NetIQ Identity Manager

安裝指南 - Windows

2018 年 3 月

NetIQ

法律聲明

如需 NetIQ 法律聲明、免責聲明、擔保聲明、出口與其他使用限制、美國政府限制的權利、專利政策與 FIPS 法規遵循的相關資訊，請參閱 https://www.netiq.com/company/legal/。

Copyright (C) 2018 NetIQ Corporation. 保留所有權利。

目錄

關於本書和文件庫 13
關於 NetIQ Corporation 15

I 介紹 17

1 Identity Manager 的元件綜覽 19

2 建立和維護 Identity Manager 環境 21
2.1 Designer for Identity Manager . . . 21
2.2 Analyzer for Identity Manager . . . 21
2.3 iManager . . . 22

3 在 Identity Manager 環境中管理資料 23
3.1 瞭解資料同步 . . . 23
3.2 瞭解稽核、報告及法規遵循 . . . 23
3.3 瞭解用於同步化身分資料的元件 . . . 24
3.3.1 Identity Vault . . . 24
3.3.2 Identity Manager 引擎 . . . 24
3.3.3 遠端載入器 . . . 24
3.3.4 Identity Reporting . . . 24

4 佈建使用者以進行安全的存取 27
4.1 瞭解 Identity Manager 中的證明程序 . . . 27
4.2 瞭解 Identity Manager 中的自助服務程序 . . . 28
4.3 瞭解管理使用者佈建的元件 . . . 28
4.3.1 使用者應用程式和 Roles Based Provisioning Module . . . 29
4.3.2 Identity Applications 管理 . . . 30
4.3.3 Identity Manager 儀表板 . . . 30
4.4 使用 Identity Manager 中的自助式密碼管理 . . . 31
4.4.1 瞭解預設自助服務程序 . . . 31
4.4.2 瞭解舊密碼管理提供程式 . . . 32
4.5 在 Identity Manager 中使用單一登入存取 . . . 33
4.5.1 瞭解使用 One SSO Provider 進行驗證的方法 . . . 33
4.5.2 瞭解 One SSO Provider 的金鑰儲存區 . . . 34
4.5.3 瞭解 One SSO Provider 的稽核事件 . . . 34

II 規劃安裝 Identity Manager 35

5 規劃綜覽 37
5.1 規劃核對清單 . . . 37
5.2 瞭解安裝程序 . . . 38
5.3 建議的安裝情境和伺服器設定 . . . 39
5.3.1 將事件傳送到稽核服務，而不在 Identity Manager 中報告 . . . 39
5.3.2 將事件傳送到 Identity Manager 並產生報告 . . . 40
5.3.3 在將事件推入 Identity Manager 前先將其傳送至外部服務 . . . 40

5.3.4 建議的伺服器設定 . . . 41
5.3.5 選取 Identity Manager 的作業系統平台 . . . 41
5.4 瞭解授權和啟用 . . . 42
5.5 下載安裝檔案 . . . 43
5.6 尋找可執行檔和預設安裝路徑 . . . 43

6 安裝注意事項 45

6.1 瞭解 Identity Manager 通訊 . . . 45
6.2 瞭解語言支援 . . . 46
6.2.1 已翻譯的元件和安裝程式 . . . 46
6.2.2 關於語言支援的特殊考量 . . . 47
6.3 確保 Identity Manager 的高可用性 . . . 47

III 安裝 Identity Manager 引擎 49

7 安裝 Identity Vault 51

7.1 規劃安裝 Identity Vault . . . 51
7.1.1 Identity Vault 安裝核對清單 . . . 51
7.1.2 安裝 Identity Vault 的先決條件和考量 . . . 52
7.1.3 瞭解 eDirectory 中的 Identity Manager 物件 . . . 54
7.1.4 Identity Vault 的系統要求 . . . 54
7.2 安裝 Identity Vault 的準備工作 . . . 55
7.2.1 當容器名稱中包含句點 (「.」) 時使用逸出字元 . . . 55
7.2.2 使用 OpenSLP 或 hosts.nds 解析網路樹名稱 . . . 56
7.2.3 改進 Identity Vault 效能 . . . 60
7.2.4 在 Identity Vault 伺服器上使用 IPv6 位址 . . . 60
7.2.5 使用 LDAP 與 Identity Vault 通訊 . . . 61
7.2.6 在裝有管理公用程式的工作站上手動安裝 NICI . . . 62
7.2.7 安裝 NMAS 用戶端軟體 . . . 62
7.3 安裝 Identity Vault . . . 62
7.3.1 使用精靈安裝 Identity Vault . . . 63
7.3.2 以靜默方式安裝和設定 Identity Vault . . . 63
7.4 安裝後設定 Identity Vault . . . 70
7.4.1 將 SecretStore 新增至 Identity Vault 綱要 . . . 70
7.4.2 使用特定的地區設定進行 Identity Vault 設定 . . . 71
7.4.3 管理 eDirectory 例項 . . . 71

8 規劃安裝引擎、驅動程式和外掛程式 73

8.1 Identity Manager 引擎、驅動程式和外掛程式的安裝核對清單 . . . 73
8.2 瞭解安裝程式 . . . 74
8.3 安裝 Identity Manager 引擎的先決條件和考量 . . . 74
8.3.1 安裝 Identity Manager 引擎的考量 . . . 75
8.3.2 隨 Identity Manager 引擎一起安裝驅動程式的考量 . . . 75
8.4 Identity Manager 引擎的系統要求 . . . 75

9 安裝引擎、驅動程式和 iManager 外掛程式 77

9.1 使用精靈安裝元件 . . . 77
9.1.1 以管理使用者身分安裝 . . . 77
9.2 執行靜默安裝 . . . 78
9.3 在具有多個 Identity Vault 例項的伺服器上安裝 . . . 79
9.4 停止和啟動 Identity Manager 驅動程式 . . . 81
9.4.1 停止驅動程式 . . . 81

9.4.2 啟動驅動程式 82

10 安裝和管理遠端載入器 85

10.1 規劃安裝遠端載入器 85
10.1.1 遠端載入器安裝核對清單 85
10.1.2 瞭解遠端載入器 86
10.1.3 瞭解 Java 遠端載入器 88
10.1.4 瞭解安裝程式 88
10.1.5 在同一個電腦上使用 32 位元和 64 位元遠端載入器 88
10.1.6 安裝遠端載入器的先決條件和考量 88
10.1.7 遠端載入器的系統要求 90
10.2 安裝遠端載入器 92
10.2.1 使用精靈安裝遠端載入器 92
10.2.2 執行遠端載入器的靜默安裝 93
10.2.3 安裝 Java 遠端載入器 94
10.2.4 安裝 .NET 遠端載入器 95
10.2.5 執行遠端載入器的靜默安裝 96
10.3 設定遠端載入器和驅動程式 96
10.3.1 與 Identity Manager 引擎建立安全連接 97
10.3.2 瞭解遠端載入器的組態參數 99
10.3.3 為驅動程式例項設定遠端載入器 107
10.3.4 為驅動程式例項設定 Java 遠端載入器 110
10.3.5 為驅動程式例項設定 .NET 遠端載入器 111
10.3.6 設定 Identity Manager 驅動程式以與遠端載入器配合使用 113
10.3.7 設定與 Identity Manager 引擎的雙向驗證 114
10.3.8 驗證組態 122
10.4 啟動和停止遠端載入器 123
10.4.1 啟動遠端載入器中的驅動程式例項 123
10.4.2 停止遠端載入器中的驅動程式例項 124

11 安裝 iManager 125

11.1 規劃安裝 iManager 125
11.1.1 iManager 的安裝核對清單 125
11.1.2 瞭解 iManager 的伺服器版本和用戶端版本 126
11.1.3 瞭解 iManager 外掛程式的安裝 126
11.1.4 安裝 iManager 的先決條件和考量 127
11.1.5 iManager 伺服器的系統要求 128
11.1.6 iManager Workstation (用戶端版本) 的系統要求 129
11.2 安裝 iManager 伺服器和 iManager Workstation 130
11.2.1 安裝 iManager 和 iManager Workstation 130
11.2.2 以靜默模式安裝 iManager 133
11.3 iManager 的安裝後任務 135
11.3.1 取代 iManager 的暫存自行簽署證書 135
11.3.2 安裝後設定 iManager 以使用 IPv6 位址 137
11.3.3 指定 eDirectory 的授權使用者 137

IV 安裝 Identity Applications 139

12 為 Identity Manager 安裝 PostgreSQL 和 Tomcat 141

12.1 規劃安裝 PostgreSQL 和 Tomcat 141
12.1.1 Tomcat 和 PostgreSQL 的安裝核對清單 141
12.1.2 瞭解 PostgreSQL 和 Tomcat 的安裝程序 142
12.1.3 安裝 PostgreSQL 的先決條件 142
12.1.4 安裝 Tomcat 的先決條件 143
12.1.5 PostgreSQL 的系統要求 143

12.1.6 Tomcat 的系統要求 . . . 143
12.2 安裝 PostgreSQL 和 Tomcat . . . 143
12.2.1 使用精靈安裝 PostgreSQL 和 Tomcat . . . 144
12.2.2 以靜默模式為 Identity Manager 安裝 Tomcat 和 PostgreSQL . . . 146

13 安裝單一登入元件 149

13.1 為 Identity Manager 規劃安裝單一登入 . . . 149
13.1.1 單一登入元件的核對清單 . . . 149
13.1.2 安裝 One SSO Provider 的先決條件 . . . 150
13.1.3 One SSO Provider 的系統要求 . . . 150
13.1.4 使用 Apache Log4j 服務記錄登入 . . . 150
13.2 為 Identity Manager 安裝單一登入 . . . 151
13.2.1 使用精靈安裝 One SSO Provider . . . 151
13.2.2 以靜默模式安裝 One SSO Provider . . . 153
13.2.3 設定單一登入存取 . . . 154

14 安裝密碼管理元件 155

14.1 為 Identity Manager 規劃安裝密碼管理功能 . . . 155
14.1.1 安裝密碼管理元件的核對清單 . . . 155
14.1.2 安裝 Self Service Password Reset 的先決條件 . . . 156
14.1.3 Self Service Password Reset 的系統要求 . . . 156
14.1.4 針對密碼事件使用 Apache Log4j 服務 . . . 156
14.2 為 Identity Manager 安裝密碼管理功能 . . . 157
14.2.1 使用精靈安裝 Self Service Password Reset . . . 157
14.2.2 以靜默模式安裝 Self Service Password Reset . . . 160
14.2.3 安裝後任務 . . . 160
14.2.4 為叢集設定 OSP 和 SSPR . . . 162

15 安裝 Identity Applications 165

15.1 規劃安裝 Identity Applications . . . 165
15.1.1 Identity Applications 的安裝核對清單 . . . 166
15.1.2 瞭解 Identity Applications 的安裝程式 . . . 167
15.1.3 安裝 Identity Applications 的先決條件和考量 . . . 167
15.1.4 Identity Applications 的系統要求 . . . 172
15.2 為 Identity Applications 準備 Identity Vault . . . 173
15.2.1 將使用者應用程式綱要做為記錄應用程式新增至稽核伺服器中 . . . 173
15.2.2 向 Identity Vault 管理員和使用者應用程式管理員帳戶指定權限 . . . 174
15.3 設定 Identity Applications 的資料庫 . . . 175
15.3.1 設定 Oracle 資料庫 . . . 175
15.3.2 設定 PostgreSQL 資料庫 . . . 177
15.3.3 設定 SQL Server 資料庫 . . . 177
15.4 準備 Identity Applications 的環境 . . . 178
15.4.1 指定許可權索引的位置 . . . 178
15.4.2 為叢集啟用許可權索引 . . . 178
15.4.3 準備 Identity Applications 的應用程式伺服器 . . . 179
15.4.4 為 Identity Applications 準備叢集 . . . 180
15.5 安裝 Identity Applications . . . 181
15.5.1 Identity Applications 的安裝核對清單 . . . 181
15.5.2 使用引導式程序安裝 Identity Applications . . . 182
15.5.3 安裝後步驟 . . . 187
15.5.4 停用阻止 HTML 框架設定以將 Identity Manager 與 SSPR 整合 . . . 189
15.5.5 驗證使用者內容 . . . 190
15.5.6 啟動 Identity Applications . . . 191
15.6 建立和部署 Identity Applications 的驅動程式 . . . 192
15.6.1 建立「使用者應用程式」驅動程式 . . . 192

15.6.2 為叢集設定使用者應用程式驅動程式 . . . 193
15.6.3 建立角色與資源服務驅動程式 . . . 193
15.6.4 部署使用者應用程式的驅動程式 . . . 194
15.7 完成 Identity Applications 的安裝 . . . 194
15.7.1 在叢集環境中檢查伺服器的狀態 . . . 194
15.7.2 手動建立資料庫綱要 . . . 195
15.7.3 手動將 Identity Applications 和 Identity Reporting 證書輸入到 Identity Vault 中 . . . 196
15.7.4 記錄萬能金鑰 . . . 196
15.7.5 設定 Identity Applications 的 Identity Vault . . . 196
15.7.6 變更使用者應用程式的預設網路位置名稱 . . . 197
15.7.7 重新設定 Identity Applications 的 WAR 檔案 . . . 199
15.7.8 設定忘記密碼管理功能 . . . 199
15.8 完成 Identity Applications 的設定 . . . 204
15.8.1 執行 Identity Applications 組態公用程式 . . . 204
15.8.2 使用者應用程式參數 . . . 204
15.8.3 Reporting 參數 . . . 214
15.8.4 驗證參數 . . . 215
15.8.5 SSO 用戶端參數 . . . 218
15.8.6 CEF 稽核參數 . . . 222

