搜尋 **<PostgreSQL 版本號碼>** 服務，然後停止該服務。

附註：相應的使用者在提供有效的驗證資訊後，可以執行停止操作。

- 6 透過執行以下動作來變更新安裝的 **PostgreSQL** 目錄的許可權：

建立一個 **postgres** 使用者：

1. 移至**控制台 > 使用者帳戶 > 使用者帳戶 > 管理帳戶**。
2. 按一下**新增使用者帳戶**。
3. 在「**新增使用者**」頁面中，指定 **postgres** 做為使用者名稱，並提供該使用者的密碼。

為 **postgres** 使用者提供對現有和新安裝的 **PostgreSQL** 目錄的許可權：

1. 在 **PostgreSQL** 目錄上按一下滑鼠右鍵，然後移至**內容 > 安全性 > 編輯**。
2. 為該使用者選取**完全控制**，以提供完全許可權。
3. 按一下**套用**。

- 7 以 **postgres** 使用者的身分存取 **PostgreSQL** 目錄。

1. 以 **postgres** 使用者身分登入伺服器。

在登入之前，請驗證是否允許 **postgres** 使用者建立遠端連接，以確定此使用者可連接到 **Windows** 伺服器。

2. 刪除新 **postgres** 安裝位置中的資料目錄。例如，
C:\NetIQ\idm\apps\postgres\data
3. 開啟指令提示符，然後使用以下指令設定 **PGPASSWORD**：

```
set PGPASSWORD=<your pg password>
```

4. 切換至新安裝的 **PostgreSQL** 目錄。
5. 以 **postgres** 資料庫使用者身分執行 **initdb**。

```
initdb.exe -D <新資料目錄> -E UTF8 -U postgres
```

例如：

```
initdb.exe -D C:\NetIQ\idm\apps\postgres\data -E UTF8 -U postgres
```

- 8 從新 **PostgreSQL** 的 **bin** 目錄升級 **PostgreSQL**。執行以下指令，然後按一下 **Enter**。

附註：確定已在 C:\NetIQ\idm\apps\postgres\data\ 目錄下的 **pg_hba.conf** 中，將方法類型由 **md5** 設定為 **trust**。

```
pg_upgrade.exe --old-datadir "C:\NetIQ\idm\apps1\postgres\data" --new-  
datadir "C:\NetIQ\idm\apps1\postgresql962\data" --old-bindir  
"C:\NetIQ\idm\apps1\postgres\bin" --new-bindir  
"C:\NetIQ\idm\apps1\postgresql962\bin"
```

- 9 成功升級後，以舊 postgres 資料目錄中的檔案取代新 postgres 目錄 (C:\NetIQ\idm\apps\postgres\data) 中的 pg_hba.conf 和 postgresql.conf 檔案。
- 10 啟動升級後的 PostgreSQL 資料庫服務。
移至服務，搜尋 <PostgreSQL 版本號碼> 服務，然後啟動該服務。

附註：相應的使用者在提供有效的驗證資訊後，可以執行啟動操作。

- 11 停用舊 PostgreSQL 服務，以確定該服務不會自動啟動。
- 12 (選擇性) 從新安裝的 PostgreSQL 服務的 bin 目錄中刪除舊資料檔案。
 1. 以 postgres 使用者的身分登入。
 2. 導覽至 bin 目錄，並執行 analyze_new_cluster.bat 和 delete_old_cluster.bat 檔案。
例如：C:\NetIQ\idm\apps\postgresql\bin

附註：僅當您想要刪除舊資料檔案時，才需要執行此步驟。

升級 Identity Applications 的驅動程式套件

您必須停止 Tomcat，並將使用者應用程式驅動程式及角色與資源服務驅動程式的套件更新至最新版本。如需將套件升級至最新版本的資訊，請參閱《[NetIQ Designer for Identity Manager Administration Guide](#)》(NetIQ Designer for Identity Manager 管理指南) 中的「[Upgrading Installed Packages](#)」(升級安裝的套件)。

升級使用者應用程式驅動程式套件後，必須手動新增工作流程範本套件：

- 1 在 Designer 中，導覽至 使用者應用程式驅動程式 > 內容。
- 2 依次按一下「套件」、.
- 3 選取建立工作流程範本。
- 4 按一下確定，然後按一下完成以完成安裝。
- 5 部署使用者應用程式驅動程式。

重要：如果在升級使用者應用程式驅動程式的過程中安裝或升級了任何電子郵件通知範本，則需要部署預設通知集物件。

升級 Identity Applications

下面的程序說明了如何升級以下元件：

- ◆ Identity Applications
- ◆ OSP

- ◆ Tomcat
- ◆ PostgreSQL
- ◆ SSPR (如果與 Identity Applications 安裝在同一部電腦上)
- ◆ ActiveMQ

升級 Identity Applications 需要執行的步驟如下：

- 1 從 NetIQ 下載網站下載 Identity_Manager_4.9.0_Windows.iso。
- 2 掛接下載的 .iso。
- 3 導覽至 <ISO 安裝位置>\IdentityApplications 資料夾，然後執行 install.exe。
- 4 選取安裝時要使用的語言，然後按一下**確定**。
- 5 在「簡介」頁面中按一下**下一步**。
- 6 閱讀並接受授權合約，然後按一下**下一步**。
安裝的元件及其版本即會顯示。
- 7 選取 **Identity Applications**，然後按一下**下一步**。
- 8 指定 Identity Applications 的組態設定。如需詳細資訊，請參閱「[Identity Applications 的組態工作表](#)」(第 50 頁)。

附註：

- ◆ 如果您將 PostgreSQL 資料庫安裝到 Identity Applications 所在的同一部伺服器上，NetIQ 建議使用 Identity Manager 安裝程式來建立工作流程資料庫。
 - ◆ 升級時，您必須手動指定資料庫 JDBC JAR 檔案。例如，如果您使用的是 PostgreSQL 資料庫，則需要指定位於 tomcat\lib 資料夾之外的資料庫 JAR 檔案的位置。
-

- 9 在「升級前摘要」頁面中查看設定，然後按一下**升級**。

依據元件的安裝位置，安裝程序會在該位置建立備份目錄，並將時戳(指示備份時間)附加至備份目錄。

例如：

- ◆ Tomcat – C:\NetIQ\idm\apps\tomcat_backup_02262018_033634
- ◆ OSP 和 SSPR - C:\NetIQ\idm\apps\osp_sspr_backup_02262018_033634
- ◆ ActiveMQ - C:\NetIQ\idm\apps\activemq_backup_02262018_033634
- ◆ 使用者應用程式 - C:\NetIQ\idm\apps\UserApplication_backup_02262018_033634
- ◆ Identity Reporting -
C:\NetIQ\idm\apps\IdentityReporting_backup_02262018_033634

升級後任務

將 Identity Manager 從 4.7.5 升級至 4.9 後，組態更新公用程式中的金鑰儲存區檔案類型將自動變更為 pkcs12。在對以下項目進行升級之前，請務必在組態更新公用程式中，將 jks 格式的金鑰儲存區檔案類型從 pkcs12 變更為 jks：

- ◆ Identity Vault 證書
- ◆ 驗證伺服器
- ◆ 驗證金鑰
- ◆ RBPM

將 Identity Applications 從 4.7.5 升級至 4.9 後，執行以下步驟：

1. 如果您已在分散式設定中安裝 Identity Applications，請編輯 configupdate.properties 並將 edition 變更為 advanced。
2. 在 configupdate 中做出以下變更：
 - ◆ 指定正確的 OSP 連接埠。
 - ◆ 確定根據 TLS 項目校正所有索引標籤中的資料。
3. 更新 ism-configuration.properties 中的以下內容：

```
com.netiq.idm.osp.oauth-truststore.file =  
C:\\\\NetIQ\\\\IDM\\\\apps\\\\tomcat\\\\conf\\\\idm.jks  
  
com.netiq.idm.osp.oauth-truststore.pwd._attr_obscurity = ENCRYPT  
  
com.netiq.idm.osp.oauth-truststore.pwd = GqJVxLBPwgWLK1/  
ULnOb4A==:JoxqTICngaIQtU3z/u7v/w==:2jk5gzsEca+kaz6x7xjE6g==
```

4. 重新啟動 tomcat 服務。

如果您要在叢集環境中升級 Identity Applications，請將主要節點中的以下檔案複製到所有使用者應用程式節點：

- ◆ ism-sensitive.properties
- ◆ ism-configuration.properties
- ◆ encrypt-keys.pkcs12

如果您將 Identity Applications 和 SSPR 安裝在不同的伺服器上，則必須將 CN 為 Identity Applications 的 SSPR 可信證書輸入至 Identity Applications 伺服器的 cacerts 中。

您還必須手動還原 Tomcat、SSPR、OSP 或 Identity Applications 的自訂設定。

針對所需元件執行升級後步驟：

- ◆ 「Java」(第 170 頁)
- ◆ 「Tomcat」(第 170 頁)
- ◆ 「Identity Applications」(第 171 頁)
- ◆ 「One SSO Provider」(第 172 頁)

- ◆ 「[Self-Service Password Reset](#)」 (第 172 頁)
- ◆ 「[Kerberos](#)」 (第 172 頁)

Java

對照舊 JRE 的位置，驗證新升級 JRE 位置中的證書：jre\lib\security\cacerts。手動將缺少的證書輸入到 cacerts 中。

- 1 使用 keytool 指令輸入 java cacerts：

```
keytool -import -trustcacerts -file Certificate_Path -alias ALIAS_NAME
-keystore cacerts
```

附註：升級後，JRE 儲存在 Identity Applications 安裝位置。例如：

C:\NetIQ\idm\apps\jre

- 2 重新啟動 Identity Vault。
- 3 驗證 JRE 主目錄位置是否為 tomcat\bin\setenv.bat。
- 4 啟動組態更新公用程式，並驗證您的 cacerts 路徑。

Tomcat

- 1 (視情況而定) 若要從升級程序先前建立的備份還原自訂檔案，請執行以下任務：

- ◆ 還原自訂的 https 證書。若要還原這些證書，請將所備份 server.xml 中的 Java Secure Socket Extension (JSSE) 內容複製到 \tomcat\conf 目錄下的新 server.xml 檔案中。
- ◆ 不要將所備份 Tomcat 目錄中的組態檔案複製到新 Tomcat 目錄中。應視需要在新版本預設組態的基礎上進行變更。如需詳細資訊，請造訪此 [Apache 網站](#)。

驗證新 server.xml 檔案是否包含以下項目

```
<Connector port="8543" protocol="HTTP/1.1"
    maxThreads="150" SSLEnabled="true" scheme="https"
    secure="true"
    clientAuth="false" sslProtocol="TLS"
    keystoreFile="path_to_keystore_file"
    keystorePass="keystore_password" />
<!--
    <Cluster
    className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
-->
```

或

```

<Connector port="8543"
protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true" scheme="https"
secure="true"
    clientAuth="false" sslProtocol="TLS"
    keystoreFile="path_to_keystore_file"
    keystorePass="keystore_password" />
<!--
    <Cluster
className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
-->

```

附註：在叢集環境中，手動取消備註 `server.xml` 中的 `Cluster` 標記，然後將第一個節點上的 `osp.jks` (位於 `C:\netiq\idm\apps\osp_backup_<date>` 中) 複製到所有節點上。

- ◆ 如果您自訂了金鑰儲存區檔案，請在新 `server.xml` 檔案中包括正確的路徑。
- ◆ 將 **Identity Applications** 證書輸入到 **Identity Vault** 中 (位於 `C:\NetIQ\eDirectory\jre\lib\security\cacerts`)。

例如，您可以使用以下 `keytool` 指令將證書輸入到 **Identity Vault** 中：

```

keytool -importkeystore -alias <User Application certificate alias>
-srckeystore <backup cacert> -srcstorepass changeit -destkeystore
C:\NetIQ\eDirectory\jre\lib\security\cacerts

```

- 2 (視情況而定) 導覽至使用者應用程式，然後透過讀取備份的組態手動還原自訂設定。

Identity Applications

將 **Identity Applications** 從 4.7.5 升級至 4.9 時，必須確定 `tomcat/bin` 資料夾內的 `setenv` 檔案中存在 `Dcom.novell.afw.wf.engine-id=IDMProv` 參數。如果升級 **Identity Applications** 後此參數缺失，則必須在 `setenv` 檔案中手動新增該參數，並重新啟動 **Tomcat** 伺服器。

One SSO Provider

logevent.conf 檔案中的 LogHost 項目預設設定為 localhost。

若要修改 LogHost 項目，請手動從升級期間建立的備份還原 OSP 自訂組態。

Self-Service Password Reset

升級 SSPR 後，使用組態更新公用程式來更新 SSO 用戶端參數。如需詳細資訊，請參閱「[SSO 用戶端參數](#)」(第 83 頁)。

若要更新 SSPR 組態詳細資料，請執行以下步驟：

- 1 以管理員身分登入 SSPR 入口網站。
- 2 更新稽核伺服器詳細資料：
 - 2a 導覽至您的 ID > 組態編輯器，指定組態密碼。
 - 2b 選取設定 > 稽核 > 稽核轉遞 > Syslog 稽核伺服器證書。
 - 2c 從伺服器輸入這些證書，然後按一下儲存。
- 3 將 LocalDB 輸入 SSPR：
 - 3a 從下拉式功能表導覽至您的 ID > 組態管理員。
 - 3b 按一下 LocalDB。
 - 3c 按一下輸入 (上傳) LocalDB 歸檔檔案。
- 4 (視情況而定) 若要限制 SSPR 的組態：
 - 4a 從清單中導覽至您的 ID > 組態管理員。
 - 4b 按一下限制組態。
- 5 設定 SSPR 的管理員許可權，請參閱「[安裝後步驟](#)」(第 55 頁)。

若要驗證升級是否成功，請啟動升級的元件。

例如，啟動 Identity Manager 儀表板，按一下關於。檢查應用程式顯示的是否為新版本，例如 4.9.0。

Kerberos

升級公用程式會在電腦上建立新的 Tomcat 資料夾。如果任何 Kerberos 檔案 (例如 keytab 和 Kerberos_login.config) 存放在舊 Tomcat 資料夾中，請從備份資料夾中將這些檔案複製到新 Tomcat 資料夾。

升級 Identity Reporting

Identity Reporting 中包含兩個驅動程式。此外，您需要將 NetIQ Event Auditing Service 中的內容移轉至 Sentinel Log Management for IGA。依照以下順序執行升級：

1. 升級 Sentinel Log Management for IGA。如需詳細資訊，請參閱《[NetIQ Identity Manager 安裝和升級指南 - Linux](#)》中的「[升級 Sentinel Log Management for IGA](#)」。
2. 升級 Identity Reporting。

升級先決條件

如果您的資料庫是透過 SSL 設定的，請在位於 C:\NetIQ\idm\apps\tomcat\conf 路徑下的 server.xml 檔案中，以 sslmode=require 取代 ssl=true。

例如，將

```
jdbc:postgresql://<postgres db>:5432/idmrptdb?ssl=true
```

變更為

```
jdbc:postgresql://<postgres db>:5432/idmrptdb?sslmode=require
```

升級 Identity Reporting

升級 Identity Reporting 前必須先升級 Identity Applications 和 SLM for IGA。若要升級 Identity Reporting，請在舊版本的基礎上安裝新版本。

升級 Identity Reporting 需要執行的步驟如下：

- 1 從 NetIQ 下載網站下載 Identity_Manager_4.9.0_Windows.iso。
- 2 掛接下載的 .iso。
- 3 導覽至 <ISO 安裝位置>\IdentityReporting 資料夾，然後執行 install.exe。
- 4 選取安裝時要使用的語言，然後按一下**確定**。
- 5 在「簡介」頁面中按下一步。
- 6 閱讀並接受授權合約，然後按下一步。
安裝的元件及其版本即會顯示。
- 7 選取 **Identity Reporting**，然後按下一步。
- 8 指定 Identity Reporting 的組態設定。如需詳細資訊，請參閱「[Identity Reporting 的組態工作表](#)」(第 52 頁)。
- 9 在「升級前摘要」頁面中查看設定，然後按一下**升級**。

附註：ism-configuration.properties 檔案中的 com.netiq.rpt.ssl-keystore.type 內容將保留升級之前設定的值 (JKS/PKCS12)。

附註：如果您將 Identity Reporting 從 4.8.7 升級至 4.9，將在 `c:\netiq\idm\apps\tomcat\conf` 位置備份基於 Java 8 的 tomcat。

Reporting 的升級後步驟

在升級期間，如果您針對何時建立 Identity Reporting 的綱要提示選取了啟動或檔案選項，則必須從 Identity Reporting 使用者介面手動新增資料來源。若要新增資料來源，請導覽至資料來源選項，按一下新增，然後從清單中選擇 IDMDCSDataSource。另外，請在啟動 Tomcat 後重新啟動一次，以確定可用資料庫正常執行。

將 Identity Reporting 升級至 4.9 之後，導覽至 `/opt/netiq/idm/apps/tomcat/conf/` 目錄中的 `ism-configuration.properties` 檔案，並執行以下動作：

- ◆ 依如下所示變更 `com.netiq.rpt.landing.url` 內容的值：

```
com.netiq.rpt.landing.url = ${com.netiq.idm.osp.url.host}/idmdash/#/landing
```

- ◆ 依如下所示變更 `com.netiq.idmdcs.landing.url` 內容的值：

```
com.netiq.idmdcs.landing.url = ${com.netiq.idm.osp.url.host}/idmdash/#/landing
```

- ◆ 採用以下格式指定 `com.netiq.rpt.redirect.url` 內容的值：`https:< 主機名稱 >:< 連接埠 >/ 路徑`

```
例如 com.netiq.rpt.redirect.url = https://192.168.0.1:8543/IDMRPT/oauth.html
```

將 Identity Manager 從 4.7.5 升級至 4.9 後，組態更新公用程式中的金鑰儲存區檔案類型將自動變更為 `pkcs12`。在對以下項目進行升級之前，請務必在組態更新公用程式中，將 `jks` 中金鑰儲存區檔案的類型從 `pkcs12` 變更為 `jks`：

- ◆ Identity Vault 證書
- ◆ 驗證伺服器
- ◆ 驗證金鑰
- ◆ RBPM

將 Identity Reporting 從 4.7.5 升級至 4.9 後，執行以下步驟：

1. (視情況而定) 如果您已在分散式設定中安裝 Identity Applications，請編輯 `configupdate.properties` 並將 `edition` 變更為 `advanced`。
2. 在 `configupdate` 中做出以下變更：
 - ◆ 指定正確的 OSP 連接埠。
 - ◆ 確定根據 TLS 項目校正所有索引標籤中的資料。
3. 更新 `ism-configuration.properties` 中的以下內容：

```
com.netiq.rpt.authserver.url = https://apps.<example>.com:8543
```

```

com.netiq.rpt.ssl-keystore.file =
C:\\\\NetIQ\\\\IDM\\\\apps\\\\tomcat\\\\conf\\\\idm.jks

com.netiq.rpt.ssl-keystore.pwd._attr_obscurity = ENCRYPT

com.netiq.rpt.ssl-keystore.pwd = GqJVxLBPwgWLK1/
ULnOb4A==:JoxqTICngaIQtU3z/u7v/w==:2jk5gzsEca+kaz6x7xjE6g==

com.netiq.rpt.ssl-keystore.type = JKS/PKCS12

com.netiq.idm.osp.oauth-truststore.file =
C:\\\\NetIQ\\\\IDM\\\\apps\\\\tomcat\\\\conf\\\\idm.jks

com.netiq.idm.osp.oauth-truststore.pwd._attr_obscurity = ENCRYPT

com.netiq.idm.osp.oauth-truststore.pwd = GqJVxLBPwgWLK1/
ULnOb4A==:JoxqTICngaIQtU3z/u7v/w==:2jk5gzsEca+kaz6x7xjE6g==

