NetIQ® Identity Manager

安裝和升級指南 - Linux

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 13

I Identity Manager 環境綜覽 15

1 Identity Manager 元件簡介 17

Identity Manager 伺服器元件 . . . 18
Identity Manager 伺服器 . . . 19
遠端載入器 . . . 19
擴送代理程式 . . . 20
Identity Console . . . 20
Identity Applications 元件 . . . 20
使用者應用程式 . . . 21
驗證服務 . . . 21
Self-Service Password Reset . . . 21
Web 應用程式伺服器 . . . 21
Identity Applications 資料庫 . . . 22
Identity Applications 的驅動程式 . . . 22
Identity Reporting 元件 . . . 22
Identity Reporting . . . 23
驗證服務 . . . 23
Self-Service Password Reset . . . 23
Identity Reporting 資料庫 . . . 23
Web 應用程式伺服器 . . . 24
Identity Reporting 的驅動程式 . . . 24
Sentinel Log Management for Identity Governance and Administration . . . 25
Identity Manager 工具 . . . 25
Designer for Identity Manager . . . 25
Analyzer for Identity Manager . . . 25
功能架構 . . . 26
Identity Manager 的部署選項 . . . 27
範例 Identity Manager 部署 . . . 28
範例進階版部署 . . . 29
範例標準版部署 . . . 31

II 規劃 Identity Manager 安裝 33

2 規劃安裝 35

執行核對清單 . . . 35
建議的安裝情境和伺服器設定 . . . 36
確定何時安裝 SLM for IGA . . . 37
在分散式環境中安裝的注意事項 . . . 37
確定硬體要求 . . . 39
系統要求工作表 . . . 39
在 SLES 伺服器上安裝 Identity Manager . . . 39

在 RHEL 伺服器上安裝 Identity Manager 41
先決條件 41
確認伺服器上已安裝相依程式庫 42
在 RHEL 9.x 上建立用於安裝媒體的儲存庫 42
在 RHEL 8.x 上建立用於安裝媒體的儲存庫 44
執行先決條件檢查 45

3 安裝 Identity Manager 元件的注意事項 47

安裝順序 47
瞭解安裝和組態程序 47
安裝 Identity Manager 引擎元件和遠端載入器的注意事項 49
安裝 Identity Applications 元件的注意事項 50
安裝考量 50
資料庫考量 51
設定 Identity Applications 的資料庫 52
安裝 Identity Reporting 元件的注意事項 54
Identity Reporting 的先決條件 54
Identity Reporting 的身分稽核事件 55
安裝 Designer 的注意事項 55
安裝 Analyzer 的注意事項 56
安裝 SLM for IGA 的注意事項 56
查看 Identity Manager 元件使用的連接埠 57

III 安裝和設定 Identity Manager 元件 59

4 安裝 Identity Manager 61

執行互動式安裝 61
以靜默模式安裝 61
以非 root 使用者身分安裝 Identity Manager 引擎 62
安裝 NICI 62
以非 root 使用者身分安裝 Identity Vault 63
以非 root 使用者身分安裝引擎 65
安裝 SSPR 65
以互動模式安裝 SSPR 66
以靜默模式安裝 SSPR 66
安裝遠端載入器 66
互動安裝 66
靜默安裝 67
安裝 Designer 67
安裝 Analyzer 67
使用精靈安裝 Analyzer 68
以靜默模式安裝 Analyzer 68
將 XULRunner 新增至 Analyzer.ini 中 69
安裝 Sentinel Log Management for Identity Governance and Administration 69
以 Root 使用者身分安裝 Sentinel Log Management 69
以非 Root 使用者身分安裝 Sentinel Log Management 70
安裝 Java 遠端載入器 71
瞭解目錄結構 72

5 設定 Identity Manager 的元件 75

在組態期間使用不可猜出的密碼 . . . 75
瞭解組態參數 . . . 75
建立和設定驅動程式集 . . . 83
設定 Identity Manager 的元件 . . . 85
執行互動式組態 . . . 85
執行靜默組態 . . . 85
設定 SSPR . . . 86
執行互動式組態 . . . 86
執行靜默組態 . . . 86
在 OSP 伺服器上修改單一登入存取設定 . . . 86

6 完成安裝的最後步驟 89

設定 Identity Vault 的組態 . . . 89
建立 Identity Vault 的值索引 . . . 89
手動將 Identity Applications 和 Identity Reporting 證書輸入至 Identity Vault 中 . . . 90
將非管理員使用者設定為 Identity Vault 管理員 . . . 90
設定遠端載入器和驅動程式 . . . 90
設定已連接系統 . . . 91
建立和設定驅動程式集 . . . 91
建立驅動程式 . . . 93
定義規則 . . . 94
設定忘記密碼管理功能 . . . 94
使用 Self Service Password Reset 進行忘記密碼管理 . . . 94
使用外部系統進行忘記密碼管理 . . . 96
針對分散式環境或叢集環境更新儀表板中的 SSPR 連結 . . . 98
設定 Identity Applications . . . 98
儲存 Configupdate 公用程式密碼 . . . 99
完成 Identity Applications 的設定 . . . 99
指定許可權索引的位置 . . . 123
部署適用於 Identity Applications 的 REST API . . . 124
設定 Identity Applications 的 Oracle 資料庫 . . . 124
使用 Oracle 服務名稱存取 Oracle 資料庫 . . . 125
手動建立資料庫綱要 . . . 126
組態 Identity Applications 的單一登入設定 . . . 127
啟動 Identity Applications . . . 127
Identity Applications 的組態和使用考量 . . . 128
設定資料收集的執行時期環境 . . . 128
將資料收集服務驅動程式設定為從 Identity Applications 收集資料 . . . 129
移轉資料收集服務驅動程式 . . . 130
新增對自訂屬性和物件的支援 . . . 132
新增多個驅動程式集支援 . . . 134
將驅動程式設定為使用 SSL 在遠端模式下執行 . . . 136
設定 Identity Reporting . . . 137
設定受管理系統閘道驅動程式 . . . 137
在「身分資料收集服務」頁面中手動新增資料來源 . . . 138
對 Oracle 資料庫執行報告 . . . 138
手動產生資料庫綱要 . . . 138
部署 Identity Reporting 的 REST API . . . 143
連接遠端 Remote PostgreSQL 資料庫 . . . 143
在 OSP 中為採用分散式設定的 Identity Reporting 註冊用戶端 . . . 144
Identity Reporting 的安裝後步驟 . . . 144

完成非 Root 使用者安裝 144
為密碼規則建立容器 145
新增電子郵件通知中的圖形支援 145
啟用 Identity Manager 145
為分散式部署建立 SSL 證書 146

IV 在 FIPS 模式下設定 Identity Manager 149

7 為 FIPS 設定 JRE 151

8 在 FIPS 模式下設定 Identity Manager 引擎 153

程序 153

9 在 FIPS 模式下設定擴送代理程式 155

程序 155

10 在 FIPS 模式下設定 Identity Applications 和 Identity Reporting 157

程序 157

11 在 FIPS 模式下設定遠端載入器 161

V 將 Identity Manager 資料移轉至新安裝中 163

12 移轉 Identity Manager 的準備工作 165

用於執行移轉的核對清單 165

13 將 Identity Manager 移轉至新伺服器 167

先決條件 167
準備用於移轉的 Designer 專案 167
將 Identity Manager 引擎移轉至新伺服器 168
複製驅動程式集的伺服器特定資訊 168
在 Designer 中複製伺服器特定資訊 169
在 Identity Console 中變更伺服器特定的資訊 169
變更使用者應用程式的伺服器特定資訊 170
移轉 Identity Applications 170
將資料庫移轉至新伺服器 170
在新伺服器上安裝 Identity Applications 172
移轉 Identity Reporting 173
更新 Identity Reporting 的驅動程式 173
部署 Identity Reporting 的驅動程式 173
將現有資料移轉至新資料庫 173
設定新 Reporting 伺服器 177
建立資料同步規則 177

VI 升級 Identity Manager **179**

14 升級 Identity Manager 的準備工作 **181**

Identity Manager 的升級核對清單 . . . 181
瞭解升級程序 . . . 182
支援的升級路徑 . . . 183
從 Identity Manager 4.7.5 版本升級 . . . 183
從 Identity Manager 4.8.x 版本升級 . . . 185
備份目前組態 . . . 186
輸出 Designer 專案 . . . 186
輸出驅動程式組態 . . . 187

15 升級 Identity Manager 的元件 **189**

升級順序 . . . 189
升級注意事項 . . . 190
升級 Designer . . . 191
升級 Identity Manager 引擎 . . . 192
安裝前驗證 Linux RPM . . . 192
升級 Identity Vault . . . 192
升級 Identity Manager 引擎 . . . 193
以非 Root 使用者身分升級 Identity Manager 引擎 . . . 195
升級遠端載入器 . . . 195
升級 Java 遠端載入器 . . . 196
停止和啟動 Identity Manager 驅動程式 . . . 196
停止驅動程式 . . . 197
啟動驅動程式 . . . 197
升級 Identity Manager 驅動程式 . . . 199
建立新驅動程式 . . . 199
以套件中的內容取代現有內容 . . . 199
保留目前內容並透過套件新增新內容 . . . 200
升級 Identity Applications . . . 200
升級注意事項 . . . 201
系統要求 . . . 203
瞭解升級程式 . . . 203
升級 PostgreSQL . . . 203
升級 Identity Applications 元件 . . . 203
Identity Applications 元件的升級後任務 . . . 206
升級後驗證版本號碼 . . . 209
升級 Identity Reporting . . . 209
升級注意事項 . . . 210
升級 Sentinel Log Management for IGA . . . 210
升級 Identity Reporting . . . 210
Reporting 的升級後步驟 . . . 211
驗證 Identity Reporting 的升級 . . . 212
升級 Analyzer . . . 213
升級後任務 . . . 213
升級服務驅動程式 . . . 213
移除未使用的 Log4j JAR . . . 214
將新伺服器新增至驅動程式集 . . . 214
從驅動程式集移除舊的伺服器 . . . 214
將自訂規則還原至驅動程式 . . . 215

使用 Designer 將自訂規則還原至驅動程式 216
使用 Identity Console 將自訂規則和規則還原至驅動程式 216

16 從進階版切換到標準版 217

VII 部署 Identity Manager 容器 219

17 規劃容器部署 221

系統要求 221
獲取 Docker 影像 221

18 Identity Manager 容器部署 223

最佳實務 223
管理容器磁碟區資料 224
建立靜默內容檔案 224
部署遠端載入器容器後自動啟動遠端載入器例項 226
容器部署模式 227
在單部伺服器上部署容器 227
先決條件 227
部署 Identity Manager 引擎容器 228
部署遠端載入器容器 228
部署擴送代理程式容器 229
透過 Identity Vault 證書管理中心產生證書 229
部署 OSP 容器 231
部署 PostgreSQL 容器 232
部署 Identity Applications 容器 233
部署表單轉譯器容器 234
部署 ActiveMQ 容器 234
部署 Identity Reporting 容器 235
部署 SSPR 容器 236
部署 Identity Console 容器 237
在分散式伺服器上部署容器 237
設定覆蓋網路 237
先決條件 238
公開容器存取的連接埠 239
部署 Identity Manager 引擎容器 240
部署遠端載入器容器 241
部署擴送代理程式容器 241
透過 Identity Vault 證書管理中心產生證書 242
部署 OSP 容器 246
部署 PostgreSQL 容器 246
部署 Identity Applications 容器 247
部署表單轉譯器容器 248
部署 ActiveMQ 容器 249
部署 Identity Reporting 容器 249
部署 SSPR 容器 250
部署 Identity Console 容器 251

19 升級 Identity Manager 容器 253

容器更新先決條件 253

更新分散式伺服器上的容器 . . . 253
更新 Identity Manager 引擎容器 . . . 254
更新遠端載入器容器 . . . 254
更新擴送代理程式容器 . . . 255
更新 OSP 容器 . . . 255
更新 PostgreSQL 容器 . . . 256
更新 Identity Applications 容器 . . . 257
更新表單轉譯器容器 . . . 257
更新 ActiveMQ 容器 . . . 257
更新 Identity Reporting 容器 . . . 258
更新 SSPR 容器 . . . 258
更新 Identity Console 容器 . . . 258
更新單部伺服器上的容器 . . . 259
更新 Identity Manager 引擎容器 . . . 259
更新遠端載入器容器 . . . 259
更新擴送代理程式容器 . . . 260
更新 OSP 容器 . . . 260
更新 PostgreSQL 容器 . . . 261
更新 Identity Applications 容器 . . . 262
更新表單轉譯器容器 . . . 262
更新 ActiveMQ 容器 . . . 262
更新 Identity Reporting 容器 . . . 263
更新 SSPR 容器 . . . 263
更新 Identity Console 容器 . . . 263

VIII 使用 Ansible 部署 Identity Manager 容器 265

20 規劃部署 267

準備 Ansible 節點 . . . 267
準備控制節點 . . . 268
準備受管理節點 . . . 269
建立 setup.csv 檔案 . . . 270

21 部署容器 273

22 部署後任務 275

IX 在 Microsoft Azure Kubernetes Service 上部署 Identity Manager 容器 277

綜覽 . . . 278

23 規劃部署 279

24 準備部署 283

25 部署程序 285

Azure 雲端的基礎架構部署 . . . 285
使用 Configuration Generator 進行部署 . . . 285
使用組態樣板進行部署 . . . 289
Azure Kubernetes Service 上的 Identity Manager 容器部署 . . . 299

在 Azure Kubernetes Service 上設定遠端載入器服務 300
在 Azure Kubernetes Service 上設定擴送代理程式服務 302

26 部署後任務 305

存取 Identity Manager 應用程式 305
在 Azure 虛擬機器上部署 Designer 305
在 Azure 虛擬機器上部署 SLM for IGA 305
處理 AKS 的 RPM 更新和協力廠商檔案 306

27 維護 Identity Manager 容器的部署 307

管理資料永續性層 307
重新啟動 Pod 308
存取 Pod 309
重新啟動 Azure Kubernetes 叢集 309
縮放 Identity Manager 引擎複製本 310
縮減 Identity Manager 引擎複製本的使用案例 311
擴增 Identity Manager 引擎複本 311
縮放 OSP 和 Identity Applications 複本 312
銷毀使用 Terraform 建立的整個資源 312

X 在 AWS EC2 上部署 Identity Manager 313

28 在 AWS EC2 上規劃和實作 Identity Manager 315

先決條件 315
部署程序 315
準備 AWS Virtual Private Cloud 317
建立和部署例項 319
準備 EC2 例項 320
安裝 Identity Manager 元件 322
安裝 Identity Applications 和 Identity Reporting 的資料庫 322
安裝 Designer 324
建立 AWS EC2 負載平衡器 324
(選擇性) 使用註冊的代管區域建立別名 DNS 329
存取 Identity Manager 元件 330
安全性考量 330

29 範例混合式 Identity Manager 方案 333

使用遠端載入器連接 333
使用多伺服器驅動程式集連接 334
使用 eDirectory 驅動程式連接 335

XI 部署 Identity Manager 以實現高可用性 337

30 在叢集環境中安裝 Identity Manager 的準備工作 339

先決條件 339
Identity Vault 339

Identity Applications 340
Identity Applications 的資料庫 340
為 Identity Applications 準備叢集 341
瞭解 Tomcat 環境中的叢集群組 341
設定工作流程引擎 ID 的系統內容 341

31 Identity Manager 叢集部署解決方案範例 343

先決條件 343
安裝程序 344
設定 iSCSI 伺服器 344
在所有節點上設定 iSCSI 啟動器 345
分割共享儲存 345
安裝 HA Extension 346
設定 Softdog 監視程式 346
設定 HA 叢集 346
在叢集節點上安裝並設定 Identity Vault 和 Identity Manager 引擎 348
設定 Identity Vault 資源 349
eDirectory 和共享儲存子資源的原始值 349
變更位置條件約束分數 350

32 Tomcat 應用程式伺服器上的 Identity Applications 叢集部署解決方案範例 353

先決條件 354
準備叢集 355
瞭解 Tomcat 環境中的叢集群組 355
設定工作流程引擎 ID 的系統內容 355
安裝程序 355
為叢集啟用許可權索引 360
為叢集設定使用者應用程式驅動程式 360
為叢集設定 OSP 和 SSPR 361
設定 SSPR 以支援叢集 361
在叢集節點上設定任務 361

33 解除安裝 Identity Manager 的元件 363

從 Identity Vault 中移除物件 363
解除安裝 Identity Manager 引擎 363
解除安裝 Identity Applications 364
解除安裝 Identity Reporting 元件 364
刪除報告驅動程式 365
解除安裝 Identity Reporting 365
解除安裝 Sentinel Log Management for IGA 365
解除安裝 Designer 365
解除安裝 Analyzer 366

34 疑難排解 367

尋找記錄檔案 367
登入相關問題疑難排解 367
安裝和解除安裝相關問題疑難排解 370
升級相關問題疑難排解 373
Ansible 部署相關問題疑難排解 377

AKS 部署相關問題疑難排解 380
Identity Manager 引擎疑難排解 386
Identity Applications 和 Identity Reporting 疑難排解 388
其他問題疑難排解 392

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分管理員，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*

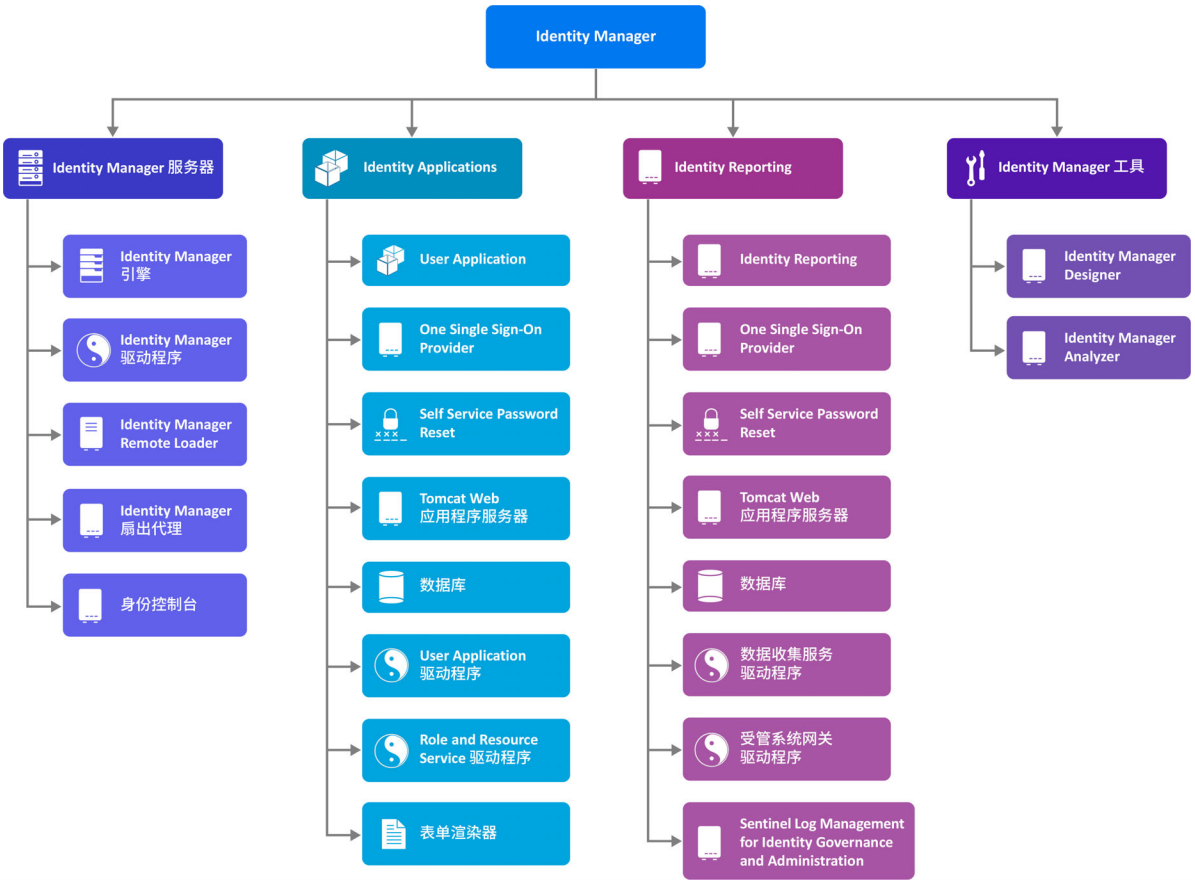
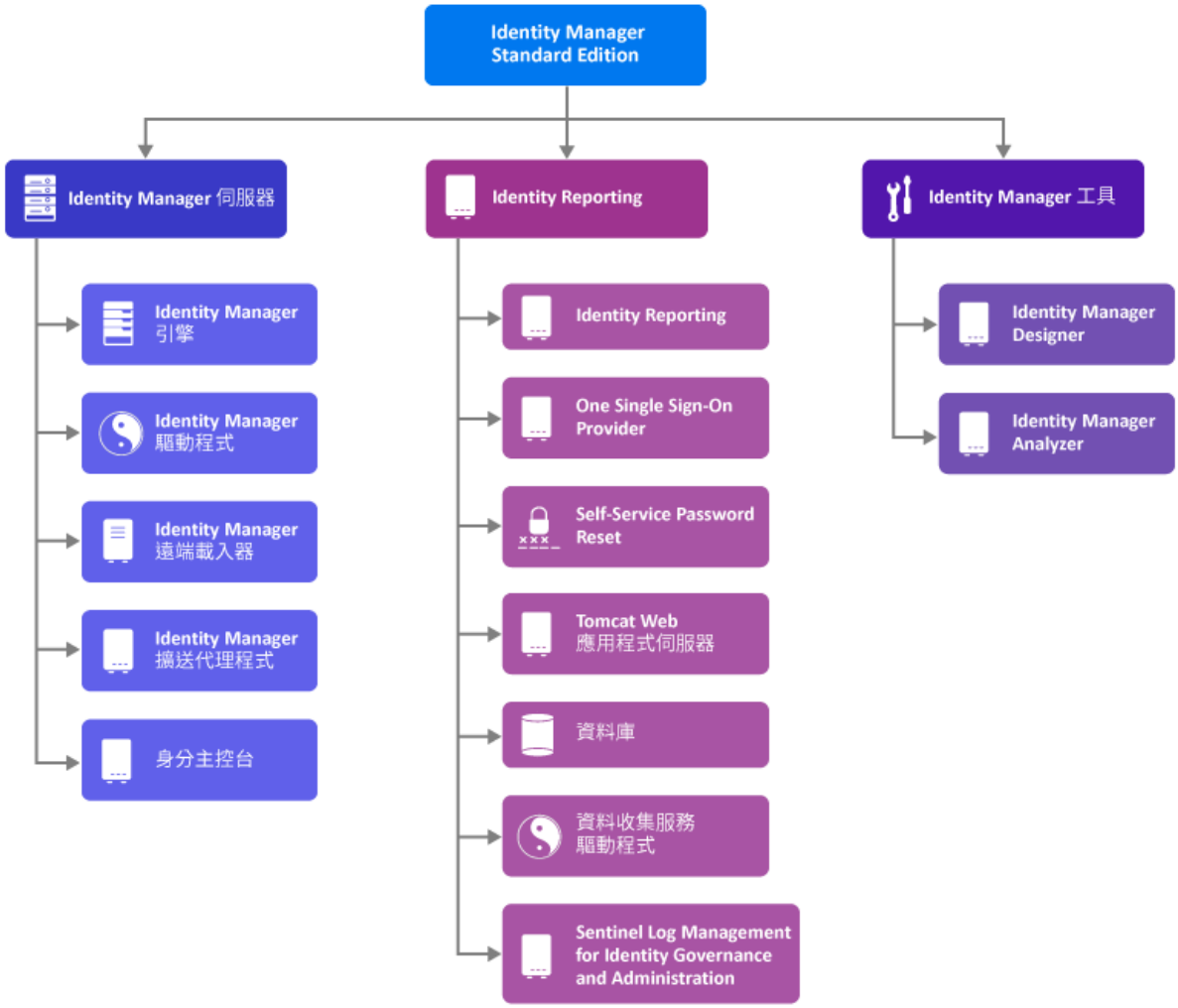


圖 1-2 列出了 Identity Manager Standard Edition 環境中部署的元件。

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 Azul 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

NetIQ Identity Console 是一款先進的 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。Identity Console 取代了 iManager。

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) (https://www.netiq.com/documentation/identity-console/identity_console-admin/data/bookinfo.html)

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 要求在本地安裝 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的應用程式開發介面 (API))
- **idmdash** (用於儀表板和 Identity Applications 管理介面)

當某個使用者與 `idmdash` 應用程式互動時，此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` 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。Identity Reporting 支援的資料庫有 PostgreSQL、Oracle 和 MS SQL。

- 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 21 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 21 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 21 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 (`SentinelLogManagementForIGA8.6.1.0.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。

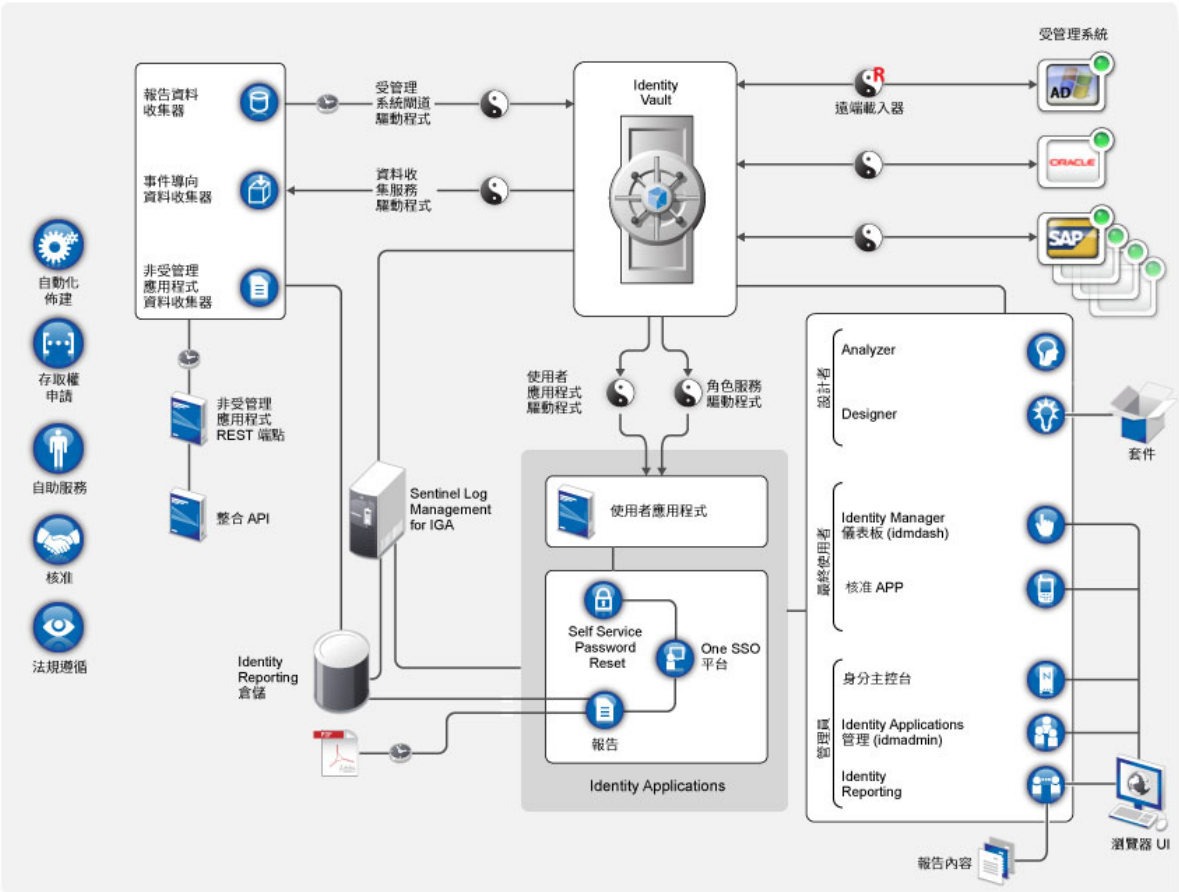
- 分析設定檔編輯器可讓您設定用於分析一或多個資料集例項的設定檔。每個分析設定檔包含一或多個測量標準，您可以依據這些測量標準來評估屬性值，以確定資料符合您所定義之資料格式標準的程度。
- 比對設定檔編輯器可讓您比較一或多個資料集中的值。您可以檢查指定的資料集中是否有重複的值，以及兩個資料集之間是否有相符的值。

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。

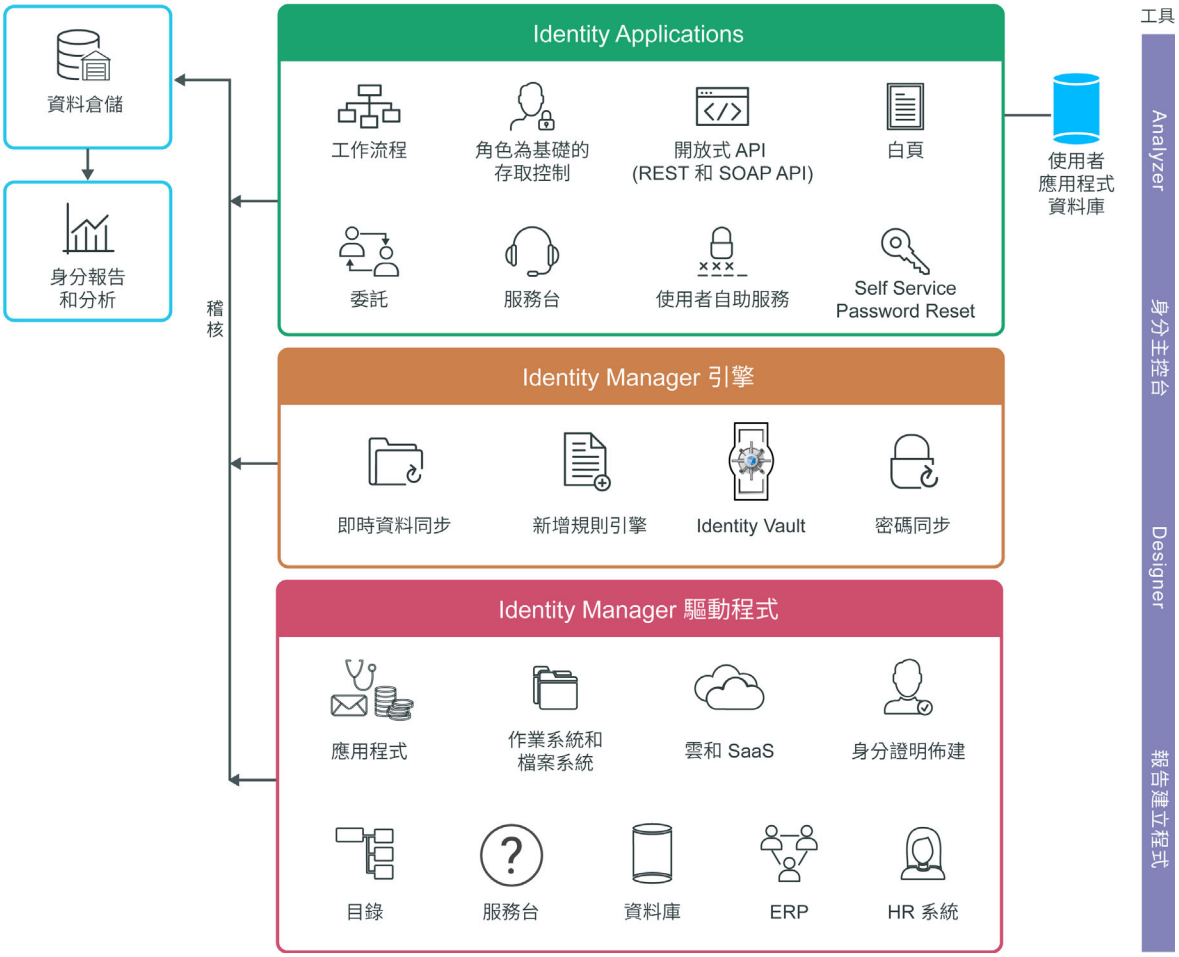
瞭解 Identity Manager 不同元件的用途及安裝方式後，請參閱圖 1-3 以瞭解元件之間的互動模式。

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 26 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。

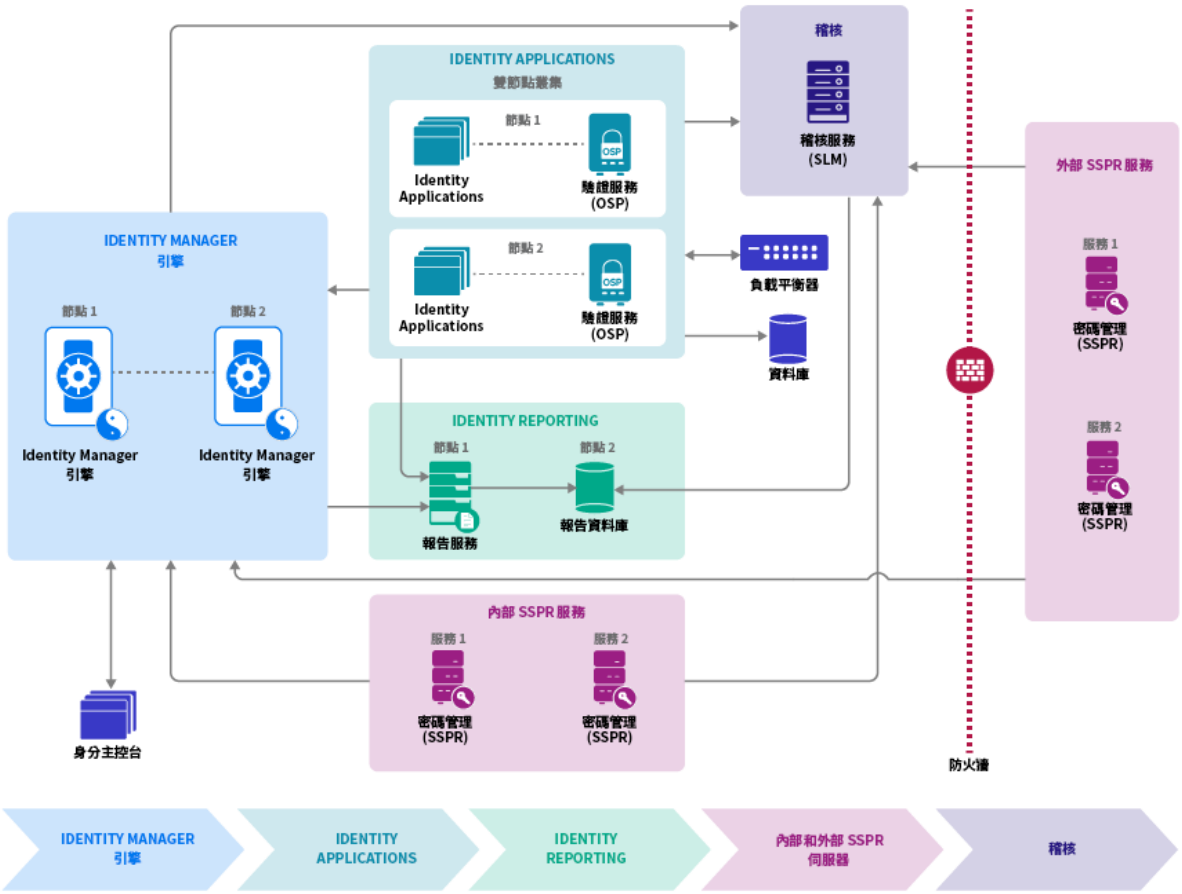
高可用性可確保關鍵網路資源 (包括資料、應用程式和服務) 的高效可管理性。您可以透過減少任何單一故障點及使用備援元件來實作高可用性。同樣地，將 Identity Management 元件的多個例項連接至負載平衡器也可以提供高度可用的環境。

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。

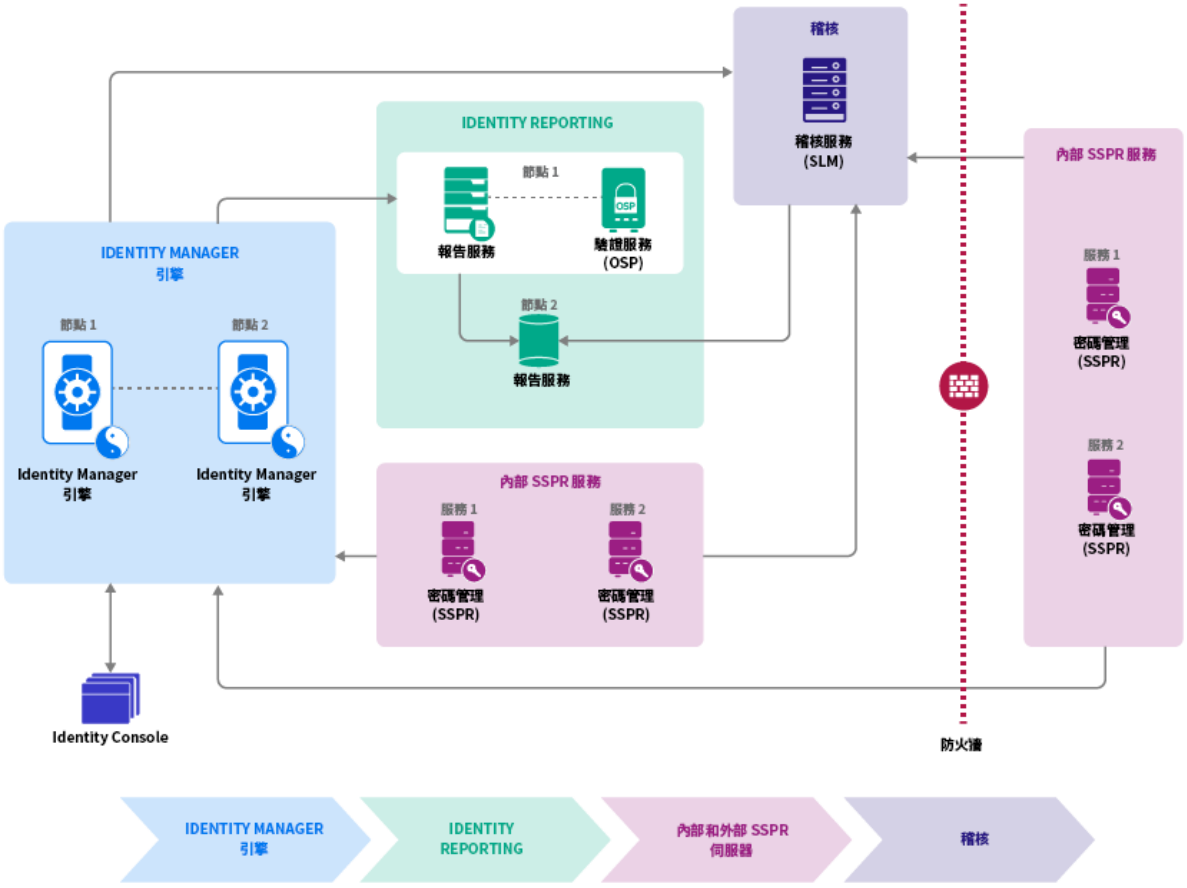
NetIQ 已對此組態進行測試，並建議使用此組態。

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
	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。
驗證	Identity Manager 伺服器
	One Single Sign-On Provider
密碼管理	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

執行核對清單

使用以下核對清單來規劃、安裝和設定 Identity Manager。

	核對清單項目
❑	1. 查看產品架構資訊，以瞭解 Identity Manager 元件。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「How Identity Manager Works」 (Identity Manager 的工作原理)。

	核對清單項目
❑	2. 查看 Identity Manager 授權資訊，以確定您需要使用 Identity Manager 的試用授權還是企業授權。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)。
❑	3. 依據您要實作的功能確定適合您環境的部署類型。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「Identity Manager Deployment Configurations」(Identity Manager 部署組態)。
❑	4. 確定您是否能以偏好的語言執行安裝程式。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 Identity Manager Localization」(瞭解 Identity Manager 當地語系化)。
❑	5. 找到安裝檔案。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)。
❑	6. 安裝 Identity Manager。如需詳細資訊，請參閱第 III 部分 「安裝和設定 Identity Manager 元件」(第 59 頁)。
❑	7. 設定安裝的元件。如需詳細資訊，請參閱第 5 章 「設定 Identity Manager 的元件」(第 75 頁)。
❑	8. 執行一些額外的組態步驟，以使各個元件可完全正常運作。如需詳細資訊，請參閱第 6 章 「完成安裝的最後步驟」(第 89 頁)。

附註：對於叢集和雲端部署，請務必查看建議的組態詳細資料和要求。

- 「部署 Identity Manager 以實現高可用性」(第 337 頁)
- 「在 AWS EC2 上部署 Identity Manager」(第 313 頁)

建議的安裝情境和伺服器設定

本節內容可協助您確定單伺服器或分散式環境中的安裝順序和伺服器設定。

- 「確定何時安裝 SLM for IGA」(第 37 頁)
- 「在分散式環境中安裝的注意事項」(第 37 頁)

確定何時安裝 SLM for IGA

Sentinel 是 Identity Manager 的偏好稽核事件目的地。Identity Manager 可使用 Sentinel Event Source Management (ESM) 來設定 Sentinel Link，從而提供將事件轉遞到 Sentinel 的功能。如果您已在使用 Sentinel 進行稽核，或者將其當成整合架構來追蹤身分，則可以選擇使用現有的 Sentinel 來稽核事件，而無需安裝 SLM for IGA。

無論您是選擇重複利用現有的 Sentinel 伺服器，還是全新安裝 Identity Manager 隨附的 SLM for IGA，都必須將 Sentinel 伺服器設定為稽核資料的來源。為此，可以透過「Identity Manager 資料收集服務」頁面在 Sentinel 伺服器上建立一個資料同步規則，以用於稽核事件。如需詳細資訊，請參閱《*Administrator Guide to NetIQ Identity Reporting*》(NetIQ Identity Reporting 管理員指南) 中的「About the Data Sync Policies tab」(關於「資料同步規則」索引標籤)。

在分散式環境中安裝的注意事項

查看以下注意事項以協助您規劃安裝：

元件粘性

元件	獨立安裝	附註
Identity Manager 引擎	是	
Identity Applications	是	必須具有自己的 OSP。必須將 Identity Applications 和 OSP 安裝在同一部電腦上。 **重要：**Identity Manager 不支援在遠端安裝的 OSP。如果您要升級至此版本，必須使用 Identity Applications 升級期間安裝的 OSP，然後將現有 OSP 伺服器中的 OSP 設定複製到安裝了 OSP 的新伺服器中。如需詳細資訊，請參閱「Identity Applications 元件的升級後任務」(第 206 頁)。
Identity Reporting	是	可以具有自己的 OSP。安裝或升級 Identity Reporting 時，安裝程式支援本地或遠端安裝的 OSP。
OSP	否	對於 Identity Applications，安裝程式不支援在遠端安裝的 OSP。必須將 OSP 和 Identity Applications 安裝在同一部電腦上。 **重要：**如果您要升級至此版本，必須使用 Identity Applications 升級期間安裝的 OSP，然後將現有 OSP 伺服器中的 OSP 設定複製到安裝了 OSP 的新伺服器上。如需詳細資訊，請參閱「Identity Applications 元件的升級後任務」(第 206 頁)。

元件	獨立安裝	附註
SSPR	是	安裝程式支援獨立安裝和升級 SSPR。 如果您在標準版中安裝或升級 SSPR，NetIQ 建議您在獨立伺服器上安裝或升級 SSPR。換而言之，SSPR 不能與 Identity Reporting 安裝在同一部伺服器上。 **重要：**如果您要在 Identity Applications 和 SSPR 部署到不同伺服器的環境中升級至此版本，並希望將現有 SSPR 設定還原到安裝了 SSPR 的新伺服器，請務必使用 ConfigUpdate 公用程式修改新 SSPR 伺服器上的 SSPR 設定。如需詳細資訊，請參閱 「Identity Applications 元件的升級後任務」(第 206 頁)。
Identity Applications 資料庫	是	
Reporting 資料庫	是	
Sentinel Log Management for Identity Governance and Administration (Sentinel Log Management)	是	

伺服器設定

在一般的線上環境中，您可能會將 Identity Manager 安裝在七個或更多個伺服器上，還會安裝在用戶端工作站上。例如：

電腦設定	元件設定
一體機 (建議僅用於展示 / POC 設定)	在一部電腦上安裝和設定所有元件 (Identity Manager 引擎、Identity Applications、Identity Reporting、OSP、SSPR、Identity Applications 資料庫和 Reporting 資料庫)，並在另一部電腦上安裝和設定 Sentinel Log Management。
分散式設定	
伺服器 1	• Identity Vault • Identity Manager 引擎
伺服器 2	Identity Applications 和 OSP (可以叢集化)
伺服器 3	Identity Reporting (OSP)
伺服器 4	SSPR
伺服器 5 和 6	Identity Manager 資料庫，用於： • Identity Applications • Identity Reporting

電腦設定	元件設定
伺服器 7	Sentinel Log Management

附註：從版本 4.7 開始，不再支援在包含多個 Identity Vault 例項的伺服器上安裝 Identity Manager。

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。
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。

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 4.9 系統要求)。如需某個特定版本的系統要求資訊，請參閱 System Requirements for Identity Manager 4.9 (Identity Manager 4.9 系統要求) 中該版本隨附的版本說明。

Identity Manager 的建置可能會因 IT 環境的需求而異，因此您應先聯絡 NetIQ 諮詢服務部門或任何 NetIQ Identity Manager 合作夥伴，再決定適合您環境的 Identity Manager 架構。

在 SLES 伺服器上安裝 Identity Manager

- 在安裝 Identity Manager 之前，請務必安裝以下相依程式庫或 RPM：
  - `libgcc*.x86_64`

- gettext.x86_64
- unzip
- bc
- lsof
- net-tools
- openssl
- pam-modules
- coreutils
- glibc-32bit-*.x86_64.rpm
- libnsl-*.x86_64.rpm
- libstdc++6-32bit
- libz1-32bit

其中 * 表示 RPM 的最新版本。

例如，若要新增 libnsl-<version>.x86_64.rpm 檔案，可輸入以下指令：

```
zypper in libsnl-<version>.x86_64.rpm
```

- (視情況而定) 如果您在 SLES 15 或 SLES 15 SPx (x 表示 Identity Manager 支援的所有 SLES 15 版本) 上安裝 Identity Manager，請確定已安裝 libncurses5*、libncurses6* 和 insserv-compat* RPM。* 符號表示 RPM 的最新版本。
- (選擇性) 若要在 SLES 上安裝 Identity Manager 所需的套件，請建立 install.sh 檔案，並將以下內容新增至其中：

```
#!/bin/bash

zypper refresh

PKGS=" libstdc*.x86_64 libgcc*.x86_64 unzip bc bash coreutils
gettext.x86_64 glibc.x86_64 lsof net-tools openssl sed insserv ss* pam-
modules"

for PKG in $PKGS ;
do
    zypper -n install "$PKG"

done
```

執行 install.sh 檔案。

附註：NetIQ 建議從您的作業系統訂閱服務獲取相依套件，以確保取得作業系統廠商的持續支援。如果您沒有訂閱服務，可以從相關網站 (例如 http://rpmfind.net/linux) 找到最新的套件。

在 RHEL 伺服器上安裝 Identity Manager

若要在執行 Red Hat Enterprise Linux 或更新版本作業系統的伺服器上安裝 Identity Manager，請確定伺服器符合一組特定的先決條件。

- 「先決條件」(第 41 頁)
- 「確認伺服器上已安裝相依程式庫」(第 42 頁)
- 「在 RHEL 9.x 上建立用於安裝媒體的儲存庫」(第 42 頁)
- 「在 RHEL 8.x 上建立用於安裝媒體的儲存庫」(第 44 頁)
- 「執行先決條件檢查」(第 45 頁)

先決條件

NetIQ 建議您檢閱以下先決條件：

- 如果 `/etc/hosts` 項目中包含系統主機名稱的迴路位址別名，則必須將其變更為主機名稱或 IP 位址。也就是說，如果 `/etc/hosts` 檔案中包含類似以下第一個範例中的項目，則需將其變更為以下第二個範例中的正確項目。

  當任何公用程式嘗試解析到 ndsd 伺服器時，下面的範例會出現問題：

  ```
  <loopback IP address> test-system localhost.localdomain localhost
  ```

  以下為 `/etc/hosts` 中正確的範例項目：

  ```
  <loopback IP address> localhost.localdomain localhost
  <IP address> test-system
  ```

  如果任何協力廠商工具或公用程式透過 localhost 解析，則需要將其變更為透過主機名稱或 IP 位址而非 localhost 位址解析。

- 如果您已在 RHEL 8.x 上設定安全增強式 Linux (SELinux)，則必須
  - 將值設定為 **permissive** 以安裝 Identity Manager 引擎。否則，引擎安裝將會失敗，並顯示以下錯誤：`Identity Vault 組態失敗，結束代碼為 10`

    例如，若要將 SELinux 的值設定為 permissive，請執行以下步驟：

    1. 修改 `/etc/selinux/` 目錄中的 `config` 檔案。
    2. 在 **SELINUX** 欄位中，將值設為 `permissive`。
    3. 儲存變更並重新啟動系統。
  - 如果安裝 Identity Reporting 的伺服器不同於安裝 Identity Manager 引擎和 Identity Applications 的伺服器，請停用 SELinux。否則，Tomcat 服務將不會啟動，並且 Identity Reporting 資料庫組態會報告 liquibase 錯誤。
- 在伺服器上安裝適當的程式庫。如需詳細資訊，請參閱 「確認伺服器上已安裝相依程式庫」(第 42 頁)。
- 務必在要安裝遠端載入器的伺服器上的環境變數 `$PATH` 或 `$JAVA_HOME` 中設定 Java 路徑。您必須先執行此動作，然後再執行 `./RHEL-Prerequisite.sh` 程序檔。若要設定 Java 路徑，請執行以下指令：

export PATH=<java 安裝位置 >/bin:$PATH

例如：export PATH=/opt/netiq/common/jre/bin/:$PATH

確認伺服器上已安裝相依程式庫

在 64 位元平台上，RHEL 所需的程式庫因所選安裝方法的不同而異。請依以下順序安裝相依程式庫或 RPM。

附註：若要新增 ksh 檔案，您可以輸入以下指令：

```
yum -y install ksh
```

- glibc-*.i686.rpm
- libgcc-*.i686.rpm
- libXtst-*.i686.rpm
- libXrender-*.i686.rpm
- libXi-*.i686.rpm
- unzip
- bc
- lsof
- net-tools
- libncurses

附註：對於 Identity Manager，您可以編輯 ./RHEL-Prerequisite.sh 程序檔，移除其中包含的所有 compat-libstdc++-33.x86_64.rpm 和 compat-libstdc++-33-*.i686.rpm。安裝 Identity Manager 時不再需要這些套件。

在 RHEL 9.x 上建立用於安裝媒體的儲存庫

如果您的 RHEL 9.x 伺服器需要用於存放安裝媒體的儲存庫，您可以手動建立一個儲存庫。

附註：RHEL 伺服器必須裝有適當的程式庫。如需詳細資訊，請參閱 「確認伺服器上已安裝相依程式庫」(第 42 頁)。

若要設定用於安裝的儲存庫，請執行以下操作：

1. 在本地伺服器上建立掛接點。

   例如：

   ```
   mkdir -p /mnt/rhel9
   ```

2. 掛接 RHEL 9.x 安裝 ISO：

   ```
   mount -o loop <RHEL9.x.iso> /mnt/rhel9
   ```

例如：

```
mount -o loop rhel-server-9.0-x86_64-dvd.iso mnt/rhel9
```

3 將掛接目錄中的 media.repo 檔案複製到 /etc/yum.repos.d/，並設定所需的許可權。

例如：

```
cp /mnt/rhel9/media.repo /etc/yum.repos.d/rhel9.repo


chmod 644 /etc/yum.repos.d/rhel9.repo
```

4 修改 rhel9.repo 檔案並新增以下內容：

```
[InstallMedia]
name=Red Hat Enterprise Linux 9.0.0
mediaid=None
metadata_expire=-1
gpgcheck=0
cost=500
enabled=1
baseurl=file:///mnt/rhel9/BaseOS/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

5 如果您要安裝 32 位元套件，請在 /etc/yum.conf 檔案中將 exactarch 參數的值從 1 變更為 0。

6 執行以下指令：

```
yum clean all
```

7 (視情況而定) 如果您要從 DVD 儲存庫擷取套件清單，請執行以下指令：

```
yum --noplugins list
```

8 安裝 yum-utils 套件。

```
yum install createrepo dnf-utils
```

9 若要在 RHEL 9.x 上安裝 Identity Manager 所需的套件，請建立 install.sh 檔案，並將以下內容新增至其中：

附註：如果您看到任何有關 RPM 重複的警告，則必須使用相應的 yum 指令手動處理該警告。

```
#!/bin/bash
yum clean all
yum repolist
yum makecache

PKGS="ksh gettext.x86_64 libXrender.i686 libXau.i686 libxcb.i686
libX11.i686 libXext.i686 libXi.i686 libXtst.i686 glibc-*.i686.rpm
libstdc++.x86_64 libgcc-*.i686.rpm unzip bc lsof net-tools"

for PKG in $PKGS;
do
yum -y install "$PKG"
done
```

10 安裝以下套件：

```
yum install libgcc*.i686 libnsl* libnsl*.i686 libncurses*
```

11 執行 `install.sh` 檔案。

12 若要確認是否符合先決條件，請執行 「執行先決條件檢查」(第 45 頁) 中所述的程序檔。

13 安裝 Identity Manager 4.9。

在 RHEL 8.x 上建立用於安裝媒體的儲存庫

如果您的 RHEL 8.x 伺服器需要用於存放安裝媒體的儲存庫，您可以手動建立一個儲存庫。

附註：RHEL 伺服器必須裝有適當的程式庫。如需詳細資訊，請參閱 「確認伺服器上已安裝相依程式庫」(第 42 頁)。

若要設定用於安裝的儲存庫，請執行以下操作：

1 在本地伺服器上建立掛接點。

例如：

```
mkdir -p /mnt/rhel8
```

2 掛接 RHEL 8 安裝 ISO：

```
mount -o loop rhel-server-8.0-x86_64-dvd.iso mnt/rhel8
```

3 將掛接目錄中的 `media.repo` 檔案複製到 `/etc/yum.repos.d/`，並設定所需的許可權。

例如：

```
cp /mnt/rhel8/media.repo /etc/yum.repos.d/rhel8.repo


chmod 644 /etc/yum.repos.d/rhel8.repo
```

4 修改 `rhel8.repo` 檔案並新增以下內容：

```
[dvd-BaseOS]
name=DVD for RHEL8 - BaseOS
baseurl=file:///RHEL8/BaseOS
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

[dvd-AppStream]
name=DVD for RHEL8 - AppStream
baseurl=file:///RHEL8/AppStream
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

5 如果您要安裝 32 位元套件，請在 `/etc/yum.conf` 檔案中將 `exactarch` 參數的值從 1 變更為 0。

6 執行以下指令：

```
yum clean all
```

7 (視情況而定) 如果您要從 DVD 儲存庫擷取套件清單，請執行以下指令：

```
yum --noplugins list
```

8 安裝 yum-utils 套件。

```
yum install createrepo yum-utils
```

9 若要在 RHEL8 上安裝 Identity Manager 所需的套件，請建立 install.sh 檔案並將以下內容新增至其中：

附註：如果您看到任何有關 RPM 重複的警告，則必須使用相應的 yum 指令手動處理該警告。

```
#!/bin/bash
yum clean all
yum repolist
yum makecache

PKGS="ksh gettext.x86_64 libXrender.i686 libXau.i686 libxcb.i686
libX11.i686 libXext.i686 libXi.i686 libXtst.i686 glibc-*.i686.rpm
libstdc++.x86_64 libgcc-*.i686.rpm unzip bc lsof net-tools"

for PKG in $PKGS;
do
yum -y install "$PKG"
done
```

10 安裝以下套件：

```
yum install libgcc*.i686 libnsl* libnsl*.i686 libncurses*
```

11 執行 install.sh 檔案。

12 若要確認是否符合先決條件，請執行 「執行先決條件檢查」(第 45 頁) 中所述的程序檔。

13 安裝 Identity Manager 4.9。

執行先決條件檢查

您可以針對每個 Identity Manager 元件產生不符合先決條件的報告。執行 ./RHEL-Prerequisite.sh 程序檔 (位於安裝套件的掛接目錄中)。

3 安裝 Identity Manager 元件的注意事項

本章提供有關安裝 Identity Manager 元件的先決條件、注意事項以及所需的系統設定。

- 「安裝順序」(第 47 頁)
- 「瞭解安裝和組態程序」(第 47 頁)
- 「安裝 Identity Manager 引擎元件和遠端載入器的注意事項」(第 49 頁)
- 「安裝 Identity Applications 元件的注意事項」(第 50 頁)
- 「安裝 Identity Reporting 元件的注意事項」(第 54 頁)
- 「安裝 Designer 的注意事項」(第 55 頁)
- 「安裝 Analyzer 的注意事項」(第 56 頁)
- 「安裝 SLM for IGA 的注意事項」(第 56 頁)
- 「查看 Identity Manager 元件使用的連接埠」(第 57 頁)

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
- Identity Manager 引擎元件
- Identity Applications 元件 (僅適用於進階版)
- Identity Reporting 元件
- Identity Console
- Designer for Identity Manager
- Analyzer for Identity Manager

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。

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。

瞭解安裝和組態程序

互動安裝：在互動式安裝過程中，必須在互動模式下指定輸入內容。Identity Manager 提供程序檔式安裝程式，用於透過兩個不同的階段來安裝和設定個別元件或一組元件。安裝階段將會安裝元件。安裝程序檔 `install.sh` 位於 Identity Manager 安裝套件 `.iso` 影像檔的根目錄中。如需有關組態的資訊，請參閱組態。

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 引擎和 Identity Manager 驅動程式。安裝程序還會安裝 Azul Zulu JDK。
Identity Manager 遠端載入器伺服器	在遠端載入器中安裝遠端載入器服務和驅動程式例項。
Identity Manager 擴送代理程式	安裝 JDBC 擴送驅動程式的擴送代理程式。如需詳細資訊，請參閱 Installing the Fanout Agent with Identity Manager 4.9 (https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/how-to-install-fan-out-agent-with-identity-manager-4-7.html) (隨 Identity Manager 4.9 一起安裝擴送代理程式)。
Identity Applications	安裝用於提供 Identity Applications 基礎架構的數個元件。 ◆ 使用者應用程式 ◆ OSP ◆ SSPR ◆ Tomcat ◆ PostgreSQL 資料庫 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。 安裝程序還會將使用者應用程式驅動程式和角色與資源服務驅動程式部署到 Identity Vault。
Identity Reporting	安裝用於提供 Identity Reporting 基礎架構的數個元件。 ◆ Identity Reporting ◆ 受管理系統閘道 (MSGW) 驅動程式 ◆ 資料收集服務驅動程式 (DCS) ◆ OSP (與 Identity Applications 不安裝在同一部伺服器上時) ◆ Tomcat (與 Identity Applications 不安裝在同一部伺服器上時) ◆ PostgreSQL 資料庫 (與 Identity Applications 不安裝在同一部伺服器上時) 為了支援 Tomcat 應用程式伺服器，安裝程式將安裝受支援版本的 JRE。

附註：Identity Manager 針對 Designer、Analyzer 和 Sentinel Log Management 提供了不同的安裝程式。

靜默安裝：安裝程式將提供以互動模式建立靜默內容檔案的選項。您可以將安裝選項記錄在內容檔案中，然後使用該檔案在環境中的其他伺服器上執行靜默安裝。靜默安裝程式會從該檔案中讀取相應的值來執行安裝。如需元件範圍組態的詳細資料，請參閱「瞭解組態參數」(第 75 頁)。

組態：Identity Manager 提供兩種組態模式：

- 一般組態
- 自訂組態

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設定大部分設定。

安裝 Identity Manager 引擎元件和遠端載入器的注意事項

- Identity Manager 引擎安裝程序要求至少提供以下數目的磁碟空間：

路徑	元件	所需的最低安全空間
/opt	Identity Manager 引擎	3 GB
/var	Identity Manager 引擎	5 GB，用於包含 100,000 個物件的 dib
/etc	Identity Manager 引擎	5 MB

- 務必先安裝 Identity Manager 引擎，然後再安裝遠端載入器。
- 可以在安裝了 Identity Manager 引擎的同一台電腦上安裝遠端載入器。確定作業系統支援這兩個元件。
- 在能與受管理系統通訊的伺服器上安裝遠端載入器。必須能夠使用相關 API 存取每個受管理系統的驅動程式。
- (視情況而定) 如果您以非 root 使用者身分安裝 Identity Manager 引擎，安裝程序將不會安裝 Linux 帳戶驅動程式或遠端載入器。您必須單獨安裝這些元件。
- NetIQ 建議您不要將 `changelog` 模組安裝在 Identity Manager 引擎或遠端載入器所在的同一部伺服器上。
- 如果您打算使用非預設部署網路位置 (即除 `o=system` 以外的任何網路位置)，NetIQ 建議您在安裝 Identity Manager 引擎之前建立自訂 LDIF 檔案。在組態設定期間，系統會提示您輸入該自訂 LDIF 檔案的位置。

  附註：如果您在安裝之前未建立 OU 結構，可以使用要在其下建立驅動程式集的所有容器的階層來定義所需 OU 結構。透過 LDIF 檔案設定新的驅動程式集時，將使用此結構和階層。

- NetIQ 建議您在開始安裝之前，針對所有語言執行以下指令：

  ```
  export LC_ALL=< 語言 >
  ```

例如：

```
export LC_ALL=zh_TW
```

安裝 Identity Applications 元件的注意事項

NetIQ 建議您在開始執行安裝程序之前，檢閱 Identity Applications 的先決條件和電腦要求。如需在安裝應用程式元件後設定 Identity Applications 環境的詳細資訊，請參閱《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》(NetIQ Identity Manager - Identity Applications 管理員指南)。

- 「安裝考量」(第 50 頁)
- 「資料庫考量」(第 51 頁)
- 「設定 Identity Applications 的資料庫」(第 52 頁)

安裝考量

- Identity Applications 安裝程序要求至少提供以下數量的磁碟空間來安裝元件：
  - /opt - 5 GB
  - /var - 100 MB
- Identity Applications 要求已安裝以下 Identity Manager 元件的受支援版本：
  - Identity Manager 引擎
  - 遠端載入器
- (選擇性) NetIQ 在安裝期間會啟用安全通訊端層 (SSL) 通訊協定。若要變更環境中 Identity Applications 元件之間的通訊設定，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 Security in the Identity Applications」(設定 Identity Applications 中的安全性)。
- 您不能將角色與資源服務驅動程式與遠端載入器配合使用，因為該驅動程式使用 jClient。
- 每個使用者應用程式例項只能為一個使用者容器提供服務。例如，您只能搜尋、查詢與該例項關聯的容器，以及向其新增使用者。此外，使用者容器與應用程式之間的關聯是永久性的。
- 在分散式環境中，Identity Applications 伺服器的金鑰儲存區 (`idm.jks`) 中必須存在 CN 為 Identity Applications 的證書。做為增強的 Java 安全措施的一部分，Identity Applications 現在需要可信證書才能與 OSP 通訊。