V 安裝 Identity Reporting 223

16 規劃安裝 Identity Reporting 225

16.1 Identity Reporting 的安裝核對清單 . . . 225
16.2 瞭解 Identity Reporting 各元件的安裝程序 . . . 226
16.3 安裝 Identity Reporting 各元件的先決條件 . . . 226
16.4 Identity Reporting 的身分稽核事件 . . . 227
16.5 Identity Reporting 的系統要求 . . . 228

17 安裝 Identity Reporting 231

17.1 使用引導式程序安裝 Identity Reporting . . . 231
17.2 以靜默模式安裝 Identity Reporting . . . 235
17.3 手動產生資料庫綱要 . . . 236
17.4 連接遠端 Remote PostgreSQL 資料庫 . . . 237

18 設定 Identity Reporting 239

18.1 對 Oracle 資料庫執行報告 . . . 239
18.2 部署 Identity Reporting 的 REST API . . . 239
18.3 連接遠端 Remote PostgreSQL 資料庫 . . . 239

19 管理執行報告所需的驅動程式 241

19.1 設定 Identity Reporting 的驅動程式 . . . 241
19.1.1 安裝 Identity Reporting 的驅動程式套件 . . . 241
19.1.2 設定受管理系統閘道驅動程式 . . . 242
19.1.3 設定資料收集服務的驅動程式 . . . 243
19.1.4 設定 Identity Reporting 以從 Identity Applications 收集資料 . . . 245
19.2 部署並啟動 Identity Reporting 的驅動程式 . . . 246
19.2.1 部署驅動程式 . . . 247
19.2.2 驗證受管理系統是否正在運作中 . . . 247
19.2.3 啟動 Identity Reporting 的驅動程式 . . . 249
19.3 設定執行時期環境 . . . 251
19.3.1 將資料收集服務驅動程式設定為從 Identity Applications 收集資料 . . . 251

19.3.2 移轉資料收集服務驅動程式 . . . 252
19.3.3 新增對自訂屬性和物件的支援 . . . 254
19.3.4 新增多個驅動程式集支援 . . . 256
19.3.5 將驅動程式設定為使用 SSL 在遠端模式下執行 . . . 257
19.4 設定驅動程式的稽核旗標 . . . 258
19.4.1 在 Identity Manager 中設定稽核旗標 . . . 258
19.4.2 在 eDirectory 中設定稽核旗標 . . . 259

VI 安裝 Designer 263

20 規劃安裝 Designer 265

20.1 Designer 安裝核對清單 . . . 265
20.2 安裝 Designer 的先決條件 . . . 266
20.3 Designer 的系統要求 . . . 266

21 安裝 Designer 269

21.1 執行 Windows 可執行檔 . . . 269
21.2 使用靜默安裝程序 . . . 269
21.3 修改包含空格字元的安裝路徑 . . . 270

VII 安裝 Analyzer 271

22 規劃安裝 Analyzer 273

22.1 Analyzer 的安裝核對清單 . . . 273
22.2 安裝 Analyzer 的系統要求 . . . 273

23 安裝 Analyzer 275

23.1 使用精靈安裝 Analyzer . . . 275
23.2 以靜默模式安裝 Analyzer . . . 276
23.3 安裝 Analyzer 的稽核用戶端 . . . 276

VIII 在 Identity Manager 中設定單一登入存取 277

24 準備單一登入存取 279

25 在 Identity Manager 中使用 One SSO Provider 進行單一登入存取 281

25.1 準備 eDirectory 以支援單一登入存取 . . . 281
25.2 修改單一登入存取的基本設定 . . . 281
25.3 將 Self Service Password Reset 設定為信任 OSP . . . 282

26 對 NetIQ Access Manager 使用 SAML 驗證進行單一登入 283

26.1 瞭解協力廠商驗證和單一登入 . . . 283
26.2 建立和安裝 SSL 證書 . . . 283
26.2.1 為 Access Manager 建立 SSL 證書 . . . 284
26.2.2 在 Identity Manager 可信證書儲存區中安裝 Access Manager 證書 . . . 284
26.2.3 在 Access Manager 可信證書儲存區中安裝 SSL 伺服器證書 . . . 285
26.3 將 Identity Manager 設定為信任 Access Manager . . . 285
26.4 將 Access Manager 設定為與 Identity Manager 配合運作 . . . 286

26.4.1 複製 Identity Manager 的中繼資料 286
26.4.2 建立 SAML 的屬性集 286
26.4.3 將 Identity Manager 新增為可信的服務提供者 287
26.5 更新 Access Manager 的登入頁面 287

27 使用 Kerberos 進行單一登入 289

27.1 在 Active Directory 中設定 Kerberos 使用者帳戶 289
27.2 設定 Identity Applications 伺服器 290
27.3 將最終使用者瀏覽器設定為使用整合式 Windows 驗證 292

28 驗證是否可對 Identity Applications 進行單一登入存取 293

29 使用 SSL 進行安全通訊 295

29.1 確保使用 SSL 連接的核對清單 295
29.2 建立金鑰儲存區和證書簽署要求 295
29.3 使用外部 CA 簽署的證書啟用 SSL 297
29.4 使用自行簽署的證書啟用 SSL 298
29.4.1 輸出證書管理中心 298
29.4.2 產生自行簽署的證書 299
29.5 在 Sentinel 與 Identity Manager 元件之間啟用 SSL 300
29.5.1 在 Sentinel 與 Identity Manager 引擎 / 遠端載入器之間啟用 SSL 300
29.5.2 在 Sentinel 與使用者應用程式之間啟用 SSL 302
29.6 更新應用程式伺服器的 SSL 設定 303
29.7 在組態公用程式中更新 SSL 設定 304
29.8 更新 Self Service Password Reset 的 SSL 設定 306

30 安裝後任務 307

30.1 設定已連接系統 307
30.2 建立和設定驅動程式集 307
30.2.1 建立驅動程式集 307
30.2.2 將預設密碼規則指定給驅動程式集 308
30.2.3 在 Identity Vault 中建立密碼規則物件 308
30.2.4 建立自訂密碼規則 309
30.2.5 在 Identity Vault 中建立預設通知集合物件 309
30.3 建立驅動程式 309
30.4 定義規則 310
30.5 管理驅動程式活動 310
30.6 啟用 Identity Manager 310
30.6.1 安裝產品啟用身分證明 310
30.6.2 檢閱 Identity Manager 和驅動程式的產品啟用 311
30.6.3 啟用 Identity Manager 驅動程式 312
30.6.4 啟用特定的 Identity Manager 元件 312

IX 升級 Identity Manager 315

31 升級 Identity Manager 的準備工作 317

31.1 Identity Manager 的升級核對清單 317
31.2 瞭解升級和移轉 319
31.3 升級順序 319
31.4 支援的升級路徑 320
31.4.1 從 Identity Manager 4.6.x 版本升級 320

31.4.2 從 Identity Manager 4.5.x 版本升級 . . . 321
31.5 備份目前組態 . . . 323
31.5.1 輸出 Designer 專案 . . . 323
31.5.2 輸出驅動程式的組態 . . . 324

32 升級 Identity Manager 的元件 327

32.1 升級 Designer . . . 327
32.2 升級 iManager . . . 328
32.2.1 在 Windows 上升級 iManager . . . 328
32.2.2 更新職能服務 . . . 329
32.2.3 重新安裝或移轉 Plug-in Studio 的外掛程式 . . . 330
32.2.4 在升級或重新安裝後更新 iManager 外掛程式 . . . 330
32.3 升級遠端載入器 . . . 331
32.4 升級 Identity Manager 引擎 . . . 331
32.5 升級 Identity Applications 和 Identity Reporting . . . 332
32.5.1 瞭解升級程式 . . . 333
32.5.2 升級的先決條件和注意事項 . . . 333
32.5.3 升級 PostgreSQL 資料庫 . . . 334
32.5.4 系統要求 . . . 336
32.5.5 升級 Identity Applications 的驅動程式套件 . . . 336
32.5.6 使用引導式程序升級 . . . 336
32.5.7 升級後任務 . . . 339
32.6 升級 Identity Reporting . . . 341
32.6.1 升級 Identity Reporting 的驅動程式套件 . . . 342
32.6.2 升級 Identity Reporting . . . 342
32.6.3 變更對資料庫中 reportRunner 的參考 . . . 342
32.6.4 驗證 Identity Reporting 的升級 . . . 343
32.7 升級 Analyzer . . . 343
32.8 升級 Identity Manager 驅動程式 . . . 343
32.8.1 建立新驅動程式 . . . 344
32.8.2 以套件中的內容取代現有內容 . . . 344
32.8.3 保留目前內容並透過套件新增新內容 . . . 344
32.9 將新伺服器新增至驅動程式集 . . . 345
32.9.1 將新伺服器新增至驅動程式集 . . . 345
32.9.2 從驅動程式集移除舊的伺服器 . . . 345
32.10 將自訂規則還原至驅動程式 . . . 346
32.10.1 使用 Designer 將自訂規則還原至驅動程式 . . . 346
32.10.2 使用 iManager 將自訂規則還原至驅動程式 . . . 347

33 從 Advanced Edition 切換到 Standard Edition 349

X 將 Identity Manager 資料移轉至新安裝中 351

34 移轉 Identity Manager 的準備工作 353

34.1 用於執行移轉的核對清單 . . . 353
34.2 在移轉期間停止和啟動 Identity Manager 驅動程式 . . . 354

35 將 Identity Manager 移轉至新伺服器 355

35.1 Identity Manager 的移轉核對清單 . . . 355
35.2 準備用於移轉的 Designer 專案 . . . 356
35.3 複製驅動程式集的伺服器特定資訊 . . . 356
35.3.1 在 Designer 中複製伺服器特定資訊 . . . 357
35.3.2 在 iManager 中變更伺服器特定資訊 . . . 358

35.3.3 變更使用者應用程式的伺服器特定資訊 . . . 358
35.4 將 Identity Manager 引擎移轉至新伺服器 . . . 358
35.5 移轉使用者應用程式驅動程式 . . . 358
35.5.1 輸入新的基礎套件 . . . 359
35.5.2 升級現有的基礎套件 . . . 359
35.5.3 部署移轉的驅動程式 . . . 359
35.6 升級 Identity Applications . . . 360
35.7 完成 Identity Applications 的移轉 . . . 360
35.7.1 衝洗瀏覽器快取 . . . 360
35.7.2 使用舊提供程式或外部提供程式來管理密碼 . . . 360
35.7.3 更新 SharedPagePortlet 的最大逾時設定 . . . 360
35.7.4 停用群組的自動查詢設定 . . . 361

36 解除安裝 Identity Manager 的元件 363

36.1 解除安裝 Identity Vault . . . 363
36.2 從 Identity Vault 中移除物件 . . . 364
36.3 解除安裝 Identity Manager 引擎 . . . 364
36.4 解除安裝遠端載入器 . . . 364
36.5 解除安裝 Identity Applications . . . 365
36.5.1 刪除 Roles Based Provisioning Module 的驅動程式 . . . 365
36.5.2 解除安裝 Identity Applications . . . 365
36.6 解除安裝 Identity Reporting 配件 . . . 365
36.6.1 刪除報告驅動程式 . . . 366
36.6.2 解除安裝 Identity Reporting . . . 366
36.7 解除安裝 Analyzer . . . 366
36.8 解除安裝 iManager . . . 367
36.8.1 在 Windows 上解除安裝 iManager . . . 367
36.8.2 解除安裝 iManager Workstation . . . 367
36.9 解除安裝 Designer . . . 367

37 疑難排解 369

37.1 使用者應用程式和 RBPM 安裝疑難排解 . . . 369
37.2 解除安裝疑難排解 . . . 370
37.3 登入疑難排解 . . . 370
37.4 SSPR 頁面申請錯誤疑難排解 . . . 371

A Windows 上的範例 Identity Manager 叢集部署解決方案 373

A.1 先決條件 . . . 373
A.2 在 eDirectory 叢集上設定 NetIQ Identity Manager . . . 373
A.3 遠端載入器叢集化 . . . 374

B 設定多伺服器環境 375

B.1 修改 eDirectory 網路樹和複本伺服器 . . . 375
B.2 將新網路樹新增至 Identity Vault 中 . . . 375
B.3 將伺服器新增至現有網路樹 . . . 376
B.4 從伺服器中移除 Identity Vault 及其資料庫 . . . 376
B.5 從網路樹中移除 eDirectory 伺服器物件和目錄服務 . . . 376

關於本書和文件庫

本 *《安裝指南》*提供關於安裝 NetIQ Identity Manager (簡稱 Identity Manager) 產品的指示。本指南介紹在分散式環境中安裝個別元件的程序。