```

4. 重新啟動 tomcat 服務。

變更對資料庫中 reportRunner 的參考

升級 Identity Reporting 後，請務必在第一次啟動 Tomcat 之前更新對資料庫中 reportRunner 的參考。

- 1 停止 Tomcat。
- 2 導覽至 Identity Reporting 安裝目錄，然後將 reportContent 資料夾重新命名為 ORG-reportContent。

例如：C:\NetIQ\idm\apps\IdentityReporting

- 3 清理 Tomcat 資料夾下的臨時目錄和工作目錄。
- 4 登入 PostgreSQL 資料庫。

4a 在下面的表中尋找 reportRunner 參考：

- ◆ idm_rpt_cfg.idmrpt_rpt_params
- ◆ idm_rpt_cfg.idmrpt_definition

4b 發出以下 delete 陳述式：

```

DELETE FROM idm_rpt_cfg.idmrpt_rpt_params WHERE
rpt_def_id='com.novell.content.reportRunner';

DELETE FROM idm_rpt_cfg.idmrpt_definition WHERE
def_id='com.novell.content.reportRunner';

```

- 5 啟動 Tomcat。

檢查記錄以確定使用正確的 reportRunner 是否可重新產生報告。

- 6 登入 Identity Reporting 並執行報告。

驗證 Identity Reporting 的升級

- 1 啟動 Identity Reporting。
- 2 驗證舊報告和新報告是否顯示在工具中。
- 3 查看行事曆，以確定是否顯示了已排程報告。
- 4 確保設定頁面顯示了受管理和不受管理應用程式的先前設定。
- 5 檢查其他所有設定看上去是否正確。
- 6 檢查應用程式是否列出已完成報告。

升級 Analyzer

NetIQ 提供了 .zip 格式的修補程式檔案以協助您升級 Analyzer。在升級 Analyzer 之前，請確保電腦符合先決條件和系統要求。如需詳細資訊，請參閱更新隨附的《版本說明》。

重要：Identity Manager 4.9 ISO 中不包含 Analyzer 工具。如果已安裝 Analyzer，請務必將其更新至版本 4.8.5，並與 Identity Manager 4.9 配合使用。

- 1 從軟體和授權頁面 (<https://sld.microfocus.com/>) 下載修補程式檔案，例如 Identity_Manager_4.9.0_Analyzer_Windows.zips。
- 2 將該 .zip 檔案擷取到包含 Analyzer 安裝檔案 (例如外掛程式、解除安裝程序檔和其他 Analyzer 檔案) 的目錄。
- 3 重新啟動 Analyzer。
- 4 若要驗證您是否已成功套用新的修補程式，請完成以下步驟：
 - 4a 啟動 Analyzer。
 - 4b 按一下說明 > 關於 Analyzer。
 - 4c 檢查程式是否顯示了新版本，例如 **4.6 Update 1** 和版次 ID **20121128**。

停止和啟動 Identity Manager 驅動程式

您可能需要啟動或停止 Identity Manager 驅動程式，以確保升級或安裝程序能夠修改或取代正確的檔案。本節將介紹以下活動：

- ♦ 「停止驅動程式」(第 176 頁)
- ♦ 「啟動驅動程式」(第 177 頁)

停止驅動程式

在修改驅動程式的任何檔案之前，必須先停止驅動程式。

- ♦ 「使用 Designer 停止驅動程式」(第 177 頁)
- ♦ 「使用 Identity Console 停止驅動程式」(第 177 頁)

使用 Designer 停止驅動程式

- 1 在 Designer 中，選取大綱索引標籤中的 Identity Vault  物件。
- 2 在「模型產生器」工具列中，按一下停止所有驅動程式圖示 。
這會停止所有屬於專案的驅動程式。
- 3 將驅動程式設定為手動啟動，以確保直到升級程序完成之前，驅動程式都不會啟動：
 - 3a 連按兩下大綱索引標籤中的驅動程式圖示 。
 - 3b 選取「驅動程式組態 > 啟動選項」。
 - 3c 選取「手動」，然後按一下「確定」。
 - 3d 對每個驅動程式重複步驟 3a 到步驟 3c。

使用 Identity Console 停止驅動程式

- 1 在 Identity Console 中，選取 Identity Manager 管理。
- 2 按一下驅動程式集物件的動作功能表。
- 3 按一下停止所有驅動程式。
- 4 對每個驅動程式集物件重複步驟 1 至 3。
- 5 將驅動程式設定為手動啟動，以確保直到升級程序完成之前，驅動程式都不會啟動：
 - 5a 在 Identity Console 中，選取 Identity Manager 管理。
 - 5b 按一下「驅動程式集」物件。
 - 5c 在驅動程式圖示的右上角，按一下動作功能表並選取啟動選項。
 - 5d 選取「手動」，然後按一下「確定」。
 - 5e 對網路樹中的每一個驅動程式，重複步驟 5a (第 177 頁) 到步驟 5d (第 177 頁)。

啟動驅動程式

在所有 Identity Manager 元件都更新後，重新啟動驅動程式。NetIQ 建議在驅動程式執行後對其進行測試，以驗證所有規則是否仍然正常運作。

- 「使用 Designer 啟動驅動程式」(第 177 頁)
- 「使用 Identity Console 啟動驅動程式」(第 178 頁)

使用 Designer 啟動驅動程式

- 1 在 Designer 中，選取大綱索引標籤中的 Identity Vault  物件。
- 2 按一下「模型產生器」工具列中的啟動所有驅動程式圖示 。這會啟動專案中的所有驅動程式。
- 3 設定驅動程式啟動選項：
 - 3a 連按兩下大綱索引標籤中的驅動程式圖示 。
 - 3b 選取驅動程式組態 > 啟動選項。

- 3c 選取「自動啟動」或選取您偏好的驅動程式啟動方法，然後按一下「確定」。
- 3d 對每個驅動程式重複步驟 3a 到步驟 3c。
- 4 測試驅動程式來驗證規則是否如設計般運作。如需如何測試您的規則的資訊，請參閱《[NetIQ Identity Manager - Using Designer to Create Policies](#)》(NetIQ Identity Manager - 使用 Designer 建立規則) 中的「[Testing Policies with the Policy Simulator](#)」(使用規則模擬器測試規則)。

使用 Identity Console 啟動驅動程式

- 1 在 Identity Console 中，選取 **Identity Manager 綜覽**。
- 2 按一下驅動程式集物件的動作功能表圖示 。
- 3 按一下啟動所有驅動程式。
- 4 如果您有多個驅動程式，請對每個驅動程式集物件重複步驟 1 至 3。
- 5 設定驅動程式啟動選項：
 - 5a 在 Identity Console 中，選取 **Identity Manager 管理**。
 - 5b 按一下「驅動程式集」物件。
 - 5c 在驅動程式圖示的右上角，按一下動作功能表並選取啟動選項。
 - 5d 選取「手動」，然後按一下「確定」。
 - 5e 對每個驅動程式重複步驟 5a (第 178 頁) 和步驟 5d (第 178 頁)。
- 6 測試驅動程式來驗證規則是否如設計般運作。

升級 Identity Manager 驅動程式

NetIQ 透過**套件**而不是驅動程式組態檔案提供新驅動程式內容。您可以在 Designer 中管理、維護和建立套件。如需管理套件的詳細資訊，請參閱《[NetIQ Designer for Identity Manager Administration Guide](#)》(NetIQ Designer for Identity Manager 管理指南) 中的「[Understanding Packages](#)」(瞭解套件)。

您可透過以下方式將驅動程式升級至套件：

- 「[建立新驅動程式](#)」(第 179 頁)
- 「[以套件中的內容取代現有內容](#)」(第 179 頁)
- 「[保留目前內容並透過套件新增新內容](#)」(第 179 頁)

重要：如果您的驅動程式使用 MapDB，請在升級該驅動程式之後，手動移除其現有的 MapDB 狀態快取檔案。之所以需要執行此操作，是因為 Identity Manager 引擎升級程序不會將這些檔案全部清理掉。如需詳細資訊，請參閱「[使用 MapDB 3.0.5](#)」(第 160 頁)。

建立新驅動程式

刪除現有驅動程式，然後建立包含套件的新驅動程式，是將驅動程式升級為套件的最簡便的方法。可以在這個新驅動程式中新增您需要的所有功能。相關步驟因驅動程式而異。如需指示，請參閱 [Identity Manager 驅動程式文件網站](#) 中個別驅動程式的指南。驅動程式現在可如往常一樣運作，但其內容來自套件而不是驅動程式組態檔案。

以套件中的內容取代現有內容

如果您需要保留驅動程式建立的關聯，則無需刪除和重新建立驅動程式。您可以保留關聯，並以套件取代現有的驅動程式內容。

若要以套件中的內容取代現有內容：

- 1 建立驅動程式及其中所有自訂內容的備份。
如需指示，請參閱「[輸出驅動程式的組態](#)」(第 154 頁)。
- 2 在 Designer 中刪除驅動程式內儲存的所有物件。請刪除驅動程式內儲存的規則、過濾器、授權及所有其他項目。

附註：Designer 提供了自動輸入機制，用於輸入最新的套件。您不需要手動將驅動程式套件輸入至套件目錄。

如需詳細資訊，請參閱《[NetIQ Designer for Identity Manager Administration Guide](#)》(NetIQ Designer for Identity Manager 管理指南) 中的「[Importing Packages into the Package Catalog](#)」(將套件輸入至套件目錄)。

- 3 將最新的套件安裝到驅動程式中。
以上步驟視驅動程式而定。如需指示，請參閱 [Identity Manager 驅動程式文件網站](#) 中各驅動程式的指南。
- 4 將任何自訂規則還原至驅動程式。如需指示，請參閱「[將自訂規則還原至驅動程式](#)」(第 181 頁)。

保留目前內容並透過套件新增新內容

您可以將驅動程式保留為目前狀態，並透過套件將新功能新增至驅動程式，只要套件中的功能與驅動程式的目前功能不重疊。

在安裝套件之前，請建立驅動程式組態檔案的備份。當您安裝套件時，它或許會覆寫現有規則，這可能會導致驅動程式停止運作。如果某個規則被覆寫，您可以輸入備份驅動程式組態檔案，然後重新建立該規則。

開始之前，確定所有自訂規則都具有與預設規則不同的規則名稱。以新的驅動程式檔案覆寫驅動程式組態時，就會覆寫現有規則。如果自訂規則的名稱不唯一，您將會遺失這些自訂規則。

若要透過套件將新內容新增至驅動程式：

- 1 建立驅動程式及其中所有自訂內容的備份。
如需指示，請參閱「[輸出驅動程式的組態](#)」(第 154 頁)。

附註：Designer 提供了自動輸入機制，用於輸入最新的套件。您不需要手動將驅動程式套件輸入至套件目錄。

如需詳細資訊，請參閱《[NetIQ Designer for Identity Manager Administration Guide](#)》(NetIQ Designer for Identity Manager 管理指南) 中的「[Importing Packages into the Package Catalog](#)」(將套件輸入至套件目錄)。

2 將套件安裝到驅動程式中。

如需指示，請參閱 [Identity Manager 驅動程式文件網站](#) 中各驅動程式的指南。

3 將所需的套件新增到驅動程式中。以上步驟視驅動程式而定。

如需詳細資訊，請造訪 [Identity Manager 驅動程式文件網站](#)。

驅動程式即包含由套件新增的新功能。

將新伺服器新增至驅動程式集

將 Identity Manager 升級或移轉至新伺服器時，您必須更新驅動程式集資訊。本節會引導您完成該程序。您可以使用 Designer 或 Identity Console 更新驅動程式集。

將新伺服器新增至驅動程式集

如果您使用的是 Identity Console，則必須將新伺服器新增至驅動程式集。Designer 包含的伺服器移轉精靈可為您執行此步驟。若您使用的是 Designer，請跳至「[在 Designer 中複製伺服器特定資訊](#)」(第 191 頁)。如果您使用的是 Identity Console，請完成以下程序：

- 1 在 Identity Console 中，按一下 **IDM 管理**。
- 2 選取驅動程式集。
- 3 按一下 。
- 4 按一下 **新增 伺服器**。
- 5 瀏覽至新的 Identity Manager 伺服器並加以選取，然後按一下「**確定**」。

從驅動程式集移除舊的伺服器

當新伺服器執行所有驅動程式後，您便可以從驅動程式集中移除舊伺服器。

- 「[使用 Designer 從驅動程式集移除舊的伺服器](#)」(第 180 頁)
- 「[使用 Identity Console 從驅動程式集移除舊的伺服器](#)」(第 181 頁)
- 「[解除舊伺服器](#)」(第 181 頁)

使用 Designer 從驅動程式集移除舊的伺服器

- 1 在 Designer 中開啟您的專案。
- 2 在模型產生器中，於驅動程式集上按一下滑鼠右鍵，然後選取「**內容**」。

- 3 選取「伺服器清單」。
- 4 在選取的伺服器清單中選取舊 Identity Manager 伺服器，然後按一下 <，以從選取的伺服器清單中移除該伺服器。
- 5 按一下確定儲存變更。
- 6 將變更部署至 Identity Vault。

如需詳細資訊，請參閱《[NetIQ Designer for Identity Manager Administration Guide](#)》(NetIQ Designer for Identity Manager 管理指南) 中的「[Deploying a Driver Set to an Identity Vault](#)」(將驅動程式集部署至 Identity Vault)。

使用 Identity Console 從驅動程式集移除舊的伺服器

- 1 在 Identity Console 中，按一下 IDM 管理。
- 2 選取驅動程式集。
- 3 按一下 .
- 4 按一下移除伺服器。
- 5 瀏覽至新的 Identity Manager 伺服器並加以選取，然後按一下「確定」。

解除舊伺服器

於此時，舊伺服器未代管任何驅動程式。如果不再需要此伺服器，則另外還必須完成以下步驟解除其職能：

- 1 從此伺服器上移除 eDirectory 複製本。
如需詳細資訊，請參閱《[NetIQ eDirectory Administration Guide](#)》(NetIQ eDirectory 管理指南) 中的「[Deleting a Replica](#)」(刪除複製本)。
- 2 從此伺服器上移除 eDirectory。
如需詳細資訊，請參閱 TID 10056593，「[Removing a Server From an NDS Tree Permanently](#)」(<https://support.microfocus.com/kb/doc.php?id=10056593>)(TID 10056593：從 NDS 樹狀結構中永久移除伺服器)(可能需要登入)。

將自訂規則還原至驅動程式

安裝或升級至驅動程式的新套件之後，您必須在覆蓋新驅動程式組態檔案後，還原驅動程式的所有自訂原則或規則。如果這些規則具有不同名稱，則它們仍然儲存在驅動程式中，但是連結會中斷，因此需要重新建立。

- 「使用 [Designer](#) 將自訂規則還原至驅動程式」(第 182 頁)
- 「使用 [Identity Console](#) 將自訂規則和規則還原至驅動程式」(第 182 頁)

使用 Designer 將自訂規則還原至驅動程式

您可以將規則新增至規則集。您應該先在測試環境中執行這些步驟，然後再將升級後的驅動程式移至線上環境中。

- 1 在大綱檢視中，選取升級的驅動程式，然後按一下顯示規則流程圖示 。
- 2 在規則集中按一下滑鼠右鍵，在這裡您需要將自訂的規則還原至驅動程式，然後選取新增規則 > 複製現有的。
- 3 瀏覽並選取自訂的規則，然後按一下「確定」。
- 4 指定自訂規則的名稱，然後按一下「確定」。
- 5 按一下檔案衝突訊息中的「是」來儲存專案。
- 6 在「規則產生器」開啟規則之後，請驗證所複製規則中的資訊是否正確。
- 7 對您需要的每個自訂規則重複步驟 2 到步驟 6，以還原驅動程式。
- 8 啟動驅動程式並測試驅動程式。

如需啟動驅動程式的詳細資訊，請參閱《[NetIQ Identity Manager Driver Administration Guide](#)》(NetIQ Identity Manager 驅動程式管理指南) 中的「[Stopping, Starting, or Restarting a Driver in Designer](#)」(在 Designer 中停止、啟動或重新啟動驅動程式)。如需測試驅動程式的詳細資訊，請參閱《[NetIQ Identity Manager - Using Designer to Create Policies](#)》(NetIQ Identity Manager - 使用 Designer 建立規則) 中的「[Testing Policies with the Policy Simulator](#)」(使用規則模擬器測試規則)。

- 9 在驗證規則是否運作之後，請將驅動程式移至生產環境。

使用 Identity Console 將自訂規則和規則還原至驅動程式

請先在測試環境中執行這些步驟，然後再將升級的驅動程式移至線上環境中。

- 1 在 Identity Console 中，移至 Identity Manager 管理。
- 2 按一下包含已升級驅動程式的「驅動程式集」物件。
- 3 按一下驅動程式圖示。
- 4 移至資料轉換和同步 > 規則，然後選取您需要在其中還原自訂規則的規則集。
- 5 按一下插入規則。
- 6 在使用現有規則快顯視窗中，瀏覽並選取自訂規則。
- 7 按一下「儲存」。
- 8 對於每一個您需要還原至驅動程式的自訂規則，重複步驟 2 到步驟 7。
- 9 啟動驅動程式並測試驅動程式。

如需啟動驅動程式的資訊，請參閱《[NetIQ Identity Manager Driver Administration Guide](#)》(NetIQ Identity Manager 驅動程式管理指南) 中的「[Stopping, Starting, or Restarting a Driver in Designer](#)」(在 Designer 中停止、啟動或重新啟動驅動程式)。Identity Console 中沒有任何規則模擬器。若要測試規則，請讓可使規則執行的事件發生。例如，建立使用者、修改使用者或刪除使用者。

- 10 在驗證規則是否運作之後，請將驅動程式移至生產環境。

17 從進階版切換到標準版

僅當您不想在環境中使用任何進階版功能，並且要縮減 Identity Manager 部署時，才應切換至標準版。

- 1 (視情況而定) 如果您已套用進階版啟用，請移除該啟用。
- 2 (視情況而定) 若要切換到標準版評估模式：
 - 2a 導覽至 C:\Novell\NDS\DIBFiles 中的 Identity Vault dib 目錄。
 - 2b 建立一個新檔案，將其命名為 .idme，並在其中新增 2(數值)。
 - 2c 重新啟動 eDirectory。
 - 2d 繼續執行步驟 4。
- 3 (視情況而定) 如果您已採購標準版啟用，請套用該啟用。
- 4 停止 Tomcat。
- 5 從 C:\NetIQ\idm\apps\tomcat\webapps 目錄中移除以下 WAR 檔案和 Webapps 資料夾：
 - ◆ IDMProv*
 - ◆ IDMRPT*
 - ◆ dash*
 - ◆ idmdash*
 - ◆ landing*
 - ◆ rra*
 - ◆ rptdoc*
- 6 將以下現有資料夾移到備份目錄：
 - ◆ IDMReporting
 - ◆ UserApplication
- 7 將 C:\NetIQ\IDM\apps\tomcat\conf 目錄中的 ism-configuration.properties 檔案複製到備份目錄。
- 8 從 Identity Manager 4.9 iso 檔案安裝 Identity Reporting。
- 9 從 <Reporting 安裝資料夾>/bin 目錄啟動 configupdate.bat，然後指定以下參數的值：

「報告」索引標籤：指定以下區段中的設定：

 - ◆ ID Vault
 - ◆ Identity Vault 使用者身分

- ◆ 報告管理員
 - ◆ 報告管理員角色容器 **DN**。例如，ou=sa,o=data
 - ◆ 報告管理員。例如，cn=uaadmin,ou=sa,o=data