資料庫考量

資料庫用於儲存 Identity Applications 的資料和組態資訊。

在安裝資料庫例項之前，請檢閱以下先決條件：

- 若要設定與 Tomcat 配合使用的資料庫，必須確定該資料庫包含所需的 JDBC jar 檔案。Identity Applications 使用標準 JDBC 呼叫來存取和更新該資料庫。Identity Applications 使用與 JNDI 網路樹結合的 JDBC 資料來源檔案來開啟資料庫連接。
- 您必須有一個指向該資料庫的現有資料來源檔案。使用者應用程式的安裝程式將在 `server.xml` 和 `context.xml` 中建立一個指向資料庫的 Tomcat 資料來源項目。
- 如果您使用受支援版本的 Oracle 或 Microsoft SQL Server 資料庫，則必須設定以下兩個資料庫例項才能使 Identity Applications 正常運作：Identity Applications (例如：`idmuserappdb`) 資料庫和工作流程 (例如：`igaworkflowdb`) 資料庫。
- 務必準備好以下資訊：
  - 資料庫伺服器的主機和連接埠。
  - 要建立之資料庫的名稱。Identity Applications 的預設資料庫為 `idmuserappdb`。
  - 資料庫使用者名稱和密碼。資料庫使用者名稱必須代表某個管理員帳戶，或必須有權在資料庫伺服器中建立表格。使用者應用程式的預設管理員為 `idmadmin`。
  - 資料庫廠商為您所用資料庫提供的驅動程式 `.jar` 檔案。NetIQ 認可協力廠商提供的驅動程式 JAR 檔案。
- 資料庫例項可以安裝在本地電腦上，也可以安裝在連接的伺服器上。
- 資料庫字元集必須使用 Unicode 編碼。例如，UTF-8 便是一種使用 Unicode 編碼的字元集，而 Latin1 則不是。如需指定字元集的詳細資訊，請參閱 「設定字元集」(第 52 頁) 或 「設定 Oracle 資料庫」(第 52 頁)。
- 如果您要連接到遠端資料庫，請確定在安裝 Identity Applications 之前建立該資料庫。如需連接到遠端 PostgreSQL 資料庫的資訊，請參閱 「連接遠端 Remote PostgreSQL 資料庫」(第 143 頁)。
- 對資料庫使用區分大小寫的定序可能會導致在移轉期間發生重複鍵錯誤。請檢查定序並予以校正，然後重新安裝 Identity Applications。
- (視情況而定) 若要將同一個資料庫例項用於稽核與 Identity Applications，NetIQ 建議在一個獨立的專屬伺服器 (而非代管執行 Identity Applications 的 Tomcat 的伺服器) 上安裝該資料庫。
- (視情況而定) 如果要移轉至新版 Identity Applications，您必須使用先前安裝所用的同一個資料庫。
- MS SQL 僅支援 SQL_Latin1_General_CP1_CI_AS 定序。

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。

安裝程序預設會為 Identity Applications 安裝 PostgreSQL 資料庫，並建立擁有該資料庫的管理使用者 `idmadmin`。但不會在 Identity Applications 的資料庫中建立綱要。您安裝 Identity Applications 時將新增綱要資訊。

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。

- 「檢查資料庫的相容性層級」(第 52 頁)
- 「設定字元集」(第 52 頁)
- 「設定管理員使用者帳戶」(第 53 頁)

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';
   ```

   預期的輸出為 12.2.xx、18.xx 或 19.xx。

   附註：從 Identity Manager 4.8.1 開始支援 Oracle 19c。

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。

若要確認受支援的 Oracle 資料庫是否設定為使用 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
```

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 資料庫使用者帳戶具有特定的權限。在 SQL Plus 公用程式中輸入以下指令：

```
CREATE USER idmuser IDENTIFIED BY password;
GRANT CREATE SESSION TO idmuser;
GRANT CREATE CLUSTER TO idmuser;
GRANT CREATE PROCEDURE TO idmuser;
GRANT CREATE SEQUENCE TO idmuser;
GRANT CREATE TABLE TO idmuser;
GRANT CREATE TRIGGER TO idmuser;
ALTER USER idmuser quota 100M on USERS;
```

其中，*idmuser* 代表使用者帳戶。

附註：建議使用支援的協力廠商 JDBC jar。例如：`ojdbc8.jar`。

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。

- 「設定字元集」(第 53 頁)
- 「設定管理員使用者帳戶」(第 53 頁)

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。

設定管理員使用者帳戶

安裝 Microsoft SQL Server 後，請使用 SQL Server Management Studio 之類的應用程式建立一個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
- REFERENCES

附註：建議使用支援的協力廠商 JDBC jar。例如 `mssql-jdbc-7.2.2.jre11.jar`。

安裝 Identity Reporting 元件的注意事項

本節提供關於準備安裝 Identity Reporting 各元件的指導準則。您可以使用 Sentinel 來稽核事件。

NetIQ 建議您在開始安裝前先查看以下資訊。

- 「Identity Reporting 的先決條件」(第 54 頁)
- 「Identity Reporting 的身分稽核事件」(第 55 頁)

Identity Reporting 的先決條件

- 安裝程序要求至少提供以下數量的磁碟空間：
  - /opt - 5 GB
  - /var - 2 GB
  - /etc - 2 GB
- 安裝程序要求已安裝且設定以下 Identity Manager 元件的受支援版本：
  - Identity Applications，包括使用者應用程式驅動程式 (僅適用於進階版)
  - 在單獨的 Linux 電腦上安裝的 Sentinel Log Management。
- 安裝程序會在 Tomcat 的 `setenv.sh` 檔案中修改 JRE 對應的 `JAVA_OPTs` 或 `CATALINA_OPTS` 項目。
- 請不要將 Identity Reporting 安裝在叢集環境中的伺服器上。
- 如果您要連接到遠端資料庫，請確定在安裝 Identity Reporting 之前建立該資料庫。如需連接到遠端 PostgreSQL 資料庫的資訊，請參閱 「連接遠端 Remote PostgreSQL 資料庫」(第 143 頁)。
- 若要針對 Oracle 資料庫執行報告，必須確定已複製支援的協力廠商 jar。如需詳細資訊，請參閱 「對 Oracle 資料庫執行報告」(第 138 頁)。
- 為任何您要授予報告功能存取權的使用者指定報告管理員角色

- 確認 Identity Manager 環境中的所有伺服器上都設定了相同的時間。如果您不同步化伺服器上的時間，有些報告在執行後可能是空的。例如，如果代管 Identity Manager 引擎與代管倉儲的伺服器的時戳不同，則此問題可能會影響與新使用者相關的資料。如果您建立了一個使用者，隨後對其進行了修改，報告中會填入相應的資料。
- 若要設定報告，必須以小寫形式指定主機名稱。Identity Reporting 6.6.0 及更新版本不再允許您使用 IP 位址來設定報告。

Identity Reporting 的身分稽核事件

本節提供有關如何識別 Identity Manager 報告與自訂報告所需的不同稽核事件的資訊。您可以解壓縮所有報告來源，並執行以下程序檔來識別稽核事件：

```
find . -name *.jrxml -print0 |xargs -0 grep -H "'000[B3]" | perl -ne
'($file) = /^\.\/(.*?)\//;@a = /000[3B]..../g; foreach $a (@a) { print
"$file;$a\n"}' |sort -u
```

本節提供有關如何識別和選取 Identity Manager 報告與自訂報告的不同稽核事件的資訊：

事件名稱	稽核旗標
驗證和密碼變更	**選擇使用 SSPR 的稽核旗標：**啟動 **SSPR 組態編輯器** > **稽核組態** > 選取以下稽核旗標之一： • 驗證 • 變更密碼 • 解除鎖定密碼 • 復原密碼 • 入侵者嘗試 • 入侵者鎖定 • 入侵者鎖定使用者 **使用 Identity Console 選取稽核旗標：**登入 Identity Console，前往**稽核** > **NCP 伺服器** > **安全性事件**，從以下稽核旗標中選取： • 變更密碼 • 驗證密碼 • 登入 • 登出
所有其他報告事件	轉到 **NetIQ Identity Manager UserApp** > **管理** > **記錄** > **啟用稽核服務**

安裝 Designer 的注意事項

- 若要在 RHEL 平台上安裝 Designer，應建立 RHEL 儲存庫。如需詳細資訊，請參閱 「在 RHEL 伺服器上安裝 Identity Manager」（第 41 頁）。

- 此版本不支援從舊的版本升級 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。
- 在執行 SLES 或 RHEL 的電腦上，請先安裝 GNU gettext 公用程式 (`gettext`)，然後再安裝 Designer。這些公用程式提供了國際化和多語言訊息的架構。

附註：NetIQ 建議從您的作業系統訂閱服務獲取相依套件，以確保可持續從作業系統廠商網站獲得支援。如果您沒有訂閱服務，可以從相關網站 (例如 http://rpmfind.net/linux (http://rpmfind.net/linux)) 找到最新的套件。

安裝 Analyzer 的注意事項

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。

- 在執行 SLES 12 SP3 平台的電腦上安裝 Analyzer 之前，請確定已安裝以下程式庫：
  - `libswt3-gtk2`
  - `libxcomposite`
  - `libgdk_pixbuf`
  - `libgtk+-x11`
  - `gettext` (GNU gettext 公用程式)
- 在執行 SLES 8 或更新版本平台的電腦上安裝 Analyzer 之前，請確定已安裝以下程式庫：
  - `gtk2.i686.rpm`。例如，可以從作業系統廠商網站下載套件。
  - `gettext` (GNU gettext 公用程式)

附註：NetIQ 建議從您的作業系統訂閱服務獲取相依套件，以確保取得作業系統廠商的持續支援。如果您沒有訂閱服務，可以從相關網站 (例如 http://rpmfind.net/linux) 找到最新的套件。

- 確定執行 Analyzer 的電腦的視頻解析度達到 1024x768 (建議 1280x1025)。

安裝 SLM for IGA 的注意事項

SLM for IGA 伺服器的作業系統必須至少包含 SLES 伺服器或 RHEL 伺服器的基礎伺服器元件。Sentinel 必須具備下列 RPM 的 64 位元版本：

- `bash`
- `bc`
- `coreutils`
- `gettext`

- glibc
- grep
- libgcc
- libstdc
- lsof
- net-tools
- openssl
- python-libs
- sed
- zlib

如需詳細資訊，請存取 NetIQ Sentinel 技術資訊網站 (https://www.microfocus.com/documentation/sentinel/8.5/)。

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

連接埠號碼	元件	連接埠用途
3000	Identity Applications	供 NGINX 服務使用
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。
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
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	*預設不監聽* 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
8600	表單轉譯器	供 NGINX 服務使用
9000	Identity Console	由 Identity Console 使用
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

III 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，請參閱第 4 章「安裝 Identity Manager」(第 61 頁)。如需設定 Identity Manager 元件的說明，請參閱第 5 章「設定 Identity Manager 的元件」(第 75 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 6 章 「完成安裝的最後步驟」(第 89 頁)。

4 安裝 Identity Manager

本章提供有關可用於安裝 Identity Manager 元件的各種方式的資訊。您可以透過以下方式安裝 Identity Manager 元件：

- 互動安裝
- 靜默安裝

執行互動式安裝

1. 從軟體和授權頁面 (https://sld.microfocus.com/) 下載 `Identity_Manager_4.9.0_Linux.iso`。
2. 掛接下載的 `.iso`。
3. 從 `.iso` 檔案的根目錄中，執行以下指令：

   ```
   ./install.sh
   ```
4. 通讀授權合約。
5. 輸入 `y` 以接受授權合約。
6. 決定要安裝的 Identity Manager 伺服器版本。輸入 `y` 將安裝進階版，輸入 `n` 將安裝標準版。
7. 在可供安裝的元件清單中選取所需的元件：
   - 若要安裝引擎，請選取 **Identity Manager 引擎**。
   - 若要安裝遠端載入器，請選取 **Identity Manager 遠端載入器**。
   - 若要安裝擴送代理程式，請選取 **Identity Manager 擴送代理程式**。
   - 若要安裝 Identity Applications，請選取 **Identity Applications**。
   - 若要安裝 Identity Reporting，請選取 **Identity Reporting**。
   - 若要安裝 Identity Console，請選取 **Identity Console**。
8. (視情況而定) 設定安裝的元件。如需詳細資訊，請參閱第 5 章 「設定 Identity Manager 的元件」 (第 75 頁)。

以靜默模式安裝

1. 從軟體和授權頁面 (https://sld.microfocus.com/) 下載 `Identity_Manager_4.9.0_Linux.iso`。
2. 掛接下載的 `.iso`。
3. 從 `.iso` 的根目錄執行 `create_silent_props.sh` 程序檔。
4. 輸入 `y` 以確認建立檔案。

5 指定靜默內容檔案的路徑。

6 決定要安裝的 Identity Manager 伺服器版本。輸入 y 將安裝進階版，輸入 n 將安裝標準版。

7 決定您是要以一般模式還是自訂模式設定元件。

8 在可供安裝的元件清單中選取所需的元件：

- 若要安裝引擎，請選取 **Identity Manager 引擎**。
- 若要安裝遠端載入器，請選取 **Identity Manager 遠端載入器**。
- 若要安裝擴送代理程式，請選取 **Identity Manager 擴送代理程式**。
- 若要安裝 Identity Applications，請選取 **Identity Applications**。
- 若要安裝 Identity Reporting，請選取 **Identity Reporting**。
- 若要安裝 Identity Console，請選取 **Identity Console**。

設定安裝的元件。如需詳細資訊，請參閱第 5 章 「設定 Identity Manager 的元件」(第 75 頁)。

9 執行以下指令以執行靜默安裝：

```
./install.sh -s -f <location of the silent properties file>
```

例如：

`./install.sh -s -f /home/silent.properties`，其中，`/home/silent.properties` 是靜默內容檔案的儲存位置。

以非 root 使用者身分安裝 Identity Manager 引擎

您可以使用非 root 使用者身分安裝 Identity Manager 引擎，以增強 Linux 伺服器的安全性。如果您是以 root 使用者身分安裝 Identity Vault，則不能以非 root 使用者身分安裝 Identity Manager 引擎。如果要以非 root 使用者身分安裝引擎，則需執行以下步驟：

1. 確定已安裝 NICI。如需詳細資訊，請參閱 「安裝 NICI」(第 62 頁)。
2. 以非 root 使用者身分安裝 Identity Vault。如需詳細資訊，請參閱 「以非 root 使用者身分安裝 Identity Vault」(第 63 頁)。
3. 以非 root 使用者身分安裝 Identity Manager 引擎。如需詳細資訊，請參閱 「以非 root 使用者身分安裝引擎」(第 65 頁)。

安裝 NICI

必須先安裝 NICI，然後再繼續 Identity Vault 安裝。由於必需的 NICI 套件將在系統範圍內使用，因此建議您使用 root 使用者身分安裝必要的套件。不過，如果需要，您也可以使用 sudo 將存取權委託給其他帳戶，然後使用該帳戶來安裝 NICI 套件。

1 從掛接的 iso 中，導覽至 `/IDVault/setup/` 目錄。

2 執行以下指令：

```
rpm -qa|grep nici64-3.2.0.0500-0.x86_64
```

3 驗證 NICI 是否設定為伺服器模式。輸入以下指令：

```
/var/opt/novell/nici/set_server_mode64
```

必須執行此步驟，以確定 Identity Vault 組態程序不會失敗。

以非 root 使用者身分安裝 Identity Vault

本節介紹如何使用 Tar 聚合檔來安裝 Identity Vault。當您擷取檔案時，系統將建立 etc、opt 和 var 目錄。

1 以對要安裝 Identity Vault 的電腦擁有相應權限的 sudo 使用者身分登入。

附註：若要指定自訂安裝路徑，也可以使用 root 使用者身分登入。

2 從掛接的 iso 中，導覽至 /IDVault/ 目錄。

3 建立一個新目錄，然後將 eDir_NonRoot.tar.gz 檔案複製到該目錄。例如，/home/user/install/eDirectory。

4 使用下列指令來解壓縮檔案：

```
tar -zxvf eDir_NonRoot.tar.gz
```

5 若要手動輸出環境變數的路徑，請輸入以下指令：

```
export LD_LIBRARY_PATH=custom_location/eDirectory/opt/novell/
eDirectory/
lib64:custom_location/eDirectory/opt/novell/eDirectory/lib64/
ndsmodules:
custom_location/eDirectory/opt/novell/lib64:$LD_LIBRARY_PATH

export PATH=custom_location/eDirectory/opt/novell/eDirectory/
bin:custom_location/eDirectory/opt/novell/eDirectory/sbin:/opt/novell/
eDirectory/bin:$PATH

export MANPATH=custom_location/eDirectory/opt/novell/
man:custom_location/
eDirectory/opt/novell/eDirectory/man:$MANPATH

export TEXTDOMAINDIR=custom_location/eDirectory/opt/novell/eDirectory/
share/locale:$TEXTDOMAINDIR
```

6 若要使用 ndspath 程序檔輸出環境變數的路徑，必須將 ndspath 程序檔置於公用程式之前。完成以下步驟：

6a 從 custom_location/eDirectory/opt 目錄中，使用以下指令執行該公用程式：

custom_location/eDirectory/opt/novell/eDirectory/bin/ndspath *utility_name_with_parameters*

6b 使用以下指令輸出目前外圍程序中的路徑：

```
. custom_location/eDirectory/opt/novell/eDirectory/bin/ndspath
```

6c 照常執行公用程式。

6d 在 /etc/profile、~/bashrc 或類似程序檔的末尾新增用於輸出路徑的指示。

執行此步驟後，每當您登入或者開啟新外圍程序時，都可以直接啟動公用程式。

7 使用以下方法之一設定 Identity Vault：

- 使用 ndsconfig 公用程式

```
ndsconfig new [-t <treename>] [-n <server_context>] [-a <admin_FDN>]
[-w
<admin password>] [-i] [-S <server_name>] [-d <path_for_dib>] [-m
<module>]
[e] [-L <ldap_port>] [-l <SSL_port>] [-o <http_port>] -O
<https_port>] [-p
<IP address:[port]>] [-c] [-b <port_to_bind>] [-B
<interface1@port1>,
<interface2@port2>,..] [-D <custom_location>] [--config-file
<configuration_file>] [--configure-eba-now <yes/no>]
```

其中，-t 表示要將伺服器新增至的樹狀結構名稱。

-n 表示要在其中新增伺服器物件的伺服器網路位置。

-a 表示對要在其中建立伺服器物件和目錄服務的環境具有監督者權限的使用者物件的完整可辨識名稱。

-s 表示伺服器名稱。

-d 表示儲存資料庫檔案的目錄路徑。

-m 表示模組名稱。

必須指定在組態過程中所指定的相同值。

例如：

```
ndsconfig new -t novell-tree -n novell -a admin.novell -S linux1 -d
/home/
mary/inst1/data -b 1025 -L 1026 -l 1027 -o 1028 -O 1029 -D /home/
inst1/var --config-file /home/inst1/nds.conf --configure-eba-now
yes
```

輸入的連接埠號碼需在 1024 到 65535 的範圍內。小於 1024 的連接埠號碼通常是為進階使用者和標準應用程式保留的。因此，您不能對任何 eDirectory 應用程式假定使用預設連接埠 524。

這可能會導致以下應用程式中斷：

- 未提供用來指定目標伺服器連接埠的選項的應用程式。
- 使用 NCP 並以 root 身分在 524 上執行的舊版應用程式。

- 使用 ndsmanage 公用程式設定一個新例項。如需詳細資訊，請參閱 《NetIQ eDirectory Installation Guide》 (NetIQ eDirectory 安裝指南) 中的 「The ndsmanage Utility」 (ndsmanage 公用程式)。

以非 root 使用者身分安裝引擎

當您使用此方法時，將無法安裝以下元件：

- **遠端載入器：**若要以非 root 使用者身分安裝遠端載入器，請使用 Java 遠端載入器。如需詳細資訊，請參閱「安裝 Java 遠端載入器」(第 71 頁)。
- **Linux 帳戶驅動程式：**需要根特權才能運作。

附註：以非 root 使用者身分安裝 Identity Manager 引擎時，安裝檔案位於非 root 使用者目錄下。例如 `/home/user`，其中 user 為非 root 使用者。執行 Identity Manager 並不需要安裝檔案。您可在安裝後刪除安裝檔案。

若要以非 root 使用者身分安裝 Identity Manager 引擎：

1. 以安裝 Identity Vault 時使用的非 root 使用者身分登入。

   該使用者帳戶必須對非 root Identity Vault 安裝的目錄和檔案具有寫入存取權。
2. 導覽至掛接 `Identity_Manager_4.9.0_Linux.iso` 的位置。
3. 從掛接位置導覽至 `/IDM` 目錄。
4. 執行下列指令：

   ```
   ./idm-nonroot-install.sh
   ```
5. 根據以下資訊完成此安裝：

   非 root eDirectory 安裝的基礎目錄

   指定非根 eDirectory 安裝的目錄。例如，`/home/user/install/eDirectory`。

   延伸 eDirectory 綱要

   如果這是在此 eDirectory 例項中安裝的第一個 Identity Manager 伺服器，請輸入 `Y` 以延伸綱要。如果未延伸綱要，則 Identity Manager 將無法運作。

   系統會提示您為由非根 eDirectory 安裝所代管之非根使用者擁有的每一個 eDirectory 例項延伸綱要。

   如果您選擇延伸綱要，請指定有權延伸綱要之 eDirectory 使用者的完整可辨識名稱 (DN)。使用者必須擁有整個網路樹的「監督者」權限才能延伸綱要。如需以非根使用者身分延伸綱要的詳細資訊，請參閱 `schema.log` 檔案，該檔案位於每一個 eDirectory 例項的 `data` 目錄中。

   完成安裝之後，執行 `/opt/novell/eDirectory/bin/idm-install-schema` 程式，以對其他 eDirectory 例項延伸綱要。
6. 若要完成安裝程序，請繼續「完成非 Root 使用者安裝」(第 144 頁)。

安裝 SSPR

安裝程式將提供用於單獨安裝 SSPR 的選項。如果您要將 Identity Applications 和 SSPR 安裝到不同的電腦上，此選項非常有用。

附註：如果您安裝的是標準版，則必須執行以下程序來安裝 SSPR。安裝標準版時預設不會安裝 SSPR。

以互動模式安裝 SSPR

1. 從 NetIQ 下載網站下載 `Identity_Manager_4.9.0_Linux.iso`。
2. 掛接下載的 `.iso`。
3. 從 `.iso` 檔案的根目錄導覽至 `sspr` 目錄。
4. 若要安裝 SSPR，請執行以下指令：

   ```
   ./install.sh
   ```
5. 通讀授權合約。
6. 輸入 `y` 以接受授權合約。
7. (視情況而定) 設定 SSPR。如需詳細資訊，請參閱 「設定 SSPR」(第 86 頁)。

以靜默模式安裝 SSPR

1. 從 NetIQ 下載網站下載 `Identity_Manager_4.9.0_Linux.iso`。
2. 掛接下載的 `.iso`。
3. 從 `.iso` 檔案的根目錄導覽至 `sspr` 目錄。

   附註：根據您的要求編輯 `sspr_silentinstall.properties` 檔案。
4. 若要執行靜默安裝，請執行以下指令：

   ```
   ./install.sh -s -f sspr_silentinstall.properties
   ```
5. (視情況而定) 設定 SSPR。如需詳細資訊，請參閱 「設定 SSPR」(第 86 頁)。

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。

互動安裝

1. 從 NetIQ 下載網站下載 `Identity_Manager_4.9.0_RL_Linux.iso`。
2. 掛接下載的 `.iso`。
3. 從掛接位置執行以下指令：

   ```
   ./install.sh
   ```
4. 通讀授權合約。
5. 輸入 `y` 以接受授權合約。

靜默安裝

1. 從 NetIQ 下載網站下載 `Identity_Manager_4.9.0_RL_Linux.iso`。
2. 掛接下載的 `.iso`。
3. 從 `.iso` 的根目錄中，執行以下指令：

   `./create_silent_props.sh`
4. 輸入 `y` 以確認建立檔案。
5. 指定檔案的位置。
6. 對於**是否要為 Docker 容器設定靜默內容檔案**參數，請指定 *n*。
7. 執行以下指令以執行靜默安裝：

   `./install.sh -s -f <location of the silent properties file>`

   例如：

   `./install.sh -s -f /home/silent.properties`，其中，`/home/silent.properties` 是靜默內容檔案的儲存位置。

安裝 Designer

您可以使用圖形使用者介面或主控台模式來安裝 Designer。

1. 從軟體授權和下載 (https://sld.microfocus.com/index) 入口網站下載 `Identity_Manager_4.9.0_Designer_Linux.tar.gz`。
2. 導覽至要擷取檔案的目錄。
3. 執行以下指令：

   `tar -zxvf Identity_Manager_4.9.0_Designer_Linux.tar.gz`
4. 執行以下指令之一來安裝 Designer。

   主控台：`./install -i console`

   圖形使用者介面：`./install`
5. 依照提示操作並繼續安裝。

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。

本節提供有關安裝 Analyzer 以及為其設定環境的各種方式的資訊。

- 使用精靈安裝 Analyzer
- 以靜默模式安裝 Analyzer
- 將 XULRunner 新增至 Analyzer.ini 中

使用精靈安裝 Analyzer

以下程序描述如何透過圖形使用者介面或主控台使用安裝精靈在 Linux 或 Windows 平台上安裝 Analyzer。若要執行靜默模式的無人管理安裝，請參閱「以靜默模式安裝 Analyzer」(第 68 頁)。

1. 以 root 或管理員身分登入您要安裝 Analyzer 的電腦。
2. (視情況而定) 如果您已下載 Analyzer 安裝檔案，請完成以下步驟：
   - **2a** 導覽至所下載影像的 .tgz 或 win.zip 檔案。
   - **2b** 將該檔案的內容擷取到本地電腦上的某個資料夾中。
3. 執行安裝程式：

   ```
   ./install
   ```
4. 依照精靈中的指示操作，直到完成 Analyzer 的安裝。
5. 安裝程序完成後，檢閱安裝後摘要，以驗證 Analyzer 的安裝狀態及其記錄檔案的位置。
6. 按一下「完成」。
7. (視情況而定) 完成「將 XULRunner 新增至 Analyzer.ini 中」(第 69 頁)中的步驟。
8. 啟用 Analyzer。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 Analyzer」(啟用 Analyzer)。

以靜默模式安裝 Analyzer

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。相反，InstallAnywhere 將使用預設 analyzerInstaller.properties 檔案中的資訊。您可以使用預設檔案執行靜默安裝，或者編輯該檔案以自訂安裝程序。

依預設，安裝程式會在 root/Analyzer 目錄中安裝 Analyzer。

1. 以 root 或管理員身分登入您要安裝 Analyzer 的電腦。
2. 如果您已從軟體和授權頁面 (https://sld.microfocus.com/) 下載 Analyzer 安裝檔案，請完成以下步驟：
   - **2a** 導覽至所下載影像的 .tgz 或 win.zip 檔案。
   - **2b** 將該檔案的內容擷取到本地電腦上的某個資料夾中。
3. (選擇性) 若要指定非預設安裝路徑，請完成以下步驟：
   - **3a** 開啟 analyzerInstaller.properties 檔案 (預設位於 < 檔案解壓縮位置 >/analyzer_install/ 目錄中)。
   - **3b** 將以下文字新增至該 properties 檔案中：

     ```
     USER_INSTALL_DIR=installation_path
     ```
4. 若要執行靜默安裝，請從內容檔案所在的目錄執行以下指令：

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

5 (視情況而定) 在 Linux 電腦上，完成 「將 XULRunner 新增至 Analyzer.ini 中」 (第 69 頁) 中的步驟。

6 啟用 Analyzer。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 Analyzer」 (啟用 Analyzer)。

將 XULRunner 新增至 Analyzer.ini 中

在 Linux 平台上執行 Analyzer 之前，必須變更 XULRunner 對應。

1 安裝 XULRunner。

2 導覽至預設位於以下位置的 `Analyzer` 安裝目錄：

```
root/analyzer
```

3 在 gedit 編輯器中開啟 `Analyzer.ini` 檔案。

4 在參數清單的末尾新增下面的行：

```
-Djava.util.Arrays.useLegacyMergeSort=true
-Dorg.eclipse.swt.internal.gtk.disablePrinting
-Dorg.eclipse.swt.browser.XULRunnerPath=/opt/xulrunner
```

5 儲存 `Analyzer.ini` 檔案。

6 啟動 Analyzer。

安裝 Sentinel Log Management for Identity Governance and Administration

您可以使用以下方法來安裝 Sentinel Log Management：

- 以 root 使用者身分安裝 Sentinel Log Management
- 以非 root 使用者身分安裝 Sentinel Log Management

附註：在安裝之前，請驗證是否正確指定了主機名稱；不應啟用 IPV6 設定。

以 Root 使用者身分安裝 Sentinel Log Management

1 從 NetIQ 下載網站下載 `SentinelLogManagementForIGA8.6.1.0.tar.gz`。

2 導覽至要擷取檔案的目錄。

3 執行以下指令來擷取檔案

```
tar -zxvf SentinelLogManagementForIGA8.6.1.0.tar.gz
```

4 導覽至 `SentinelLogManagementforIGA` 目錄。

5 執行以下指令：

```
./install.sh
```

6 輸入 y 以接受授權合約並繼續安裝。

安裝作業會利用幾秒鐘的時間來載入安裝套件。

7 指定 2 以執行 SLM for IGA 的自訂組態。

8 輸入 1 以使用預設的試用版授權金鑰 .

或

輸入 2 以輸入為 SLM for IGA 購買的授權金鑰。

9 指定管理員使用者 (admin) 的密碼，並再次確認密碼。

10 指定資料庫使用者 (dbauser) 的密碼，並再次確認密碼。

dbauser 帳戶是 SLM for IGA 用來與資料庫互動的身分。您在此處輸入的密碼可用來執行資料庫維護工作，包括在忘記或遺失管理員密碼時重設管理員密碼。

11 指定應用程式使用者 (appuser) 的密碼，並再次確認密碼。

12 透過輸入所需的連接埠號碼變更連接埠指定。

例如，Web 伺服器的預設連接埠為 8443。若要修改 Web 伺服器的連接埠號碼，請指定 4。為 Web 伺服器輸入新的連接埠值，例如，8643。

13 變更連接埠後，請指定 8 來完成作業。

14 輸入 1 ，僅以內部資料庫來驗證使用者。

或

如果您已在網域中設定 LDAP 目錄，請輸入 2 以利用 LDAP 目錄驗證來驗證使用者。

預設值為 1。

15 當系統提示您啟用 FIPS 140-2 模式時，請輸入 n。

16 當系統提示您啟用可擴充儲存時，請輸入 n。

安裝即告完成，伺服器會隨之啟動。由於系統會執行一次性的啟始化，因此在安裝完成後所有服務都需要幾分鐘的時間才能啟動。等到安裝完成後，再登入 Sentinel 伺服器。

若要存取 SLM for IGA 主要介面，請在網頁瀏覽器中指定如下 URL：

```
https://<IP_Address/DNS_SLM for IGA_server>:<port>/sentinel/views/
main.html
```

其中，*<IP_Address/DNS_SLM for IGA_server>* 是 SLM for IGA 伺服器的 IP 位址或 DNS 名稱，*<port>* 是 SLM for IGA 伺服器的連接埠。

以非 Root 使用者身分安裝 Sentinel Log Management

您必須以 novell 使用者身分安裝 Sentinel Log Management。NetIQ 不支援 novell 使用者以外的非 root 使用者安裝，雖然安裝會順利地進行。

1 建立名為 novell 的非 root 使用者。

```
useradd novell
```

2 建立名為 novell 的非 root 群組。

```
groupadd novell
```

3 建立用於安裝 Sentinel 的目錄。

```
mkdir /home/slmnonroot
```

4 為 novell 使用者指定對非根目錄的安裝目錄的許可權。

```
chown novell:novell /home/slmnonroot
```

5 設定適當的密碼。

```
sudo passwd < 密碼 >
```

6 以 novell 使用者身分登入。

7 從 NetIQ 下載網站下載 SentinelLogManagementForIGA8.6.1.0.tar.gz。

8 導覽至要擷取檔案的目錄。

9 執行以下指令來擷取檔案

```
tar -zxvf SentinelLogManagementForIGA8.6.1.0.tar.gz
```

10 導覽至 SentinelLogManagementforIGA 目錄。

11 執行以下指令：

```
./install.sh --location=/home/slmnonroot
```

12 依照「以 Root 使用者身分安裝 Sentinel Log Management」(第 69 頁) 中的步驟 6 至 16 操作。

安裝 Java 遠端載入器

您需要在作業系統與原生遠端載入器不相容的電腦上安裝 Java 遠端載入器 dirxml_jremote。不過，Java 遠端載入器也可以在您可能安裝了原生遠端載入器的同一部伺服器上執行。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。您可以在裝有任何公開支援的 Java 版本的任何受支援 Linux 電腦上安裝 dirxml_jremote。

1 在代管 Identity Manager 引擎的伺服器上，複製預設位於 /opt/novell/eDirectory/lib/dirxml/classes 目錄中的應用程式 Shim .iso 或 .jar 檔案。

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 若要存取安裝程式，請完成下列其中一個步驟：

4a (視情況而定) 如果您已獲取 Identity Manager 安裝套件的 .iso 影像檔，請導覽至包含 Java 遠端載入器安裝檔案的目錄 (預設為 /IDM/packages/java_remoteloader)。

4b (視情況而定) 如果您已從軟體和授權頁面 (https://sld.microfocus.com/) 下載了 Java 遠端載入器安裝檔案，請完成以下步驟：

4b1 導覽至所下載影像的 .tgz 檔案。

4b2 將該檔案的內容擷取到本地電腦上的某個資料夾中。

5 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 /usr/idm 中。

6 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。

7 在目標電腦上，解壓縮並擷取 .tar.gz 檔案。

例如 tar -zxvf dirxml_jremote.tar.gz

8 將您在步驟 1 中從 dirxml/classes 目錄複製的應用程式 shim 的 .iso 或 .jar 檔案放在 lib 目錄下。

9 若要自訂 dirxml_jremote 程序檔，以便能夠透過 RDXML_PATH 環境變數存取 Java 可執行檔，請完成下列其中一個步驟：

9a 輸入下列其中一個指令，以設定環境變數 RDXML_PATH：

- set RDXML_PATH=path
- export RDXML_PATH

9b 編輯 dirxml_jremote 程序碼，並在執行 Java 的程序碼行上，將路徑預增至 Java 執行檔。

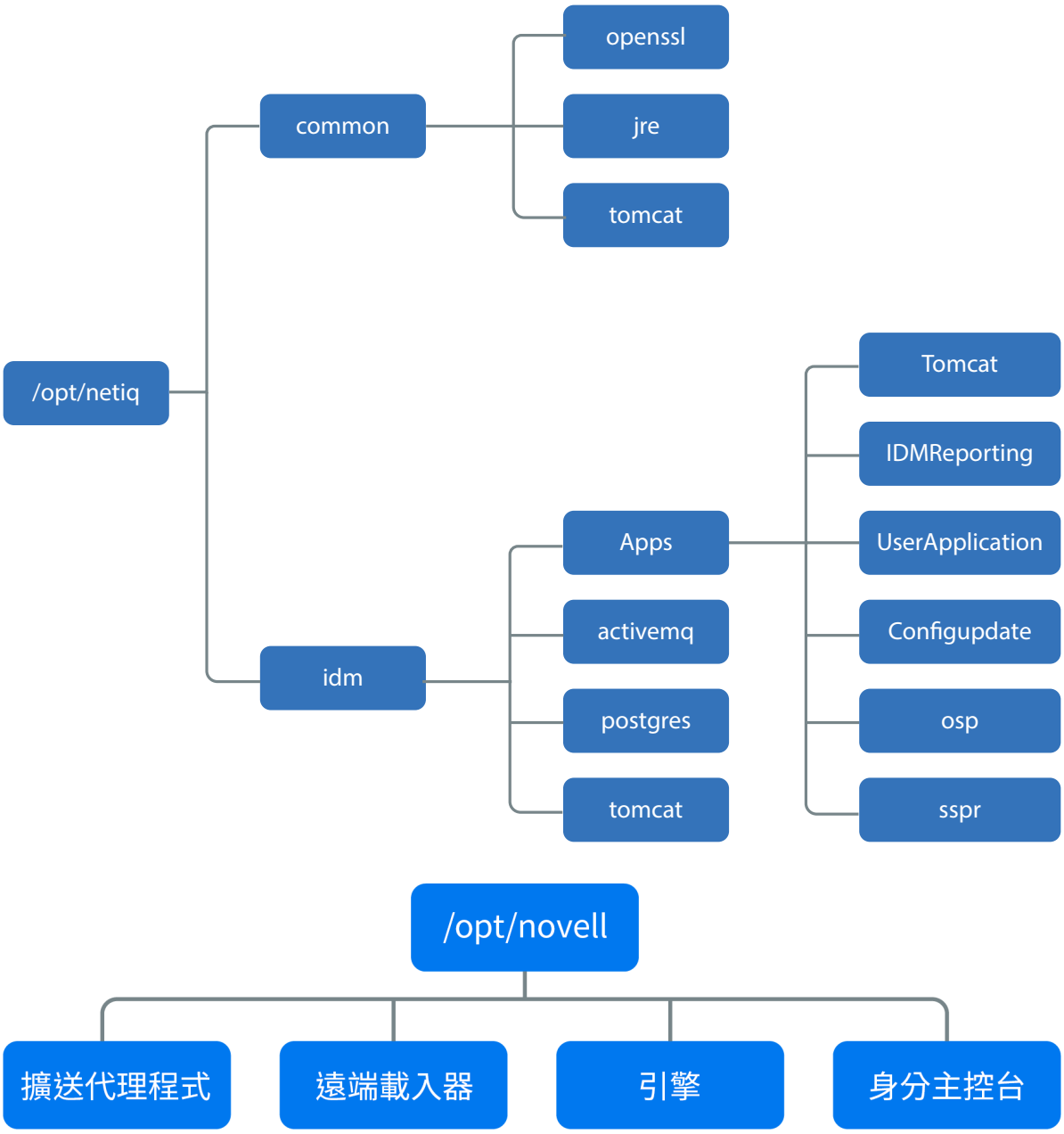
10 必須在 dirxml_jremote 程序檔中指定 jar 檔案的位置。這些檔案位於 dirxml_jremote.tar.gz 解壓縮目錄的 lib 子目錄中。例如，/lib/*.jar。

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

依預設，該範例檔案位於 /opt/novell/dirxml/doc 目錄中。如需詳細資訊，請參閱「設定遠端載入器和驅動程式」(第 90 頁)。

瞭解目錄結構

安裝程序會建立以下目錄結構：



- `/opt/netiq` 目錄是目錄結構的起始點。其他每個檔案和目錄都在此目錄下。
- `common` 目錄包含支援軟體。此軟體會在需要它的元件之間共享。
- `idm` 目錄包含元件特定的子目錄，其中包括用於安裝和設定元件的二進位檔案。
- 引擎、擴送代理程式、遠端載入器和 Identity Console 安裝在 `/opt/novell` 目錄中。

5 設定 Identity Manager 的元件

本章將引導您完成設定 Identity Manager 元件的過程。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「瞭解組態參數」(第 75 頁)。

某些元件 (例如 Designer、Analyzer、遠端載入器和擴送代理程式) 可能不需要組態。

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。

瞭解組態參數

本節定義設定 Identity Manager 安裝需要指定的參數。您可以使用安裝程式在安裝元件後立即對其進行設定，也可以稍後執行 `configure.sh` 程序檔來設定。

附註：

- 在一般組態模式下設定的 Identity Applications 和 Identity Reporting 無法連接至另一部電腦上安裝的資料庫伺服器。
- 安裝程序不允許您為 Identity Manager 元件啟用稽核。您必須在完成安裝後為每個元件設定稽核。如需詳細資訊，請參閱《*NetIQ Identity Manager - Configuring Auditing in Identity Manager*》(NetIQ Identity Manager - 在 Identity Manager 中設定稽核)。
- Identity Vault 將隨 OES 一併自動安裝。若要在 OES 平台上設定 Identity Manager 引擎，必須依次選取**自訂組態**和**新增至現有 Vault**。
- 確定使用 FQDN 或 IP 位址以統一方式設定 Identity Applications、Identity Reporting 和資料庫。換而言之，不能使用 FQDN 和 IP 位址的組合來設定這些元件。
- 對於容器，建議指定 FQDN 值，而不要指定 IP 位址。

表格 5-1 介紹了在一般模式下設定 Identity Manager 元件所需的參數。

表格 5-1 *一般組態*

參數	靜默內容檔案中的參數	一般組態
Identity Manager 引擎		

參數	靜默內容檔案中的參數	一般組態
通用密碼	IS_COMMON_PASSWORD	指定是否要設定通用密碼。
Identity Vault 主機名稱 /IP 位址	ID_VAULT_HOST	指定安裝了 Identity Vault 的伺服器的 IP 位址。
Identity Vault 管理員名稱	ID_VAULT_ADMIN_LDAP	指定網路樹中管理員物件的相對可辨識名稱 (RDN)，該管理員至少對要新增此伺服器的網路位置擁有完整權限。
Identity Applications		
通用密碼	IS_COMMON_PASSWORD	指定是否要設定通用密碼。確定密碼符合 「在組態期間使用不可猜出的密碼」(第 75 頁) 章節中指定的注意事項。
通用 One SSO 服務密碼	SSO_SERVICE_PWD	指定 One SSO 伺服器的驗證服務密碼。
SSPR 組態密碼		指定 SSPR 的驗證服務密碼。
Identity Applications 管理員名稱	UA_ADMIN	指定 Identity Applications 管理員帳戶的名稱。
Identity Applications 管理員密碼		指定 Identity Applications 的管理員密碼。
Identity Applications 和工作流程引擎資料庫使用者密碼		指定 Identity Applications 和工作流程引擎資料庫使用者密碼。
Identity Applications 和工作流程引擎資料庫管理員密碼		指定 Identity Applications 和工作流程引擎資料庫管理員密碼。
NGINX 連接埠	NGINX_HTTPS_PORT	指定 NGINX 連接埠。
Identity Reporting		
通用密碼	IS_COMMON_PASSWORD	指定是否要設定通用密碼。確定密碼符合 「在組態期間使用不可猜出的密碼」(第 75 頁) 章節中指定的注意事項。
Identity Reporting 資料庫帳戶密碼	RPT_DATABASE_SHARE_PASSWORD	指定 Identity Reporting 的資料庫帳戶密碼。
Identity Reporting 管理員名稱	RPT_ADMIN	指定 Identity Reporting 的管理員名稱。預設值為 cn=uaadmin,ou=sa,o=data。
Identity Reporting 管理員密碼		指定管理員物件的密碼。例如，*password*。
Identity Console		
Identity Console 伺服器名稱	ID_CONSOLE_SERVER_HOST	指定用於代管 Identity Console 的伺服器名稱。

參數	靜默內容檔案中的參數	一般組態
Identity Console 伺服器連接埠	ID_CONSOLE_SERVER_SSL_PORT	指定用於代管 Identity Console 的連接埠。
用於透過 Identity Console 進行授權的 OSP	ID_CONSOLE_USE_OSP	指定您是否要選擇使用 OSP 透過 Identity Console 進行授權 (y/n)。
One SSO 服務密碼	SSO_SERVICE_PWD	*僅當您已選擇透過 OSP 進行授權時 (即前面選擇了是) 才適用。* 指定 One SSO 服務密碼。
可信根證書資料夾路徑	ID_CONSOLE_CA_CERT_LOCATION	指定可信根證書 (SSCert.pem) 資料夾路徑。
伺服器證書路徑，包括檔案名稱	ID_CONSOLE_SERVER_CERT_LOCATION	指定伺服器證書路徑，包括檔案名稱。
伺服器證書密碼	ID_CONSOLE_SERVER_CERT_PASSWD	指定伺服器證書密碼。

表格 5-2 介紹了在自訂模式下設定 Identity Manager 元件所需的參數。

表格 5-2 *自訂組態*

參數	靜默內容檔案中的參數	自訂組態
Identity Manager 引擎		
建立新的 Identity Vault	TREE_CONFIG	指定要安裝的 Identity Vault。
新增至本地機器上的現有 Identity Vault		指定是否要連接至要安裝 Identity Manager 引擎的同一部伺服器上的現有 Identity Vault。
新增至遠端機器上的現有 Identity Vault		指定是否要連接至未與 Identity Manager 引擎安裝到同一部伺服器上的 Identity Vault。
Identity Vault 網路樹名稱	ID_VAULT_TREENAME	為 Identity Vault 指定新的網路樹。網路樹名稱必須符合以下要求： ◆ 網路樹名稱在網路中必須是唯一的。 ◆ 網路樹名稱的長度必須為 2 至 32 個字元。 ◆ 網路樹名稱只能包含字母 (A-Z)、數字 (0-9)、連字號 (-) 和底線 (_) 之類的字元。 **附註：**如果您要在 OES 上安裝 Identity Manager，請指定現有的樹狀結構名稱。
Identity Vault 伺服器名稱	ID_VAULT_SERVERNAME	指定 Identity Vault 伺服器名稱。

參數	靜默內容檔案中的參數	自訂組態
Identity Vault 網路位置 DN	ID_VAULT_SERVER_CONTEXT	指定現有 Identity Vault 伺服器的網路位置 DN。預設值為 servers.system。
Identity Vault 管理員名稱	ID_VAULT_ADMIN_LDAP	指定網路樹中管理員物件的相對可辨識名稱 (RDN)，該管理員至少對要新增此伺服器的網路位置擁有完整權限。
Identity Vault 管理員密碼	ID_VAULT_PASSWORD	指定管理員物件的密碼。例如，*password*。
RSA 金鑰大小	ID_VAULT_RSA_KEYSIZE	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	ID_VAULT_EC_CURVE	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	ID_VAULT_CA_LIFE	*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)。
NDS var 資料夾位置	ID_VAULT_VARDIR	指定此 Identity Vault 例項在此伺服器上的路徑。預設路徑為 /var/opt/novell/eDirectory。
NDS 資料位置	ID_VAULT_DIB	指定本地系統中要安裝目錄資訊資料庫 (DIB) 檔案的路徑。DIB 檔案是您的 Identity Vault 資料庫檔案。預設位置為 /var/opt/novell/eDirectory/data/dib。
NCP 連接埠	ID_VAULT_NCP_PORT	指定 Identity Vault 用來與 Identity Manager 各元件通訊的 NetWare 核心協定 (NCP) 連接埠。預設值為 524。
LDAP 非 SSL 連接埠	ID_VAULT_LDAP_PORT	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 SSL 連接埠	ID_VAULT_LDAPS_PORT	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。
Identity Vault HTTP 連接埠	ID_VAULT_HTTP_PORT	指定 HTTP 堆疊以純文字格式運作所需使用的連接埠。預設值為 8028。
Identity Vault HTTPS 連接埠	ID_VAULT_HTTPS_PORT	指定 HTTP 堆疊採用 TLS/SSL 通訊協定運作所需使用的連接埠。預設值為 8030。
含路徑的 NDS 組態檔案	ID_VAULT_CONF	指定 Identity Vault 組態檔案的位置。預設值為 /etc/opt/novell/eDirectory/conf/nds.conf。
Identity Vault 驅動程式集名稱	ID_VAULT_DRIVER_SET	為新的 Identity Manager 驅動程式集物件指定名稱。
Identity Vault 驅動程式集部署網路位置	ID_VAULT_DEPLOY_CTX	指定要在其中建立驅動程式集物件的容器的 LDAP DN。

參數	靜默內容檔案中的參數	自訂組態
Identity Applications		
通用密碼	IS_COMMON_PASSWORD	指定是否要設定通用密碼。確定密碼符合「在組態期間使用不可猜出的密碼」(第 75 頁) 章節中指定的注意事項。
主機名稱 (小寫 FQDN)	UA_SERVER_HOST	指定伺服器完全合格的可辨識名稱或預設 IP 位址。 **附註：**確定以小寫字元指定 FQDN。另外，必須將代管元件的伺服器設定為使用小寫 FQDN。
Identity Vault 主機名稱 /IP 位址	ID_VAULT_HOST	指定安裝了 Identity Vault 的伺服器的 IP 位址或主機名稱。
Identity Vault 管理員名稱	ID_VAULT_ADMIN_LDAP	指定網路樹中管理員物件的相對可辨識名稱 (RDN)，該管理員至少對要新增此伺服器的網路位置擁有完整權限。
Identity Vault 管理員密碼	ID_VAULT_PASSWORD	指定管理員物件的密碼。例如，*password*。
OSP 自訂登入畫面名稱	OSP_CUSTOM_NAME	指定將顯示在 OSP 登入畫面上的名稱。
使用者搜尋容器 DN	USER_CONTAINER	指定 Identity Vault 中所有使用者物件的預設容器。
管理員搜尋容器 DN	ADMIN_CONTAINER	指定 Identity Vault 中包含驗證服務 (OSP) 必須驗證的任何管理員使用者物件的容器可辨識名稱。例如 `o=data`。
應用程式伺服器 DNS/IP 位址	TOMCAT_SERVLET_HOSTNAME	指定 Tomcat 伺服器的 IP 位址或主機名稱。
One SSO 伺服器 SSL 連接埠	SSO_SERVER_SSL_PORT	指定單一登入服務要使用的連接埠。預設值為 `8543`。
Identity Application One SSO 服務密碼	SSO_SERVICE_PWD	*僅當將通用密碼設定為否時才適用。* 指定 Identity Applications 使用的單一登入用戶端的密碼。
Identity Applications 管理員名稱	UA_ADMIN	指定 Identity Applications 管理員帳戶的名稱。
SSPR 組態密碼	CONFIGURATION_PWD	*僅當將通用密碼設定為否時才適用。* 指定 Identity Applications 用於進行密碼管理的密碼。
OAuth 金鑰儲存區密碼	OSP_KEYSTORE_PWD	*僅當將通用密碼設定為否時才適用。* 指定您要建立以用於在 OAuth 伺服器上載入新金鑰儲存區的密碼。

參數	靜默內容檔案中的參數	自訂組態
資料庫平台	UA_DB_PLATFORM_OPTION	指定 Identity Applications 所需的資料庫。
在目前伺服器上設定 PostgreSQL	INSTALL_PG_DB	指定是否要在同一部伺服器上設定 PostgreSQL 資料庫。
Identity Applications 資料庫連接埠	UA_DB_PORT	指定 Identity Applications 的資料庫連接埠。
Identity Applications 資料庫名稱	UA_DATABASE_NAME	指定資料庫的名稱。預設值為 idmuserappdb。
Identity Applications 資料庫和工作流程引擎使用者名稱	UA_WFE_DATABASE_USER	指定 Identity Applications 資料庫管理員的使用者名稱 .
使用者 postgres 的 Identity Applications 和工作流程引擎資料庫管理員密碼	UA_WFE_DATABASE_ADMIN_PWD	指定使用者 postgres 的 Identity Applications 和工作流程引擎資料庫管理員密碼
使用自訂容器做為根容器	ENABLE_CUSTOM_CONTAINER_CREATION	指定是否要使用自訂容器做為根容器。依預設，安裝程式會建立 o=data 並選取它做為使用者容器，然後指定密碼規則和所需的託管者權限。 若要建立自訂容器，請選擇是。
建立 Identity Applications 的使用者應用程式及角色與資源服務驅動程式	UA_CREATE_DRIVERS	指定是否要安裝 UA 和 RRSD 驅動程式。如果您選取 **N**，則必須指定現有使用者應用程式驅動程式的名稱。
現有使用者應用程式驅動程式的名稱	UA_DRIVER_NAME	僅當您已將用於建立 UA 和 RRSD 驅動程式的值設定為否時才適用。 指定現有使用者應用程式驅動程式 DN 詳細資料。
使用者應用程式工作流程引擎 ID	UA_WORKFLOW_ENGINE_ID	指定 Identity Applications 工作流程引擎 ID。
Identity Applications 和工作流程引擎資料庫平台	UA_WFE_DB_PLATFORM_OPTION	指定 Identity Applications 和工作流程引擎資料庫平台。支援的值為 Postgres、Oracle 和 MsSQL。
Identity Applications 和工作流程引擎資料庫連接埠	UA_WFE_DB_PORT	指定 Identity Applications 和工作流程引擎資料庫連接埠。
工作流程引擎資料庫名稱	WFE_DATABASE_NAME	指定工作流程引擎資料庫名稱 . 預設資料庫名稱為 igaworkflowdb。
Identity Applications 和工作流程引擎資料庫密碼	UA_WFE_DATABASE_PWD	指定 Identity Applications 和工作流程引擎資料庫密碼。

參數	靜默內容檔案中的參數	自訂組態
Identity Applications 和工作流程引擎資料庫 JDBC 驅動程式 jar 檔案	UA_WFE_DB_JDBC_DRIVER_JAR	指定資料庫平台的 JAR 檔案。
建立綱要	UA_WFE_DB_CREATE_OPTION	當您要在安裝過程中為 Identity Applications 和工作流程引擎建立資料庫綱要時，請指定該參數。可用選項有現在、啟動和檔案。
建立新資料庫，或者從工作流程引擎的現有資料庫升級 / 移轉	WFE_DB_NEW_OR_EXIST	指定是要在新資料庫中建立表，還是從工作流程引擎的現有資料庫更新 / 升級。支援的值為 new 和 exist。
建立新資料庫，或者從 Identity Applications 的現有資料庫升級 / 移轉	UA_DB_NEW_OR_EXIST	指定是要建立新資料庫，還是從現有資料庫升級。
根容器	ROOT_CONTAINER	指定根容器。預設值為 o=data。
群組搜尋根容器 DN	GROUP_ROOT_CONTAINER	指定群組搜尋根容器的 DN。
Identity Applications 自訂證書	CUSTOM_UA_CERTIFICATE	指定是否要為 Identity Applications 使用自訂證書
自訂容器 LDIF 檔案路徑		*僅當將自訂容器設定為*是時適用。 為自訂容器指定 LDIF 檔案的路徑。
NGINX 連接埠	NGINX_HTTPS_PORT	指定 NGINX 連接埠。
Identity Reporting		
通用密碼	IS_COMMON_PASSWORD	指定是否要設定通用密碼。確定密碼符合 「在組態期間使用不可猜出的密碼」(第 75 頁) 章節中指定的注意事項。
主機名稱 (小寫 FQDN)		指定伺服器完全合格的可辨識名稱或預設 IP 位址。 **附註：**確定以小寫字元指定 FQDN。另外，必須將代管元件的伺服器設定為使用小寫 FQDN。
Identity Vault 主機名稱 /IP 位址	ID_VAULT_HOST	指定安裝了 Identity Vault 的伺服器的 IP 位址或主機名稱。
Identity Vault 管理員名稱	ID_VAULT_ADMIN_LDAP	指定網路樹中管理員物件的相對可辨識名稱 (RDN)，該管理員至少對要新增此伺服器的網路位置擁有完整權限。
Identity Vault 管理員密碼	ID_VAULT_PASSWORD	指定管理員物件的密碼。例如，*password*。
應用程式伺服器 HTTPS 連接埠	TOMCAT_HTTPS_PORT	指定 Tomcat 伺服器在與用戶端電腦通訊時使用的 HTTPS 連接埠。預設值為 8543。

參數	靜默內容檔案中的參數	自訂組態
應用程式伺服器 DNS/IP 位址	TOMCAT_SERVLET_HOSTNAME	指定 Tomcat 伺服器的 IP 位址或主機名稱。
選取用於 Identity Reporting 的資料庫平台	RPT_DATABASE_PLATFORM_OPTION	指定要用於 Identity Reporting 的資料庫。
在目前伺服器上設定 PostgreSQL	INSTALL_PG_DB_FOR_REPORTING	指定是否要在同一部伺服器上設定 PostgreSQL 資料庫。
Identity Reporting 資料庫帳戶密碼	RPT_DATABASE_SHARE_PASSWORD	指定 Identity Reporting 的資料庫帳戶密碼。
建立新資料庫或從現有資料庫升級 / 移轉	RPT_DATABASE_NEW_OR_EXIST	指定是要建立新資料庫，還是從現有資料庫升級。
Identity Reporting 管理員名稱	RPT_ADMIN	指定 Identity Reporting 的管理員名稱。預設值為 cn=uaadmin,ou=sa,o=data。
Identity Reporting 管理員密碼	RPT_ADMIN_PWD	指定 Identity Reporting 的管理員密碼。
Identity Reporting 資料庫名稱	RPT_DATABASE_NAME	指定 Identity Reporting 的資料庫名稱。預設值為 idmrptdb。
Identity Reporting 資料庫使用者	RPT_DATABASE_USER	指定允許 Identity Reporting 存取和修改資料庫中資料的管理帳戶。預設值為 rptadmin。
Identity Reporting 資料庫主機		指定需要在其中建立資料庫的伺服器的 DNS 名稱或 IP 位址。
Identity Reporting 資料庫連接埠	RPT_DATABASE_PORT	指定用於連接資料庫的連接埠。預設連接埠為 5432。
Identity Application 資料庫 JDBC jar 檔案	RPT_DATABASE_JDBC_DRIVER_JAR	指定資料庫平台的 JAR 檔案。
包含主體交替名稱的 Identity Reporting Tomcat 金鑰儲存區檔案	RPT_COMM_TOMCAT_KEYSTORE_FILE	指定 Tomcat 金鑰儲存區檔案的位置。 **附註：**系統僅支援 PKCS 類型的自訂證書。
建立綱要	RPT_DATABASE_CREATE_OPTION	做為安裝程序的一部分，指出要在何時建立資料庫綱要。可用選項有現在、啟動和檔案。
為 Identity Reporting 建立 MSGW 和 DCS 驅動程式	RPT_CREATE_DRIVERS	指定是否要建立 MSGW 和 DCS 驅動程式。
NGINX HTTPS 連接埠	NGINX_HTTPS_PORT	指定 NGINX 的連接埠。
Identity Console		
Identity Console 伺服器名稱	ID_CONSOLE_SERVER_HOST	指定用於代管 Identity Console 的伺服器名稱。

參數	靜默內容檔案中的參數	自訂組態
Identity Console 伺服器連接埠	ID_CONSOLE_SERVER_SSL_PORT	指定用於代管 Identity Console 的連接埠。
用於透過 Identity Console 進行授權的 OSP	ID_CONSOLE_USE_OSP	指定您是否要選擇使用 OSP 透過 Identity Console 進行授權 (y/n)。
One SSO 服務密碼	SSO_SERVICE_PWD	*僅當您已選擇透過 OSP 進行授權時 (即前面選擇了是)* 才適用。 指定 One SSO 服務密碼。
可信根證書資料夾路徑	ID_CONSOLE_CA_CERT_LOCATION	指定可信根證書 (SSCert.pem) 資料夾路徑。
伺服器證書路徑，包括檔案名稱	ID_CONSOLE_SERVER_CERT_LOCATION	指定伺服器證書路徑，包括檔案名稱。
伺服器證書密碼	ID_CONSOLE_SERVER_CERT_PASSWD	指定伺服器證書密碼。
Identity Vault 網路樹名稱	ID_CONSOLE_TREENAME	輸入用於代管 Identity Console 的 Identity Vault 網路樹名稱。

建立和設定驅動程式集

使用 Identity Manager 安裝套件 IDM/LDIF/ 目錄中的 sample-driverset.ldif 檔案可協助您建立驅動程式集。該檔案包含以下內容：

```
dn: cn=driverset1,o=system
changetype: add
DirXML-LogLimit: 0
DirXML-ConfigValues::
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48Y29u

ZmlndXJhdGlvbi12YWx1ZXM+Cgk8ZGVmaW5pdGlvbnMvPgo8L2NvbmZpZ3VyYXRpb24tdmFsdW
VzPg==
objectClass: DirXML-DriverSet
objectClass: Top
objectClass: Partition
objectClass: nsimPasswordPolicyAux
```

```
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
description: This Password Policy is used by IDM Engine
nspmMaximumLength: 64
nspmConfigurationOptions: 596
passwordUniqueRequired: FALSE
passwordMinimumLength: 1
passwordAllowChange: TRUE
objectClass: nspmPasswordPolicy
objectClass: Top
cn: DirXML-PasswordPolicy
nsimAssignments: cn=driverset1,o=system
```

在全新安裝過程中建立驅動程式集

在文字編輯器中開啟 `sample-driverset.ldif` 檔案，並進行以下變更。如果您提供了自訂 LDIF 檔案路徑，請指定該自訂路徑：

1. 將驅動程式集 DN 指向新驅動程式集。例如，將 `dn: cn=driverset1,o=system` 變更為 `dn:cn=Driverset47,ou=drivers,o=acme`。
2. 將 `nsimAssignments` 屬性值變更為新驅動程式集的 DN。例如，將 `nsimAssignments: cn=driverset1,o=system` 變更為 `nsimAssignments: cn=Driverset47,ou=drivers,o=acme`。

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。

在現有伺服器上設定驅動程式集

如果已在 eDirectory 樹狀結構中的某部伺服器上安裝 Identity Manager，則該樹狀結構中會存在 DirXML-PasswordPolicy。您的選擇如下：

- **使用現有密碼規則**

  進行以下變更

  ```
  dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
  changetype: modify
  add: nsimAssignments
  nsimAssignments: cn=driverset1,o=system
  ```

- **使用其他密碼規則**

請使用

```
dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: add
```

在文字編輯器中開啟 `sample-driverset.ldif` 檔案，並進行以下變更：

1. 將驅動程式集 DN 指向新驅動程式集。
2. 將 nsimAssignments 屬性值變更為新驅動程式集的 DN。
3. 將 DirXML-PasswordPolicy 屬性變更為指向現有 DirXML-PasswordPolicy 物件或其他密碼規則。

設定 Identity Manager 的元件

您可透過以下方式執行組態：

- 互動組態
- 靜默組態

執行互動式組態

1. 導覽至掛接 `Identity_Manager_4.9.0_Linux.iso` 檔案的位置。
2. 在指令行中指定下列指令以執行 `configure.sh` 程序檔：

   ```
   ./configure.sh
   ```

3. 決定是要執行一般組態還是自訂組態。組態選項將因您選取要設定的元件而異。
4. 若要設定元件，請參閱 「瞭解組態參數」(第 75 頁) 中的資訊。

附註：在 Identity Manager 引擎組態設定期間，簡單繫結的 TLS 設定為 **Yes**。如果您要將簡單繫結的 TLS 值變更為 **No**，請在安裝 Identity Manager 引擎的伺服器上執行以下指令：

```
ldapconfig set "Require TLS for Simple Binds with Password=no"
```