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。

關於 NetIQ Corporation

我們是一家全球性企業軟體公司，著重於處理您環境中三個不斷出現的挑戰：變動、複雜性和風險，以及我們可以如何協助您進行控制。

我們的觀點

因應變動及管理複雜性和風險已不是新資訊

事實上，在您所面對的挑戰中，這些或許是最明顯的變數，可控制您是否可以安全地測量、監控及管理您的實體、虛擬和雲端運算環境。

更有效、更快速地啟用重要的業務服務

我們認為對 IT 組織提供最大控制權限，是提供及時服務交付並符合成本效益的唯一方式。隨著組織繼續推動革新，用來進行管理的技術也日益複雜，由變動及複雜性所帶來的壓力只會繼續提高。

經營理念

不只銷售軟體，而是銷售智慧型解決方案

為提供可靠的控制，我們首先務瞭解 IT 組織 (如貴組織) 的實際日常營運情況。這是我們能夠開發出實際的智慧型 IT 解決方案的唯一方式，這些解決方案也已順利產生經過證明且可測量的成效。這比單純銷售軟體更有價值。

協助您成功是我們的目標

我們將您的成就視為我們的業務核心。從產品設計之初到部署，我們深知：您需要與您以前購買的解決方案配合使用且能完美整合的解決方案；您需要在部署後獲得持續的支援並接受後續的訓練；您還需要真正易於合作的夥伴一起應對變化。到了最後，您的成功就是我們的成就。

我們的解決方案

- 身分與存取治理
- 存取管理
- 安全性管理
- 系統與應用程式管理
- 工作量管理
- 服務管理

聯絡銷售支援

若有關於產品、價格及功能等方面的問題，請聯絡當地合作夥伴。如果您無法聯絡合作夥伴，請聯絡我們的銷售支援團隊。

全球：	www.netiq.com/about_netiq/officelocations.asp
美國和加拿大：	1-888-323-6768
電子郵件：	info@netiq.com
網站：	www.netiq.com

聯絡技術支援

若有關於特定產品的問題，請聯絡我們的技術支援團隊。

全球：	www.netiq.com/support/contactinfo.asp
北美與南美：	1-713-418-5555
歐洲、中東和非洲：	+353 (0) 91-782 677
電子郵件：	support@netiq.com
網站：	www.netiq.com/support

聯絡文件支援

我們的目標是提供符合您需求的文件。NetIQ 網站上提供了本產品 HTML 與 PDF 格式的文件，您無需登入即可存取該文件頁面。若您有任何改善文件的建議，請按一下 www.netiq.com/documentation 上張貼之 HTML 版本文件任一頁面底部的**對本主題發表備註**。您也可以將電子郵件寄至 Documentation-Feedback@netiq.com。我們重視您的意見並期待您提出建議。

聯絡線上使用者社群

NetIQ 線上社群 NetIQ Communities 是一個協同網路，將您與同行和 NetIQ 專家聯繫起來。透過提供更多即時的資訊、有用資源的實用連結以及諮詢 NetIQ 專家的管道，NetIQ Communities 協助確保您精通知識，以充分發揮您所仰賴之 IT 投資的全部潛力。如需詳細資訊，請造訪 community.netiq.com。

介紹

NetIQ Identity Manager 可協助您建構智慧型身分管理架構 (無論是在防火牆內還是在雲端中)，來為您的企業提供服務。Identity Manager 會集中管理使用者存取權，並確保從您的實體與虛擬網路到雲端，每個使用者都具有一致的身分。

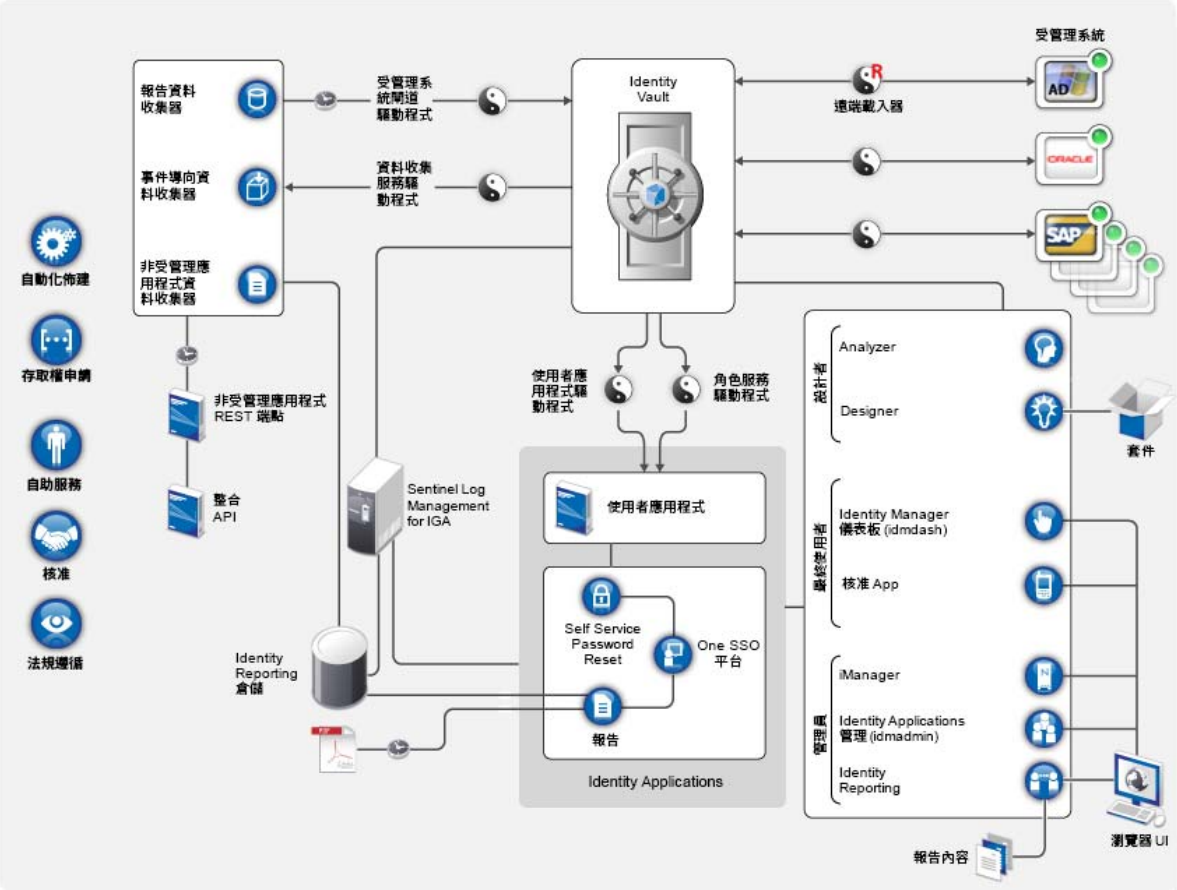
一般而言，您可以將構成 Identity Manager 的各個元件分成下列功能群組：

- 建立和維護 Identity Manager 環境。如需詳細資訊，請參閱第 2 章 「建立和維護 Identity Manager 環境」(第 21 頁)。
- 監控 Identity Manager 環境，包括稽核和報告使用者佈建活動的功能。如此，您便可以證明對業務、IT 及企業規則的遵循狀況。如需詳細資訊，請參閱第 3 章 「在 Identity Manager 環境中管理資料」(第 23 頁)。
- 管理使用者佈建活動，例如個別使用者的角色、證明和自助服務。如需詳細資訊，請參閱第 4 章 「佈建使用者以進行安全的存取」(第 27 頁)。

此部分介紹可協助您執行這些活動的各個 Identity Manager 元件。掌握這些知識之後，您便可以開始規劃產品安裝。若要瞭解這些元件如何是互連的，請參閱第 1 章 「Identity Manager 的元件綜覽」(第 19 頁)。

1 Identity Manager 的元件綜覽

Identity Manager 可確保從您的實體與虛擬網路到雲端，每個使用者都具有一致的身分。下圖顯示了支援 Identity Manager 功能的各元件的高層級檢視窗。其中的部分元件可安裝在同一個伺服器上，具體視您身分管理解決方案的大小而定。不過，某些元件 (例如 Identity Applications) 提供基於瀏覽器的介面，供使用者從工作站或行動平台存取。



在 Identity Manager 中，**受管理系統** (也稱為**已連接系統**或**應用程式**) 指任何您要管理身分資訊的系統、目錄、資料庫或作業系統。例如，連接的系統可以是 PeopleSoft 應用程式或 LDAP 目錄。**驅動程式** (例如資料收集服務驅動程式) 提供受管理系統與 Identity Vault 之間的連接。它還可以在各系統之間啟用資料同步和共享。Identity Manager 將驅動程式和程式庫物件儲存在稱為**驅動程式集**的容器中。

2 建立和維護 Identity Manager 環境

大多數組織使用單獨的環境來開發和調整 Identity Manager，然後再將其部署到線上環境。若要建立和維護 Identity Manager 環境，您可以使用下列 Identity Manager 元件：

- 第 2.1 節「Designer for Identity Manager」(第 21 頁)
- 第 2.2 節「Analyzer for Identity Manager」(第 21 頁)
- 第 2.3 節「iManager」(第 22 頁)

這些元件還可以協助您調整 Identity Manager，以符合業務不斷變更的需要，從而確保業務持續運作，並提高整個企業的使用者生產力。

2.1 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。

如需使用 Designer 的詳細資訊，請參閱 《*NetIQ Designer for Identity Manager Administration Guide*》(NetIQ Designer for Identity Manager 管理指南)。

2.2 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。

如需使用 Analyzer 的詳細資訊，請參閱 《*NetIQ Analyzer for Identity Manager Administration Guide*》(NetIQ Analyzer for Identity Manager 管理指南)。

2.3 iManager

NetIQ iManager 是一款基於瀏覽器的工具，提供許多 Novell 及 NetIQ 產品 (包括 Identity Manager) 的單一管理點。安裝 iManager 的 Identity Manager 外掛程式之後，您便可以管理 Identity Manager，並接收 Identity Manager 系統的即時健康和狀態資訊。

使用 iManager，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 iManager 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 iManager 的詳細資訊，請參閱 *《NetIQ iManager Administration Guide》*(NetIQ iManager 管理指南)。

3 在 Identity Manager 環境中管理資料

Identity Manager 在實體、虛擬和雲端網路之間實施一致的存取控制，並使用可讓您證明法規遵循的動態報告。基本上，Identity Manager 可同步化儲存在所連接應用程式或 Identity Vault 中任何類型的資料。Identity Manager 解決方案的下列元件可提供資料同步，包括密碼同步：

- Identity Vault
- Identity Manager 引擎
- Identity Manager 遠端載入器
- Identity Reporting
- Identity Manager 驅動程式
- 已連接系統

3.1 瞭解資料同步

Identity Manager 可讓您在多種連接的系統 (例如 SAP、PeopleSoft、Microsoft SharePoint、Lotus Notes、Microsoft Exchange、Microsoft Active Directory、NetIQ eDirectory 與 LDAP 目錄) 之間同步化、轉換及配送資訊。Identity Manager 可讓您執行下列活動：

- 控制連接的系統之間的資料流程。
- 決定共享哪些資料、哪個系統是某項資料的管理來源，以及如何解譯和轉換資料來符合其他系統的要求。
- 在各系統之間同步化密碼。例如，如果使用者在 Active Directory 中變更自己的密碼，Identity Manager 可以將這個密碼同步至 Lotus Notes 和 Linux。
- 在各目錄 (例如 Active Directory) 以及系統 (例如 PeopleSoft 與 Lotus Notes) 中建立新使用者帳戶及移除現有的帳戶。例如，當您將新員工新增至 SAP HR 系統時，Identity Manager 可以自動在 Active Directory 中建立新的使用者帳戶，並在 Lotus Notes 中建立新帳戶。

3.2 瞭解稽核、報告及法規遵循

如果沒有 Identity Manager，提供使用者就會變成一項繁重、費時又浪費成本的工作。然後，您必須驗證佈建活動符合組織的規則、要求和規定。每個人是否都適得其所，能夠存取正確的資源嗎？您是否確定未經授權的人員無法存取這些資源？昨天到職的員工能夠存取網路、電子郵件及工作所需的其他系統嗎？是否已把上星期離職員工的存取取消？

有了 Identity Manager，您就輕鬆多了，因為您的所有使用者佈建活動 (過去與現在的) 都會被追蹤並記錄下來，以備隨時稽核。透過查詢身分資訊倉儲，您可以擷取確定您所在組織完全遵守相關商業法律與法規所需的所有資訊。

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

3.3 瞭解用於同步化身分資料的元件

- 第 3.3.1 節「Identity Vault」(第 24 頁)
- 第 3.3.2 節「Identity Manager 引擎」(第 24 頁)
- 第 3.3.3 節「遠端載入器」(第 24 頁)
- 第 3.3.4 節「Identity Reporting」(第 24 頁)

3.3.1 Identity Vault

Identity Vault 包含 Identity Manager 需要的所有資訊。Identity Vault 充當要在各個連接的系統之間同步化之資料的 Metadirectory。例如，從 PeopleSoft 系統同步至 Lotus Notes 的資料會先新增至 Identity Vault，然後再傳送至 Lotus Notes 系統。Identity Vault 還會儲存特定於 Identity Manager 的資訊，例如驅動程式組態、參數和規則。