「驗證」索引標籤：指定以下區段中的設定：

- ◆ 驗證伺服器
 - ◆ **OAuth 伺服器主機識別碼**。例如，驗證伺服器的 IP 位址或 DNS 名稱 (如 192.99.17.22)
 - ◆ **OAuth 伺服器 TCP 連接埠**
 - ◆ **OAuth 伺服器正在使用 TLS/SSL**
- ◆ 驗證組態
 - ◆ **OAuth 金鑰儲存區檔案**。例如，C:\NetIQ\idm\apps\osp\osp.jks
 - ◆ **OAuth 使用之金鑰的金鑰別名**
 - ◆ **OAuth 所用金鑰的金鑰密碼**
 - ◆ **工作階段逾時 (分鐘)**。例如，60 分鐘。

「SSO 用戶端」索引標籤：指定以下區段中的設定：

- ◆ 報告
 - ◆ **抵達頁面的 URL 連結**。例如，http://192.168.0.1:8180/IDMRPT
- ◆ Self Service Password Reset
 - ◆ **OAuth 用戶端 ID**。例如，sspr
 - ◆ **OAuth 用戶端機密**。例如，<sspr 用戶端機密>
 - ◆ **OSP OAuth 重新導向 URL**。例如，http://192.168.0.2:8180/sspr/public/oauth

如需組態公用程式的詳細資訊，請參閱「[執行 Identity Applications 組態公用程式](#)」(第 67 頁)。

10 儲存變更並結束組態公用程式。

11 啟動 Tomcat。

VIII 將 Identity Manager 資料移轉至新安裝中

此部分提供關於將 Identity Manager 元件中的現有資料移轉至新安裝的資訊。大多數移轉任務都適用於 Identity Applications。若要升級 Identity Manager 的元件，請參閱第 VII 部分「升級 Identity Manager」(第 145 頁)。如需升級與移轉之間差異的詳細資訊，請參閱「瞭解升級和移轉」(第 148 頁)。

18 移轉 Identity Manager 的準備工作

本章提供的資訊可協助您為將 Identity Manager 解決方案移轉至新安裝做好準備。

用於執行移轉的核對清單

若要執行移轉，NetIQ 建議您完成以下核對清單中的步驟。

	核對清單項目
☐	1. 確保您已取得用於移轉 Identity Manager 資料的最新安裝套件。
☐	2. 確保您的電腦符合更新版本 Identity Manager 的硬體和軟體先決條件。
☐	3. 將 Identity Vault 升級至支援的最新版本。
☐	4. 將目前 Identity Manager 伺服器上的 eDirectory 複製本新增至新伺服器。如需詳細資訊，請參閱第 19 節「將 Identity Manager 移轉至新伺服器」(第 189 頁)。
☐	5. 在新伺服器上安裝 Identity Manager。如需詳細資訊，請參閱「規劃 Identity Manager 安裝」(第 33 頁)。
☐	6. (視情況而定) 如果驅動程式集中有任何驅動程式為遠端載入器驅動程式，請升級每個驅動程式的遠端載入器伺服器。如需詳細資訊，請參閱「升級遠端載入器」(第 162 頁)。
☐	7. (視情況而定) 如果您是在舊伺服器上執行使用者應用程式，請更新該元件及其驅動程式。如需詳細資訊，請參閱「Identity Manager 的移轉核對清單」(第 189 頁)。
☐	8. 將新伺服器新增至驅動程式集。如需詳細資訊，請參閱「將新伺服器新增至驅動程式集」(第 180 頁)。
☐	9. 變更每個驅動程式的伺服器特定資訊。如需詳細資訊，請參閱「在 Designer 中複製伺服器特定資訊」(第 191 頁)。
☐	10. (視情況而定) 如果您在使用 RBPM，請將使用者應用程式的伺服器特定資訊從舊伺服器更新為新伺服器。如需詳細資訊，請參閱「複製驅動程式集的伺服器特定資訊」(第 190 頁)。
☐	11. 將驅動程式更新為套件格式。如需詳細資訊，請參閱「升級 Identity Manager 驅動程式」(第 178 頁)。
☐	12. (視情況而定) 如果您有自訂的原則和規則，請還原自訂設定。如需詳細資訊，請參閱「將自訂規則還原至驅動程式」(第 181 頁)。
☐	13. 從驅動程式集移除舊的伺服器。如需詳細資訊，請參閱「從驅動程式集移除舊的伺服器」(第 180 頁)。

	核對清單項目
	14. 啟用升級後的 Identity Manager 解決方案。如需詳細資訊，請參閱「 啟用 Identity Manager 」(第 143 頁)。

19 將 Identity Manager 移轉至新伺服器

本章提供關於如何從使用者應用程式移轉至新伺服器上的 Identity Applications 的資訊。當您無法升級現有安裝時，可能也需要執行移轉。本章包括以下活動：

- 「Identity Manager 的移轉核對清單」(第 189 頁)
- 「準備用於移轉的 Designer 專案」(第 190 頁)
- 「複製驅動程式集的伺服器特定資訊」(第 190 頁)
- 「將 Identity Manager 引擎移轉至新伺服器」(第 192 頁)
- 「移轉使用者應用程式驅動程式」(第 192 頁)
- 「升級 Identity Applications」(第 194 頁)
- 「移轉 Identity Applications」(第 194 頁)
- 「完成 Identity Applications 的移轉」(第 196 頁)

Identity Manager 的移轉核對清單

NetIQ 建議您完成以下核對清單中的步驟。

	核對清單項目
☐	1. 備份 Identity Manager 解決方案的目錄和資料庫。
☐	2. 確保您已安裝最新版本的 Identity Manager 元件 (Identity Applications 除外)。 附註： 若要繼續使用目前的使用者應用程式資料庫，請在安裝程式中指定現有資料庫。
☐	3. 執行 Identity Vault 狀態檢查，以確保綱要可正常延伸。請使用 TID 3564075 完成健康狀態檢查。
☐	4. 將現有的使用者應用程式驅動程式輸入到 Designer 中。
☐	5. 將 Designer 專案歸檔。它代表移轉前狀態的驅動程式。如需詳細資訊，請參閱「準備用於移轉的 Designer 專案」(第 190 頁)。
☐	6. (視情況而定) 若要將 Identity Manager 引擎移轉至某個新伺服器，請將 eDirectory 複製本複製到這個新伺服器上。如需詳細資訊，請參閱「將 Identity Manager 引擎移轉至新伺服器」(第 192 頁)。
☐	7. 在最新版 Designer 中建立一個新 Designer 專案，然後輸入使用者應用程式驅動程式，為移轉做好準備。
☐	8. 移轉使用者應用程式驅動程式。如需詳細資訊，請參閱「移轉使用者應用程式驅動程式」(第 192 頁)。

	核對清單項目
☐	9. 將兩個驅動程式部署到 Identity Vault。
☐	10. 升級 Identity Applications。如需詳細資訊，請參閱「 升級 Identity Applications 」(第 164 頁)。
☐	11. 確保您的瀏覽器不包含先前版本 Identity Manager 的內容。如需詳細資訊，請參閱「 衝洗瀏覽器快取 」(第 197 頁)。
☐	12. (視情況而定) 恢復 SharedPagePortlet 的自訂設定。如需詳細資訊，請參閱「 更新 SharedPagePortlet 的最大逾時設定 」(第 197 頁)。
☐	13. 確保在使用者未提供過濾參數時，搜尋群組選項不會顯示任何資訊。如需詳細資訊，請參閱「 停用群組的自動查詢設定 」(第 197 頁)。

準備用於移轉的 Designer 專案

在移轉驅動程式之前，您需要執行一些設定步驟，以準備用於移轉的 Designer 專案。

附註：如果您沒有用於移轉的現有 Designer 專案，請使用檔案 > 輸入 > 專案 (來自 Identity Vault) 建立一個新專案。

- 1 啟動 Designer。
- 2 (視情況而定) 如果某個現有 Designer 專案包含要移轉的使用者應用程式，請備份該專案：
 - 2a 在「專案」檢視窗中該專案的名稱上按一下滑鼠右鍵，然後選取**複製專案**。
 - 2b 指定專案的名稱，然後按一下**確定**。
- 3 若要更新現有專案的綱要，請完成以下步驟：
 - 3a 在「模型產生器」檢視窗中，選取「Identity Vault」。
 - 3b 選取**即時 > 綱要 > 輸入**。
- 4 (選擇性) 若要驗證專案中 Identity Manager 的版本號碼是否正確，請完成以下步驟：
 - 4a 在「模型產生器」檢視窗中，選取「Identity Vault」，然後按一下**內容**。
 - 4b 在左側導覽功能表中，選取**伺服器清單**。
 - 4c 選取一個伺服器，然後按一下**編輯**。
Identity Manager 版本欄位應該會顯示最新版本。

複製驅動程式集的伺服器特定資訊

您必須將儲存在每個驅動程式和驅動程式集中的所有伺服器特定資訊複製為新伺服器的資訊。這也包括新伺服器中原本沒有，但需要從驅動程式集複製的 GCV 和其他資料。伺服器特定資訊位於：

- ◆ 全域組態值

- ◆ 引擎控制值
- ◆ 具名密碼
- ◆ 驅動程式驗證資訊
- ◆ 驅動程式啟動選項
- ◆ 驅動程式參數
- ◆ 驅動程式集資料

可以在 **Designer** 或 **Identity Console** 中執行此操作。若您使用 **Designer**，則為自動程序。如果使用 **Identity Console**，則需要手動完成此程序。若要從版本早於 3.5 的 **Identity Manager** 伺服器移轉至 3.5 或更新版本的 **Identity Manager** 伺服器，您應該使用 **Identity Console**。對於所有其他受支援的移轉路徑，您可以使用 **Designer**。

- ◆ 「在 **Designer** 中複製伺服器特定資訊」(第 191 頁)
- ◆ 「在 **Identity Console** 中變更伺服器特定的資訊」(第 192 頁)
- ◆ 「變更使用者應用程式的伺服器特定資訊」(第 192 頁)

在 **Designer** 中複製伺服器特定資訊

此程序會影響驅動程式集中儲存的所有驅動程式。

- 1 在 **Designer** 中開啟您的專案。
- 2 在「大綱」標籤中，在伺服器上按一下滑鼠右鍵，然後選取「移轉」。
- 3 閱讀綜覽以查看移轉至新伺服器的項目，然後按「下一步」。
- 4 從列出的可用伺服器中選取目標伺服器，然後按「下一步」。
只有目前與驅動程式集沒有關聯且與來源伺服器的 **Identity Manager** 版本相同或更新的伺服器會被列出。
- 5 選取以下選項之一：
 - ◆ **啟用目標伺服器**：將來源伺服器的設定複製到目標伺服器，並停用來源伺服器上的驅動程式。**NetIQ** 建議您使用此選項。
 - ◆ **將來源伺服器保持為啟用**：不要複製設定，並停用目標伺服器上的所有驅動程式。
 - ◆ **同時啟用目標和來源伺服器**：將來源伺服器的設定複製到目標伺服器，但不停用來源或目標伺服器上的驅動程式。不建議使用此選項。如果兩者的驅動程式皆啟動，則會將相同資訊寫入兩個不同佇列，這可能會造成資料損毀。
- 6 按一下「移轉」。
- 7 將變更的驅動程式部署至 **Identity Vault**。
如需詳細資訊，請參閱《*NetIQ Designer for Identity Manager Administration Guide*》(**NetIQ Designer for Identity Manager** 管理指南) 中的「**Deploying a Driver to an Identity Vault**」(將驅動程式部署至 **Identity Vault**)。
- 8 啟動驅動程式。
如需詳細資訊，請參閱《*NetIQ Identity Manager Driver Administration Guide*》(**NetIQ Identity Manager** 驅動程式管理指南) 中的「**Stopping, Starting, or Restarting a Driver in Designer**」(在 **Designer** 中停止、啟動或重新啟動驅動程式)。

在 Identity Console 中變更伺服器特定的資訊

- 1 在 Identity Console 中，移至 **Identity Manager** 管理。
- 2 按一下包含所需驅動程式的驅動程式集物件。
- 3 按一下動作功能表圖示 ，然後按一下 **停止驅動程式**。
- 4 按一下驅動程式圖示。
- 5 移至 **組態**。tab.
- 6 將所有伺服器專屬驅動程式參數、全域組態值、引擎控制值、具名密碼、驅動程式驗證資料以及包含舊伺服器資訊的驅動程式啟動選項複製或移轉至新伺服器的資訊中。全域組態值及其他驅動程式集參數 (例如堆積大小上限、Java 設定等) 必須與舊伺服器的值相同。
- 7 按一下 **儲存** 以儲存所有變更並結束。
- 8 按一下  動作功能表，然後按一下 **啟動驅動程式**。
- 9 對驅動程式集中的每個驅動程式重複 **步驟 3** 到 **步驟 8** ([第 192 頁](#))。

變更使用者應用程式的伺服器特定資訊

您必須重新設定使用者應用程式，以識別新伺服器。執行 configupdate.bat。

- 1 導覽至預設位於使用者應用程式安裝子目錄中的組態更新公用程式。
- 2 在指令提示符處，啟動組態更新公用程式 (configupdate.bat)。
- 3 依照「[完成 Identity Applications 的設定](#)」([第 66 頁](#)) 所述指定值。

將 Identity Manager 引擎移轉至新伺服器

將 Identity Manager 引擎移轉至新伺服器時，您可以保留舊伺服器上目前所使用的 eDirectory 複製本。

- 1 在新伺服器上安裝受支援的 eDirectory 版本。
- 2 將目前 Identity Manager 伺服器上的 eDirectory 複製本複製到新伺服器上。
如需詳細資訊，請參閱《[NetIQ eDirectory Administration Guide](#)》(NetIQ eDirectory 管理指南) 中的「[Administering Replicas](#)」(管理複製本)。
- 3 在新伺服器上安裝 Identity Manager 引擎。

移轉使用者應用程式驅動程式

在升級至新版 Identity Manager 或移轉至另一個伺服器時，您可能需要輸入使用者應用程式的新基礎套件，或升級現有套件。例如 **使用者應用程式基礎版本 2.2.0.20120516011608**。

當您開始處理 Identity Manager 專案時，Designer 會自動提示您將新套件輸入該專案。此時，您也可以手動輸入套件。

輸入新的基礎套件

- 1 在 Designer 中開啟您的專案。
- 2 在套件目錄 > 輸入套件上按一下滑鼠右鍵，然後選取相應的套件。
- 3 (視情況而定) 如果「輸入套件」對話方塊未列出使用者應用程式基礎套件，請完成以下步驟：
 - 3a 按一下「瀏覽」按鈕。
 - 3b 導覽至 *Designer 根目錄/packages/eclipse/plugins/NOVLUABASE_最新套件的版本.jar*。
 - 3c 按一下「確定」。
- 4 按一下「確定」。

升級現有的基礎套件

- 1 在 Designer 中開啟您的專案。
- 2 在「使用者應用程式驅動程式」上按一下滑鼠右鍵。
- 3 按一下驅動程式 > 內容 > 套件。

如果基礎套件可以升級，應用程式會在升級欄中顯示一個核取記號。
- 4 按一下套件對應的選取操作。出現此項表示該套件可升級。
- 5 在下拉式清單中，按一下升級。
- 6 選取升級的目標版本。按一下「確定」。
- 7 按一下套用。
- 8 在各欄位中填入用於升級套件的適當資訊。然後按「下一步」。
- 9 查看安裝摘要。然後按一下「完成」。
- 10 關閉「套件管理」頁面。
- 11 取消選取僅顯示適用的套件版本。

部署移轉的驅動程式

只有將使用者應用程式驅動程式部署到 Identity Vault 後，驅動程式移轉才真正完成。移轉後，專案所處的狀態只允許部署整個移轉的組態。您無法將任何定義輸入至移轉的組態。在部署整個移轉組態後，此限制即會解除，您便可以部署個別物件以及輸入定義。

- 1 在 Designer 中開啟專案，然後對移轉的物件執行專案檢查。

如需詳細資訊，請參閱《*NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications*》(NetIQ Identity Manager - 面向管理員的 Identity Applications 設計指南) 中的「[Validating Provisioning Objects](#)」(驗證佈建物件)。如果驗證組態時發現了錯誤，系統會告知相應的錯誤。只有校正了這些錯誤，您才能部署驅動程式。
- 2 在大綱檢視窗中的使用者應用程式驅動程式上按一下滑鼠右鍵。
- 3 選取部署。
- 4 對驅動程式集中的每個使用者應用程式驅動程式重複此程序。

升級 Identity Applications

在執行 Identity Applications 的升級程式時，請務必注意以下事項：

- 使用先前的使用者應用程式所用的同一個資料庫。「先前安裝」是指您要從中移轉資料的安裝。在安裝程式中，指定現有資料庫做為資料庫類型。
- 您可為使用者應用程式網路位置指定其他名稱。
- 指定不同於先前安裝的安裝位置。
- 指向受支援版本的 Tomcat。
- 不要對資料庫使用區分大小寫的定序。區分大小寫的定序不受支援。使用區分大小寫的定序可能會導致移轉期間出現重複鍵錯誤。如果遇到重複鍵錯誤，請檢查定序並予以校正，然後重新安裝 Identity Applications。唯一受支援的定序是 SQL_Latin1_General_CP1_CI_AS。

如需升級 Identity Applications 的詳細資訊，請參閱「[升級 Identity Applications](#)」(第 164 頁)。

移轉 Identity Applications

不要對資料庫使用區分大小寫的定序。區分大小寫的定序不受支援。使用區分大小寫的定序可能會導致移轉期間發生重複鍵錯誤。如果遇到重複鍵錯誤，請檢查定序並予以校正，然後重新安裝 Identity Applications。唯一受支援的定序是 SQL_Latin1_General_CP1_CI_AS。

在移轉 Identity Applications 之前，必須從 /opt/netiq/common/openssl/lib64/ 目錄安裝 libssl.so.1.0.0 和 libcrypto.so.1.0.0 程式庫。

Identity Applications 移轉過程包括以下步驟：

- 「[將資料庫移轉至新伺服器](#)」(第 194 頁)
- 「[在新伺服器上安裝 Identity Applications](#)」(第 195 頁)

將資料庫移轉至新伺服器

如果您的使用者應用程式資料庫位於 PostgreSQL 中，請執行以下步驟：

- 1 登入安裝了 PostgreSQL 的伺服器。
- 2 開啟指令提示符，導覽至 postgres bin 目錄並將資料輸出至 .sql 檔案。
範例：pg_dumpall -U postgres > dump.sql
- 3 登入要安裝 PostgreSQL 的新伺服器。
- 4 如下所述安裝 PostgreSQL：
 - 4a 從軟體授權和下載 (<https://sldlogin.microfocus.com/>) 入口網站下載並掛接 Identity_Manager_4.9.x_Windows.iso。
 - 4b 導覽至掛接 Identity_Manager_4.9.x_Windows.iso 的位置。

- 4c 導覽至：<掛接位置>\common\packages\postgres\ 目錄。
- 4d 執行 PostgreSQL 安裝程式。
- 5 導覽至 C:\NetIQ\IDM\postgres 並刪除 Data 目錄。
- 6 在 PostgreSQL 安裝位置建立一個 data 目錄，並確定 postgres 使用者有權存取該目錄。
- 7 開啟指令提示符，導覽至 postgres bin 目錄並如下所示啟始化資料庫：
- 範例：initdb.exe -D C:\NetIQ\IDM\postgres\data -E WIN1252 -U postgres。
- 8 確定 C:\NetIQ\IDM\postgres\data 下的 pg_hba.conf 檔案中存在以下項目。
- # IPv6 local connections:
- host all all ::1/128 trust
- host all all 0.0.0.0/0 trust
- 9 確定已在 postgresql.conf 檔案中取消備註以下項目：
- listen_addresses = '*'
- port = 5432
- 10 從執行功能表執行 services.msc，重新啟動 postgres 服務。
- 11 開啟指令提示符，導覽至 postgres bin 目錄，將資料輸入至新的 PostgreSQL 資料庫，然後依照步驟 2 中所述使用收集的傾印。
- 範例：psql -U postgres < dump.sql。