執行靜默組態

1. 導覽至掛接 `Identity_Manager_4.9.0_Linux.iso` 檔案的位置。
2. 若要執行靜默安裝，請執行以下指令：

   ```
   ./configure.sh -s -f <location of the silent properties file>
   ```

   例如：

   `./configure.sh -s -f /home/silent.properties`，其中，`/home/silent.properties` 是靜默內容檔案的儲存位置。
3. 若要設定元件，請參閱 「瞭解組態參數」(第 75 頁) 中的資訊。

設定 SSPR

下列各節提供有關設定 SSPR 的資訊。在設定元件之前，請查看「瞭解組態參數」(第 75 頁)中的資訊。

附註：在設定 SSPR 之前，請確定 Identity Vault 中存在以下容器和使用者物件：

- 使用者搜尋容器
- 管理員搜尋容器
- Identity Applications 管理員使用者

執行互動式組態

1. 導覽至掛接 `Identity_Manager_4.9.0_Linux.iso` 的位置。
2. 導覽至 `sspr` 目錄。
3. 執行下列指令：

   ```
   ./configure.sh
   ```
4. 組態設定。

執行靜默組態

在開始組態之前，請確定已將 `sspr_silentinstall.properties` (`<iso 掛接路徑 >/sspr/`) 檔案複製到某個可寫入的目錄。例如，將該檔案複製到 `/tmp` 目錄。

1. 導覽至掛接 `Identity_Manager_4.9.0_Linux.iso` 的位置。
2. 導覽至 `sspr` 目錄。
3. 執行下列指令：

   `./configure.sh -s -f <location of the silent properties file>`

   例如：

   `./configure.sh -s -f /tmp/sspr_silentinstall.properties`，其中，`/tmp/sspr_silentinstall.properties` 是靜默內容檔案的儲存位置。
4. 組態設定。

在 OSP 伺服器上修改單一登入存取設定

如果將 SSPR 和 OSP 安裝在不同的伺服器上 (安裝 SSPR 的伺服器不同於安裝 Identity Applications 或 Identity Reporting 的伺服器)，則您必須在 OSP 伺服器上組態單一登入存取設定。本節的內容可協助您確保這些設定適合您的環境。

1. 在安裝 OSP 的伺服器上啟動 RBPM 組態更新公用程式。
2. 導覽至 **SSO 用戶端** > **Self Service Password Reset**。

3 在 **OSP OAuth 重新導向 URL** 欄位中指定 SSPR 伺服器詳細資料。例如 `https://<SSPR 主機名稱 IP>:連接埠 /sspr/public/oauth`。

4 按一下**確定**儲存所做的變更，然後關閉組態公用程式。

5 重新啟動 Tomcat 以使變更生效。

6 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 89 頁)
- 「將非管理員使用者設定為 Identity Vault 管理員」(第 90 頁)
- 「設定遠端載入器和驅動程式」(第 90 頁)
- 「設定已連接系統」(第 91 頁)
- 「設定忘記密碼管理功能」(第 94 頁)
- 「設定 Identity Applications」(第 98 頁)
- 「設定資料收集的執行時期環境」(第 128 頁)
- 「設定 Identity Reporting」(第 137 頁)
- 「完成非 Root 使用者安裝」(第 144 頁)
- 「啟用 Identity Manager」(第 145 頁)
- 「為分散式部署建立 SSL 證書」(第 146 頁)

設定 Identity Vault 的組態

- 建立 Identity Vault 的值索引
- 手動將 Identity Applications 和 Identity Reporting 證書輸入至 Identity Vault 中

建立 Identity Vault 的值索引

Identity Applications 必須能夠與 Identity Vault 中的物件互動。為了提高 Identity Applications 的效能，Identity Vault 管理員應該為 manager、和 srvprvUUID 屬性建立值索引。如果這些屬性沒有值索引，Identity Applications 使用者可能會遭遇效能不佳問題，這在叢集環境中尤為突出。

您可以在完成 Identity Applications 安裝後使用以下方法之一建立這些值索引：

- Identity Console。使用索引管理員。如需詳細資訊，請參閱《NetIQ eDirectory Administration Guide》(NetIQ eDirectory 管理指南) 中的「Creating an Index」(建立索引)。
- 組態公用程式。導覽至其他 > **Identity Vault 索引**，然後在伺服器 DN 中選取建立並指定 DN 值。按一下確定，然後重新啟動 Identity Vault 以儲存變更。

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（/opt/netiq/common/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 (/opt/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>
  ```

將非管理員使用者設定為 Identity Vault 管理員

如果 Identity Applications 設定為使用某個非管理員使用者做為 Identity Vault 管理員，該非管理員使用者必須對使用者所在子樹狀結構中的 oidpInstanceData 屬性擁有 [寫入] 許可權。否則，OSP 登入可能會失敗。

若要為非管理員使用者設定對 oidpInstanceData 屬性的寫入許可權，請執行以下操作：

1. 登入 Identity Console。
2. 在 **eDirectory** 檢視中，按一下**權限管理 > 修改託管者**。
3. 選取非管理員使用者物件，然後按一下**確定**。
4. 「託管者」即會顯示，按一下**指定的權限**。
5. 對 oidpInstanceData 屬性設定**比較**、**讀取**和**寫入**許可權。
6. 按一下**套用**以儲存並套用您的變更。

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，而無需在該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。一次只能有一個驅動程式集在伺服器上處於使用中狀態。您可以使用 Designer 工具來建立驅動程式集。

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 91 頁)
- 「將預設密碼規則指定給驅動程式集」(第 91 頁)
- 「在 Identity Vault 中建立密碼規則物件」(第 92 頁)
- 「建立自訂密碼規則」(第 93 頁)
- 「在 Identity Vault 中建立預設通知集合物件」(第 93 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 92 頁) 與「建立自訂密碼規則」(第 93 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 DirMXL-PasswordPolicy 物件，請執行以下動作以從檔案輸入屬性：

從包含 ldapmodify 公用程式的目錄中，輸入以下指令：

```
ldapmodify -x -c -h hostname_or_IP_address -p 389 -D
"cn=admin,ou=sa,o=system" -w password -f path_to_ldif_file
```

例如：

```
ldapmodify -x -ZZ -c -h server1.test.com -p 389 -D
"cn=admin,ou=sa,o=system" -w test123 -f /root/dirxmlpasswordpolicy.ldif
```

依預設，ldapmodify 公用程式位於 `/opt/novell/eDirectory/bin` 目錄中。

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 92 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/) 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。

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 94 頁)
- 「使用外部系統進行忘記密碼管理」(第 96 頁)
- 「針對分散式環境或叢集環境更新儀表板中的 SSPR 連結」(第 98 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，您也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 95 頁)
- 「為 Identity Manager 設定 Self Service Password Reset」(第 95 頁)
- 「鎖定 SSPR 組態」(第 96 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 RBPM 組態公用程式。如需詳細資訊，請參閱 「執行 Identity Applications 組態公用程式」(第 99 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 **SSPR**。
5. 選取**忘記密碼**。
6. 導覽至 **SSO 用戶端 > Self Service Password Reset**。
7. 對於 **OSP 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 **OSP 用戶端密碼**，請指定 SSPR 單一登入用戶端的密碼。
9. 對於 **OSP 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，然後關閉公用程式。

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* (https://www.netiq.com/documentation/self-service-password-reset-47/sspr-adminguide/data/bookinfo.html)》 (NetIQ Self Service Password Reset 管理指南) 中的「Configuring Self Service Password Reset (https://wwwtest.netiq.com/documentation/self-service-password-reset-47/sspr-adminguide/data/b14gnrxl.html)」 (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 96 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 97 頁)
- 「測試外部忘記密碼組態」(第 97 頁)
- 「設定應用程式伺服器之間的 SSL 通訊」(第 98 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 「執行 Identity Applications 組態公用程式」(第 99 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 98 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

- 「儲存 Configupdate 公用程式密碼」(第 99 頁)
- 「完成 Identity Applications 的設定」(第 99 頁)
- 「指定許可權索引的位置」(第 123 頁)
- 「部署適用於 Identity Applications 的 REST API」(第 124 頁)
- 「設定 Identity Applications 的 Oracle 資料庫」(第 124 頁)
- 「使用 Oracle 服務名稱存取 Oracle 資料庫」(第 125 頁)
- 「手動建立資料庫綱要」(第 126 頁)
- 「組態 Identity Applications 的單一登入設定」(第 127 頁)
- 「啟動 Identity Applications」(第 127 頁)
- 「Identity Applications 的組態和使用考量」(第 128 頁)

儲存 Configupdate 公用程式密碼

啟動 configupdate 時，系統將提示使用者輸入主金鑰儲存區 (encrypt-keys.pkcs12) 密碼。此密碼預設為 changeit。此金鑰儲存區位於 /opt/netiq/idm/apps/tomcat/conf。

執行以下步驟，以變更並重新加密密碼：

1. 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 /
   opt/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：

   ```
   /opt/netiq/common/jre/bin/java -cp /opt/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 /opt/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

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。您也可以在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.sh) 的檔案位於 /opt/netiq/idm/apps/configupdate 目錄中：

附註：

- 您應該只從 configupdate 目錄執行 configudate.sh。從自訂位置執行 configupdate.sh 將導致失敗。
- 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

1 在 configupdate.sh.properties 中，確認以下選項已正確設定：

```
edit_admin="true"

use_console="false"
```

附註：僅當您要以主控台模式執行該公用程式時，才應將 `-use_console` 的值設定為 `true`。

2 儲存並關閉 `configupdate.sh.properties`。

3 在指令提示符處，執行以下指令來執行組態公用程式：

```
./configupdate.sh
```

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。

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 100 頁)
- 「Identity Vault DN」(第 101 頁)
- 「Identity Vault 使用者身分」(第 104 頁)
- 「Identity Vault 使用者群組」(第 105 頁)
- 「Identity Vault 證書」(第 105 頁)
- 「電子郵件伺服器組態」(第 106 頁)
- 「可信金鑰儲存區」(第 108 頁)
- 「NetIQ Sentinel 數位簽名證書與金鑰」(第 108 頁)
- 「其他」(第 108 頁)
- 「容器物件」(第 110 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，會將它用做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.sh` 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.sh` 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.sh` 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.sh` 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.sh` 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。在 Linux 上，使用者必須具有寫入此檔案的許可權。

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。

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，`/opt/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，安裝程式會使用預設值 `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

若要提高 Identity Applications 的效能，可以為 manager、ismanager 和 srvprvUUID 屬性建立值索引。

您可以在完成 Identity Applications 安裝後，使用組態公用程式建立值索引。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。
- 若要建立索引，請在**伺服器 DN** 設定中選取**建立**，並指定**伺服器 DN** 的值。按一下**確定**，然後重新啟動 Identity Vault 以使變更生效。
- 若要刪除索引，請在**伺服器 DN** 設定中選取**刪除**，並指定**伺服器 DN** 的值。按一下**確定**，然後重新啟動 Identity Vault 以使變更生效。

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 110 頁)
- 「報告保留值」(第 111 頁)
- 「修改地區設定」(第 111 頁)
- 「職能組態」(第 111 頁)
- 「傳出代理」(第 112 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 `/opt/netiq/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

僅當使用 Identity Manager 4.8.1 或更新版本時才適用。

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 112 頁)
- 「驗證組態」(第 113 頁)
- 「驗證方法」(第 113 頁)
- 「密碼管理」(第 115 頁)
- 「Sentinel 數位簽名證書和金鑰」(第 116 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。

- **名稱和密碼**：OSP 使用 Identity Vault 確認驗證。

- **Kerberos**：OSP 接受來自 Kerberos 票證伺服器和 Identity Vault 的驗證。
- **SAML 2.0**：OSP 接受來自 SAML 身分提供者和 Identity Vault 的驗證。

啟用 reCAPTCHA

僅當您指定了名稱和密碼時才適用。

指定是否要在登入頁面上啟用 reCAPTCHA。

reCAPTCHA 會要求使用者確認他們不是傀儡程式，這提供了一層額外的安全防護。它會顯示一些影像，使用者必須依據相符準則選取相應影像。如果回應正確，Access Manager 將驗證使用者的驗證身分證明。如果回應不正確，Access Manager 將不會驗證使用者身分證明，而是重新導向至登入頁面。

啟用雙因素驗證

僅當您指定了名稱和密碼時才適用。

指定是否要啟用雙因素驗證。

這需要在第二個因素索引標籤中完成一些組態。如需詳細資訊，請參閱 「第二個因素參數」(第 121 頁)。

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。

啟用後援 reCAPTCHA

僅當您指定了 Kerberos 時才適用。

指定在無法使用 Kerberos 時，是否要透過後援使用者名稱和密碼啟用 reCAPTCHA。

需要啟用 reCAPTCHA 前的嘗試次數

僅當您選取了啟用後援 reCAPTCHA 核取方塊時才適用。

指定登入嘗試失敗多少次後啟用 reCAPTCHA。將值設定為零表示永遠需要啟用 reCAPTCHA。

網站金鑰

僅當您選取了啟用後援 reCAPTCHA 核取方塊時才適用。

指定從 Google reCAPTCHA 網站獲取的 reCAPTCHA 網站金鑰值。

私密金鑰

僅當您選取了啟用後援 reCAPTCHA 核取方塊時才適用。

指定從 Google reCAPTCHA 網站獲取的 reCAPTCHA 私密金鑰值。

啟用後援雙因素驗證

僅當您指定了 Kerberos 時才適用。

指定在無法使用 Kerberos 時，是否要透過後援使用者名稱和密碼啟用雙因素驗證。

這需要在第二個因素索引標籤中完成一些組態。如需詳細資訊，請參閱 「第二個因素參數」(第 121 頁)。

使用者登出抵達頁面

僅當您指定了 **Kerberos** *時才適用。*

指定是否要在成功登出後啟用抵達頁面，而不是重新導向至登入頁面。

抵達頁面

僅當您指定了 **SAML** *時才適用。*

- **無**：指定不使用抵達頁面。如果指定了 IDP URL，請選取此選項。
- **內部**：指定要使用內部 OSP 抵達頁面。
- **外部**：指定要將您重新導向至外部 OSP 抵達頁面。

URL

僅當您在 **抵達頁面** *欄位中選取了* **外部** *時才適用。*

指定外部抵達頁面的 URL。

中繼資料來源

僅當您指定了 **SAML** *時才適用。*

指定 IDP 中繼資料的來源。您可以從 URL 載入中繼資料，也可以複製先前獲取的中繼資料。

中繼資料 URL

僅當您在 **中繼資料 URL** 欄位中指定了 **URL** 時才適用。

指定是否要從 URL 載入中繼資料，並在結束應用程式之前將中繼資料儲存到組態中。

儲存時載入

僅當您在 **中繼資料 URL** 欄位中指定了 **URL** 時才適用。

指定 OSP 用來將驗證要求重新導向至 SAML 的 URL。

IDP 中繼資料

僅當您在 **中繼資料 URL** 欄位中指定了 **複製 / 粘貼** 時才適用。

指定您要粘貼的資料 (該資料從 SAML IDP 獲取)。

結束時設定 Access Manager

僅當您在 **中繼資料 URL** 欄位中指定了 **複製 / 粘貼** 時才適用。

指定是否要在 Access Manager 中自動設定 SAML 服務提供者定義。

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。

忘記密碼

僅當您要使用 SSPR 時，此核取方塊參數才適用。

指定是否希望使用者不聯絡服務台，自行復原忘記的密碼。

您還必須為「忘記密碼」功能設定處理安全回應規則。如需詳細資訊，請參閱 *《NetIQ Self Service Password Reset Administration Guide》*(https://wwwtest.netiq.com/documentation/self-service-password-reset-47/sspr-adminguide/data/bookinfo.html)(NetIQ Self Service Password Reset 管理指南)。

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
```

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

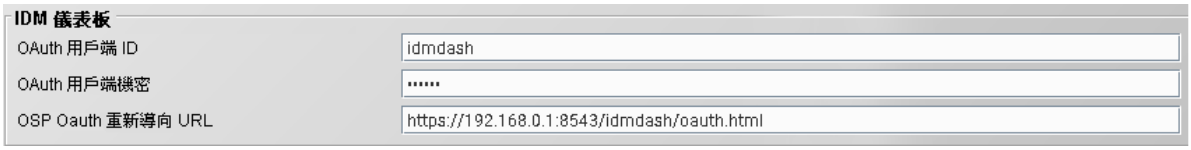
在設定 Identity Applications 時，此索引標籤定義用於管理對應用程式進行單一登入存取的值。

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 117 頁)
- 「IDM 管理員」(第 118 頁)
- 「RBPM」(第 118 頁)
- 「報告」(第 119 頁)
- 「IDM 資料收集服務」(第 120 頁)
- 「DCS 驅動程式」(第 120 頁)
- 「Self Service Password Reset」(第 120 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。



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

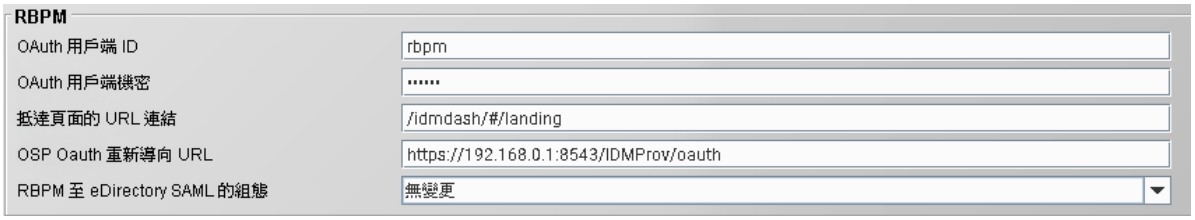
必需

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。



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`。

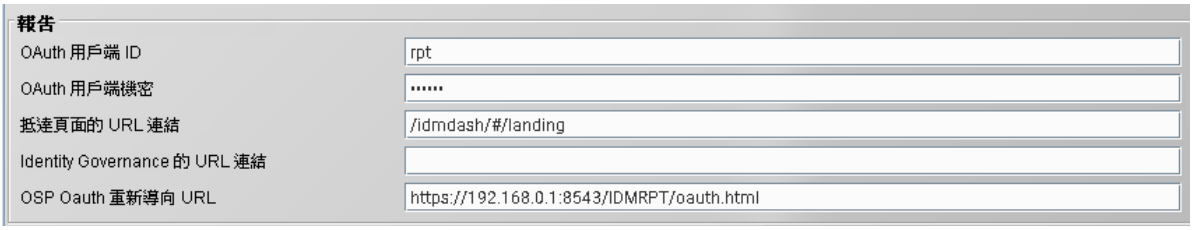
RBPM 至 eDirectory SAML 的組態

必需

指定 SSO 驗證所需的 RBPM 至 Identity Vault 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。



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

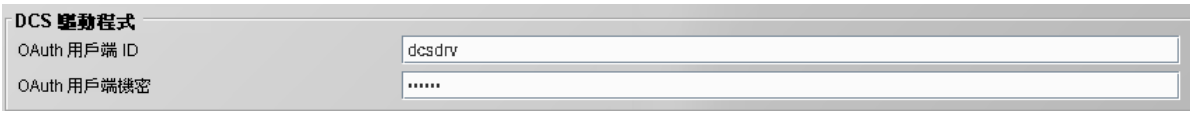
必需

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。



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。

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/sspr/public/oauth.html`。

第二個因素參數

在繼續後續操作之前，請確定已在進階驗證中建立了方法、驗證鏈和事件。您必須將 OSP 設定為接受來自進階驗證的驗證。

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：

AAF 管理員

此區段定義進階驗證管理員的設定：

管理員名稱 (儲存庫 \ 名稱)

必需

指定 OSP 用來與進階驗證進行互動的進階驗證管理員帳戶的儲存庫合格名稱。通常，該帳戶位於 LOCAL 儲存庫中。

預設的進階驗證管理員帳戶名稱為 admin。如果您已使用此帳戶，則管理員名稱值為：

LOCAL\admin (即儲存庫名稱 \ 使用者名稱)

管理員密碼

必需

指定上方所設定進階驗證管理使用者的密碼。

AAF 使用者儲存庫

此區段定義進階驗證使用者儲存庫的設定：

使用者儲存庫名稱

必需

指定您在進階驗證中所建立儲存庫的名稱。此儲存庫對應於 Identity Manager 的 Identity Vault。

AAF 伺服器

此區段定義進階驗證伺服器的設定：

允許測試 TLS 證書

必需

指定是否要忽略來自 AAF 伺服器的無效測試證書標題。這僅適用於初始組態和測試。

按一下**新增**，然後指定進階驗證伺服器的 DNS 名稱或 IP 位址。如果您使用的連接埠不是 443，另請指定所用的連接埠。

(視情況而定) 如果您已將進階驗證伺服器叢集化，請再次按一下**新增**，然後指定叢集中每部伺服器的每個 DNS 名稱或 IP 位址。

顯示調整參數

必需

指定是否要啟用調整參數。

登出工作階段清理 (分鐘)：*僅當您已選取**顯示調整參數**核取方塊時才適用。*

指定多久之後將使用中 AAF 登入工作階段視為發生逾時和清理問題。

活動訊號間隔 (毫秒)：*僅當您已選取**顯示調整參數**核取方塊時才適用。*

指定多久之後向 AAF 伺服器傳送活動訊號申請以檢查可用性。

AAF 端點

此區段定義進階驗證端點的設定：

建立新端點

必需

指定是否要建立用於雙因素驗證的新端點。

識別碼：*僅當您未選取**建立新端點**核取方塊時才適用。*

指定 AAF 管理中設定的端點識別碼。

秘密：*僅當您未選取**建立新端點**核取方塊時才適用。*

指定 AAF 管理中設定的端點機密。

名稱：*僅當您已選取**建立新端點**核取方塊時才適用。*

指定新端點的名稱，以用於在 AAF 管理頁面中識別該端點。

描述：*僅當您已選取**建立新端點**核取方塊時才適用。*

指定上方所設定新端點的描述。

第二個因素條件

此區段定義第二個因素條件的設定。

所有使用者，任何時間

必需

指定是否允許所有使用者在任何時間提供第二個因素驗證。

使用者登入條件：*僅當您未選取**所有使用者，任何時間**核取方塊時才適用。*

指定您可以定義要讓 Identity Manager 使用第二個因素驗證所需符合的特定運算式和條件。

第二個因素驗證方法

此區段定義進階驗證方法的設定。

指定是否要為不同的方法啟用第二個因素驗證。

若要對某個方法停用第二個因素驗證，請取消選取該方法名稱旁邊的核取方塊。

如果使用者已在多個方法中註冊，Identity Manager 將使用第二個因素方法的相對優先程度。

CEF 稽核參數

本節定義用於管理單一登入用戶端的 CEF 稽核參數的值。

傳送稽核事件

指定是否要使用 CEF 來稽核事件。

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。選取**使用 TLS** >「顯示進階選項」，並提供 **Identity Manager 金鑰儲存區檔案名稱**和 **Identity Manager 金鑰儲存區密碼**。

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。如果您要提供自選的中間事件儲存目錄，必須先確定該目錄的許可權和擁有權已變更為 `novlua`。若要變更目錄的許可權，請執行以下指令：

```
chown novlua:novlua <directory_path>
```

```
chmod 755 <directory_path>
```

其中，`<directory_path>` 是中間事件儲存目錄的路徑。

如需有關設定 CEF 稽核的完整文件，請參閱《*NetIQ Identity Manager - Configuring Auditing in Identity Manager*》(NetIQ Identity Manager - 在 Identity Manager 中設定稽核) 中的「Configuring Identity Applications」(設定 Identity Applications)。

指定許可權索引的位置

當您安裝 Identity Applications 時，安裝程序將為 Tomcat 建立一個許可權索引。如果您未指定該索引的位置，安裝程式會在暫存目錄中建立一個資料夾。例如，Tomcat 上的 `/opt/netiq/idm/apps/tomcat/temp/permindex`。

在測試環境中，該位置一般來說是無關緊要的。但是，在線上或預備環境中，您可能不想將許可權索引放在暫存目錄中。

若要指定索引的位置：

1. 停止 Tomcat。
2. 在文字編輯器中，開啟 `ism-configuration.properties` 檔案。
3. 在該檔案的末尾新增以下文字：

   `com.netiq.idm.cis.indexdir = path/permindex`

   例如：

   `com.netiq.idm.cis.indexdir = /opt/netiq/idm/apps/tomcat/temp/permindex`
4. 儲存然後關閉該檔案。
5. 刪除暫存目錄中現有的 `permindex` 資料夾。
6. 啟動 Tomcat。

若要為叢集啟用許可權索引，請參閱第 32 章 「Tomcat 應用程式伺服器上的 Identity Applications 叢集部署解決方案範例」 (第 353 頁)。

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`。

附註：若要輸出工作流程資料庫表，請在 `ism-configuration.properties` 檔案中新增下面一項：

```
com.microfocus.workflow.migration.tables = <list-of-tables-to-exported-comma-separated>
```

例如：

```
com.microfocus.workflow.migration.tables = afmodel,afform,
afprocess,afdocument,afactivity,afactivitytimertasks,afbranch,afcomment,af
provisioningstatus,afquorum,afworktask,configuration,email_approval_token,
localization,processed_eba_mails
```

設定 Identity Applications 的 Oracle 資料庫

執行以下步驟來設定 Oracle 資料庫：

1. 下載並安裝最新版本的 Oracle 資料庫。

該資料庫的預設 SID 為 orcl。

2 建立資料庫例項：

2a 在指令行中執行以下指令，以啟動資料庫組態助手 (Database Configuration Assistor)。

```
dbca
```

2b 在**全域資料庫名稱**欄位中指定資料庫名稱。例如 idappsdb。

3 建立資料庫使用者：

3a 登入 Oracle SQL 開發人員工具。

3b 執行以下指令：

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

其中，

idmadmin 表示使用者帳戶，

<password> 表示使用者密碼。

4 重複步驟 2 和 3 以設定工作流程引擎資料庫。

附註：為 Identity Applications 設定 Oracle 資料庫時，請確定使用上述章節中指定的相同詳細資料。

使用 Oracle 服務名稱存取 Oracle 資料庫

您可以使用 Oracle 系統 ID (SID) 和 Oracle 服務名稱連接至 Oracle 資料庫。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。您也可以在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 126 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：

```
/opt/netiq/idm/apps/UserApplication
```

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

```
/opt/netiq/common/jre/bin/java -Xms256m -Xmx256m  -
Dwar.context.name=IDMProv -Ddriver.dn="cn=User Application
Driver,cn=driverset1,o=system" -Duser.container="o=data" -jar /opt/
netiq/idm/apps/UserApplication/liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase --
driver=org.postgresql.Driver --classpath=/opt/netiq/idm/apps/
postgresql/postgresql-9.4.1212jdbc42.jar opt/netiq/idm/apps/
UserApplication/IDMProv.war --changeLogFile=DatabaseChangeLog.xml  --
url="jdbc:postgresql://localhost:5432/idmuserappdb" --
contexts="prov,newdb" --logLevel=info --logFile=/opt/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 126 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.service
```

```
systemctl restart netiq-activemq.service
```

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。
  - 確保 Identity Vault 的索引處於線上模式。如需在安裝期間或之後設定索引的詳細資訊，請參閱 「建立 Identity Vault 的值索引」(第 89 頁)。
  - 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 SSPR 可信證書輸入至 Identity Applications 伺服器的 `idm.jks` 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 129 頁)
- 「移轉資料收集服務驅動程式」(第 130 頁)
- 「新增對自訂屬性和物件的支援」(第 132 頁)
- 「新增多個驅動程式集支援」(第 134 頁)
- 「將驅動程式設定為使用 SSL 在遠端模式下執行」(第 136 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。如需軟體要求的詳細資訊，請參閱 「安裝 Identity Reporting 元件的注意事項」(第 54 頁)。
   - **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**。

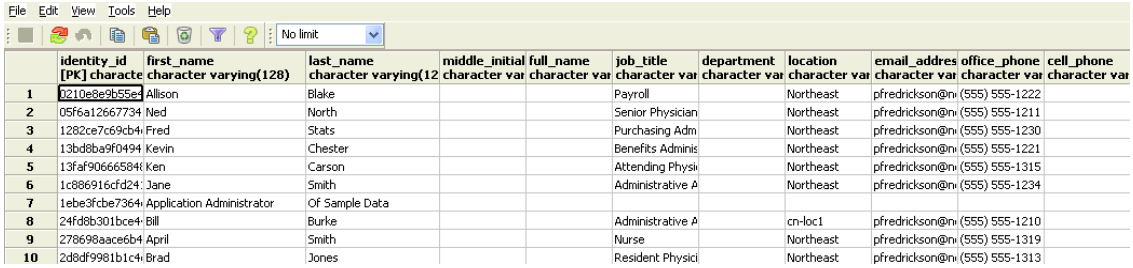
4 選取包含相關資料的組織，然後按一下**啟動**。

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。

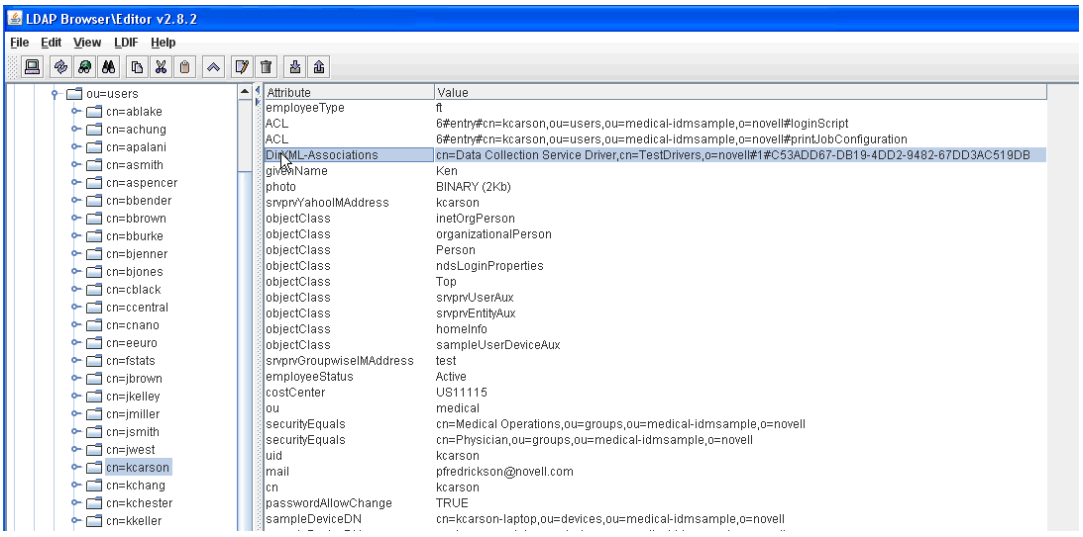
6 確保 **idmrpt_identity** 和 **idmrpt_acct** 表格 (提供關於 Identity Vault 中身分和帳戶的資訊) 中包含以下類型的資訊：



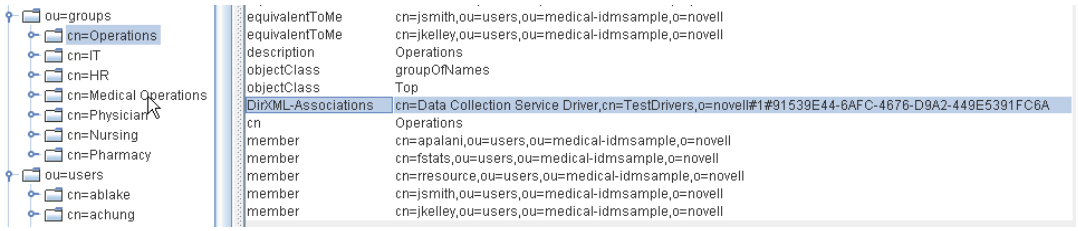
	identity_id [PK] characte	first_name character varying(128)	last_name character varying(12	middle_initial character var	full_name character var	job_title character var	department character var	location character var	email_addres character var	office_phone character var	cell_phone character var
1	0210e8e9b55e4	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	1ebe3fcbe7364	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 Physici		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：



- 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 character var	group_desc character var	dynamic_gro boolean	dynamic_rule character var	nested_grou boolean	idmrpt_valid_from timestamp without tin	idmrpt_deleted boolean	idmrpt_syn_state 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 Resourc	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 Operatic	Medical Operatic	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閘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 132 頁)
- 「包含資料庫中的名稱和描述」(第 133 頁)
- 「將延伸屬性新增至已知物件類型」(第 133 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 (NOVLDCSSCPNG) 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 按一下 **+** 圖示，**建立伺服器證書**索引標籤隨即出現

1c 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。

1d 指定證書綽號。

1e 選取**標準**建立方法，然後按**下一步**。

1f 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 136 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 136 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 1d (第 136 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。

- 「設定受管理系統閘道驅動程式」(第 137 頁)
- 「在「身分資料收集服務」頁面中手動新增資料來源」(第 138 頁)
- 「對 Oracle 資料庫執行報告」(第 138 頁)
- 「手動產生資料庫綱要」(第 138 頁)
- 「部署 Identity Reporting 的 REST API」(第 143 頁)
- 「連接遠端 Remote PostgreSQL 資料庫」(第 143 頁)
- 「在 OSP 中為採用分散式設定的 Identity Reporting 註冊用戶端」(第 144 頁)
- 「Identity Reporting 的安裝後步驟」(第 144 頁)

設定受管理系統閘道驅動程式

安裝程式將為 Identity Reporting 建立並設定資料收集服務驅動程式和受管理系統閘道驅動程式。

設定受管理系統閘道驅動程式後，NetIQ 建議您將 KMO 修改為 **SSL EC 證書 DNS**。若要修改 KMO，請執行以下步驟：

1 登入 Identity Console。

2 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。

3 按一下**受管理系統閘道驅動程式**圖示並移至**驅動程式組態**。

4 在**組態**索引標籤中，按一下**驅動程式參數**下拉式功能表並執行以下步驟：

4a 從**顯示連接參數**欄位中選取顯示。

4b 在 **KMO 名稱**欄位中，將值從 **SSL CertificateDNS** 變更為 **SSL EC 證書 DNS**。

4c 按一下**套用**，然後按一下**確定**。

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 138 頁)
- 「針對 Oracle 資料庫設定 Create_rpt_roles_and_schemas.sql 綱要」(第 139 頁)
- 「針對 MS SQL 資料庫設定 Create_rpt_roles_and_schemas.sql 綱要」(第 141 頁)
- 「清除資料庫檢查總數」(第 141 頁)
- 「(選擇性) 增加欄資料大小」(第 142 頁)

針對 PostgreSQL 資料庫設定 Create_rpt_roles_and_schemas.sql 綱要

1. 使用位於 `/opt/netiq/idm/apps/IDMReporting/sql/` 中的 `create_dcs_roles_and_schemas.sql` 和 `create_rpt_roles_and_schemas.sql` SQL，將所需的角色新增至資料庫。
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 /opt/netiq/idm/apps/IDMReporting/sql/ 中 get_formatted_user_dn.sql 的內容複製到查詢工具，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 (sysdba) 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 SQL Developer，然後建立 Create_dcs_roles 和綱要，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 指定以下許可權：

```
GRANT CREATE PUBLIC SYNONYM to IDM_RPT_CFG;
```

6 將 /opt/netiq/idm/apps/IDMReporting/sql/ 中 get_formatted_user_dn-oracle.sql 的內容複製到 SQL Developer，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，則必須手動將 get_formatted_user_dn-oracle.sql 函數新增至資料庫。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 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 /opt/netiq/idm/apps/IDMReporting/sql/ 中的 create_dcs_roles_and_schemas.mssql 和 create_rpt_roles_and_schemas.mssql，將所需的角色新增至資料庫。

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_RPT_ROLES_AND_SCHEMAS \'<Set pwd for IDM_RPT_CFG>\'
```

6 將 /opt/netiq/idm/apps/IDMReporting/sql/ 中 get_formatted_user_dn.sql 的內容複製到 SQL Developer，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 /opt/netiq/idm/apps/IDMReporting/sql 中找到以下 .sql 檔案。

- DbUpdate-001-run-as-idm_rpt_data.sql
- 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
go
```

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:@192.168.0.1:1521/orcl
-- Liquibase version: 3.5.1
--
*********************************************************************
**
update databasechangelog set md5sum = null
go
```

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。

(選擇性) 增加欄資料大小

在 Identity Manager 的先前版本中，因為存在字元數限制，長資料欄位無法與 Identity Reporting 伺服器進行資料同步。Identity Manager 4.9 提供了一個選項，可提高 PostgreSQL、Oracle 和 MS SQL 資料庫中以下表及其相應欄的字元數限制：

表名稱	欄名稱
idm_rpt_data.idmrpt_idv_ent_bindings	ent_param_str
idm_rpt_data.idmrpt_idv_ent_bindings	ent_param_val
idm_rpt_data.idmrpt_idv_identity_trust	idv_ent_ref
idm_rpt_data.idmrpt_idv_identity_trust	trust_params
idm_rpt_data.idmrpt_idv_ent_bindings_hist	ent_param_str
idm_rpt_data.idmrpt_idv_ent_bindings_hist	ent_param_val
idm_rpt_data.idmrpt_idv_identity_trust_hist	idv_ent_ref
idm_rpt_data.idmrpt_idv_identity_trust_hist	trust_params

- 對於 PostgreSQL，Identity Manager 4.9 中已自動為上表所述的所有欄位提高了字元數限制。

- 對於 Oracle，您必須從 /opt/netiq/idm/apps/IDMReporting/sql/ 目錄執行 alter_column_length-oracle.sql 程序檔，以提高上表所述的所有欄的字元數限制。
- 對於 MS SQL，您必須從 /opt/netiq/idm/apps/IDMReporting/sql/ 目錄執行 alter_column_length-mssql.sql 程序檔，以僅提高已編製索引的欄的字元數限制。在此例中，ENT_PARAM_STR 是表 idmrpt_idv_ent_bindings 中唯一編製索引的欄。

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。若要允許遠端 TCP/IP 連接，請將下面的項目新增至 /opt/netiq/idm/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，請將下面的項目新增至 /opt/netiq/idm/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。

在 OSP 中為採用分散式設定的 Identity Reporting 註冊用戶端

1 導覽至 OSP 的安裝位置，並編輯 `configupdate.sh.properties` 檔案中的以下項目：

```
app_versions="ua#<version>,rpt#<version>"
sso_apps=ua,rpt
```

範例：

```
app_versions="ua#4.9.0,rpt#7.2.0"
sso_apps=ua,rpt
```

2 啟動 configupdate，在以下欄位中更新 Identity Reporting 的用戶端詳細資料：

- 報告用戶端
- 資料收集服務
- DCS 驅動程式

3 重新啟動 OSP 的 tomcat。

Identity Reporting 的安裝後步驟

如果在安裝期間針對「建立 Identity Reporting 的綱要」選取了**啟動**或**檔案**，請務必執行以下操作：

1. 登入 Identity Reporting。
2. 從 Identity Reporting 儲存庫中刪除現有資料來源和報告定義。
3. 新增新的 Identity Manager 資料收集服務資料來源。

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。

完成非 Root 使用者安裝

以非 `root` 使用者身分安裝 Identity Manager 引擎和外掛程式時，安裝程序會執行所有預期的安裝活動。本節將指導您執行完成安裝所需的手動程序。

為密碼規則建立容器

Identity Manager 需要 Identity Vault 中的密碼規則物件。但是，非 root 使用者安裝程序不會為密碼規則建立容器。

1 登入 Identity Console 並移至**樹狀檢視**。

2 導覽至 Identity Vault 中的安全性容器。

3 為密碼規則建立容器。

新增電子郵件通知中的圖形支援

如果您以非 root 使用者身分安裝 Identity Vault 和 Identity Manager 引擎，電子郵件通知可能無法包含電子郵件樣板中提供的圖形或影像。例如，執行 do-send-email-from-template 動作時，Identity Manager 會傳送電子郵件，但是包含的影像皆為空白。您必須更新驅動程式集以確保獲得圖形支援。

1 在 Designer 中登入您的專案。

2 在「大綱」窗格中，展開 **Identity Vault**。

3 以滑鼠右鍵按一下**驅動程式集**。

4 選取**內容 > Java**。

5 對於 JVM 選項，輸入以下內容：

```
-Dcom.novell.nds.dirxml.util.mail.templatepath=path_to_graphics_files
```

例如：

```
-Dcom.novell.nds.dirxml.util.mail.templatepath=/prod/eDirectory/opt/
novell/eDirectory/lib/dirxml/rules/manualtask/mt_files
```

6 按一下**確定**。

7 部署對驅動程式集進行的變更：

7a 以滑鼠右鍵按一下**驅動程式集**。

7b 選取**即時 > 部署**。

7c 選取**部署**。

8 重新啟動 Identity Vault。

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)。

為分散式部署建立 SSL 證書

以下程序說明如何為分散式部署建立 SSL 證書：

1 執行以下指令設定 Java 路徑：

```
export PATH=/opt/netiq/common/jre/bin:$PATH
```

確定已在伺服器上設定 Java 路徑。例如：

```
export PATH=/opt/netiq/common/jre/bin/:$PATH
```

2 建立一個範例工作目錄。

```
mkdir -p /opt/certs
```

3 產生 PKCS 金鑰儲存區：

```
keytool -genkey -alias < alias_name > -keyalg RSA -keystore <absolute
path of keystore > -validity 3650 -keysize 1024 -dname "CN=<Subject
Alternate Name>" -keypass <keypass> -storepass <storepass>
```

4 產生 CSR (證書簽署申請)：

```
keytool -certreq -v -alias < alias_name >  -file < name of the csr file
> -keypass < keypass >  -keystore < absolute path of the keystore >  -
storepass < storepass >
```

5 產生自行簽署的證書：

5a 啟動 Identity Console 並登入。

5b 導覽至**證書管理** > **核發證書**。

5c 瀏覽至在步驟 3 中建立的 .csr 檔案。例如 ua.csr。

5d 按一下「**開啟**」。

5e 在**金鑰使用規範**下拉式清單中指定金鑰類型。

5f 在**延伸金鑰使用規格**下拉式清單中指定延伸金鑰類型。

5g 對於證書類型，請在**基本約束**下拉式清單中選取**未指定**。

5h 在**證書參數**下拉式清單中指定證書的有效期。

5i 在**證書格式**下拉式清單中選取 **二進位 DER 格式的檔案**。

5j 按一下「下一步」。

5k 按一下**確定**。

5l 下載證書並將其複製到 /data 目錄。

6 輸出 .der 格式的根證書：

6a 啟動 Identity Console 並登入。

6b 導覽至**證書管理** > **伺服器證書管理**。

6c 選取 **SSL 證書 DNS** 核取方塊並按一下**輸出**。

6d 在**證書**下拉式清單中選取「組織 CA」。

6e 在**輸出格式**下拉式清單中選取 DER。

6f 按一下**確定**。

6g 下載證書並將其複製到 /data 目錄。

7 將證書輸入至前面所述的 PKCS 金鑰儲存區。

```
keytool -import -trustcacerts -alias root -keystore <name of the
keystore> -file <root certificate > -storepass <password> -noprompt
```

例如：

```
keytool -import -alias <alias name> -keystore <name of the keystore> -
file <self-signed certificate> -storepass <password> -noprompt
```

8 針對 osp, userapp 和 reporting (如果它們在不同的機器中使用) 重複上述程序。

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。

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，請查看「儲存 Configupdate 公用程式密碼」(第 99 頁)。

本部分提供關於在 FIPS 模式下設定和操作 Identity Manager 的資訊。

- 第 7 章「為 FIPS 設定 JRE」(第 151 頁)
- 第 8 章「在 FIPS 模式下設定 Identity Manager 引擎」(第 153 頁)
- 第 9 章「在 FIPS 模式下設定擴送代理程式」(第 155 頁)
- 第 10 章「在 FIPS 模式下設定 Identity Applications 和 Identity Reporting」(第 157 頁)
- 第 11 章「在 FIPS 模式下設定遠端載入器」(第 161 頁)

7 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>/conf/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。若要使用安全 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`。

---

8 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 /opt/netiq/common/jre/lib/ 目錄：
  - 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)
- 若要啟用對上述 .jar 檔案的許可權，請執行以下指令：

  ```
  chown novlua:novlua <jar-file>
  chmod 755 <jar-file>
  ```
- 若要設定環境變數，請執行以下指令：

  ```
  export IS_FIPS_ENABLED=true
  export BC_FIPS_VERSION=1.0.2.4
  export JAVA_OPTS =" -Dorg.bouncycastle.fips.approved_only=true  -Dorg.bouncycastle.rsa.allow_multi_use=true"
  export CLASSPATH=/opt/netiq/common/jre/lib/bc-fips-1.0.2.4.jar
  ```

  完成設定後，可以使用 echo 指令驗證所有環境變數。

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

程序

1. 導覽至 /opt/netiq/common/jre/conf/security/ 目錄。
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 `keystore.type`，將其註解化，然後新增以下項目：

```
keystore.type=bcfks
```

4 導覽至 `/opt/netiq/common/jre/lib/security/` 目錄。

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`。將 `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=/opt/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。

9 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，並在 config 資料夾中產生金鑰儲存區檔案。
- 將以下 jar 檔案放入 /opt/novell/dirxml/fanoutagent/lib/ 目錄：
  - bc-fips-1.0.2.4.jar
  - bcpkix-fips-1.0.7.jar
  - bctls-fips-1.0.18.jar
- 若要啟用對上述 .jar 檔案的許可權，請執行以下指令：

  ```
  chown root:bin <jar-file>
  ```

  ```
  chmod 755 <jar-file>
  ```
- 若要設定環境變數，請執行以下指令：

  ```
  export IS_FIPS_ENABLED=true
  ```

  ```
  export BC_FIPS_VERSION=1.0.2.4
  ```

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

  ```
  export CLASSPATH=/opt/novell/dirxml/fanoutagent/lib/bc-fips-1.0.2.4.jar
  ```

  完成設定後，可以使用 echo 指令驗證所有環境變數。

程序

1. 導覽至 /opt/netiq/common/jre/conf/security/ 目錄。
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 keystore.type，將其註解化，然後新增以下項目：

keystore.type=bcfks

4 導覽至 /opt/netiq/common/jre/lib/security/ 位置：

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
```

7 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 /opt/novell/dirxml/fanoutagent/
config/keystore.jks -srcstorepass changeit -srcstoretype PKCS12 -
destkeystore /opt/novell/dirxml/fanoutagent/config/keystore.jks -
deststorepass changeit -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

8 導覽至 /opt/novell/dirxml/fanoutagent/bin/ 目錄，在 startAgent.sh 檔案中進行以下變更：

```
${JAVA} --add-opens=java.base/sun.security.internal.spec=ALL-UNNAMED -
Djavax.net.ssl.trustStore=/opt/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 ${CLASS_PATH}
com.netiq.idm.fanoutagent.FanoutAgent $filename $SERVERONLY &
```

9 使用以下指令啟動擴送代理程式：

```
./startAgent
```

10 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：

- 在代管 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。例如 /home/fips
2. 在建立的資料夾中備份以下檔案：

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

3. 導覽至 /mnt/osp/packages/misc/ 目錄，並將 osp-tomcat8-pwd-handler-<version>.jar 複製到 /opt/netiq/idm/apps/tomcat/lib 目錄。
4. 導覽至 /opt/netiq/idm/apps/tomcat/bin/ 目錄，並按照以下方式編輯 setenv.sh 檔案：
   - 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=/opt/netiq/idm/apps/tomcat/conf/idm.bcfks -Djavax.net.ssl.trustStorePassword=novell

- BCFIPS_JARS=/opt/netiq/common/jre/lib/bc-fips-1.0.2.4.jar:/opt/netiq/common/jre/lib/bcpkix-fips-1.0.7.jar:/opt/netiq/common/jre/lib/bctls-fips-1.0.18.jar
- export CLASSPATH="${BCFIPS_JARS}"
- 搜尋 CATALINA_OPTS，將 encrypt-keys.pkcs12 變更為 encrypt-keys.bcfks，並將 storetype 變更為 bcfks

5 導覽至 /opt/netiq/idm/apps/tomcat/conf/ 目錄，並執行以下指令：

```
keytool -importkeystore -srckeystore idm.jks -srcstorepass novell -
srcstoretype PKCS12 -destkeystore idm.bcfks -deststorepass novell -
deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH

keytool -importkeystore -srckeystore tomcat.ks -srcstorepass novell -
srcstoretype PKCS12 -destkeystore tomcat.bcfks -deststorepass novell -
deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH

keytool -importkeystore -srckeystore idm.jks -srcstorepass novell -
srcstoretype PKCS12 -destkeystore /opt/netiq/idm/apps/osp/osp.bcfks -
deststorepass novell -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH

keytool -importkeystore -srckeystore tomcat.ks -srcstorepass novell -
srcstoretype PKCS12 -destkeystore /opt/netiq/idm/apps/osp/osp.bcfks -
deststorepass novell -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH --noprompt

java -jar <mount-location>/osp/packages/misc/osp-keymanager-6.7.1.jar -
genkeys -keystore /opt/netiq/idm/apps/osp/osp.bcfks -storepass novell -
storetype BCFKS -application idm -providerClass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerPath
$CLASSPATH -keypass novell -use Encrypting,Signing,TLS

keytool -importkeystore -srckeystore encrypt-keys.pkcs12 -srcstorepass
changeit -srcstoretype PKCS12 -destkeystore 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="novell" 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 = /opt/netiq/idm/apps/tomcat/conf/
tomcat.bcfks

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

com.netiq.idm.osp.oauth-keystore.file =/opt/netiq/idm/apps/tomcat/conf/
osp.bcfks

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

com.netiq.rpt.ssl-keystore.file = /opt/netiq/idm/apps/tomcat/conf/
idm.bcfks

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

DirectoryService/realms/jndi/params/KEYSTORE_PATH = /opt/netiq/idm/
apps/tomcat/conf/idm.bcfks

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

com.netiq.idm.osp.oauth-truststore.file = /opt/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 導覽至 /opt/netiq/idm/apps/tomcat/conf/ 目錄，並執行以下指令：

```
keytool -storepasswd -new <new master keystore password> -keystore /
opt/netiq/idm/apps/tomcat/conf/encrypt-keys.bcfks -storepass changeit -
storetype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH

keytool -keypasswd -alias ism.config.encrypt.0 -keypass changeit -new
<new master keystore password> -keystore /opt/netiq/idm/apps/tomcat/
conf/encrypt-keys.bcfks -storepass novell  -storetype BCFKS -
providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

執行此指令會產生一個 keystorepass 值：

```
java -cp ../lib/obscurity-0.13.2-uber.jar
com.netiq.ism.obfuscate.server.util.PasswordObfuscator novell
```

9 獲取 keystorepass 值後，按照以下方式更新 ism-sensitive.properties 檔案中的以下幾行：

```
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 目錄：

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

11 按照以下方式編輯 configupdate.bat.properties 檔案：

```
master_keystore=/opt/netiq/idm/apps/tomcat/conf/encrypt-keys.bcfks
master_keystore_type=bcfks
```

12 按照以下方式編輯 configupdate.sh 檔案：

```
set "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=/opt/netiq/idm/apps/tomcat/conf/idm.bcfks -
Djavax.net.ssl.trustStorePassword=novell  "

set CLASSPATH=/opt/netiq/common/jre/lib/bc-fips-1.0.2.4.jar:/opt/netiq/
common/jre/lib/bcpkix-fips-1.0.7.jar:/opt/netiq/common/jre/lib/bctls-
fips-1.0.18.jar:%CLASSPATH%
```

13 啟動 configupdate.sh 公用程式。

14 啟動 Tomcat。

11 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 /opt/novell/dirxml/remoteloader/lib/ 目錄：
   - bc-fips-1.0.2.4.jar
   - bcpkix-fips-1.0.7.jar
   - bctls-fips-1.0.18.jar
2. 導覽至 /opt/novell/dirxml/doc/ 目錄。
3. 設定 RL 例項時，將 is_fips_enabled=true 旗標新增至組態檔案。例如，可以將該旗標新增至範例組態檔案 config8000.txt。
4. 儲存該檔案，並使用 rdxml 指令啟動遠端載入器例項。

V 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 VI 部分 「升級 Identity Manager」 (第 179 頁)。如需升級與移轉之間差異的詳細資訊，請參閱「瞭解升級程序」 (第 182 頁)。

12 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. 將 eDirectory 升級至 Identity Vault 的最新受支援版本。如需詳細資訊，請參閱 「升級 Identity Vault」(第 192 頁)。
❑	3. 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 「將 Identity Manager 引擎移轉至新伺服器」(第 168 頁)。
❑	4. 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)。
❑	5. (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 195 頁)。
❑	6. (視情況而定) 如果您要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 「先決條件」(第 167 頁)。
❑	7. 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 169 頁)。
❑	8. (視情況而定) 如果您正在執行使用者應用程式，請將使用者應用程式的舊伺服器中的伺服器特定資訊更新到新伺服器。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 168 頁)。
❑	9. 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 199 頁)。
❑	10. (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 215 頁)。
❑	11. 安裝 Identity Reporting 和關聯的驅動程式。如需詳細資訊，請參閱 「移轉 Identity Reporting」(第 173 頁)。
❑	12. 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 214 頁)。

	核對清單項目
❑	13. 啟用升級後的 Identity Manager 解決方案。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)。

13 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：

- 「先決條件」(第 167 頁)
- 「準備用於移轉的 Designer 專案」(第 167 頁)
- 「將 Identity Manager 引擎移轉至新伺服器」(第 168 頁)
- 「複製驅動程式集的伺服器特定資訊」(第 168 頁)
- 「移轉 Identity Applications」(第 170 頁)
- 「移轉 Identity Reporting」(第 173 頁)

先決條件

- 備份 Identity Manager 解決方案的目錄和資料庫。
- 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**。如需詳細資訊，請參閱第 4 章 「安裝 Identity Manager」(第 61 頁)。

- 執行 Identity Vault 狀態檢查，以確保網要可正常延伸。請使用 TID 3564075 完成健康狀態檢查。
- 將現有的使用者應用程式驅動程式輸入到 Designer 中。

準備用於移轉的 Designer 專案

必須將 Designer 專案歸檔。它代表移轉前狀態的驅動程式。

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。

將 Identity Manager 引擎移轉至新伺服器

1 從軟體和授權頁面 (https://sld.microfocus.com/) 下載 `Identity_Manager_4.9.0_Linux.iso`。

2 掛接下載的 `.iso`。

3 透過 `.iso` 安裝 Identity Manager 引擎。

```
./install.sh
```

4 設定 Identity Manager 引擎。

```
configure.sh
```

5 為新伺服器上的驅動程式集分割區和資料分割區建立讀寫複製本。

6 將新伺服器新增至 Designer 專案。

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 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 169 頁)
- 「在 Identity Console 中變更伺服器特定的資訊」(第 169 頁)
- 「變更使用者應用程式的伺服器特定資訊」(第 170 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。如果使用此選項，則必須停用來源伺服器或目的地伺服器上的驅動程式，直到每個驅動程式在新伺服器上成功執行。NetIQ 建議不要同時在兩部伺服器上快取驅動程式的事件。

     附註：當驅動程式在伺服器上處於使用中狀態時，它會快取事件。停用驅動程式會停止在伺服器上快取事件並刪除快取 (.TAO) 檔案。
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「啟動驅動程式」(第 197 頁)。

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。

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.sh`。

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.sh
```

3 依照 「完成 Identity Applications 的設定」 (第 99 頁) 所述指定值。

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 170 頁)
- 「在新伺服器上安裝 Identity Applications」 (第 172 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 以 `postgres` 使用者身分登入裝有 PostgreSQL 的伺服器。

```
#su - postgres
```

2 將資料輸出至 `.sql` 檔案：確定 Postgres 使用者對您要將檔案輸出到的目錄具有完整存取權：

```
pg_dump -p < 連接埠號碼 > -U < 使用者名稱 > -d < 資料庫名稱 > -f < 輸出位置 >
```

例如：

```
pg_dump -p 5432 -U postgres -d idmuserappdb -f /tmp/idmuserappdb.sql
```

3 登入要安裝 PostgreSQL 的新伺服器。

4 安裝 PostgreSQL。

4a 導覽至掛接 Identity_Manager_4.9.0_Linux.iso 的位置。

4b 導覽至 /common/packages/postgres/ 目錄。

4c 使用以下指令安裝 PostgreSQL：

```
rpm -ivh netiq-postgresql-9.6.6-0.noarch.rpm
```

4d 使用以下指令將群組關聯到 postgres 使用者。

```
/usr/sbin/usermod -a -G postgres postgres
```

4e 在 /etc/passwd 檔案中，將 postgres 使用者的主目錄路徑變更為 /opt/netiq/idm/postgres/。

4e1 導覽至 /etc/ 目錄。

4e2 編輯 passwd 檔案。

```
vi /etc/passwd
```

4e3 將 postgres 使用者的主目錄變更為 /opt/netiq/idm/postgres/。

4f 以 postgres 使用者身分登入。

例如：

```
su - postgres
```

4g 在 PostgreSQL 安裝位置中建立 data 目錄。

```
mkdir -p <POSTGRES_HOME>/data, where <POSTGRES_HOME> is /opt/netiq/idm/postgres
```

例如：

```
mkdir -p /opt/netiq/idm/postgres/data
```

4h 輸出 PostgreSQL home 目錄 .