Identity Vault 使用 NetIQ eDirectory 資料庫。如需關於使用 eDirectory 的詳細資訊，請參閱 《NetIQ eDirectory 9.1 Administration Guide》 (NetIQ eDirectory 8.8 管理指南)。

3.3.2 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。對於 Identity Vault 中發生的事件，引擎會處理變更，並透過驅動程式發出指令給應用程式。對於應用程式中發生的事件，引擎會接收驅動程式送來的變更、處理變更，然後發出指令給 Identity Vault。**驅動程式** 可將 Identity Manager 引擎連接至多個應用程式。驅動程式有兩項基本責任：將應用程式中的資料變更 (事件) 報告給 Identity Manager 引擎；將 Identity Manager 引擎提交的資料變更 (指令) 貫徹到應用程式。驅動程式必須安裝在連接的應用程式所在的伺服器上。

Identity Manager 引擎也稱為 Metadirectory 引擎。用來執行 Identity Manager 引擎的伺服器稱為 **Identity Manager 伺服器**。您的環境中可以有多個 Identity Manager 伺服器，具體視伺服器工作負載而定。

3.3.3 遠端載入器

Identity Manager 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，請參閱第 10.1.2 節「瞭解遠端載入器」(第 86 頁)。

3.3.4 Identity Reporting

Identity Manager 中包含 **身分資訊倉儲**，後者是用於儲存組織中 Identity Vault 與所連接系統實際和預期狀態相關資訊的智慧型儲存庫。身分資訊倉儲可提供的資訊供您查看授權過去和目前的狀態，以及為組織中各個身分授予的許可權，從而讓您全方位瞭解您的企業授權。

在查詢身分資訊倉儲時，您可以擷取確定您所在組織完全遵守相關商業法律與法規所需的所有資訊。具備了這些知識，您甚至可以回答最為複雜的組織治理、風險管理及法規遵循 (GRC) 方面的查詢。

身分資訊倉儲的基礎架構需要使用下列元件：

- 「Identity Manager 的 Identity Reporting」(第 25 頁)
- 「資料收集服務」(第 25 頁)
- 「受管理系統閘道驅動程式」(第 25 頁)

Identity Manager 的 Identity Reporting

身分資訊倉儲將其資訊儲存在 Sentinel Log Management for IGA 的 SIEM 資料庫中。**Identity Reporting** 元件可讓您稽核和建立有關 Identity Manager 解決方案的報告。您可以使用這些報告來確保符合貴企業的法規遵循規定。您可以執行預先定義的報告，以證明對業務、IT 及企業規則的遵循狀況。如果預先定義的報告不符合您的需要，您也可以建立自訂報告。使用 Identity Reporting 可報告有關 Identity Manager 組態各方面的重要業務資訊，包括從 Identity Vault 和連接的系統收集而來的資訊。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)。

資料收集服務

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

受管理系統閘道驅動程式

受管理系統閘道驅動程式會查詢 Identity Vault，以便從受管理系統中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

4 佈建使用者以進行安全的存取

Identity Manager 會集中管理存取權，並確保從您的實體與虛擬網路到雲端，每個使用者都具有一致的身分。此外，使用者通常需要依據自己在組織內的角色來存取資源。例如，法律事務所的律師需要存取的資源，可能就與助理不一樣。

Identity Manager 可讓您根據使用者在組織裡的角色來提供使用者。您應該根據組織的需求來定義角色和進行指定。指定角色給使用者時，Identity Manager 就會將此角色關聯的資源存取權提供給使用者。具有多個角色的使用者會得到與所有角色所關聯之資源的存取權。

您可以讓使用者因組織中發生的事件而自動新增至某些角色。例如，您可以將職稱為「律師」的新使用者新增至 SAP HR 資料庫。如果需要核准才能將使用者新增至某個角色，您可以建立工作流程，將角色申請呈報給適當的核准人。您也可以手動指定使用者的角色。

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

Identity Manager 解決方案提供了下列元件用來佈建使用者：

- Identity Manager 儀表板
- Identity Applications 管理
- 使用者應用程式

儀表板為所有 Identity Manager 使用者和管理員提供了單一存取點。在儀表板中可以存取所有現有的使用者應用程式功能。從 Identity Manager 4.7 版開始，儀表板取代了 Identity Manager 首頁和佈建儀表板。

4.1 瞭解 Identity Manager 中的證明程序

Identity Manager 可透過證明程序，協助您驗證角色指定的正確性。不正確的角色指定可能會導致違背企業與政府法規的規定。組織內的負責人員可以透過證明程序來證明與角色關聯的資料：

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

這些證明報告主要用於協助您確定角色指定正確，以及允許存在衝突角色的例外情況具有正當理由。

4.2 瞭解 Identity Manager 中的自助服務程序

Identity Manager 以身分為基礎來為使用者授予對各系統、應用程式和資料庫的存取權。每個使用者的唯一識別碼及角色定義了對身分資料的特定存取權限。例如，身分是主管的使用者可以存取其直屬下屬的薪資資訊，但不能存取組織中其他員工的薪資資訊。透過 Identity Manager，您可以將管理職務委託給應負責的人。例如，您可讓個別使用者具有實現下列目標的能力：

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

除了使用者個人的自助服務以外，對於負責輔助、監看和核准使用者申請的職掌工作 (管理、「服務台」等等)，Identity Manager 還提供自助服務管理。例如，John 使用 Identity Manager 自助服務功能來申請存取他需要的文件。John 的主管和財務長透過自助服務功能收到了申請，並且可以核准該申請。已建立的核准工作流程可讓 John 啟始並監看他的申請進度，也可讓 John 的主管和財務長回應他的申請。John 的主管和財務長核准申請後，觸發了系統佈建 John 存取和檢視財務文件所需的 Active Directory 權限。

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

您可以讓工作流程在某個事件發生 (例如，有新的使用者新增至您的 HR 系統) 時自動啟動，也可以透過使用者申請來手動啟動。為了確保適時進行核准，您可以設定代理核准人和核准小組。

4.3 瞭解管理使用者佈建的元件

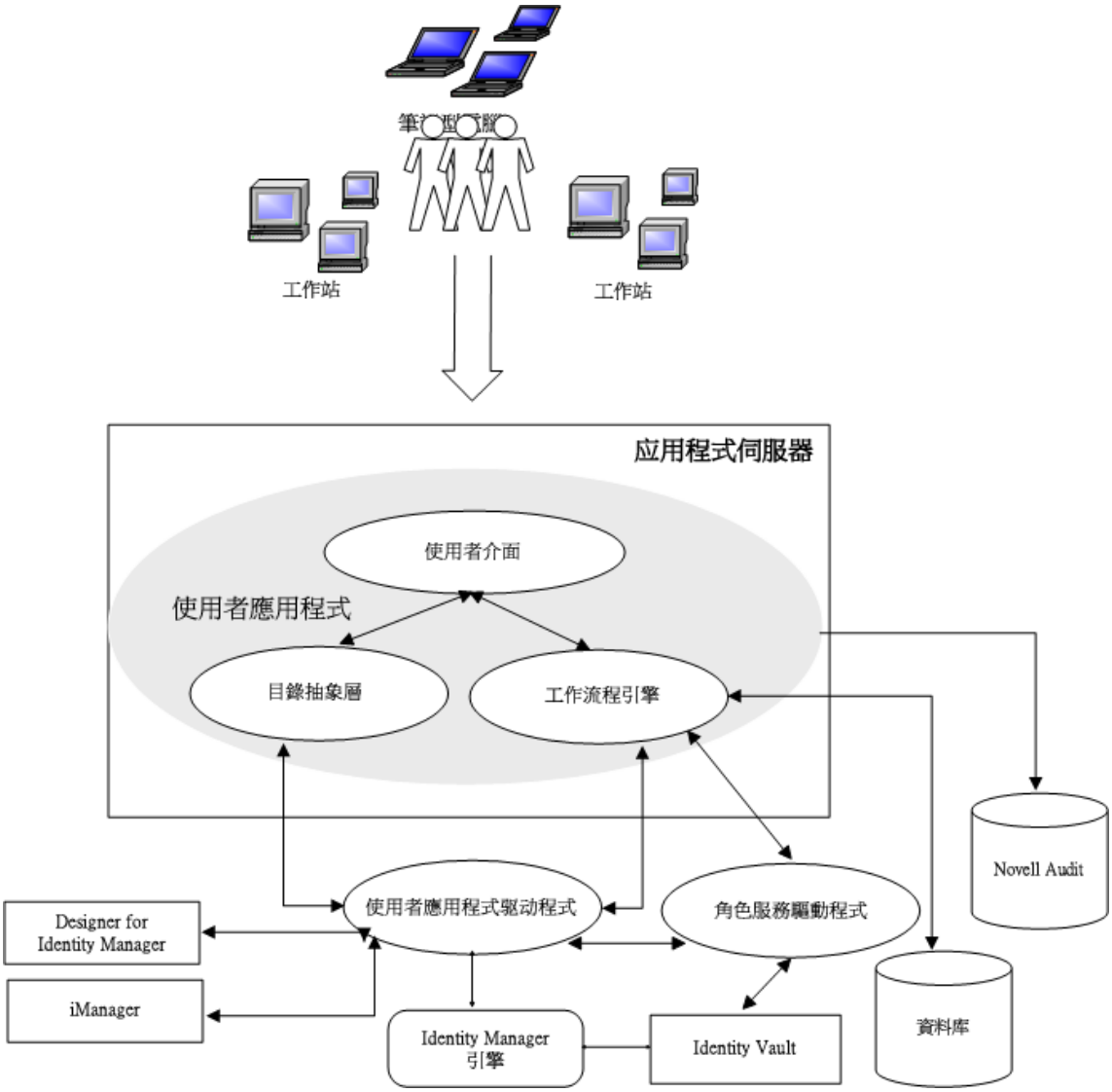
本節說明下列元件的用途：

- 第 4.3.1 節「使用者應用程式和 Roles Based Provisioning Module」(第 29 頁)
- 第 4.3.2 節「Identity Applications 管理」(第 30 頁)
- 第 4.3.3 節「Identity Manager 儀表板」(第 30 頁)

4.3.1 使用者應用程式和 Roles Based Provisioning Module

Identity Manager **使用者應用程式**可讓您的使用者和業務管理員瞭解 Identity Manager 的資訊、資源和功能。使用者應用程式是基於瀏覽器的 Web 應用程式，可讓使用者執行多種身分自助服務和角色佈建任務。使用者可以管理密碼與身分資料，啟始和監控佈建與角色指定申請，管理佈建申請的核准程序，以及驗證證明報告。

使用者應用程式依賴於許多共同執行的獨立元件運作。



使用者應用程式在 **Roles Based Provisioning Module** (RBPM) 架構上執行，該架構包括一個工作流程引擎，用於透過適當的核准程序控制申請的呈報。這些元件需要下列驅動程式：

使用者應用程式驅動程式

儲存組態資訊，以及在每次 Identity Vault 中發生變更時通知使用者應用程式。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

管理所有角色和資源指定。該驅動程式可啟動相應工作流程來處理需要核准的角色和資源指定申請，以及根據群組和容器成員資格維護間接的角色指定。該驅動程式還可依據使用者的角色成員資格為其授予和撤銷授權。它會對已完成的申請執行清理程序。

使用者可以從任何受支援的網頁瀏覽器存取使用者應用程式。如需使用者應用程式和 RBPM 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)。

4.3.2 Identity Applications 管理

在 **Identity Applications 管理**介面中可以使用相應的管理員角色管理以下任務：

- 建立和管理角色、資源及其指定
- 設定職務分離 (SoD) 條件約束，以免系統中的兩個不同角色之間發生衝突
- 設定允許使用者透過電子郵件核准許可權申請的功能
- 設定 Identity Applications 組成部分 (例如角色、資源和委託) 的預設設定。

管理員可以從電腦或平板電腦上使用任何受支援的網頁瀏覽器來存取「管理」頁面。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)。

4.3.3 Identity Manager 儀表板

Identity Manager 儀表板 (簡稱「儀表板」) 中包含了每個使用者的許可權、任務和申請的個人化檢視窗。它有助於讓使用者著重關注以下幾個基本方面的功能：

我需要某些項目。

如果使用者需要某個項目，無論該項目是筆記型電腦之類的某個設備，還是對特定伺服器或應用程式的存取權之類的無形項目，您都可以申請該項目。

我需要執行某個動作。

如果想要知道自己需要管理的任務，可以使用我的任務頁面顯示 Identity Manager 系統中您所有的待核准或待佈建任務。

我擁有哪些項目？

如果想要查看您目前的許可權，可以使用我的許可權頁面顯示您有權存取的角色和資源清單。

我是如何獲取的？

如果想要查看過往申請的清單，可以使用申請歷程頁面顯示您最近申請的每個項目，以及您的等待中申請的狀態。

如果您具有 Identity Applications 的管理角色，則可以在儀表板中針對所有使用者自訂應用程式頁面。您可以對頁面進行設定，以顯示您的使用者需要看到的項目和連結，並將其組織成適合您企業的類別。您可以包括以下幾種類型的項目：

- Identity Manager 功能，例如建立群組或執行報告
- 大部分使用者都需要申請的許可權
- 指向經常存取的網站或 Web 應用程式的連結

- REST 端點
- 徽章，例如使用者可以存取的特定類型的項目數

使用者可以從電腦或平板電腦上使用任何受支援的網頁瀏覽器來存取儀表板。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)。