在新伺服器上安裝 Identity Applications

以下程序說明如何在新伺服器上安裝 Identity Application：

- 1 從 [NetIQ 下載網站 \(https://dl.netiq.com/\)](https://dl.netiq.com/) 下載 Identity_Manager_4.9.x_Windows.iso。
- 2 掛接 .iso 檔案。
- 3 導覽至 Identity apps 目錄，安裝 **Identity Applications**，並跳過使用者應用程式及角色與資源服務驅動程式的部署。
 - 3a 選取「自訂安裝」模式。
 - 3b 輸入 Identity Vault 詳細資料。
 - 3c 取消核取部署 **Identity Applications** 驅動程式。
- 4 選取現有 **PostgreSQL** 伺服器，提供所需的詳細資料，然後繼續安裝。

完成 Identity Applications 的移轉

在升級或移轉 Identity Applications 後，請完成移轉程序。

準備 Oracle 資料庫以執行 SQL 檔案

在安裝期間，您可能選擇了撰寫一個 SQL 檔案來更新 Identity Applications 資料庫。如果資料庫在 Oracle 平台上執行，則您必須先執行一些步驟才能執行該 SQL 檔案。

- 1 在資料庫中執行以下 SQL 陳述式：

```
ALTER TABLE DATABASECHANGELOG ADD ORDEREXECUTED INT;
UPDATE DATABASECHANGELOG SET ORDEREXECUTED = -1;
ALTER TABLE DATABASECHANGELOG MODIFY ORDEREXECUTED INT NOT NULL;
ALTER TABLE DATABASECHANGELOG ADD EXECTYPE VARCHAR(10);
UPDATE DATABASECHANGELOG SET EXECTYPE = 'EXECUTED';
ALTER TABLE DATABASECHANGELOG MODIFY EXECTYPE VARCHAR(10) NOT NULL;
```

- 2 執行以下 updateSQL 指令：

```
C:\NetIQ\idm\jre\bin\java -Xms256m -Xmx256m -Dwar.context.name=IDMProv
-
Ddriver.dn="cn=User Application Driver,cn=driverset1,o=system" -
Duser.container="o=data" -jar C:\NetIQ\idm\jre\liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase --
driver=org.postgresql.Driver --
classpath=C:\NetIQ\idm\apps\postgresql\postgresql-9.4.1212jdbc42.jar
C:\NetIQ\idm\apps\UserApplication\IDMProv.war --
changeLogFile=DatabaseChangeLog.xml --url="jdbc:postgresql://
localhost:5432/
idmuserappdb" --contexts="prov,newdb" --logLevel=info --
logFile=C:\NetIQ\idm\apps\UserApplication\db.out --username=***** --
password=***** update
```

- 3 在文字編輯器中，開啟預設位於 */installation_path/userapp/sql* 目錄中的 SQL 檔案。
- 4 在函數 `CONCAT_BLOB` 的定義後面插入一個反斜線 (`/`)。例如

```
-- Changeset icfg-data-load.xml::700::IDMRBPM
CREATE OR REPLACE FUNCTION CONCAT_BLOB(A IN BLOB, B IN BLOB) RETURN BLOB
AS
    C BLOB;
BEGIN
    DBMS_LOB.CREATETEMPORARY(C, TRUE);
    DBMS_LOB.APPEND(C, A);
    DBMS_LOB.APPEND(C, B);
    RETURN c;
END;
/
```

- 5 執行 SQL 檔案。

有關執行 SQL 檔案的詳細資訊，請參閱「[手動建立資料庫綱要](#)」(第 88 頁)。

附註：請不要使用 SQL*Plus 來執行該 SQL 檔案。該檔案中的行長度超過了 4000 個字元。

衝洗瀏覽器快取

在您登入 Identity Applications 之前，應該先衝洗瀏覽器上的快取。如果不衝洗快取，您可能會遇到一些執行時期錯誤。

更新 SharedPagePortlet 的最大逾時設定

如果您之前自訂了 SharedPagePortlet 的任何預設設定或優先設定，那麼，這些自訂已經儲存到資料庫中，並且此設定將會被覆寫。因此，導覽至「身分自助服務」索引標籤可能並不總是反白顯示正確的共享頁面。為確保不會遇到此問題，請完成以下步驟：

- 1 以使用者應用程式管理員身分登入。
- 2 導覽至**管理 > 入口網站應用程式管理**。
- 3 展開**共享頁面導覽**。
- 4 在左側的入口網站應用程式樹中，按一下**共享頁面導覽**。
- 5 在頁面的右側按一下**設定**。
- 6 確保**最大逾時**設定為 0。
- 7 按一下「**儲存設定**」。

停用群組的自動查詢設定

依預設，目錄抽象層中「群組」實體的「DNLookup 顯示」處於啟用狀態。這意味著，每次為群組指定開啟物件選擇器時，您無需搜尋，所有群組預設就會顯示。您應該變更此設定，因為用於搜尋群組的視窗在使用者輸入搜尋內容之前不應顯示任何結果。

您可以在 Designer 中取消核取**執行自動查詢**來變更此設定，如下所示：

使用者

名

使用者照片

使用者優先設定

使用者優先設定

姓

直屬員工

查詢清單

偏好通知

區域

部門

群組

電子郵件

電話號碼

管理員

隱藏的屬性清單

職稱

使用者查閱

容器

群組

清單

針對您擁有文字字串或運算式的屬性提供預設值：

文字字串：

運算式：

UI 控制架構

指定顯示屬性時的格式或特殊控制項：

資料類型：DN

格式類型：<無>

控制項類型：DNLookup

DNLookup 顯示

針對「查閱」操作選取要顯示的「實體」和「屬性」：

查閱實體：群組

查閱屬性

+

描述

×

☐ 執行自動查詢

如果您不希望自動執行查詢，請取消核取此方塊

在 Microsoft Azure 上部署 Identity Manager

本部分介紹如何在 Microsoft Azure 雲端規劃和實作 Identity Manager。

- ◆ [第 20 章 「在 Microsoft Azure 上規劃和實作 Identity Manager」 \(第 201 頁\)](#)
- ◆ [第 21 章 「範例混合式 Identity Manager 方案」 \(第 211 頁\)](#)

20 在 Microsoft Azure 上規劃和實作 Identity Manager

Identity Manager 現支援在 Microsoft Azure 上部署以下 Identity Manager 元件。

- ◆ Identity Manager 引擎
- ◆ Identity Manager 驅動程式和遠端載入器
- ◆ Designer
- ◆ Identity Applications
- ◆ Identity Reporting

附註：不支援在 Microsoft Azure 上部署 Sentinel Log Management。

先決條件

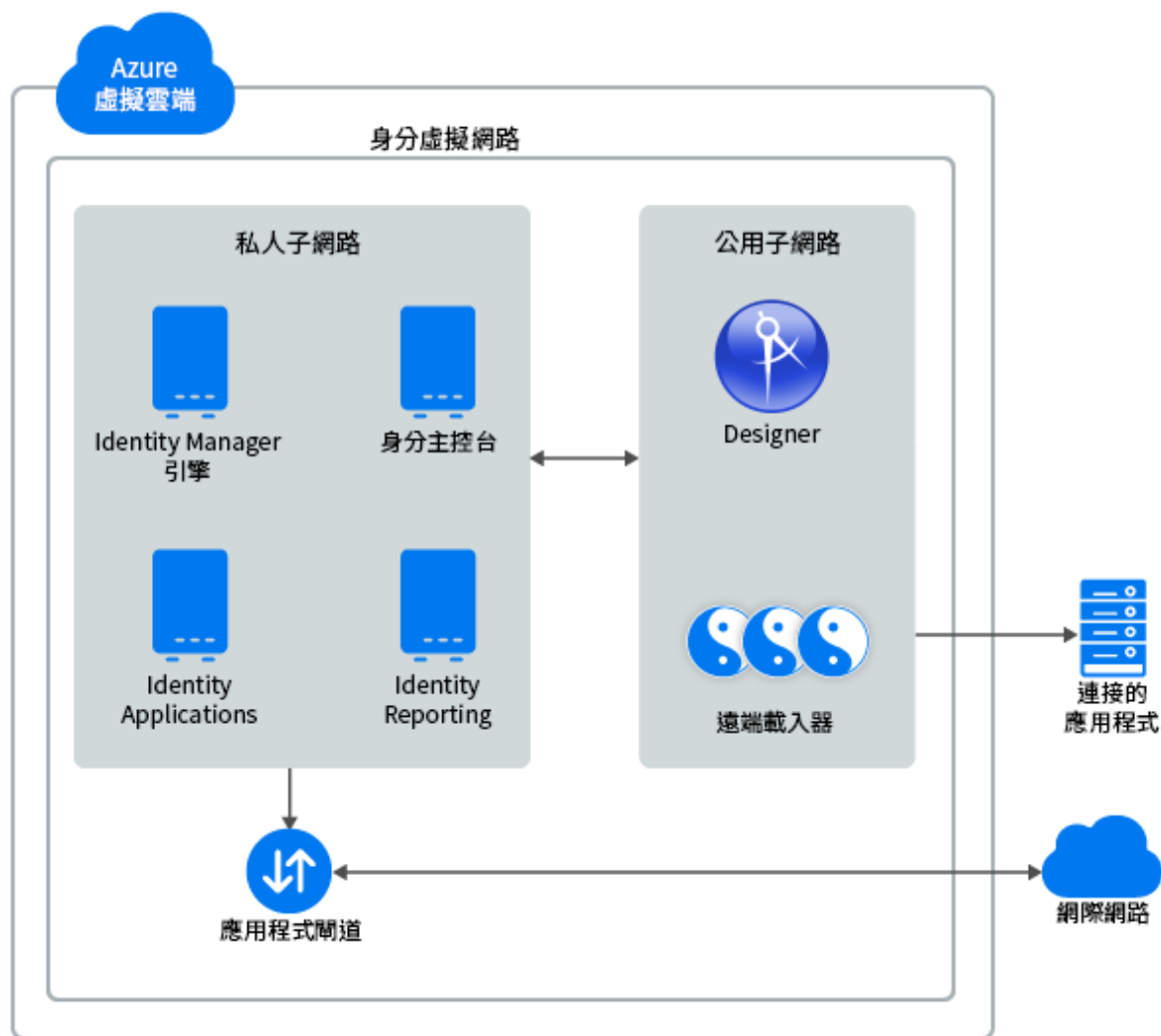
除了 Identity Manager 元件的系統要求以外，請確定您符合以下先決條件：

- ◆ Microsoft Azure 上的管理帳戶。
- ◆ 已下載及解壓縮 Identity_Manager_4.9.0_Windows.iso 和 Designer，並且可在 Identity Manager 元件例項上使用這些檔案。
- ◆ 用於從本地用戶端機器連接至 Azure 虛擬機器例項的遠端桌面。

部署程序

您可以依據自己的要求在私人或公用網路中部署 Identity Manager 元件。[圖 20-1](#) 演示了一個範例部署，後續章節中將用到該部署。

圖 20-1 在 Microsoft Azure 上部署 Identity Manager



您可以依據 Identity Manager 元件在不同伺服器上的分散方式，以不同的組合在 Microsoft Azure 上部署這些元件。不過，所有方案的部署程序都是相同的。

部署程序包括以下步驟：

- ◆ 「建立資源群組」(第 203 頁)
- ◆ 「建立虛擬網路和子網路」(第 203 頁)
- ◆ 「建立應用程式閘道」(第 204 頁)
- ◆ 「建立虛擬機器例項」(第 205 頁)
- ◆ 「更新 VM 中的主機項目」(第 206 頁)
- ◆ 「安裝 Designer」(第 207 頁)
- ◆ 「設定應用程式閘道」(第 208 頁)

建立資源群組

NetIQ 建議您建立一個資源群組並將所需資源新增至該群組，以與 Identity Manager 配合使用。執行以下步驟建立新的資源群組：

- 1 登入 Azure 入口網站。
- 2 按一下資源群組。
- 3 按一下建立。
- 4 在基本資訊索引標籤中：
 - 4a 從下拉式清單中選取您的訂閱。
 - 4b 輸入新的資源群組名稱。
 - 4c 從區域下拉式清單中選取位置。例如印度中部。
 - 4d 按下一步：標籤 >。
- 5 在標籤索引標籤中，按下一步：檢閱 + 建立 >。
- 6 在檢閱 + 建立索引標籤中，按一下建立。

建立虛擬網路和子網路

- 1 登入 Azure 入口網站。
- 2 在搜尋中輸入虛擬網路。
- 3 在「服務」下，選取虛擬網路。
- 4 按一下建立。
- 5 在基本資訊索引標籤中指定以下詳細資料：

欄位	描述
訂購	從下拉式清單中選取您的訂閱。
資源群組	從下拉式清單中選取現有的資源群組。
名稱	指定虛擬網路的名稱。
區域	從下拉式清單中選取位置。例如印度中部。

- 5a 按下一步：IP 位址 >。
- 6 在「IP 位址」索引標籤中，按一下新增子網路。
 - 6a 按一下新增子網路。
 - 6a1 指定子網路名稱。例如 default。
 - 6a2 指定子網路位址範圍。例如 10.1.0.0/24。
 - 6a3 按一下新增。
 - 6b 按下一步：安全性 >。
 - 7 在安全性索引標籤中，保留所有欄位的預設值，然後按下一步：標籤 >。

- 8 在標籤索引標籤中，按下一步：檢閱 + 建立 >。
- 9 在檢閱 + 建立索引標籤中檢閱您的設定，然後按一下建立。

建立應用程式閘道

- 1 登入 Azure 入口網站。
- 2 按一下建立資源。
- 3 移至類別 > 網路 > 應用程式閘道。
- 4 在基本資訊索引標籤中指定以下詳細資料：

欄位	描述
訂購	從下拉式清單中選取您的訂閱。
資源群組	從下拉式清單中選取現有的資源群組。
應用程式閘道名稱	指定應用程式閘道名稱。
區域	從下拉式清單中選取位置。例如印度中部。
層級	選取所需的層。例如標準 V2。
最小執行個體計數	指定值 0。
最大執行個體計數	指定值 10。
虛擬網路	選取虛擬網路和已建立的對應子網路。請參閱「 建立虛擬網路和子網路 」(第 203 頁)。

- 4a 保留其餘欄位的預設值，然後按下一步：前端 >。
- 5 在前端索引標籤中：
 - 5a 選取公用。
 - 5b 在公用 IP 位址下，按一下新增。
 - 5b1 指定公用 IP 位址名稱。例如 idmgateway.centralindia.cloudapp.azure.com。
 - 5b2 按一下確定。
 - 5c 按下一步：後端 >
- 6 在後端索引標籤中：
 - 6a 按一下新增後端集區。
 - 6a1 指定後端集區名稱。
 - 6a2 選取是以新增一個沒有目標的後端集區。
 - 6a3 按一下新增。
 - 6b 按下一步：組態 >。
- 7 在組態索引標籤中：
 - 7a 在路由規則下，按一下新增路由規則。
 - 7b 指定規則名稱。

7c 在**監聽程式索引**標籤中指定以下詳細資料：

欄位	描述
監聽程式名稱	指定監聽程式名稱。
前端 IP	從下拉式清單中選取 公用 。
通訊協定	選取 HTTP 。
連接埠	指定值 80 。

7d 保留其餘欄位的預設值。

7e 在**後端目標索引**標籤中指定以下詳細資料：

欄位	描述
後端目標	從下拉式清單中選取後端目標。
HTTP 設定	按一下 新增 ，指定 HTTP 設定名稱。保留所有欄位的預設值，然後按一下 新增 。

7e1 按一下**新增**。

7f 按下一步：**標籤 >**。

8 在**標籤索引**標籤中，按下一步：**檢閱 + 建立 >**。

9 在**檢閱 + 建立 >** 索引標籤中檢閱您的設定，然後按一下**建立**。

附註：如需關於設定應用程式閘道的詳細資訊，請參閱「[設定應用程式閘道](#)」(第 208 頁)。

建立虛擬機器例項

建立單獨的虛擬機器以代管 Identity Manager 元件。

- 1 登入 **Azure** 入口網站。
- 2 在搜尋中輸入**虛擬機器**。
- 3 在「服務」下，選取**虛擬機器**。
- 4 按一下**建立**，然後選取**虛擬機器**。
- 5 在**基本資訊索引**標籤中：
 - 5a 從下拉式清單中選取您的**訂閱**。
 - 5b 從下拉式清單中選取現有的資源群組 (參閱「[建立資源群組](#)」(第 203 頁))。
 - 5c 指定**虛擬機器名稱**。
 - 5d 從**區域**下拉式清單中選取位置。例如**印度中部**。
 - 5e 從**影像**下拉式清單中選取所需的 **Windows Server**。例如 **Windows Server 2019**。
 - 5f 從**大小**下拉式清單中選取**虛擬機器大小**。
 - 5g 指定**使用者名稱**、**密碼**並**確認密碼**。

- 5h 在「授權」下，選取 **Windows Server 授權**，然後選取符合條件的附帶軟體保證的 **Windows Server 授權**以確認。
- 5i 保留其餘欄位的預設值。
- 5j 按下一步：**磁碟**。
- 6 在**磁碟索引標籤**中：
 - 6a 從 **OS 磁碟類型**下拉式清單中選取磁碟類型。例如進階 SSD。
 - 6b 從下拉式清單中選取所需的加密類型。
 - 6c 按下一步：**網路**。
- 7 在**網路索引標籤**中：
 - 7a 選取虛擬網路和已建立的對應子網路。請參閱「[建立虛擬網路和子網路](#)」(第 203 頁)。
 - 7b 在網路安全性群組下，選取進階。
 - 7c 從下拉式清單中選取現有的網路安全性群組。
 - 7c1 (視情況而定) 如果沒有可用的網路安全性群組，請按一下**新建**。
 - 7c2 指定網路安全性群組名稱。
 - 7c3 按一下**新增輸入角色**，指定所需的詳細資料。
 - 7c4 按一下**新增輸出角色**，指定所需的詳細資料。
 - 7c5 按一下**確定**。
 - 7d 保留其餘欄位的預設值。
 - 7e 按下一步：**管理**。
- 8 在**管理索引標籤**中，保留所有欄位的預設值，然後按下一步：**進階**。
- 9 在**進階索引標籤**中，保留所有欄位的預設值，然後按下一步：**標籤**。
- 10 在**標籤索引標籤**中，保留所有欄位的預設值，然後按下一步：**檢閱 + 建立**。
- 11 在**檢閱 + 建立索引標籤**中檢閱您的設定，然後按一下**建立**。

更新 VM 中的主機項目

您可以使用應用程式間道的公用 DNS 名稱或透過別名 DNS 記錄集來存取 Identity Manager 元件。若要使 Identity Manager 元件能夠互相通訊，請編輯每個 VM 上的 hosts 檔案，並新增一個項目來解析此 VM 的主機名稱。

表格 20-1 更新主機項目

配件	描述
Identity Engine	導覽至 Identity Engine VM 中的 hosts 檔案。例如： <pre>C:\Windows\System32\drivers\etc\hosts</pre> 修改 hosts 檔案，在其中包含以下項目： <Identity Engine VM 的 IP 位址> <Identity Engine VM 的私用 DNS 名稱> 例如： <pre>10.0.1.1 identityengine.example.com</pre> <Identity Applications VM 的 IP 位址> <應用程式閘道的公用 DNS 名稱> 例如： <pre>10.0.1.2 idmgateway.centralindia.cloudapp.azure.com</pre>
Identity Applications	導覽至 Identity Engine VM 中的 hosts 檔案。例如： <pre>C:\Windows\System32\drivers\etc\hosts</pre> 修改 hosts 檔案，在其中包含以下項目： <Identity Engine VM 的 IP 位址> <Identity Engine VM 的私用 DNS 名稱> 例如： <pre>10.0.1.1 identityengine.example.com</pre> <Identity Applications VM 的 IP 位址> <應用程式閘道的公用 DNS 名稱> 例如： <pre>10.0.1.2 idmgateway.centralindia.cloudapp.azure.com</pre>