```
export PGHOME=<postgres home directory path>
```

例如：

```
export PGHOME=/opt/netiq/idm/postgres
```

4i 輸出 PostgreSQL 密碼：

```
export PGPASSWORD=< 輸入資料庫密碼 >
```

4j 啟始化資料庫。

```
LANG=en_US.UTF-8 <POSTGRES 主目錄 >/bin/initdb -D <POSTGRES 主目錄 >/data
```

例如：

```
LANG=en_US.UTF-8 /opt/netiq/idm/postgres/bin/initdb -D /opt/netiq/idm/postgres/data
```

4k 導覽至 /opt/netiq/idm/postgres/bin 目錄。

4l 為以下元件建立資料庫：

```
$ createdb idmuserappdb
$ psql -s idmuserappdb
# create user idmadmin password 'somepassword';
# GRANT ALL PRIVILEGES ON DATABASE idmuserappdb TO idmadmin;
# ALTER DATABASE idmuserappdb OWNER TO idmadmin;
```

5 將資料輸入到新 PostgreSQL 資料庫中。

5a 將步驟 2 中輸出的檔案複製到 postgres 使用者具有完整存取權的位置。

5b 執行以下指令以將資料輸入到 PostgreSQL 資料庫。

```
psql -d < 資料庫名稱 > -U < 使用者名稱 > -f < 輸出檔案所在位置的完整路徑 > -W
```

例如：

```
psql -d idmuserappdb -U idmadmin -f /tmp/idmuserappdb.sql -W
```

在新伺服器上安裝 Identity Applications

1 從 NetIQ 下載網站下載 Identity_Manager_4.9.0_Linux.iso。

2 掛接 .iso。

3 將 iso 的內容複製到您具有寫入存取權的另一個目錄。

例如：

```
cp /mnt/* /home
```

4 編輯組態檔案的內容，以跳過使用者應用程式和角色與資源服務驅動程式的部署。

附註：依預設，Identity Applications 安裝程式會建立並部署角色與資源服務和使用者應用程式的驅動程式。

4a 導覽至 /home/user_application 目錄。

4b 編輯 configure.sh 檔案。

```
vi configure.sh
```

4c 將下行設為備註：

```
install_service_drivers "UA" "${ID_VAULT_ADMIN_LDAP}"
"${ID_VAULT_PASSWORD}" "${ID_VAULT_HOST}" ${ID_VAULT_LDAPS_PORT}
"cn=${ID_VAULT_DRIVER_SET},${ID_VAULT_DEPLOY_CTX}"
```

4d 儲存 configure.sh 檔案。

5 從 /mnt 目錄安裝 Identity Applications。

```
./install.sh
```

6 從 /mnt 目錄設定 Identity Applications。

```
./configure.sh
```

7 選取自訂組態，並在出現以下提示時選取否：

是否要在目前伺服器上設定 PostgreSQL 資料庫？

8 導覽至 /opt/netiq/idm/apps/configupdate 目錄中的組態更新公用程式，並確定組態設定正確無誤：

```
./configupdate.sh
```

移轉 Identity Reporting

Identity Reporting 移轉過程包括以下步驟：

- 「更新 Identity Reporting 的驅動程式」(第 173 頁)
- 「部署 Identity Reporting 的驅動程式」(第 173 頁)
- 「將現有資料移轉至新資料庫」(第 173 頁)
- 「設定新 Reporting 伺服器」(第 177 頁)
- 「建立資料同步規則」(第 177 頁)

更新 Identity Reporting 的驅動程式

1 升級資料收集服務和受管理服務閘道驅動程式套件。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「Upgrading Installed Packages」(升級安裝的套件)。

附註：升級套件時，請務必指定新 Identity Reporting 伺服器的詳細資料。

---

2 部署驅動程式。如需詳細資訊，請參閱 「部署 Identity Reporting 的驅動程式」(第 173 頁)。

3 (視情況而定) 如果您是從 4.5.x 移轉且需要移轉 EAS 資料，請執行 「將現有資料移轉至新資料庫」(第 173 頁) 中所述的步驟。

部署 Identity Reporting 的驅動程式

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 Objectss」(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 在大綱檢視中，用滑鼠右鍵按一下資料收集服務驅動程式。

3 選取部署。

4 對驅動程式集中的每個資料收集服務驅動程式重複此過程。部署資料收集服務驅動程式後，對受管理服務閘道驅動程式重複此過程。

將現有資料移轉至新資料庫

您必須建立必要的角色和表空間，以確保移轉期間不會出現故障。

準備新 PostgreSQL 資料庫

1 停止 EAS 以確保不會有任何事件傳送到 EAS 伺服器。

2 使用 Identity Console 停止 DCS 驅動程式：

2a 登入 Identity Console。

2b 停止 DCS 驅動程式。

2c 編輯驅動程式內容，以將啟動選項設定為手動。

此步驟可確保驅動程式不會自動啟動。

3 使用 PGAdmin 執行以下 SQL 指令，以建立必要的角色、表空間和資料庫。

此步驟可確保移轉期間不會出現故障。

3a 執行以下指令以建立必要角色：

```
CREATE ROLE esec_app
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE esec_user
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE admin LOGIN
  ENCRYPTED PASSWORD '<specify the password for admin>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
GRANT esec_user TO admin;

CREATE ROLE appuser LOGIN
  ENCRYPTED PASSWORD '<specify the password for appuser>'
  NOSUPERUSER INHERIT NOCREATEDB CREATEROLE;
GRANT esec_app TO appuser;

CREATE ROLE dbauser LOGIN
  ENCRYPTED PASSWORD '<specify the password for dbauser>'
  SUPERUSER INHERIT CREATEDB CREATEROLE;

CREATE ROLE idmrptsrv LOGIN
  ENCRYPTED PASSWORD '<specify the password for idmrptsrv>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
GRANT esec_user TO idmrptsrv;

CREATE ROLE idmrptuser LOGIN
  ENCRYPTED PASSWORD '<specify the password for idmrptuser>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE rptuser LOGIN
  ENCRYPTED PASSWORD '<specify the password for rptuser>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
GRANT esec_user TO rptuser;
```

3b (視情況而定) 執行以下指令以建立表空間：

```
 CREATE TABLESPACE sendata1
  OWNER dbauser
  LOCATION '<provide the location where table space has to be
created>';
```

例如：

```
CREATE TABLESPACE sendata1
  OWNER dbauser
  LOCATION '</opt/netiq/idm/apps/postgres/data>';
```

3c (視情況而定) 如果您要移轉現有的 EAS 資料，NetIQ 建議執行以下指令來建立 SIEM 資料庫：

```
CREATE DATABASE "SIEM"
  WITH OWNER = dbauser
       ENCODING = 'UTF8'
       TABLESPACE = sendata1
       CONNECTION LIMIT = -1;
```

3d 執行以下指令以建立 Reporting 資料庫：

```
CREATE DATABASE "idmrptdb"
  WITH OWNER = dbauser
       ENCODING = 'UTF8'
       CONNECTION LIMIT = -1;
```

輸出 EAS 資料

請僅在您目前執行的是 Identity Manager 4.5.x 並想要將現有 EAS 資料移轉至 SIEM 資料庫時，才執行以下動作：

- 「輸出 EAS 資料」(第 175 頁)
- 「將 EAS 資料輸入至新的 PostgreSQL 資料庫中」(第 176 頁)

輸出 EAS 資料

1. 停止 EAS 以確保不會有任何事件傳送到 EAS 伺服器。
2. 使用 Identity Console 停止 DCS 驅動程式：
   - **2a** 登入 Identity Console。
   - **2b** 停止 DCS 驅動程式。
   - **2c** 編輯驅動程式內容，以將啟動選項設定為手動。

     此步驟可確保驅動程式不會自動啟動。
3. 將 EAS 資料庫中的資料輸出到檔案：
   - **3a** 登入 EAS 使用者帳戶：

     ```
     # su - novleas
     ```
   - **3b** 指定 EAS 使用者具有完全存取權的位置，例如 `/home/novleas`。
   - **3c** 導覽至 PostgreSQL 安裝目錄並執行以下指令：

例如：

```
export PATH=/opt/novell/sentinel_eas/3rdparty/postgresql/bin/:$PATH
```

```
export LD_LIBRARY_PATH=/opt/novell/sentinel_eas/3rdparty/
postgresql/lib/:$LD_LIBRARY_PATH
```

3d 使用以下指令將資料輸出到 .sql 檔案：

```
./pg_dump -p < 連接埠號碼 > -U < 使用者名稱 > -d < 資料庫名稱 > -f < 輸出位置
>
```

例如：

```
./pg_dump -p 15432 -U dbauser SIEM -f /home/novleas/SIEM.sql
```

將 EAS 資料輸入至新的 PostgreSQL 資料庫中

1. 停止 EAS 以確保不會有任何事件傳送到 EAS 伺服器。
2. 使用 Identity Console 停止 DCS 驅動程式：
   - **2a** 登入 Identity Console。
   - **2b** 停止 DCS 驅動程式。
   - **2c** 編輯驅動程式內容，以將啟動選項設定為手動。

     此步驟可確保驅動程式不會自動啟動。
3. 將 EAS 資料輸入至新的 PostgreSQL 資料庫中：
   - **3a** 將輸出的 .sql 檔案複製到 postgres 使用者具有完整存取權的位置。例如，/opt/netiq/idm/postgres
   - **3b** 執行以下指令以將 EAS 資料輸入至 PostgreSQL 資料庫中。

     ```
     psql -d < 資料庫名稱 > -U < 使用者名稱 > -f < 輸出檔案所在位置的完整路徑 >
     ```

     例如：

     ```
     psql -d SIEM -U postgres -f /opt/netiq/idm/apps/postgres/SIEM.sql
     ```
4. 檢查有無任何移轉記錄錯誤，如有則予以解決。

輸出報告資料

請僅在您目前執行的是 Identity Manager 4.7.x 並想要將現有報告資料移轉至新伺服器時，才執行以下動作：

- 「輸出報告資料」(第 176 頁)
- 「將資料輸入至新 Reporting 伺服器中」(第 177 頁)

輸出報告資料

1. 以 postgres 使用者身分登入裝有 PostgreSQL 的伺服器。

   ```
   #su - postgres
   ```
2. 將資料輸出至 .sql 檔案：確定 Postgres 使用者對您要將檔案輸出到的目錄具有完整存取權：

pg_dump -p <連接埠號碼> -U <使用者名稱> -d <資料庫名稱> -f <輸出位置>

例如：

pg_dump -p 5432 -U dbauser -W idmrptdb -f /tmp/idmrptdb.sql

將資料輸入至新 Reporting 伺服器中

1 以 postgres 使用者身分登入裝有 PostgreSQL 的伺服器。

#su - postgres

2 將資料輸入到新 PostgreSQL 資料庫中。

2a 將輸出的 .sql 檔案複製到 postgres 使用者具有完整存取權的位置。

2b 執行以下指令以將資料輸入到 PostgreSQL 資料庫。

psql -d <資料庫名稱> -U <使用者名稱> -f <輸出檔案所在位置的完整路徑>

例如：

psql -d idmrptdb -U dbauser -f /tmp/idmrptdb.sql

3 檢查有無任何移轉記錄錯誤，如有則予以解決。

設定新 Reporting 伺服器

1 從軟體和授權頁面 (https://sld.microfocus.com/) 下載 Identity_Manager_4.9.0_Linux.iso。

2 掛接 .iso。

3 在 ISO 掛接位置執行以下指令：

./install.sh

4 設定 Identity Reporting。

./configure.sh

5 選取自訂組態，並在出現以下提示時選擇否：

是否要在目前伺服器上設定 PostgreSQL 資料庫？

是否要安裝新驅動程式集？

附註：依預設，Identity Reporting 安裝程式會建立並部署受管理服務閘道和資料收集服務的驅動程式。

6 導覽至 /opt/netiq/idm/apps/configupdate 目錄中的組態更新公用程式，並確定組態設定正確無誤：

./configupdate.sh

建立資料同步規則

設定 Reporting 伺服器之後，您需要建立資料同步規則，以將事件從 SLM for IGA 轉遞到 Reporting 資料庫。

VI 升級 Identity Manager

此部分提供升級 Identity Manager 各元件的資訊。

- 第 14 章 「升級 Identity Manager 的準備工作」 (第 181 頁)
- 第 15 章 「升級 Identity Manager 的元件」 (第 189 頁)
- 第 16 章 「從進階版切換到標準版」 (第 217 頁)

14 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。

警告：您必須永遠透過 Identity Manager 修補程式下載網站來更新隨 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 181 頁)
- 「瞭解升級程序」(第 182 頁)
- 「支援的升級路徑」(第 183 頁)
- 「備份目前組態」(第 186 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. 瞭解升級程序。如需詳細資訊，請參閱「瞭解升級程序」(第 182 頁)。
❑	2. 查看支援升級至 Identity Manager 4.9 的升級路徑。如需受支援升級路徑的資訊，請參閱「支援的升級路徑」(第 183 頁)。
❑	3. 確定您已取得用於升級 Identity Manager 的安裝套件。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. 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 186 頁)。
❑	5. 安裝最新版本的 Designer。
❑	6. 將 Sentinel Log Management for IGA 升級至最新版本。如需詳細資訊，請參閱「升級 Sentinel Log Management for IGA」(第 210 頁)。
❑	7. 將 Identity Vault (eDirectory) 升級至 9.2.9。如需詳細資訊，請參閱「升級 Identity Vault」(第 192 頁)。
❑	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「停止驅動程式」(第 197 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 193 頁)。 **附註：**若要將 Identity Manager 引擎移轉至新伺服器，您可以使用目前 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 168 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 195 頁)。
❑	11. (視情況而定) 升級現有驅動程式的套件 (如果有更新的套件版本可用)。如需詳細資訊，請參閱 「升級 Identity Manager 驅動程式」 (第 199 頁)。 僅當您要使用現有驅動程式的新套件中的功能時，才需要進行升級。
❑	12. 升級 Identity Applications。如需詳細資訊，請參閱 「升級 Identity Applications」 (第 200 頁)。
❑	13. 升級 Identity Reporting。如需詳細資訊，請參閱 「升級 Identity Reporting」 (第 209 頁)。
❑	14. 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 「啟動驅動程式」 (第 197 頁)。
❑	15. (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 214 頁)。
❑	16. (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 215 頁)。
❑	17. 升級 Analyzer。如需詳細資訊，請參閱 「升級 Analyzer」 (第 213 頁)。
❑	18. 啟用升級後的 Identity Manager 解決方案。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)。

瞭解升級程序

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，如果新版 Identity Manager 不支援從現有版本直接升級的路徑，您必須先升級至可從其升級至 4.9 版的版本。或者，您可以移轉至新機器。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該新伺服器的過程。

升級

- **Identity Manager 4.8 Standard Edition：**如果您要從 Identity Manager 4.9 升級至 Identity Manager 4.9 Standard Edition，請執行 《Quick Start Guide for Installing NetIQ Identity Manager 4.9 Standard Edition》 (NetIQ Identity Manager 4.8 Standard Edition 安

裝和升級快速入門指南) 中的「Upgrading Identity Manager 4.8 Standard Edition to Identity Manager 4.7 Standard Edition」(將 Identity Manager 4.6 Standard Edition 升級至 Identity Manager 4.7 Standard Edition) 部分所列的步驟。

- **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 181 頁)。

移轉

在某些情況下，您無法直接升級。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。如果您無法同時升級這些伺服器，驅動程式會繼續與其他版本的 Identity Manager 配合運作，直到每部伺服器都升級完畢。

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 16 章 「從進階版切換到標準版」(第 217 頁)。

支援的升級路徑

Identity Manager 4.9 支援從 4.7.5 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 183 頁)
- 「從 Identity Manager 4.8.x 版本升級」(第 185 頁)

附註：Identity Manager 4.9 僅與 eDirectory 9.2.8 和 9.2.9 版本相容。請務必先將 eDirectory 升級至 9.2.8 或 9.2.9，然後再升級 Identity Manager 引擎。

從 Identity Manager 4.7.5 版本升級

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 4.7 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	4.7.5	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、角色與資源驅動程式，以及資料收集服務驅動程式套件。更新套件後，重新啟動驅動程式。 5. 將 Identity Applications 升級至 4.9。 6. 啟動 Tomcat 和 NGINX 服務。
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 7.2.0。 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 NetIQ 文件 (https://www.netiq.com/documentation/identity-manager-49/) 頁面您所用版本的版本說明中查看相關資訊。

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 4.7 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。 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、角色與資源驅動程式，以及資料收集服務驅動程式套件。更新套件後，重新啟動驅動程式。 5. 將 Identity Applications 升級至 4.9。 6. 啟動 Tomcat 和 NGINX 服務。
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 升級至支援的版本。 4. 將 Identity Reporting 升級至 7.2.0。

NetIQ 建議開始升級前先在 NetIQ 文件 (https://www.netiq.com/documentation/identity-manager-49/) 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 186 頁)
- 「輸出驅動程式組態」(第 187 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 186 頁)
- 「從 Identity Vault 建立新專案」(第 186 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**：表示 Identity Vault 伺服器的 IP 位址或 DNS 名稱
- **使用者名稱**：表示用於向 Identity Vault 驗證的使用者 DN
- **密碼**：表示驗證使用者的密碼

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。

輸出驅動程式組態

建立驅動程式的輸出可以備份目前的組態。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。

15 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。

- 「升級順序」(第 189 頁)
- 「升級注意事項」(第 190 頁)
- 「升級 Designer」(第 191 頁)
- 「升級 Identity Manager 引擎」(第 192 頁)
- 「停止和啟動 Identity Manager 驅動程式」(第 196 頁)
- 「升級 Identity Manager 驅動程式」(第 199 頁)
- 「升級 Identity Applications」(第 200 頁)
- 「升級 Identity Reporting」(第 209 頁)
- 「升級 Analyzer」(第 213 頁)
- 「升級後任務」(第 213 頁)
- 「將新伺服器新增至驅動程式集」(第 214 頁)
- 「將自訂規則還原至驅動程式」(第 215 頁)

升級順序

一次只能升級一個 Identity Manager 元件。依以下順序升級元件：

1. Designer
2. Sentinel Log Management for IGA
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 (同時安裝標準版 OSP)
9. Analyzer
10. (視情況而定) SSPR
11. Identity Console

附註：

- 務必將 Analyzer 更新至 4.8.5，並將其與 Identity Manager 4.9 配合使用。
- 如果 SSPR 安裝在遠端伺服器上，則需要單獨更新 SSPR。
- 如果所有 Identity Manager 元件都在同一部伺服器上執行，請務必將它們都更新至最新版本。

升級注意事項

在開始升級 Identity Manager 元件之前，請查看以下注意事項：

- 只能以主控台模式升級元件。不支援靜默升級。
- 一次只能升級一個元件。
- 必須單獨升級 Identity Vault。此版本支援 eDirectory 9.2.8 及更新版本。
- 如果在 BTRFS 檔案系統上設定了 Identity Vault，則升級程序將不會成功。此版本僅支援 Ext3、Ext4 和 XFS 檔案系統。
- 在開始升級 Identity Manager 引擎之前，請確定快取檔案中沒有任何事件。如果驅動程式使用的是 MapDB，請確定升級後的驅動程式能正常與升級後的引擎配合工作。如需詳細資訊，請參閱 「使用 MapDB 3.0.9」(第 194 頁)。
- 在升級元件之前，必須查看建議的伺服器設定。Identity Manager 要求 Identity Applications 和 OSP 必須安裝在同一部電腦上。不過，Identity Reporting 支援本地或在遠端安裝的 OSP。
- 確定使用 FQDN 以統一方式設定 Identity Applications、Identity Reporting 和資料庫。
- 如果您使用受支援版本的 Oracle 或 Microsoft SQL Server 資料庫，則必須設定以下兩個資料庫例項才能使 Identity Applications 正常運作：Identity Applications (`idmuserappdb`) 資料庫和工作流程 (`igaworkflowdb`) 資料庫。確定在同一部伺服器上設定這些資料庫例項。
- 如果您使用 Identity Applications 的 NAM 反向代理組態來載入表單，則必須使用 NAM 5.x 版本。
- 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電子郵件帳戶密碼將自動移轉至 `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。
- 升級 Self Service Password Reset (SSPR) 時，需注意以下事項：
  - 如果在 SSPR 伺服器上啟用了 Syslog 輸出格式類型為 CEF 的稽核功能，則必須從 Sentinel Syslog 伺服器中解除安裝 NetIQ Self Service Password Reset Collector，否則 Syslog 伺服器將無法剖析 SSPR 稽核事件。

- SSPR 支援對稽核事件使用 CEF 和 JSON 兩種輸出格式類型。SSPR 4.7.0.1 將繼續支援 NetIQ Self Service Password Reset Collector 收集 JSON 輸出格式類型的事件。如果有多部 SSPR 伺服器連接至同一部 Sentinel Syslog 伺服器，只能為所有伺服器的稽核事件選取一種格式類型。
- 如果 SSPR 安裝在單獨的伺服器上，請將該元件升級至 Identity Manager 4.9 中捆綁的最新版本。

將 Identity Manager 更新至版本 4.9 後，SSPR 將升級至版本 4.7.0.1，這就需要使用 Universal CEF Collector 來收集 CEF 格式類型的稽核事件。

附註：如果您是首次啟用輸出格式類型為 CEF 的 SSPR 稽核功能，請確定未在 Sentinel Syslog 伺服器上設定 NetIQ Self Service Password Reset Collector。

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. 若要解除安裝目前的 Designer 版本，請執行以下操作：

   3a 關閉 Designer

   3b 導覽至包含解除安裝程序檔的目錄。依預設，該程序檔位於 < 安裝目錄 >/designer/UninstallDesigner/Uninstall Designer for Identity Manager 中

   3c 若要執行該程序檔，請輸入 `./uninstall`
4. 您可以使用圖形使用者介面或主控台模式來安裝 Designer。

   4a 從軟體授權和下載 (https://sld.microfocus.com/index) 入口網站下載 `Identity_Manager_4.9.0_Designer_Linux.tar.gz`。

   4b 導覽至要擷取檔案的目錄。

   4c 執行以下指令：

   ```
   tar -zxvf Identity_Manager_4.9.0_Designer_Linux.tar.gz
   ```

   4d 執行以下指令之一來安裝 Designer。

   主控台：`./install`

圖形使用者介面：`./install -i console`

4e 依照提示操作並繼續安裝。

5 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

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。

安裝前驗證 Linux RPM

請執行以下步驟來驗證 RPM：

1 從軟體和授權頁面 (https://sld.microfocus.com/) 下載 `Identity_Manager_4.9.0_Linux.iso`。

2 掛接下載的 `.iso`。

3 導覽至存放公用金鑰的以下位置：

```
<ISO-MOUNT-location>/common/license/
```

例如 `cd /mnt/common/license/`

4 執行以下指令以輸入金鑰：

```
rpm --import MicroFocusGPGPackageSign.pub
```

```
rpm --import OT-package-sign.pub
```

5 (選擇性) 執行以下指令以驗證簽名：

```
rpm --checksig -v <mount-location>/IDVault/setup/<RPM Name>
```

例如：

```
rpm --checksig -v /mnt/IDVault/setup/novell-NDSbase-*.x86_64.rpm
```

升級 Identity Vault

1 依照《*NetIQ Identity Manager Overview and Planning Guide*》(NetIQ Identity Manager 綜覽和規劃指南)「Where to Get Identity Manager」(從何處獲取 Identity Manager) 中的說明下載 `Identity_Manager_4.9.0_Linux.iso`。

2 掛接下載的 `.iso`。

3 從 `.iso` 檔案的根目錄中，導覽至 `IDVault/setup` 目錄。

4 執行以下指令：

```
./nds-install
```

5 由於 iManager 即將廢棄，請對以下警告提示輸入您的回應：

```
This version of eDirectory installation will upgrade various packages
required by eDirectory and iManager.The updated packages may impact
iManager running on the same server.Do you want to continue
installation/upgrade (y/n)
```

5a (選擇性) 如果要繼續，請執行步驟 6。

5b (選擇性) 如果不繼續，更新將會終止。

6 接受授權合約並繼續安裝。

7 指定 **adminDN**。例如，`cn=admin.ou=sa.o=system`。

8 當系統提示停止 eDirectory 例項並升級 NICI 時，指定 `y`。

9 指定是否要設定**增強型背景驗證**。

附註：如果升級 DIB 失敗，並且 `nds-install` 指令提示執行 `ndsconfig upgrade`，請在執行 `nds-install` 之後執行該指令。如果升級之後 eDirectory 服務未啟動，請執行 `ndsconfig upgrade` 指令。如需詳細資訊，請參閱《NetIQ eDirectory Installation Guide》(NetIQ eDirectory 安裝指南)。

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 197 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_Linux.iso`。

2 掛接下載的 `.iso`。

3 執行以下指令：

```
./install.sh
```

4 通讀授權合約。

5 輸入 `y` 以接受授權合約。

6 指定是否要升級 Identity Manager 元件。可用選項有 **y** 和 **n**。

7 選取 Identity Manager 引擎。

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。

引擎升級程序會在 Identity Vault 的 DIB 目錄中保留某些現有的 MapDB 快取檔案 (`dx*`)。升級使用 MapDB 的驅動程式後，必須手動移除該驅動程式的這些檔案。如需詳細資訊，請參閱 「使用 MapDB 3.0.9」(第 194 頁)。

使用 MapDB 3.0.9

Identity Manager 支援 MapDB 3.0.9。除了 Identity Manager 引擎外，一些驅動程式 (例如 Office365 和 Azure Active Directory) 也使用 MapDB。

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 194 頁)
- 「(選擇性) 手動移除 MapDB 快取檔案」(第 194 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。

(選擇性) 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 (`/var/opt/novell/eDirectory/data/dib`) 中保留某些現有的 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 狀態快取檔案的版本。必須移除所有包含上述名稱的 MapDB 狀態快取檔案，無論其版本是什麼。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>_0`、`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

以非 Root 使用者身分升級 Identity Manager 引擎

僅當您以非 root 使用者身分安裝了 Identity Manager 引擎時，才能執行此動作。

1. 從軟體和授權頁面 (https://sld.microfocus.com/) 下載 Identity_Manager_4.9.0_Linux.iso。
2. 掛接下載的 .iso。
3. 執行以下指令：

   ./install.sh
4. 選取 **Identity Manager 引擎**並按 Enter。
5. 指定 Identity Manager 引擎的非根目錄安裝位置。例如 /home/user/eDirectory/。
6. 指定 y 以完成升級。

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。

1. 建立遠端載入器組態檔案的備份。
2. 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 197 頁)。
3. 停止每一個驅動程式的遠端載入器服務或精靈。

   rdxml -config *path_to_configfile* -u
4. 從 NetIQ 下載網站下載 Identity_Manager_4.9.0_Linux.iso。
5. 掛接下載的 .iso。
6. 執行以下指令：

   ./install.sh
7. 通讀授權合約。
8. 輸入 y 以接受授權合約。
9. 指定是否要升級 Identity Manager 元件。可用選項有 **y** 和 **n**。
10. 選取遠端載入器。
11. 完成安裝後，驗證組態檔案是否包含您的環境資訊。
12. (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。
13. 啟動每一個驅動程式的遠端載入器服務或精靈。

    rdxml -config *path_to_config_file*

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 3.0.9」(第 194 頁)。

升級 Java 遠端載入器

1. 建立 Java 遠端載入器組態檔案的備份。
2. 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 197 頁)。
3. 停止每一個驅動程式的遠端載入器服務或精靈。

   `dirxml_jremote -config path_to_configfile -u`
4. 從 NetIQ 下載網站下載 `Identity_Manager_4.9.0_Linux.iso`。
5. 掛接下載的 `.iso`。
6. 導覽至 `/IDM/packages/java_remoteloader` 目錄。
7. 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。
8. 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`
9. 將步驟 7 和 8 中複製的檔案解壓縮。

   例如 `tar -zxvf dirxml_jremote.tar.gz`
10. (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。
11. 啟動每一個驅動程式的遠端載入器服務或精靈。

    `dirxml_jremote -config path_to_config_file`

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、移轉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 197 頁)
- 「啟動驅動程式」(第 197 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 197 頁)
- 「使用 Identity Console 停止驅動程式」(第 197 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 到步驟 5d。

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 198 頁)
- 「使用 Identity Console 啟動驅動程式」(第 198 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 5c 和步驟 5d。

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**提供新驅動程式內容。您可以在 Designer 中管理、維護和建立套件。Designer 不會保留您在 Identity Console 中對驅動程式內容所做的任何變更。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 199 頁)
- 「以套件中的內容取代現有內容」(第 199 頁)
- 「保留目前內容並透過套件新增新內容」(第 200 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 (https://www.netiq.com/documentation/identity-manager-49-drivers/) 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「輸出驅動程式組態」(第 187 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 (https://www.netiq.com/documentation/identity-manager-49-drivers/) 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 215 頁)。

保留目前內容並透過套件新增新內容

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 「輸出驅動程式組態」(第 187 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 (https://www.netiq.com/documentation/identity-manager-49-drivers/) 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 (https://www.netiq.com/documentation/identity-manager-49-drivers/)。

驅動程式即包含由套件新增的新功能。

附註：升級 LDAP 驅動程式後，請確定從 temp 目錄中刪除 `ldap_*.zoomdb` 資料夾。為了避免在刪除 `ldap_*.zoomdb` 資料夾時遺失資料，請執行以下操作：

1. 移至 Designer。
2. 導覽至**內容 > 驅動程式組態 > 驅動程式參數 > 發行者選項**。
3. 將**首次啟動時要同步的搜尋結果**屬性變更為**同步所有內容**。

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
- Self-Service Password Reset (SSPR)
- Tomcat、JDK 和 ActiveMQ

- PostgreSQL 資料庫
- One SSO Provider (OSP)

重要：Identity Manager 4.9 要求將 Identity Applications 和 OSP 安裝在同一部電腦上。升級至此版本時，請使用升級 Identity Applications 時安裝的 OSP，然後將現有 OSP 伺服器中的 OSP 設定複製到新的 OSP 伺服器。如需詳細資訊，請參閱 「Identity Applications 元件的升級後任務」(第 206 頁)。

本節提供關於以下主題的資訊：

- 「升級注意事項」(第 201 頁)
- 「系統要求」(第 203 頁)
- 「瞭解升級程式」(第 203 頁)
- 「升級 PostgreSQL」(第 203 頁)
- 「升級 Identity Applications 元件」(第 203 頁)
- 「Identity Applications 元件的升級後任務」(第 206 頁)
- 「升級後驗證版本號碼」(第 209 頁)

升級注意事項

Identity Applications 升級程序可能會因您升級 Identity Applications 元件的方式而異。在升級 Identity Applications 之前，請注意以下事項：

- 在開始升級 Identity Applications 之前，如果您使用 Oracle 或 MS SQL 資料庫，則必須建立 `igaworkflowdb`，並向擁有這些資料庫的 `idmadmin` 使用者指定所有特權。
- 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)。
- 如果將 Identity Applications 和 SSPR 安裝在不同的伺服器上，則您可以選擇單獨升級 SSPR。
- 在升級期間，請確定驗證資料庫名稱和其他預設值，並視需要進行修改。
- Identity Manager 支援在 Identity Applications 伺服器本地安裝 OSP。升級程式不支援將 OSP 獨立升級至此版本，在升級 Identity Applications 時，它會安裝 OSP 的新副本。若要將現有 OSP 設定還原至新安裝的 OSP，請參閱「Identity Applications 元件的升級後任務」(第 206 頁) 中的 One SSO Provider。

表格 15-1 Identity Applications 的升級程序

Identity Applications 部署	升級程序
Identity Applications、SSPR 和 OSP 安裝在同一部伺服器上	若要升級所有元件，請依照「升級 Identity Applications」(第 204 頁) 中的步驟操作。
Identity Applications 和 OSP 安裝在同一部伺服器上。SSPR 安裝在其他伺服器上。	1. 若要升級 Identity Applications 和 OSP，請依照「升級 Identity Applications」(第 200 頁) 中的步驟操作。 2. 若要升級其他伺服器上的 SSPR，請依照「升級 SSPR」(第 206 頁) 中的步驟操作。
Identity Applications 未與 SSPR 和 OSP 安裝在同一部伺服器上。在這種情況下，可以將 SSPR 安裝在 Identity Applications 伺服器或單獨的伺服器上。但是，必須將 OSP 安裝在 Identity Applications 伺服器上。	1. 若要升級 Identity Applications 和 OSP，請依照「升級 Identity Applications」(第 200 頁) 中的步驟操作。 2. 若要升級其他伺服器上的 SSPR，請依照「升級 SSPR」(第 206 頁) 中的步驟操作。 3. 啟動組態更新公用程式，並提供安裝了 OSP 的新伺服器的詳細資料。在本例中，新伺服器是安裝了 Identity Applications 的伺服器。如需詳細資訊，請參閱「SSO 用戶端參數」(第 117 頁)。

- 如果您要升級在 Open Enterprise Server (OES) 23.4 版本上執行的 Identity Applications，請確定 Identity Manager 引擎使用的 JRE 具有連接至使用者應用程式所需的證書。Identity Manager 驅動程式使用 Identity Manager 引擎的金鑰儲存區來存取使用者應用程式。如果角色與資源服務驅動程式在目標位置無法找到所需證書，您可能會在該驅動程式的追蹤記錄中看到一個錯誤。如需瞭解對此錯誤進行疑難排解的詳細資訊，請參閱 《NetIQ Identity Manager - Administrator's Guide to the Identity Applications》 (NetIQ Identity Manager - Identity Applications 管理員指南)。

系統要求

升級程序會為所安裝元件的目前組態建立備份。確定服務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。如需詳細資訊，請造訪 NetIQ Identity Manager 技術資訊網站 (https://www.microfocus.com/en-us/products/netiq-identity-manager/specs)。

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。當您使用這些組態檔案時，升級程序會在內部呼叫指定元件的升級程式。此外，升級程式還會建立目前安裝的備份。

升級 PostgreSQL

升級 PostgreSQL 需要執行的步驟如下：

1. 從 NetIQ 下載網站下載並解壓縮 `Identity_Manager_4.9.0_Linux.iso`。
2. 導覽至 `/common/scripts` 目錄。
3. 執行以下指令：

   ```
   ./pg-upgrade.sh
   ```
4. 指定以下詳細資料以完成安裝：

   現有 Postgres 的安裝位置：指定 PostgreSQL 的安裝位置。預設位置為 `/opt/netiq/idm/postgres/`。

   附註：確定 Postgres 使用者對 `/opt/netiq/idm/postgres` 目錄具有相應的許可權。

   現有的 Postgres 資料目錄：指定 PostgreSQL 資料目錄所在的位置。預設位置為 `/opt/netiq/idm/postgres/data`。

   現有的 Postgres 資料庫密碼：指定 PostgreSQL 密碼。

   新的 Postgres 資料目錄：指定新的 PostgreSQL 資料目錄。例如 `/opt/netiq/idm/postgres_new/data`。

升級 Identity Applications 元件

- 升級 Identity Applications 的驅動程式套件
- 升級 Identity Applications
- 升級 SSPR

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、角色與資源服務驅動程式，以及資料收集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並選取 「內容」。
2 依次按一下 「套件」、。
3 選取僅顯示適用的套件版本核取方塊。
4 選取建立工作流程範本。
5 按一下確定，然後按一下完成以完成安裝。
6 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合物件。

升級 Identity Applications

下面的程序介紹如何升級 Identity Applications。

1 從 NetIQ 下載網站下載 `Identity_Manager_4.9.0_Linux.iso`。
2 掛接下載的 `.iso`。
3 執行以下指令：

```
./install.sh
```

4 通讀授權合約。
5 輸入 `y` 以接受授權合約。
6 指定是否要升級 Identity Applications。可用選項有 **y** 和 **n**。
7 如果您要繼續升級，請指定以下詳細資料：

用於備份的 OSP 安裝資料夾

僅當 OSP 和 Identity Applications 安裝在同一部伺服器上時才適用。

指定用於儲存 OSP 備份資料的 OSP 備份資料夾。

SSPR 安裝資料夾

僅當 SSPR 和 Identity Applications 安裝在同一部伺服器上時才適用。

指定 SSPR 安裝資料夾。

在系統中未找到 SSPR。是否要安裝並設定？

僅當 Identity Applications 和 SSPR 安裝在不同的伺服器上時才適用。

如果您選取 **y**，將會在安裝了 Identity Applications 的伺服器上安裝 SSPR。您需要將現有的自訂設定複製到安裝 SSPR 的新伺服器上。

- **SSPR 組態密碼**：指定 SSPR 組態密碼。
- **One SSO 伺服器 DNS/IP 位址**：指定安裝了 OSP 的伺服器的 IP 位址。
- **One SSO 伺服器 SSL 連接埠**：指定 OSP SSL 連接埠。

如果您選取 **n**，將不會安裝 SSPR，但會升級 Identity Applications。

使用者應用程式安裝資料夾

指定使用者應用程式安裝資料夾。

Identity Applications One SSO 服務密碼

指定 One SSO 密碼。指定的密碼將更新您在組態更新公用程式中為所有用戶端設定的用戶端機密。如果需要，您可以從組態更新公用程式重設相關用戶端的密碼。如需詳細資訊，請參閱 「SSO 用戶端參數」(第 117 頁)。

Identity Applications 資料庫 JDBC jar 檔案

指定資料庫 JAR 檔案。例如，如果您要使用安裝在同一部伺服器上的 PostgresQL 資料庫，則現有資料庫 jar 檔案的預設位置為 `/opt/netiq/idm/postgres/postgresql-42.6.1.jar`。

建立 Identity Applications 的綱要

指定何時建立資料庫綱要。可用選項有**現在**、**啟動**和**檔案**。預設選項為**現在**。

附註：如果您要使用 MsSQL 或 Oracle，並為 idmadmin 使用者指定對此資料庫的所有權限，則必須建立 `igaworkflowdb`。

Identity Applications 資料庫使用者密碼

指定資料庫管理員密碼

Identity Applications 資料庫管理員密碼

指定資料庫管理員密碼。

8 啟動 Tomcat。如果您選擇立即建立資料庫綱要，請選取**現在**。

```
systemctl start netiq-tomcat.service
```

(選擇性) 在升級期間，如果您選取**啟動**或**寫入檔案**選項來建立資料庫綱要，則必須將資料輸入至工作流程資料庫。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)。

9 重新啟動 NGINX 服務。

```
systemctl restart netiq-nginx.service
```

升級 SSPR

在進階版中，如果 SSPR 未與 Identity Applications 安裝在同一部伺服器上，請使用此方法。

在標準版中，只能透過此方法來升級 SSPR。

若要升級 SSPR，請執行以下操作：

1. 從 NetIQ 下載網站下載 `Identity_Manager_4.9.0_Linux.iso`。
2. 掛接下載的 `.iso`。
3. 從 `.iso` 檔案的根目錄導覽至 `sspr` 目錄。
4. 執行以下指令：

   ```
   ./install.sh
   ```
5. 通讀授權合約。
6. 輸入 `y` 以接受授權合約。
7. 指定 **y** 以升級 SSPR。
8. 指定 **Identity Vault 管理員密碼**並完成升級。

Identity Applications 元件的升級後任務

在開始使用 Identity Applications 之前，請執行以下任務：

- 手動刪除先前版本的 Tomcat 和 ActiveMQ 服務。例如，執行以下指令：

  ```
  /etc/init.d/idmapps_tomcat_init
  ```

  ```
  /etc/init.d/idmapps_activemq_init
  ```
- 您必須手動還原 Tomcat、SSPR、OSP 和 Kerberos 的自訂設定。
- Identity Applications 伺服器的金鑰儲存區 (`idm.jks`) 中應存在 CN 為 Identity Applications 的證書。做為增強的 Java 安全措施的一部分，Identity Applications 現在需要可信證書才能與 OSP 通訊。
- 使用現有的 Identity Applications 金鑰儲存區檔案將已簽署證書輸入至 idm.jks 中。例如：

  ```
  ./keytool -import -alias mycerts -keystore /opt/netiq/idm/apps/tomcat/
  conf/idm.jks -file /opt/certs/chap8.der
  ```

  附註：從版本 4.7.5 升級至 4.9 時需要執行此步驟。
- 如果您是在叢集環境中升級 Identity Applications，則必須在升級 Identity Applications 之後執行以下步驟：
  - 導覽至 `/opt/netiq/idm/apps/tomcat/conf` 目錄，然後在 `context.xml` 檔案的 `Context` 標記中新增下面一行：

    ```
    <Manager notifyListenersOnReplication="true"
    expireSessionsOnShutdown="false"
    className="org.apache.catalina.ha.session.DeltaManager"/>
    ```

- 導覽至 /opt/netiq/idm/apps/tomcat/conf 目錄，然後在 server.xml 檔案的 Cluster 標記中新增下面一行：

```
<Channel className="org.apache.catalina.tribes.group.GroupChannel">
            <Membership
className="org.apache.catalina.tribes.membership.McastService"
                        address="228.0.0.4"
                        port="45564"
                        frequency="500"
                        dropTime="3000"/>
            <Receiver
className="org.apache.catalina.tribes.transport.nio.NioReceiver"
                      address="auto"
                      port="5000"
                      selectorTimeout="100"
                      maxThreads="6"/>

            <Sender
className="org.apache.catalina.tribes.transport.ReplicationTransmit
ter">
              <Transport
className="org.apache.catalina.tribes.transport.nio.PooledParallelS
ender"/>
            </Sender>
            <Interceptor
className="org.apache.catalina.tribes.group.interceptors.TcpFailure
Detector"/>
            <Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDis
patchInterceptor"/>
            <Interceptor
className="org.apache.catalina.tribes.group.interceptors.Throughput
Interceptor"/>
          </Channel>

          <Valve
className="org.apache.catalina.ha.tcp.ReplicationValve"

filter=".*\.gif|.*\.js|.*\.jpeg|.*\.jpg|.*\.png|.*\.htm|.*\.html|.*
\.css|.*\.txt"/>

          <Deployer
className="org.apache.catalina.ha.deploy.FarmWarDeployer"
                    tempDir="/tmp/war-temp/"
                    deployDir="/tmp/war-deploy/"
                    watchDir="/tmp/war-listen/"
                    watchEnabled="false"/>

          <ClusterListener
className="org.apache.catalina.ha.session.ClusterSessionListener"/>
```

- 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

- 如果您的資料庫是透過 SSL 設定的，請在位於 /opt/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

Tomcat

- 在叢集環境中，手動將 server.xml 中的 Cluster 標記取消備註，然後將第一個節點上 /opt/netiq/idm/apps/osp_backup_< 日期 > 中的 osp.jks 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。

SSPR

如果 Identity Applications 和 SSPR 部署在不同的伺服器上，而您選擇將現有的 SSPR 自訂設定還原到安裝了 SSPR 的新伺服器，請務必使用 ConfigUpdate 公用程式修改新 SSPR 伺服器上的 SSPR 設定。如需詳細資訊，請參閱 「SSO 用戶端參數」(第 117 頁)。

One SSO Provider

如果在升級前的設定中，Identity Applications 和 OSP 部署在不同的伺服器上，請將現有的 OSP 設定複製到安裝了 OSP 的新伺服器 (Identity Applications 伺服器)，然後在此伺服器上執行安裝套件中的 merge_jars 方法來還原設定。

1. 在升級了 Identity Applications 的伺服器上停止 Tomcat(升級 Identity Applications 時會安裝 OSP)。
2. 還原自訂設定。
   - **2a** 導覽至現有 OSP 伺服器中的 OSP 安裝目錄，並找到 osp-custom-resource.jar 檔案。

     例如 /opt/netiq/backup_idm/osp/osp-extras/l10n-resources/osp-custom-resource.jar。
   - **2b** 將 osp-custom-resource.jar 檔案複製到升級了 Identity Applications 的伺服器上的某個位置。
   - **2c** 導覽至 <Identity_Manager_4.9.0_Linux.iso 掛接位置 >/osp/scripts/merge_cust_loc.sh。

     此程序檔包含用於將現有自訂設定合併到新安裝的 OSP 的 merge_jars 方法。
   - **2d** 開啟指令提示符並執行以下指令：

```
merge_jars ${IDM_BACKUP_FOLDER in the remote OSP server}/tomcat/lib/
osp-custom-resource.jar ${IDM 4.9_OSP_INSTALLED_HOME}/osp-extras/
l10n-resources/osp-custom-resource.jar)
```

例如：

```
merge_jars /opt/netiq/backup_idm/osp/osp-extras/l10n-resources/osp-
custom-resource.jar /opt/netiq/idm/apps/osp/osp-extras/l10n-
resources/osp-custom-resource.jar
```

其中，`backup_idm` 目錄包含現有 OSP 伺服器中的 OSP 設定。

3 在安裝了 OSP 的新伺服器上啟動 Tomcat。

若要更新其他設定，請參閱 「SSO 用戶端參數」(第 117 頁)。

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`) 存放於舊 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。

升級後驗證版本號碼

升級至 Identity Manager 4.9 後，請驗證元件是否已升級至以下版本：

- Tomcat – `9.0.85`
- ActiveMQ – `5.18.3`
- Java – `1.8.0_222`
- One SSO Provider – `6.7.0`
- Self-Service Password Reset – `4.7.0.1`

升級 Identity Reporting

Identity Reporting 中包含兩個驅動程式。依照以下順序執行升級：

附註：確定資料庫已升級至支援的版本。

1. 將資料庫升級至支援的版本。如需升級 PostgreSQL 資料庫的資訊，請參閱 「升級 PostgreSQL」(第 203 頁)。
2. 升級 Sentinel Log Management for IGA。如需詳細資訊，請參閱 「升級 Sentinel Log Management for IGA」(第 210 頁)。
3. 升級 Identity Reporting。如需詳細資訊，請參閱 「升級 Identity Reporting」(第 210 頁)。

4. 設定受管理系統閘道驅動程式。如需詳細資訊，請參閱 「設定受管理系統閘道驅動程式」(第 137 頁)。
5. 設定資料收集。如需詳細資訊，請參閱 《Administrator Guide to NetIQ Identity Reporting》(NetIQ Identity Reporting 管理員指南) 中的「Configuring Settings and Data Collection」(組態設定和資料收集)。

升級注意事項

在升級期間，請務必指定 `postgresql-9.4.1212.jar` 檔案的正確位置。預設位置為 `/opt/netiq/idm/postgres/`。在下列情況下，資料庫連接將失敗：

- 如果提供的路徑不正確
- 如果提供的 jar 檔案不正確
- 如果啟用了防火牆
- 如果資料庫不接受來自遠端機器的連接

升級 Sentinel Log Management for IGA

1 從 NetIQ 下載網站下載 `SentinelLogManagementForIGA8.6.1.0.tar.gz`。
2 導覽至要擷取檔案的目錄。
3 執行以下指令來擷取檔案：

```
tar -zxvf SentinelLogManagementForIGA8.6.1.0.tar.gz
```

4 導覽至 `SentinelLogManagementforIGA` 目錄。
5 若要安裝 SLM for IGA，請執行以下指令：

```
./install.sh
```

6 指定要用於安裝的語言，然後按 `Enter`。
7 輸入 `y` 以接受授權合約並完成升級。

附註：升級 SLM for IGA 後，請手動輸入最新的收集器。

1. 導覽至 `SentinelLogManagementForIGA8.6.1.0.tar.gz` 檔案的解壓縮目錄。
2. 導覽至 `/content/` 目錄。
3. 輸入並設定收集器。如需詳細資訊，請參閱 《*NetIQ Identity Manager - Configuring Auditing in Identity Manager*》(NetIQ Identity Manager - 在 Identity Manager 中設定稽核) 中的「Installing and Configuring the Sentinel Collectors」(安裝和設定 Sentinel 收集器)。

升級 Identity Reporting

1 從 NetIQ 下載網站下載 `Identity_Manager_4.9.0_Linux.iso`。
2 掛接下載的 `.iso`。
3 執行以下指令：

```
./install.sh
```

4 通讀授權合約。

5 輸入 y 以接受授權合約。

6 指定是否要升級 Identity Manager 元件。可用選項有 **y** 和 **n**。

7 選取 Identity Reporting 以繼續升級。

8 指定以下詳細資料：

已安裝 OSP：指定是否已安裝 OSP。

OSP 安裝資料夾：指定 OSP 的備份安裝資料夾。

用於備份的 Reporting 安裝資料夾：指定 Reporting 安裝資料夾。

您希望何時建立 Identity Reporting 的綱要：指定是要現在還是以後建立資料庫的綱要。可用選項有**現在**、**啟動**和**檔案**。

Identity Reporting 資料庫 JDBC jar 檔案：指定 Identity Reporting 的資料庫 JAR 檔案。現有資料庫 jar 檔案的預設位置為 `/opt/netiq/idm/apps/postgres/postgresql-9.4.1212.jar`。

Identity Reporting 資料庫使用者：指定 Reporting 資料庫使用者的名稱。

Identity Reporting 資料庫帳戶密碼：指定 Reporting 資料庫密碼。

附註：將 Identity Manager 升級至 4.9 後，

- IDMDCS UI 中將不會顯示資料同步規則。如果您打算建立新規則，則必須移除 Sentinel 伺服器中現有的資料同步規則，然後在設定 Identity Reporting 之後使用 IDMDCS UI 建立新的資料同步規則。
- `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 `/opt/netiq/idm/apps/deprecate-tomcat-jre8` 位置備份基於 Java 8 的 tomcat。

Reporting 的升級後步驟

- 在分散式設定中，將 Identity Applications 和 Identity Reporting 從 4.8.x 升級至 4.9 之後，請執行以下步驟：

  1. 執行以下指令以從 Identity Applications 的 `idm.jks` 檔案輸入 OSP 證書，並將其置於新的 Java 金鑰儲存區檔案中：

     ```
     /opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore /opt/netiq/idm/apps/tomcat/conf/idm.jks -srcstorepass novell-destkeystore ./idm.jks -deststorepass novell -srcalias "cn=< 使用者名稱 >, o=< 組織名稱 >" -destalias "cn=< 使用者名稱 >" -noprompt
     ```

     例如：

```
/opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore /
opt/netiq/idm/apps/tomcat/conf/idm.jks -srcstorepass novell-
destkeystore ./idm.jks -deststorepass novell -srcalias "cn=sean,
o=novell" -destalias "cn=sean" -noprompt
```

2. 以這個新建立的金鑰儲存區檔案取代 Identity Reporting 伺服器中現有的 Java 金鑰儲存區檔案，然後重新啟動 Identity Reporting 伺服器。

- 如果在升級期間針對「建立 Identity Reporting 的綱要」選取了**啟動**或**檔案**，請務必執行以下操作：

  1. 登入 Identity Reporting。
  2. 從 Identity Reporting 儲存庫中刪除現有資料來源和報告定義。
  3. 新增新的 Identity Manager 資料收集服務資料來源。

  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。

- 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`

  完成所需的變更後，儲存檔案並重新啟動 Tomcat。

- 如果您的資料庫是透過 SSL 設定的，請在位於 `/opt/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
  ```

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

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 `Identity_Manager_4.8.5_Linux_Analyzer.tar.gz`。

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 檢查程式顯示的是否為新版本。

升級後任務

升級後，請執行以下動作：

升級服務驅動程式

附註：更新驅動程式套件之前，請確定已將 Identity Applications 更新至最新版本。

將 Identity Applications 更新至最新版本後，您可以將使用者應用程式驅動程式套件更新至 4.8.8.20240401125038，將角色與資源服務驅動程式套件更新至 4.8.8.20231216023752，將資料收集服務驅動程式套件更新至 2.4.2.20230627174512。

請執行以下步驟來更新驅動程式套件：

1 開啟包含所需服務驅動程式的專案。

2 在服務驅動程式上按一下滑鼠右鍵，然後按一下**驅動程式** > **內容**。

3 按一下**套件**。

「可用升級」欄中的核取記號表示相應套件有新版本。

4 (視情況而定) 如果是 UAD 套件，請對 `NOVLUABASE_4.8.8.20240401125038.jar` 套件按一下**選取**操作。

5 (視情況而定) 如果是 RRSD 套件，請對 `NOVLRSERVB_4.8.8.20231216023752.jar` 套件按一下**選取**操作。

6 (視情況而定) 如果是 DCS 套件，請對 NOVLRSERVB_2.4.2.20230627174512.jar 套件按一下**選取**操作。

7 在下拉式清單中，按一下**升級**。

8 選取要升級至的版本，然後按一下**確定**。

附註：Designer 會列出可用於升級的所有版本。

9 按一下**套用**。

10 (視情況而定) 在欄位中填寫適當的資訊以升級該套件，然後按**下一步**。

根據您選擇升級的套件，您必須相應地填寫升級該套件所需的資訊。

11 查看將安裝的套件摘要，然後按一下**完成**。

12 查看升級的套件，然後按一下**確定**以關閉「套件維護」頁面。

13 部署變更，然後重新啟動驅動程式。

14 重新啟動 eDirectory 服務。

移除未使用的 Log4j JAR

安裝 Identity Manager 4.9 時，會在 /opt/netiq/idm/lightWeightDesigner/plugins/com.novell.soa.eai.integrationActivity_4.0.0.201910221801/lib 目錄中安裝 log4j-1.2.13.jar。Identity Manager 不再使用此 jar 檔案。請在該目錄中找到並刪除 log4j-1.2.13.jar。

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。

例如，如果您使用的是 Identity Console，請執行以下步驟：

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 215 頁)
- 「使用 Identity Console 從驅動程式集移除舊的伺服器」(第 215 頁)
- 「解除舊伺服器」(第 215 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)。
2. 從此伺服器上移除 eDirectory。

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 216 頁)
- 「使用 Identity Console 將自訂規則和規則還原至驅動程式」(第 216 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 <TBD - provide a link to the book where you will have the Starting the Drivers section>。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相關資訊，請參閱「啟動驅動程式」(第 197 頁)。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。

16 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 Identity Vault `dib` 目錄。

`/var/opt/novell/eDirectory/data/dib`

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 Identity Vault。

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 `/opt/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 < 安裝資料夾 >`/tomcat/conf` 目錄中的 `ism-configuration.properties` 檔案複製到備份目錄。

8 安裝 Identity Reporting。如需詳細資訊，請參閱 第 4 章 「安裝 Identity Manager」 (第 61 頁)。

9 從 *<Reporting 安裝資料夾 >*`/bin` 目錄啟動 `configupdate.sh`，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 `192.168.0.1`)
  - **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，`/opt/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://192.168.0.1:8180/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 99 頁)。

10 儲存變更並結束組態公用程式。

11 啟動 Tomcat。

VII 部署 Identity Manager 容器

Identity Manager 提供了透過容器化機制來部署 Identity Manager 元件的靈活選項。Identity Manager 使用 Docker 來管理容器。支援容器化的 Identity Manager 元件以 Docker 影像的形式提供。Docker 影像是自足性的，能夠獨立執行。

此 Docker 影像可用於以下 Identity Manager 元件：

- Identity Manager 引擎
- 遠端載入器
- One SSO Provider (OSP)
- 擴送代理程式
- ActiveMQ
- PostgreSQL (Redistribution)
- Identity Applications
- Self Service Password Reset (SSPR)
- 表單轉譯器
- Identity Reporting
- Identity Console

附註：Identity Configuration Generator 影像用於產生靜默內容檔案。

可透過企業安裝模式實現的所有功能和操作也可以透過容器化機制來實現。

17 規劃容器部署

下列各節介紹 Docker 環境中基於容器的部署所需的高階規劃：

- 「系統要求」 (第 221 頁)
- 「獲取 Docker 影像」 (第 221 頁)

系統要求

您必須確定符合部署容器的下列要求：

軟體	認證的版本
Docker	24.0.7-ce 或更新版本

獲取 Docker 影像

獲取 Docker 影像需要執行的步驟如下：

1. 從軟體授權和下載 (https://sld.microfocus.com) 入口網站下載 `Identity_Manager_4.9.0_Containers.tar.gz`。
2. 執行以下指令以解壓縮 `.tar` 檔案：

   ```
   tar -zxvf Identity_Manager_4.9.0_Containers.tar.gz
   ```

18 Identity Manager 容器部署

Identity Manager 容器部署程序包括安裝前、安裝期間以及安裝後工作。本章中使用的範例提供有關在進階版中部署容器的資訊，但您也可以在標準版中部署容器。

有些容器相依於其他容器。下表提供了這些相依於其他容器的容器的相關詳細資料。

表格 18-1 *相依的容器*

容器	相依的容器
OSP	• Identity Engine
Identity Applications	• OSP • Identity Applications 的資料庫
表單轉譯器	Identity Applications
Identity Reporting	• Identity Applications • Identity Reporting 的資料庫
SSPR	Identity Applications

最佳實務

本節包含部署 Docker 容器的一些提示和最佳實務：

- NetIQ 建議您為容器設定 CPU 使用量限制。可透過在 docker run 指令中使用 `--cpuset-cpus` 旗標來指定此設定。
- 若要設定容器的重新啟動規則，請在 docker run 指令中使用 `--restart` 旗標。建議選擇故障時重新啟動規則，並將重新啟動嘗試次數限制為 5 次。
- 若要設定容器可使用的記憶體容量限制，請在 docker run 指令中使用 `--memory` 旗標。
- 如果您要備份已部署驅動程式的追蹤檔案，可將追蹤檔案放到 `/config/idm/` 下，或將追蹤檔案手動複製到磁碟區資料夾中。
- 若要設定在任意時間點允許執行的程序數限制，請在 docker run 指令中使用 --pids-limit 旗標。建議將 PID 值限制為 300。
- 對於 Identity Manager 引擎容器，如果您要檢視位於 `/proc` 檔案系統 /process 目錄下的 `environ` 檔案，請在 docker run 指令中使用 `--cap-add=SYS_PTRACE` 旗標。系統預設會限制大部分特權，只會啟用必需的特權。如需詳細資訊，請參閱 Docker 文件。
- 確定協力廠商 jar 檔案為已掛接的磁碟區，這樣每次啟動容器時這些檔案才可用。例如，如果容器的 `/opt/netiq/idm/apps/tomcat/lib` 目錄中存在 `ojdbc.jar`，則您必須使用以下指令對 jar 檔案進行磁碟區掛接操作：

  ```
  -v /host/ojdbc.jar:/opt/netiq/idm/apps/tomcat/lib/ojdbc.jar
  ```

例如，可執行包含上述所有引數的以下範例指令來部署容器：

```
docker run -itd --cap-add=SYS_PTRACE --pids-limit< 調整容器 pid 限制 > --
memory=< 容器可使用的最大記憶體容量 > --restart=on-failure:5 --cpuset-cpus=< 允許
在其中執行的 CPU> --network=< 將容器連接至網路 > -v < 繫結掛接磁碟區 > --name=< 指定
容器的名稱 > < 影像名稱 >
```

管理容器磁碟區資料

Docker 支援使用多種機制來實現資料儲存和持續性。實現容器資料持續性的其中一個機制是使用容器中的共用磁碟區。

本指南中使用的範例假設您建立和使用的是共用磁碟區。例如，在 Docker 主機上建立名為 /data 的共用磁碟區。

```
mkdir /data
```

建立的共用磁碟區需要許可權。使用以下指令提供許可權：

```
chmod -R 777 /data
```

不過，您也可以使用 Docker 支援的其他磁碟區。如需詳細資訊，請參閱 Docker 文件。

附註：確定您對共用磁碟區擁有讀取和寫入許可權。

建立靜默內容檔案

大多數 Identity Manager 容器都提供互動安裝模式。不過，NetIQ 建議使用靜默內容檔案來部署不同的容器。

附註：產生 `silent.properties` 檔案後，會在 Docker 主機的 `/data` 中提供該檔案。

1. 在解壓縮 `Identity_Manager_4.9.0_Containers.tar.gz` 檔案的位置，導覽至 `Identity_Manager_4.9.0_Containers/docker-images` 目錄。
2. 執行以下指令以載入影像：

   ```
   docker load --input IDM_490_idm_conf_generator.tar.gz
   ```

3. 使用以下範例指令部署容器：

   附註：務必將主機名稱的值指定為機器 FQDN。

   ```
   docker run -it --name=idm_conf_generator --
   hostname=identitymanager.example.com -v /data:/config
   idm_conf_generator:idm-4.9.0-580
   ```

4. 導覽至 `idm` 目錄。
5. 執行 `create_silent_props.sh` 檔案：

```
./create_silent_props.sh
```

6 輸入 y 以繼續安裝並設定元件。

7 若要安裝 JRE，請輸入 y。

8 指定內容檔案的路徑。

附註：務必在共用磁碟區的位置 (例如 /config) 建立 silent.properties 檔案。

9 指定以下設定以建立靜默內容檔案：

參數	描述
包含絕對路徑的靜默內容檔案名稱	指定靜默內容檔案的路徑。
設定 Docker 容器的靜默內容	指定是否要為 Docker 容器設定內容檔案。
產生 Kubernetes 協調流程的輸入	*僅當您已在為 Docker 容器設定靜默內容選項中選取了 y 時才適用。* 指定是否要產生 Kubernetes 的 YAML 檔案。
包含用於建立 kube yaml 檔案的絕對路徑的目錄名稱	*僅當您已在產生用於 Kubernetes Orchestration 的輸入選項中選取了 y 時才適用。* 指定用於建立 Kubernetes YAML 檔案的路徑。 **附註：**建議您為 Identity Applications 和 Identity Reporting YAML 檔案提供不同的路徑。
Kubernetes 磁碟區掛接路徑	*僅當您已在「產生用於 Kubernetes Orchestration 的輸入」選項中選取了「y」時才適用。* 指定 Kubernetes 磁碟區的路徑。
Kubernetes 部署的 Identity Manager 引擎主機名稱	*僅當您已在產生用於 Kubernetes Orchestration 的輸入選項中選取了 y 時才適用。* 指定 Identity Manager 引擎的主機名稱。

10 決定要安裝的 Identity Manager 伺服器版本。輸入 y 將安裝進階版，輸入 n 將安裝標準版。

11 決定您是要以一般模式還是自訂模式設定元件。

12 在可供安裝的元件清單中選取所需的元件：

- 若要安裝引擎，請選取 **Identity Manager 引擎**。
- 若要安裝 Identity Reporting，請選取 **Identity Reporting**。
- 若要安裝 Identity Applications，請選取 **Identity Applications**。

如需組態參數的資訊，請參閱 「瞭解組態參數」(第 75 頁)。

附註：

- 必須一次性為所有元件產生 silent.properties 檔案。
- 針對所有與 IP 相關的組態提示使用 FQDN。
- SSO_SERVER_SSL_PORT、TOMCAT_HTTPS_PORT、UA_SERVER_SSL_PORT 和 RPT_TOMCAT_HTTPS_PORT 必須是唯一的連接埠。例如，分別將 SSO_SERVER_SSL_PORT 修改為 8543，將 TOMCAT_HTTPS_PORT 和 UA_SERVER_SSL_PORT 修改為 18543，將 RPT_TOMCAT_HTTPS_PORT 修改為 28543。
- (視情況而定) 如果您要使用主機網路模式在單部伺服器上部署容器，那麼針對特定於 OSP、Identity Applications 和 Identity Reporting 的證書相關提示，必須將 tomcat.ks 路徑指定為 /opt/netiq/idm/apps/tomcat/conf/tomcat.ks。

13 (視情況而定) 如果您要使用主機網路模式在單部伺服器上部署容器，則必須在產生靜默內容檔案後執行以下步驟：

- 確定 CUSTOM_OSP_CERTIFICATE 的值設定為 n。
- 將以下項目新增至 Designer.ini 檔案的結尾處：

```
SKIP_PORT_CHECK=1
CUSTOM_UA_CERTIFICATE="n"
TOMCAT_SSL_KEYSTORE_PASS="<password>"
CUSTOM_RPT_CERTIFICATE="n"
```

部署遠端載入器容器後自動啟動遠端載入器例項

如果您希望在部署遠端載入器容器後自動啟動遠端載入器例項，請執行以下步驟：

1 在 Docker 主機上，導覽至共用目錄。例如 data。

2 建立 rdxml 目錄。

附註：此步驟僅在首次部署容器時適用。換言之，如果您正在更新容器並且以前已建立 rdxml 目錄，請跳過此步驟。

3 導覽至 rdxml 目錄。

4 在 rdxml 目錄中建立 driverconf 目錄。

附註：如果您對不同的遠端載入器例項執行了多個組態檔案，請複製所有檔案。

5 將所有必要的組態檔案複製到 driverconf 目錄。例如 config8000.txt。

6 在 rdxml 目錄中建立 keystore 目錄。

7 將所有必要的金鑰儲存區檔案和證書複製到 keystore 目錄。

8 在 rdxml 目錄中建立一個新的 .txt 檔案。例如 StartupRL.txt。

9 在 StartupRL.txt 檔案中，用以下格式指定所需內容：

< 遠端載入器組態檔案 > -sp < 驅動程式密碼 > < 遠端載入器密碼 >

例如：

```
config8000.txt -sp dirxml dirxml
```

或者，也可以用以下格式指定項目：

< 遠端載入器組態檔案 > -ksp < 金鑰儲存區密碼 > -kp < 金鑰密碼 >

例如：

```
config8000.txt -ksp dirxml -kp dirxml
```

10 透過在 docker run 指令中傳遞 RL_DRIVER_STARTUP 環境變數來部署遠端載入器容器。例如 -e RL_DRIVER_STARTUP="StartupRL.txt"。

容器部署模式

NetIQ 建議使用以下模式來部署容器：

- 在單部伺服器上部署容器
- 在分散式伺服器上部署容器

在單部伺服器上部署容器

此範例使用主機網路模式將所有 Identity Manager 容器部署在單個 Docker 主機上。

先決條件

- 確定主機名稱採用如下所示的 FQDN 格式：

  < 主機 IP> <FQDN> < 簡短名稱 >

  例如：

  ```
  172.120.0.1     identitymanager.example.com      identitymanager
  ```

- 必須在部署容器之前產生靜默內容檔案。如需產生靜默內容檔案的詳細資訊，請參閱「建立靜默內容檔案」(第 224 頁)。

必須依以下順序部署容器：

- 「部署 Identity Manager 引擎容器」(第 228 頁)
- 「部署遠端載入器容器」(第 228 頁)
- 「部署擴送代理程式容器」(第 229 頁)
- 「透過 Identity Vault 證書管理中心產生證書」(第 229 頁)
- 「部署 OSP 容器」(第 231 頁)
- 「部署 PostgreSQL 容器」(第 232 頁)
- 「部署 Identity Applications 容器」(第 233 頁)

- 「部署表單轉譯器容器」(第 234 頁)
- 「部署 ActiveMQ 容器」(第 234 頁)
- 「部署 Identity Reporting 容器」(第 235 頁)
- 「部署 SSPR 容器」(第 236 頁)

部署 Identity Manager 引擎容器

1 產生靜默內容檔案。如需詳細資訊，請參閱建立靜默內容檔案。

2 在解壓縮 Identity_Manager_4.9.0_Containers.tar.gz 檔案的位置，導覽至 Identity_Manager_4.9.0_Containers 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_identityengine.tar.gz
```

4 使用以下指令部署容器：

```
docker run --restart unless-stopped -d --network=host --name=engine-
container -v /data:/config -e SILENT_INSTALL_FILE=/config/
silent.properties --stop-timeout 100 identityengine:idm-4.9.0-580
```

5 若要驗證是否已成功部署容器，請執行以下指令來檢查記錄檔案：

```
tail -f /data/idm/log/idmconfigure.log
```

6 若要登入容器，請執行以下指令：

```
docker exec -it < 容器 > < 指令 >
```

例如：

```
docker exec -it engine-container bash
```

附註：若要執行 ndstrace 或 ndsrepair 等 Identity Vault 公用程式，請以非 root 使用者 nds 的身分登入容器。如果您以 root 使用者身分登入，則無法執行這些公用程式。若要以 nds 使用者身分登入容器，請執行 `docker exec -it engine-container sudo nds` 指令。

部署遠端載入器容器

1 在解壓縮 Identity_Manager_4.9.0_Containers.tar.gz 檔案的位置，導覽至 Identity_Manager_4.9.0_Containers 目錄。

2 執行以下指令以載入影像：

```
docker load --input IDM_490_remoteloader.tar.gz
```

3 使用以下指令部署容器：

```
docker run -d --network=host --name=rl-container -v /data:/config
remoteloader:idm-4.9.0-580
```

此指令會部署 64 位元和 32 位元版本的遠端載入器。容器的 /opt/novell/eDirectory/lib/dirxml/classes/ 目錄中提供了驅動程式檔案。

4 (視情況而定) 如果您不想在部署容器時使用組態檔案，請使用以下指令部署容器：

```
docker run --restart unless-stopped -d --network=host --name=rl-container -v /data:/config --stop-timeout 100 remoteloader:idm-4.9.0-580
```

5 若要登入容器，請執行以下指令：