4.4 使用 Identity Manager 中的自助式密碼管理

Identity Manager 中包含 NetIQ Self Service Password Reset (SSPR)，以協助可存取 Identity Applications 的使用者重設其密碼，而無需管理人員介入。當您安裝或升級到 Identity Manager 的最新版本時，安裝程序預設會啟用 SSPR。在新安裝中，SSPR 會使用專屬通訊協定來管理驗證方法。不過，在升級之後，您可以指示 SSPR 使用 Identity Manager 慣常用於其舊密碼管理程式的 NetIQ Modular Authentication Services (NMAS)。

根據您是否要使用複雜的密碼管理，您可以設定下列其中一個提供程式：

SSPR

NetIQ Self Service Password Reset 是您安裝或升級 Identity Manager 時的預設選項。如需詳細資訊，請參閱第 4.4.1 節「瞭解預設自助服務程序」(第 31 頁)。

舊密碼管理提供程式

使用 Identity Manager 4.0.2 中的密碼管理程序，它支援使用多個密碼規則。如需詳細資訊，請參閱第 4.4.2 節「瞭解舊密碼管理提供程式」(第 32 頁)。

協力廠商密碼管理提供程式

您可以使用協力廠商程式來管理忘記的密碼。您需要修改 Identity Manager 的某些組態設定。如需詳細資訊，請參閱「使用外部系統進行忘記密碼管理」(第 202 頁)。

4.4.1 瞭解預設自助服務程序

SSPR 自動與 Identity Applications 和 Identity Reporting 的單一登入程序整合。它是 Identity Manager 的預設密碼管理程式，即使您未安裝 SSPR 也是如此。當使用者申請重設密碼時，SSPR 需要使用者回答處理安全回應問題。如果答案正確，SSPR 便會以下列其中一種方式回應：

- 允許使用者建立新密碼
- 建立新密碼並將它傳送給使用者
- 建立新密碼並將它傳送給使用者，同時將舊密碼標記為已過期。

您可在 SSPR 組態編輯器中設定此回應。升級至 Identity Manager 的新版本之後，您可以將 SSPR 設定為使用 Identity Manager 慣常用來進行密碼管理的 NMAS 方法。不過，SSPR 不能辨識您用來管理忘記之密碼的現有密碼規則。若要繼續使用您的規則，請參閱第 4.4.2 節「瞭解舊密碼管理提供程式」(第 32 頁)。

您也可以將 SSPR 設定為使用其專屬通訊協定而不是 NMAS。進行此變更後，若要恢復為使用 NMAS，將只能透過重設密碼規則來實現。

若需要更多相關資訊 ...	請參閱 ...
安裝 SSPR	第 14.2 章「為 Identity Manager 安裝密碼管理功能」(第 157 頁)
設定 Identity Applications 的密碼管理	「使用 Self Service Password Reset 進行忘記密碼管理」(第 199 頁)
管理和設定 SSPR	*《NetIQ Self Service Password Reset Administration Guide》*(NetIQ Self Service Password Reset 管理指南)

4.4.2 瞭解舊密碼管理提供程式

附註：此版本廢棄了使用者應用程式的舊密碼自助服務功能。NetIQ 強烈建議您開始使用 SSPR 來執行所有密碼特定的任務。安裝程序預設會啟用 SSPR。如需詳細資訊，請參閱第 4.2 節「瞭解 Identity Manager 中的自助服務程序」(第 28 頁)。

如果您從 Identity Manager 的較舊版本升級，Identity Applications 預設使用 SSPR 做為密碼管理程式。SSPR 可以使用 Identity Manager 慣常用來進行密碼管理的 NMAS 方法。不過，SSPR 不能辨識您用來管理忘記之密碼的現有密碼規則。您可以略過 SSPR，使用舊密碼管理提供程式。

當使用者申請密碼重設時，舊提供程式會將使用者的身分證明與您設定的密碼規則進行比較。例如，它可能需要使用者回答處理安全回應問題。根據套用於該使用者的規則，程式會以下列其中一種方式回應：

- 重設密碼
- 顯示密碼提示
- 透過電子郵件將密碼提示傳送給使用者
- 透過電子郵件將新密碼傳送給使用者

如果您的企業使用多個或複雜的密碼規則，請使用舊提供程式。例如，您的密碼規則基於使用者角色運作。實習醫生可能只需要自動產生的密碼，而不需要提供處理安全回應；而對於可以存取安全資料的主管，您可能有更嚴格的要求。此使用者可能需要定期重設密碼。對於這兩個案例，您都希望使用者自助完成密碼申請。

若要使用舊提供程式，請在安裝或升級 Identity Manager 之後修改 Identity Applications 的組態設定。升級之後，您將不需要重新設定密碼規則。

若需要更多相關資訊 ...	請參閱 ...
將 Identity Manager 設定為使用舊提供程式	「使用舊提供程式進行忘記密碼管理」(第 201 頁)
使用舊提供程式進行密碼管理	*《NetIQ Identity Manager Password Management Guide》*(NetIQ Identity Manager 密碼管理指南)

4.5 在 Identity Manager 中使用單一登入存取

為了提供單一登入存取 (SSO)，Identity Manager 使用了驗證服務 NetIQ One SSO Provider (OSP)。您必須對下列元件使用 OSP ：

- Identity Applications 管理
- Identity Manager 儀表板
- Identity Reporting
- Self-Service Password Reset
- 使用者應用程式

Identity Manager 安裝程式的 .iso 影像提供安裝 OSP 的途徑。如需安裝 OSP 的詳細資訊，請參閱第 14.2 章 「為 Identity Manager 安裝密碼管理功能」(第 157 頁)。

4.5.1 瞭解使用 One SSO Provider 進行驗證的方法

OSP 支援 OAuth2 規格，需要使用 LDAP 驗證伺服器。依預設，Identity Manager 使用 Identity Vault (eDirectory)。OSP 可以與其他類型的**驗證來源**或 **Identity Vault** 通訊，以處理驗證申請。您可以設定要讓 OSP 使用的驗證類型： userID 和密碼、Kerberos 或 SAML。不過，OSP 不支援 MIT 樣式的 Kerberos 或 SAP 登入票證。

OSP 和 SSO 如何運作？

如果您使用 Identity Vault 做為驗證服務，並且 Identity Vault 中的指定容器具有 CN 和密碼，則授權使用者在 Identity Manager 安裝好後便可立即登入其中。如果沒有這些登入帳戶，則只有安裝期間指定的管理員可以立即登入。

當使用者登入其中一個基於瀏覽器的元件時，程序會將使用者的名稱 / 密碼配對重新導向至 OSP 服務，該服務隨即會查詢驗證伺服器。伺服器會驗證使用者身分證明。隨後，OSP 將 OAuth2 存取記號發給該元件和瀏覽器。瀏覽器在使用者的工作階段期間使用該記號來提供對任何基於瀏覽器之元件的 SSO 存取權。

如果您使用 Kerberos 或 SAML，OSP 會接受來自 Kerberos 票證伺服器或 SAML IDP 的驗證，然後將 OAuth2 存取記號核發給使用者所登入的元件。

OSP 如何與 Kerberos 配合工作？

OSP 和 Kerberos 可確保使用者能夠登入系統一次，以便使用其中一個 Identity Applications 及 Identity Reporting 建立工作階段。如果使用者的工作階段逾時，授權會自動進行，無需使用者介入。每次登出之後，使用者都應關閉瀏覽器，以確保其工作階段結束。否則，應用程式會將使用者重新導向至登入視窗，並且 OSP 會重新授權該使用者工作階段。

如何設定驗證和單一登入存取？

若要讓 OSP 與 SSO 正常運作，您必須安裝 OSP。然後指定用戶端用於存取每個元件的 URL、將驗證申請重新導向至 OSP 的 URL，以及驗證伺服器的設定。您可以在安裝期間或安裝之後使用 RBPM 組態公用程式提供此資訊。您還可以指定 Kerberos 票證伺服器或 SAML IDP 的設定。

如需設定驗證和單一登入存取的詳細資訊，請參閱第 VIII 部分 「在 Identity Manager 中設定單一登入存取」(第 277 頁)。

在叢集中，所有叢集成員的組態設定都必須相同。

4.5.2 瞭解 One SSO Provider 的金鑰儲存區

Identity Manager 使用支援在 OSP 服務與驗證伺服器之間進行 http 和 https 通訊的金鑰儲存區。金鑰儲存區是在您安裝 OSP 時建立的。您也可以建立一個密碼，供 OSP 服務用於與驗證伺服器進行授權互動。如需詳細資訊，請參閱第 14.2 章 「為 Identity Manager 安裝密碼管理功能」(第 157 頁)。

4.5.3 瞭解 One SSO Provider 的稽核事件

OSP 會產生單個事件，來說明使用者何時登入或登出使用者應用程式或 Identity Reporting ：

- 003E0204 (登入)
- 003E0201 (登出)

然後，XDAS 分類法會將這些 OSP 事件解譯為登入 / 登出或 SOAP 呼叫使用者應用程式成功，或是「不成功」。

規劃安裝 Identity Manager

此部分提供關於規劃 Identity Manager 環境的實用資訊。若要瞭解安裝 Identity Manager 各元件的電腦所需符合的先決條件和系統要求，請參閱相關元件的安裝章節。

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。

- 第 5 章 「規劃綜覽」(第 37 頁)
- 第 6 章 「安裝注意事項」(第 45 頁)

5 規劃綜覽

本章的內容可協助您規劃 Identity Manager 的安裝程序。有些元件必須依特定的順序安裝，因為安裝程序需要存取先前安裝的元件。例如，您應該先安裝並設定 Identity Vault，然後再安裝 Identity Manager 引擎。

- 第 5.1 節「規劃核對清單」(第 37 頁)
- 第 5.2 節「瞭解安裝程序」(第 38 頁)
- 第 5.3 節「建議的安裝情境和伺服器設定」(第 39 頁)
- 第 5.4 節「瞭解授權和啟用」(第 42 頁)
- 第 5.5 節「下載安裝檔案」(第 43 頁)
- 第 5.6 節「尋找可執行檔和預設安裝路徑」(第 43 頁)

5.1 規劃核對清單

下面的核對清單提供了在環境中規劃安裝 Identity Manager 的概要步驟。關於安裝 Identity Manager 各元件的章節提供了更具體的核對清單。

	核對清單項目
❑	1. 檢閱產品架構資訊，以瞭解 Identity Manager 的元件。如需詳細資訊，請參閱第 I 部分「介紹」(第 17 頁)。
❑	2. 確定要使用的安裝程式類型。如需詳細資訊，請參閱第 5.2 節「瞭解安裝程序」(第 38 頁)。
❑	3. 確定最適合欲安裝產品的作業系統平台。如需詳細資訊，請參閱第 5.3.5 節「選取 Identity Manager 的作業系統平台」(第 41 頁)。 **附註：**Identity Manager 僅支援在 Linux 伺服器上安裝 Sentinel Log Management for Identity Governance and Administration (Sentinel Log Management for IGA)。如果要在您的環境中使用 Sentinel Log Management for IGA，請參閱《*NetIQ Identity Manager 安裝指南 - Linux*》中的「安裝 Sentinel Log Management for Identity Governance and Administration」，瞭解此安裝所需的先決條件和系統設定。不過，如果您的身分解決方案僅在 Windows 上執行，您可以使用其他稽核服務。
❑	4. 確定元件的安裝順序，以及每個元件的安裝位置。如需詳細資訊，請參閱第 5.3 節「建議的安裝情境和伺服器設定」(第 39 頁)。
❑	5. 確保您已獲得執行 Identity Manager 的授權。如需詳細資訊，請參閱第 5.4 節「瞭解授權和啟用」(第 42 頁)。
❑	6. 檢閱每個 Identity Manager 元件的預設連接埠，以確定是否需要自訂安裝設定。如需詳細資訊，請參閱第 6.1 節「瞭解 Identity Manager 通訊」(第 45 頁)。
❑	7. 確定您是否能以偏好的語言執行安裝程式。如需詳細資訊，請參閱第 6.2 節「瞭解語言支援」(第 46 頁)。