若要更新 Identity Reporting 的主機項目，請參閱[表格 20-1 \(第 207 頁\)](#) 中的 **Identity Applications**。

附註：如需 Identity Manager 元件的安裝方法，請參閱「[安裝程序](#)」(第 43 頁)。

安裝 Designer

- 1 在公用子網路中，啟動虛擬機器例項。請參閱「[建立虛擬機器例項](#)」(第 205 頁)。

對於 Windows 安全性群組，請僅使用 rdesktop 連接埠。例如 3389。

- 2 安裝 Designer。請參閱第 V 部分「安裝 Designer」(第 125 頁)。

設定應用程式閘道

設定應用程式閘道後，外部網路便可使用虛擬機器上代管的 Identity Manager 元件。

- 1 為 Identity Applications、表單和 Identity Reporting 等 Identity Manager 元件設定單獨的後端池。
 - 1a 在後端池中，按一下新增。
 - 1b 指定以下詳細資料：

欄位	描述
名稱	指定用於識別 Identity Manager 元件的後端池名稱。
類型	以下列方式之一指定類型： ◆ IP 位址或 FQDN：指定所需 Identity Manager 元件的 IP 位址或 FQDN。 ◆ 虛擬機器：選取代管所需 Identity Manager 元件的虛擬機器。

- 1c 按一下「確定」。

重複此步驟以設定更多後端池。

- 2 為 Identity Applications、表單和 Identity Reporting 等 Identity Manager 元件設定單獨的 HTTP 設定。

附註：確定您已輸出所需 Identity Manager 元件的公用證書。

- 2a 在 **HTTP 設定** 中按一下新增。

- 2b 指定以下詳細資料：

欄位	描述
名稱	指定用於識別 Identity Manager 元件的 HTTP 設定名稱。
通訊協定	選取 HTTPS。
連接埠	指定 Identity Manager 元件的連接埠。 例如： ◆ Identity Applications：8543 ◆ Forms：8600 ◆ Identity Reporting：8643
後端驗證證書	1. 選取「建立新證書」。 2. 指定證書的名稱。 3. 瀏覽並上傳為對應 Identity Manager 元件輸出的公用證書。 4. 按一下「新增證書」。

2c 按一下「確定」。

重複此步驟以組態更多 HTTP 設定。

- 3** 為每個 Identity Manager 元件 (例如 Identity Applications、表單和 Identity Reporting) 設定單獨的監聽程式。

附註：確定已從 Identity Vault 輸出 .PFX 證書。

3a 在監聽程式中按一下**基本**。

3b 指定以下詳細資料：

欄位	描述
名稱	指定用於識別 Identity Manager 元件的監聽程式名稱。
前端 IP 組態	1. 選取之前建立的虛擬網路和子網路。請參閱「建立虛擬網路和子網路」(第 203 頁)。 2. 指定應用程式的名稱和連接埠號碼。例如： Identity Applications：8543 Forms：8600 Identity Reporting：8643
通訊協定	選取 HTTPS。
證書	1. 瀏覽並上傳 PFX 證書。 2. 指定證書的名稱和密碼。

3c 按一下「確定」。

重複此步驟以設定更多監聽程式。

- 4 為 Identity Applications、表單和 Identity Reporting 等 Identity Manager 元件建立基本規則，並將此規則與相應的後端池、監聽程式和 HTTP 設定關聯。

4a 在規則中按一下新增。

4b 指定以下詳細資料：

欄位	描述
名稱	指定有助於識別 Identity Manager 元件的規則名稱。
監聽程式	選取在步驟 3 中建立的相應監聽程式。
後端池	選取在步驟 1 中建立的相應後端池。
HTTP 設定	選取在步驟 2 中建立的相應 HTTP 設定。

4c 按一下「確定」。

重複此步驟以設定更多規則。

21 範例混合式 Identity Manager 方案

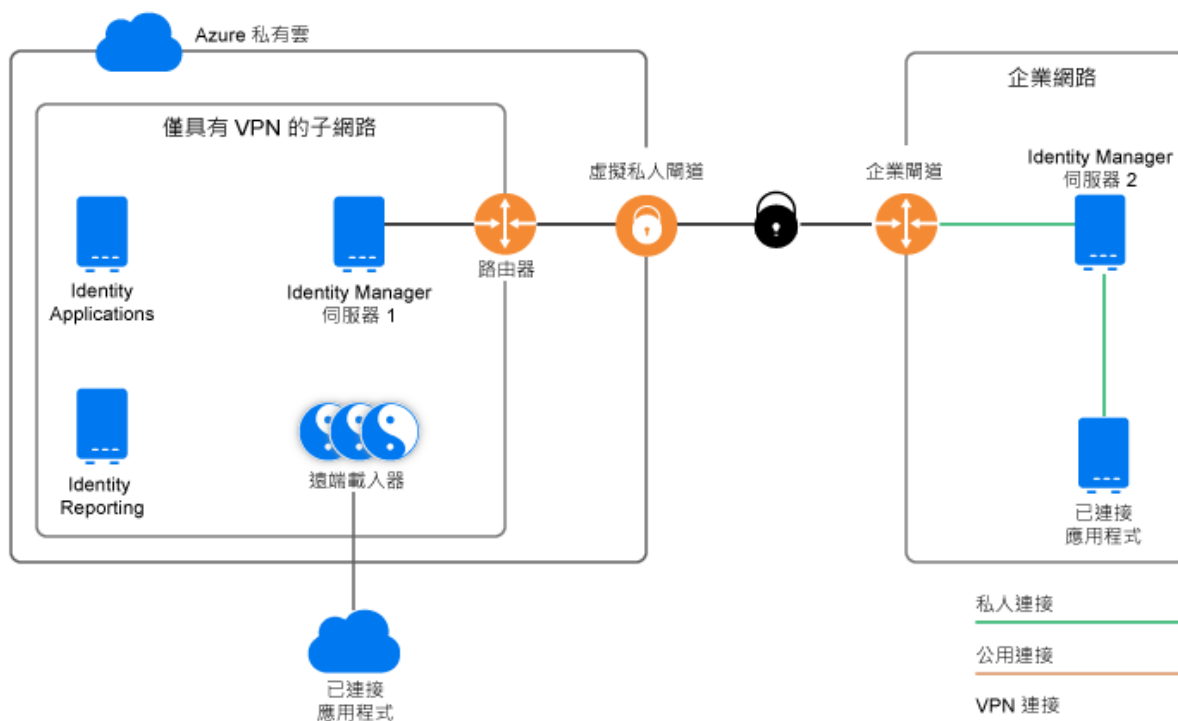
您可以對 Identity Manager 元件進行設定，以使其中的身分在企業本地與 MS Azure 雲端之間無縫同步。若要實作此類混合式方案，您需要在 Azure 子網路與企業網路之間設定 VPN 連接。本章將會對下面的混合式方案進行說明：

- 「使用多伺服器驅動程式集連接」(第 211 頁)
- 「使用 eDirectory 驅動程式集連接」(第 212 頁)

使用多伺服器驅動程式集連接

在此方案中，至少有兩部 Identity Manager 伺服器使用相同的 eDirectory 樹狀結構和驅動程式集，其中的一部伺服器安裝在 AWS 雲端，另一部伺服器安裝在企業本地。其中包括透過 VPN 連接使用 Identity Vault 複製通道同步身分的完整複本伺服器。在企業網路中或 Azure 雲端執行的 Identity Manager 伺服器會分別在各自的已連接應用程式之間同步身分。

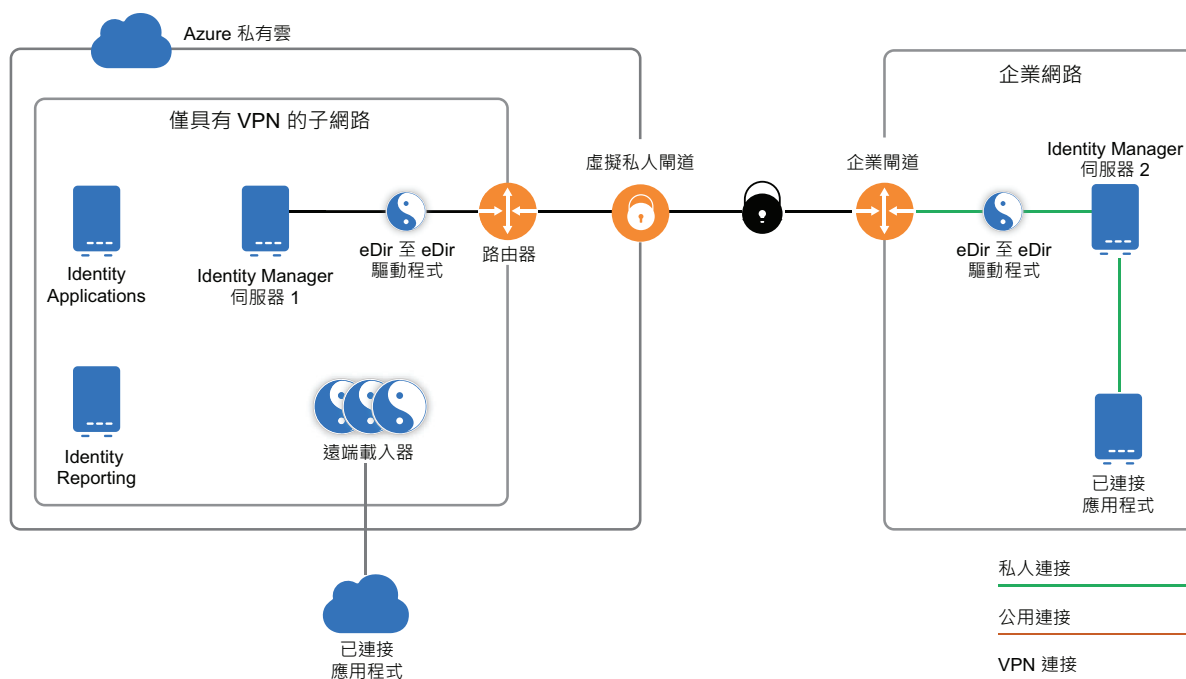
圖 21-1 使用多伺服器驅動程式集連接的混合式方案



使用 eDirectory 驅動程式連接

如果您的 Identity Manager 伺服器安裝在兩個不同的 eDirectory 樹狀結構中，其中一個樹狀結構屬於 Azure 雲端，另一個樹狀結構屬於企業網路，則適合使用此方案。此組態使用 eDirectory 驅動程式透過 VPN 連接在 Azure 雲端與企業網路之間同步身分。在企業網路中或 Azure 雲端執行的 Identity Manager 伺服器會分別在各自的已連接應用程式之間同步身分。

圖 21-2 使用 eDirectory 驅動程式連接的混合式方案



Azure 雲端與企業網路之間的通訊會受到限制。此方案只能同步增量變更。您可以透過設定驅動程式過濾器來控制要同步的屬性。您還可以利用規則引擎來定義有關同步屬性的更多控制措施。例如，限制同步密碼屬性，並允許使用者在 Azure 雲端和企業網路中使用不同的密碼存取 Identity Manager 伺服器。

X 部署 Identity Manager 以實現高可用性

高可用性可確保關鍵網路資源 (包括資料、應用程式和服務) 的高效可管理性。NetIQ 透過叢集或超級管理程式叢集 (例如 VMWare Vmotion) 支援 Identity Manager 解決方案的高可用性。規劃高可用性環境時，應考慮以下事項：

- ◆ 您可以在高可用性環境中安裝以下元件：
 - ◆ Identity Vault
 - ◆ Identity Manager 引擎
 - ◆ 遠端載入器
 - ◆ Identity Applications，不包括 Identity Reporting
- ◆ 當您在叢集環境中執行 Identity Vault 時，Identity Manager 引擎也會叢集化。

附註：Identity Manager 不支援在 Identity Vault 與 Identity Applications 之間進行負載平衡 LDAP 或 LDAPS 通訊。

若需要更多相關資訊 ...

請參閱 ...

確定 Identity Manager 元件的伺服器組態

請參閱《[NetIQ Identity Manager Overview and Planning Guide](#)》(NetIQ Identity Manager 綜覽和規劃指南) 中的「[High Availability Configuration](#)」(高可用性組態)。

在叢集中執行 Identity Vault

[Identity Manager 叢集部署解決方案範例](#)

《[NetIQ eDirectory Installation Guide](#)》(NetIQ eDirectory 安裝指南) 中的「[Deploying eDirectory on High Availability Clusters](#)」(在高可用性叢集上部署 eDirectory)

在叢集中執行 Identity Applications

[範例 Identity Applications 叢集部署解決方案](#)

如需在 Identity Manager 環境中實作高可用性和災難備援的詳細資訊，請聯絡 [NetIQ 技術支援 \(https://www.netiq.com/support/\)](#)。

以下幾章提供了有關在高可用性環境中安裝和設定 Identity Manager 元件的步驟：

- ◆ 第 22 章「在叢集環境中安裝 Identity Manager 的準備工作」(第 215 頁)
- ◆ 第 23 章「Identity Manager 叢集部署解決方案範例」(第 219 頁)
- ◆ 第 24 章「範例 Identity Applications 叢集部署解決方案」(第 221 頁)

22 在叢集環境中安裝 Identity Manager 的準備工作

- ◆ 先決條件
- ◆ 為 Identity Applications 準備叢集

先決條件

- ◆ Identity Vault
- ◆ Identity Applications
- ◆ Identity Applications 的資料庫

Identity Vault

NetIQ 建議您在叢集環境中安裝 Identity Vault 之前檢閱以下考量：

- ◆ 您必須有兩部或更多部裝有叢集軟體的 Windows 伺服器。
- ◆ 您必須有叢集軟體支援的外部共享儲存區，其磁碟空間足以儲存所有 Identity Vault 和 NCI 資料：
 - ◆ Identity Vault DIB 必須位於叢集共享儲存中。Identity Vault 的狀態資料必須位於共享儲存中，以便可供目前正執行服務的叢集節點使用。
 - ◆ 必須將每個叢集節點上的根 Identity Vault 例項設定為使用共享儲存中的 DIB。
 - ◆ 此外，您還必須共享 NCI (NetIQ International Cryptographic Infrastructure) 資料，以便在叢集節點之間複製伺服器特定的金鑰。所有叢集節點使用的 NCI 資料都必須位於叢集共享儲存中。
 - ◆ NetIQ 建議在共享儲存中儲存所有其他 eDirectory 組態和記錄資料。
- ◆ 您必須有一個虛擬 IP 位址。
- ◆ (視情況而定) 如果您要使用 eDirectory 做為 Identity Vault 的支援結構，nds-cluster-config 公用程式僅支援設定根 eDirectory 例項。eDirectory 不支援設定多個例項，並且不支援以非 root 身分在叢集環境中安裝 eDirectory。

如需在叢集環境中安裝 Identity Vault 的詳細資訊，請參閱《[NetIQ eDirectory Installation Guide](#)》(NetIQ eDirectory 安裝指南) 中的「[Deploying eDirectory on High Availability Clusters](#)」(在高可用性叢集上部署 eDirectory)。

Identity Applications

您可以在 Tomcat 叢集支援的環境中安裝 Identity Applications 的資料庫，不過需要注意以下事項：

- ◆ 叢集必須具有唯一的叢集分割區名稱、多路廣播位址和多路廣播連接埠。使用唯一的識別碼可以區分多個叢集，防止出現效能問題和異常行為。
 - ◆ 對於叢集的每個成員，必須為 Identity Applications 資料庫的監聽連接埠指定相同連接埠號。
 - ◆ 對於叢集的每個成員，必須為代管 Identity Applications 資料庫的伺服器指定相同主機名稱或 IP 位址。
- ◆ 必須同步化叢集中各伺服器的時鐘。如果伺服器時鐘不同步，工作階段可能會提前逾時，導致 HTTP 工作階段容錯移轉無法正常運作。
- ◆ NetIQ 建議不要在同一個主機上的瀏覽器索引標籤或瀏覽器工作階段之間使用多個登入。某些瀏覽器在索引標籤以及程序之間共享 Cookie，因此，允許多個登入可能會導致 HTTP 工作階段容錯移轉出現問題（此外，如果多個使用者共享一台電腦，則還可能會出現未預期的驗證功能風險）。
- ◆ 叢集節點位於同一個子網路中。
- ◆ 容錯移轉代理或負載平衡解決方案安裝在單獨的電腦上。

Identity Applications 的資料庫

資料庫叢集化是每個資料庫伺服器各自的功能。NetIQ 不會對任何叢集資料庫組態進行正式測試，因為叢集化獨立於產品功能。因此，我們在支援叢集資料庫伺服器的同時，也提出了以下告誡：

- ◆ 依預設，最大連接數設定為 100。此值可能太低，無法處理叢集中的工作流程申請負載。您可能會看到以下例外：

```
(java.sql.SQLException: Data source rejected establishment of  
connection, message from server: "Too many connections.")
```

若要增加最大連接數，請在 my.cnf 檔案中將 max_connections 變數設定為更高的值。

- ◆ 您可能需要停用叢集資料庫伺服器的某些功能或方面。例如，必須對某些表停用交易複製，因為在嘗試插入重複鍵時會出現條件約束違規。
- ◆ 我們不提供有關叢集資料庫伺服器安裝、組態或最佳化方面的協助，包括將我們的產品安裝到叢集資料庫伺服器中。
- ◆ 我們會盡最大努力來解決在叢集資料庫環境中使用我們的產品時可能出現的問題。在複雜環境中採用的疑難排解方法通常需要雙方的合作才能解決問題。NetIQ 提供分析、規劃 NetIQ 產品及對其進行疑難排解的專業知識。而客戶必須具有分析、規劃任何協力廠商產品及對其進行疑難排解的專業知識。我們將會要求客戶在非叢集環境中再現問題或分析其元件的行為，以協助將潛在的叢集設定問題與 NetIQ 產品問題分離開來。

為 Identity Applications 準備叢集

Identity Applications 支援 HTTP 工作階段複製和工作階段容錯移轉。如果某個執行中的工作階段所在的節點發生故障，無需使用者介入，該工作階段便可在叢集中的另一部伺服器上繼續進行。在叢集中安裝 Identity Applications 前應先準備好環境。

- 「瞭解 Tomcat 環境中的叢集群組」(第 217 頁)
- 「設定工作流程引擎 ID 的系統內容」(第 217 頁)
- 「為叢集中的每個使用者應用程式使用相同的萬能金鑰」(第 217 頁)

瞭解 Tomcat 環境中的叢集群組

使用者應用程式叢集群組使用 UUID 名稱，以最大程度地避免與使用者可能新增至伺服器的其他叢集群組發生衝突。您可以透過使用者應用程式管理功能來修改使用者應用程式叢集群組的組態設定。只有在重新啟動伺服器節點後，對叢集組態所做的變更才會在該節點上生效。

設定工作流程引擎 ID 的系統內容

在叢集中代管 Identity Applications 的每個伺服器都可以執行一個工作流程引擎。為確保叢集和工作流程引擎的效能，叢集中的每個伺服器都應使用相同的分割區名稱和分割區 UDP 群組。此外，叢集中的每個伺服器都必須使用唯一的工作流程引擎 ID 啟動，因為工作流程引擎的叢集化獨立於 Identity Applications 的快取架構運作。

為確保工作流程引擎正常執行，您必須設定 Tomcat 的系統內容。

- 1 對叢集中的每個 Identity Applications 伺服器建立一個新 JVM 系統內容。
- 2 將系統內容命名為 `com.novell.afw.wf.引擎 ID`，其中的引擎 ID 是一個唯一值。