```
docker exec -it < 容器 > < 指令 >
```

例如：

```
docker exec -it rl-container bash
```

6 設定遠端載入器。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)。

7 確定組態檔案在共用磁碟區中可用。

部署擴送代理程式容器

1 在解壓縮 `Identity_Manager_4.9.0_Containers.tar.gz` 檔案的位置，導覽至 `Identity_Manager_4.9.0_Containers` 目錄。

2 執行以下指令以載入影像：

```
docker load --input IDM_490_fanoutagent.tar.gz
```

3 使用以下指令部署容器：

```
docker run --restart unless-stopped -d --network=host --name=foa-container -v /data:/config --stop-timeout 100 fanoutagent:idm-4.9.0-580
```

4 若要登入容器，請執行以下指令：

```
docker exec -it < 容器 > < 指令 >
```

例如：

```
docker exec -it foa-container bash
```

5 設定擴送代理程式。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)* 中的「Configuring the Fanout Agent」(設定擴送代理程式) (https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/how-to-configure-fan-out-agent.html)。

透過 Identity Vault 證書管理中心產生證書

(視情況而定) 僅當您使用 Identity Vault 做為證書管理中心時，本節內容才適用。

以下元件需要您先產生證書才能部署。在為以下元件產生證書之前，請務必先部署 Identity Manager 引擎和 Identity Console 容器。

- OSP

- Identity Applications
- Identity Reporting

執行以下步驟來產生證書：

1. 確定安裝的 Java 是 Azul Zulu 1.8.0_392 或更新版本。
2. 請務必設定 Java 路徑。例如，執行以下指令：

   ```
   export PATH=<java 安裝位置 >/bin:$PATH
   ```

   例如：

   ```
   export PATH=/opt/netiq/common/jre/bin/:$PATH
   ```

3. 產生 PKCS 金鑰儲存區：

   ```
   keytool -genkey -alias idm -keyalg RSA -storetype pkcs12 -keystore /
   data/tomcat.ks -validity 3650 -keysize 2048 -dname
   "CN=identitymanager.example.com" -keypass <password> -storepass
   <password>
   ```

4. 產生證書簽署申請：

   ```
   keytool -certreq -v -alias idm -file /config/idm.csr -keypass
   <password> -keystore /config/tomcat.ks -storepass <password>
   ```

5. 產生自行簽署的證書：
   - **5a** 啟動 Identity Console 並登入。
   - **5b** 導覽至**證書管理** > **核發證書**。
   - **5c** 瀏覽至在步驟 3 中建立的 `.csr` 檔案。例如 `idm.csr`。
   - **5d** 按一下「**開啟**」。
   - **5e** 在**金鑰使用規範**下拉式清單中指定金鑰類型。
   - **5f** 在**延伸金鑰使用規格**下拉式清單中指定延伸金鑰類型。
   - **5g** 對於證書類型，請在**基本約束**下拉式清單中選取**未指定**。
   - **5h** 在**證書參數**下拉式清單中指定證書的有效期。
   - **5i** 在**證書格式**下拉式清單中選取 **二進位 DER 格式的檔案**。
   - **5j** 按一下「下一步」。
   - **5k** 按一下**確定**。
   - **5l** 下載證書並將其複製到 `/data` 目錄。
6. 輸出 `.der` 格式的根證書：
   - **6a** 啟動 Identity Console 並登入。
   - **6b** 導覽至**證書管理** > **伺服器證書管理**。
   - **6c** 選取 **SSL 證書 DNS** 核取方塊並按一下**輸出**。
   - **6d** 在**證書**下拉式清單中選取「組織 CA」。
   - **6e** 在**輸出格式**下拉式清單中選取 `DER`。
   - **6f** 按一下**確定**。
   - **6g** 下載證書並將其複製到 `/data` 目錄。

7 將證書輸入至您在步驟 2 中建立的 PKCS 金鑰儲存區中：

```
keytool -import -trustcacerts -alias root -keystore /config/tomcat.ks -
file /config/cert.der -storepass <password> -noprompt
```

```
keytool -import -alias idm -keystore /config/tomcat.ks -file /config/
idm.der -storepass <password> -noprompt
```

附註：請確定指定為部署輸入的路徑中有金鑰儲存區。

部署 OSP 容器

1 產生靜默內容檔案。如需詳細資訊，請參閱建立靜默內容檔案。

2 確定 SSO_SERVER_SSL_PORT 內容設定為某個唯一的連接埠。

3 在解壓縮 Identity_Manager_4.9.0_Containers.tar.gz 檔案的位置，導覽至 Identity_Manager_4.9.0_Containers 目錄。

4 執行以下指令以載入影像：

```
docker load --input IDM_490_osp.tar.gz
```

5 使用以下指令部署容器：

```
docker run --restart unless-stopped -d --network=host --name=osp-
container -v /data:/config -e SILENT_INSTALL_FILE=/config/
silent.properties --stop-timeout 100 osp:idm-4.9.0-580
```

6 若要驗證是否已成功部署容器，請執行以下指令來檢查記錄檔案：

```
tail -f /data/osp/log/idmconfigure.log
```

7 使用以下指令來停止容器：

```
docker stop osp-container
```

8 執行以下指令來修改 server.xml 檔案中的 Tomcat 關閉連接埠。在下面的範例中，連接埠 8005 將變更為 18005：

```
sed -i "s~8005~18005~g" /data/osp/tomcat/conf/server.xml
```

9 使用以下指令啟動 容器：

```
docker start osp-container
```

10 若要登入容器，請執行以下指令：

```
docker exec -it < 容器 > < 指令 >
```

例如：

```
docker exec -it osp-container bash
```

部署 PostgreSQL 容器

1 在解壓縮 Identity_Manager_4.9.0_Containers.tar.gz 檔案的位置，導覽至 Identity_Manager_4.9.0_Containers 目錄。

2 執行以下指令以載入影像：

```
docker load --input IDM_490_postgres.tar.gz
```

3 在共用磁碟區 data 下建立一個子目錄，例如 postgres。

```
mkdir postgres
```

4 使用以下指令部署容器：

```
docker run --restart unless-stopped -d --network=host --
name=postgresql-container -e POSTGRES_PASSWORD=<password> -v /data/
postgres:/var/lib/postgresql/data --stop-timeout 100 postgres:12.18
```

例如：

```
docker run --restart unless-stopped -d --network=host --
name=postgresql-container -e POSTGRES_PASSWORD=novell -v /data/
postgres:/var/lib/postgresql/data --stop-timeout 100 postgres:12.18
```

5 建立 Identity Applications 的 idmdamin 使用者。

```
docker exec -it postgresql-container psql -U postgres -c "CREATE USER
idmadmin WITH ENCRYPTED PASSWORD '<password>'"
```

6 建立 Identity Applications、工作流程和 Identity Reporting 資料庫。

```
docker exec -it postgresql-container psql -U postgres -c "CREATE
DATABASE idmuserappdb"

docker exec -it postgresql-container psql -U postgres -c "CREATE
DATABASE igaworkflowdb"

docker exec -it postgresql-container psql -U postgres -c "CREATE
DATABASE idmrptdb"
```

附註：當您設定 Identity Applications 和 Identity Reporting 容器時，會用到這些資料庫。

7 為 idmadmin 使用者授予對資料庫的所有特權：

```
docker exec -it postgresql-container psql -U postgres -c "GRANT ALL
PRIVILEGES ON DATABASE idmuserappdb TO idmadmin"

docker exec -it postgresql-container psql -U postgres -c "GRANT ALL
PRIVILEGES ON DATABASE igaworkflowdb TO idmadmin"
```

8 若要登入容器，請執行以下指令：

```
docker exec -it < 容器 > < 指令 >
```

例如：

```
docker exec -it postgresql-container bash
```

部署 Identity Applications 容器

1 在解壓縮 Identity_Manager_4.9.0_Containers.tar.gz 檔案的位置，導覽至 Identity_Manager_4.9.0_Containers 目錄。

2 執行以下指令以載入影像：

```
docker load --input IDM_490_identityapplication.tar.gz
```

3 使用以下指令部署容器：

```
docker run --restart unless-stopped -d --network=host --name=idapps-
container -v /data:/config -e SILENT_INSTALL_FILE=/config/
silent.properties --stop-timeout 100 identityapplication:idm-4.9.0-580
```

4 若要驗證是否已成功部署容器，請執行以下指令來檢查記錄檔案：

```
tail -f /data/userapp/log/idmconfigure.log
```

5 執行以下指令以輸入金鑰儲存區：

附註：在執行此步驟之前，請確定容器已成功部署。

```
/opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore /config/
tomcat.ks -srcstorepass <password> -destkeystore /opt/netiq/idm/apps/
tomcat/conf/idm.jks -deststorepass <password>
```

6 系統會提示您將覆寫 alias idm 的現有項目。若要覆寫，請輸入 yes。

7 系統會提示您將覆寫 alias root 的現有項目。若要覆寫，請輸入 yes。

8 使用以下指令來停止容器：

```
docker stop idapps-container
```

9 執行以下指令來修改 server.xml 檔案中的 Tomcat 關閉連接埠。在下面的範例中，連接埠 8005 將變更為 28005：

```
sed -i "s~8005~28005~g" /data/userapp/tomcat/conf/server.xml
```

10 使用以下指令啟動 Docker 容器：

```
docker start idapps-container
```

11 若要登入容器，請執行以下指令：

```
docker exec -it < 容器 > < 指令 >
```

例如：

```
docker exec -it idapps-container bash
```

附註：若要在組態更新公用程式中修改任何設定，請從 Identity Applications 容器的 /opt/netiq/idm/apps/configupdate/ 目錄啟動 configupdate.sh。只能在主控台模式下啟動組態更新公用程式。

部署表單轉譯器容器

1. 產生靜默內容檔案。在產生靜默內容檔案時選取 **Identity Applications**。如需詳細資訊，請參閱建立靜默內容檔案。
2. 在解壓縮 `Identity_Manager_4.9.0_Containers.tar.gz` 檔案的位置，導覽至 `Identity_Manager_4.9.0_Containers` 目錄。
3. 執行以下指令以載入影像：

   ```
   docker load --input IDM_490_formrenderer.tar.gz
   ```

4. 使用以下指令部署容器：

   ```
   docker run --restart unless-stopped -d --network=host --name=fr-
   container -v /data:/config -e SILENT_INSTALL_FILE=/config/
   silent.properties --stop-timeout 100 formrenderer:idm-4.9.0-580
   ```

5. 若要登入容器，請執行以下指令：

   ```
   docker exec -it < 容器 > < 指令 >
   ```

   例如：

   ```
   docker exec -it fr-container bash
   ```

部署 ActiveMQ 容器

1. 在解壓縮 `Identity_Manager_4.9.0_Containers.tar.gz` 檔案的位置，導覽至 `Identity_Manager_4.9.0_Containers` 目錄。
2. 執行以下指令以載入影像：

   ```
   docker load --input IDM_490_activemq.tar.gz
   ```

3. 使用以下指令部署容器：

   ```
   docker run --restart unless-stopped -d --network=host --name=amq-
   container -v /data:/config --env-file /data/silent.properties --stop-
   timeout 100 activemq:idm-4.9.0-580
   ```

4. 若要登入容器，請執行以下指令：

   ```
   docker exec -it < 容器 > < 指令 >
   ```

   例如：

   ```
   docker exec -it amq-container bash
   ```

5. 設定 ActiveMQ。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/how-to-setup-activemq-startup-service.html) 中的 *「Setting Up ActiveMQ Startup Service 」(設定 ActiveMQ 啟動服務) (https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/netiq-identity-manager-for-jdbc-fan-out-driver-implementation-guide.html)*。

部署 Identity Reporting 容器

1 在解壓縮 Identity_Manager_4.9.0_Containers.tar.gz 檔案的位置，導覽至 Identity_Manager_4.9.0_Containers 目錄。

2 執行以下指令以載入影像：

```
docker load --input IDM_490_identityreporting.tar.gz
```

3 使用以下指令部署容器：

```
docker run --restart unless-stopped -d --network=host --name=rpt-
container -v /data:/config -e SILENT_INSTALL_FILE=/config/
silent.properties --stop-timeout 100 identityreporting:idm-4.9.0-580
```

4 若要驗證是否已成功部署容器，請執行以下指令來檢查記錄檔案：

```
tail -f /data/reporting/log/idmconfigure.log
```

5 執行以下指令以輸入金鑰儲存區：

附註：在執行此步驟之前，請確定容器已成功部署。

```
/opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore /config/
tomcat.ks -srcstorepass <password> -destkeystore /opt/netiq/idm/apps/
tomcat/conf/idm.jks -deststorepass <password>
```

6 系統會提示您將覆寫 alias idm 的現有項目。若要覆寫，請輸入 yes。

7 系統會提示您將覆寫 alias root 的現有項目。若要覆寫，請輸入 yes。

8 使用以下指令來停止容器：

```
docker stop rpt-container
```

9 執行以下指令來修改 server.xml 檔案中的 Tomcat 關閉連接埠。在下面的範例中，連接埠 8005 將變更為 38005：

```
sed -i "s~8005~38005~g" /data/reporting/tomcat/conf/server.xml
```

10 *(視情況而定) 僅當您使用 Identity Vault 做為證書管理中心時才適用。*

在 setenv.sh 檔案的 export CATALINA_OPTS 項目中新增 -Dcom.sun.net.ssl.checkRevocation=false 參數。在此範例中，setenv.sh 檔案位於 /data/reporting/tomcat/bin/ 目錄下。

11 使用以下指令啟動 Docker 容器：

```
docker start rpt-container
```

12 若要登入容器，請執行以下指令：

```
docker exec -it < 容器 > < 指令 >
```

例如：

```
docker exec -it rpt-container bash
```

部署 SSPR 容器

部署 SSPR 容器需要執行的任務如下：

1 產生 SSPR 的靜默內容檔案。如需詳細資訊，請參閱建立靜默內容檔案。

2 在共用磁碟區 data 下建立一個子目錄，例如 sspr。

```
mkdir sspr
```

3 在解壓縮 Identity_Manager_4.9.0_Containers.tar.gz 檔案的位置，導覽至 Identity_Manager_4.9.0_Containers 目錄。

4 執行以下指令以載入影像：

```
docker load --input IDM_490_sspr.tar.gz
```

5 使用以下範例指令部署容器：

```
docker run --restart unless-stopped -d --network=host --name=sspr-
container -v /data/sspr:/config --stop-timeout 100 sspr/sspr-
webapp:4.7.0.1-580
```

6 在 Docker 主機上執行以下指令，以將 Docker 主機中的 silent.properties 檔案複製到 SSPR 容器：

```
docker cp /data/silent.properties sspr-container:/tmp
```

7 將靜默內容檔案載入到 SSPR 容器。

```
docker exec -it sspr-container /app/command.sh ImportPropertyConfig /
tmp/silent.properties
```

附註：檢查是否在 SSPR 容器的 /config 目錄下建立了 SSPRConfiguration.xml，並驗證該檔案的內容。

---

8 將 OAuth 證書輸入至 SSPR 中：

8a 在 Docker 主機上編輯 /data/sspr/ 目錄中的 SSPRConfiguration.xml 檔案，將 configIsEditable 旗標的值設定為 **true** 並儲存變更。

8b 啟動瀏覽器並輸入 https://identitymanager.example.com:8443/sspr URL。

8c 使用管理員身分證明 (例如 uaadmin) 登入。

8d 按一下右上角的使用者 (例如 uaadmin)，然後按一下**組態編輯器**。

8e 指定組態密碼，然後按一下**登入**。

8f 按一下**設定** > **單一登入 (SSO) 用戶端** > **OAuth**，確定所有 URL 都使用 HTTPS 通訊協定和正確的連接埠。

8g 在 **OAuth 伺服器證書**下，按一下**從伺服器輸入**以輸入新證書，然後按一下**確定**。

8h 按一下右上角的 以儲存證書。

8i 檢視變更並按一下**確定**。

8j SSPR 應用程式重新啟動之後，編輯 SSPRConfiguration.xml 檔案，將 configIsEditable 旗標的值設定為 **true** 並儲存變更。

部署 Identity Console 容器

如需部署 Identity Console 容器的詳細資訊，請參閱 Deploying Identity Console as Docker Container (將 Identity Console 部署為 Docker 容器)。

在分散式伺服器上部署容器

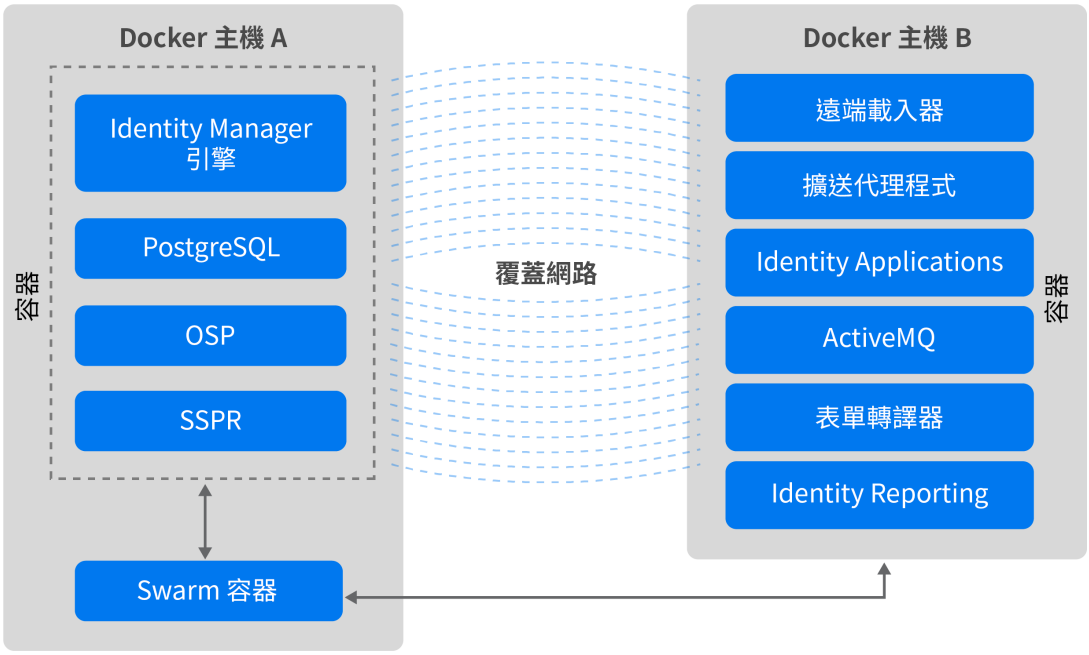
設定覆蓋網路

NetIQ 建議您使用覆蓋網路或橋接網路模式在分散式設定中部署所有 Identity Manager 容器。本指南中所述的方案特定於覆蓋網路中的容器部署。但是，您也可以使用橋接網路來部署容器。在以下分散式伺服器方案中，Identity Manager 引擎、PostgreSQL、OSP 和 SSPR 容器將部署在 Docker 主機 A 上。遠端載入器、擴送代理程式、Identity Applications、ActiveMQ、表單渲染器和 Identity Reporting 容器將部署在 Docker 主機 B 上。

下圖演示了部署在覆蓋網路中兩部 Docker 主機上的 Identity Manager 容器。

附註：由於不再支援叢集儲存，我們可以使用 Docker swarm 來設定覆蓋網路。若要詳細瞭解棄用了哪些功能，請查看「cluster store」(叢集儲存) (https://docs.docker.com/engine/deprecated/#classic-swarm-and-overlay-networks-using-cluster-store)。

***圖 18-1** 覆蓋網路中的容器部署架構*



設定重疊網路需要執行的步驟如下：

1 在 Docker 主機 A 上執行以下指令：

```
docker swarm init
```

2 記下依據步驟 1 的輸出產生的 join 指令，然後在 Docker 主機 B 上執行此 join 指令，以便在這兩部主機之間建立 swarm 網路。

例如：

```
docker swarm join --token SWMTKN-1-
24vozonapa4anwszd3ykthgomo84e9y3p3vbcrtibz6jzo94k2-
148g7yrnepmz963x3z5udnae4 10.71.142.191:2377
```

附註：如果您前面來不及記下用於連接工作節點的指令，請執行以下指令來取得該 join 指令：

```
docker swarm join-token worker
```

3 執行以下指令來檢查所有主機的狀態：

```
docker node ls
```

4 使用以下指令在 Docker 主機 B 上建立覆蓋網路：

```
docker network create --driver overlay --subnet=<subnet-cidr> --
gateway=<gateway-ip> --attachable <network-name>
```

例如：

```
docker network create --driver overlay --subnet=192.168.0.0/24 --
gateway=192.168.0.1 --attachable idmoverlaynetwork
```

5 執行以下指令來驗證是否已建立覆蓋網路：

```
docker network ls
```

附註：由於 swarm 會動態指定 IP，因此在容器部署期間，請確定 swarm 負載平衡器使用尚未由任何 Identity Manager 元件佔用的新 IP 位址，否則您可能會遇到以下錯誤：

來自精靈的錯誤回應：掛接網路失敗，請確定您的網路選項正確，並檢查管理員記錄：已超過網路位置期限

執行以下指令來檢查 swarm 負載平衡器的 IP：

```
docker inspect idmoverlaynetwork | grep lb-idmoverlaynetwork -A 7
```

先決條件

- 對於 Docker 部署中的所有 Docker 主機，必須使用主機上執行的所有容器的詳細資料來更新該主機的 /etc/hosts 檔案。確定所有容器的主機名稱僅採用完全合格的網域名稱 (FQDN) 格式。

  所有元件的主機檔案項目可採用以下格式：

  < 容器的 IP> <FQDN> < 簡短名稱 >

  在本指南使用的範例部署中，於 /etc/hosts 檔案中新增以下項目：

```
192.168.0.12     identityengine.example.com       identityengine
192.168.0.2     remoteloader.example.com         remoteloader
192.168.0.3     fanoutagent.example.com          fanoutagent
192.168.0.5     osp.example.com                  osp
192.168.0.6     postgresql.example.com           postgresql
192.168.0.7     identityapps.example.com         identityapps
192.168.0.8     formrenderer.example.com         formrenderer
192.168.0.9     activemq.example.com             activemq
192.168.0.10    identityreporting.example.com    identityreporting
192.168.0.11    sspr.example.com                 sspr
```

- 確定協力廠商 jar 檔案為已掛接的磁碟區，這樣每次啟動容器時這些檔案才可用。例如，如果容器的 `/opt/netiq/idm/apps/tomcat/lib` 目錄中存在 `ojdbc.jar`，則您必須使用如下範例指令對 jar 檔案進行磁碟區掛接操作：

  ```
  -v /host/ojdbc.jar:/opt/netiq/idm/apps/tomcat/lib/ojdbc.jar
  ```

- 必須在部署容器之前產生靜默內容檔案。如需產生靜默內容檔案的詳細資訊，請參閱「建立靜默內容檔案」(第 224 頁)。

公開容器存取的連接埠

做為先決條件，您必須知道要用於容器的連接埠。您必須公開所需的連接埠，並將容器連接埠對應至 Docker 主機上的連接埠。下表依據指南中的範例提供了您必須在 Docker 主機上公開的連接埠資訊。

表格 18-2 *根據範例部署公開的預設連接埠*

容器	假定根據範例部署使用的預設連接埠
遠端載入器	8090
擴送代理程式	不適用
OSP	8543
Identity Applications	18543
Identity Reporting	28543
表單轉譯器	8600
ActiveMQ	◆ 8161 ◆ 61616
PostgreSQL	5432
SSPR	8443 **附註：**SSRP 容器僅可在 8443 連接埠上執行。

不過，您可以依據自己的需要自訂連接埠。在公開連接埠時，請遵循以下注意事項：

- 確定您要公開的並非使用中的連接埠。
- 必須將容器連接埠對應至 Docker 主機上的相同連接埠。例如，必須將容器上的 8543 連接埠對應至 Docker 主機上的 8543 連接埠。

必須依以下順序部署容器：

- 「部署 Identity Manager 引擎容器」(第 240 頁)
- 「部署遠端載入器容器」(第 241 頁)
- 「部署擴送代理程式容器」(第 241 頁)
- 「部署 OSP 容器」(第 246 頁)
- 「部署 PostgreSQL 容器」(第 246 頁)
- 「部署 Identity Applications 容器」(第 247 頁)
- 「部署表單轉譯器容器」(第 248 頁)
- 「部署 ActiveMQ 容器」(第 249 頁)
- 「部署 Identity Reporting 容器」(第 249 頁)
- 「部署 SSPR 容器」(第 250 頁)

部署 Identity Manager 引擎容器

1. 產生靜默內容檔案。如需詳細資訊，請參閱建立靜默內容檔案。
2. 在解壓縮 `Identity_Manager_4.9.0_Containers.tar.gz` 檔案的位置，導覽至 `Identity_Manager_4.9.0_Containers` 目錄。
3. 執行以下指令以載入影像：

   ```
   docker load --input IDM_490_identityengine.tar.gz
   ```
4. 使用以下指令部署容器：

   ```
   docker run --restart unless-stopped -d --ip=192.168.0.12 --
   network=idmoverlaynetwork --hostname=identityengine.example.com --
   name=engine-container -v /etc/hosts:/etc/hosts -v /data:/config -p
   8028:8028 -p 524:524 -p 389:389 -p 8030:8030 -p 636:636 -e
   SILENT_INSTALL_FILE=/config/silent.properties --stop-timeout 100
   identityengine:idm-4.9.0-580
   ```
5. 若要驗證是否已成功部署容器，請執行以下指令來檢查記錄檔案：

   ```
   tail -f /data/idm/log/idmconfigure.log
   ```
6. 若要登入容器，請執行以下指令：

   ```
   docker exec -it < 容器 > < 指令 >
   ```

   例如：

   ```
   docker exec -it engine-container bash
   ```

附註：若要執行 ndstrace 或 ndsrepair 等 Identity Vault 公用程式，請以非 root 使用者 nds 的身分登入容器。如果您以 root 使用者身分登入，則無法執行這些公用程式。若要以 nds 使用者身分登入容器，請執行 `docker exec -it engine-container sudo nds` 指令。

部署遠端載入器容器

1. 在解壓縮 Identity_Manager_4.9.0_Containers.tar.gz 檔案的位置，導覽至 Identity_Manager_4.9.0_Containers 目錄。
2. 執行以下指令以載入影像：

   ```
   docker load --input IDM_490_remoteloader.tar.gz
   ```

3. 使用以下指令部署容器：

   ```
   docker run -d --ip=192.168.0.2 --network=idmoverlaynetwork --
   hostname=remoteloader.example.com -p 8090:8090 --name=rl-container -v /
   etc/hosts:/etc/hosts -v /data:/config remoteloader:idm-4.9.0-580
   ```

   此指令會部署 64 位元和 32 位元版本的遠端載入器。容器的 /opt/novell/eDirectory/lib/dirxml/classes/ 目錄中提供了驅動程式檔案。

4. (視情況而定) 如果您不想在部署容器時使用組態檔案，請使用以下指令部署容器：

   ```
   docker run --restart unless-stopped -d --ip=192.168.0.2 --
   network=idmoverlaynetwork --hostname=remoteloader.example.com -p
   8090:8090 --name=rl-container -v /etc/hosts:/etc/hosts -v /data:/config
   --stop-timeout 100 remoteloader:idm-4.9.0-580
   ```

5. 若要登入容器，請執行以下指令：

   ```
   docker exec -it < 容器 > < 指令 >
   ```

   例如：

   ```
   docker exec -it rl-container bash
   ```

6. 設定遠端載入器。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)。

部署擴送代理程式容器

1. 在解壓縮 Identity_Manager_4.9.0_Containers.tar.gz 檔案的位置，導覽至 Identity_Manager_4.9.0_Containers 目錄。
2. 執行以下指令以載入影像：

   ```
   docker load --input IDM_490_fanoutagent.tar.gz
   ```

3. 使用以下指令部署容器：

   ```
   docker run --restart unless-stopped -d --ip=192.168.0.3 --
   network=idmoverlaynetwork --hostname=fanoutagent.example.com --
   name=foa-container -v /etc/hosts:/etc/hosts -v /data:/config --stop-
   timeout 100 fanoutagent:idm-4.9.0-580
   ```

4 若要登入容器，請執行以下指令：

```
docker exec -it < 容器 > < 指令 >
```

例如：

```
docker exec -it foa-container bash
```

5 設定擴送代理程式。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) 中的 「Configuring the Fanout Agent」 (設定擴送代理程式) (https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/how-to-configure-fan-out-agent.html)。

透過 Identity Vault 證書管理中心產生證書

(視情況而定) 僅當您使用 Identity Vault 做為證書管理中心時，本節內容才適用。

下列元件需要您先產生證書才能部署。在為以下元件產生證書之前，請務必先部署 Identity Manager 引擎容器。

- OSP
- Identity Applications
- Identity Reporting

產生 OSP 的證書

產生證書需要執行的步驟如下：

1 確定安裝的 Java 是 Azul Zulu 1.8.0_392 或更新版本。

2 確定在 Docker 主機中設定 Java 路徑。例如，執行以下指令：

```
export PATH=<java installed location>/bin:$PATH
```

例如：

```
export PATH=/opt/netiq/common/jre/bin/:$PATH
```

3 產生 PKCS 金鑰儲存區：

```
keytool -genkey -alias osp -keyalg RSA -storetype pkcs12 -keystore /
data/tomcat-osp.ks -validity 3650 -keysize 2048 -dname
"CN=osp.example.com" -keypass <password> -storepass <password>
```

4 產生證書簽署申請：

```
keytool -certreq -v -alias osp -file /config/osp.csr -keypass
<password> -keystore /config/tomcat-osp.ks -storepass <password>
```

5 產生自行簽署的證書：

5a 啟動 Identity Console 並登入。

5b 導覽至**證書管理** > **核發證書**。

5c 瀏覽至在步驟 3 中建立的 .csr 檔案。例如 osp.csr。

5d 按一下「開啟」。

5e 在金鑰使用規範下拉式清單中指定金鑰類型。

5f 在延伸金鑰使用規格下拉式清單中指定延伸金鑰類型。

5g 對於證書類型，請在基本約束下拉式清單中選取未指定。

5h 在證書參數下拉式清單中指定證書的有效期。

5i 在證書格式下拉式清單中選取 二進位 DER 格式的檔案。

5j 按一下「下一步」。

5k 按一下確定。

5l 下載證書並將其複製到 /data 目錄。

6 輸出 .der 格式的根證書：

6a 啟動 Identity Console 並登入。

6b 導覽至證書管理 > 伺服器證書管理。

6c 選取 SSL 證書 DNS 核取方塊並按一下輸出。

6d 在證書下拉式清單中選取「組織 CA」。

6e 在輸出格式下拉式清單中選取 DER。

6f 按一下確定。

6g 下載證書並將其複製到 /data 目錄。

7 將證書輸入至您在步驟 2 中建立的 PKCS 金鑰儲存區中：

```
keytool -import -trustcacerts -alias root -keystore /config/tomcat-
osp.ks -file /config/cert.der -storepass <password> -noprompt
```

```
keytool -import -alias osp -keystore /config/tomcat-osp.ks -file /
config/osp.der -storepass <password> -noprompt
```

附註：請確定指定為部署輸入的路徑中有金鑰儲存區。

產生 Identity Applications 的證書

產生證書需要執行的步驟如下：

1 確定安裝的 Java 是 Azul Zulu 1.8.0_392 或更新版本。

2 請務必設定 Java 路徑。例如，執行以下指令：

```
export PATH=<java installed location>/bin:$PATH
```

例如：

```
export PATH=/opt/netiq/common/jre/bin/:$PATH
```

3 產生 PKCS 金鑰儲存區：

```
keytool -genkey -alias ua -keyalg RSA -storetype pkcs12 -keystore /
config/tomcat-ua.ks -validity 3650 -keysize 2048 -dname
"CN=identityapps.example.com" -keypass <password> -storepass <password>
```

4 產生證書簽署申請：

```
keytool -certreq -v -alias ua -file /config/ua.csr -keypass <password>
-keystore /config/tomcat-ua.ks -storepass <password>
```

5 產生自行簽署的證書：

5a 啟動 Identity Console 並登入。

5b 導覽至**證書管理** > **核發證書**。

5c 瀏覽至在步驟 3 中建立的 .csr 檔案。例如 ua.csr。

5d 按一下「**開啟**」。

5e 在**金鑰使用規範**下拉式清單中指定金鑰類型。

5f 在**延伸金鑰使用規格**下拉式清單中指定延伸金鑰類型。

5g 對於證書類型，請在**基本約束**下拉式清單中選取**未指定**。

5h 在**證書參數**下拉式清單中指定證書的有效期。

5i 在**證書格式**下拉式清單中選取 **二進位 DER 格式的檔案**。

5j 按一下「下一步」。

5k 按一下**確定**。

5l 下載證書並將其複製到 /data 目錄。

6 輸出 .der 格式的根證書：

6a 啟動 Identity Console 並登入。

6b 導覽至**證書管理** > **伺服器證書管理**。

6c 選取 **SSL 證書 DNS** 核取方塊並按一下**輸出**。

6d 在**證書**下拉式清單中選取「組織 CA」。

6e 在**輸出格式**下拉式清單中選取 DER。

6f 按一下**確定**。

6g 下載證書並將其複製到 /data 目錄。

7 將證書輸入至步驟 2 中的 PKCS 金鑰儲存區：

```
keytool -import -trustcacerts -alias root -keystore /config/tomcat-
ua.ks -file /config/cert.der -storepass <password> -noprompt
```

```
keytool -import -alias ua -keystore /config/tomcat-ua.ks -file /config/
ua.der -storepass <password> -noprompt
```

附註：請確定指定為部署輸入的路徑中有證書。

產生 Identity Reporting 的證書

產生證書需要執行的步驟如下：

1 確定安裝的 Java 是 Azul Zulu 1.8.0_392 或更新版本。

2 請務必設定 Java 路徑。例如，執行以下指令：

```
export PATH=<java installed location>/bin:$PATH
```

例如：

```
export PATH=/opt/netiq/common/jre/bin/:$PATH
```

3 產生 PKCS 金鑰儲存區：

```
keytool -genkey -alias rpt -keyalg RSA -storetype pkcs12 -keystore /
config/tomcat-rpt.ks -validity 3650 -keysize 2048 -dname
"CN=identityreporting.example.com" -keypass <password> -storepass
<password>
```

4 產生證書簽署申請：

```
keytool -certreq -v -alias rpt -file /config/rpt.csr -keypass
<password> -keystore /config/tomcat-rpt.ks -storepass <password>
```

5 產生自行簽署的證書：

5a 啟動 Identity Console 並登入。

5b 導覽至**證書管理** > **核發證書**。

5c 瀏覽至在步驟 3 中建立的 .csr 檔案。例如 rpt.csr。

5d 按一下「**開啟**」。

5e 在**金鑰使用規範**下拉式清單中指定金鑰類型。

5f 在**延伸金鑰使用規格**下拉式清單中指定延伸金鑰類型。

5g 對於證書類型，請在**基本約束**下拉式清單中選取**未指定**。

5h 在**證書參數**下拉式清單中指定證書的有效期。

5i 在**證書格式**下拉式清單中選取 **二進位 DER 格式的檔案**。

5j 按一下「下一步」。

5k 按一下**確定**。

5l 下載證書並將其複製到 /data 目錄。

6 輸出 .der 格式的根證書：

6a 啟動 Identity Console 並登入。

6b 導覽至**證書管理** > **伺服器證書管理**。

6c 選取 **SSL 證書 DNS** 核取方塊並按一下**輸出**。

6d 在**證書**下拉式清單中選取「組織 CA」。

6e 在**輸出格式**下拉式清單中選取 DER。

6f 按一下**確定**。

6g 下載證書並將其複製到 /data 目錄。

7 將證書輸入至您在步驟 2 中建立的 PKCS 金鑰儲存區中：

```
keytool -import -trustcacerts -alias root -keystore /config/tomcat-
rpt.ks -file /config/cert.der -storepass <password> -noprompt
```

```
keytool -import -alias rpt -keystore /config/tomcat-rpt.ks -file /
config/rpt.der -storepass <password> -noprompt
```

附註：請確定指定為部署輸入的路徑中有證書。

部署 OSP 容器

附註：在部署 OSP 容器之前，請務必產生所需的證書。如需詳細資訊，請參閱產生 OSP 的證書。

1. 產生靜默內容檔案。如需詳細資訊，請參閱建立靜默內容檔案。
2. 在解壓縮 Identity_Manager_4.9.0_Containers.tar.gz 檔案的位置，導覽至 Identity_Manager_4.9.0_Containers 目錄。
3. 執行以下指令以載入影像：

   ```
   docker load --input IDM_490_osp.tar.gz
   ```

4. 使用以下指令部署容器：

   ```
   docker run --restart unless-stopped -d --ip=192.168.0.5 --
   network=idmoverlaynetwork --hostname=osp.example.com -p 8543:8543 --
   name=osp-container -v /etc/hosts:/etc/hosts -v /data:/config -e
   SILENT_INSTALL_FILE=/config/silent.properties --stop-timeout 100
   osp:idm-4.9.0-580
   ```

5. 若要驗證是否已成功部署容器，請執行以下指令來檢查記錄檔案：

   ```
   tail -f /data/osp/log/idmconfigure.log
   ```

6. 若要登入容器，請執行以下指令：

   ```
   docker exec -it < 容器 > < 指令 >
   ```

   例如：

   ```
   docker exec -it osp-container bash
   ```

部署 PostgreSQL 容器

1. 在解壓縮 Identity_Manager_4.9.0_Containers.tar.gz 檔案的位置，導覽至 Identity_Manager_4.9.0_Containers 目錄。
2. 執行以下指令以載入影像：

   ```
   docker load --input IDM_490_postgres.tar.gz
   ```

3. 在共用磁碟區 data 下建立一個子目錄，例如 postgres。

   ```
   mkdir postgres
   ```

4. 使用以下範例指令部署容器：

   ```
   docker run --restart unless-stopped -d --ip=192.168.0.6 --
   network=idmoverlaynetwork --hostname=postgresql.example.com --
   name=postgresql-container -p 5432:5432 -e POSTGRES_PASSWORD=<password>
   -v /data/postgres:/var/lib/postgresql/data -v /etc/hosts:/etc/hosts -v
   /data:/config --stop-timeout 100 postgres:12.18
   ```

例如：

```
docker run --restart unless-stopped -d --ip=192.168.0.6 --
network=idmoverlaynetwork --hostname=postgresql.example.com --
name=postgresql-container -p 5432:5432 -e POSTGRES_PASSWORD=novell -v /
data/postgres:/var/lib/postgresql/data -v /etc/hosts:/etc/hosts -v /
data:/config --stop-timeout 100 postgres:12.18
```

5 建立 Identity Applications 的 idmdamin 使用者。

```
docker exec -it postgresql-container psql -U postgres -c "CREATE USER
idmadmin WITH ENCRYPTED PASSWORD '<password>'"
```

6 建立 Identity Applications、工作流程和 Identity Reporting 資料庫。

```
docker exec -it postgresql-container psql -U postgres -c "CREATE
DATABASE idmuserappdb"
```

```
docker exec -it postgresql-container psql -U postgres -c "CREATE
DATABASE igaworkflowdb"
```

```
docker exec -it postgresql-container psql -U postgres -c "CREATE
DATABASE idmrptdb"
```

附註：當您設定 Identity Applications 和 Identity Reporting 容器時，會用到這些資料庫。

7 為 idmadmin 使用者授予對資料庫的所有特權：

```
docker exec -it postgresql-container psql -U postgres -c "GRANT ALL
PRIVILEGES ON DATABASE idmuserappdb TO idmadmin"
```

```
docker exec -it postgresql-container psql -U postgres -c "GRANT ALL
PRIVILEGES ON DATABASE igaworkflowdb TO idmadmin"
```

8 若要登入容器，請執行以下指令：

```
docker exec -it < 容器 > < 指令 >
```

例如：

```
docker exec -it postgresql-container bash
```

部署 Identity Applications 容器

附註：在部署 Identity Applications 容器之前，請務必產生所需的證書。如需詳細資訊，請參閱產生 Identity Applications 的證書。

1 產生靜默內容檔案。如需詳細資訊，請參閱建立靜默內容檔案。

附註：將應用程式伺服器連接埠的值指定為公開的連接埠 18543。

2 在解壓縮 Identity_Manager_4.9.0_Containers.tar.gz 檔案的位置，導覽至 Identity_Manager_4.9.0_Containers 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_identityapplication.tar.gz
```

4 使用以下指令部署容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.7 --
network=idmoverlaynetwork --hostname=identityapps.example.com -p
18543:18543 --name=idapps-container -v /etc/hosts:/etc/hosts -v /data:/
config -e SILENT_INSTALL_FILE=/config/silent.properties --stop-timeout
100 identityapplication:idm-4.9.0-580
```

5 若要驗證是否已成功部署容器，請執行以下指令來檢查記錄檔案：

```
tail -f /data/userapp/log/idmconfigure.log
```

6 若要登入容器，請執行以下指令：

```
docker exec -it < 容器 > < 指令 >
```

例如：

```
docker exec -it idapps-container bash
```

7 執行以下指令：

附註：在執行此步驟之前，請確定容器已成功部署。

```
/opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore /config/
tomcat-osp.ks -srcstorepass <password> -destkeystore /opt/netiq/idm/
apps/tomcat/conf/idm.jks -deststorepass <password>
```

8 輸入 yes 以覆寫 root 別名的項目。

9 重新啟動 Identity Applications 容器。

```
docker restart idapps-container
```

附註：若要在組態更新公用程式中修改任何設定，請從 Identity Applications 容器的 /opt/netiq/idm/apps/configupdate/ 目錄啟動 configupdate.sh。只能在主控台模式下啟動組態更新公用程式。

部署表單轉譯器容器

1 產生靜默內容檔案。如需詳細資訊，請參閱建立靜默內容檔案。

2 在解壓縮 Identity_Manager_4.9.0_Containers.tar.gz 檔案的位置，導覽至 Identity_Manager_4.9.0_Containers 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_formrenderer.tar.gz
```

4 使用以下指令部署容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.8 --
network=idmoverlaynetwork --hostname=formrenderer.example.com -p
8600:8600 --name=fr-container -v /etc/hosts:/etc/hosts -v /data:/config
-e SILENT_INSTALL_FILE=/config/silent.properties --stop-timeout 100
formrenderer:idm-4.9.0-580
```

5 若要登入容器，請執行以下指令：

```
docker exec -it < 容器 > < 指令 >
```

例如：

```
docker exec -it fr-container bash
```

部署 ActiveMQ 容器

1. 產生靜默內容檔案。如需詳細資訊，請參閱建立靜默內容檔案。
2. 在解壓縮 `Identity_Manager_4.9.0_Containers.tar.gz` 檔案的位置，導覽至 `Identity_Manager_4.9.0_Containers` 目錄。
3. 執行以下指令以載入影像：

   ```
   docker load --input IDM_490_activemq.tar.gz
   ```

4. 使用以下指令部署容器：

   ```
   docker run --restart unless-stopped -d --ip=192.168.0.9 --
   network=idmoverlaynetwork --hostname=activemq.example.com -p
   61616:61616 --name=amq-container -v /etc/hosts:/etc/hosts -v /data:/
   config --env-file /data/silent.properties --stop-timeout 100
   activemq:idm-4.9.0-580
   ```

5. 若要登入容器，請執行以下指令：

   ```
   docker exec -it < 容器 > < 指令 >
   ```

   例如：

   ```
   docker exec -it amq-container bash
   ```

6. 設定 ActiveMQ。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/how-to-setup-activemq-startup-service.html) 中的 *「Setting Up ActiveMQ Startup Service 」(設定 ActiveMQ 啟動服務) (https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/netiq-identity-manager-for-jdbc-fan-out-driver-implementation-guide.html)*。

部署 Identity Reporting 容器

附註：在部署 Identity Reporting 容器之前，請務必產生所需的證書。如需詳細資訊，請參閱產生 Identity Reporting 的證書。

1. 產生靜默內容檔案。如需詳細資訊，請參閱建立靜默內容檔案。

   附註：將應用程式伺服器連接埠的值指定為公開的連接埠 28543。

2. 在解壓縮 `Identity_Manager_4.9.0_Containers.tar.gz` 檔案的位置，導覽至 `Identity_Manager_4.9_Containers` 目錄。
3. 執行以下指令以載入影像：

```
docker load --input IDM_490_identityreporting.tar.gz
```

4 使用以下指令部署容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.10 --
network=idmoverlaynetwork --hostname=identityreporting.example.com -p
28543:28543 --name=rpt-container -v /etc/hosts:/etc/hosts -v /data:/
config -e SILENT_INSTALL_FILE=/config/silent.properties --stop-timeout
100 identityreporting:idm-4.9.0-580
```

5 若要驗證是否已成功部署容器，請執行以下指令來檢查記錄檔案：

```
tail -f /data/reporting/log/idmconfigure.log
```

6 若要登入容器，請執行以下指令：

```
docker exec -it < 容器 > < 指令 >
```

例如：

```
docker exec -it rpt-container bash
```

7 執行以下指令：

附註：在執行此步驟之前，請確定容器已成功部署。

```
/opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore /config/
tomcat-osp.ks -srcstorepass <password> -destkeystore /opt/netiq/idm/
apps/tomcat/conf/idm.jks -deststorepass <password>
```

8 輸入 yes 以覆寫 root 別名的項目。

9 重新啟動 Identity Reporting 容器。

```
docker restart rpt-container
```

部署 SSPR 容器

部署 SSPR 容器需要執行的任務如下：

1 產生 SSPR 的靜默內容檔案。在產生靜默內容檔案時選取 **Identity Applications**。如需詳細資訊，請參閱建立靜默內容檔案。

2 在共用磁碟區 data 下建立一個子目錄，例如 sspr。

```
mkdir sspr
```

3 在解壓縮 Identity_Manager_4.9.0_Containers.tar.gz 檔案的位置，導覽至 Identity_Manager_4.9.0_Containers 目錄。

4 執行以下指令以載入影像：

```
docker load --input IDM_490_sspr.tar.gz
```

5 使用以下範例指令部署容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.11 --
network=idmoverlaynetwork --hostname=sspr.example.com --name=sspr-
container -v /etc/hosts:/etc/hosts -v /data/sspr:/config -p 8443:8443 -
-stop-timeout 100 sspr/sspr-webapp:4.7.0.1-580
```

6 在 Docker 主機上執行以下指令，以將 Docker 主機中的 `silent.properties` 檔案複製到 SSPR 容器：

```
docker cp /data/silent.properties sspr-container:/tmp
```

7 將靜默內容檔案載入到 SSPR 容器。

```
docker exec -it sspr-container /app/command.sh ImportPropertyConfig /
tmp/silent.properties
```

附註：檢查是否在 SSPR 容器的 `/config` 目錄下建立了 `SSPRConfiguration.xml`，並驗證該檔案的內容。

---

8 將 OAuth 證書輸入至 SSPR 中：

8a 在 Docker 主機上編輯 `/data/sspr` 目錄中的 `SSPRConfiguration.xml` 檔案，將 `configIsEditable` 旗標的值設定為 **true** 並儲存變更。

8b 啟動瀏覽器並輸入 `https://sspr.example.com:8443/sspr` URL。

8c 使用管理員身分證明 (例如 `uaadmin`) 登入。

8d 按一下右上角的使用者 (例如 `uaadmin`)，然後按一下**組態編輯器**。

8e 指定組態密碼，然後按一下**登入**。

8f 按一下**設定** > **單一登入 (SSO) 用戶端** > **OAuth**，確定所有 URL 都使用 HTTPS 通訊協定和正確的連接埠。

8g 在 **OAuth 伺服器證書**下，按一下**從伺服器輸入**以輸入新證書，然後按一下**確定**。

8h 按一下右上角的 以儲存證書。

8i 檢視變更並按一下**確定**。

8j SSPR 應用程式重新啟動之後，編輯 `SSPRConfiguration.xml` 檔案，將 `configIsEditable` 旗標的值設定為 **true** 並儲存變更。

部署 Identity Console 容器

如需部署 Identity Console 容器的詳細資訊，請參閱 Deploying Identity Console as Docker Container (將 Identity Console 部署為 Docker 容器)。

19 升級 Identity Manager 容器

本章提供關於更新 Identity Manager 各個容器的資訊。

後續章節會介紹容器更新程序。

- 「容器更新先決條件」(第 253 頁)
- 「更新分散式伺服器上的容器」(第 253 頁)
- 「更新單部伺服器上的容器」(第 259 頁)

容器更新先決條件

在更新每個 Identity Manager 容器之前，請執行以下步驟。

重要：本節不適用於 PostgreSQL 容器。如需更新 PostgreSQL 容器的資訊，請參閱 *「更新分散式伺服器上的容器」(第 253 頁)* 一節中的更新 PostgreSQL 容器，或 *「更新單部伺服器上的容器」(第 259 頁)* 一節中的更新 PostgreSQL 容器。

---

1 停止所有 Identity Manager 容器。

```
docker stop < 容器名稱 >
```

例如：

```
docker stop engine-container
```

2 備份共用目錄。本指南中的範例假設共用目錄為 `/data`。

3 刪除所有 Identity Manager 容器。

```
docker rm < 容器名稱 >
```

例如：

```
docker rm engine-container
```

4 (視情況而定) 刪除所有已過時的 Docker 影像。

```
docker rmi < 影像 ID>
```

更新分散式伺服器上的容器

必須依照以下順序更新容器：

- 「更新 Identity Manager 引擎容器」(第 254 頁)
- 「更新遠端載入器容器」(第 254 頁)
- 「更新擴送代理程式容器」(第 255 頁)
- 「更新 OSP 容器」(第 255 頁)

- 「更新 PostgreSQL 容器」(第 256 頁)
- 「更新 Identity Applications 容器」(第 257 頁)
- 「更新表單轉譯器容器」(第 257 頁)
- 「更新 ActiveMQ 容器」(第 257 頁)
- 「更新 Identity Reporting 容器」(第 258 頁)
- 「更新 SSPR 容器」(第 258 頁)
- 「更新 Identity Console 容器」(第 258 頁)

更新 Identity Manager 引擎容器

1 在共用目錄 /data 下建立包含以下內容的 credentials.properties 檔案。

```
ID_VAULT_ADMIN_LDAP="<ID_VAULT_ADMIN_LDAP>"
ID_VAULT_PASSWORD="<ID_VAULT_PASSWORD>"
```

其中，ID_VAULT_ADMIN_LDAP 必須採用逗號分隔格式。

例如：

```
ID_VAULT_ADMIN_LDAP="cn=admin,ou=sa,o=system"
```

```
ID_VAULT_PASSWORD="novell"
```

2 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

3 導覽至 docker-images 目錄。

4 執行以下指令以載入影像：

```
docker load --input IDM_490_identityengine.tar.gz
```

5 如果您要使用覆蓋網路部署 Identity Manager 引擎，請使用以下指令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.12 --
network=idmoverlaynetwork --hostname=identityengine.example.com --
name=engine-container -v /etc/hosts:/etc/hosts -v /data:/config -p
8028:8028 -p 524:524 -p 389:389 -p 8030:8030 -p 636:636 -e
SILENT_INSTALL_FILE=/config/credentials.properties --stop-timeout 100
identityengine:idm-4.9.0-580
```

如果您要使用主機網路部署 Identity Manager 引擎，請使用以下指令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=engine-
container -v /etc/hosts:/etc/hosts -v /data:/config -e
SILENT_INSTALL_FILE=/config/credentials.properties --stop-timeout 100
identityengine:idm-4.9.0-580
```

更新遠端載入器容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_remoteloader.tar.gz
```

4 執行以下指令來部署容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.2 --
network=idmoverlaynetwork --hostname=remoteloader.example.com -p
8090:8090 --name=rl-container -v /etc/hosts:/etc/hosts -v /data:/config
--stop-timeout 100 remoteloader:idm-4.9.0-580
```

容器的 /opt/novell/eDirectory/lib/dirxml/classes/ 目錄中提供了驅動程式檔案。

5 (視情況而定) 如果遠端載入器例項未執行，請啟動遠端載入器例項。

更新擴送代理程式容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_fanoutagent.tar.gz
```

4 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.3 --
network=idmoverlaynetwork --hostname=fanoutagent.example.com --
name=foa-container -v /etc/hosts:/etc/hosts -v /data:/config --stop-
timeout 100 fanoutagent:idm-4.9.0-580
```

5 啟動擴送代理程式。

更新 OSP 容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_osp.tar.gz
```

4 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.5 --
network=idmoverlaynetwork --hostname=osp.example.com -p 8543:8543 --
name=osp-container -v /etc/hosts:/etc/hosts -v /data:/config --stop-
timeout 100 osp:idm-4.9.0-580
```

5 執行以下指令以登入該容器：

```
docker exec -it <container> <command>
```

例如：

```
docker exec -it osp-container bash
```

更新 PostgreSQL 容器

附註：在更新 PostgreSQL 容器之前，請務必停止 Identity Applications 和 / 或 Identity Reporting 等相依容器。

1. 在 Docker 主機上，導覽至任意位置。例如：

   ```
   cd /tmp
   ```

2. 執行以下指令備份現有的 PostgreSQL 容器資料。

   ```
   docker exec postgresql-container pg_dumpall -U postgres > dump.sql
   ```

3. 停止 PostgreSQL 容器。

   ```
   docker stop <container name>
   ```

   例如：

   ```
   docker stop postgresql-container
   ```

4. 刪除 PostgreSQL 容器。

   ```
   docker rm < 容器名稱 >
   ```

5. 刪除現有的 PostgreSQL 資料目錄。

   ```
   rm -rf /data/postgres
   ```

6. (視情況而定) 刪除 PostgreSQL Docker 影像。

   ```
   docker rmi < 影像 ID>
   ```

7. 在共用目錄 /data 下建立一個子目錄，例如 postgres。

   ```
   mkdir postgres
   ```

8. 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

9. 導覽至 docker-images 目錄。

10. 執行以下指令以載入影像：

    ```
    docker load --input IDM_490_postgres.tar.gz
    ```

11. 使用以下指令更新容器：

    ```
    docker run --restart unless-stopped -d --ip=192.168.0.6 --
    network=idmoverlaynetwork --hostname=postgresql.example.com --
    name=postgresql-container -p 5432:5432 -e POSTGRES_PASSWORD=<password>
    -v /data/postgres:/var/lib/postgresql/data -v /etc/hosts:/etc/hosts -v
    /data:/config --stop-timeout 100 postgres:12.18
    ```

    例如：

    ```
    docker run --restart unless-stopped -d --ip=192.168.0.6 --
    network=idmoverlaynetwork --hostname=postgresql.example.com --
    name=postgresql-container -p 5432:5432 -e POSTGRES_PASSWORD=novell -v /
    data/postgres:/var/lib/postgresql/data -v /etc/hosts:/etc/hosts -v /
    data:/config --stop-timeout 100 postgres:12.18
    ```

12. 將您在 Docker 主機上備份的資料檔案 (步驟 2) 複製到新的 PostgreSQL data 目錄。

```
cp /tmp/dump.sql /data/postgres
```

13 執行以下指令以登入該容器：

```
docker exec -it <container> <command>
```

例如：

```
docker exec -it postgresql-container bash
```

14 導覽至 /var/lib/postgresql/data/ 目錄。

15 將在步驟 2 中備份的資料還原至新的 PostgreSQL 容器。

```
psql -U postgres < dump.sql >
```

16 執行以下指令以結束容器。

```
exit
```

更新 Identity Applications 容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_identityapplication.tar.gz
```

4 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.7 --
network=idmoverlaynetwork --hostname=identityapps.example.com -p
18543:18543 --name=idapps-container -v /etc/hosts:/etc/hosts -v /data:/
config --stop-timeout 100 identityapplication:idm-4.9.0-580
```

更新表單轉譯器容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_formrenderer.tar.gz
```

4 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.8 --
network=idmoverlaynetwork --hostname=formrenderer.example.com -p
8600:8600 --name=fr-container -v /etc/hosts:/etc/hosts -v /data:/config
--stop-timeout 100 formrenderer:idm-4.9.0-580
```

更新 ActiveMQ 容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_activemq.tar.gz
```

4 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.9 --
network=idmoverlaynetwork --hostname=activemq.example.com -p
61616:61616 --name=amq-container -v /etc/hosts:/etc/hosts -v /data:/
config --stop-timeout 100 activemq:idm-4.9.0-580
```

更新 Identity Reporting 容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_identityreporting.tar.gz
```

4 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.10 --
network=idmoverlaynetwork --hostname=identityreporting.example.com -p
28543:28543 --name=rpt-container -v /etc/hosts:/etc/hosts -v /data:/
config --stop-timeout 100 identityreporting:idm-4.9.0-580
```

更新 SSPR 容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_sspr.tar.gz
```

4 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.11 --
network=idmoverlaynetwork --hostname=sspr.example.com --name=sspr-
container -v /etc/hosts:/etc/hosts -v /data/sspr:/config -p 8443:8443 -
-stop-timeout 100 sspr/sspr-webapp:4.7.0.1-580
```

更新 Identity Console 容器

如需更新 Identity Console 容器的詳細資訊，請參閱 Upgrading Identity Console As Docker Container (將 Identity Console 升級為 Docker 容器)。

更新單部伺服器上的容器

必須依照以下順序更新容器：

- 「更新 Identity Manager 引擎容器」(第 259 頁)
- 「更新遠端載入器容器」(第 259 頁)
- 「更新擴送代理程式容器」(第 260 頁)
- 「更新 OSP 容器」(第 260 頁)
- 「更新 PostgreSQL 容器」(第 261 頁)
- 「更新 Identity Applications 容器」(第 262 頁)
- 「更新表單轉譯器容器」(第 262 頁)
- 「更新 ActiveMQ 容器」(第 262 頁)
- 「更新 Identity Reporting 容器」(第 263 頁)
- 「更新 SSPR 容器」(第 263 頁)
- 「更新 Identity Console 容器」(第 263 頁)

更新 Identity Manager 引擎容器

1 在共用目錄 /data 下建立包含以下內容的 credentials.properties 檔案。

```
ID_VAULT_ADMIN_LDAP="<ID_VAULT_ADMIN_LDAP>"
ID_VAULT_PASSWORD="<ID_VAULT_PASSWORD>"
```

其中，ID_VAULT_ADMIN_LDAP 必須採用逗號分隔格式。

例如：

```
ID_VAULT_ADMIN_LDAP="cn=admin,ou=sa,o=system"

ID_VAULT_PASSWORD="novell"
```

2 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

3 導覽至 docker-images 目錄。

4 執行以下指令以載入影像：

```
docker load --input IDM_490_identityengine.tar.gz
```

5 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=engine-
container -v /etc/hosts:/etc/hosts -v /data:/config -e
SILENT_INSTALL_FILE=/config/credentials.properties --stop-timeout 100
identityengine:idm-4.9.0-580
```

更新遠端載入器容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_remoteloader.tar.gz
```

4 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=<container
name> -v /data:/config --stop-timeout 100 remoteloader:idm-4.9.0-580
```

例如：

```
docker run --restart unless-stopped -d --network=host --name=rl-
container -v /data:/config --stop-timeout 100 remoteloader:idm-4.9.0-
580
```

容器的 /opt/novell/eDirectory/lib/dirxml/classes/ 目錄中提供了驅動程式檔案。

5 (視情況而定) 如果遠端載入器例項未執行，請啟動遠端載入器例項。

更新擴送代理程式容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_fanoutagent.tar.gz
```

4 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=foa-
container -v /data:/config --stop-timeout 100 fanoutagent:idm-4.9.0-580
```

5 啟動擴送代理程式。

更新 OSP 容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_osp.tar.gz
```

4 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=osp-
container -v /data:/config --stop-timeout 100 osp:idm-4.9.0-580
```

5 執行以下指令以登入該容器：

```
docker exec -it <container> <command>
```

例如：

```
docker exec -it osp-container bash
```

更新 PostgreSQL 容器

附註：在更新 PostgreSQL 容器之前，請務必停止 Identity Applications 和 / 或 Identity Reporting 等相依容器。

1. 在 Docker 主機上，導覽至任意位置。例如：

   ```
   cd /tmp
   ```

2. 執行以下指令備份現有的 PostgreSQL 容器資料。

   ```
   docker exec postgresql-container pg_dumpall -U postgres > dump.sql
   ```

3. 停止 PostgreSQL 容器。

   ```
   docker stop < 容器名稱 >
   ```

   例如：

   ```
   docker stop postgresql-container
   ```

4. 刪除 PostgreSQL 容器。

   ```
   docker rm < 容器名稱 >
   ```

5. 刪除現有的 PostgreSQL 資料目錄。

   ```
   rm -rf /data/postgres
   ```

6. (視情況而定) 刪除 PostgreSQL Docker 影像。

   ```
   docker rmi < 影像 ID>
   ```

7. 在共用目錄 /data 下建立一個子目錄，例如 postgres。

   ```
   mkdir postgres
   ```

8. 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

9. 導覽至 docker-images 目錄。

10. 執行以下指令以載入影像：

    ```
    docker load --input IDM_490_postgres.tar.gz
    ```

11. 使用以下指令更新容器：

    ```
    docker run --restart unless-stopped -d --network=host --
    name=postgresql-container -e POSTGRES_PASSWORD=<password> -v /data/
    postgres:/var/lib/postgresql/data --stop-timeout 100 postgres:12.18
    ```

    例如：

    ```
    docker run --restart unless-stopped -d --network=host --
    name=postgresql-container -e POSTGRES_PASSWORD=novell -v /data/
    postgres:/var/lib/postgresql/data --stop-timeout 100 postgres:12.18
    ```

12. 將您在 Docker 主機上備份的資料檔案 (步驟 2) 複製到新的 PostgreSQL data 目錄。

    ```
    cp /tmp/dump.sql /data/postgres
    ```

13. 執行以下指令以登入該容器：

    ```
    docker exec -it <container> <command>
    ```

例如：

```
docker exec -it postgresql-container bash
```

14 導覽至 /var/lib/postgresql/data/ 目錄。

15 將在步驟 2 中備份的資料還原至新的 PostgreSQL 容器。

```
psql -U postgres < dump.sql
```

16 執行以下指令以結束容器。

```
exit
```

更新 Identity Applications 容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_identityapplication.tar.gz
```

4 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=idapps-
container -v /data:/config --stop-timeout 100 identityapplication:idm-
4.9.0-580
```

更新表單轉譯器容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_formrenderer.tar.gz
```

4 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=fr-
container -v /data:/config --stop-timeout 100 formrenderer:idm-4.9.0-
580
```

更新 ActiveMQ 容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_activemq.tar.gz
```

4 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=amq-
container -v /data:/config --stop-timeout 100 activemq:idm-4.9.0-580
```

更新 Identity Reporting 容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_identityreporting.tar.gz
```

4 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=rpt-
container -v /data:/config --stop-timeout 100 identityreporting:idm-
4.9.0-580
```