	核對清單項目
❑	8. 確保您有 Identity Manager 的安裝檔案。如需詳細資訊，請參閱第 5.5 節「下載安裝檔案」(第 43 頁)。 **重要：**為了順利安裝，請勿在安裝 Identity Manager 元件時執行任何需要大量 CPU 的應用程式。您必須在開始 Identity Manager 安裝前停止 Windows 模組安裝程式和 Windows 更新等 Windows 服務，並且僅當完成安裝後方可啟動這些服務。
❑	9. (視情況而定) 若要在叢集中安裝 Identity Manager，請確保您的環境符合要求。如需詳細資訊，請參閱第 6.3 節「確保 Identity Manager 的高可用性」(第 47 頁)。
❑	10. 確保您擁有在伺服器上安裝 Identity Manager 各元件所需的相應身分證明，以及在安裝期間可能建立的帳戶。
❑	11. 確保安裝 Identity Manager 各元件的電腦符合指定的要求。如需詳細資訊，請參閱以下各節： ◆ **Designer**：「規劃安裝 Designer」(第 265 頁) ◆ **用於管理角色和資源的 Identity Applications**：「規劃安裝 Identity Applications」(第 165 頁) ◆ **Identity Manager 引擎**：「規劃安裝引擎、驅動程式和外掛程式」(第 73 頁) ◆ **Identity Vault**：「安裝 Identity Vault」(第 51 頁) ◆ **iManager**：(選擇性)「規劃安裝 iManager」(第 125 頁) ◆ **密碼重設 (SSPR)**：「為 Identity Manager 規劃安裝密碼管理功能」(第 155 頁) ◆ **PostgreSQL**：「規劃安裝 PostgreSQL 和 Tomcat」(第 141 頁) ◆ **遠端載入器**：「規劃安裝引擎、驅動程式和外掛程式」(第 73 頁) ◆ **報告**：「規劃安裝 Identity Reporting」(第 225 頁) ◆ **單一登入存取 (OSP)**：「為 Identity Manager 規劃安裝密碼管理功能」(第 155 頁) ◆ **Tomcat**：「規劃安裝 PostgreSQL 和 Tomcat」(第 141 頁) **附註：**NetIQ 建議您記下在安裝期間建立的每個帳戶。
❑	12. 啟用 Identity Manager 的元件。如需詳細資訊，請參閱第 30.6 節「啟用 Identity Manager」(第 310 頁)。

5.2 瞭解安裝程序

NetIQ 提供了 Identity Manager 元件的獨立安裝程式，讓您可以更靈活地設定環境。例如，許多 Identity Manager 元件都屬於資料密集型 (如 Identity Vault)，應安裝在獨立的伺服器上。

獨立安裝程序提供以下功能：

- 允許您自訂元件設定，包括 Identity Vault 中的樹狀結構
- 允許您在分散式和叢集環境中安裝
- 允許您選取驅動程式，並建立想要新增至身分管理解決方案中的驅動程式集
- 允許您選取想要新增至身分管理解決方案中的 iManager 外掛程式
- 允許您使用非管理員帳戶安裝某些元件
- 支援多種資料庫平台
- 針對所有受支援的作業系統使用 Apache Tomcat

- 建立支援的線上環境
- 可用於升級先前版本的 Identity Manager

為獲得最佳效果，請依照身分管理解決方案指定的順序執行獨立安裝程式。如需詳細資訊，請參閱第 5.3 節「建議的安裝情境和伺服器設定」(第 39 頁)。

5.3 建議的安裝情境和伺服器設定

執行獨立安裝時，您應依照特定的順序在特定伺服器上安裝元件。某些元件的安裝程式需要使用先前所安裝元件的相關資訊。

本節的內容可協助您根據特定的稽核和報告情境，確定安裝順序和伺服器類型。

- 第 5.3.1 節「將事件傳送到稽核服務，而不在 Identity Manager 中報告」(第 39 頁)
- 第 5.3.2 節「將事件傳送到 Identity Manager 並產生報告」(第 40 頁)
- 第 5.3.3 節「在將事件推入 Identity Manager 前先將其傳送至外部服務」(第 40 頁)
- 第 5.3.4 節「建議的伺服器設定」(第 41 頁)
- 第 5.3.5 節「選取 Identity Manager 的作業系統平台」(第 41 頁)

5.3.1 將事件傳送到稽核服務，而不在 Identity Manager 中報告

在此情境中，您計劃使用 Sentinel 來稽核 Identity Manager 中發生的事件，不打算在 Identity Manager 中產生報告。請依照以下順序安裝元件：

1. Sentinel Log Management for IGA (在 Windows 上不受支援)

   附註：NetIQ 僅支援在 Linux 伺服器上安裝此元件。如需安裝說明，請參閱《*NetIQ Identity Manager Setup Guide for Linux*》(NetIQ Identity Manager 安裝指南 - Linux)。不過，如果您的身分解決方案僅在 Windows 上執行，您可以使用其他稽核服務。

2. Identity Vault
3. Identity Manager 引擎、驅動程式和 iManager 外掛程式
4. (選擇性) iManager
5. Designer
6. Tomcat 和 PostgreSQL
7. OSP
8. SSPR
9. Identity Applications
10. (選擇性) Analyzer

5.3.2 將事件傳送到 Identity Manager 並產生報告

在此情境中，您計劃使用 Identity Manager 隨附的 Sentinel Log Management for IGA 來稽核 Identity Manager。您可能還會針對這些事件產生報告。請依照以下順序安裝元件：

1. Identity Vault
2. Sentinel Log Management for IGA (在 Windows 上不受支援)

   附註：NetIQ 僅支援在 Linux 伺服器上安裝此元件。如需安裝說明，請參閱 《*NetIQ Identity Manager Setup Guide for Linux*》 (NetIQ Identity Manager 安裝指南 - Linux)。不過，如果您的身分解決方案僅在 Windows 上執行，您可以使用其他稽核服務。

3. Identity Manager 引擎、驅動程式和 iManager 外掛程式
4. (選擇性) iManager
5. Designer
6. Tomcat 和 PostgreSQL
7. OSP
8. SSPR
9. Identity Applications
10. Identity Reporting
11. (選擇性) Analyzer

5.3.3 在將事件推入 Identity Manager 前先將其傳送至外部服務

此此情境中，您計劃使用某個服務 (例如 Sentinel) 來稽核 Identity Manager。請依照以下順序安裝元件：

1. 外部稽核服務，例如 Sentinel
2. Identity Vault
3. Identity Manager 引擎、驅動程式和 iManager 外掛程式
4. (選擇性) iManager
5. Designer
6. Tomcat 和 PostgreSQL
7. OSP
8. SSPR
9. Identity Applications
10. Identity Reporting
11. (選擇性) Analyzer

5.3.4 建議的伺服器設定

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
伺服器 1 和 2 (雙伺服器目錄複本)	◆ Identity Vault ◆ Identity Manager 引擎
伺服器 3 和 4 (雙伺服器叢集)	◆ Identity Applications ◆ iManager ◆ One SSO Provider ◆ 遠端載入器 ◆ Self Service Password Reset **附註：**NetIQ 建議您將 Identity Applications 和 One SSO Provider 安裝在同一部伺服器上。
伺服器 5 (或伺服器叢集)	Identity Manager 資料庫： ◆ Identity Applications ◆ Identity Reporting
伺服器 6	Identity Reporting
伺服器 7	Sentinel Log Management for IGA
用戶端工作站 (1 個以上)	◆ Designer ◆ iManager Workstation ◆ 可存取 Identity Applications 和報告功能的網際網路瀏覽器

5.3.5 選取 Identity Manager 的作業系統平台

您可以在各種作業系統平台上安裝 Identity Manager 的元件。下表可協助您確定需要為身分管理解決方案使用哪些伺服器。

平台	元件
Windows 桌面	Designer iManager Workstation (用戶端) 可存取 Identity Applications 和 Identity Reporting 的瀏覽器

平台	元件
Windows Server	Analyzer
	Designer
	Identity Applications
	Identity Manager 引擎
	Identity Reporting
	Identity Vault
	iManager (伺服器)
	.NET 遠端載入器
	One SSO Provider
	PostgreSQL
	遠端載入器
	Self Service Password Reset
	Tomcat

如需系統要求與先決條件的詳細資訊，請參閱以下各節：

- 「規劃安裝 Designer」(第 265 頁)
- 「規劃安裝 iManager」(第 125 頁)
- 「安裝 Identity Vault」(第 51 頁)
- 「規劃安裝引擎、驅動程式和外掛程式」(第 73 頁)
- 「規劃安裝 Identity Applications」(第 165 頁)
- 「為 Identity Manager 規劃安裝密碼管理功能」(第 155 頁)
- 「規劃安裝 PostgreSQL 和 Tomcat」(第 141 頁)

5.4 瞭解授權和啟用

Identity Manager 包含眾多不同的功能。為了符合不同客戶的需求，Identity Manager 功能以 Advanced Edition 和 Standard Edition 兩種版本提供。Identity Manager 的 Advanced Edition 包括全套功能。Standard Edition 僅提供 Advanced Edition 的一部分功能。如需 Advanced Edition 和 Standard Edition 中可用功能的比較，請參閱「Identity Manager Version Comparison」(Identity Manager 版本比較)。NetIQ 為每個版本提供了不同的授權模式。

NetIQ 在一個 ISO 檔案中提供 Advanced 和 Standard 兩個版本，以更佳方式提供新功能、修補程式、文件及支援，同時可讓客戶選取最符合其需求的解決方案功能。

您可以安裝 Identity Manager 的評估版本，免費使用 90 天。不過，您必須在安裝後的 90 天內啟用 Identity Manager 的元件，否則它們到時會停止運作。您可以在 90 天評估期內，也可以在評估期過後，購買產品授權並啟用 Identity Manager。如需詳細資訊，請參閱第 30.6 節「啟用 Identity Manager」(第 310 頁)。

NetIQ 將依據您採購的版本為您提供相應的授權金鑰，以在 Identity Manager 中啟用合適的功能。若要購買 Identity Manager 產品授權，請參閱 NetIQ Identity Manager How to Buy (NetIQ Identity Manager 如何購買) 網站。當您購買產品授權後，NetIQ 會向您傳送一個客戶 ID。這封電子郵件還包含 NetIQ 網站的 URL，您可以透過該網站取得產品啟用身分證明。如果您忘記了自己的客戶 ID 或者未收到該 ID，請聯絡您的業務代表。

5.5 下載安裝檔案

NetIQ 會提供 ISO 檔案，其中包含了構成 Identity Manager 完整安裝的所有元件。每個檔案都包含產品的版本。ISO 檔案的名稱可識別平台。例如，Identity_Manager_*版本*_Windows.iso。

附註：ISO 影像檔很大，請務必將其下載到支援相應檔案大小的磁碟區或 DVD。

若要下載 Identity Manager 安裝檔案：

1. 造訪 NetIQ 下載網站。
2. 在「產品或技術」功能表中，選取「**Identity Manager**」，然後按一下「搜尋」。
3. 在「NetIQ Identity Manager 下載」頁面上，按一下您要下載之 ISO 檔案旁邊的下載按鈕。
4. 按照畫面上的提示，將檔案下載到您電腦上的目錄中。
5. 將下載的 .iso 檔案掛接為磁碟區，或使用該 .iso 檔案建立軟體 DVD。

5.6 尋找可執行檔和預設安裝路徑

下表提供了關於產品 ISO 檔案中可執行檔的位置，以及元件在檔案系統中的預設安裝路徑的資訊：

Identity Manager 元件	**版本 (Advanced/ Standard)**	**ISO 中可執行檔的位置**	**預設安裝路徑**
Identity Vault	Advanced 和 Standard	Setup.exe，位於 \products\eDirectory\x64\ 中	C:\NetIQ
iManager	Advanced 和 Standard	◆ **伺服器安裝：** iManagerInstall.exe，位於 \extracted_directory\products\iManager\installs\win\ ◆ **工作站安裝：**iManager.bat，位於 imanager\bin	C:\Program Files\Novell
Identity Manager 引擎、驅動程式和外掛程式	Advanced 和 Standard	idm_install.exe，位於 \products\idm\windows\setup 中	C:\Novell
遠端載入器	Advanced 和 Standard	idm_install.exe，位於 \products\idm\windows\setup 中	C:\Novell
PostgreSQL 和 Tomcat (受支援的資料庫和應用程式伺服器)	Advanced 和 Standard	TomcatPostgreSQL.exe，位於 products\CommonApplication\postgre_tomcat_install\ 中	C:\NetIQ\idm\apps\tomcat

Identity Manager 元件	版本 (Advanced/ Standard)	ISO 中可執行檔的位置	預設安裝路徑
單一登入 (OSP)	Advanced 和 Standard	osp-install-win.exe，位於 \products\CommonApplication\osp_install 中	C:\NetIQ\idm\apps\osp
Self Service Password Reset (SSPR)	Advanced 和 Standard	sspr-install-win.exe，位於 \products\CommonApplication\sspr_install 中	C:\NetIQ\idm\apps\sspr
Identity Applications	僅限 Advanced Edition	IdmUserApp.exe，位於 products\UserApplication 中	C:\NetIQ\idm\apps\UserApplication
Designer for Identity Manager	Advanced 和 Standard	install.exe，位於 \products\Designer\	c:\NetIQ\idm\apps\Designer
Identity Reporting	Advanced Edition 中完全支援 Standard Edition 中提供有限制的支援	rpt-install-win.exe，位於 \products\Reporting 中	C:\NetIQ\idm\apps\IdentityReporting
Analyzer for Identity Manager	Advanced 和 Standard	install.exe，位於 \products\Analyzer\	C:\NetIQ\idm\apps\Analyzer

6 安裝注意事項

本章列出了將用於代管 Identity Manager 各元件的電腦需要符合的一般先決條件。一般而言，您應該安裝所有元件，以便在環境中提供完整的身分管理功能。但是，您並不需要用到所有元件，例如 Analyzer 或 iManager。

Identity Manager 執行可能依 IT 環境需求而異，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。

如需建議的硬體、支援的作業系統和瀏覽器資訊，請造訪 NetIQ Identity Manager 技術資訊網站。

- 第 6.1 節「瞭解 Identity Manager 通訊」(第 45 頁)
- 第 6.2 節「瞭解語言支援」(第 46 頁)
- 第 6.3 節「確保 Identity Manager 的高可用性」(第 47 頁)