為叢集中的每個使用者應用程式使用相同的萬能金鑰

Identity Applications 使用萬能金鑰來加密敏感性資料。叢集中的所有 Identity Applications 都必須使用相同的萬能金鑰。本節的內容可協助您確保叢集中的所有 Identity Applications 都使用相同的萬能金鑰。

如需加密 Identity Applications 中敏感性資料的詳細資訊，請參閱《[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)》(NetIQ Identity Manager - Identity Applications 管理員指南) 中的「[Encrypting Sensitive Identity Applications Data](#)」(加密 Identity Applications 敏感性資料)。

- 1 在叢集中的第一個節點上安裝使用者應用程式。
- 2 在安裝程式的「安全性 - 萬能金鑰」視窗中，記下將要包含 Identity Applications 新萬能金鑰的 `master-key.txt` 檔案所在的位置。依預設，該檔案位於安裝目錄中。
- 3 在叢集中的其餘節點上安裝 Identity Applications。

- 4 在「安全性 - 萬能金鑰」視窗中，按一下是，然後按下一步。
- 5 在「輸入萬能金鑰」視窗中，複製在[步驟 2](#)中建立之文字檔案中的萬能金鑰。

23 Identity Manager 叢集部署解決方案範例

本章透過逐步說明介紹如何在 Windows 2016 平台上的叢集環境中設定 Identity Manager。

- 「先決條件」(第 219 頁)
- 「在 eDirectory 叢集上設定 NetIQ Identity Manager」(第 219 頁)
- 「遠端載入器叢集化」(第 219 頁)

先決條件

在 Windows 2016 上的叢集環境中執行的 Identity Vault 9.2。如需設定 eDirectory 叢集的詳細資訊，請參閱《[NetIQ eDirectory Installation Guide](#)》(NetIQ eDirectory 安裝指南)中的「[Clustering eDirectory Services on Windows](#)」(在 Windows 上將 eDirectory 服務叢集化)。

附註：Identity Vault 不支援使用多個叢集節點進行負載平衡。eDirectory 叢集只是用於實現容錯移轉功能。

在 eDirectory 叢集上設定 NetIQ Identity Manager

本節假設您已設定 eDirectory 叢集。

請依照以下程序在 eDirectory 叢集環境中設定 Identity Manager。

- 1 在主要節點上的叢集管理員中，將 eDirectory 叢集角色優先程度設定為**不自動啟動**。
- 2 停止次要節點。
- 3 在 Identity Manager 安裝精靈中，透過選取 **Metadirectory 伺服器** 選項在主要節點上安裝 Identity Manager 引擎。

重要：確認您是在本地儲存上安裝 Identity Manager 引擎。

- 4 Identity Manager 安裝精靈會在安裝期間停止 eDirectory 叢集角色。當此角色停止時，此角色的狀態可能會顯示為失敗。安裝後，請從叢集管理員中啟動 eDirectory 叢集角色。
- 5 為 eDirectory 叢集角色設定必要的優先程度，並將次要節點設為主動節點。
- 6 使用 DCLUSTER_INSTALL 指令在次要節點上安裝 Identity Manager 引擎。

例如 `idm_install.exe -DCLUSTER_INSTALL="true"`

遠端載入器叢集化

- 1 在主要和次要叢集節點上安裝遠端載入器。

附註：對於主要和次要節點，請確認遠端載入器安裝在相同的共享儲存路徑上。

2 (視情況而定) 如果您與遠端載入器之間使用的是安全通訊，請將所有 SSL 證書都儲存在共享儲存中。

3 在建立遠端載入器叢集角色前，開啟遠端載入器主控台，然後選取遠端載入器做為 **Windows 服務**。

4 在叢集管理員 > 角色中，建立一個新的遠端載入器叢集角色。

指定該角色的以下資訊：

角色類型：一般服務

選取服務：遠端載入器例項會註冊為 Windows 服務。

名稱：叢集角色名稱

位址：唯一的 IP 位址

選取儲存：共享叢集儲存

複製登錄設定：

1. HKEY_LOCAL_MACHINE\SOFTWARE\Novell\RLConsole
2. HKEY_LOCAL_MACHINE\SOFTWARE\Novell\DirXML Remote Loader\Command port 8000

指定您要叢集化的遠端載入器例項的登錄路徑。

3. HKEY_LOCAL_MACHINE\SOFTWARE\Novell\PassSync

附註：

- ◆ 每個叢集角色預設僅接受一項 Windows 服務。因此，請指定對每個遠端載入器例項而言唯一的指令連接埠和相應的登錄路徑。
 - ◆ Windows 叢集不支援 Active Directory 驅動程式的密碼過濾器。
-

24 範例 Identity Applications 叢集部署解決方案

本章透過一個範例部署說明如何在 Tomcat 應用程式伺服器上的叢集環境中設定 Identity Applications。

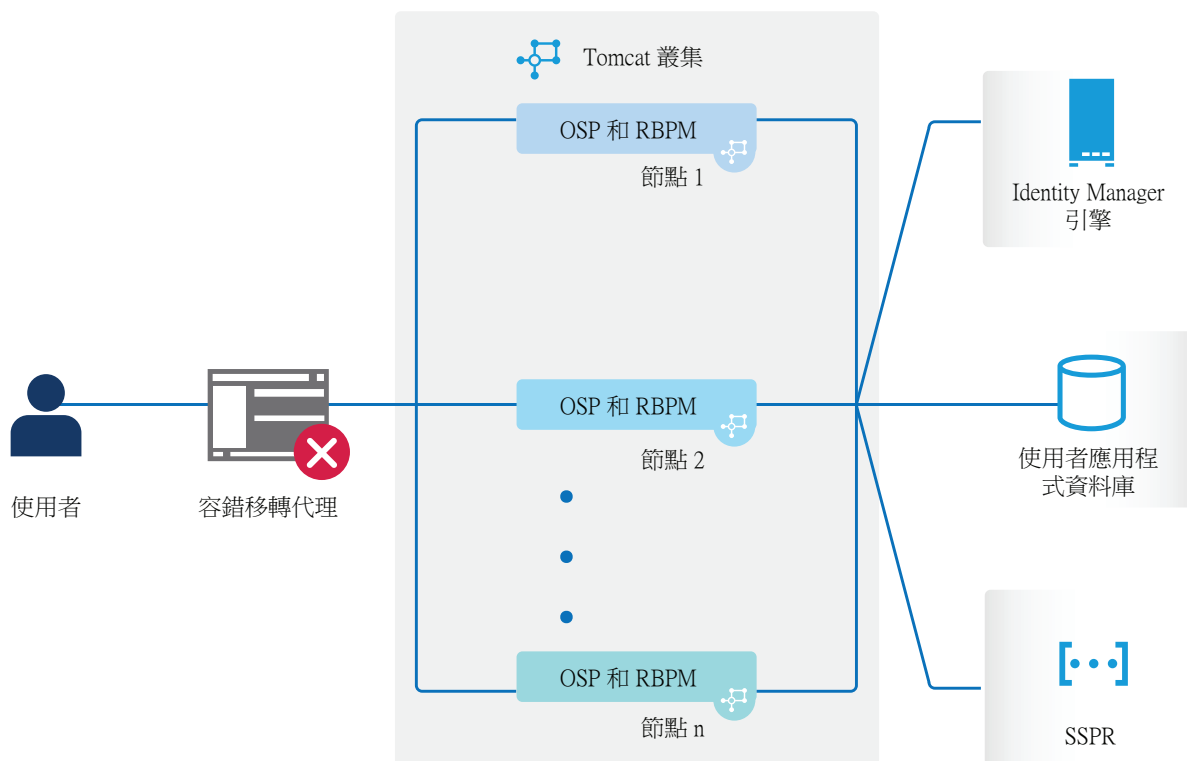
使用叢集，您可以在多部平行伺服器（叢集節點）上執行 Identity Applications，同時實現高可用性。若要建立叢集，需要將若干個 Tomcat 例項（節點）組合在一起。負載將分散在不同的伺服器之間，即使有任何伺服器發生故障，您仍可透過其他叢集節點來存取 Identity Applications。若要實現容錯移轉，您可以建立一個 Identity Applications 叢集，然後對這些 Identity Applications 進行設定以做為單部伺服器。不過，此組態不包括 Identity Reporting。

建議使用負載平衡器軟體，它會處理所有使用者申請並將它們發送給叢集中的伺服器節點。負載平衡器通常是叢集的一部分。它瞭解叢集組態及容錯移轉規則。您可以選取最適合您的解決方案。

圖 24-1 顯示了一個包含雙節點叢集的範例部署，並做出如下假設：

- ◆ 所有通訊都透過負載平衡器路由。
- ◆ Identity Manager 引擎和使用者應用程式等元件安裝在單獨的伺服器上。建議對生產層級部署採用此方法。
- ◆ 您熟悉 eDirectory、Identity Manager 引擎、Identity Applications、Apache Tomcat 應用程式伺服器和使用者應用程式資料庫的安裝程序。
- ◆ OSP (One Single-Sign On Provider) 與使用者應用程式安裝在同一個叢集節點上。但在生產環境中，您可以將 OSP 安裝其他伺服器上。在此情況下，您需要執行「[安裝程序](#)」（第 223 頁）中所述的一些組態變更。
- ◆ SSPR (Single Sign-On Password Reset) 安裝在單獨的電腦上。建議對生產層級部署採用此方法。
- ◆ 使用 PostgreSQL 做為使用者應用程式的資料庫。不過，您可以使用 Identity Manager 4.9 支援的任何資料庫，例如 Oracle、SQL Server 或 PostgreSQL。
- ◆ 所有使用者應用程式節點均與 eDirectory 和使用者應用程式資料庫的同一個例項通訊。您可以依據自己的要求，增加使用者應用程式例項數量。

圖 24-1 叢集部署解決方案範例



附註：雙節點叢集是實現高可用性的最低組態。不過，您可以輕鬆地對包含更多節點的叢集沿用本章中的思路。

為了協助您瞭解逐步組態，本文後續小節中通篇都會參考此範例部署。

先決條件

- ◆ 兩部執行 Windows Server 2022、Windows Server 2022 R2 或 Windows Server 2016 的伺服器做為節點。
- ◆ 已安裝不早於 4.9 版的 Identity Manager 元件。若要升級至 Identity Manager 4.9，請參閱第 16 章「升級 Identity Manager 的元件」(第 157 頁)。
- ◆ 所有節點的應用程式伺服器時鐘都相同。確保這一點最簡單的方法就是，將節點設定為使用同一部網路時間伺服器來透過 NTP 同步時間。
- ◆ 叢集節點位於同一個子網路中。
- ◆ 容錯移轉代理或負載平衡解決方案安裝在單獨的電腦上。
- ◆ 若要實現表單叢集化，請在伺服器上啟動兩個負載平衡器例項，一個用於 Identity Applications，另一個用於表單轉譯器。

安裝程序

本節提供在 Tomcat 上安裝新 Identity Applications 例項，然後針對叢集設定該例項的逐步說明。

1. 安裝 Identity Manager 引擎。如需逐步指示，請參閱「[安裝程序](#)」(第 43 頁)。對於生產層級部署，建議將 Identity Manager 引擎安裝在單獨的伺服器上。
2. 為 Identity Applications 建立並部署以下驅動程式：
 - ◆ 使用者應用程式驅動程式
 - ◆ 角色與資源服務驅動程式
3. 在節點 1 上安裝以下 Identity Manager 元件：

- a. 使用者應用程式

在安裝過程中進行以下設定：

- i. 選取 **Tomcat** 做為應用程式伺服器。
- ii. 選取 **PostgreSQL** 做為資料庫平台。

附註：您可以使用 Identity Manager 4.9 支援的任何資料庫。

- iii. 在後續頁面中提供必需的資料庫詳細資料。
- iv. 將 PostgreSQL 伺服器上的資料庫驅動程式 jar 檔案 postgresql-42.6.1.jar 複製到叢集中的所有使用者應用程式節點上。

附註：如果您使用的是 Identity Manager 4.9 支援的其他資料庫 (例如 Oracle 或 SQL Server)，請務必將安裝資料庫的伺服器上的相應驅動程式 jar 檔案複製到叢集中的所有使用者應用程式節點上。如需詳細資訊，請參閱「[設定 Identity Applications 的資料庫](#)」(第 64 頁)。

- v. 瀏覽並選取所複製的資料庫驅動程式 jar 檔案。
- vi. 在新資料庫或現有資料庫詳細資料頁面中，選取**新資料庫**選項。
- vii. 在 Identity Manager 「組態」頁面的**工作流程引擎 ID**欄位中提供唯一的名稱。例如，您可以為節點 1 使用唯一的名稱 **Engine1**。
- viii. 若要建立新的萬能金鑰，請在「安全性 – 萬能金鑰」頁面中選取否。

Identity Applications 使用萬能金鑰來加密敏感性資料。由於這是叢集中的第一個 Identity Applications 例項，因此必須選取否以指示安裝程式建立新的萬能金鑰。在叢集中，使用者應用程式叢集要求每個使用者應用程式例項都使用相同的萬能金鑰。為確保使用相同的萬能金鑰，請在設定這些例項時選取是以輸入現有金鑰。

4. 在節點 2 上執行以下動作：

- a. 使用便捷安裝程式安裝 Tomcat (在安裝過程中僅選取 Tomcat)。
- b. 安裝 OSP。

安裝期間，請在驗證詳細資料頁面中提供 Identity Manager 引擎 (eDirectory) 伺服器的 IP 位址和連接埠號碼。

- c. 安裝使用者應用程式。
在安裝過程中進行以下設定：
 - i. 選取 **Tomcat** 做為應用程式伺服器。
 - ii. 選取 **PostgreSQL** 做為資料庫平台。

附註：您可以使用 **Identity Manager 4.9** 支援的任何資料庫。

- iii. 在安裝程序的後續頁面中提供必需的資料庫詳細資料。
- iv. 將 **PostgreSQL** 伺服器上的資料庫驅動程式 **jar** 檔案 `postgresql-9.4.1212.jar` 複製到節點 2 上。

附註：如果您使用的是 **Identity Manager 4.9** 支援的任何其他資料庫 (例如 **Oracle** 或 **SQL Server**)，請務必將安裝資料庫的伺服器上的相應驅動程式 **jar** 檔案複製到叢集中的所有使用者應用程式節點上。

- v. 瀏覽並選取所複製的資料庫驅動程式 **jar** 檔案。
- vi. 在新資料庫或現有資料庫詳細資料頁面中，選取**現有資料庫**選項。
- vii. 在 **Identity Manager** 「組態」頁面的**工作流程引擎 ID** 欄位中提供唯一的名稱。例如，您可以為節點 2 使用唯一的名稱 **Engine2**。
- viii. 若要在「安全性 – 萬能金鑰」頁面中建立新的萬能金鑰，請選取**是**。
使用者應用程式叢集要求每個使用者應用程式例項都使用相同的萬能金鑰。為確保使用相同的萬能金鑰，請選取**是**以輸入現有金鑰。此金鑰是您在節點 1 中安裝第一個使用者應用程式例項時建立的。
您可以從節點 1 上位於 `C:\NetIQ\IDM\apps\tomcat\conf` 中的 **ism-configuration** 內容檔案獲取萬能金鑰。包含萬能金鑰的參數是 `com.novell.idm.masterkey`。
- ix. 按一下**安裝**以完成安裝。

附註：如需安裝 **Identity Applications** 的詳細資訊，請參閱「**安裝程序**」(第 43 頁)。

- 5. 在負載平衡器伺服器中，針對所有叢集節點使用 **Identity Applications** 連接埠號碼啟動一個負載平衡器例項，使用表單轉譯器連接埠號碼啟動另一個負載平衡器例項。例如：
 - ◆ `./balance 8543 apps1-au.edu.in:8543 ! apps2-au.edu.in:8543`
 - ◆ `./balance 8600 apps1-au.edu.in:8600 ! apps2-au.edu.in:8600`
- 6. 在單獨的電腦上安裝 **SSPR**。
安裝前請記下以下設定，並在安裝過程中指定這些設定：
 - a. 安裝 **Tomcat**。如需安裝說明，請參閱步驟 4a。
 - b. 安裝 **SSPR**。

在 SSPR 安裝期間，執行以下動作：

- i. 在應用程式伺服器連接頁面中，選取**連接至外部驗證伺服器**，並提供安裝了負載平衡器的伺服器的 DNS 名稱。
- ii. 在驗證詳細資料頁面中，提供 Identity Manager 引擎伺服器的 IP 位址和連接埠。CA 證書的密碼為 changeit。
- c. 完成 SSPR 安裝後，啟動 SSPR (<https://<IP>:<port>/sspr/private/config/ConfigEditor>) 並登入其中。按一下**組態編輯器 > 設定 > 安全性 > 重新導向白名單**。
 - i. 按一下**新增值**並指定以下 URL：
`https:<容錯移轉的 DNS><連接埠>/osp`
 - ii. 儲存變更。
 - iii. 在 SSPR 「組態」頁面中，按一下**設定 > OAuth SSO**，然後修改 OSP 連結 - 以安裝負載平衡器軟體的伺服器的 DNS 名稱取代 IP 位址。
 - iv. 按一下**設定 > 應用程式**，然後更新轉遞和登出 URL - 以安裝負載平衡器軟體的伺服器的 DNS 名稱取代 IP 位址。
- d. 若要在節點 1 上更新 SSPR 資訊，請啟動位於 `C:\NetIQ\idm\apps\UserApplication\configupdate.bat` 的組態公用程式。在隨即開啟的視窗中，按一下**SSO 用戶端 > Self Service Password Reset**，並為用戶端 ID、密碼和 OSP OAuth 重新導向 URL 參數輸入值。

附註：驗證節點 2 中是否更新了這些參數的值。

7. 在叢集節點上執行以下組態任務：
 - a. 在所有叢集節點上重新啟動 Tomcat。
 - b. 若要變更「變更我的密碼」連結，請參閱「[針對分散式環境或叢集環境更新儀表板中的 SSPR 連結](#)」(第 63 頁)。
 - c. 在節點 2 上，驗證「忘記密碼」連結和「變更我的密碼」連結是否已用 SSPR IP 位址更新。

附註：如果「變更密碼」和「忘記密碼」連結已用 SSPR IP 位址更新，則不需要執行其他變更。

8. 在節點 1 中，停止 Tomcat，並使用以下指令指定負載平衡器伺服器的 DNS 名稱，以產生新 osp.jks 檔案：

```
C:\NetIQ\Common\JRE\bin\keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass <password> -keypass <password> -alias osp -validity 1800 -dname "cn=<loadbalancer IP/DNS>"
```

```
例如：C:\NetIQ\idm\apps\jre\bin\ -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass changeit -keypass changeit -alias osp -validity 1800 -dname "cn=mydnsname"
```

附註：確認金鑰密碼與在 OSP 安裝期間提供的密碼相同。或者，可以使用組態更新公用程式並包括金鑰儲存區密碼來變更該密碼。

9. (視情況而定) 若要驗證 osp.jks 檔案是否已透過這些變更更新，請執行以下指令：

```
C:\NetIQ\Common\JRE\bin\keytool -list -v -keystore osp.jks -storepass changeit
```

10. 備份位於 C:\NetIQ\idm\apps\osp 中的原始 osp.jks 檔案，並將新的 osp.jks 檔案複製到此位置。新 osp.jks 檔案是在步驟 8 中建立的。

11. 將節點 1 上的新 osp.jks 檔案複製到叢集中的其他使用者應用程式節點上。

12. 在每個叢集節點上：

- a. 導覽至 C:\netiq\idm\apps\sites 目錄，然後編輯 ServiceRegistry.json 檔案以新增負載平衡器詳細資料。

```
{"serviceRegistries": [{"serviceID": "IDM", "restUrl": "https://<DNS of the load balancer>:8543/IDMProv"}]}
```