更新 SSPR 容器

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的位置。

2 導覽至 docker-images 目錄。

3 執行以下指令以載入影像：

```
docker load --input IDM_490_sspr.tar.gz
```

4 使用以下指令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=sspr-
container -v /data/sspr:/config --stop-timeout 100 sspr/sspr-
webapp:4.7.0.1-580
```

更新 Identity Console 容器

如需更新 Identity Console 容器的詳細資訊，請參閱 Upgrading Identity Console As Docker Container (將 Identity Console 升級為 Docker 容器)。

VIII 使用 Ansible 部署 Identity Manager 容器

此 Identity Manager 版本支援使用 Ansible 部署 Identity Manager 容器。使用 Ansible 部署方法可以透過自動化程序輕鬆部署容器。部署程序更簡單且更省時。Identity Manager 隨附了用於自動完成容器部署的 Ansible 教戰手冊。

本章提供關於透過 Ansible 部署容器的指示。

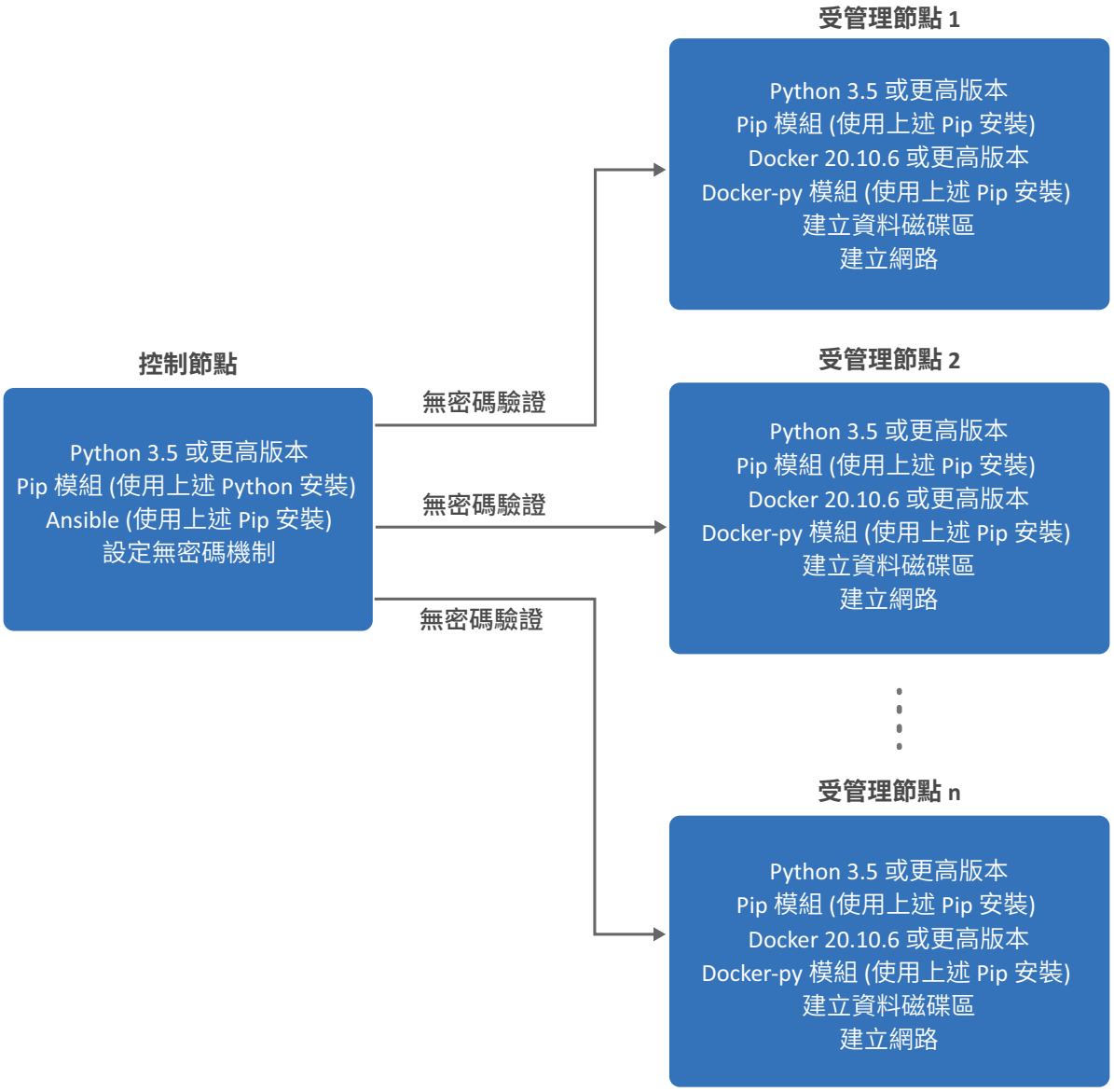
20 規劃部署

在部署容器之前，需要做出一些規劃並滿足先決條件。本節提供關於規劃部署的詳細資料。

為基於 Ansible 的容器部署確定兩部或更多伺服器。其中一部伺服器稱為 Ansible 控制節點，其餘伺服器稱為受管理節點。如需控制節點和受管理節點的更多詳細資料，請參閱 Ansible (https://docs.ansible.com/ansible/latest/network/getting_started/basic_concepts.html#basic-concepts) 文件。

準備 Ansible 節點

在開始部署之前，必須確定已正確設定 Ansible 節點。控制節點和受管理節點的先決條件各不相同。下圖概要性地說明了如何準備控制節點和受管理節點。



準備控制節點

確定在控制節點上執行以下任務：

- 確定已安裝 Python3 或更新版本。若要檢查 Python 版本，請導覽至 `/usr/bin/` 目錄並執行以下指令：

  例如：

  ```
  python3 --version
  ```

  如需詳細資訊，請參閱 Python 文件。
- 確定已安裝 pip。若要檢查 pip 版本，請執行以下指令：

  例如：

  ```
  pip --version
  ```

確定已透過先前安裝的 Python3 或更新版本安裝了 `pip`。

如需詳細資訊，請參閱 Python 文件。

- 執行以下指令，以使用 pip 安裝 Docker 模組：

  例如：

  ```
  pip install docker
  ```

  確定 Docker 為 20.10.6 或更新版本。如需詳細資訊，請參閱 Docker 文件。

- 使用先前安裝的 pip 安裝 Ansible。務必安裝 Ansible 2.10.5 或更新版本。

  例如：

  ```
  pip install ansible
  ```

  如需詳細資訊，請參閱 Ansible (https://docs.ansible.com/ansible/latest/installation_guide/intro_installation.html#installing-ansible-with-pip) 文件。

- 確定可從控制節點連接受管理節點。例如，可以使用 `ping` 或任何相關機制來確定可連接這些節點。
- 確定在部署中的控制節點與所有受管理節點之間建立無密碼驗證。請執行以下步驟：
  1. 產生 SSH 金鑰。

     例如：

     ```
     ssh-keygen
     ```

  2. 不要輸入任何密碼，而是繼續產生金鑰。
  3. 執行以下指令啟用對受管理節點的無密碼驗證：

     ```
     ssh-copy-id root@< 受管理節點的 FQDN 或 IP 位址 >
     ```

     例如：

     ```
     ssh-copy-id root@192.168.0.25
     ```

  4. 指定受管理節點的密碼。

     例如，`password`。

  5. 測試與受管理節點的連接：

     ```
     ssh 'root@< 受管理節點的 FQDN 或 IP 位址 >'
     ```

     例如：

     ```
     ssh 'root@<192.168.0.25>'
     ```

準備受管理節點

確定在所有受管理節點上執行以下任務：

- 確定已安裝 Python3 或更新版本。若要檢查 Python 版本，請導覽至 `/usr/bin/` 目錄並執行以下指令：

  例如：

  ```
  python3 --version
  ```

  如需詳細資訊，請參閱 Python 文件。

- 確定已安裝 pip。若要檢查 pip 版本，請執行以下指令：

  例如：

  ```
  pip --version
  ```

  確定已透過先前安裝的 Python3 或更新版本安裝了 pip。

  如需詳細資訊，請參閱 Python 文件。
- 安裝 Docker。確定 Docker 為 20.10.6 或更新版本。如需詳細資訊，請參閱 Docker 文件。
- 使用 pip 安裝 Docker python 模組：

  例如：

  ```
  pip install docker-py
  ```
- 建立共用目錄。如需詳細資訊，請參閱 「管理容器磁碟區資料」(第 224 頁)。

建立 setup.csv 檔案

setup.csv 檔案是部署容器時 Ansible 會使用的輸入檔案。Identity Manager 將 setup.csv 檔案的預設樣板綑綁在 Identity Manager 容器 tar 檔案中。

setup.csv 檔案的預設樣板位於 /< 容器 tar 檔案解壓縮到的位置 >/ansible/input/ 目錄。您可以根據要求編輯 setup.csv 檔案。

以下章節介紹了 setup.csv 檔案包含的參數，以及每個參數的用途：

- **元件：** 表示您要部署的容器。例如 engine。
- **部署：**表示您是否要部署容器。支援的值為 **yes** 和 **no**。
- **DockerHost：**表示要將容器部署到的 Docker 主機。換言之，它可以是您為部署識別的任何受管理節點。例如 DockerHostA
- **IP 位址：**表示要將容器部署到的 Docker 主機的 IP 位址。例如 192.168.0.15
- **ContainerName：**表示容器的名稱。例如 engine-container。
- **ContainerHostname：**表示要將容器部署到的 Docker 主機或伺服器的主機名稱。NetIQ 建議您用 FQDN 格式指定主機名稱。例如 identityengine.example.com。
- **ExposedPorts：**表示您要為容器公開的監聽連接埠。例如 636。

  附註：確定為每個容器公開唯一連接埠，並指定您在建立 silent.properties 檔案時提供的相同連接埠。例如，您可以參考表格 18-2 (第 239 頁) 中提供的範例連接埠來規劃要公開的連接埠。

- **FileMounting：**表示任何自訂檔案 (例如 ojdbc.jar) 的路徑。例如 /opt/novell/eDirectory/lib/dirxml/classes/ojdbc.jar。

  附註：
  - 如果有多個值，請用空格分隔的變數清單形式指定這些值。例如 /opt/novell/eDirectory/lib/dirxml/classes/ojdbc.jar /opt/novell/eDirectory/lib/dirxml/classes/mssql.jar

- (視情況而定) 僅當您已在 Deploy 欄中將 Core DNS 容器的值設定為 **no** 時，此參數才適用。

  確定已在 FileMounting 欄位中對應 hosts 檔案。例如 /etc/hosts。

- **SharedVolume**：表示您希望容器用來儲存資料的共用目錄。例如，/data。需要跨 Docker 主機建立此目錄。

21 部署容器

執行以下步驟來部署容器：

1 在控制節點上執行以下步驟：

1a 下載並解壓縮 Identity Manager 容器 tar 檔案。如需詳細資訊，請參閱「獲取 Docker 影像」(第 221 頁)。

1b 導覽至 /<tar 檔案解壓縮到的位置 >/docker-images/ 目錄。

1c 複製 IDM_490_idm_conf_generator.tar.gz 檔案並將其放在任一受管理節點上。

2 在任一受管理節點上執行以下步驟：

2a 將在步驟 1c 中複製的 IDM_490_idm_conf_generator.tar.gz 檔案放在任意位置。例如 /home。

2b 建立 silent.properties 檔案。如需詳細資訊，請參閱「建立靜默內容檔案」(第 224 頁)。

3 在控制節點上執行以下步驟：

3a 導覽至 /<tar 檔案解壓縮到的位置 >/ansible/input/ 目錄並在其中放置以下檔案：

- 在步驟 2b 中建立的 silent.properties 檔案
- 在「建立 setup.csv 檔案」(第 270 頁)一節中建立的 setup.csv 檔案
- 從外部證書管理中心取得的任何自訂證書

附註：如果您使用 Identity Vault 做為產生證書的證書管理中心，請執行「透過 Identity Vault 證書管理中心產生證書」(第 242 頁)中所述的步驟。

- 任何自訂檔案，例如 ojdbc.jar 或自訂 LDIF 檔案

附註：確定在 setup.csv 檔案的 **FileMounting** 欄中指定這些檔案的目標路徑。如需詳細資訊，請參閱「建立 setup.csv 檔案」(第 270 頁)。

3b 導覽至 /<tar 檔案解壓縮到的位置 >/ansible/ 目錄。

3c (選擇性) 此步驟適用於進階使用者。檢閱用於部署的 ansible.cfg 檔案。

3d 執行以下指令來部署 setup.yml 教戰手冊：

```
ansible-playbook setup.yml
```

3e (選擇性) 此步驟適用於進階使用者。檢視用於部署的 idminventory.ini 檔案。

3f 執行以下指令來部署 deploy.yml 教戰手冊：

```
ansible-playbook deploy.yml -e 'network_set=<Docker 網路名稱 >'
```

例如：

```
ansible-playbook deploy.yml -e 'network_set=idmoverlaynetwork'
```

22 部署後任務

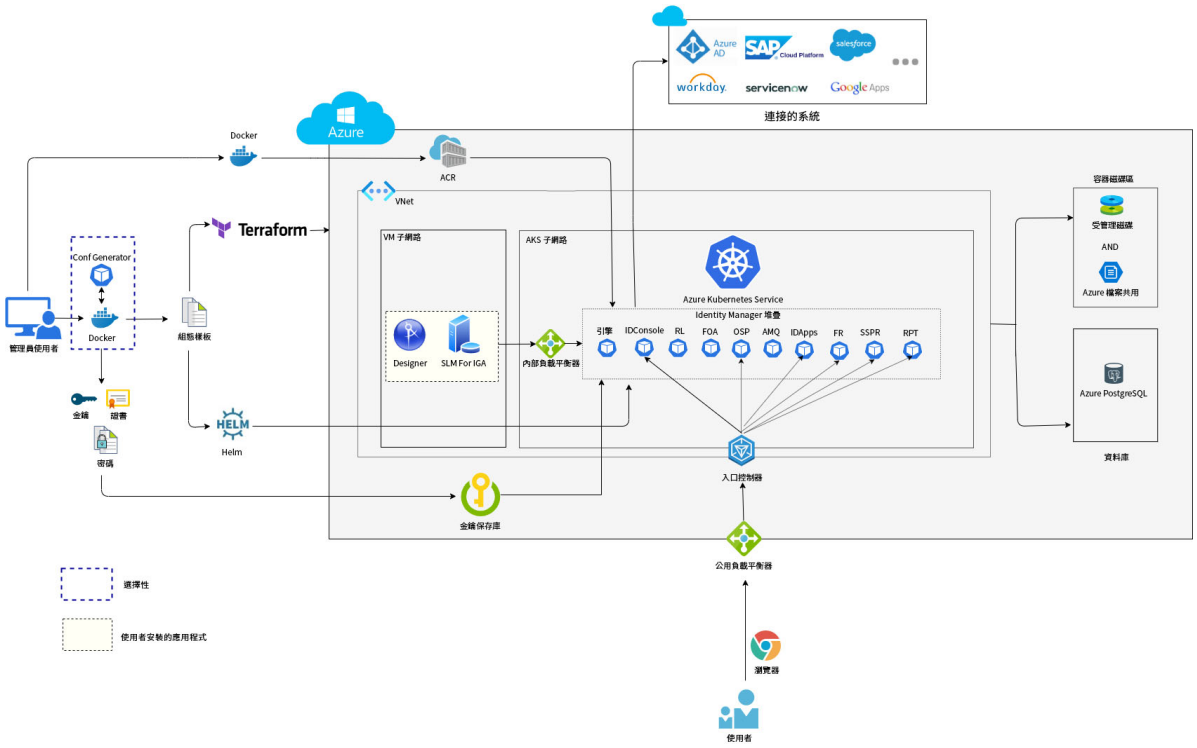
完成 Identity Manager 容器的部署後，必須執行某些任務才能確定 Identity Manager 解決方案在您的環境中正常運作。

必須將 OAuth 證書輸入 SSPR。如需詳細資訊，請參閱 「部署 SSPR 容器」(第 250 頁) 一節的步驟 8。

IX 在 Microsoft Azure Kubernetes Service 上部署 Identity Manager 容器

此版本允許您在 Microsoft Azure Kubernetes Service 上部署 Identity Manager 容器。可以借助 Terraform 和 Helm 圖表來自動完成 Identity Manager 容器部署。

下圖提供了在 Azure 上部署容器的架構檢視。



- `ACRcreate.sh` 檔案建立新的 Azure 容器登錄，並允許使用者在 Azure 入口網站中上傳 / 儲存 Docker 影像。
- Identity Manager Configuration Generator 影像用於完成下列任務：
  - 產生組態檔案 (Terraform 檔案和 Helm 圖表)。
  - 建立 Azure 資源群組。
  - 在 Azure 資源群組下建立金鑰保存庫。
  - 將所有敏感性資訊推入金鑰保存庫。
- 使用者可以使用 Terraform 程序檔設定基礎架構，例如：
  - 網路建立。

    - Azure PostgreSQL (選擇性)。
    - Azure Kubernetes Service (AKS)。
- 使用者可以使用 Helm 圖表在 Azure Kubernetes 叢集內部署 Identity Manager 容器。
- NGINX 入口控制器用做反向代理，用於存取 AKS 叢集內執行的 Identity Manager Web 應用程式 (包括 Identity Applications、Identity Reporting 和 Identity Console 等)。
    - 需要購買單一網域 (例如 `identitymanager.eastus.cloudapp.azure.com`)。
    - 該網域將指定給 Nginx 入口控制器。
- 內部負載平衡器用於引擎 Docker 主機與 Kubernetes 叢集之間的內部通訊。
- 永續性儲存是動態建立的，將在整個基礎架構中掛接。
- 可將 Identity Applications 和 Identity Reporting 設定為使用 Azure 提供的 Azure PostgreSQL 資料庫。
- 用於 Identity Governance 管理的 Designer 和 Sentinel Log Management (SLM) 應在 Terraform 執行完成後由使用者手動部署。

綜覽

若要規劃 Azure Kubernetes 叢集上的 Identity Manager 容器部署，請參閱以下章節：

- 第 23 章 「規劃部署」 (第 279 頁)
- 第 24 章 「準備部署」 (第 283 頁)
- 第 25 章 「部署程序」 (第 285 頁)
- 第 26 章 「部署後任務」 (第 305 頁)
- 第 27 章 「維護 Identity Manager 容器的部署」 (第 307 頁)

23 規劃部署

本章將指導您完成部署規劃程序，並提供在 Azure 上部署容器所要滿足的先決條件清單。

Identity Manager 容器部署程序需要以下 Azure 資源：

1 確定您的 Azure 帳戶擁有建立基礎架構所需的讀寫許可權。

   1a Azure Kubernetes Service (AKS)。

   1b 網路建立。

   1c (選擇性) Azure PostgreSQL。

   附註：這些元素由 Terraform 部署程序檔建立。

附註：在部署之前，請確定資源各有差異，並且尚未為您的 Azure 帳戶建立 Identity Manager 組態檔案。

2 請購買網域以存取 Identity Manager 中的不同應用程式。

   您可以在相應資源群組中使用自己的網域。例如 `identitymanager.eastus.cloudapp.azure.com`。

附註：在上面的範例中，**eastus** 表示位置，**cloudapp.azure.com** 表示一般的 Azure 尾碼網域。

3 從任一證書管理中心 (CA) 取得網域的 SSL 證書 (`.crt` 和 `.key` 檔案)。

4 (選擇性) 在指令行介面中執行以下指令，產生您自己的自行簽署證書：

```
openssl req -new -newkey rsa:2048 -nodes -keyout domain.key -out
domain.csr
```

   4a 為以下提示指定輸入：

表格 23-1

提示	描述
國家 / 地區名稱 (雙字母代碼)	使用雙字母代碼指定國家 / 地區名稱。
州或省名稱	指定州或省的全名。
地區名稱	指定市名。
組織名稱	指定組織名稱。例如 Internet Widgits Pty Ltd。
組織單位名稱	指定組織單位名稱。例如 section。
公用名稱	指定伺服器完全合格的網域名稱 (FQDN)。例如 `identitymanager.eastus.cloudapp.azure.com`。
電子郵件地址	指定您的電子郵件地址。
挑戰密碼	指定唯一密碼。
選擇性的公司名稱	指定選擇性的公司名稱。

4b 執行以下指令將私密金鑰轉換為 RSA 格式：

```
openssl rsa -in domain.key -out tls.key
```

4c 執行以下步驟取得根證書。

4c1 登入 `https://<IP 位址或主機名稱>:9000/identityconsole/#/`。

4c2 導覽至**證書管理** > **伺服器證書管理**。

4c3 按一下「**輸出**」。

4c4 在「證書」下拉式清單中選取**組織 CA**。

4c5 在「輸出格式」下拉式清單中選取 **BASE64**。

4c6 按一下**確定**。

4c7 按一下**儲存輸出的證書**。

4d 執行以下步驟，將您的 CSR 提交至證書管理中心 (CA) 並取得簽署的伺服器證書。

4d1 登入 `https://<IP 位址或主機名稱>:9000/identityconsole/#/`。

4d2 導覽至**證書管理** > **核發證書**。

4d3 按一下**選擇檔案**，上傳在步驟 4b (第 280 頁)中產生的 < 網域 >.csr 檔案。

4d4 在**證書參數**下拉式清單中選取有效期。例如「最大」。

4d5 在**證書格式**下拉式清單中選取 **Base64 格式的檔案**。

4d6 按「**下一步**」。

4d7 檢閱提供的輸入，然後按一下**確定**。

4d8 按一下**下載核發的證書**。

4e 執行以下指令以串連伺服器證書和根證書。

```
cat domain.b64 <(echo) cert.b64 <(echo) > tls.crt
```

5 若要產生服務主體身分證明，請執行以下步驟。

重要：必須擁有服務主體身分證明才能產生組態並將所有敏感性資訊推入 Azure 金鑰保存庫。

5a 登入 Azure 入口網站。

5b 按一下  。

5c 在終端機視窗中執行以下指令：

```
az ad sp create-for-rbac --skip-assignment
```

附註：請記下指令輸出中的 appid、密碼和租用戶 ID。

24 準備部署

本章提供關於在部署 Identity Manager 容器之前所要完成的任務的指示。

1 從軟體和授權頁面 (https://sld.microfocus.com/) 下載 `Identity_Manager_4.9.0_Containers.tar.gz`。

2 執行以下指令以解壓縮 `Identity_Manager_4.9.0_Containers.tar.gz` 檔案：

```
tar -zxvf Identity_Manager_4.9.0_Containers.tar.gz
```

3 導覽至 `Identity_Manager_4.9.0_Containers` 目錄並執行以下指令：

```
./ACRCreate.sh
```

附註：目前的目錄中至少需有 6 GB 空間才能執行程序檔。

3a 執行以下步驟登入 Microsoft Azure CLI。

3a1 登入 https://microsoft.com/devicelogin。

3a2 輸入顯示的代碼。

3a3 按「下一步」。

3a4 按一下**繼續**。

3b 為以下提示指定輸入：

提示	描述
依原樣輸入上面顯示的相應 Azure 帳戶 ID (不包括雙引號)。	指定在上述步驟中產生的 Azure 帳戶 ID。
是否要建立 Azure 容器登錄？	指定您是否要建立 Azure 容器登錄。 ◆ (視情況而定) 如果您選取「是」： 1. 指定您是否要建立新的資源群組。 ◆ (視情況而定) 如果您選取「是」，請指定 Azure 資源群組名稱。 ◆ (視情況而定) 如果您選取「否」，請指定現有的 Azure 資源群組名稱。 **附註：**資源群組名稱中只能包含英數字元。 2. 輸入 Azure 資源群組位置。例如 `eastus`。 ◆ (視情況而定) 如果您選取「否」，請輸入現有的 Azure 容器登錄 URL。例如 `azureregname.azurecr.io`。

3c (視情況而定) 若要取得 Azure 容器登錄詳細資料，請執行以下步驟：

3c1 登入 Azure 入口網站。

3c2 移至您的資源群組。

3c3 在「資源」下，按一下**容器登錄**。

3c4 移至**設定** > **存取金鑰**並啟用**管理員使用者**切換開關。

3c5 記下登錄詳細資料以備後用。

25 部署程序

本章介紹在 Azure 上部署 Identity Manager 容器所涉及的部署程序。部署程序分為兩個階段：

- 「Azure 雲端的基礎架構部署」(第 285 頁)
- 「Azure Kubernetes Service 上的 Identity Manager 容器部署」(第 299 頁)
- 「在 Azure Kubernetes Service 上設定遠端載入器服務」(第 300 頁)
- 「在 Azure Kubernetes Service 上設定擴送代理程式服務」(第 302 頁)

Azure 雲端的基礎架構部署

Azure 雲端的基礎架構部署是使用 terraform 組態定義的。可採用兩種不同的方法在 Azure 上部署基礎架構。您可以根據自己的要求，選擇使用 Configuration Generator 或組態樣板來部署基礎架構。

- 「使用 Configuration Generator 進行部署」(第 285 頁)
- 「使用組態樣板進行部署」(第 289 頁)

使用 Configuration Generator 進行部署

執行以下步驟，以使用 Identity Manager Configuration Generator 產生組態檔案。

重要：必須有一部已安裝並執行 Docker 的機器才能執行以下步驟。

1. 建立共用磁碟區。如需詳細資訊，請參閱 「管理容器磁碟區資料」(第 224 頁)。
2. 將您網域的證書複製到共用磁碟區。
3. 執行以下指令載入 Docker 影像：

   ```
   docker load --input docker-images/IDM_490_idm_conf_generator.tar.gz
   ```

4. 導覽至解壓縮位置，並執行以下指令來部署 Configuration Generator 容器：

   ```
   docker run --rm -it --name=idm_conf_generator -v /data:/config
   idm_conf_generator:idm-4.9.0-580
   ```

5. 下表提供了關於新提示的資訊：

   附註：如需所有現有提示的資訊，請參閱 「瞭解組態參數」(第 75 頁) 一節。

提示	描述
是否要在 Azure 上部署 Identity Manager 容器？對於次要伺服器部署，請選取「n」並繼續產生靜默內容檔案 (y/n)？	指定您是否要部署 Identity Manager 容器。 ◆ (視情況而定) 如果您選取「是」，請繼續回答下一則提示。 ◆ (視情況而定) 如果您選取「否」，請輸入包含絕對路徑的靜默內容檔案名稱。例如 `/config/silent.properties`。 **附註：**對於次要伺服器部署，請輸入 **n** 並繼續建立靜默內容檔案。
指定 Kubernetes 部署的名稱空間。	輸入 Kubernetes 部署的名稱空間。例如 idm。
是否要建立新的 Azure PostgreSQL 伺服器例項？	指定您是否要建立新的 Azure PostgreSQL 伺服器例項。 ◆ (視情況而定) 如果您選取「是」，請指定 Azure PostgreSQL 伺服器名稱的首碼。例如 idmpgserver。 **附註：**輸入的首碼中將附加一個連字號和一個隨機產生的 14 位數。 ◆ (視情況而定) 如果您選取「否」，請繼續回答下一則提示。
輸入用於存取 Identity Manager Web 應用程式的完全合格網域名稱 (FQDN)。	指定 FQDN 以存取 Identity Manager Web 應用程式。例如 `identitymanager.eastus.cloudapp.azure.com`。 **附註：**Identity Manager Web 應用程式包括 Identity Applications、Identity Reporting、SSPR、OSP 以及 Identity Console。
輸入 TLS 證書檔案。	指定 PEM 格式的 TLS 證書檔案，其中包含上面指定之網域的主體別名和通用名稱。例如 `/config/tls.crt`。
輸入 TLS 證書的私密金鑰檔案。	指定 TLS 證書的私密金鑰檔案。例如 `/config/tls.key`。
輸入要在 Azure 上為 Identity Manager 引擎部署的例項 (Pod 複製本) 數目。	指定要在 Azure 上為 Identity Manager 引擎部署的例項 (Pod 複製本) 數目。例如，5。
輸入要在 Azure 上為 OSP 部署的例項 (Pod 複製本) 數目。	指定要在 Azure 上為 OSP 部署的例項 (Pod 複製本) 數目。例如，5。
輸入要在 Azure 上為 Identity Applications 部署的例項 (Pod 複製本) 數目。	指定要在 Azure 上為 Identity Applications 部署的例項 (Pod 複製本) 數目。例如，5。
輸入 Azure 服務主體 ID。	指定在「規劃部署」一章的「步驟 5」中產生的 Azure 服務主體 ID。

提示	描述
輸入 Azure 服務密碼。	指定在「規劃部署」一章的「步驟 5」中產生的 Azure 服務密碼。
輸入您的服務主體的租用戶 ID。	指定在「規劃部署」一章的「步驟 5」中產生的租用戶 ID。
輸入現有的 Azure 容器登錄伺服器名稱。	指定 Azure 容器登錄伺服器名稱。請參閱步驟 3c。
輸入 Azure 容器登錄使用者名稱。	指定 Azure 容器登錄使用者名稱。請參閱步驟 3c。
輸入 Azure 容器登錄使用者密碼。	指定 Azure 容器登錄密碼。請參閱步驟 3c。
依原樣輸入上面顯示的相應 Azure 帳戶 ID (不包括雙引號)。	指定在上述步驟中產生的 Azure 帳戶 ID。
輸入 Azure 資源群組名稱。	指定 Azure 資源群組名稱。例如 `idvault-rg`。
輸入 Azure 資源群組位置。	指定資源群組位置。例如 `eastus`。

回答所有提示後，Identity Manager Configuration Generator 將執行以下動作：

- 如果 Azure 中沒有可用的資源群組，則會建立一個資源群組。
- 將在資源群組下建立一個金鑰保存庫和儲存帳戶。
- 所有敏感性資訊將推入金鑰保存庫。

  附註：若要存取 Azure 金鑰保存庫中的敏感性資訊，請參閱 《Quickstart: Azure Key Vault》 (快速入門：Azure 金鑰保存庫)。

- 將在共用磁碟區下建立 `IDM_4.9.0_Cloud_Deployment_files.zip` 檔案，其中包括 Terraform 檔案和 Helm 圖表。

6 登入 Azure 入口網站。

附註：將使用初始登入帳戶自動對 Azure Cloud Shell 進行驗證。如果您需要使用其他帳戶，請執行 `az login` 指令並登入 Azure-CLI。

7 執行以下步驟，將 `IDM_4.9.0_Cloud_Deployment_files.zip` 檔案上傳至 Azure Cloud Shell。

7a 按一下  。

7b 在終端機視窗中按一下  。

7c 選取要上傳至 Azure 的 zip 檔案。

8 執行以下指令以解壓縮 zip 檔案的內容：

```
unzip IDM_4.9.0_Cloud_Deployment_files.zip
```

9 導覽至 `IDM_4.9.0_Cloud_Deployment_files` 目錄。

10 在 `values.yaml` 檔案中進行以下變更：

區段	欄位	描述
Identity Manager Web 應用程式的 TLS 組態	kubernetesSecret	將值指定為 `false`。
	azurekeyVault	將值指定為 `true`。 入口 TLS 證書將做為 kubernetes 機密進行管理。
敏感性資料的機密管理員	kubernetesSecret	將值指定為 `false`。
	azurekeyVault	將值指定為 `true`。 Azure 金鑰保存庫用做機密管理員。
AWS Secret Manager 用做機密管理員	awsSecretManager	將值指定為 `false`。

11 (選擇性) 檢閱 `terraform.tfvars` 和 `values.yaml`。

12 (選擇性) 執行以下指令建立儲存帳戶金鑰：

```
ACCOUNT_KEY=$(az storage account keys list --resource-group
$AZURE_RESOURCE_GROUP_NAME --account-name
$AZURE_STORAGE_ACCOUNT_FOR_TFSTATE --query '[0].value' -o tsv)
```

例如：

```
ACCOUNT_KEY=$(az storage account keys list --resource-group idvault-rg
--account-name stract10226600913781 --query '[0].value' -o tsv)
```

13 (選擇性) 執行以下指令：

```
export ARM_ACCESS_KEY=$ACCOUNT_KEY
```

14 執行以下指令，以下載基礎架構部署所需的所有必要外掛程式。

```
terraform init
```

15 執行以下指令以根據輸入規劃和瞭解部署。

```
terraform plan
```

16 執行以下指令以建立輸入中定義的基礎架構。

```
terraform apply --auto-approve
```

17 (選擇性) 執行以下指令以識別 Azure 帳戶特定的資訊，例如儲存帳戶名稱、金鑰保存庫名稱和資料庫管理員詳細資料。

```
terraform output
```

成功執行 Terraform 指令後，執行 「Azure Kubernetes Service 上的 Identity Manager 容器部署」(第 299 頁) 中所述的步驟以完成 Azure 上的 Identity Manager 容器部署。

使用組態樣板進行部署

執行以下步驟以更新虛擬機器中的組態樣板。

1 導覽至 Identity_Manager_4.9.0_Containers.tar.gz 檔案解壓縮到的目錄。

2 導覽至 Identity_Manager_4.9.0_Containers/terraform/ 目錄，並執行以下指令來解壓縮 zip 檔案的內容。

```
unzip IDM_4.9.0_Azure_Terraform_Configuration.zip
```

3 移至 IDM_Azure_Terraform_Configuration 資料夾，並更新 terraform.tfvars 檔案中的以下欄位。

表格 25-1

欄位	描述
resource_group_name	指定 Azure 資源群組名稱。例如 idvault-rg。
resource_group_location	指定資源群組位置。例如 eastus。
resource_group_exists	指定您是否想要知道現有資源群組存在與否。例如 true。
keyvault_name	指定唯一的金鑰保存庫名稱。
keyvault_exists	指定您是否想要知道現有金鑰保存庫存在與否。例如 true。
image_registry_server	指定 Azure 容器登錄伺服器名稱。
image_registry_server_username	指定 Azure 容器登錄使用者名稱。
image_registry_server_password	指定 Azure 容器登錄密碼。
aks_kubernetes_namespace	輸入 Kubernetes 部署的名稱空間。例如 idm。
azure_postgres_server_name	指定 Azure PostgreSQL 伺服器名稱。例如 idmpgserver。

附註：產生 terraform.tfvars 檔案時會預先填入所有剩餘欄位。

4 執行以下指令並登入 Azure-CLI。

```
az login
```

5 執行以下步驟，以將 terraform 狀態檔案儲存在 Azure 儲存帳戶中：

5a 執行以下指令以在 Azure 中建立儲存帳戶。

```
az storage account create --name
"${AZURE_STORAGE_ACCOUNT_FOR_TFSTATE}" --resource-group
"${AZURE_RESOURCE_GROUP_NAME}" --location
"${AZURE_RESOURCE_GROUP_LOCATION}" --sku Standard_LRS --encryption-
services blob
```

例如：

```
az storage account create --name stract10226600913781 --resource-group idvault-rg --location eastus --sku Standard_LRS --encryption-services blob
```

5b 執行以下指令建立 Azure 儲存容器：

```
az storage container create -n terraform-state --account-name "${AZURE_STORAGE_ACCOUNT_FOR_TFSTATE}"
```

例如：

```
az storage container create -n terraform-state --account-name stract10226600913781
```

5c 導覽至 `Identity_Manager_4.8.7_Containers/terraform/IDM_Azure_Terraform_Configuration/` 目錄，移至 `main.tf` 檔案，並更新 `backend "azurerm"` 欄位下的以下詳細資料。

欄位	描述
resource_group_name	指定 Azure 資源群組名稱。例如 idvault-rg。
storage_account_name	指定 Azure 儲存帳戶名稱。例如 stract89671501132193。
container_name	表示 Azure 容器名稱。此欄位是自動產生的。
key	表示 Azure 金鑰名稱。此欄位是自動產生的。

6 檢閱 `terraform.tfvars` 和 `main.tf` 檔案中已修改的詳細資料，然後將已更新的 `IDM_4.9.0_Azure_Terraform_Configuration.zip` 檔案上傳至 Azure Cloud Shell。

7 執行以下指令，以下載基礎架構部署所需的所有必要外掛程式。

```
terraform init
```

8 執行以下指令以根據輸入規劃和瞭解部署。

```
terraform plan
```

9 執行以下指令以建立輸入中定義的基礎架構。

```
terraform apply --auto-approve
```

10 (選擇性) 執行以下指令以識別 Azure 帳戶特定的資訊，例如儲存帳戶名稱、金鑰保存庫名稱和資料庫管理員詳細資料。

```
terraform output
```

11 執行以下指令，以在金鑰保存庫中建立機密值。

```
az keyvault secret set --name idm-common-password --vault-name <key vault name> --value "novell@123"
```

附註：您可以根據自己的要求，使用 Values.yaml 檔案指定多個機密值。

12 導覽至在其中產生了 TLS 證書的目錄，執行以下指令以將證書和金鑰輸出為 .pfx 格式。

```
openssl pkcs12 -export -out tls.pfx -inkey tls.key -in tls.crt -passout pass:''
```

附註：tls.pfx 檔案將在金鑰保存庫中用於驗證機密值和金鑰。

13 在 Azure Cloud Shell 中上傳 tls.pfx 檔案，並執行以下指令以將該檔案輸入金鑰保存庫。

```
az keyvault certificate import --vault-name <key vault name> -n "ingress-tls-cert" -f tls.pfx
```

例如：

```
az keyvault certificate import --vault-name idmkv20220712 -n "ingress-tls-cert" -f tls.pfx
```

14 導覽至 Identity_Manager_4.9.0_Containers/helm_charts/ 目錄並更新 value.yaml 檔案中的以下欄位。

表格 25-2

區段	欄位	描述
Identity Manager Advanced Edition	IS_ADVANCED_EDITION	指定您是否要部署 Identity Manager Advanced Edition。(true/false)
Azure PostgreSQL 伺服器例項	AZURE_POSTGRESQL_REQUIRED	指定您是否要使用 Azure PostgreSQL 伺服器例項做為 Identity Applications 和 Identity Reporting 的資料庫伺服器。(y/n)
Identity Manager Docker 影像的登入身分證明	登錄	指定 Azure 容器登錄伺服器名稱。
	name	指定包含登錄登入身分證明的 Kubernetes 機密名稱。
資料永續性	**Identity Engine 的永續性儲存** volumeClaimTemplate： ◆ storageClassName ◆ storageSize	指定 Identity Engine 使用的磁碟區宣告樣板的儲存類別名稱和儲存大小。
	共用永續性儲存 ◆ existingClaim dynamicClaim： ◆ storageClassName ◆ storageSize	如果您要使用現有的永續性磁碟區宣告 (PVC)，請輸入現有宣告的名稱。 否則，請指定儲存類別名稱和儲存大小進行 PVC 動態佈建。

區段	欄位	描述
密碼、金鑰和證書等敏感性資料的機密管理員	azureKeyVaultName：	指定 Azure 金鑰保存庫的名稱。
	azureKeyVaultTenantId	指定 Azure 金鑰保存庫租用戶 ID。請參考步驟 10 的 terraform 輸出。
	azureUserAssignedIdentityID	指定 Azure 金鑰保存庫機密提供者使用之使用者定義受管理身分的用戶端 ID。可以執行以下 az cli 指令來擷取身分的用戶端 ID： `az aks show -g <資源群組> -n <AKS 叢集名稱> --query addonProfiles.azureKeyvaultSecretsProvider.identity.clientId -o tsv`
入口組態	host	指定用於存取 Identity Manager Web 應用程式的網域名稱。
	azureKeyVaultCertificateName	指定包含 TLS 證書和私密金鑰的 Azure 金鑰保存庫證書名稱。

區段	欄位	描述
Identity Engine 組態	部署	指定您是否要部署 Identity Engine。(true/false)
	replicaCount	指定 Identity Engine 複製本 Pod 的數目。例如：「2」。
	ID_VAULT_TREENAME	指定 Identity Vault 樹狀結構名稱。
	ID_VAULT_SERVER_CONTEXT	指定 Identity Vault 伺服器網路位置。
	ID_VAULT_DRIVER_SET	指定 Identity Vault 預設驅動程式集名稱。
	ID_VAULT_DEPLOY_CTX	指定 Identity Vault 預設驅動程式集部署網路位置。
	ID_VAULT_ADMIN_LDAP	指定 Identity Vault 管理員 DN。
	ID_VAULT_PASSWORD: secret	指定包含 Identity Vault 管理員密碼的 Azure 金鑰保存庫機密。
	ID_VAULT_RSA_KEYSIZE	指定用於建立 RSA 證書管理中心金鑰和伺服器金鑰的金鑰大小。
	ID_VAULT_EC_CURVE	指定用於建立 EC 證書管理中心金鑰和伺服器金鑰的橢圓曲線演算法。
	ID_VAULT_CA_LIFE	指定用於建立預設伺服器證書的證書壽命。
	資源申請和限制 ◆ cpu ◆ 記憶體	指定 Identity Engine 資源申請和限制的 CPU 與記憶體值。如需更多詳細資料，請參閱 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/) (Pod 和容器的資源管理)

區段	欄位	描述
One SSO Provider (OSP) 組態	部署	指定您是否要部署 OSP。(true/false)
	replicaCount	指定 Identity Engine 複製本 Pod 的數目。例如：「2」。
	OSP_CUSTOM_NAME	指定 OSP 自訂登入畫面名稱。
	SSO_SERVICE_PWD:	指定包含 OSP 用戶端密碼的 Azure 金鑰保存庫機密。
	secret	
	資源申請和限制 ◆ cpu ◆ 記憶體	指定 OSP 資源申請和限制的 CPU 與記憶體值。如需更多詳細資料，請參閱 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/) (Pod 和容器的資源管理)

區段	欄位	描述
Identity Applications 組態	部署	指定您是否要部署 Identity Applications。(true/false)
	replicaCount	指定 Identity Engine 複製本 Pod 的數目。例如：「2」。
	UA_ADMIN	指定 Identity Applications 管理員 DN
	UA_ADMIN_PWD: secret	指定包含 Identity Applications 管理員密碼的 Azure 金鑰保存庫機密。
	UA_WFE_DB_PLATFORM_OPTION	指定 Identity Applications 和工作流程引擎資料庫平台。支援的值為：postgres、oracle 和 mssql
	UA_ORACLE_DATABASE_TYPE	如果資料庫平台為 Oracle， 請指定資料庫的組態。(sid/ 服務)
	UA_WFE_DB_HOST	指定 Identity Applications 和工作流程引擎資料庫伺服器主機。
	UA_WFE_DB_PORT	指定 Identity Applications 和工作流程引擎資料庫伺服器連接埠號碼。
	UA_DATABASE_NAME	指定 Identity Applications 資料庫名稱。
	WFE_DATABASE_NAME	指定工作流程引擎資料庫名稱。
	UA_WFE_DATABASE_USER	指定 Identity Applications 資料庫使用者名稱。
	UA_WFE_DATABASE_PWD: secret	指定包含 Identity Applications 資料庫使用者密碼的 Azure 金鑰保存庫機密。
	資源申請和限制 ◆ cpu ◆ 記憶體	指定 Identity Application 資源申請和限制的 CPU 與記憶體值。如需更多詳細資料，請參閱 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/) (Pod 和容器的資源管理)

區段	欄位	描述
表單轉譯器組態	部署	指定您是否要部署表單轉譯器。(true/false)
	資源申請和限制 - cpu - 記憶體	指定表單轉譯器資源申請和限制的 CPU 與記憶體值。如需更多詳細資料，請參閱 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/) (Pod 和容器的資源管理)
ActiveMQ 組態	部署	指定您是否要部署 ActiveMQ。(true/false)
	資源申請和限制 - cpu - 記憶體	指定表單轉譯器資源申請和限制的 CPU 與記憶體值。如需更多詳細資料，請參閱 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/) (Pod 和容器的資源管理)

區段	欄位	描述
Identity Reporting 組態	部署	指定您是否要部署 Identity Reporting。(true/false)
	RPT_ADMIN	指定 Identity Reporting 管理員 DN
	RPT_ADMIN_PWD: secret	指定包含 Identity Reporting 管理員密碼的 Azure 金鑰保存庫機密。
	RPT_DATABASE_PLATFORM_OPTION	指定 Identity Reporting 資料庫平台。支援的值為：postgres、oracle 和 mssql
	RPT_ORACLE_DATABASE_TYPE	如果資料庫平台為 Oracle， 請指定資料庫的組態。(sid/service)
	RPT_DATABASE_HOST	指定 Identity Reporting 資料庫主機。
	RPT_DATABASE_PORT	指定 Identity Reporting 資料庫連接埠號碼。
	RPT_DATABASE_NAME	指定 Identity Reporting 資料庫名稱。
	RPT_DATABASE_USER	指定 Identity Reporting 資料庫使用者。
	RPT_DATABASE_SHARE_PASSWORD: secret	指定包含 Identity Reporting 資料庫帳戶密碼的 Azure 金鑰保存庫機密
	資源申請和限制 ◆ cpu ◆ 記憶體	指定表單轉譯器資源申請和限制的 CPU 與記憶體值。如需更多詳細資料，請參閱 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/) (Pod 和容器的資源管理)

區段	欄位	描述
Self Service Password Reset (SSPR) 組態	部署	指定您是否要部署 SSPR。(true/false)
	CONFIGURATION_PWD:	指定要為管理員建立的用於設定 SSPR 的密碼。
	secret:	
	資源申請和限制 ◆ cpu ◆ 記憶體	指定 SSPR 資源申請和限制的 CPU 與記憶體值。如需更多詳細資料，請參閱 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/) (Pod 和容器的資源管理)
Identity Console 組態	部署	指定您是否要部署 Identity Console。(true/false)
	ID_CONSOLE_USE_OSP	不支援使用 One SSO Provider (OSP) 做為 Identity Console 的登入方法，因此預設值應為「n」。
	資源申請和限制 ◆ cpu ◆ 記憶體	指定 Identity Console 資源申請和限制的 CPU 與記憶體值。如需更多詳細資料，請參閱 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/) (Pod 和容器的資源管理)
進階組態	**DATA_CONTAINERS**：	
	DATA_CONTAINERS_LDIF	指定用於建立資料容器的 LDIF 組態。
	ROOT_CONTAINER GROUP_ROOT_CONTAINER USER_CONTAINER ADMIN_CONTAINER	指定根容器、群組根容器、使用者容器和管理員容器的 DN
	Kubernetes 叢集網域：	指定 Kubernetes 叢集網域
	KUBE_SUB_DOMAIN	

區段	欄位	描述
Identity Manager Web 應用程式的 TLS 組態	kubernetesSecret	將值指定為 `false`。
	azurekeyVault	將值指定為 `true`。 入口 TLS 證書將做為 kubernetes 機密進行管理。
敏感性資料的機密管理員	kubernetesSecret	將值指定為 `false`。
	azurekeyVault	將值指定為 `true`。 Azure 金鑰保存庫用做機密管理員。
AWS Secret Manager 用做機密管理員	awsSecretManager	將值指定為 `false`。

更新 `terraform.tfvars` 和 `values.yaml` 檔案後，按照 「Azure Kubernetes Service 上的 Identity Manager 容器部署」(第 299 頁) 中所述的步驟完成 Azure 上的 Identity Manager 容器部署。

Azure Kubernetes Service 上的 Identity Manager 容器部署

本節提供關於在 Azure Kubernetes Service 上部署 Identity Manager 容器的資訊。

1 執行以下指令連接到 Kubernetes 叢集並儲存所需的組態：

```
az aks get-credentials --resource-group <resource group> --name
<cluster name> --overwrite-existing
```

例如：

```
az aks get-credentials --resource-group idvault-rg --name cluster-name
--overwrite-existing
```

2 執行以下指令建立用於執行負載平衡器的 Nginx 例項：

```
helm repo add ingress-nginx https://kubernetes.github.io/ingress-nginx
```

3 執行以下步驟，以從 Azure 入口網站取得 Kubernetes Service 的公用 IP 位址。

3a 移至 Azure 首頁並按一下所有資源。

3b 在搜尋方塊中，輸入「負載平衡器」並按 Enter。

3c 在 Azure Cloud Shell 中執行以下指令以建立新的公用 IP：

```
az network public-ip create     --resource-group <aks-cluster-
resource-group-name> --name <name-public-ip> --sku Standard  --
version IPv4 --zone 1 2 3 --ip-tags 'RoutingPreference=Internet' --
dns-name <Domain Name>   --query publicIp.ipAddress -o tsv
```

3d 按一下與您的資源群組和 AKS 叢集關聯的負載平衡器。

3e 移至設定 > 前端 IP 組態並提供步驟 3c (第 299 頁) 建立的公用 IP。

3f 按一下「儲存」。

4 導覽至 IDM_4.9.0_Cloud_Deployment_files 目錄，執行以下指令安裝 Nginx-ingress 控制器：

```
helm install ingress-nginx ingress-nginx/ingress-nginx --namespace
<your namespace> --set controller.replicaCount=1 --set
controller.nodeSelector."kubernetes\.io/os"=linux --set
defaultBackend.nodeSelector."kubernetes\.io/os"=linux --set
controller.service.loadBalancerIP=<Kubernetes public IP address
obtained from the Azure portal> --set
controller.service.externalTrafficPolicy=Local --set
controller.service.annotations."service\.beta\.kubernetes\.io/azure-
dns-label-name"=<Domain Name>
```

使用您在步驟 3c (第 299 頁) 中建立的公用 IP 位址。

例如：

```
helm install ingress-nginx ingress-nginx/ingress-nginx --namespace idm
--set controller.replicaCount=1 --set
controller.nodeSelector."kubernetes\.io/os"=linux --set
defaultBackend.nodeSelector."kubernetes\.io/os"=linux --set
controller.service.loadBalancerIP="20.33.59.34" --set
controller.service.externalTrafficPolicy=Local --set
controller.service.annotations."service\.beta\.kubernetes\.io/azure-
dns-label-name"=identitymanager
```

5 若要執行 Helm 圖表，請執行以下指令：

```
helm install identity-manager helm_charts/identity-manager-1.4.0.tgz --
namespace <namespace> -f values.yaml
```

例如：

```
helm install identity-manager helm_charts/identity-manager-1.4.0.tgz --
namespace idm -f values.yaml
```

6 執行以下指令檢視 Azure Kubernetes Service 中執行的 Pod 清單：

```
kubectl get pods --watch -n <namespace>
```

例如：

```
kubectl get pods --watch -n idm
```

在 Azure Kubernetes Service 上設定遠端載入器服務

執行以下步驟以在 Azure Kubernetes Service 上設定遠端載入器服務：

1. 建立永續性磁碟區 (PV) 和永續性磁碟區宣告 (PVC) 以儲存遠端載入器資料。
2. 在 PV 內建立 `rdxml` 目錄。
3. 在 `rdxml` 目錄中建立 `driverconf` 目錄。
4. 在 `rdxml` 目錄中建立 `keystore` 目錄。

5 將所有必要的金鑰儲存區檔案和證書複製到 keystore 目錄。

6 在 rdxml 目錄中建立一個新的 .txt 檔案。例如 StartupRL.txt。

7 在 StartupRL.txt 檔案中，用以下格式指定所需內容：

< 遠端載入器組態檔案 > -sp < 驅動程式密碼 > < 遠端載入器密碼 >

例如：

```
config8000.txt -sp dirxml dirxml
```

或者，也可以用以下格式指定項目：

< 遠端載入器組態檔案 > -ksp < 金鑰儲存區密碼 > -kp < 金鑰密碼 >

例如：

```
config8000.txt -ksp dirxml -kp dirxml
```

8 從容器 tarball 中複製 helm-charts/rl-values.yaml，並更新該檔案中的以下欄位：

表格 25-3

區段	欄位	描述
遠端載入器 Docker 影像的登錄身分證明	登錄	指定 Azure 容器登錄伺服器名稱。
	name	指定包含登錄登入身分證明的 Kubernetes 機密名稱。
資料永續性	**共用永續性儲存** ◆ existingClaim dynamicClaim： ◆ storageClassName ◆ storageSize	如果您要使用現有的永續性磁碟區宣告 (PVC)，請輸入現有宣告的名稱。 否則，請指定儲存類別名稱和儲存大小進行 PVC 動態佈建。
驅動程式啟動檔案	driverStartupFileName	指定驅動程式啟動檔案的名稱。例如 StartupRL.txt
遠端載入器服務	ports	指定遠端載入器服務監聽的連接埠清單。

區段	欄位	描述
資源申請和限制	資源申請 • cpu • 記憶體	指定資源申請的 CPU 與記憶體值。如需更多詳細資料，請參閱 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/) (Pod 和容器的資源管理)
	限制 • cpu • 記憶體	指定限制的 CPU 與記憶體值。如需更多詳細資料，請參閱 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/) (Pod 和容器的資源管理)

9 從容器 tarball 中複製 `helm-charts/remote-loader-1.4.0.tgz`，並執行以下 helm 指令安裝遠端載入器：

```
helm install remote-loader helm_charts/remote-loader-1.4.0.tgz --
namespace idm -f rl-values.yaml
```

10 (選擇性) 如果您要安裝多個遠端載入器，請從容器 tarball 中複製 `helm-charts/remote-loader-1.4.0.tgz`，並執行以下 helm 指令：

```
helm install <remote-loader-n> helm_charts/remote-loader-1.4.0.tgz --
namespace idm -f rl-values.yaml
```

`remote-loader-n` 中的 n 表示安裝的第 n 個遠端載入器。

例如：

如果您要安裝兩個遠端載入器，那麼用於安裝第二個遠端載入器的指令是

```
helm install remote-loader-2 helm_charts/remote-loader-1.4.0.tgz --
namespace idm -f rl-values.yaml
```

在 Azure Kubernetes Service 上設定擴送代理程式服務

執行以下步驟在 Azure Kubernetes Service 上進行設定：

1 從容器 tarball 中複製 `helm-charts/fa-values.yaml`，並更新該檔案中的以下欄位：

表格 25-4

區段	欄位	描述
遠端載入器 Docker 影像的登錄身分證明	登錄	指定 Azure 容器登錄伺服器名稱。
	name	指定包含登錄登入身分證明的 Kubernetes 機密名稱。
資料永續性	**共用永續性儲存** ◆ existingClaim dynamicClaim： ◆ storageClassName ◆ storageSize	如果您要使用現有的永續性磁碟區宣告 (PVC)，請輸入現有宣告的名稱。 否則，請指定儲存類別名稱和儲存大小進行 PVC 動態佈建。
擴送代理程式服務	ports	指定遠端載入器服務監聽連接埠的值。
資源申請和限制	資源申請 ◆ cpu ◆ 記憶體	指定資源申請的 CPU 與記憶體值。如需更多詳細資料，請參閱「Resource Management for Pods and Containers」(Pod 和容器的資源管理) (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/)
	限制 ◆ cpu ◆ 記憶體	指定限制的 CPU 與記憶體值。如需更多詳細資料，請參閱「Resource Management for Pods and Containers」(Pod 和容器的資源管理) (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/)

區段	欄位	描述
ActiveMQ 服務	install	指定您是否要為擴送代理程式部署 ActiveMQ 服務 (true/false)
	資源申請 ◆ cpu ◆ 記憶體	指定 ActiveMQ 服務資源申請的 CPU 與記憶體值。如需更多詳細資料，請參閱 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/) (Pod 和容器的資源管理)
	限制 ◆ cpu ◆ 記憶體	指定 ActiveMQ 服務限制的 CPU 與記憶體值。如需更多詳細資料，請參閱 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/) (Pod 和容器的資源管理)

2 從容器 tarball 中複製 `helm-charts/fanout-agent-1.4.0.tgz`，並執行以下 helm 指令來安裝擴送代理程式：

```
helm install fanout-agent helm_charts/fanout-agent-1.4.0.tgz --
namespace idm -f rl-values.yaml
```

3 (選擇性) 如果您要安裝多個擴送代理程式，請從容器 tarball 中複製 `helm-charts/fanout-agent-1.4.0.tgz`，並執行以下 helm 指令：

```
helm install <fanout-agent-n> helm_charts/fanout-agent-1.4.0.tgz --
namespace idm -f rl-values.yaml
```

`fanout-agent-n` 中的 n 表示安裝的第 n 個擴送代理程式。

例如：

如果您要安裝兩個擴送代理程式，那麼用於安裝第二個擴送代理程式的指令是

```
helm install fanout-agent-2 helm_charts/fanout-agent-1.4.0.tgz --
namespace idm -f rl-values.yaml
```

26 部署後任務

本章提供關於在部署 Identity Manager 容器之後所要完成的任務的指示。

存取 Identity Manager 應用程式

若要存取任何 Identity Manager 應用程式，請在瀏覽器中輸入以下 URL。

`https://< 網域名稱 >/< 應用程式名稱 >`

例如：

`https://identitymanager.eastus.cloudapp.azure.com/idmdash`

在 Azure 虛擬機器上部署 Designer

執行以下步驟在 VM 子網路下的 Azure 虛擬機器上部署 Designer。

1. 請參閱《Quickstart: Linux VMs》(快速入門：Linux VM) 建立 Linux 機器，或參閱《Quickstart: Windows VMs》(快速入門：Windows VM) 建立 Windows VM。
2. 指定一個公用 IP 位址用於連接 Designer。
3. 在建立的虛擬機器中下載並安裝 Designer。如需詳細資訊，請參閱 「安裝 Designer」(第 67 頁) 或 Installing Designer (安裝 Designer) (適用於 Windows)。

在 Azure 虛擬機器上部署 SLM for IGA

執行以下步驟，在 VM 子網路下的 Azure 虛擬機器上部署 Sentinel Log Management (SLM) for Identity Governance and Administration (IGA)。

1. 建立 Linux 機器，具體請參閱《Quickstart: Linux VMs》(快速入門：Linux VM)。
2. 指定一個公用 IP 位址用於連接 SLM for IGA 安裝程式。
3. 在建立的虛擬機器中下載並安裝 SLM for IGA。如需詳細資訊，請參閱 「安裝 Sentinel Log Management for Identity Governance and Administration」(第 69 頁)。

處理 AKS 的 RPM 更新和協力廠商檔案

此 Service Pack 提供了一種處理容器中 RPM 更新和協力廠商檔案的有效方式。可將所需的 RPM 檔案、程式庫 (.so) 檔案和協力廠商 .jar 檔案放入 mountfiles，來實現這種處理。將強制更新 mountfiles 目錄中的 RPM 檔案。重新啟動容器時，.so 和 .jar 檔案將分別自動軟連結到 /opt/novell/eDirectory/lib64/nds-modules/ 和 /opt/novell/eDirectory/lib/dirxml/classes/ 目錄。這種做法旨在更新 Docker 容器中的驅動程式。

附註：目前，此增強功能適用於 Identity Manager 引擎和遠端載入器容器。

1. 登入 Azure 入口網站並按一下 。
2. 執行以下指令登入您的永續性磁碟區：

   ```
   kubectl exec –it -n idm <container name> bash
   ```

   例如

   ```
   kubectl exec –it -n idm identityengine-0 bash
   ```

3. 將所需檔案複製到容器特定的相應 mountfiles 目錄。

   3a (視情況而定) 對於 Identity Manager 引擎容器，請執行以下指令將檔案複製到 /config/idm/mountfiles：

   ```
   kubectl cp -n < 名稱空間 > < 要複製的檔案 > < 容器名稱 >:/config/idm/mountfiles
   ```

   3b (視情況而定) 對於 Identity Manager 遠端載入器容器，請執行以下指令將檔案複製到 /config/rdxml/mountfiles：

   ```
   kubectl cp -n < 名稱空間 > < 要複製的檔案 > < 容器名稱 >:/config/rdxml/mountfiles
   ```

   附註：支援的檔案格式為 .so、.jar 和 .rpm。

4. 執行以下指令以重新啟動容器：

   ```
   helm upgrade identity-manager helm_charts/identity-manager-1.4.0.tgz --namespace <namespace> -f values.yaml
   ```

重要：無論掛接檔案中的哪個 rpm 優先程度最高，將來更新時，您都需要小心移除現有 rpm 並更新最新 rpm。

27 維護 Identity Manager 容器的部署

本章介紹如何維護 Azure Kubernetes 叢集上的 Pod (包含一或多個容器的群組) 部署。

重要：如果您需要在部署中新增更多圖表、重新建立部署或者增加 (或減少) 部署中的 Pod 數目，請執行以下步驟：

1 登入 Azure 入口網站。

2 按一下  ，然後執行以下指令。

```
helm upgrade identity-manager helmcharts/identity-manager-1.4.0.tgz --
namespace < 名稱空間 > -f values.yaml
```

管理資料永續性層

在 Visual Studio Code 應用程式中執行以下步驟來修改 Pod 的資料層：

1 下載並安裝 Visual Studio Code。請參閱 code.visualstudio.com/download。

2 開啟 Visual Studio Code 應用程式，按一下  。

3 在搜尋方塊中輸入 **Azure**，然後按 Enter。

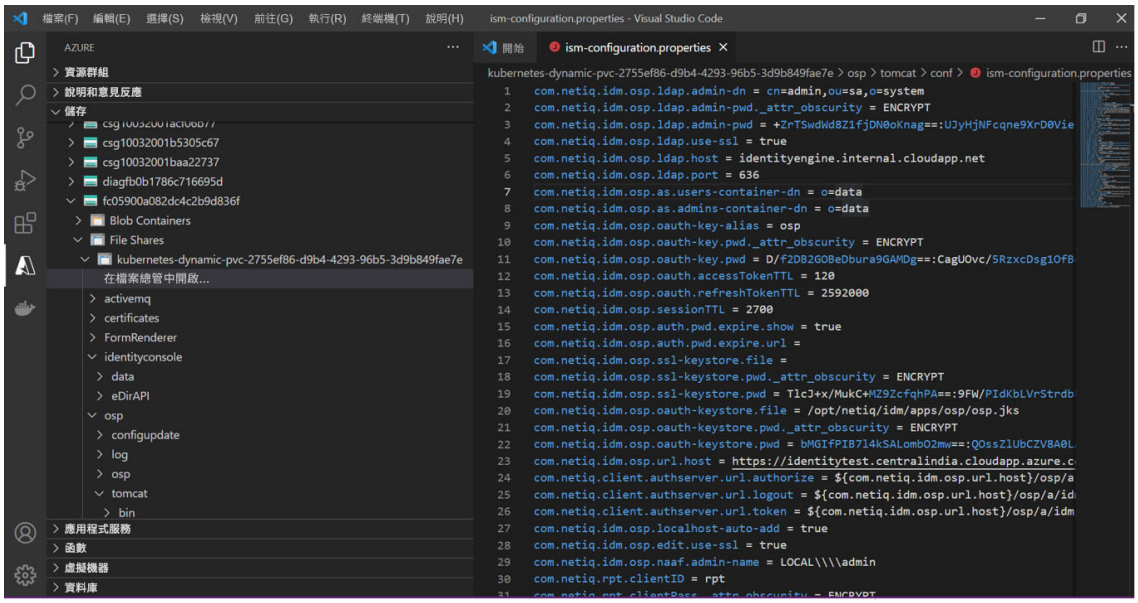
4 在「Azure 工具」中按一下安裝。

5 按一下  。

6 移至儲存 > **Security-IdentityMgmtAZ-NonProd** > **fc05900a082dc4c2b9d836f** > 檔案共用 > **Kubernetes 動態 PVC** (如需詳細資訊，請參閱圖 27-1(第 308 頁))。

附註：上面導覽路徑中提及的 **Security-IdentityMgmtAZ-NonProd** 和 **fc05900a082dc4c2b9d836f** 金鑰僅供參考，請根據您的登入身分證明予以變更。

圖 27-1 Visual Studio 儲存



7 選取檔案並變更所需內容。

8 移至**檔案**功能表，按一下**儲存**。

9 儲存所有變更後，重新啟動 Pod (請參閱 「重新啟動 Pod」(第 308 頁))。

重新啟動 Pod

執行以下步驟重新啟動 Azure 中的 Pod。

例如，如果您對資料層進行了任何變更，則需要重新啟動容器。

1 登入 Azure 入口網站。

2 在搜尋方塊中輸入「所有資源」，然後按 Enter。

3 在「服務」下，選取**所有資源**。

4 移至您的 Kubernetes 叢集。

5 在「Kubernetes 資源」下，按一下**工作負載**。

6 移至 **Pod** 索引標籤，按一下**依名稱空間過濾**下拉式清單，然後選取 **idm**。

7 選取要重新啟動的 Pod。

8 按一下「**刪除**」。如需詳細資訊，請參閱圖 27-2(第 309 頁)。

附註：系統將識別已刪除的 Pod，並自動觸發部署到新 Pod 的操作。

圖 27-2 Kubernetes 叢集



存取 Pod

執行以下步驟存取 Azure 中的 Pod：

1 登入 Azure 入口網站。

2 按一下 。

3 執行以下指令識別 Pod 的名稱：