6.1 瞭解 Identity Manager 通訊

為使 Identity Manager 各元件之間能夠正常通訊，NetIQ 建議您開啟下表中列出的預設連接埠。

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。

埠號碼	元件電腦	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
435	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

埠號碼	元件電腦	連接埠用途
8080	Identity Applications iManager	Tomcat 使用該連接埠進行 HTTP 純文字通訊
8090	遠端載入器	遠端載入器使用該連接埠監聽來自遠端介面 shim 的 TCP/IP 連接 **附註：**應該為每個遠端載入器例項指定唯一的連接埠。
8180	Identity Applications	執行 Identity Applications 的 Tomcat 應用程式伺服器使用該連接埠進行 HTTP 通訊
8443	Identity Applications iManager	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
9009	iManager	Tomcat 對 MOD_JK 使用該連接埠
15432	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

6.2 瞭解語言支援

NetIQ 會翻譯 (當地化) Identity Manager 的介面及其安裝程式，以支援您本地電腦上的作業系統語言。但是，我們無法支援所有語言。在安裝期間，有些安裝程式會檢查電腦的地區設定，以確定安裝程序使用的語言。

若要以特定的語言執行安裝程式，可以透過區域設定選項變更地區設定。

6.2.1 已翻譯的元件和安裝程式

下表列出了每個元件安裝可用的翻譯版本。未列在此表中的元件只提供英語版。如果元件未翻譯成作業系統的語言，安裝程式預設會使用英語。此外，安裝程式中的「終端使用者授權合約」可能未以所有支援的語言提供。

地區設定	Designer	Identity Manager 引擎	iManager	iManager 外掛程式	Identity Applications
簡體中文	是	是	是	是	是
繁體中文	是	是	是	是	是
丹麥文	–	–	–	–	是
荷蘭文	是	–	–	–	是
英文	是	是	是	是	是
法文	是	是	是	是	是

地區設定	Designer	Identity Manager 引擎	iManager	iManager 外掛程式	Identity Applications
德文	是	是	是	是	是
意大利文	是	–	是	–	是
日文	是	是	是	是	是
葡萄牙文 (巴西	是	–	是	–	是
俄文	–	–	是	–	是
西班牙文	是	–	是	–	是
瑞典文	–	–	–	–	是

Identity Applications 指儀表板、Identity Applications 管理、Identity Reporting、身分核准和使用者應用程式。

6.2.2 關於語言支援的特殊考量

NetIQ 建議您檢閱以下考量來確定是否要使用 Identity Manager 的翻譯版本。

- 一般而言，如果某個 Identity Manager 元件不支援作業系統的語言，則該元件的介面預設會使用英語。例如，Identity Manager 驅動程式的語言與 Identity Manager 引擎的語言相同。如果 Identity Manager 不支援驅動程式的語言，則驅動程式組態預設會使用英語。
- 以下 iManager 外掛程式提供了西班牙語、俄語、義大利語、葡萄牙語以及上表中列出的語言版本。
- 在啟動 Identity Manager 元件的安裝程式時，需注意以下事項：
  - 如果作業系統使用的是安裝程式支援的語言，則安裝程式預設會使用該語言。不過，您也可以指定使用其他語言來完成安裝程序。
  - 如果安裝程式不支援作業系統的語言，則預設會使用英語。
  - 如果作業系統使用某種拉丁語，則安裝程式允許您指定任何一種拉丁語。
  - 如果作業系統使用支援的亞洲語言或俄語，則安裝程式只允許您指定與作業系統相符的語言，或指定英語。

6.3 確保 Identity Manager 的高可用性

高可用性可確保關鍵網路資源 (包括資料、應用程式和服務) 的高效可管理性。NetIQ 透過叢集或超級管理程式叢集 (例如 VMWare Vmotion) 支援 Identity Manager 解決方案的高可用性。規劃高可用性環境時，應考慮以下事項：

- 您可以在高可用性環境中安裝以下元件：
  - Identity Vault
  - Identity Manager 引擎
  - 遠端載入器
  - Identity Applications，不包括 Identity Reporting
- 當您在叢集環境中執行 Identity Vault (eDirectory) 時，Identity Manager 引擎也會叢集化。

若需要更多相關資訊 ...	請參閱 ...
確定 Identity Manager 元件的伺服器組態	第 5.3.4 節「建議的伺服器設定」(第 41 頁)
在叢集中執行 Identity Vault	「安裝 Identity Vault 的先決條件」(第 52 頁)
	第 A.2 節「在 eDirectory 叢集上設定 NetIQ Identity Manager」(第 373 頁)
	《*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	第 14.2.4 節「為叢集設定 OSP 和 SSPR」(第 162 頁)
	第 15.1.3 節「安裝 Identity Applications 的先決條件和考量」(第 167 頁)
	第 15.4.2 節「為叢集啟用許可權索引」(第 178 頁)
	第 15.4.4 節「為 Identity Applications 準備叢集」(第 180 頁)
	第 15.6.2 節「為叢集設定使用者應用程式驅動程式」(第 193 頁)
	「針對分散式環境或叢集環境更新儀表板中的 SSPR 連結」(第 203 頁)

III 安裝 Identity Manager 引擎

此部分提供關於安裝 Identity Manager 伺服器某些基本架構的資訊。此安裝程式允許您安裝以下元件：

- Identity Manager 驅動程式
- Identity Manager 引擎
- Identity Manager 的 iManager 外掛程式

為方便起見，NetIQ 將這些元件綑綁在同一個安裝程式中。您可以選擇在同一個伺服器上安裝這些元件，也可以分開安裝。安裝檔案位於 Identity Manager 安裝套件的 \products\idm 目錄中。依預設，安裝程式會在 C:\Netiq 中安裝元件。

NetIQ 建議您在開始之前檢閱安裝程序。如需詳細資訊，請參閱第 8.1 節「Identity Manager 引擎、驅動程式和外掛程式的安裝核對清單」(第 73 頁)。

附註：此安裝程式還可以安裝遠端載入器。如需詳細資訊，請參閱第 10 部分「安裝和管理遠端載入器」(第 85 頁)。

---

7 安裝 Identity Vault

本章將引導您完成安裝 Identity Vault 所需元件的程序。Identity Vault 用於儲存 Identity Manager 特定的資訊，例如驅動程式組態、參數和規則。

安裝檔案位於 Identity Manager 安裝套件 .iso 影像檔中的 \products\eDirectory\ *處理器類型*\ 目錄內。依預設，安裝程式將在 C:\NetIQ\eDirectory 中安裝 Identity Vault。

NetIQ 建議您在開始之前檢閱安裝程序。如需詳細資訊，請參閱第 7.1 章 「規劃安裝 Identity Vault」 (第 51 頁)。

7.1 規劃安裝 Identity Vault

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

- 第 7.1.1 節 「Identity Vault 安裝核對清單」 (第 51 頁)
- 第 7.1.2 節 「安裝 Identity Vault 的先決條件和考量」 (第 52 頁)
- 第 7.1.3 節 「瞭解 eDirectory 中的 Identity Manager 物件」 (第 54 頁)
- 第 7.1.4 節 「Identity Vault 的系統要求」 (第 54 頁)

7.1.1 Identity Vault 安裝核對清單

NetIQ 建議您執行以下核對清單中的步驟：

	核對清單項目
❑	1. 瞭解 Identity Manager 各元件之間的互動。如需詳細資訊，請參閱第 I 部分 「介紹」 (第 17 頁)。
❑	2. 確定要為 Identity Manager 的元件使用哪些伺服器。如需詳細資訊，請參閱第 5.3.4 節 「建議的伺服器設定」 (第 41 頁)。
❑	3. 檢閱關於安裝 Identity Vault 的考量，以確保電腦符合先決條件。如需詳細資訊，請參閱第 7.1.2 節 「安裝 Identity Vault 的先決條件和考量」 (第 52 頁)。
❑	4. 檢閱將要代管 Identity Vault 的電腦需要符合的硬體和軟體要求。如需詳細資訊，請參閱第 7.1.4 節 「Identity Vault 的系統要求」 (第 54 頁)。
❑	5. 瞭解當 Identity Vault 中的容器名稱包含句點 (「.」) 時如何使用逸出字元。如需詳細資訊，請參閱第 7.2.1 節 「當容器名稱中包含句點 (「.」) 時使用逸出字元」 (第 55 頁)。
❑	6. 瞭解如何在使用 IPv6 位址的環境中使用 Identity Vault。如需詳細資訊，請參閱第 7.2.4 節 「在 Identity Vault 伺服器上使用 IPv6 位址」 (第 60 頁)。

	核對清單項目
❑	7. 瞭解需要使用哪些連接埠進行 LDAP 通訊。如需詳細資訊，請參閱第 7.2.5 節「使用 LDAP 與 Identity Vault 通訊」(第 61 頁)。
❑	8. 如需安裝說明，請參閱下列其中一個章節： ◆ 若要執行引導式安裝 (使用精靈)，請參閱第 7.3.1 節「使用精靈安裝 Identity Vault」(第 63 頁)。 ◆ 若要執行靜默安裝 (無人管理安裝)，請參閱第 7.3.2 節「以靜默方式安裝和設定 Identity Vault」(第 63 頁)。
❑	9. (選擇性) 從任何防病毒或備份軟體程序中排除 eDirectory 伺服器上的 DIB 目錄。
❑	10. (選擇性) 備份 DIB 目錄。如需詳細資訊，請參閱《*NetIQ eDirectory Administration Guide*》(NetIQ eDirectory 管理指南) 中的「Backing Up and Restoring NetIQ eDirectory」(備份與還原 NetIQ eDirectory)。
❑	11. 安裝 Identity Manager 引擎。如需詳細資訊，請參閱第 8 章 「規劃安裝引擎、驅動程式和外掛程式」(第 73 頁)。

7.1.2 安裝 Identity Vault 的先決條件和考量

Identity Vault 使用一個目錄來儲存透過 Identity Manager 解決方案同步化的物件。以下章節包含的指導準則可協助您規劃要用做 Identity Vault 架構之 NetIQ eDirectory 的部署。

- 「安裝 Identity Vault 的先決條件」(第 52 頁)
- 「在叢集環境中安裝 Identity Vault 的先決條件」(第 53 頁)

安裝 Identity Vault 的先決條件

NetIQ 建議您在安裝用做 Identity Vault 架構的 eDirectory 之前檢閱以下考量：

- 若要使 eDirectory 基礎架構有效執行，您必須在伺服器上設定一個靜態 IP 位址。如果在伺服器上使用 DHCP 位址，eDirectory 可能會發生無法預期的結果。
- 在所有網路伺服器之間同步化時間。NetIQ 建議使用網路時間通訊協定 (NTP) 的 ntp 選項。
- (視情況而定) 若要安裝次要伺服器，用於安裝該產品的分割區中所有複本都應處於「開啟」狀態。
- (視情況而定) 若要以非管理員使用者身分在現有網路樹中安裝次要伺服器，請建立一個容器，然後將其分割。確保您具有以下權限：
  - 對要新增該伺服器的分割區擁有「監督者」權限。
  - 對要新增該伺服器的容器擁有「監督者」權限。
  - 「所有屬性」權限：對 W0.KAP.Security 物件擁有讀取、比較和寫入權限。
  - 「屬性」權限：對安全性容器物件擁有讀取和比較權限。
  - 「存取」權限：對安全性容器物件擁有瀏覽權限。

  當複本計數小於 3 時，若要新增複本，便需要擁有這些權限。

- (視情況而定) 若要以非管理員使用者身分在現有網路樹中安裝次要伺服器，請確保網路樹中至少有一個伺服器的 eDirectory 版本等於或高於以容器管理員身分新增之次要伺服器的 eDirectory 版本。如果要新增之次要伺服器的版本更高，網路樹的管理員必須在使用容器管理員身分新增次要伺服器之前延伸綱要。
- 設定 eDirectory 時，必須在防火牆中啟用 NetWare 核心協定 (NCP) 連接埠 (預設為 524)，以允許新增次要伺服器。此外，您還可以依據自己的要求啟用以下預設服務連接埠：
  - LDAP 純文字 - 389
  - LDAP 安全 - 636
  - HTTP 純文字 - 8028
  - HTTP 安全 - 8030
- 您必須使用適用於 eDirectory 的管理公用程式 (例如 iManager) 在每個工作站上安裝 Novell International Cryptographic Infrastructure (NICI)。NICI 和 eDirectory 支援的最大金鑰大小為 4096 位元。如需詳細資訊，請參閱《*NetIQ eDirectory Installation Guide*》(NetIQ eDirectory 安裝指南) 中的「Installing NICI」(安裝 NICI)。
- (視情況而定) 如果 eDirectory 網路樹中容器的名稱包含句點，您在安裝期間以及在將伺服器新增至現有網路樹時，必須使用逸出字元指定管理員名稱、管理網路位置和伺服器網路位置參數。如需詳細資訊，請參閱第 7.2.1 節「當容器名稱中包含句點 (「.」) 時使用逸出字元」(第 55 頁)。
- 您必須擁有該 伺服器的管理權限，並且對 eDirectory 網路樹中包含具備網域功能之「使用者」物件的所有部分擁有管理權限。要安裝到現有的網路樹，您需要管理網路樹物件的權限，這樣您才可以延伸綱要與建立物件。
- 由於 NTFS 提供比 FAT 檔案系統更安全的交易程序，您只能在 NTFS 分割區上安裝 eDirectory。因此，如果您只有 FAT 檔案系統，請採用下列其中一種方法：
  - 使用「磁碟管理者」。如需詳細資訊，請參閱相應的 Windows Server 文件。
  - 建立新的分割區並格式化為 NTFS。
  - 使用 CONVERT 指令將現存的 FAT 檔案系統轉換為 NTFS。
  - 如需詳細資訊，請參閱相應的 Windows Server 文件。