- b. 導覽至 C:\netiq\idm\apps\sites\ 目錄，然後編輯 config.ini 檔案以新增負載平衡器 DNS 和連接埠號碼。

```
OSPIssuerUrl=https://<DNS of the load balancer>:8543/osp/a/idm/auth/oauth2
OSPRedirectUrl=https://<DNS of the load balancer>:8600/forms/oauth.html
ClientID=forms
OSPLogoutUrl=https://<DNS of the load balancer>:8543/osp/a/idm/auth/app/logout
```

13. 在節點 1 中啟動組態公用程式，並在「SSO 用戶端」索引標籤下將所有 URL 設定 (例如抵達頁面的 URL 連結和 OAuth 重新導向 URL) 變更為負載平衡器 DNS 名稱。

- a. 儲存在組態公用程式中所做的變更。檢查 ism-configuration properties 檔案是否體現了相應變更，若有任何 URL 仍指向節點 1 DNS 和連接埠，請予以修改。

- b. 若要在叢集的所有其他節點中反映此變更，請將節點 1 上位於 C:\NetIQ\IDM\apps\tomcat\conf 中的 ism-configuration properties 檔案複製到叢集中的其他使用者應用程式節點上。

附註：您之前已將節點 1 上的 ism.properties 檔案複製到叢集中的其他節點上。如果您在使用者應用程式安裝期間指定了自訂安裝路徑，請在叢集節點中使用組態更新公用程式確保參考路徑正確。

此情境中，OSP 和使用著應用程式安裝在同一部伺服器上；因此，為重新導向 URL 使用了相同的 DNS 名稱。

如果 OSP 和使用著應用程式安裝在不同的伺服器上，請將 OSP URL 變更為指向負載平衡器的不同 DNS 名稱。請對安裝了 OSP 的所有伺服器執行此操作。執行此操作可確保所有 OSP 申請均透過負載平衡器發送到 OSP 叢集 DNS 名稱。這涉及到為 OSP 節點建立一個單獨的叢集。

14. 在位於 /TOMCAT_INSTALLED_HOME/bin/ 目錄下的 setenv.sh 檔案中執行以下動作：
 - a. 為確保 mcast_addr 繫結成功，JGroups 要求將 preferIPv4Stack 內容設定為 **true**。為此，請在所有節點上的 setenv.sh 檔案中新增 JVM 內容「-Djava.net.preferIPv4Stack=true」。
 - b. 在節點 1 上的 setenv.sh 檔案中新增「-Dcom.novell.afw.wf.Engine-id=Engine1」。同樣，為叢集中的每個節點新增唯一的引擎名稱。例如，對於節點 2，可以新增引擎名稱 Engine2。
15. 在使用者應用程式中啟用叢集。
 - a. 在節點 1 上啟動 Tomcat。
不要啟動任何其他伺服器。
 - b. 以使用者應用程式管理員身分登入使用者應用程式。
 - c. 按一下**組態 > 快取和叢集**選項。
使用者應用程式將顯示「快取管理」頁面。
 - d. 按一下**叢集快取組態**，並為叢集已開啟內容選取 **True**。
 - e. 按一下**儲存**。
 - f. 重新啟動 Tomcat。

附註：如果您已選取「啟用本地」設定，請針對叢集中的每個伺服器重複此程序。

使用者應用程式叢集使用 JGroups 在採用預設 UDP 的節點間進行快取同步。如果您想將此通訊協定變更為使用 TCP，請參閱「[Configuring User Application to use TCP](#)」（將使用者應用程式設定為使用 TCP）。

16. 為叢集啟用許可權索引。如需詳細資訊，請參閱「[為叢集啟用許可權索引](#)」（第 228 頁）。

17. 啟用 Tomcat 叢集。

在所有叢集節點上開啟 /TOMCAT_INSTALLED_HOME/conf/ 中的 Tomcat server.xml 檔案，並取消注釋此檔案中的下行：

```
<Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
```

對於進階 Tomcat 叢集組態，請依照 [Apache 文件網站](#) 中的步驟操作。

18. 在所有節點上重新啟動 Tomcat。

19. 為叢集設定使用者應用程式驅動程式。

在叢集環境中，可以將單個使用者應用程式驅動程式與多個使用者應用程式例項配合使用。該驅動程式會儲存應用程式特定的各種資訊（例如工作流程組態和叢集資訊）。必須將驅動程式設定為使用叢集的發送器或負載平衡器的主機名稱或 IP 位址。

- a. 登入用於管理 Identity Vault 的 Identity Console 例項。
- b. 在「Identity Manager」磚下，選取 **Identity Manager 管理**。
- c. 選取包含您的使用者應用程式驅動程式的驅動程式集。
- d. 按一下**驅動程式圖示**。
- e. 移至**組態**。
- f. 按一下**驅動程式參數**下拉式清單。

- g. 在**驅動程式設定索引標籤**中，將主機變更為負載平衡器的主機名稱或 IP 位址。
 - h. 按一下「儲存」。
 - i. 重新啟動驅動程式。
20. 若要變更角色與資源服務驅動程式的 URL，請重複步驟 19a 至 19f，然後按一下**驅動程式組態**，並以負載平衡器 DNS 名稱更新**使用者應用程式 URL**。
 21. 確認針對使用者應用程式節點的負載平衡器軟體中建立的叢集啟用了工作階段綁定。

大多數負載平衡器都提供狀態檢查功能，以確定 HTTP 伺服器是否已啟動且正在監聽。使用者應用程式包含一個 URL，可用於設定負載平衡器上的 HTTP 狀態檢查。該 URL 為：

`http://< 節點 IP>: 連接埠 /IDMProv/jsps/healthcheck.jsp`

為叢集啟用許可權索引

本節提供為叢集啟用許可權索引的說明。

- 1 在節點 1 中登入 Identity Console，然後導覽至**樹狀檢視**。
- 2 在樹狀檢視的左側窗格中，選取**系統** > 包含使用者應用程式驅動程式的**驅動程式集**。
- 3 然後選取 **AppConfig** > **AppDefs**。
- 4 在右側窗格中選取**組態**。
- 5 在**值屬性**下選取 **XMLData** 屬性，並將 `com.netiq.idm.cis.clustered` 內容設定為 **true**。

例如：

```
<property>
  <key>com.netiq.idm.cis.clustered</key>
  <value>true</value>
</property>
```

- 6 按一下「儲存」。

25 解除安裝 Identity Manager 的元件

本章介紹解除安裝 Identity Manager 各元件的程序。解除安裝某些元件需要符合一些先決條件。在開始執行解除安裝程序之前，請務必檢閱每個元件的相關完整章節。

附註：在解除安裝 Identity Manager 元件之前，必須先停止所有服務，例如 Tomcat、PostgreSQL 和 ActiveMQ。

解除安裝 Identity Vault

在解除安裝 Identity Vault 之前，您必須瞭解 eDirectory 樹狀結構和複本佈置。例如，您應該知道網路樹中是否包含多個伺服器。

1 (視情況而定) 如果 eDirectory 網路樹中有多個伺服器，請完成以下步驟：

1a (視情況而定) 如果安裝 eDirectory 的伺服器保留了任何主複製本，請在移除 eDirectory 之前，將複本環中的另一個伺服器升級為主伺服器。

如需詳細資訊，請參閱《[NetIQ eDirectory Administration Guide](#)》(NetIQ eDirectory 管理指南) 中的「[Managing Partitions and Replicas](#)」(管理分割區和複製本)。

1b (視情況而定) 如果安裝 eDirectory 的伺服器上的樹中保留了某個分割區的唯一副本，請將此分割區合併到母分割區中，或者將此分割區的複製本新增至另一個伺服器中，並使該伺服器成為主複製本持有者。

如需詳細資訊，請參閱《[NetIQ eDirectory Administration Guide](#)》(NetIQ eDirectory 管理指南) 中的「[Managing Partitions and Replicas](#)」(管理分割區和複製本)。

1c 對 eDirectory 資料庫執行狀態檢查。在繼續下一步之前，修復發生的所有錯誤。

如需詳細資訊，請參閱《[NetIQ eDirectory Administration Guide](#)》(NetIQ eDirectory 管理指南) 中的「[Keeping eDirectory Healthy](#)」(維護 eDirectory 的健康)。

2 解除安裝 Identity Vault：

使用用於新增和移除程式的控制台公用程式。例如，在 Windows Server 2012 R2 上，按一下**程式和功能**。在 **NetIQ eDirectory** 上按一下滑鼠右鍵，然後按一下**解除安裝**。

3 (視情況而定) 如果 eDirectory 網路樹中有多個伺服器，請完成以下步驟：

3a 刪除網路樹中左側的所有伺服器特定物件。

3b 再次執行狀態檢查，以驗證是否已從網路樹中正確移除伺服器。

如需詳細資訊，請參閱《[NetIQ eDirectory Administration Guide](#)》(NetIQ eDirectory 管理指南) 中的「[Keeping eDirectory Healthy](#)」(維護 eDirectory 的健康)。

從 Identity Vault 中移除物件

解除安裝 Identity Manager 的第一步是從 Identity Vault 刪除所有 Identity Manager 物件。建立驅動程式集時，精靈會提示您將驅動程式集設定為分割區。如果有任何驅動程式集物件也是 eDirectory 中的分割區根物件，則該分割區必須合併至母分割區，然後您才能刪除該驅動程式集物件。

若要從 Identity Vault 中移除物件：

- 1 在繼續操作之前，對 eDirectory 資料庫執行狀態檢查，然後修復出現的所有錯誤。
如需詳細資訊，請參閱《[NetIQ eDirectory Administration Guide](#)》(NetIQ eDirectory 管理指南) 中的「[Keeping eDirectory Healthy](#)」(維護 eDirectory 的健康)。
- 2 以對 eDirectory 樹狀結構具有完整權限的管理員身分登入 Identity Console。
- 3 選取分割區管理。
- 4 瀏覽並選取作為分割區根物件的驅動程式集物件，然後按一下「確定」。
- 5 等待合併程序完成，然後按一下「確定」。
- 6 刪除驅動程式集物件。
當您刪除驅動程式集物件時，刪除程序會刪除與該驅動程式集關聯的所有驅動程式物件。
- 7 對於每一個位於 eDirectory 資料庫的驅動程式集物件，重複步驟 3 到步驟 6，直到它們全都刪除為止。
- 8 重複步驟 1，以確保所有合併均已完成，而且所有物件均已刪除。

解除安裝 Identity Manager 引擎

當您安裝 Identity Manager 引擎時，安裝程序會在 Identity Manager 伺服器上新增一個解除安裝程序檔。使用此程序檔可以移除安裝期間建立的所有服務、套件和目錄。

附註：在解除安裝 Identity Manager 引擎之前，請準備 Identity Vault。如需詳細資訊，請參閱「[從 Identity Vault 中移除物件](#)」(第 230 頁)。

若要在 Windows 伺服器上解除安裝 Identity Manager 引擎，請使用用於新增和移除程式的控制台公用程式。例如，在 Windows 2012 R2 上，按一下程式和功能。在 Identity Manager 上按一下滑鼠右鍵，然後按一下解除安裝。

解除安裝遠端載入器

當您安裝遠端載入器時，安裝程序會在伺服器上新增一個解除安裝程序檔。使用此程序檔可以移除安裝期間建立的所有服務、套件和目錄。

若要在 Windows 伺服器上解除安裝遠端載入器，請使用用於新增和移除程式的控制台公用程式。

解除安裝 Identity Applications

您必須解除安裝 Roles Based Provisioning Module (RBPM) 的每個元件，例如驅動程式和資料庫。

如果您需要解除安裝與 RBPM 相關聯的執行時期元件，解除安裝程式會自動將伺服器重新開機，除非您是以靜默模式在 Windows 上執行解除安裝程式。您必須手動將 Windows 伺服器重新開機。

附註：在解除安裝 RBPM 之前，請先解除安裝 Identity Manager 引擎。如需詳細資訊，請參閱「[解除安裝 Identity Manager 引擎](#)」(第 230 頁)。

刪除 Roles Based Provisioning Module 的驅動程式

可以使用 Designer 或 Identity Console 來刪除使用者應用程式驅動程式和角色與資源服務驅動程式。

- 1 停止使用者應用程式驅動程式以及角色與資源服務驅動程式。根據所用的元件完成下列其中一個動作：
 - ◆ **Designer**：在驅動程式行上按一下滑鼠右鍵，然後按一下「即時」>「停止驅動程式」。
 - ◆ **Identity Console**：在「驅動程式集綜覽」頁面中，按一下驅動程式影像的右上角，然後按一下停止驅動程式。
- 2 刪除使用者應用程式驅動程式以及角色與資源服務驅動程式。根據所用的元件完成下列其中一個動作：
 - ◆ **Designer**：在驅動程式行上按一下滑鼠右鍵，然後按一下「刪除」。
 - ◆ **Identity Console**：在「驅動程式集綜覽」頁面中，按一下驅動程式 > 刪除驅動程式，然後按一下要刪除的驅動程式。

解除安裝 Identity Applications

必須從 Tomcat 中解除安裝使用者應用程式及其資料庫。此程序描述如何從 Tomcat 和 PostgreSQL 中移除使用者應用程式及其資料庫。如果您使用的是其他應用程式伺服器與資料庫，相關指示請參閱該產品的文件。

重要：請謹慎移除使用者應用程式，因為這會從安裝了使用者應用程式程序檔和支援檔案的資料夾中移除所有資料夾和檔案。移除這些檔案時，您有可能會無意中解除安裝 Tomcat 或 PostgreSQL。例如，安裝資料夾通常為 C:\NetIQ\idm\apps\UserApplication。此資料夾中還包含 Tomcat 和 PostgreSQL 的資料夾。

- 1 登入安裝了使用者應用程式的伺服器。
- 2 開啟用於新增和移除程式的控制台公用程式。例如，在 Windows Server 2012 R2 上，按一下程式和功能。
- 3 在 **Identity Manager** 使用者應用程式上按一下滑鼠右鍵，然後按一下解除安裝。

解除安裝 Identity Reporting 元件

您必須依照以下順序解除安裝 Identity Reporting 的元件：

1. 刪除驅動程式。如需詳細資訊，請參閱「[刪除報告驅動程式](#)」(第 232 頁)。
2. 刪除 Identity Reporting。如需詳細資訊，請參閱「[解除安裝 Identity Reporting](#)」(第 232 頁)。
3. 刪除 Sentinel。如需詳細資訊，請參閱《[NetIQ Identity Manager 安裝和升級指南 - Linux](#)》中的「[解除安裝 Sentinel Log Management for IGA](#)」。

附註：為了節省磁碟空間，Identity Reporting 的安裝程式不會安裝 Java 虛擬機器 (JVM)。因此，若要解除安裝一或多個元件，請確保您有可用的 JVM，並且該 JVM 位於 PATH 中。如果在解除安裝期間遇到錯誤，請將 JVM 的位置新增至本地 PATH 環境變數，然後再次執行解除安裝程式。

刪除報告驅動程式

您可以使用 Designer 或 Identity Console 來刪除資料收集驅動程式和受管理系統閘道驅動程式。

- 1 停止驅動程式。根據所用的元件完成下列其中一個動作：
 - ◆ **Designer**：對於每個驅動程式，在驅動程式行上按一下滑鼠右鍵，然後按一下**即時 > 停止驅動程式**。
 - ◆ **Identity Console**：在「驅動程式集綜覽」頁面中，按一下每個驅動程式影像的右上角，然後按一下**停止驅動程式**。
- 2 刪除驅動程式。根據所用的元件完成下列其中一個動作：
 - ◆ **Designer**：對於每個驅動程式，在驅動程式行上按一下滑鼠右鍵，然後按一下**刪除**。
 - ◆ **Identity Console**：在「驅動程式集綜覽」頁面中，按一下**驅動程式 > 刪除驅動程式**，然後按一下要刪除的驅動程式。

解除安裝 Identity Reporting

在刪除 Identity Reporting 之前，請確保您已刪除資料收集驅動程式和受管理系統閘道驅動程式。如需詳細資訊，請參閱「[刪除報告驅動程式](#)」(第 232 頁)。

重要：在執行 Identity Reporting 解除安裝程式之前，請確保您已將產生的報告從 Reporting 安裝目錄複製到電腦上的其他位置，因為解除安裝程序會從 Reporting 安裝目錄中移除所有檔案和資料夾。例如，Reporting 安裝資料夾 C:\NetIQ\idm\apps\IDMReporting。

若要解除安裝 Identity Reporting，請使用用於新增和移除程式的控制台公用程式。例如，在 Windows Server 2012 R2 上，按一下**程式和功能**。在 **Identity Reporting** 上按一下滑鼠右鍵，然後按一下**解除安裝**。

解除安裝 Analyzer

重要：Identity Manager 4.9 ISO 中不包含 Analyzer 工具。如果已安裝 Analyzer，請務必將其更新至版本 4.8.5，並與 Identity Manager 4.9 配合使用。

- 1 關閉 Analyzer。
- 2 解除安裝 Analyzer。

使用用於新增和移除程式的控制台公用程式。例如，在 Windows Server 2008 上，按一下程式和功能。在 **Analyzer for Identity Manager** 上按一下滑鼠右鍵，然後按一下**解除安裝**。

解除安裝 Designer

- 1 關閉 Designer。
- 2 根據作業系統解除安裝 Designer：

使用用於新增和移除程式的控制台公用程式。例如，在 Windows Server 2008 上，按一下程式和功能。在 **Designer for Identity Manager** 上按一下滑鼠右鍵，然後按一下**解除安裝**。

26 疑難排解

本章提供對 Identity Manager 安裝問題進行疑難排解的實用資訊。如需 Identity Manager 疑難排解的詳細資訊，請參閱具體元件的指南。

Identity Manager 引擎疑難排解

下表列出了您可能會遇到的問題，以及為解決這些問題建議執行的動作。如果問題持續發生，請聯絡您的 NetIQ 代表。

問題	建議執行的動作
當 eDirectory 啟始化程序正在進行時，Identity Manager 引擎無法啟動。如果 eDirectory DIB 極大，則很有可能會出現此問題。	請執行以下步驟來解決此問題： 1. 建立名為 SLEEP_BEFORE_ENGINE_STARTUP 的系統環境變數，並將該變數的值設定為 0 至 600。該值以秒為單位。 附註：如果提供的值無效或大於 600，將使用預設值 600。 2. 重新啟動 eDirectory。 3. (視情況而定) 檢查 dhost.log 以檢視訊息和記錄。
在多伺服器環境中顯示了一個無法辨識的延伸例外。	確定主要伺服器具有次要伺服器的讀寫分割區： 1. 登入 Identity Console。 2. 按一下分割區管理。 3. 選取次要伺服器。 4. 在複製本檢視中，指定對該伺服器的讀寫許可權。 附註：確定已在驅動程式集中新增了次要伺服器。

對 Identity Applications 和 RBPM 安裝進行疑難排解

下表列出了您可能會遇到的問題，以及為解決這些問題建議執行的動作。如果問題持續發生，請聯絡您的 NetIQ 代表。

問題	建議執行的動作
「儀表板」頁面上的角色和自己的任務工具集不顯示任何資料。如果您簽入瀏覽器的主控台，將會顯示 404 錯誤。將預設 IDMPProv 部署網路位置變更為自訂網路位置後會出現此問題。	若要解決此問題，必須變更受影響工具集上的 REST API URL。請執行以下步驟： 1. 以管理員身分登入 Identity Manager 儀表板。 2. 導覽至「儀表板」頁面，然後按一下「管理儀表板」。 3. 若要編輯角色工具集中的工具集組態，請執行以下操作： a. 按一下 . b. 在 URL 欄位中，如下所示將預設 IDMPProv 網路位置變更為自訂網路位置：<code>/<custom-context>/rest/access/assignments/advanced?nextIndex=1&sortBy=name&sortOrder=ASC&forceRefresh=true&searchScope=role&size=20</code> 其中，<custom-context> 是您在 Identity Manager 部署中使用的網路位置。 c. 按一下套用。 4. 若要編輯自己的任務工具集中的工具集組態，請執行以下操作： a. 按一下 . b. 在 URL 欄位中，如下所示將預設 IDMPProv 網路位置變更為自訂網路位置：<code>/<custom-context>/rest/access/tasks/list?fromIndex=1&size=10&q=*&sortOrder=asc&sortBy=createTime&assignedTo=assignedTo&recipient=recipientAsMe&expireUnit=weeks&expireWithin=&proxyUser=&assignStatus=&delegatedTasks=false&status=</code> c. 按一下套用。 5. 按一下完成編輯。