```
kubectl get pods --watch -n <namespace>
```

例如：

```
kubectl get pods --watch -n idm
```

4 執行以下指令：

```
kubectl exec -it -n idm <pod-name> bash
```

例如：

```
kubectl exec -it -n idm userapp-d54f98b58-qcpmz bash
```

重新啟動 Azure Kubernetes 叢集

執行以下步驟以確定所有 IDM 元件正常關閉：

1 登入 Azure 入口網站。

2 移至您的 Kubernetes 叢集。

3 在「Kubernetes 資源」下，按一下**工作負載**。

4 移至**部署**索引標籤，按一下**依名稱空間過濾**下拉式清單，然後選取您的名稱空間。

5 選取部署並按一下**刪除**。

6 移至 **Pod** 索引標籤，按一下**依名稱空間過濾**下拉式清單，然後選取您的名稱空間。

7 按一下**重新整理**，檢查是否已完全移除元件 Pod。

8 移至**具狀態集**索引標籤，按一下**依名稱空間過濾**下拉式清單，然後選取您的名稱空間。

9 選取具狀態集並按一下**刪除**。

10 同樣，移至 **Pod** 索引標籤，按一下**依名稱空間過濾**下拉式清單，然後選取您的名稱空間。

11 按一下**重新整理**，檢查是否已完全移除元件。

12 移至「Kubernetes 資源」下的「綜覽」，按一下**停止**並等待一段時間。

13 叢集完全停止後，按一下**啟動**。

14 在 Azure CLI 中，執行以下指令重新啟動 Nginx-ingress 控制器：

```
helm upgrade nginx-ingress ingress-nginx/ingress-nginx --namespace
<your namespace> --set controller.replicaCount=1 --set
controller.service.loadBalancerIP=<Public IP address assigned to load
balancer> --set
controller.service.annotations."service\.beta\.kubernetes\.io/azure-
dns-label-name"=<LoadBalancerName>
```

例如

```
helm upgrade nginx-ingress ingress-nginx/ingress-nginx --namespace idm
--set controller.replicaCount=1 --set
controller.service.loadBalancerIP=192.168.0.1 --set
controller.service.annotations."service\.beta\.kubernetes\.io/azure-
dns-label-name"=identitymanager
```

15 執行以下指令重新啟動剩餘元件：

```
helm upgrade identity-manager helm_charts/identity-manager-1.4.0.tgz --
namespace <namespace> -f values.yaml
```

例如

```
helm upgrade identity-manager helm_charts/identity-manager-1.4.0.tgz --
namespace idm -f values.yaml
```

16 等待所有 Pod 進入就緒狀態。

若要檢查 Pod 的目前狀態，請執行以下指令：

```
kubectl get pods --watch -n <namespace>
```

17 執行以下指令重新啟動引擎服務：

```
kubectl rollout restart -n <namespace> statefulset/identityengine
```

例如

```
kubectl rollout restart -n idm statefulset/identityengine
```

18 重複 步驟 16.

縮放 Identity Manager 引擎複製本

縮放 Identity Manager 引擎複製本的程序分為兩個部分：

縮減 Identity Manager 引擎複製本的使用案例

本主題將介紹一個基本使用案例，您可以參考該案例來縮減 Identity Manager 引擎複製本。

開始之前

- 在縮減 Identity Manager 引擎複製本規模之前，請仔細瞭解該程序。
- 一次只能縮減一個 Pod。

使用案例

假設有 3 個 Identity Manager 引擎例項，其 Pod 名稱為：

- identityengine-0
- identityengine-1
- identityengine-2

縮減為兩個 Identity Manager 引擎例項時，identityengine-2 將會關閉。

在縮減之前，需要在 Identityengine-2 上執行以下動作：

1. 將例項 Identityengine-2 上執行的驅動程式移轉至另一個例項，或者在另一例項上重新建立驅動程式。
2. 從樹狀結構中刪除伺服器。
3. 執行以下指令列出永續性磁碟區宣告 (PVC)：

   `kubectl get pvc -n < 名稱空間 >`

   例如：

   `kubectl get pvc -n idm`
4. 執行以下指令刪除 identityengine-2 的 PVC：

   `kubectl delete pvc -n < 名稱空間 > <identityengine 複製本名稱 >`

   例如：

   `kubectl delete pvc -n idm identityenginedata-identityengine-2`
5. 在 `values.yaml` 檔案中將引擎複製本計數設定為 2。
6. 使用以下指令進行縮減：

   ```
   helm upgrade identity-manager helm_charts/identity-manager-1.4.0.tgz --
   namespace < 名稱空間 > -f values.yaml
   ```

擴增 Identity Manager 引擎複本

執行以下步驟來擴增 Identity Manager 引擎複製本：

1. 登入 Azure 入口網站。
2. 按一下  。

3 在 values.yaml 檔案中增加 Identity Manager 引擎複製本計數。

4 使用以下指令進行擴增：

```
helm upgrade identity-manager helm_charts/identity-manager-1.4.0.tgz --
namespace < 名稱空間 > -f values.yaml
```

縮放 OSP 和 Identity Applications 複本

執行以下步驟來擴增或縮減 OSP 和 Identity Applications 複製本：

1 登入 Azure 入口網站。

2 按一下  。

3 在 values.yaml 檔案中增加或減少 OSP/Identity Applications 複製本計數。

4 使用以下指令進行擴增或縮減：

```
helm upgrade identity-manager helm_charts/identity-manager-1.4.0.tgz --
namespace < 名稱空間 > -f values.yaml
```

銷毀使用 Terraform 建立的整個資源

執行以下步驟來銷毀使用 Terraform 建立的資源：

附註：請在經過慎重思考後再繼續執行此程序。

1 導覽至您在其中使用 terraform 建立了資源的目錄。

2 執行以下指令來刪除資源：

```
terraform destroy --auto-approve
```

3 (選擇性) 如果在執行上述指令期間出現任何錯誤，請重新執行該指令。

X 在 AWS EC2 上部署 Identity Manager

本部分介紹如何在 AWS 雲端規劃和實作 Identity Manager。

- 第 28 章 「在 AWS EC2 上規劃和實作 Identity Manager」 (第 315 頁)
- 第 29 章 「範例混合式 Identity Manager 方案」 (第 333 頁)

28 在 AWS EC2 上規劃和實作 Identity Manager

Identity Manager 現在支援在 Amazon Web Services (AWS) EC2 上以服務的形式部署以下 Identity Manager 元件：

- Identity Vault
- Identity Manager 引擎
- Identity Manager 驅動程式和遠端載入器
- Designer
- Identity Applications
- Identity Reporting

如需 AWS EC2 支援之作業系統的更多詳細資料，請參閱 System Requirements for Identity Manager 4.9 (Identity Manager 4.9 系統要求)

先決條件

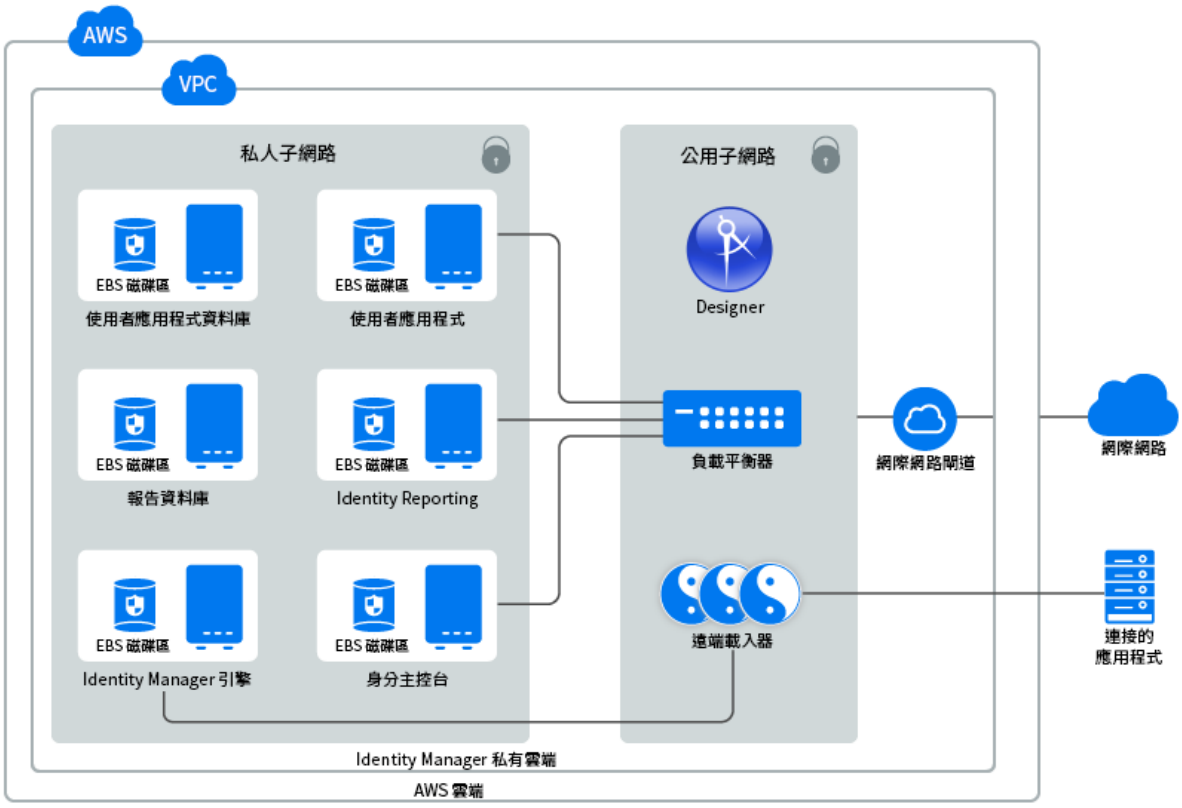
除了 Identity Manager 元件的系統要求以外，請確定您符合以下先決條件：

- 在 AWS EC2 上有管理帳戶。
- 已下載及解壓縮 `Identity_Manager_4.9.0_Linux.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 AWS EC2 例項的 SSH 用戶端。

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。特性 28-1 「AWS EC2 上的 Identity Manager 部署」 (第 316 頁) 演示了一個範例部署，後續章節中將用到該部署。

圖 28-1 AWS EC2 上的 Identity Manager 部署



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：

- 「準備 AWS Virtual Private Cloud」(第 317 頁)
- 「建立和部署例項」(第 319 頁)
- 「準備 EC2 例項」(第 320 頁)
- 「安裝 Identity Manager 元件」(第 322 頁)
- 「安裝 Identity Applications 和 Identity Reporting 的資料庫」(第 322 頁)
- 「安裝 Designer」(第 324 頁)
- 「建立 AWS EC2 負載平衡器」(第 324 頁)
- 「(選擇性) 使用註冊的代管區域建立別名 DNS」(第 329 頁)
- 「存取 Identity Manager 元件」(第 330 頁)

準備 AWS Virtual Private Cloud

本節介紹將 AWS VPC 設定為與 Identity Manager 配合使用的一般步驟。如需詳細資訊，請參閱 Amazon Elastic Compute Cloud 文件。

建立 AWS VPC 服務需要執行的步驟如下：

1 登入 AWS Management Console (AWS 管理主控台)。

2 按一下 **Services** (服務) 並建立以下服務：

服務	步驟
VPC	1. 按一下 **Networking & Content Delivery** (網路和內容遞送) 下的 **Services > VPC** (服務 > VPC)。 2. 按一下 **Start VPC Wizard** (啟動 VPC 精靈)。 3. 選取 VPC 組態類型，然後按一下 **Select** (選取)。 4. 在表單中指定詳細資料，然後按一下 **Create VPC** (建立 VPC)。 如此即會建立指定大小的私人網路。VPC 和子網路建立程序使用 CIDR 表示法來表示位址範圍。最大的 VPC 大小為 /16 網路。 如需詳細資訊，請參閱 Amazon Virtual Private Cloud 文件 (https://docs.aws.amazon.com/vpc/index.html)。
重要：使用 **Start VPC Wizard** (啟動 VPC 精靈) 建立 VPC 會建立該 VPC 的子網路、網際網路閘道和路由表。您可以依如下所述檢視或編輯這些項目：	
次網路	若要依圖 28-1 中所示部署 Identity Manager 元件，請在 VPC 中建立三個子網路。例如 privateSN、publicSN1 和 publicSN2。 建立子網路需要執行的步驟如下。 1. 在左側功能表中，按一下 **Subnets** (子網路)。 2. 按一下 **Create Subnet** (建立子網路)。 3. 指定用於識別子網路的名稱標記。 4. 指定 VPC 中的 **IPv4 CIDR 區塊**。 例如：`10.0.0.0/24` 您必須在不同的可用性區域中建立公用子網路。 5. 依次按一下 **Yes (是)**、**Create (建立)**。 6. (視情況而定) 對於公用子網路，啟用自動指定公用 IP 位址： a. 選取 **Subnet Actions > Modify auto-assign IP settings** (子網路動作 > 修改自動指定 IP 設定)。 b. 選取 **Enable auto-assign public IPv4 address** (啟用自動指定公用 IPv4 位址)。 c. 按一下 **Save** (儲存)。 重複上述步驟以建立更多子網路。

服務	步驟
網際網路閘道	1. 在左側功能表中，按一下 **Internet Gateways** (網際網路閘道)。 2. 按一下 **Create Internet Gateway** (建立網際網路閘道)。 3. 指定名稱標記，然後按一下 **Create** (建立)。 4. 選取新建立的網際網路閘道，並將其連接至 VPC： a. 選取 **Actions > Attach to VPC** (動作 > 連接至 VPC)。 b. 從清單中選取該 VPC，然後按一下 **Attach** (連接)。
路由表	1. 在左側功能表中，按一下 **Route Tables** (路由表)。 2. 選取系統自動為此 VPC 建立的路由表。 3. 在 **Routes** (路由) 索引標籤中： a. 按一下 **Edit** (編輯)。 b. 按一下 **Add another route** (新增另一個路由)。 c. 在 **Destination** (目的地) 中，指定 `0.0.0.0/0`。 d. 在 **Target** (目標) 中，選取與此 VPC 關聯的網際網路閘道表。請參閱**網際網路閘道**。 e. 按一下 **Save** (儲存)。 4. 在 **Subnet Association** (子網路關聯) 索引標籤中： a. 按一下 **Edit** (編輯)。 b. 找到要與此 VPC 關聯的子網路，然後按一下 **Save** (儲存)。
(選擇性) 代管的區域	如果您已註冊網域，可以執行以下動作以使用該網域來代管 Identity Manager 元件： 1. 按一下 **Services > Route 53 > Hosted Zones** (服務 > Route 53 > 代管的區域)。 2. 按一下 **Create Hosted Zone** (建立代管的區域)，並指定如下所述的詳細資料： ◆ **網域名稱**：指定網域名稱。 ◆ **備註**：新增備註。 ◆ **類型**：指定所代管區域的類型。 3. 按一下 **Create** (建立)。
彈性 IP 位址	1. 按一下 **Services > EC2** (服務 > EC2)。 2. 在左側功能表中，選取 **Elastic IPs** (彈性 IP)。 3. 按一下 **Allocate New address** (配置新位址)。 4. 按一下 **Allocate** (配置)。 系統即會配置一個其他任何資源均未使用的靜態 IPv4 位址。 5. 按一下 **Cose** (關閉)。

建立和部署例項

本節介紹建立和部署 Identity Manager 基本設定 (包含 Identity Manager 引擎、Identity Applications、Reporting、使用者應用程式資料庫和 Reporting 資料庫) 例項的步驟。

建立 Identity Manager 元件例項需要執行的步驟如下。

1 按一下 **Services** (服務) > **EC2**。

2 按一下 **Launch Instance** (啟動例項)。

3 選取 `SLES 15 SPx` 或影像。

4 選取符合基礎作業系統及 Identity Manager 元件部署要求的例項類型。請參閱 System Requirements for Identity Manager 4.9 (Identity Manager 4.9 系統要求)。

5 按一下 **Next: Configure Instance Details** (下一步：設定例項詳細資料)。

確定該例項使用的是正確的 VPC 和子網路。此頁面中會自動填入子網路設定。

欄位	動作
Auto-assign Public IP (自動指定公用 IP)	對於公用子網路，請設定為 `Enable` (啟用)。使用此設定會自動填入子網路設定。對於私人子網路，請將值設定為 `Disable` (停用)。

6 按一下 **Next: Add Storage** (下一步：新增儲存)。

預設儲存大小為 10 GB。請依據您的要求變更儲存大小。請參閱 System Requirements for Identity Manager 4.9 (Identity Manager 4.9 系統要求)。

7 按一下 **Next: Add Tags** (下一步：新增標記)。

請視需要新增標記。使用標記可以組織例項。例如，可將以下兩個標記新增至每個例項：

- 一個標記指示該例項的用途
- 一個標記指示此機器的擁有者

8 按一下 **Next: Configure Security Group** (下一步：設定安全性群組)。

安全性群組是例項群組的虛擬防火牆規則。建議對防火牆要求相同的每組例項單獨建立一個安全性群組。

例如，您可對 Identity Manager 引擎的所有節點、Identity Applications 的所有節點以及 Identity Reporting 的所有節點分別設定一個安全性群組。依預設，新安全性群組僅允許連接埠 22 上的內送流量，因此，您只能使用 SSH 連接至例項。

如需詳細資訊，請參閱 「Amazon EC2 Security Groups for Linux Instances」 (Linux 例項的 Amazon EC2 安全性群組) (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html)。

9 建立新的安全性群組；指定該群組的名稱和描述。

在安裝以下 Identity Manager 元件之前，請新增額外的連接埠規則：

配件	埠	描述
Identity Vault 的 LDAP	TCP 636	需要使用它來進行 LDAP 安全通訊。
Identity Applications	TCP 8543	需要使用它來進行 HTTPS 通訊，以便存取 Identity Applications。
Identity Reporting	TCP 8643	需要使用它來進行 HTTPS 通訊，以便存取 Identity Reporting。
PostgreSQL 資料庫	TCP 5432	需要使用它來進行安全資料庫通訊，以便存取 PostgreSQL。

10 按一下 **Review and Launch** (查看並啟動)。

11 查看詳細資料後，按一下 **Launch** (啟動)。

12 選取現有的金鑰組或建立新的金鑰組。

此金鑰組用於透過 SSH 存取例項。您可在多部機器上使用相同金鑰組。

13 按一下 **Download Key Pair** (下載金鑰組)。

重要：您只能使用私密金鑰來連接和管理例項。因此，在下載金鑰組後，請勿遺失私密金鑰。

14 連接啟始化例項時建立的彈性 IP 位址。

15 重複步驟 1 至步驟 13 以建立其他例項。

準備 EC2 例項

啟動某個例項，並驗證軟體儲存庫。若要驗證設定的軟體儲存庫，請執行以下操作：

1 使用金鑰組登入某個例項。

2 切換至 `root` 使用者。

3 驗證您的作業系統中是否存在以下更新：

SLES 上的 SLES12-SP3-Pool 和 SLES12-SP3-Updates：若要進行驗證，請執行 `zypper lr -n` 指令。

RHEL 上的 rhui-REGION-rhel-server-releases/7Server/x86_64：若要進行驗證，請執行 `yum repolist` 指令。

附註：如果您的作業系統中沒有儲存庫，請驗證設定的彈性 IP 位址是否已連接至該例項，然後重新啟動該例項。

4 為作業系統安裝以下先決元件：

SLES

使用 `zypper` 指令安裝 `glibc-32bit` 程式庫。

Red Hat

使用 `yum install` 指令安裝以下先決元件：

- `unzip`
- `ksh`
- `bc`
- `glibc-*.i686`
- `libXau-1.0.8-2.1.el7.i686`
- `libxcb.i686`
- `libX11.i686`
- `libXtst.i686`
- `libXrender.i686`
- `libgcc.i686`
- `lsof`

對於 Identity Manager 引擎，您可以編輯 `prerequisite.sh` 程序檔，移除其中包含的 `compat-libstdc++-33.x86_64`。Identity Manager 安裝不再需要此套件。

5 設定 `/etc/hosts` 和 `hostname`：

5a 使用例項的私人 IP 位址在防火牆中保護 Identity Manager 伺服器。

5b 為例項指定 DNS 名稱並更新 `hosts` 檔案。

例如：

```
# 10.0.0.1 identityEngine.example.com identityEngine
```

5c 設定主機名稱和網域名稱。

SLES

```
yast lan
```

RHEL

```
hostnamectl set-hostname idmengine.example.com
```

6 (視情況而定) 建立加密的彈性區塊儲存 (EBS) 磁碟區，以加密雲端的資料。

6a 按一下 **Services > EC2** (服務 > EC2)。

6b 在 **Elastic Block Store** (彈性區塊儲存) 中，選取 **Volumes** (磁碟區) 並按一下 **Create Volume** (建立磁碟區)。

6c 指定所需的磁碟區大小。

6d 選取 **Encrypt this volume** (加密此磁碟區) 並按一下 **Create Volume** (建立磁碟區)。

6e 在清單中選取新建立的磁碟區。

6f 在 **Actions** (動作) 中按一下 **Attach Volume** (連接磁碟區)，以將該磁碟區連接至 EC2 例項。

6g 對每個例項重複上述步驟。

如需 EBS 的詳細資訊，請參閱 「Amazon EBS」。

7 使用作業系統工具格式化該磁碟區並掛接分割區：

SLES

執行 `yast disk` 指令格式化該磁碟區。

RHEL

執行 `mkfs` 進行格式化，並新增至 `/etc/fstab`。如需詳細資訊，請參閱《Red Hat Enterprise Linux Deployment Guide》(Red Hat Enterprise Linux 部署指南)。

附註：

- 掛接 Identity Manager 引擎資料分割區。資料分割區預設為 `/var/opt/novell/`。
- 在 `/opt/netiq/` 中掛接其他 Identity Manager 元件。

---

8 在所有例項上的 `/etc/hosts` 檔案中，更新所有機器的 DNS 或 IP 位址。

安裝 Identity Manager 元件

在安裝 Identity Manager 元件之前，請執行以下步驟：

1 在要安裝 Identity Manager 元件的例項上下載 `Identity_Manager_4.9.0_Linux.iso`。

2 掛接下載的 `.iso` 檔案。

3 (視情況而定) 建立 Identity Applications 和 Identity Reporting 的資料庫。如需詳細資訊，請參閱 「安裝 Identity Applications 和 Identity Reporting 的資料庫」(第 322 頁)。

4 從 `.iso` 檔案的根目錄中執行 `./install.sh` 指令。

5 通讀授權合約，然後輸入 `y` 以接受授權合約。

6 選取自訂安裝選項，然後選取要在例項上安裝的元件。設定該元件。如需詳細資訊，請參閱表格 5-2 「自訂組態」(第 77 頁)。

7 在 Identity Reporting 和 Identity Applications 上執行 `configupdate.sh` 以設定所有用戶端。

安裝 Identity Applications 和 Identity Reporting 的資料庫

如果您要在外部伺服器上安裝 Identity Applications 和 Identity Reporting 的 PostgreSQL 資料庫，應在安裝前執行以下步驟：

1 導覽至掛接 `Identity_Manager_4.9.0_Linux.iso` 的位置。

2 找到 `/common/packages/postgres/` 目錄並安裝 PostgreSQL。

```
rpm -ivh netiq-postgresql-9.6.6-0.noarch.rpm
```

3 執行以下指令以將群組關聯到 `postgres` 使用者：

```
/usr/sbin/usermod -a -G postgres postgres
```

4 在 /etc/passwd 檔案中，將 postgres 使用者的主目錄路徑變更為 /opt/netiq/idm/postgres/。

4a 導覽至 /etc/ 目錄。

4b 編輯 passwd 檔案。

```
vi /etc/passwd
```

4c 將 postgres 使用者的主目錄變更為 /opt/netiq/idm/postgres/。

5 以 postgres 使用者身分登入。

例如：

```
su - postgres
```

6 在 PostgreSQL 安裝位置中建立 data 目錄。

```
mkdir -p <POSTGRES_HOME>/data, where <POSTGRES_HOME> is /opt/netiq/idm/postgres
```

例如：

```
mkdir -p /opt/netiq/idm/postgres/data
```

7 輸出 PostgreSQL home 目錄

```
export PGHOME=<postgres home directory path>
```

例如：

```
export PG_HOME=/opt/netiq/idm/postgres
```

8 輸出 PostgreSQL 密碼：

```
export PGPASSWORD=< 輸入資料庫密碼 >
```

9 啟始化資料庫。

```
"LANG=en_US.UTF-8 <POSTGRES 主目錄 >/bin/initdb -D <POSTGRES 主目錄 >/data"
```

例如：

```
"LANG=en_US.UTF-8 /opt/netiq/idm/postgres/bin/initdb -D /opt/netiq/idm/postgres/data"
```

10 在 /opt/netiq/idm/postgres/ 目錄中建立以下元件的資料庫。

Identity Applications

```
$ createdb idmuserappdb
$ psql -s idmuserappdb
# create user idmadmin password 'somepassword';
# GRANT ALL PRIVILEGES ON DATABASE idmuserappdb TO idmadmin;
# ALTER DATABASE idmuserappdb OWNER TO idmadmin;
```

Identity Reporting

```
$ createdb idmrptdb
```

11 以 postgres 使用者身分登出。

12 修改 postgresql.conf 檔案，以允許 PostgreSQL 例項監聽除 localhost 以外的網路例項。

12a 導覽至 /opt/netiq/idm/postgres/data/ 目錄。

12b 編輯 postgresql.conf 檔案：

```
vi postgresql.conf
```

12c 在檔案中新增下一行：

```
listen_addresses = '*'
```

13 在 <postgres home directory path>/data 下建立 pg_log 目錄。

例如：

```
mkdir -p /opt/netiq/idm/postgres/data/pg_log
```

14 變更 pg_log 目錄的許可權。

```
chown -R postgres:postgres <postgres directory path>/data/pg_log
```

例如：

```
chown -R postgres:postgres /opt/netiq/idm/postgres/data/pg_log
```

15 啟動 PostgreSQL 服務。

```
systemctl start netiq-postgresql
```

此指令將啟動新的 PostgreSQL 服務。

安裝 Designer

若要使用 Designer，必須在 Windows 機器上安裝 Designer。

1 在公用子網路中，啟動支援的 Windows 例項。

對於 Windows 安全性群組，請僅使用 rdesktop 連接埠。例如 3389。

2 在 Windows 例項上安裝 Designer。如需詳細資訊，請參閱《*NetIQ Identity Manager 安裝和升級指南 - Windows*》中的「*安裝 Designer*」。

建立 AWS EC2 負載平衡器

您可以建立負載平衡器以在各 Identity Manager 元件之間平衡內送申請的負載。負載平衡器可用於保護 Identity Manager 伺服器免遭公用存取。

以下程序說明了為範例部署方案設定負載平衡器所需的組態詳細資料：

為負載平衡器建立證書以使用安全通訊

負載平衡器使用此證書在各 Identity Manager 元件之間建立安全通訊。可透過三種方式為負載平衡器建立證書：

- 「使用 AWS Certificate Manager (ACM)」 (第 325 頁)

- 「將外部證書上傳到 ACM」 (第 325 頁)
- 「將外部證書上傳到 IAM」 (第 325 頁)

使用 AWS Certificate Manager (ACM)

1 按一下 **Services > Certificates Manager** (服務 > Certificates Manager)。
2 按一下 **Request Certificate** (申請證書)。
3 指定要為其建立證書的 DNS 名稱。
4 驗證 DNS 機構。

將外部證書上傳到 ACM

1 按一下 **Services > Certificates Manager** (服務 > Certificates Manager)。
2 按一下 **Import Certificate** (輸入證書)。
3 指定證書詳細資料。

將外部證書上傳到 IAM

1 按一下 **Services** (服務)。
2 在 **Security, Identity & Compliance** (安全性、身分與合規) 中，按一下 **IAM**。
3 使用 IAM API 指定證書詳細資料。如需詳細資訊，請參閱 「Uploading Server Certificate Using IAM API」 (使用 IAM API 上傳伺服器證書)。

建立目標群組

使用目標群組可將負載平衡器關聯至負載將分散到的各個例項 (目標) 的 IP 位址。

建立目標群組需要執行的步驟如下：

1 在 EC2 儀表板中，按一下 **LOAD BALANCING** (負載平衡) 下的 **Target Groups** (目標群組)。
2 按一下 **Create target group** (建立目標群組)。
3 指定以下詳細資料：

欄位	描述
Target group name (目標群組名稱)	指定目標群組的名稱。 您可以指定要設定此目標群組的元件的名稱。例如 Identity Applications、Identity Reporting。
通訊協定	選取 **HTTPS**。
Port (連接埠)	指定伺服器設定為要監聽的連接埠。 下面是不同 Identity Manager 元件使用的範例連接埠值： ◆ **Identity Applications**：8543 ◆ **Identity Reporting**：8643

欄位	描述
Target type (目標類型)	選取 **Instance** (例項)。
VPC	選取您為 Identity Manager 元件例項所選的相同 VPC。
Health Check Settings (狀態檢查設定)	
Protocol (通訊協定)	選取 **HTTPS**。 負載平衡器在執行狀態檢查時將使用此通訊協定。
Path (路徑)	指定狀態檢查的目的地路徑。 要執行狀態檢查的 Identity Manager 元件的預設路徑如下： ◆ **Identity Applications**：`/idmdash/index.html` ◆ **Identity Reporting**：`/IDMRPT/index.html`
Advanced health check settings (進階狀態檢查設定)	保留預設值。

4 按一下 **Create** (建立)。

5 啟用工作階段粘性。

5a 選取您建立的目標群組。

5b 在 **Description** (描述) 索引標籤中，按一下 **Edit attributes** (編輯屬性)。

5c 對 **Stickiness** (粘性) 選取 **Enable** (啟用)。

6 重複上述步驟為每個應用程式建立目標群組。

附註：如果將 SSPR 安裝在其他伺服器上，請為此元件單獨建立一個目標群組。

建立負載平衡器

建立負載平衡器需要執行的步驟如下：

1 在左側功能表中，按一下 **Load Balancers** (負載平衡器)。

2 按一下 **Create Load Balancers** (建立負載平衡器)。

3 按一下 **Application Load Balancer** (應用程式負載平衡器) 下的 **Create** (建立)。

4 指定以下詳細資料：

欄位	描述
Name (名稱)	指定負載平衡器的名稱。
Scheme (配置)	選取 **internet-facing** (網際網路對向)。

欄位	描述
Listeners (監聽程式)	若要新增更多監聽程式至負載平衡器，請按一下 **Add Listener** (新增監聽程式)。 依如下所述指定監聽程式連接埠： **對於 Identity Applications：** ◆ **Load Balancer Protocol** (負載平衡器通訊協定)：HTTPS ◆ **Load Balancer Port** (負載平衡器連接埠)：8543 **對於 Identity Reporting：** ◆ **Load Balancer Protocol** (負載平衡器通訊協定)：HTTPS ◆ **Load Balancer Port** (負載平衡器連接埠)：8643
Availability Zones (可用性區域)	1. 選取您之前為 Identity Manager 元件建立的同一個 **VPC**。 2. 選取可在其中使用公用子網路的可用性區域。 **附註：**您必須至少選取兩個子網路。
Tags (標記)	(選擇性) 您可以新增一個標記來識別您的負載平衡器。

5 按一下 **Next: Configure Security Settings** (下一步：組態安全性設定)。

6 指定證書詳細資料以使用 HTTPS 通訊協定。您以執行以下操作之一：

- 選取您在 「為負載平衡器建立證書以使用安全通訊」(第 324 頁) 中建立的證書類型。
- 將證書上傳到 IAM 或 ACM - 指定證書詳細資料。

7 按一下 **Next: Configure Security Groups** (下一步：設定安全性群組)。

8 在 **Assign a security group** (指定安全性群組) 中，選取 **Create a new security group** (建立新的安全性群組)。

9 (選擇性) 指定負載平衡器的名稱和描述。

10 新增規則至安全性群組，以便將流量路由到設定的監聽程式：

欄位	描述
Type (類型)	選取 **Custom TCP Rule** (自訂 TCP 規則)。
Protocol (通訊協定)	如此會顯示用於規則的通訊協定類型。
Port Range (連接埠範圍)	選取 Identity Manager 元件的連接埠範圍： ◆ **Identity Applications：**8543 ◆ **Identity Reporting：**8643
Source (來源)	選取 **Anywhere** (任意位置)，以連接至部署了 Identity Manager 元件的例項。

11 按一下 **Next: Configure Routing** (下一步：設定路由)。

12 在 Target group (目標群組) 中指定以下詳細資料：

欄位	描述
Target group (目標群組)	選取 Existing target group (現有目標群組)。此清單顯示在 「建立目標群組」(第 325 頁) 中為 Identity Manager 元件建立的目標群組。
Name (名稱)	從該清單中選取一個目標群組。 在此處只能選取一個目標群組。例如，選取您為 Identity Applications 建立的目標群組。 建立負載平衡器後，您需要修改監聽程式連接埠 8443，以使用針對 HTTPS 通訊協定設定的目標群組。請參閱本節中的步驟 18 (第 328 頁)。
通訊協定	系統將填入您在指定的目標群組中設定的值。請查看列出的值以確定其正確無誤。
Port (連接埠)	系統將填入您在指定的目標群組中設定的值。請查看列出的值以確定其正確無誤。
Target type (目標類型)	系統將填入您在指定的目標群組中設定的值。請查看列出的值以確定其正確無誤。

13 查看 Health Checks (狀態檢查) 下的以下詳細資料：

欄位	描述
Protocol (通訊協定)	系統將依據您在步驟 12 中選取的目標群組組態填入 HTTPS 或 HTTP。 請參閱 「建立目標群組」(第 325 頁)。
Path (路徑)	系統將填入您在步驟 12 中選取的目標群組內設定的狀態 URL。 請參閱 「建立目標群組」(第 325 頁)。
Advanced health check settings (進階狀態檢查設定)	保留預設值。

14 按一下 Next: Register Targets (下一步：註冊目標)。

在所選目標群組中註冊的所有目標都會列出。您只能在建立負載平衡器後修改此清單。

15 按一下 Next: Review (下一步：檢閱)。

16 驗證負載平衡器詳細資料是否正確。

17 依次按一下 Create (建立)、Close (關閉)。

18 (視情況而定) 如果您跳過為 Identity Manager 元件建立監聽程式連接埠的步驟，或者想要新增新的監聽程式連接埠，請更新監聽程式連接埠以使用相應的目標群組：

18a 選取您建立的負載平衡器。

18b 選取 Listeners (監聽程式) 索引標籤。

18c 按一下 **Add Listener** (新增監聽程式)，然後為每個監聽程式指定所需的詳細資料。詳情請參閱步驟 4。

18d 選取用於負載平衡器的證書。詳情請參閱 「為負載平衡器建立證書以使用安全通訊」(第 324 頁)。

18e 按一下 **Create** (建立)。

如果在單獨的機器上設定 SSPR，您可能需要新增一個監聽程式。

重要：若要在分散式設定中使用單個負載平衡器，請單獨建立一條 DNS 別名記錄來區分該設定中的伺服器。否則，請為每個 Web 應用程式單獨建立一個負載平衡器。

(選擇性) 使用註冊的代管區域建立別名 DNS

如果您已註冊了某個網站，可以使用它為每個 Identity Manager 元件建立個別記錄集。

1. 按一下 **Services > Route 53** (服務 > Route 53)。
2. 在左側功能表中按一下 **Hosted Zones** (代管的區域)，然後選取設定 AWS EC2 服務時建立的代管區域。請參閱 「準備 AWS Virtual Private Cloud」(第 317 頁)。
3. 按一下 **Go to Record Sets** (移至記錄集)。
4. 按一下 **Create Record Set** (建立記錄集)：

欄位	描述
Name (名稱)	為記錄集指定有意義的名稱。 例如：將 Identity Applications 記錄集命名為 `rbpm`。
Type (類型)	選取 **A – IPv4 address** (A – IPv4 位址)。
Alias (別名)	選取 **Yes** (是)。
Alias Target (別名目標)	選取設定為連接 Identity Manager 元件的負載平衡器
Routing Policy (路由規則)	選取 **Simple** (簡單)

5. 按一下 **Create** (建立)。
6. 重複步驟 4 和步驟 5，以便為每個 Identity Manager 例項建立一個記錄集。
7. 在 Identity Applications、Identity Reporting 和 OSP 例項上執行 `configupdate.sh`，並使用公用 DNS 名稱更新 SSO 組態。
8. 重新啟動 Tomcat。
9. 透過使用公用 DNS 存取應用程式來驗證組態。

   `https://< 公用 DNS 名稱 >:< 連接埠 >/< 應用程式網路位置名稱 >`

存取 Identity Manager 元件

您可以使用負載平衡器的公用 DNS 名稱或透過別名 DNS 記錄集來存取 Identity Manager 例項。若要使 Identity Manager 例項能夠互相通訊，請編輯每個例項上的 /etc/hosts 檔案，並新增一個項目，以將此例項的主機名稱解析為其私人 IP 位址。

更新以下例項以在內部存取其他例項

例項	描述
OSP	OSP 例項需要存取 SSPR 例項才能重設密碼。 **主機檔案位置：**/etc/hosts 修改 hosts 檔案，在其中包含以下項目： <IP_address> <Private_DNS_Name> <Public_DNS_Name> 例如： 10.0.1.5 sspr.privatedns.local sspr.publicdns.com
Identity Applications	Identity Applications 例項需要存取 OSP 例項才能完成登入。 **主機檔案位置：**/etc/hosts 修改 hosts 檔案，在其中包含以下項目： <IP_address> <Private_DNS_Name> <Public_DNS_Name> 例如： 10.0.1.6 osp.privatedns.local osp.publicdns.com
Identity Reporting	Identity Reporting 例項需要存取 OSP 例項才能完成登入。 **主機檔案位置：**/etc/hosts 修改 hosts 檔案，在其中包含以下項目： <IP_address> <Private_DNS_Name> <Public_DNS_Name> 例如： 10.0.1.6 osp.privatedns.local osp.publicdns.comm

安全性考量

NetIQ 建議您查看有關在 AWS 雲端部署 Identity Manager 元件的以下注意事項：

- 系統會在不提供公用存取權或者已連接至彈性 IP 位址的私人網路中設定 Identity Manager 元件。
- 透過負載平衡器來存取 Identity Applications、Identity Reporting 等 Web 應用程式。
- Identity Manager 元件設定為使用安全通訊通道。
- 系統會在單獨的加密 EBS 磁碟區上設定每個元件的資料。

- Identity Manager 伺服器上的以下連接埠可以在子網路中使用。

連接埠	應用程式
636	LDAP
8543	Identity Applications
8643	Identity Reporting
5432	PostgreSQL

29 範例混合式 Identity Manager 方案

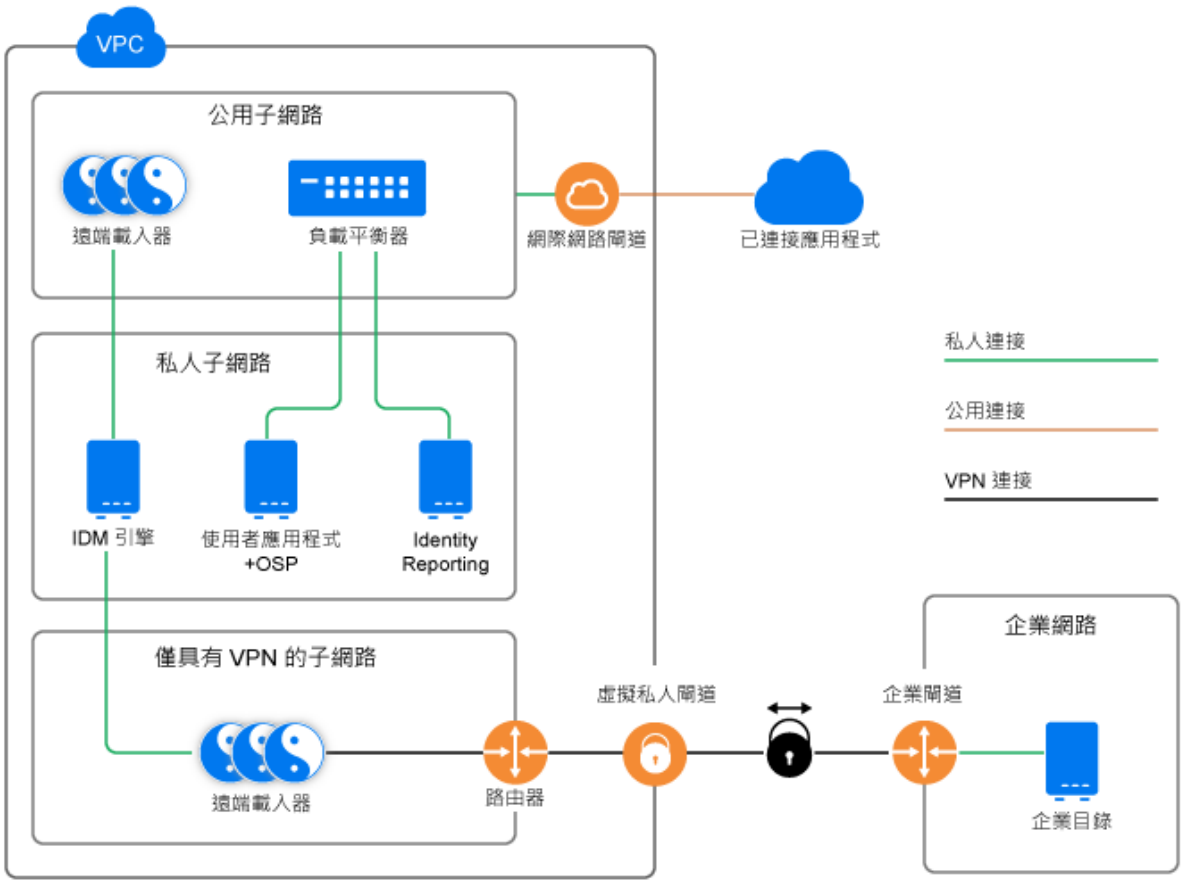
您可以對 Identity Manager 元件進行設定，以使其中的身分在企業本地與 AWS 雲端之間無縫同步。實作此類混合式方案需要您在 AWS 子網路與企業網路之間設定 VPN 連接。本章將會對下面的混合式 Identity Manager 方案進行說明：

- 「使用遠端載入器連接」(第 333 頁)
- 「使用多伺服器驅動程式集連接」(第 334 頁)
- 「使用 eDirectory 驅動程式連接」(第 335 頁)

使用遠端載入器連接

遠端載入器安裝在設定了 VPN 的子網路中。啟用同步後，遠端載入器驅動程式 shim 將連接至企業網路中執行的應用程式，並在 AWS 雲端的 Identity Manager 與應用程式之間同步身分。

圖 29-1 使用遠端載入器連接的混合式方案



此方案適合用於連接的應用程式較少的系統，需要為遠端載入器開啟一個監聽程式連接埠。該連接僅允許在同步期間傳遞設定的屬性。

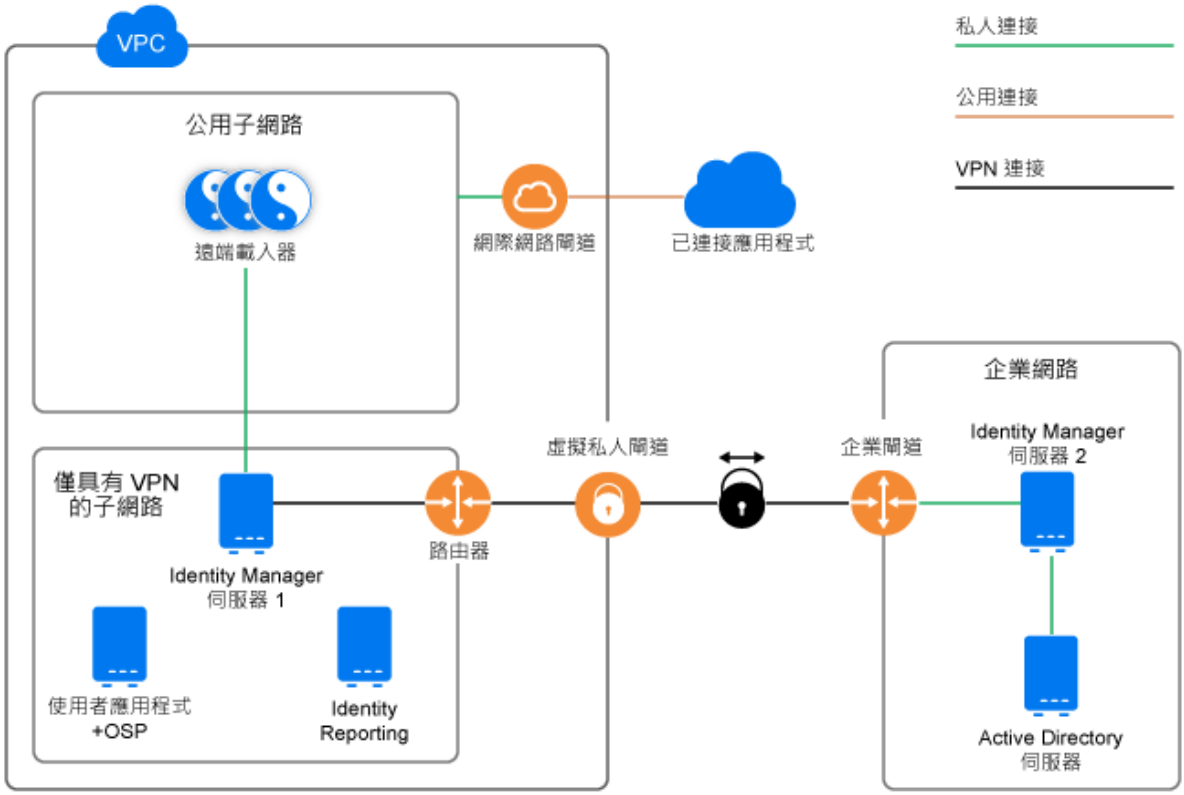
限制：

- 此方案適用於為遠端載入器的使用提供支援的驅動程式。
- 如果有大量連接的應用程式，傳輸至遠端載入器的流量將會增大。

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 AWS 雲端執行的 Identity Manager 伺服器會在各自的已連接應用程式之間同步身分。

圖 29-2 *使用多伺服器驅動程式集連接的混合式方案*

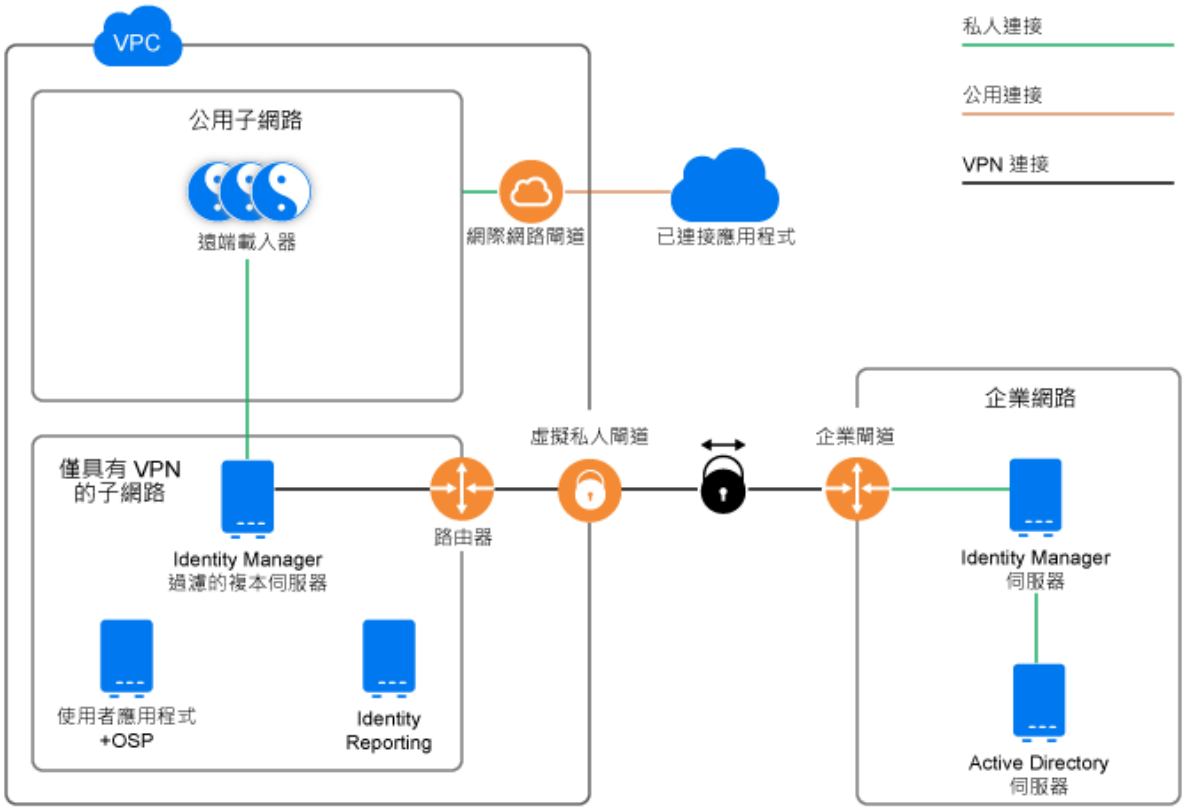


此組態僅將 VPN 連接用於同步任何一端的 Identity Manager 伺服器之間的增量變更。

使用過濾複製

這是多伺服器驅動程式集方案的一種變體，包含 AWS 雲端伺服器上的資料分割區的已過濾讀寫複本。對於驅動程式集分割區，您應永遠使用任何一端的完整複本分割區。

圖 29-3 使用受控複製的混合式方案

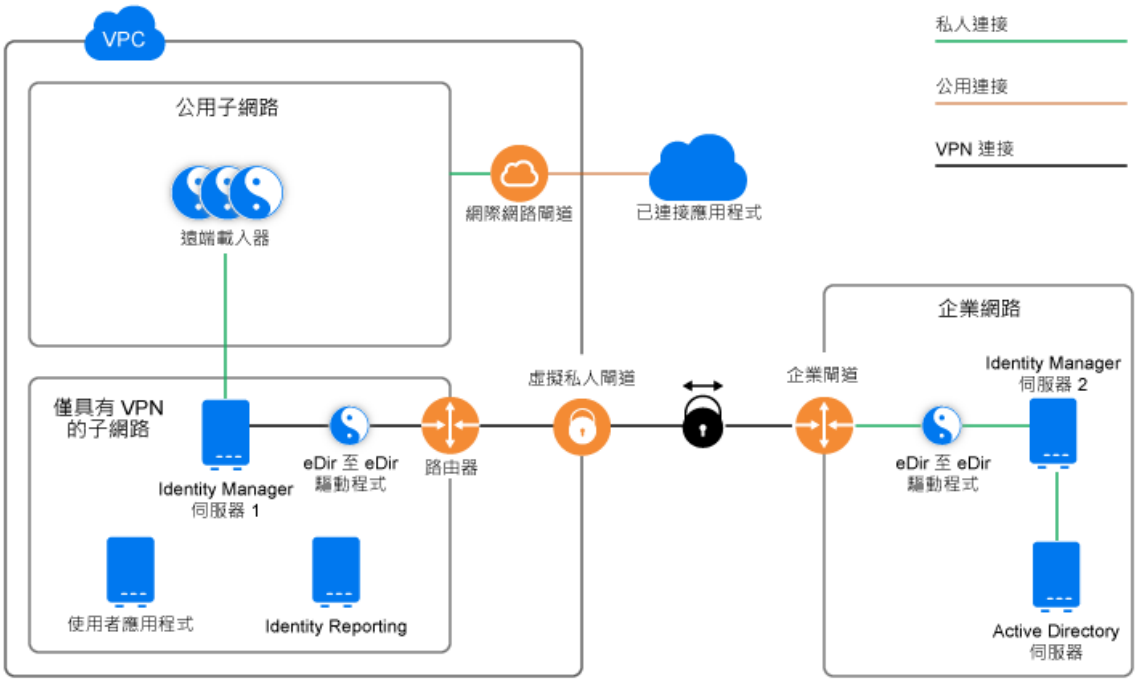


此方案增強了對要同步的屬性的控制能力。例如，您可以防止與 AWS 雲端的 Identity Manager 伺服器同步敏感性屬性。

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 AWS 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 AWS 雲端與企業網路之間同步身分。在企業網路中或 AWS 雲端執行的 Identity Manager 伺服器會在各自的已連接應用程式之間同步身分。

圖 29-4 使用 eDirectory 驅動程式連接的混合式方案



AWS 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 AWS 雲端和企業網路中使用不同的密碼存取 Identity Manager 伺服器。

XI 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
- 若要管理 Identity Manager 環境的網路資源可用性，請將 SUSE Linux Enterprise High Availability Extension 與已安裝最新修補程式的 SUSE Linux Enterprise Server (SLES) 12 SP3 或更新版本配合使用。
- 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	Tomcat 應用程式伺服器上的 Identity Applications 叢集部署解決方案範例

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 30 章 「在叢集環境中安裝 Identity Manager 的準備工作」 (第 339 頁)
- 第 31 章 「Identity Manager 叢集部署解決方案範例」 (第 343 頁)
- 第 32 章 「Tomcat 應用程式伺服器上的 Identity Applications 叢集部署解決方案範例」 (第 353 頁)

30 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」(第 339 頁)
- 「Identity Applications」(第 340 頁)
- 「Identity Applications 的資料庫」(第 340 頁)

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 NICI 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 NICI (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 NICI 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 341 頁)
- 「設定工作流程引擎 ID 的系統內容」(第 341 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。
3. Identity Vault 和 Identity Manager 引擎中包含 Identity Applications 和 Identity Reporting。

31 Identity Manager 叢集部署解決方案範例

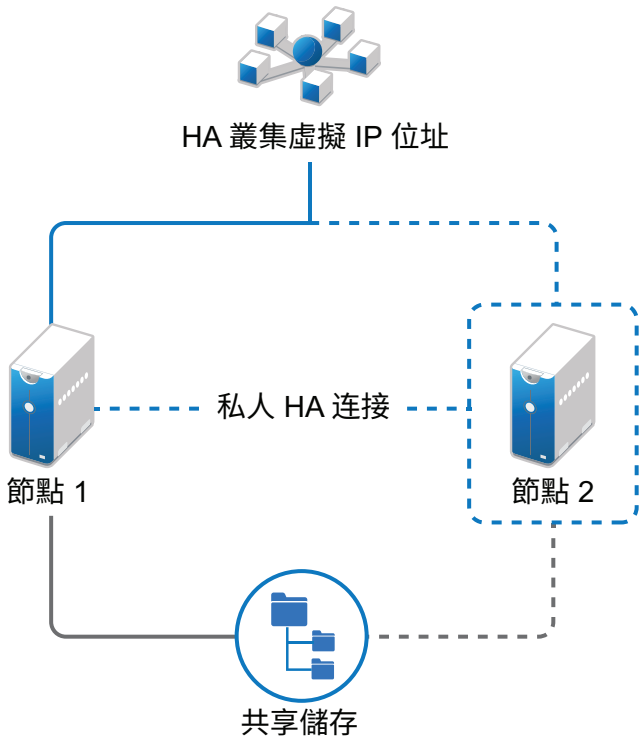
本章透過逐步說明介紹如何在使用共用儲存的受支援 SUSE Linux Enterprise Server (SLES) 叢集環境中設定 eDirectory 和 Identity Manager，並提供了一個 Identity Manager 叢集部署範例。

- 「先決條件」(第 343 頁)
- 「安裝程序」(第 344 頁)

對於使用共享儲存的線上層級 Linux 高可用性 (HA) 解決方案，建議在叢集中執行圍籬區隔機制。雖然在叢集中執行圍籬區隔機制的方法有多種，但在此範例中，我們會使用一個利用電腦分裂偵測器 (SBD) 的 STONITH 資源。

圖 31-1(第 343 頁) 顯示了一個叢集部署解決方案範例。

圖 31-1 *叢集部署解決方案範例*



先決條件

- 兩部執行 SLES 12 SP3 64 位元的伺服器做為節點
- 一個執行 SLES 12 SP3 64 位元的伺服器，做為 iSCSI 伺服器
- SLES12 SP3 64 位元 HA Extension ISO 影像檔

- 六個靜態 IP：
  - 每個節點有兩個靜態 IP 位址。
  - 一個靜態 IP 位址用於叢集。此 IP 位址將會動態指定給目前執行 eDirectory 的節點。
  - 一個靜態 IP 位址用於 iSCSI 伺服器。

安裝程序

本節說明在叢集環境中安裝 Identity Manager 的步驟。如需設定 SLES High Availability Extension 的詳細資訊，請參閱《SUSE Linux Enterprise High Availability Extension 指南》。

- 設定 iSCSI 伺服器
- 在所有節點上設定 iSCSI 啟動器
- 分割共享儲存
- 安裝 HA Extension
- 設定 Softdog 監視程式
- 設定 HA 叢集
- 在叢集節點上安裝並設定 Identity Vault 和 Identity Manager 引擎
- 設定 Identity Vault 資源
- eDirectory 和共享儲存子資源的原始值
- 變更位置條件約束分數

設定 iSCSI 伺服器

iSCSI 目標是指設定為叢集中所有節點的通用儲存的裝置。它是 Linux 伺服器上建立的虛擬磁碟，可使 iSCSI 啟動器能夠透過乙太網路連接進行遠端存取。iSCSI 啟動器是指叢集中設定用於聯絡服務目標 (iSCSI) 的任一節點。iSCSI 目標應該永遠處於正常運作狀態，如此，任何充當啟動器的主機才能聯絡目標。在 iSCSI 伺服器上安裝 iSCSI 目標之前，請確保 iSCSI 目標上有足夠的空間用於通用儲存。安裝 SLES 12 SP3 後，請在其餘兩個節點上安裝 iSCSI 啟動器套件。

在安裝 SLES 12 SP3 期間：

1. 建立一個獨立的分割區，並將分割區路徑指定為 iSCSI 共享儲存分割區。
2. 安裝 iSCSI 目標套件。

若要設定 iSCSI 伺服器：

1. 在目標伺服器上建立一個區塊裝置。
2. 在終端機中輸入 `yast2 disk` 指令。
3. 建立一個新的 Linux 分割區，並選取不格式化。
4. 選取不掛接分割區。
5. 指定分割區大小。
6. 在終端機中輸入 `yast2 iscsi-server` 或 `yast2 iscsi-lio-server` 指令。

7 按一下**服務**索引標籤，然後在**服務啟動**選項中選取**開機時**。

8 在**目標**索引標籤中，按一下**新增**，以輸入分割區路徑 (在安裝 SLES 期間建立的路徑)。

9 在**修改 iSCSI 目標啟始者設定**頁面中，指定目標伺服器的 iSCSI 用戶端啟始者主機名稱，然後按**下一步**。

例如，*iqn.sles12sp3node3.com* 和 *iqn.sles12sp2node3.com*。

10 按一下**完成**。

11 在終端機中執行 `cat /proc/net/iet/volume` 指令，以驗證是否已安裝 iSCSI 目標。

在所有節點上設定 iSCSI 啟動器

為了連接到 iSCSI 目標，您必須在所有叢集節點上設定 iSCSI 啟動器。

若要設定 iSCSI 啟動器：

1 安裝 iSCSI 啟動器套件。

2 在終端機中執行 `yast2 iscsi-client`。

3 按一下**服務**索引標籤，然後在**服務啟動**選項中選取**開機時**。

4 按一下**已連接目標**索引標籤，然後按一下**新增**，以輸入 iSCSI 目標伺服器的 IP 位址。

5 選取**無驗證**。

6 按**下一步**，然後按一下**連接**。

7 按一下**切換啟動方式**，將啟動選項從手動變更為自動，然後按**下一步**。

8 按一下**「下一步」**，然後按一下**「確定」**。

9 若要檢查目標伺服器上連接的啟動器的狀態，請在目標伺服器上執行 `cat /proc/net/iet/session` 指令。已連接到 iSCSI 伺服器的啟動器清單即會顯示。

分割共享儲存

建立兩個共享儲存分割區：一個用於 SBD，另一個用於叢集檔案系統。

若要分割共享儲存：

1 在終端機中執行 `yast2 disk` 指令。

2 在**進階磁碟分割程式**對話方塊中選取共享磁碟區。在本範例中，請從**進階磁碟分割程式**對話方塊中選取 **sdb**。

3 按一下**新增**，選取**主分割區**選項，然後按**下一步**。

4 選取**自訂大小**，然後按**下一步**。在此範例中，自訂大小為 100 MB。

5 在**格式化選項**下，選取**不格式化分割區**。在此範例中，檔案系統 ID 為 0x83 Linux。

6 在**掛接選項**下，選取**不掛接分割區**，然後按一下**完成**。

7 按一下**新增**，然後選取**主分割區**。

8 按**下一步**，選取**最大大小**，然後按**下一步**。

9 在格式化選項中，選取不格式化分割區。在此範例中，我們指定 0x83 Linux 做為檔案系統 ID。

10 在掛接選項中，選取不掛接分割區，然後按一下完成。

安裝 HA Extension

若要安裝 HA Extension：

1 造訪 SUSE 下載網站。

對於每個可用平台，SUSE Linux Enterprise High Availability Extension (SLE HA) 提供了兩個 ISO 影像供您下載。媒體 1 包含二進位套件，媒體 2 包含原始程式碼。

附註：根據您的系統架構選取並安裝相應的 HA Extension ISO 檔案。

---

2 將媒體 1 ISO 檔案下載到每部伺服器上。

3 開啟 **YaST 控制中心**對話方塊，然後按一下**附加產品 > 新增**。

4 按一下**瀏覽**並選取 DVD 或本地 ISO 影像，然後按**下一步**。

5 在**模式**索引標籤中的**主要功能**下，選取**高可用性**。

確定已安裝高可用性下的所有元件。

6 按一下「接受」。

設定 Softdog 監視程式

在 SLES HA Extension 中，核心中的監視程式支援預設處於啟用狀態。該產品隨附了多個不同的核心模組，用於提供硬體特定的監視程式驅動程式。系統開機時會自動載入適當的硬體監視程式驅動程式。

1 啟用 softdog 監視程式：