問題	建議執行的動作
升級叢集中安裝的 Identity Applications 並重新啟動 Tomcat 後，叢集未依預期運作。	在叢集的所有節點上執行以下動作： 1. 導覽至 C:\NetIQ\IDM\apps\tomcat\conf 資料夾中的 server.xml 檔案。 2. 在 server.xml 中取消備註下面一行。 <pre><Cluster className="org.apache.catalina.ha. tcp.SimpleTcpCluster"/></pre> 3. 從 Tomcat 備份目錄還原所有自訂組態。 4. 重新啟動 Tomcat。
升級程序不會將預設的 Identity Applications 管理帳戶設定為 cn=uaadmin.ou=sa.o=data。catalina.out 檔案中記錄了以下錯誤。 <pre>AuthorizationManagerService [RBPM] Error occured calculating effective rights for attribute: nrfAccessMgrRevokeRole on object: cn=complianceAdmin,cn=System,cn=Level20, cn=RoleDefs,cn=RoleConfig,cn=AppConfig,c n=UserApplication,cn=Driver Set,o=system for trustee: cn=uaadmin,ou=sa,o=data.com.novell.srvpr v.spi.security.IDMAuthorizationException : Error occured calculating effective rights for attribute: nrfAccessMgrRevokeRole on object: cn=complianceAdmin,cn=System,cn=Level20, cn=RoleDefs,cn=RoleConfig,cn=AppConfig,c n=UserApplication,cn=Driver Set,o=system for trustee: cn=uaadmin,ou=sa,o=data.at com.novell.idm.security.authorization.ld ap.LdapRightsUtil.getPropertyRights(Ldap RightsUtil.java:152) Unable to fetch roles from edirectory in the predefined time set.</pre>	1. 導覽至 setenv.bat 檔案，然後在 CATALINA_OPTS 項目中將 -Dnrcpclient_req_timeout 內容的值變更為 1150。 2. 重新啟動 Tomcat。
您需要修改安裝過程中建立的以下一或多個 Identity Applications 組態設定： ◆ Identity Vault 連接和證書 ◆ 電子郵件設定 ◆ Identity Manager 引擎使用者身分和使用使用者群組 ◆ Access Manager 或 iChain 設定	不依賴安裝程式來執行組態公用程式。 從安裝目錄 (預設為 C:\NetIQ\idm\apps\UserApplication\) 執行以下指令： <pre>configupdate.bat</pre>

問題	建議執行的動作
啟動 Tomcat 會導致以下例外： <pre>port 8180 already in use</pre>	關閉任何可能已在執行的 Tomcat 例項 (或其他伺服器軟體) 。如果將 Tomcat 重新設定為使用 8180 以外的連接埠，請編輯使用者應用程式驅動程式的 config 設定。
當 Tomcat 啟動時，應用程式報告找不到可信證書。	請務必使用安裝 Identity Applications 期間指定的 JDK 來啟動 Tomcat 。
無法登入入口網站管理頁面。	確定存在 Identity Applications 管理員帳戶。此帳戶與 Identity Console 管理員帳戶不同。
即使使用管理員帳戶也無法建立新使用者。	Identity Applications 管理員必須是頂層容器的託管者，並且應該具有「監督者」權限。您可以嘗試將 Identity Applications 管理員的權限設定為與 LDAP 管理員的權限相同 (使用 Identity Console) 。
啟動應用程式伺服器時拋出金鑰儲存區錯誤。	應用程式伺服器未使用安裝 Identity Applications 期間指定的 JDK 。 使用 keytool 指令，來輸入證書檔案： <pre>keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit</pre> ♦ 以您為此證書選擇的唯一名稱來取代 <i>aliasName</i> 。 ♦ 以證書檔案的完整路徑和名稱來取代 <i>certFile</i> 。 ♦ 預設金鑰儲存區密碼為 changeit (如果您有不同的密碼，請指定它) 。
電子郵件通知無法傳送。	執行 configupdate 公用程式檢查您是否提供了以下 Identity Applications 組態參數的值：Email From 和 Email Host 。 從安裝目錄 (預設為 C:\NetIQ\idm\apps\UserApplication\) 執行以下指令： <pre>configupdate.bat</pre>

安裝和解除安裝疑難排解

下表列出了您可能會遇到的問題，以及為解決這些問題建議執行的動作。如果問題持續發生，請聯絡您的 NetIQ 代表。

問題	建議執行的動作
Identity Manager 使用數位證書進行授權並與其元件安全通訊。必須將 Identity Vault 證書輸入 idm.jks 和 tomcat.keystore 金鑰儲存區檔案。但是，輸入證書後嘗試存取 Identity Applications 時，您可能會遇到以下錯誤： <pre>javax.net.ssl.SSLHandshakeException: PKIX path validation failed: java.security.cert.CertPathValidatorException: Could not determine revocation status.</pre> 透過檢查 CRL 發佈點 (CDP) 欄位指定的證書撤銷清單 (CRL) 來驗證證書，以確定證書是否已撤銷。根證書以及金鑰儲存區檔案 tomcat.keystore 和 idm.jks 中的中繼證書都會提供 CRLDP。但是，預設已停用證書撤銷檢查。因此，PKIX 信任管理員無法確定證書的撤銷狀態。 升級 Identity Manager 後，非管理員使用者在 Identity Manager 儀表板中的登入速度非常緩慢。載入「應用程式」和「儀表板」頁面時出現很高的延遲。 此問題是由預設已啟用的巢狀群組搜尋所導致。無論環境中是否存在任何巢狀群組，應用程式都會透過巢狀群組成員資格尋找已登入使用者繼承的許可權。	若要解決此問題，請將 - Dcom.sun.security.enableCRLDP 內容設定為 true 以啟用 CRL 發佈點檢查。 若要設定該內容，請執行以下動作： 1. 停止 Tomcat。 2. 移至位於 Tomcat 的 bin 資料夾中的 setenv.sh 檔案。例如 C:\NetIQ\idm\apps\tomcat\bin\setenv.bat。 3. 如下所示在 CATALINA_OPTS 中新增內容 - Dcom.sun.security.enableCRLDP=true： export CATALINA_OPTS="- Dcom.sun.security.enableCRLDP=true" 4. 啟動 Tomcat。 (視情況而定) 以下步驟適用於 Identity Manager 4.8.5 和更新版本。 1. 登入其中 Identity Applications 已升級至版本 4.8.5 的伺服器。 2. 導覽至 C:\NetIQ\IDM\apps\tomcat\conf 位置。 3. 在文字編輯器中開啟 ism-configuration.properties 檔案。 4. 在該檔案的末尾新增以下內容： DirectoryService/realms/jndi/params/USE_NESTED_GROUPS=false 5. 儲存該檔案並重新啟動 Tomcat。

問題	建議執行的動作
將 Identity Applications 升級至版本 4.8.x 後，您無法登入 Identity Applications 儀表板。如果在 Identity Applications 升級期間未將 Identity Vault 可信證書儲存區路徑更新為正確的金鑰儲存區 (cacerts) 檔案位置，則會出現此問題。catalina.out 檔案中記錄了以下例外： <pre>com.netiq.idm.auth.oauth.AuthenticationCommunicationException: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path validation failed: sun.security.validator.ValidatorException: TrustAnchor with subject "CN=***, OU=idm, O=***, L=***, ST=***, C=***" is not a CA certificate"</pre> Identity Applications 使用設定為 < 安裝路徑 >\Common\JRE 的 JAVA_HOME 環境變數。如果未在 JAVA_HOME 中將可信證書儲存區路徑設定為 cacerts 檔案所在位置，則 SSL 通訊會失敗，導致出現與「TrustAnchor」相關的 SSL 錯誤 (信賴起點用做 SSL 證書的增強式 Java 安全性檢查措施)。 將分散式環境中的 Identity Manager 升級至版本 4.8.1 後，登入 Identity Applications 失敗。將會顯示以下錯誤訊息： 您的登入程序未成功完成。 登入 Identity Applications 需要提供信賴起點證書，以便在 Identity Applications 與 OSP 之間建立安全連接。信賴起點證書必須包含「標題類型」設定為「CA」的「基本限制」延伸。Identity Manager 利用 jdk.security.allowNonCaAnchor 內容來驗證證書中的信賴起點。此內容預設為 false。因此，如果在證書中找不到信賴起點，則無法在 Identity Applications 與 OSP 之間建立連接，登入也會失敗。您還會在 idm-osp.log 檔案中看到以下例外： <pre>sun.security.validator.ValidatorException: TrustAnchor with subject "CN=***, L=***, O=***" is not a CA certificate</pre>	若要解決此問題，請執行以下動作： 1. 停止 Tomcat 服務。 2. 登入 Identity Applications 伺服器，並啟動位於 < 安裝路徑 >\idm\apps\configupdate 中的 configupdate 公用程式。 3. 在「使用者應用程式」索引標籤中，移至 Identity Vault 證書，並確定可信證書儲存區路徑設定為 < 安裝路徑 >\Common\JRE\lib\security\cacerts。 4. 啟動 Tomcat 服務。 若要解決此問題，必須符合下列任一條件： ◆ 確定用於在 Identity Applications 與 OSP 之間建立安全連接的證書是包含正確「基本限制」延伸的可信 CA 證書。 ◆ 如果使用的是用戶端信任的自行簽署的證書和自訂證書，您可以變更 jdk.security.allowNonCaAnchor 內容，以允許使用不包含「基本限制」延伸的非 CA 證書。請執行以下動作來修改 Java 安全性設定： 1. 導覽至 C:\NetIQ\idm\apps\jre\lib\security\java.security 目錄。 2. 設定內容值 jdk.security.allowNonCaAnchor=true。 3. 儲存檔案。

問題	建議執行的動作
升級至 Identity Applications 4.8.1 版本後，在 Identity Applications 儀表板中申請許可權時無法開啟表單。	若要解決此問題，請執行以下步驟： 1. 在鍵盤上按 Windows + R，輸入 <code>services.msc</code>，然後選取確定以開啟 Windows 的「服務」介面。 2. 搜尋服務名稱 NetIQ Nginx Service 和 NetIQ IGA Form Renderer Service。在相應服務上按一下滑鼠右鍵並選取重新啟動選項。 Identity Applications 使用 NGNIX 服務在 Identity Applications 儀表板中轉譯表單。
將 Identity Applications 或 Identity Reporting 升級至版本 4.8 後，控制台中會顯示多個 PostgreSQL 項目。	在控制台中解除安裝以前的 PostgreSQL 版本。
解除安裝程序報告未完成，但記錄檔案未顯示失敗資訊。	依預設，解除安裝程序無法刪除包含安裝檔案的 <code>netiq</code> 目錄。如果您已從電腦中移除所有 NetIQ 軟體，則可以自己來刪除該目錄。
當您升級 Identity Manager 後，系統會將以下內容新增至 <code>ism-configuration.properties</code> 檔案： <pre>com.netiq.idm.osp.ldap.admin-dn = cn=admin,ou=sa,o=system</pre>	請在 <code>ism-configuration.properties</code> 檔案中將該內容設為備註，然後重新啟動 Tomcat。它不會導致功能受損。
升級 Identity Manager 後，即使您的部署中不包含 SSPR，系統也會將以下 SSPR 內容新增至 <code>ism-configuration.properties</code> 檔案： <pre>com.netiq.sspr.redirect.url = https:// __SSPR_IP__:__SSPR_TOMCAT_HTTPS_PORT__ /sspr/public/oauth</pre>	請在 <code>ism-configuration.properties</code> 檔案中將該內容設為備註，然後重新啟動 Tomcat。它不會導致功能受損。

問題	建議執行的動作
升級 Identity Manager 之後，無法啟動 Tomcat。在 Tomcat 記錄中，您會發現幾項例外以及工作流程引擎與 Identity Vault 之間的通訊失敗事件。	1. 登入 Identity Console。 2. 導覽至證書管理 > 伺服器證書管理。 3. 選取 SSL 證書 DNS 核取方塊並按一下輸出。 4. 在證書下拉式清單中，選取 SSL CertificateDNS。 5. 清除輸出私密金鑰核取方塊。確定輸出格式設定為 DER。 6. 按一下確定 > 儲存輸出的證書以將證書下載到您的系統中。 7. 登入 Identity Applications 伺服器。 8. 停止 Tomcat。 9. 導覽至 <code>opt/netiq/common/jre/bin</code> 目錄，並使用以下指令將證書輸入至 <code>idm.jks</code> 檔案： <pre>opt/netiq/common/jre/bin/keytool -import -trustcacerts -alias <certificate_alias_name> - keystore /opt/netiq/idm/apps/ tomcat/conf/idm.jks -file <certificate_file_downloaded></pre> 10. 重新啟動 Tomcat。
將 Identity Manager 從 4.7.4 升級至 4.8 後，Tomcat 服務不會啟動，並且記錄檔案中未報告任何錯誤。如果未在 <code>igaworkflow</code> 資料庫的 <code>afenginestate</code> 表中正確更新活動訊號計時器，便會出現此問題。	若要解決此問題，請登入 <code>pgAdmin</code> 等資料庫管理工具。執行以下查詢，以手動更新 <code>igaworkflow</code> 資料庫的 <code>afenginestate</code> 表中的活動訊號計時器。 <pre>update afenginestate set heartbeat=now()::timestamp;</pre>

登入疑難排解

下表列出了您可能會遇到的問題，以及為解決這些問題建議執行的動作。如果問題持續發生，請聯絡您的 NetIQ 代表。

問題	建議執行的動作
如果 Identity Applications 和 Identity Reporting 安裝於同一部伺服器上，而您使用 <reporting install folder>\bin 目錄中的組態更新公用程式來變更組態，Identity Manager 儀表板將無法啟動。catalina.out 記錄檔案中會報告以下錯誤： <pre>EboPortalBootServlet [RBPM] +++++WARNING!!!! : This portal application context, IDMProv, does not match the portal.context property set in the PortalService-conf/config.xml file.Only one portal per database is allowed.Data has been loaded using the previous portal context.To correct this you must revert back to the previous portal name of, NoCacheFilter, please consult the documentation.</pre> 在大型環境 (超過兩百萬個物件) 中，使用者無法登入 當您從 Identity Applications 頁面登出時，SSPR 顯示錯誤 5053 ERROR_APP_UNAVAILABLE。 在第一次登入 Identity Applications 時不提示處理安全回應。	若要進行任何組態變更，請使用 C:\NetIQ\idm\apps\UserApplication 目錄中的組態更新公用程式。 在 eDirectory 主要伺服器和複本伺服器中為 mail(Internet Mail Address) 屬性新增索引，並將規則集設定為 Value。 忽略此錯誤，它不會導致功能受損。 1. 確定 SSPR 服務器具有使用 FQDN 建立的證書。 2. 登入 Identity Application 伺服器並啟動 ConfigUpdate 公用程式 (< 安裝路徑 >\apps\UserApplication)。 3. 導覽至 SSO 用戶端 > Self Service Password Reset，確定設定正確無誤。 如果將 SSPR 安裝在單獨的伺服器上，請確定已將 SSPR 證書輸入至 Identity Applications 伺服器上 / netiq/idm/apps/tomcat/conf 中的 idm.jks。

問題	建議執行的動作
存取 SSPR URL 時瀏覽器顯示空白頁面。	未使用 OSP 正確設定 SSPR 時，會出現這種情況。SSPR 記錄會顯示以下資訊： <pre>2018-01-24T22:24:02Z, ERROR, oauth.OAuthConsumerServlet, 5071 ERROR_OAUTH_ERROR (unexpected error communicating with oauth server: password.pwm.error.PwmUnrecoverableException: 5071 ERROR_OAUTH_ERROR (io error during oauth code resolver http request to oauth server: Certificate for <IP> doesn't match any of the subject alternative names: [IP]))</pre> 1. 驗證執行 OSP 的 Tomcat 伺服器是否具有使用 FQDN 建立的有效證書。登入 Identity Applications 伺服器，並啟動 ConfigUpdate 公用程式。導覽至 SSO 用戶端 > Self Service Password Reset，並確定設定正確。 2. 透過覆寫 OSP 登入方法登入 SSPR(例如，<code>https://<sspr sserver ip>:<port>/sspr/private/Login?sso=false</code>)。 3. 導覽至頁面右上角的組態編輯器。 4. 指定設定密碼，然後按一下登入。 5. 導覽至 LDAP > LDAP 目錄 > 預設 > 連接。 6. 如果 LDAP 證書不正確，請按一下清除。 7. 若要重新輸入證書，請按一下從伺服器輸入。 8. 導覽至設定 > 單一登入 (SSO) 用戶端 > OAuth，並在 OAuth Web 服務伺服器證書 下驗證證書是否正確。 9. 如果證書不正確，請按一下清除。 10. 若要重新輸入證書，請按一下從伺服器輸入。

SSPR 頁面申請錯誤疑難排解

下表列出了您可能會遇到的問題，以及為解決這些問題建議執行的動作。如果問題持續發生，請聯絡您的 NetIQ 代表。

問題	建議執行的動作
SSPR 報告頁面申請無序錯誤 如果在 SSPR 頁面中按上一步按鈕，則會出現此問題。SSPR 在 SSPR 錯誤記錄中顯示如下所示的錯誤順序訊息： ERROR, password.pwm.servlet.TopServlet, 5035 ERROR_INCORRECT_REQUEST_SEQUENCE (expectedPageID=3, submittedPageID=4, url=<some sspr url>	透過 SSPR 組態管理器 > 設定 > 安全性 > Web 安全性 停用「上一步」按鈕。 附註： 變更此設定不會影響到最終使用者。

如需驗證到或登入 Identity Applications 期間遇到的一般問題，請參閱《[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)》(NetIQ Identity Manager - Identity Applications 管理員指南)。

對在 Windows 2016 上無法啟動 .NET 遠端載入器的問題進行疑難排解

下表列出了您可能會遇到的問題，以及為解決這些問題建議執行的動作。如果問題持續發生，請聯絡您的 NetIQ 代表。

問題	建議執行的動作
此問題隨機出現。如果 .NET 遠端載入器的指令提示符的前端設定與主機作業系統的預設設定不同，便可能發生此問題。	透過刪除 HKEY_CURRENT_USER\Console 登錄機碼將指令提示符設定變更為與系統預設設定相符，然後重新啟動伺服器。

在 Azure 部署中載入表單時出現「502 錯誤的閘道」疑難排解

下表列出了您可能會遇到的問題，以及為解決這些問題建議執行的動作。如果問題持續發生，請聯絡您的 NetIQ 代表。

問題	建議執行的動作
在 Azure 環境中部署 IDM 4.8 元件之後。在 IDM 儀表板中，當您按一下服務台票證或嘗試核准任何任務時，您可能會看到以下錯誤。 502 - Web server received an invalid response while acting as a gateway or proxy server.	請執行以下步驟來解決此問題： 1. 導覽至系統中的 Nginx\conf 位置。 例如 C:\NetIQ\Common\Nginx\conf 2. 在 nginx.conf 檔案中： a. 在 error_page 502 /502.html; 一行下面新增 error_page 404 =200 / 404.html。 b. 將 proxy_intercept_errors off; 設定為 proxy_intercept_errors on;。 3. 在 Services.msc 中重新啟動 NetIQ Nginx Service。