```
echo softdog > /etc/modules-load.d/watchdog.conf
systemctl restart systemd-modules-load
```

2 測試 softdog 模組是否已正確載入：

```
lsmod | grep dog
```

設定 HA 叢集

此範例假設您要在叢集中設定兩個節點。

設定第一個節點：

1 以 root 身分登入要做為叢集節點的實體或虛擬機器。

2 執行以下指令：

```
ha-cluster-init
```

該指令會檢查是否存在 NTP 組態與硬體監視程式服務。這會產生 SSH 存取與 Csync2 同步所需的公用和私密 SSH 金鑰，並啟動相應的服務。

3 設定叢集通訊層：

3a 輸入要繫結到的網路位址。

3b 輸入多路廣播位址。程序檔會建議一個隨機位址，您可將其做為預設值。

3c 輸入多路廣播連接埠。預設埠號碼為 5405。

4 將 SBD 設定為節點圍籬區隔機制：

4a 按 *y* 以使用 SBD。

4b 輸入要為 SBD 使用的區塊裝置分割區的永久路徑。該路徑對於叢集中的兩個節點必須一致。

5 設定用於叢集管理的虛擬 IP 位址：

5a 按 *y* 以設定虛擬 IP 位址。

5b 輸入一個未使用的 IP 位址，做為 SUSE Hawk 圖形使用者介面的管理 IP。例如，*192.168.1.3*。

您可以連接至該虛擬 IP 位址，而無需登入個別叢集節點。

第一個節點啟動並執行後，使用 `ha-cluster-join` 指令新增第二個叢集節點。

設定第二個節點：

1 以 root 身分登入要用於連接叢集的實體機器或虛擬機器。

2 執行以下指令：

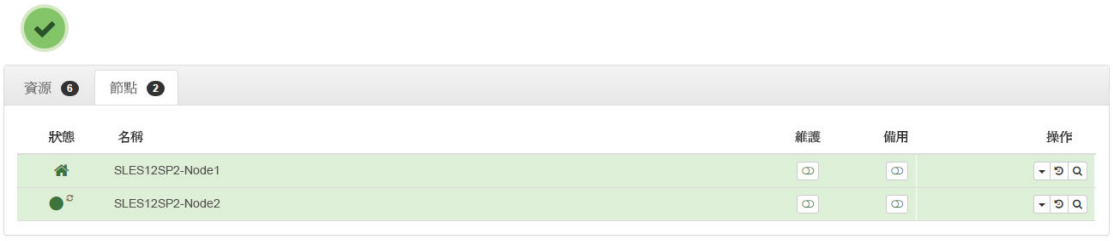
```
ha-cluster-join
```

如果未設定 NTP，則會顯示一則訊息。該指令會檢查是否存在硬體監視程式裝置，如果不存在，將發出通知。

3 輸入第一個節點的 IP 位址。

4 輸入第一個節點的 root 密碼。

5 登入 SUSE Hawk 圖形使用者介面，然後按一下**狀態** > **節點**。例如，`https://192.168.1.3:7630/cib/live`。



在叢集節點上安裝並設定 Identity Vault 和 Identity Manager 引擎

1 在叢集節點上安裝 Identity Manager 引擎：

1a 從 NetIQ 下載網站下載 `Identity_Manager_4.9.0_Linux.iso`。

1b 掛接下載的 `.iso`。

1c 在 ISO 掛接位置執行以下指令：

```
./install.sh
```

1d 通讀授權合約。

1e 輸入 `y` 以接受授權合約。

1f 決定要安裝的 Identity Manager 伺服器版本。輸入 `y` 將安裝進階版，輸入 `n` 將安裝標準版。

1g 從清單中選取 **Identity Manager 引擎**並繼續安裝。

此步驟將安裝支援的 Identity Vault 版本。

2 在所有節點上設定 Identity Manager 引擎。

2a 導覽至掛接 `Identity_Manager_4.9.0_Linux.iso` 的位置。

2b 在 ISO 掛接位置執行以下指令：

```
./configure.sh
```

2c 決定是要執行一般組態還是自訂組態。組態選項將因您選取要設定的元件而異。

2d 從清單中選取 **Identity Manager 引擎**元件。

2e 如果您是第一次設定 Identity Vault，請選取**建立新 Identity Vault** 選項。如果您之前已安裝 Identity Vault 並想要連接到該 Identity Vault 例項，請選取**新增至本地機器上的現有 Identity Vault** 或**新增至本地機器上的現有 Identity Vault** 選項。

3 導覽至 `/etc/opt/novell/eDirectory/conf` 目錄。

4 編輯 `nds.conf` 檔案，並在 `n4u.nds.preferred-server` 欄位中指定叢集的虛擬 IP 位址。

5 停止 Identity Vault 服務。

```
ndsmanage stopall
```

6 備份 `/var/opt/novell/nici`、`/etc/opt/novell/eDirectory/conf` 和 `/var/opt/novell/eDirectory/` 目錄中的所有資料夾與檔案。

7 導覽至 `/opt/novell/eDirectory/bin` 目錄。

8 執行以下指令：

```
nds-cluster-config -s /<shared cluster path>
```

其中，`<shared cluster path>` 表示您要用於 Identity Vault 共用叢集資料的位置。

9 啟動 Identity Vault 服務。

```
ndsmanage startall
```

如需在叢集設定中設定 Identity Vault 的詳細資訊，請參閱《eDirectory Installation Guide》(eDirectory 安裝指南) 中的「Deploying eDirectory on High Availability Clusters」(在高可用性叢集上部署 eDirectory)。

設定 Identity Vault 資源

1 登入 SUSE Hawk 圖形使用者介面。

2 按一下**新增資源**，然後建立新群組。

2a 按一下**群組**旁邊的 ⊕。

2b 指定群組 ID。例如，*群組 1*。

建立群組時，確定選取了以下子資源：

- *stonith-sbd*
- *admin_addr (叢集 IP 位址)*

3 在**中繼資料屬性**索引標籤中，將 **target-role** 欄位設定為 *Started*，並將 **is-managed** 欄位設定為 *Yes*。

4 按一下「**建立**」。

5 按一下**編輯組態**，然後按一下在步驟 2 中建立的群組旁邊的 ✎。

6 在**子項**欄位中，新增以下子資源：

- *shared-storage*
- *eDirectory-resource*

例如，在該群組中，應該依以下順序新增資源：

- *stonith-sbd*
- *admin_addr (叢集 IP 位址)*
- *shared-storage*
- *eDirectory-resource*

您可以視需要變更資源名稱。每個資源都有一組參數需要定義。如需 shared-storage 和 eDirectory 資源範例的資訊，請參閱 eDirectory 和共享儲存子資源的原始值。

eDirectory 和共享儲存子資源的原始值

依預設，系統會在啟始化叢集節點時透過高可用性叢集指令設定 *stonith-sbd* 和 admin_addr 資源。

表格 31-1 shared-storage 的範例

資源 ID	共享儲存資源的名稱
Class	ocf
Provider	heartbeat
Type	Filesystem
device	/dev/sdc1
directory	/shared
fstype	xfs
operations	◆ start (60, 0) ◆ stop (60, 0) ◆ monitor (40, 20)
is-managed	Yes
resource-stickiness	100
target-role	Started

表格 31-2 eDirectory-resource 的範例

資源 ID	eDirectory 資源的名稱
Class	systemd
Type	ndsdtmpl-shared-conf-nds.conf@-shared-conf-env
operations	◆ start (100, 0) ◆ stop (100, 0) ◆ monitor (100, 60)
target-role	Started
is-managed	Yes
resource-stickiness	100
failure-timeout	125
migration-threshold	0

變更位置條件約束分數

將位置條件約束分數變更為 0。

1. 登入 SUSE Hawk 圖形使用者介面。
2. 按一下**編輯組態**。
3. 在條件約束索引標籤中，按一下叢集節點 1 旁邊的 。

4 在**簡單**索引標籤中，將分數設定為 *0*。

5 按一下**套用**。

務必將叢集中所有節點的分數設定為 *0*。

附註：當從 SUSE Hawk 圖形使用者介面中使用**狀態** > **資源** > **移轉**選項，將資源從一個節點移轉至另一個節點時，位置條件約束分數將變更為 *Infinity* 或 *-Infintity*。如此僅會將優先設定提供給叢集中的一個節點，並且將導致 eDirectory 操作延遲。

---

32 Tomcat 應用程式伺服器上的 Identity Applications 叢集部署解決方案範例

本章透過範例部署來說明如何在 Tomcat 上的叢集環境中設定 Identity Applications。

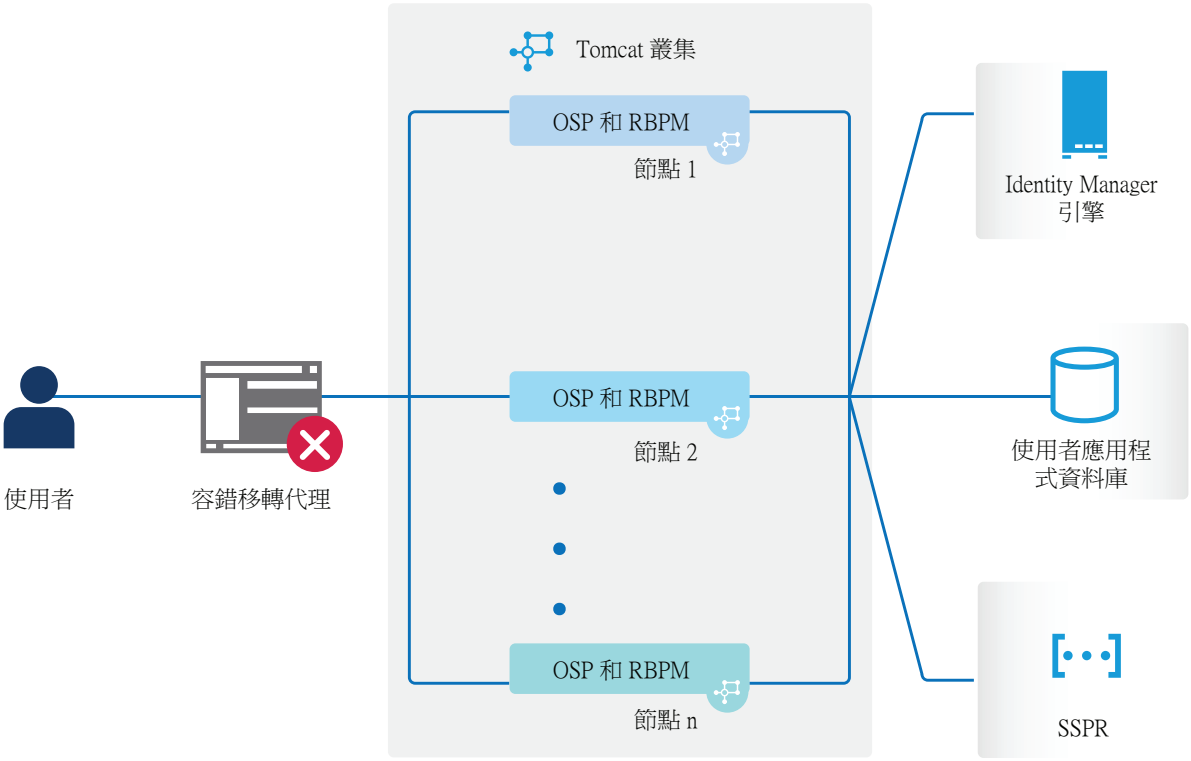
使用叢集，您可以在多部平行伺服器 (叢集節點) 上執行 Identity Applications，從而實現高可用性。若要建立叢集，需要將若干個 Tomcat 例項 (節點) 組合在一起。負載將分散在不同的伺服器之間，即使有任何伺服器發生故障，您仍可透過其他叢集節點來存取 Identity Applications。若要實現容錯移轉，您可以建立一個 Identity Applications 叢集，然後將這些 Identity Applications 設定為充當單部伺服器。不過，此組態不包括 Identity Reporting。

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 32-1 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使用此方法。
- 您熟悉 eDirectory、Identity Manager 引擎、Identity Applications、Tomcat 應用程式伺服器和使用者應用程式資料庫的安裝程序。
- 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，您可以使用支援的任何資料庫，例如 Oracle 或 MsSQL。
- 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 32-1 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

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。
- 叢集中的伺服器之間已同步時鐘時間。否則，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。
- 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。

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 355 頁)
- 「設定工作流程引擎 ID 的系統內容」(第 355 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。

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。

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。

---

1. 安裝 Identity Manager 引擎。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 安裝資料庫。可以使用隨 Identity Applications 一併安裝的 PostgreSQL 資料庫。不過，建議將資料庫安裝在單獨的伺服器上。
3. 在節點 1 上，安裝並設定 Identity Applications。

   在組態期間，請確定：

   - 選取新資料庫選項
   - 提供唯一的工作流程引擎 ID。例如，節點 `1`。
   - 叢集中的所有使用者應用程式節點上均有可用的資料庫 jar 檔案。對於 PostgreSQL，`postgresql-42.6.1.jar` 位於 `/opt/netiq/idm/postgres`。

   Identity Applications 使用萬能金鑰來加密敏感性資料。在 Identity Applications 組態期間，安裝程式將建立新的萬能金鑰。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。萬能金鑰儲存在 `/opt/netiq/idm/apps/tomcat/conf/` 目錄中 `ism-configuration.properties` 檔案內的內容 `com.novell.idm.masterkey` 下。
4. 在節點 2 上，安裝並設定 Identity Applications。

   在組態期間，請確定：

   - 選取現有資料庫選項
   - 提供唯一的工作流程引擎 ID。例如，節點 `2`。
   - 叢集中的所有使用者應用程式節點上均有可用的資料庫 jar 檔案。對於 PostgreSQL，`postgresql-9.4.1212.jar` 位於 `/opt/netiq/idm/postgres`。

   完成節點 2 上的使用者應用程式組態後，複製節點 1 的 `ism-configuration.properties` 中的萬能金鑰值，並取代節點 2 的 `ism-configuration.properties` 中儲存的相應萬能金鑰值。萬能金鑰儲存在 `ism-configuration.properties` (`/opt/netiq/idm/apps/tomcat/conf/`) 中的內容 `com.novell.idm.masterkey` 下。
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。

   完成 SSPR 安裝後，啟動 SSPR (`https://<IP>:<` 連接埠 `>/sspr/private/config/editor`) 並登入其中。按一下**組態編輯器** > **設定** > **安全性** > **Web 安全性** > **重新導向白名單**。

   a. 按一下**新增值**並指定以下 URL：

      `https://<` 容錯移轉的 `DNS>/osp`

   b. 儲存變更。

   c. 在 SSPR 組態頁面中，按一下**設定** > **單一登入 (SSO) 用戶端** > **OAuth**，然後修改 **OAuth 登入 URL**、**OAuth 代碼解析服務 URL** 和 **OAuth 設定檔服務 URL** 連結，具體方法是以安裝了負載平衡器軟體的伺服器的 DNS 名稱取代 IP 位址。

d. 按一下**設定** > **應用程式** > **應用程式**，然後更新**轉遞 URL** 和**登出 URL**，具體方法是以安裝了負載平衡器軟體的伺服器的 DNS 名稱取代 IP 位址。透過提供安裝了 SSPR 的伺服器 / 系統的 IP 位址或主機名稱來更新**網站 URL**。

e. 若要在節點 1 上更新 SSPR 資訊，請啟動位於 `/opt/netiq/idm/apps/configupdate/` 中的組態公用程式。

```
./configupdate.sh
```

附註：您應只從 configupdate 目錄執行 `configudate.sh` 檔案。從自訂位置執行 `configupdate.sh` 將導致失敗。

f. 按一下 **SSO 用戶端** > **Self Service Password Reset**，輸入**用戶端 ID**、**密碼**和 **OSP Auth 重新導向 URL** 參數的值。如需詳細資訊，請參閱 「Self Service Password Reset」(第 120 頁)。

附註：驗證節點 2 中是否更新了這些參數的值。

7. 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：

```
/opt/netiq/common/jre/bin/keytool -genkey -storetype PKCS12 -keyalg RSA -keysize 2048 -keystore osp.jks -storepass < 密碼 > -keypass < 密碼 > -alias osp -validity 1800 -dname "cn=< 負載平衡器 IP/DNS>"
```

例如：`/opt/netiq/common/jre/bin/keytool -genkey -storetype PKCS12 -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。

8. (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：

```
/opt/netiq/common/jre/bin/keytool -list -v -keystore osp.jks -storepass changeit
```

9. 備份位於 `/opt/netiq/idm/apps/osp/` 中的原始 `osp.jks` 檔案，並將新 `osp.jks` 檔案複製到此位置。
10. 將節點 1 上位於 `/opt/netiq/idm/apps/osp/` 中的新 `osp.jks` 文件複製到叢集中的其他使用者應用程式節點上。
11. 在每個叢集節點上：

a. 導覽至 `/opt/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。

```
{"serviceRegisteries":[{"serviceID":"IDM","restUrl":"https://<DNS of the load balancer>:8543/IDMProv"}]}
```

b. 導覽至 /opt/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
```

12. 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 /TOMCAT_INSTALLED_HOME/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-configuration.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。
    - 將 ism-configuration.properties 檔案從一個節點複製到另一個節點後，請確定對該檔案具有 novlua:novlua 許可權。
    - 此情境中，OSP 和使用者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 和使用者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。

13. 指定對 osp.jks 檔案的 novlua 許可權：

    ```
    chown novlua:novlua osp.jks
    ```

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，您可以新增引擎名稱 *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。如果您要變更此通訊協定以使用 TCP，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 User Application Caching to use TCP (https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/b6iiw3v.html)」(將使用者應用程式快取設定為使用 TCP)。

---

16. 為叢集啟用許可權索引。

a. 在 IDVault 中登入 Identity Console，然後導覽至**樹狀檢視**。

b. 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**。

c. 然後選取 **AppConfig** > **AppDefs**。

d. 在右側窗格中選取**組態**。

e. 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>
```

f. 按一下「**儲存**」。

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 https://tomcat.apache.org/tomcat-8.5-doc/cluster-howto.html 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。

在叢集中，必須將使用者應用程式驅動程式設定為使用叢集負載平衡器的 DNS 名稱。可以使用 Identity Console 來設定使用者應用程式驅動程式。

a. 登入用於管理 Identity Manager 引擎的 Identity Console。

b. 按一下 **Identity Manager 管理**。

c. 選取包含您的使用者應用程式驅動程式、角色與資源服務驅動程式，以及資料收集服務驅動程式的驅動程式集。

d. 按一下**使用者應用程式驅動程式**圖示。

e. 移至**組態**索引標籤。

f. 在**驅動程式參數**下拉式清單中，將**主機**變更為負載平衡器的主機名稱或 IP 位址。

g. 按一下「**儲存**」。

h. 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 19e，然後按一下**驅動程式參數**下拉式清單，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。

22. 在 Identity Manager 儀表板上設定用戶端設定。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「Configuring Client Settings Mode」(設定用戶端設定模式)。

為叢集啟用許可權索引

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**」。

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。

1 登入用於管理 Identity Vault 的 Identity Console 例項。

2 按一下 **Identity Manager 管理**。

3 選取包含您的使用者應用程式驅動程式的驅動程式集。

4 按一下使用者應用程式驅動程式圖示。

5 移至組態索引標籤。

6 在驅動程式參數下拉式清單中，將主機變更為發送器的主機名稱或 IP 位址。

7 按一下「儲存」。

8 重新啟動驅動程式。

為叢集設定 OSP 和 SSPR

Identity Manager 支援 Tomcat 叢集環境中的 SSPR 組態。

設定 SSPR 以支援叢集

若要在叢集的第一個節點中更新 SSPR 資訊，請啟動 `/opt/netiq/idm/apps/configupdate/configupdate.sh` 中的組態公用程式。

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。

在叢集節點上設定任務

在叢集節點上執行以下組態任務：

1 若要以 SSPR IP 位址更新 「忘記密碼」連結，請在第一個節點上登入使用者應用程式，然後按一下管理 > 忘記密碼。

如需 SSPR 組態的詳細資訊，請參閱 「設定忘記密碼管理功能」(第 94 頁)。

2 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 98 頁)。

3 在叢集中的其他節點上，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。

---

4 在第一個節點中，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：

```
/opt/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：`/opt/netiq/common/jre/bin/keytool -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。

---

5 (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：

```
/opt/netiq/common/jre/bin/keytool -list -v -keystore osp.jks -storepass changeit
```

6 備份位於 /opt/netiq/idm/apps/osp 中的原始 osp.jks 檔案，並將新 osp.jks 檔案複製到此位置。新 osp.jks 檔案是在步驟 4 中建立的。

7 將第一個節點上位於 /opt/netiq/idm/apps/osp 中的新 osp.jks 檔案複製到叢集中的所有其他使用者應用程式節點上。

8 在第一個節點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。

8a 儲存在組態公用程式中所做的變更。

8b 若要在叢集的所有其他節點中反映此變更，請將第一個節點上位於 /TOMCAT_INSTALLED_HOME/conf 中的 ism-configuration.properties 檔案複製到所有其他使用者應用程式節點。

附註：您之前已將第一個節點上的 ism.properties 檔案複製到叢集中的其他節點。如果您在安裝使用者應用程式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 和使用者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 與使用者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。這可確保所有 OSP 申請均透過負載平衡器傳發送到 OSP 叢集 DNS 名稱。這涉及到為 OSP 節點建立一個單獨的叢集。

---

9 在 /TOMCAT_INSTALLED_HOME/bin/ 目錄下的 setenv.sh 檔案中執行以下動作：

9a 為確保成功進行 mcast_addr 繫結，JGroups 要求 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」。

9b 在第一個節點上的 setenv.sh 檔案中新增 「-Dcom.novell.afw.wf.engine-id=*Engine*」。

引擎名稱應該是唯一的。請提供安裝第一個節點時指定的名稱。如果之前未指定名稱，則預設名稱為 「Engine」。

同樣，為叢集中的其他節點新增唯一的引擎名稱。例如，對於第二個節點，引擎名稱可以是 Engine2。

33 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：在開始解除安裝 Identity Manager 元件之前，請務必執行以下動作：

- 停止 Tomcat、PostgreSQL 和 ActiveMQ 服務。
- 備份 `/var/opt/netiq/idm/log/` 目錄中的安裝記錄檔案。

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. 瀏覽並選取做為分割區根物件的驅動程式集物件，然後按一下 。
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

安裝程式提供了 Identity Manager 的解除安裝程序檔。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 363 頁）。

若要解除安裝 Identity Manager 引擎：

1. 導覽至安裝時掛接 iso 的位置。
2. 從 `.iso` 檔案的根目錄中，執行以下指令：

   ```
   ./uninstall.sh
   ```
3. 指定 **Identity Manager 引擎**的值。
4. 如果您要將 Identity Vault 隨 Identity Manager 引擎一併解除安裝，請對**是否要取消設定並解除安裝 IDVault** 參數指定 **y**，並指定以下詳細資料：
   - **Identity Vault 網路樹名稱：**指定 Identity Vault 樹狀結構名稱。
   - **Identity Vault 管理員名稱：**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。

解除安裝 Identity Applications

1. 導覽至安裝時掛接 `.iso` 的位置。
2. 從 `.iso` 檔案的根目錄中，執行以下指令：

   ```
   ./uninstall.sh
   ```
3. 指定 **Identity Applications** 的值。

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 365 頁）。
2. 刪除 Identity Reporting。如需詳細資訊，請參閱「解除安裝 Identity Reporting」（第 365 頁）。
3. 刪除 Sentinel。如需詳細資訊，請參閱「解除安裝 Sentinel Log Management for IGA」（第 365 頁）。

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 365 頁)。

1 導覽至安裝時掛接 `.iso` 的位置。
2 從 `.iso` 檔案的根目錄中，執行以下指令：

   ```
   ./uninstall.sh
   ```
3 指定 **Identity Reporting** 的值。

解除安裝 Sentinel Log Management for IGA

1 登入 Sentinel 伺服器。
2 導覽至包含解除安裝程序檔的目錄：

   ```
   /opt/novell/sentinel/setup/
   ```
3 執行下列指令：

   ```
   ./uninstall.sh
   ```
4 當系統提示您重新確認要繼續解除安裝時，請按 `y`。

   程序檔會先停止服務，然後再將服務完全移除。

解除安裝 Designer

1 關閉 Designer。
2 解除安裝 Designer

導覽至包含解除安裝程序檔的目錄 (預設為 < *安裝目錄* >/designer/UninstallDesigner/Uninstall Designer for Identity Manager)。

若要執行該程序檔，請輸入 ./uninstall

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. 根據作業系統解除安裝 Analyzer：

   導覽至預設位於 < 安裝目錄 >/analyzer/UninstallAnalyzer *目錄中的* Uninstall Analyzer for Identity Manager 程序檔。

   若要執行該程序檔，請輸入 ./ 解除安裝

34 疑難排解

本章提供有關對 Identity Manager 安裝和升級問題進行疑難排解的實用資訊。如需其他疑難排解秘訣，請參閱特定元件的指南。

尋找記錄檔案

Identity Manager 將維護記錄以協助使用者對任何問題進行除錯。記錄檔案位於以下位置：

- 所有 Identity Manager 元件的安裝記錄檔案：`/var/opt/netiq/idm/log/idminstall.log`
- 所有 Identity Manager 元件的組態記錄檔案：`/var/opt/netiq/idm/log/idmconfigure.log`
- 使用者應用程式：`/opt/netiq/idm/apps/tomcat/logs/catalina.out` 和 `/opt/netiq/idm/apps/tomcat/logs/idapps.out`
- Identity Reporting：`/opt/netiq/idm/apps/tomcat/logs/localhost.<` 日期 `>.log`
- DCS：`/opt/netiq/idm/apps/tomcat/logs/catalina.out`
- eDirectory：`/var/opt/novell/eDirectory/log/ndsd.log`
- Tomcat：`/opt/netiq/idm/apps/tomcat/logs/catalina.out`
- OSP：`/opt/netiq/idm/apps/tomcat/logs/osp-idm.log`
- SSPR：`/opt/netiq/idm/apps/tomcat/logs/catalina.out`
- Sentinel Log Management for IGA：`/var/opt/novell/sentinel/log/server0.0log`
- 表單轉譯器：`opt/netiq/common/nginix/logs`

登入相關問題疑難排解

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
啟動 Designer 時顯示以下錯誤，並且 Designer 讀我檔案不顯示： 例外 . . . 「更新資訊清單中缺少必需的 addons 內容。」	忽略該錯誤並啟動 Designer。不會出現功能缺失。
在大型環境 (超過兩百萬個物件) 中，使用者無法登入	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`。

問題	建議執行的動作
當您從 Identity Applications 頁面登出時，SSPR 顯示錯誤 `5053 ERROR_APP_UNAVALIABLE`。	忽略此錯誤，它不會導致功能受損。
在第一次登入 Identity Applications 時不提示處理安全回應	1. 確定 SSPR 服務器具有使用 FQDN 建立的證書。 2. 登入使用者應用程式伺服器，並啟動 ConfigUpdate (`/opt/netiq/idm/apps/configupdate/`) 公用程式。 3. 導覽至 **SSO 用戶端 > Self Service Password Reset**，並確定設定正確。 如果 SSPR 安裝在其他伺服器上，請確定 SSPR 證書已輸入到使用者應用程式伺服器上 `/opt/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： `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]))`  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。登入使用者應用程式伺服器，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，`https://<sspr sserver ip>:<port>/sspr/private/Login?sso=false`)。 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**。
從不同的目錄啟動 ConfigUpdate 公用程式時發生錯誤	ConfigUpdate 公用程式會報告錯誤。它將不儲存任何變更。例如，如果您使用 `/opt/netiq/idm/apps/configupdate/configupdate.sh` 指令啟動 configupdate 公用程式，它不會啟動。 您應導覽至 `/opt/netiq/idm/apps/configupdate/` 目錄，然後執行 `./configupdate.sh` 指令。

問題	建議執行的動作

以管理員身分登入分散式設定中部署的 SSPR 容器時，無法跳過系統提出的安全性問題。	在 ssprconfiguration.xml 中，確定移除以下行中 objectclass 周圍的任何多餘空格：
	
	`<setting key="pwmAdmin.queryMatch" syntax="USER_PERMISSION" syntaxVersion="2">`
	
	`<label>Administrator Permission</label>`
	
	`<value>{"ldapProfileID":"default","ldapQuery":"(objectClass=*)","ldapBase":"cn=admin,ou=sa,o=system"}</value>`
	
	`<value>{"ldapProfileID":"default","ldapQuery":"(objectClass=*)","ldapBase":"cn=uaadmin,ou=sa,o=data"}</value>`
	
	`</setting>`

安裝和解除安裝相關問題疑難排解

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
如果在 Open Enterprise Server (OES) 24.2 上安裝 Identity Manager 4.9，會導致無法滿足相依關係錯誤 (未安裝 glibc-32bit*.rpm)。當升級至 Identity Manager 4.9 時，也會發生此錯誤。	在安裝 Identity Manager 之前，請務必安裝以下相依程式庫或 RPM： ◆ glibc-32bit-*.x86_64.rpm ◆ libz1-32bit 如果系統中已安裝 glibc-32bit-*.x86_64.rpm，則可忽略此錯誤。
在 SLES 15 SP5 一體化組態中安裝 Identity Manager 4.9 時，無法載入 SSPR 頁面，並顯示 SSPR 5203 CONFIG_FORMAT_ERROR。	重新啟動 Tomcat 服務。

問題	建議執行的動作
重新啟動系統 (其中的 Identity Manager 4.9 安裝在 RHEL 8 作業系統上) 後，您無法存取 Identity Manager 儀表板。`catalina.log` 檔案包含以下警告訊息： `WARN [com.novell.soa.af.impl.core.WorkflowEngineImpl] (main) [WORKFLOW] Duplicate engine id detected.This engine may not have been shutdown cleanly or another engine is running with engine-id: ENGINE .Waiting 60000 ms for heartbeat to timeout.` 如果重新啟動系統之前未停止 Tomcat 服務，則會出現此問題。當工作流程引擎啟動時，它會遇到叢集中的另一個節點，而該節點的引擎 ID 已在使用中，因此工作流程引擎會記錄警告。	永遠建議在重新啟動系統之前停止 Tomcat 服務。如果您確實看到了該警告，可以透過變更 `igaworkflowdb` 資料庫中 afenginestate 表內的引擎狀態來解決問題。登入 pgAdmin 之類的資料庫管理工具，並手動將引擎狀態更新為關閉狀態。
在 RHEL 8.3 上安裝 Identity Manager 4.9 時，PostgreSQL 服務無法正常啟動。	請執行以下步驟： 1. 在 RHEL 8 上安裝 Identity Manager 4.9。 2. 將 RHEL OS 版本升級至 8.3。

當您在 SLES 15 或 SLES 15 SPx (x 表示 Identity Manager 支援的所有 SLES 15 版本) 上安裝 Identity Manager 時，Tomcat 和 ActiveMQ 服務處於停用狀態。	請執行以下步驟：
	
	1. 登入停用了 Tomcat 和 ActiveMQ 服務的伺服器。
	2. 安裝 `insserv-compat*` RPM。* 符號表示 RPM 的最新版本。
	
	附註：NetIQ 建議從您的作業系統訂閱服務獲取相依套件，以確保取得作業系統廠商的持續支援。如果您沒有訂閱服務，可以從相關網站 (例如 http://rpmfind.net/linux) 找到最新的套件。
	
	3. 執行以下指令以啟用 Tomcat 和 ActiveMQ 服務：
	
	`systemctl enable netiq-tomcat.service`
	
	`systemctl enable netiq-activemq.service`

問題	建議執行的動作

如果您是在 RHEL 8.1 上安裝 Identity Manager 4.9，執行以下操作時會顯示如下錯誤訊息：
• 執行 RHEL-Prerequisite.sh 程序檔：
`dnf-utils rpm required but not found`
`RHEL 8.1 iso does not contain dnf-utils packages, its replaced by yum-utils`
• 安裝 Identity Manager 引擎元件：
`Some of the dependencies required for installation of Identity Vault are not found`
	請忽略錯誤訊息並繼續安裝。

將 Identity Applications 升級至版本 4.9 後，在 Identity Applications 上無法轉譯工作流程表單。在某些情況下，/opt/netiq/idm/apps/sites/config.ini 中的用戶端密碼 (CientPass) 會保留為空白。	若要解決此問題，請執行以下步驟： 1. 導覽至 /opt/netiq/idm/apps/sites/ 目錄。 2. 編輯 config.ini 檔案，為 ClientPass 參數提供 base64 編碼的密碼。 **附註：**指定您在組態更新公用程式中為 **forms client** 指定的相同密碼。 3. 重新啟動 NGINX 服務。 `systemctl restart netiq-nginx.service` 如需詳細資訊，請參閱 TID 7024492。
在容器環境中，如果超過了針對 Identity Manager 儀表板設定的閒置時間並且工作階段逾時，延期按鈕不會依預期運作。	在 OSP 容器的 ism-configuration.properties 檔案中新增 com.netiq.idm.session-timeout 內容。
在多伺服器環境中，嘗試將驅動程式部署到次要伺服器時顯示 LDAP 例外。	安裝次要伺服器並在 Identity Vault 中為次要伺服器新增分割區之後，必須在兩部伺服器上重新啟動 ndsd。如果您要在容器部署過程中安裝 Identity Manager 引擎，此規則同樣適用。
在叢集環境中，如果您中斷某個節點 (例如節點 2) 與網路的連接，然後在使用中節點 (例如節點 1) 上建立角色，當節點 2 重新連接至網路後，這些新增的角色不會同步到節點 2 上。	在節點 2 上執行以下步驟： 1. 刪除 .../temp/permindex 檔案。 2. 重新啟動 Tomcat。
在進行 Identity Applications 組態期間，如果您要連接至遠端伺服器上安裝的 SSPR，將會跳過 SSPR 組態。但是，當您重新啟動 Tomcat 時，系統將會部署在安裝過程中安裝的 sspr.war。	如果您要連接至遠端伺服器上安裝的 SSPR，請在設定 Identity Applications 之前，先從 /opt/netiq/idm/apps/tomcat/webapps 目錄中移除 sspr.war。

問題	建議執行的動作
在進行 Identity Applications 組態期間，如果您為 Identity Applications 管理員使用自訂子容器 (例如 cn=uaadmin,ou=univ,o=data)，則會在預設容器 (ou=sa,o=data) 下建立 uaadmin。	如果您要為 Identity Applications 管理員使用自訂子容器，請執行以下步驟之一： ◆ 在設定 Identity Applications 之前，建立 ou=univ,o=data 自訂子容器。 ◆ 在組態過程中，請在出現是否要使用自訂容器做為根容器提示時指定否。要輸入的自訂 LDIF 檔案應包含自訂根容器和子容器詳細資料。
建立靜默內容檔案時，靜默安裝程序不檢查系統要求。在靜默安裝期間，記錄檔案顯示一則錯誤訊息，指出不符合系統要求。	如果您遇到此錯誤，請在 silent.properties 檔案中手動新增 IS_SYSTEM_CHECK_DONE 參數。若要跳過系統要求檢查，請將 IS_SYSTEM_CHECK_DONE 參數的值設定為 1。
解除安裝和重新安裝 Identity Applications 或 Identity Reporting 時，組態程序在設定資料庫使用者與綱要時失敗。如果在重新安裝元件期間進行一般組態，則會出現此問題。	重新安裝 Identity Applications 或 Identity Reporting 元件時，必須進行自訂組態。
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 netiq 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。

升級相關問題疑難排解

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 Open Enterprise Server (OES) 24.2 上升級 Identity Manager 引擎時，idmupgrade.log 記錄中報告了以下錯誤： [SEVERE]: Could not connect to the server Exception: Connect ErrorLDAPException: I/O Exception on host <IP_address>, port <port_number> Connect Error java.net.SocketException: Connection or outbound has closed	忽略此錯誤，它不會導致功能受損。

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.ks` 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： `javax.net.ssl.SSLHandshakeException: PKIX path validation failed: java.security.cert.CertPathValidatorException: Could not determine revocation status.` 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.ks` 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。	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` 目錄中的 `setenv.sh` 檔案。例如 `/opt/netiq/idm/apps/tomcat/bin/setenv.sh`。 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。
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。	(視情況而定) 以下步驟適用於 Identity Manager 4.9： 1. 登入其中 Identity Applications 已升級至版本 4.9 的伺服器。 2. 導覽至 `/opt/etiq/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 從舊版升級至版本 4.9 後，表單轉譯器不依預期運作。將預設 IDMProv 部署網路位置修改為自訂網路位置後會出現此問題。	若要解決此問題，請執行以下步驟： 1. 登入其中 Identity Applications 已升級至版本 4.9 的伺服器。 2. 導覽至 `/opt/netiq/idm/apps/sites` 目錄。 3. 編輯 `ServiceRegistry.json` 檔案。 4. 將部署網路位置從 `IDMProv` 修改為在升級之前指定的自訂網路位置。 5. 儲存 `ServiceRegistry.json` 檔案。 6. 導覽至 `/opt/netiq/idm/apps/sites/forms/` 目錄。 7. 編輯 `main.<version>.js` 檔案，其中 *<version>* 是隨機產生的英數字元值。 8. 將部署網路位置從 `IDMProv` 修改為在升級之前指定的自訂網路位置。 9. 儲存 `main.<version>.js` 檔案。 10. 重新啟動 Tomcat。
將分散式環境中的 Identity Manager 升級至版本 4.9 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。您將在 `idm-osp.log` 檔案中看到以下例外： `sun.security.validator.ValidatorException: TrustAnchor with subject "CN=***, L=***, O=***" is not a CA certificate`	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 `/opt/netiq/common/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 4.9 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，請使用以下指令手動重新啟動 NGNIX 和 Golang 服務： ◆ **NGNIX：** `/opt/netiq/common/ngnix/ngnix` ◆ **Golang：** `/etc/init.d/netiq-golang.sh` Identity Applications 使用 NGNIX 服務在 Identity Applications 儀表板中轉譯表單。
在標準版中升級 Identity Reporting 後，`configupdate.sh.properties` 中的 **is_prov** 參數設定為 `true`。因為在標準版中無法使用 Identity Applications，所以此參數的值必須設定為 `false`。	在 `configupdate.sh.properties` 檔案中手動將 **is_prov** 參數設定為 `false`。
如果先前的 Identity Manager 引擎升級失敗，將無法重新執行 Identity Manager 引擎安裝程式。例如，如果第一次嘗試將 Identity Manager 引擎升級至 4.9 失敗，然後再次嘗試升級 Identity Manager 引擎，則無法觸發升級程序。	請執行以下步驟： 1. 使用 `novell-DXMLengnx` RPM 將 Identity Manager 引擎降級至舊版本。 2. 升級 Identity Manager 引擎。
當您升級 Identity Manager 後，系統會將以下內容新增至 `ism-configuration.properties` 檔案： `com.netiq.idm.osp.ldap.admin-dn = cn=admin,ou=sa,o=system`	請在 `ism-configuration.properties` 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 `ism-configuration.properties` 檔案： `com.netiq.sspr.redirect.url = https://___SSPR_IP___:___SSPR_TOMCAT_HTTPS_PORT___/sspr/public/oauth`	請在 `ism-configuration.properties` 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，`ism-configuration.properties` 檔案中會填入 `java.protocol.handler.pkgs` 內容的某些重複值。	不會出現功能受損的情況。若要解決此問題，請執行以下動作： 1. 導覽至 `/opt/netiq/idm/apps/tomcat/conf` 目錄中的 `ism-configuration.properties` 檔案。 2. 修改 `ism-configuration.properties` 檔案，移除 `java.protocol.handler.pkgs` 內容的重複值。 3. 儲存該檔案並重新啟動 Tomcat。

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 `opt/netiq/common/jre/bin` 目錄，並使用以下指令將證書輸入至 `idm.jks` 檔案： `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>` 10. 重新啟動 Tomcat。

Ansible 部署相關問題疑難排解

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
在部署中首次執行 `deploy.yml` 時，您會看到以下訊息，指出目標節點上不存在 Docker 影像。例如，如果您正在部署 Core DNS 容器，您將看到以下錯誤： `fatal: [<ip address/DNS>]: FAILED! => {"changed": true, "cmd": "docker images | grep coredns | grep 1.8.0", "delta": "0:00:00.914078", "end": "msg": "non-zero return code", "rc": 1, "start": "stderr": "", "stderr_lines": [], "stdout": "", "stdout_lines": []}`	目前尚未提供解決方式。但是，您可以忽略該訊息並繼續部署。這不會造成任何功能性損失。

問題	建議執行的動作
如果 IP 位址已由網路中的其他容器使用，容器部署將會失敗。主控台會報告以下例外。 `fatal: [<ip address/DNS>]: FAILED! => {"changed": false, "msg": "Error starting container b1eb07f42cf6bd63787ae6167f5e3a0f7cbee0f8be80a5764bcc7c7f9d6b96b1 : 403 Client Error for http+docker://localhost/v1.40/containers/ b1eb07f42cf6bd63787ae6167f5e3a0f7cbee0f8be80a5764bcc7c7f9d6b96b1 /start: Forbidden (\"Address already in use\")"}`	為容器指定不同的 IP 位址。

問題	建議執行的動作
部署 Identity Applications 容器後，當您登入 Identity Manager 儀表板並導覽至任務頁面時，儀表板不依預期擷取任務清單。catalina.out 檔案中報告了以下錯誤。 SEVERE [main] org.apache.catalina.startup.ContextConfig.processAnnotationsWebResource Unable to process web resource [/WEB-INF/classes/com/microfocus/idm/nrf/resources/NRFRsrc_fr.class] for annotations java.io.EOFException at java.io.DataInputStream.readFully(DataInputStream.java:197) at java.io.DataInputStream.readUTF(DataInputStream.java:609) at java.io.DataInputStream.readUTF(DataInputStream.java:564) at org.apache.tomcat.util.bcel.classfile.ConstantUtf8.getInstance(ConstantUtf8.java:36) at org.apache.tomcat.util.bcel.classfile.Constant.readConstant(Constant.java:79) at org.apache.tomcat.util.bcel.classfile.ConstantPool.<init>(ConstantPool.java:53) at org.apache.tomcat.util.bcel.classfile.ClassParser.readConstantPool(ClassParser.java:174) at org.apache.tomcat.util.bcel.classfile.ClassParser.parse(ClassParser.java:83) at org.apache.catalina.startup.ContextConfig.processAnnotationsStream(ContextConfig.java:2351) at org.apache.catalina.startup.ContextConfig.processAnnotationsWebResource(ContextConfig.java:2250) at org.apache.catalina.startup.ContextConfig.processAnnotationsWebResource(ContextConfig.java:2244) at org.apache.catalina.startup.ContextConfig.processAnnotationsWebResource(ContextConfig.java:2244) at org.apache.catalina.startup.ContextConfig.processAnnotationsWebResource(ContextConfig.java:2244) at org.apache.catalina.startup.ContextConfig.processAnnotationsWebResource(ContextConfig.java:2244) at org.apache.catalina.startup.ContextConfig.processAnnotationsWebResource(ContextConfig.java:2244) at org.apache.catalina.startup.ContextConfig.processClasses(ContextConfig.java:1397) at org.apache.catalina.startup.ContextConfig.webConfig(ContextConfig.java:1302) at org.apache.catalina.startup.ContextConfig.configureStart(ContextConfig.java:985)	若要解決此問題，請執行下列步驟： 1. 導覽至 /opt/netiq/idm/apps/tomcat/webapps/ 目錄。 2. 刪除 workflow 資料夾。 3. (選擇性) 重新啟動 Tomcat。

AKS 部署相關問題疑難排解

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 入口網站中執行 Terraform 指令時，您可能會遇到阻礙基礎架構部署的錯誤。下面列出了一些可能的錯誤。
 	
`Error: making Read request on Azure KeyVault Secret slesvmpwd: azure.BearerAuthorizer#WithAuthorization: Failed to refresh the Token for request to https://idmkv88211894240361.vault.azure.net/secrets/slesvmpwd/?api-version=7.1: StatusCode=401 -- Original Error: adal: Refresh request failed.Status Code = '401'.Response body: {"error":{"code":"invalid_request","message":"Required audience parameter not specified"}} Endpoint http://localhost:50342/oauth2/token | | with module.server.data.azurerm_key_vault_secret.slesvmpwd, | on sles15sp2-server/main.tf line 42, in data "azurerm_key_vault_secret" "slesvmpwd": | 42: data "azurerm_key_vault_secret" "slesvmpwd" { kubernetes_secret.example3: Creation complete after 1s [id=idm/ingress-tls] ? | Error: error detecting capabilities: error PostgreSQL version: dial tcp 52.186.162.130:5432: connect: connection timed out | | with module.dbserver.postgresql_database.igaworkflowdb, | on Azure-PG-Server/main.tf line 217, in resource "postgresql_database" "igaworkflowdb": | 217: resource "postgresql_database" "igaworkflowdb" { | az aks get-credentials --resource-group rajj_rg --name cluster-name --overwrite-existing | Error: making Read request on Azure KeyVault Secret uawfedbuser: azure.BearerAuthorizer#WithAuthorization: Failed to refresh the Token for request to https://idmkv80357639695488.vault.azure.net/secrets/uawfedbuser/?api-version=7.1: StatusCode=401 -- Original Error: adal: Refresh request failed.Status Code = '401'.Response body: {"error":{"code":"invalid_request","message":"Required audience parameter not specified"}} Endpoint http://localhost:50342/oauth2/token | | with module.dbserver.data.azurerm_key_vault_secret.uawfedbuser, | on Azure-PG-Server/main.tf line 28, in data "azurerm_key_vault_secret" "uawfedbuser": | 28: data "azurerm_key_vault_secret" "uawfedbuser" { module.dbserver.null_resource.delay: Creation complete after 5m0s [id=5961346882319865424] ?| Error: waiting for creation of Managed Kubernetes Cluster "test-akscluster" (Resource Group "idmtest_rg"): Code="ReconcileStandardLoadBalancerError" Message="Reconcile standard load balancer failed.Details: outboundReconciler retry failed: Category: ClientError; SubCode: PublicIPCountLimitReached; Dependency: Microsoft.Network/PublicIPAddresses; OrginalError: Code=\"PublicIPCountLimitReached\" Message=\"Cannot create more than 10 public IP addresses for this subscription in this region.\" Details=[]; AKSTeam: Networking, Retriable: false." | | with module.aks.azurerm_kubernetes_cluster.main, | on .terraform/modules/aks/main.tf line 10, in resource "azurerm_kubernetes_cluster" "main": | 10: resource "azurerm_kubernetes_cluster" "main" {`
	若要解決此問題，請執行以下步驟：
	
	1. 登入 Azure 入口網站。
	2. (選擇性) 找到 Azure Kubernetes 叢集組態檔案路徑。
	3. 執行以下指令覆寫預設組態檔案 ~/.kube/config。
	
	`aks get-credentials --resource-group < 資源群組名稱 > --name <kube 叢集名稱 > --overwrite-existing`
	
	`export KUBE_CONFIG_PATH=~/.kube/config`
	
	4. 重新執行 Terraform 指令。如需詳細資訊，請參閱使用 Configuration Generator 進行部署中的步驟 14、步驟 15、步驟 16。

問題	建議執行的動作
當您嘗試在 Azure 上建立公用 IP 位址時，可能會出現以下錯誤。 `| Error: waiting for creation of Managed Kubernetes Cluster "cluster-name" (Resource Group "raj_rg"): Code="ReconcileStandardLoadBalancerError" Message="Reconcile standardload balancer failed.Details: outboundReconciler retry failed: Category: ClientError; SubCode: PublicIPCountLimitReached; Dependency: Microsoft.Network/PublicIPAddresses;OrginalError: Code=\"PublicIPCountLimitReached\" Message=\"Cannot create more than 10 public IP addresses for this subscription in this region.\" Details=[]; AKSTeam: Networking, Retriable: false." | | with module.aks.azurerm_kubernetes_cluster.main, | on .terraform/modules/aks/main.tf line 10, in resource "azurerm_kubernetes_cluster" "main": | 10: resource "azurerm_kubernetes_cluster" "main" {`	請聯絡 Azure 團隊來提高訂閱配額，或嘗試移除已指定的但未使用的公用 IP 位址。

問題	建議執行的動作

在 Azure 入口網站中執行 `terraform apply` 指令時，可能會出現以下例外：
 	
`(AgentPoolK8sVersionNotSupported) 版本 <version> 在此區域中不受支援。請使用 [az aks get-versions] 指令取得此區域中支援的版本清單。如需詳細資訊，請查看 https://aka.ms/supported-version-list`
	若要解決此問題，請執行以下步驟：
	
	1. 登入 Azure 入口網站。
	2. 按一下  。
	3. 執行以下指令來識別您所在區域支援的版本：
	
	`az aks get-versions -l <location>`
	
	例如：
	
	`az aks get-versions -l eastus`
	
	4. 導覽至 `IDM_4.9_Cloud_Deployment_files` 目錄，移至 `main.tf` 檔案並編輯以下值：
	
	`kubernetes_version = "< 版本 >"`
	
	`orchestrator_version = "< 版本 >"`
	
	例如：
	
	`kubernetes_version = "1.20.15"`
	
	`orchestrator_version = "1.20.15"`
	
	附註：版本 `1.20.x` 已經過認證，在 AKS Kubernetes 上受支援。
	
	5. 重新執行以下指令：
	
	`terraform apply --auto-approve`

問題	建議執行的動作
在 Azure Kubernetes Service 上部署多例項容器時，您可能會發現有一些 Pod 處於等待中狀態。	若要解決該問題，請執行以下步驟： 1. 登入 Azure 入口網站。 2. 在搜尋方塊中輸入「kubernetes service」，然後按 Enter。 3. 選取您的 kubernetes 叢集。 4. 按一下**診斷並解決問題** > **疑難排解**。 5. (視情況而定) 如果使用疑難排解方法未能解決問題，請檢查您的 Azure 帳戶的使用配額。 a. 移至「首頁」，在搜尋方塊中輸入「配額」，然後按 Enter。 b. 按一下**計算**。 c. (視情況而定) 如果「目前使用率」欄顯示 100% 並帶有紅線，請按一下**申請提高配額**。 d. 在**新限制**文字方塊中輸入新限制。 e. 按一下**「提交」**。
當您重新啟動引擎例項 Pod 時，現有 Identity Vault 的驅動程式部署將會失敗。Designer 應用程式中可能會出現以下錯誤： 「`cn=Azure AD Driver,cn=Driver Set,o=system`」部署失敗並出現錯誤和 / 或警告。	移至 Designer 應用程式，並將 Identity Vault 重新輸入 Designer。
當您重新啟動主要伺服器時，將為它指定新 IP 位址，此 IP 位址與次要伺服器的 SSL 證書中的 IP 位址不相符。	重新啟動次要伺服器會導致它使用新 IP 位址重新核發 SSL 證書。

問題	建議執行的動作
在 Identity Manager Reporting 中，當您嘗試輸入總大小超過 1MB 的多個報告時，會顯示錯誤 413。發生此錯誤的原因是 nginx-ingress 控制器允許的預設申請本文大小為 1MB。 呼叫 URL (/IDMRPT-CORE/rpt/definitions/import?uploadid=<id>&content=text/html&format=application/json&overwrite=true) 時發生錯誤。伺服器傳回狀態碼 413 及以下不可剖析的 JSON 資料：	若要解決此問題，可以允許指定更大的申請本文大小，為此，請在入口組態區段下的 values.yaml 檔案中新增以下註釋： nginx.ingress.kubernetes.io/proxy-body-size: 3m

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
在 OES 上安裝 Identity Manager 引擎時，主控台以及 /var/opt/netiq/idm/log/ 目錄下的 idminstall.log 檔案中報告以下訊息。	請確定 OES 伺服器上存在 /etc/OES-brand 檔案。如果該檔案不存在，請建立一個新檔案並再次嘗試安裝 Identity Manager 引擎。
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. 導覽至 /etc/opt/novell/eDirectory/conf/ 目錄。 2. 在 env_idm 檔案中，新增 SLEEP_BEFORE_ENGINE_STARTUP 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。 3. 重新啟動 eDirectory。 4. (視情況而定) 檢查 ndsd.log 以檢視訊息和記錄。

問題	建議執行的動作
在 Linux 系統上執行 Identity Manager 引擎時，雖然有可用的空間，但仍出現 /tmp 目錄磁碟空間不足的錯誤。您可以使用 df (disk free) 和 du (disk used) 指令來檢查此狀態。df 指令指出沒有任何可用空間，而 du 指令則指出並未用完為 /tmp 配置的所有空間。之所以出現此問題，是因為每個具現化 Identity Manager 驅動程式都會在記憶體中載入多個程式庫。JVM 會將這些驅動程式暫時複製到 /tmp 目錄，並在事後會將其刪除。已刪除的檔案會繼續佔用記憶體，直到建立這些檔案的 JVM 程序終止為止。您可以使用 lsof 指令來查出此行為。處於此狀態的檔案標示為已刪除。使用的總磁碟空間取決於伺服器上執行的驅動程式數。	消耗的空間是相對靜態的。因此，請務必在 /tmp 目錄中提供足夠的額外空間。如果該問題持續出現，請重新啟動 eDirectory。
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 iManager。 2. 按一下角色和任務 > 分割區和複本 > 複本檢視。 3. 選取次要伺服器。 4. 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。
透過 dxcmd 執行大規模查詢時，dxcmd 會結束並顯示 625 ERR_TRANSPORT_FAILURE 錯誤，而且不會產生任何結果檔案。 Identity Manager 引擎使用環境變數 NCPCLIENT_REQ_TIMEOUT 的值做為執行 dxcmd 查詢的預設時間。依預設，NCP 連接的逾時為 115 秒。如果執行查詢和傳回結果所需的時間超過此值，將會顯示錯誤。	透過將環境變數 NCPCLIENT_REQ_TIMEOUT 的值設定為大於查詢所需總時間的秒數來提高逾時值。可透過在 dxcmd 程序檔 /opt/novell/eDirectory/bin/dxcmd 中新增 export NCPCLIENT_REQ_TIMEOUT=value 來永久設定 dxcmd 的環境變數。也可在執行 dxcmd 之前從執行該程序檔的終端機中執行 export NCPCLIENT_REQ_TIMEOUT=value 來手動設定變數。
將 Identity Manager 引擎升級至 4.9 時，記錄中可能會出現關於 OES 從伺服器中斷連接的錯誤。	此問題的原因是未定義參數 ${IDM_KEYSTORE_PWD}。 可以忽略此問題，但如果您想要避免其發生，請在靜默內容或環境中定義參數 ${IDM_KEYSTORE_PWD}。

Identity Applications 和 Identity Reporting 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
如果在「證書標題」和「應用程式組態」中指定的 LDAP 伺服器名稱不同，則在升級 Identity Manager 後，Identity Applications 將無法連接到 Identity Vault。	Java 對 LDAPS 連接啟用端點識別，因此，在連接到 Identity Manager 伺服器時指定的伺服器名稱必須與證書中傳回的伺服器名稱相同。如果伺服器名稱不同，請執行以下步驟： 1. 導覽至 `/opt/netiq/idm/apps/configupdate` 目錄。 2. 執行以下指令啟動組態更新公用程式。 `./configupdate.sh` 3. 導覽至**使用者應用程式**索引標籤，按一下 **Identity Vault 伺服器**，然後將伺服器名稱變更為 LDAP 伺服器證書標題中指定的名稱。 此動作將更新 `ism-configuration.properties` 檔案中的 `DirectoryService/realms/jndi/params/AUTHORITY` 內容。 4. 按一下**確定**。
如果將 Identity Applications 和 Identity Reporting 安裝在同一部伺服器上，而您使用 `<reporting install folder>/bin` 目錄中的組態更新公用程式來進行組態變更，Identity Manager 儀表板將無法啟動。`catalina.out` 記錄檔案中會報告以下錯誤： `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.`	若要進行任何組態變更，請使用 `/opt/netiq/idm/apps/configupdate/` 目錄中的組態更新公用程式。

問題	建議執行的動作
無法使用組態更新公用程式變更某個內容的密碼。	您可以透過執行以下步驟，從指令行變更某個內容 (例如 com.netiq.rpt.ssl-keystore) 的密碼： 1. 使用以下公用程式加密您的密碼： `/opt/netiq/common/jre/bin/java -jar tomcat/lib/obscurity-0.13.2-uber.jar com.netiq.ism.obfuscate.server.util.PasswordObfuscator << 密碼 >>` 2. 導覽至 /opt/netiq/idm/apps/tomcat/conf 目錄中的 ism-configuration.properties 檔案。 3. 修改 ism-configuration.properties 檔案，以新增在步驟 2 中為 com.netiq.rpt.ssl-keystore.pwd 參數指定的加密密碼。 4. 儲存該檔案並重新啟動 Tomcat。
如果將 Identity Reporting 安裝在獨立的伺服器上，並且您透過儀表板啟動 Identity Reporting 或 IDM DCS URL，URL 將無法啟動。	啟動 Identity Reporting 或 IDM DCS URL 之後，請執行以下步驟： 1. 導覽至網址列。 2. 修改 URL，並手動提供安裝了 Identity Reporting 的伺服器的主機名稱和連接埠詳細資料。 此外，導覽至安裝了 Identity Applications 的伺服器上的 configupdate.sh.properties 檔案，並在 sso_apps 參數中新增 rpt 項目，然後儲存變更。例如 **sso_apps=ua,rpt**
如果 Identity Applications 和 Identity Reporting 安裝在同一部伺服器上，並針對 OSP 和 Identity Applications 啟用了 CEF 稽核，則 Reporting 元件將無法啟動。	請執行以下步驟來解決此問題： 1. 導覽至 /opt/netiq/idm/apps/tomcat/conf 目錄中的 idmrptcore_logging.xml 檔案。 2. 在 idmrptcore_logging.xml 檔案中新增 <keystore file> 參數，並指定金鑰儲存區檔案路徑。例如，新增下面一行： `<keystore-file>/opt/netiq/idm/app/tomcat/conf/idm.jks</keystore-file>` 3. 重新啟動 Tomcat。
如果 Identity Applications 和 Identity Reporting 安裝在同一部伺服器上，並且您為資料庫建立選項選取了**啟動**，將會在記錄中看到一些例外。	若要清除這些例外，請手動重新啟動 Tomcat。

問題	建議執行的動作
如果現有的 Identity Applications 或 Identity Reporting 組態中未設定連接埠，而您嘗試對 Identity Manager 進行升級，組態更新公用程式中**驗證**和 **SSO 用戶端**索引標籤下列出的 IP 位址與連接埠將顯示錯誤的值。	升級 Identity Applications 和 Identity Reporting 後，請執行以下步驟： 1. 導覽至 `/opt/netiq/idm/apps/configupdate` 目錄。 2. 執行以下指令： `./configupdate.sh` 3. 在**驗證**索引標籤上的 **OAuth 伺服器主機識別碼**和 **OAuth 伺服器 TCP 連接埠**欄位中，分別指定正確的 IP 位址和連接埠。 4. 在 **SSO 用戶端**索引標籤中，確定 IDM Administrator、Reporting 和 IDM 資料收集服務的 URL 格式正確。 5. 重新啟動 Tomcat。
您要修改安裝過程中建立的下列一或多個使用者應用程式組態設定： ◆ 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。 **Linux**：從安裝目錄 (預設為 `/opt/netiq/idm/apps/configupdate/`) 中執行以下指令： `./configupdate.sh`
啟動 Tomcat 會導致以下例外： `port 8180 already in use`	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。	請務必使用安裝使用者應用程式期間指定的 JDK 來啟動 Tomcat。
無法登入入口網站管理頁面。	確保使用者應用程式管理員帳戶存在。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。	使用者應用程式管理員必須是頂層容器的託管者，並且應具有「監督者」權限。您可以嘗試將使用者應用程式管理員的權限設定為與 LDAP 管理員的權限相同 (使用 Identity Console)。

問題	建議執行的動作
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使用者應用程式期間指定的 JDK。 使用 keytool 指令，來輸入證書檔案： `keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit` ◆ 以您為此證書選擇的唯一名稱來取代 *aliasName*。 ◆ 以證書檔案的完整路徑和名稱來取代 *certFile*。 ◆ 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，以檢查您是否已提供以下使用者應用程式組態參數的值：**Email From** 和 **Email Host**。 **Linux**：從安裝目錄 (預設為 /opt/netiq/idm/apps/configupdate/) 中執行以下指令： `./configupdate.sh`
組態更新公用程式中未顯示 **IG SSO 用戶端**索引標籤	在 configupdate.sh.properties 檔案中的 sso_apps 參數內新增 ig 項目，然後儲存變更。如果 sso_apps 參數已包含 Identity Applications 和 Identity Reporting 項目，請將 Identity Governance 項目新增至清單中。例如 **sso_apps=ua,rpt,ig**
部署 Identity Applications 容器時顯示以下例外： 錯誤 [com.novell.afw.portlet.consumer.core.EboPortletProducerChangeListener] (main) [RBPM] portletID 為「HeaderPortlet」的入口網站應用程式註冊不存在。 com.novell.afw.portlet.exception.EboPortletRegistrationException：portletID 為「HeaderPortlet」的入口網站應用程式註冊不存在。	重新啟動 Identity Applications 容器。

問題	建議執行的動作

部署 Identity Applications 容器後，當您嘗試申請與新表單關聯的許可權時，該表單不依預期載入。此問題是隨機出現的。	確定已在 nginx.conf 檔案中指定表單轉譯器伺服器和連接埠詳細資料。若要更新 nginx.conf 檔案，請執行以下步驟：
	1. 登入表單轉譯器容器。
	`docker exec -it < 容器 > < 指令 >`
	例如：
	`docker exec -it fr-container bash`
	2. 導覽至 /opt/netiq/common/nginx/ 目錄。
	3. 編輯 nginx.conf 檔案。
	4. 指定表單轉譯器伺服器和連接埠詳細資料。例如：
	`server {`
	`listen 8600 ssl;`
	`server_name formrenderer.example.com;`

其他問題疑難排解

下面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
如果在 Identity Manager 引擎中啟用了 FIPS，嘗試連接至 Identity Console 時，啟用了 FIPS 的 Identity Vault/eDirectory 的密碼驗證會失敗。	導覽至 Identity Console 目錄並執行以下檔案： `./identityconsole_install` 然後遵照 《*Identity Console Installation Guide*》(Identity Console 安裝指南) 中 「Performing an Interactive Installation」 (執行互動式安裝) 程序的步驟 5 及後續步驟進一步操作。