  若您的伺服器只提供 FAT 檔案系統而且您忘記或忽視了這項程序，安裝程式會提示您要提供 NTFS 分割區。
- 您必須執行最新版本的 Windows SNMP 服務。
- 在您開始執行安裝程序之前，您的 Windows 作業系統執行的必須是最新的 Service Pack。
- 若要在使用 DHCP 位址的虛擬機器上安裝，或者要在未廣播 SLP 的實體機器或虛擬機器上安裝，請確保網路中已設定目錄代理程式。

在叢集環境中安裝 Identity Vault 的先決條件

NetIQ 建議您在叢集環境中安裝 Identity Vault 之前檢閱以下考量：

- 您必須有兩部或更多部裝有叢集軟體的 Windows 伺服器。
- 您必須有叢集軟體支援的外部共享儲存區，其磁碟空間足以儲存所有 Identity Vault 和 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)。

7.1.3 瞭解 eDirectory 中的 Identity Manager 物件

下列清單指出 eDirectory 中儲存的主要 Identity Manager 物件，以及它們彼此之間的關係。安裝程序不會建立物件。您需要在設定 Identity Manager 解決方案時自己建立 Identity Manager 物件。

- **驅動程式集**：驅動程式集是一種容器，可以保存 Identity Manager 驅動程式及程式庫物件。一次只能有一個驅動程式集在伺服器上處於使用中狀態。但可能會有多部伺服器與同一個驅動程式集相關聯。一個驅動程式也可能同時與多部伺服器相關聯。但驅動程式同一時間只應在一部伺服器上執行。在其他伺服器上，該驅動程式應處於停用狀態。任何與驅動程式集相關聯的伺服器上都必須安裝 Identity Manager 伺服器。
- **程式庫**：「程式庫」物件是可以從多個位置參照之常用規則的儲存庫。程式庫儲存於驅動程式集中。您可以將規則存放於程式庫中，以便驅動程式集中的每一個驅動程式都可以參考它。
- **驅動程式**：驅動程式可讓應用程式與 Identity Vault 產生連結。它還可以在各系統之間啟用資料同步和共享。驅動程式儲存於驅動程式集中。
- **工作**：工作可實現週期性任務的自動化。例如，工作可以設定系統，讓它在特定日子停用某個帳戶，或啟始化一個工作流程來申請延伸某人對公司資源的存取期限。工作儲存於驅動程式集中。

7.1.4 Identity Vault 的系統要求

本節提供要安裝 Identity Vault 的伺服器的最低要求。請務必檢閱安裝的先決條件和注意事項，特別是與作業系統有關的內容。

附註：BTRFS 檔案系統不支援 Identity Vault。

類別	要求
處理器	1 GHz
磁碟空間	◆ Identity Vault 需要 300 MB ◆ 每 50,000 個使用者需要 150 MB 的額外磁碟空間
記憶體	2 GB

類別	要求
作業系統 (已認證)	以下 64 位元作業系統之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 NetIQ 建議您在安裝 Identity Manager 之前，依照製造商的自動更新機制來套用最新的作業系統修補程式。 **附註：***已認證*指作業系統已進行全面測試且受支援。
作業系統 (受支援)	已認證作業系統的最新版 Service Pack **附註：***受支援*指作業系統尚未進行測試，但預期可正常運作。
虛擬化系統	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 及更新版本 ◆ 包含 Hyper-V 的 Windows Server 2012 R2 Virtualization (受支援) NetIQ 允許您在為執行 NetIQ 產品的作業系統提供官方支援的企業級虛擬化系統上執行 Identity Manager。只要虛擬化系統的廠商為這些作業系統提供官方支援，NetIQ 就支援在這些系統上執行整個 Identity Manager 堆疊。
目錄服務	NetIQ eDirectory 9.1

7.2 安裝 Identity Vault 的準備工作

必須適當設定 Identity Vault 的環境。例如，伺服器必須能夠透過某種方法 (服務或指定的檔案) 將 Identity Vault 中的網路樹名稱解析成伺服器轉介。本節的內容可協助您在安裝 Identity Vault 之前準備好環境。

7.2.1 當容器名稱中包含句點 (「.」) 時使用逸出字元

可以將伺服器名稱中包含句點的 Windows 伺服器新增至目錄樹中，例如 O=netiq.com 或 C=u.s.a。但是，如果網路樹中之容器的名稱包含句點 (「.」)，則您必須使用逸出字元。請檢閱以下考量：

- 不要在伺服器名稱的開頭使用句點，例如 .netiq。
- 使用反斜線 (「\」) 來逸出容器名稱中的句點。例如：

  O=novell\.com

  或

  C=a\.b\.c

為 iMonitor、iManager、DHost iConsole、DSRepair、Backup、DSMerge、DSLogin 和 ldapconfig 等公用程式輸入帶點的管理員名稱和網路位置時，請包含逸出字元。例如，在登入 iMonitor 時，如果網路樹中 O 的名稱為 netiq.com，請輸入 'admin.netiq\.com' 或 admin.netiq\.com。

7.2.2 使用 OpenSLP 或 hosts.nds 解析網路樹名稱

在安裝 Identity Vault 基礎架構之前，伺服器應該能夠透過某種方法 (服務或指定的檔案) 將 Identity Vault 中的網路樹名稱解析成伺服器轉介。NetIQ 建議使用服務位置通訊協定 (SLP) 服務來解析網路樹名稱。先前版本的 eDirectory 的安裝程式中包含了 OpenSLP。但從 eDirectory 8.8 起，安裝程式中不再包含 OpenSLP。您必須單獨安裝 SLP 服務，或使用 hosts.nds 檔案。如果您使用 SLP 服務，該服務的目錄代理程式 (SLPDA) 必須穩定。

這個單元將提供下列資訊：

- 「使用 hosts.nds 檔案解析網路樹名稱」(第 56 頁)
- 「瞭解 OpenSLP」(第 57 頁)
- 「為 Identity Vault 設定 SLP」(第 59 頁)

使用 hosts.nds 檔案解析網路樹名稱

hosts.nds 檔案是一個靜態查閱表，Identity Vault 應用程式使用它來搜尋 Identity Vault 分割區和伺服器。當網路中沒有 SLP DA 時，它可以協助您避免 SLP 多路廣播延遲。對於每個網路樹或伺服器，您必須在 hosts.nds 檔案內單獨一行中指定以下資訊：

- **伺服器名稱或網路樹名稱**：網路樹名稱應以尾隨點 (.) 結尾。
- **網際網路位址**：可以是 DNS 名稱，也可以是 IP 位址。請不要使用 localhost。
- **伺服器連接埠**：選填資訊，透過一個冒號 (:) 附加在網際網路位址的後面。

除非本地伺服器在監聽非預設 NCP 連接埠，否則不需要在該檔案中包含一個本地伺服器項目。

若要設定 hosts.nds 檔案：

1. 建立新的 hosts.nds 檔案或開啟一個現有檔案。
2. 新增以下資訊：

   partition_name.tree_name. host_name/ip-addr:port server_name dns-addr/ip-addr:port

   例如：

   ```
   # This is an example of a hosts.nds file:
   # Tree name Internet address/DNS Resolvable Name
     CORPORATE. myserver.mycompany.com
     novell.CORPORATE. 1.2.3.4:524

   # Server name Internet address
     CORPSERVER myserver.mycompany.com:524
   ```

3. (選擇性) 如果您日後決定使用 SLP 來解析網路樹名稱，並確定 Identity Vault 網路樹在網路中可用，請將以下文字新增至 hosts.nds 檔案：

   /usr/bin/slptool findattrs services:ndap.novell///(svcname-ws==[*treename or **])"

   例如，若要搜尋其 svcname-ws 屬性與 SAMPLE_TREE 值相符的服務，請輸入以下指令：

   /usr/bin/slptool findattrs services:ndap.novell///(svcname-ws==SAMPLE_TREE)"

附註：請在安裝 SLP 和 Identity Vault 之後執行此動作。

如果您的某個服務的 svcname-ws 屬性註冊為 SAMPLE_TREE，則輸出將類似於 service:ndap.novell:///SAMPLE_TREE。否則，您將不會收到輸出回應。

瞭解 OpenSLP

OpenSLP 是 IETF Request-For-Comments (RFC) 2608 中所述 IETF 服務位置通訊協定版本 2.0 標準的開放原始碼執行方式。

OpenSLP 原始碼提供的介面是 RFC 2614 中所述的、以程式設計方式存取 SLP 功能的另一種 IETF 標準執行方式。

若要全面瞭解 SLP 的工作原理，最好是閱讀這些文件並加以融會貫通。它們未必通俗易懂，但若要在內部網路中正確設定 SLP 組態，您必須瞭解這些知識。

如需 OpenSLP 專案的詳細資訊，請造訪 OpenSLP 和 SourceForge 網站。OpenSLP 網站上的多個文件包含了實用組態秘訣。其中的許多文件在本文件發佈時並不完整。

本節包含關於 SLP 的用途，以及它與 Identity Vault 具有何種關聯的以下論述：

- 「NetIQ 服務位置提供者」(第 57 頁)
- 「使用者代理程式」(第 58 頁)
- 「服務代理程式」(第 58 頁)
- 「目錄代理程式」(第 58 頁)

NetIQ 服務位置提供者

NetIQ 版本的 SLP 對 SLP 標準進行了一定的變動，以提供更穩健的服務通告環境，但這也在一定程度上降低了延展性。

例如，為了改進服務通告架構的延展性，您可以限制子網路上廣播或多路廣播的封包數。SLP 規格透過對服務代理程式和使用者代理程式施加目錄代理程式查詢方面的限制來管理此問題。第一個探查到的為所需範圍提供服務的目錄代理程式，就是服務代理程式 (因而也就是本地使用者代理程式) 要為將來對該範圍發出之所有要求使用的代理程式。

實際上，NetIQ SLP 執行方式會掃描它所知道的所有目錄代理程式以取得查詢資訊。它認為來回一次花費 300 毫秒時間太長，如果這樣，它可以在 3 到 5 秒內掃描 10 個伺服器。如果在網路中正確設定了 SLP，並且 OpenSLP 認為事實上針對 SLP 流量正確設定了網路，則不需要進行此掃描。OpenSLP 的回應逾時值大於 NetIQ SLP 服務提供者的逾時值，並且它會將目錄代理程式的數量限制為做出回應的第一個代理程式，不管該代理程式的資訊是否完整準確。

使用者代理程式

使用者代理程式 (UA) 以與某個應用程式連結之靜態或動態程式庫的實體形式存在。它允許該應用程式查詢 SLP 服務。使用者代理程式的任務是提供一個程式設計介面，供用戶端查詢服務，以及供服務通告自身。使用者代理程式將聯絡目錄代理程式，以查詢位於指定範圍內、屬於指定服務類別的已註冊服務。

使用者代理程式遵循某種演算法，來取得將要向其傳送查詢的目錄代理程式位址。在取得指定範圍的目錄代理程式 (DA) 位址後，對於該範圍，它們將會一直使用該位址，直到該目錄代理程式不再做出回應，到那時，使用者代理程式將取得該範圍的另一個 DA 位址。使用者代理程式透過以下方式查找指定範圍的目錄代理程式位址：

1. 檢查以確定目前要求的通訊端識別指標是否已連接到指定範圍的 DA。如果該要求正好是一個多部分要求，則表示可能已存在該要求的快取連接。
2. 檢查它的本地已知 DA 快取中有無與指定範圍相符的 DA。
3. 向本地服務代理程式 (SA) 確認有無屬於指定範圍的 DA (並將新位址新增至快取中)。
4. 向 DHCP 查詢透過網路設定且與指定範圍相符的 DA 位址 (並將新位址新增至快取中)。
5. 在已知的連接埠上多路廣播 DA 探查要求 (並將新位址新增至快取中)。

指定的範圍為「default」(如果未指定)。也就是說，如果未在 SLP 組態檔案中靜態定義任何範圍，並且未在查詢中指定任何範圍，那麼，使用的範圍將是「default」一字。此外，還應注意，Identity Vault 永遠不會在其註冊中指定範圍。如果存在靜態設定的範圍，在指定範圍不存在的情況下，該靜態設定的範圍將是所有本地 UA 要求和 SA 註冊的預設範圍。

服務代理程式

服務代理程式在主機機器上以某個獨立程序的實體形式存在。slpd.exe 做為本地機器上的服務執行。使用者代理程式透過向已知連接埠上的迴路位址傳送訊息來查詢本地服務代理程式。

服務代理程式的任務是為已將自身註冊到 SLP 的本地服務提供永久的儲存和維護點。服務代理程式本質上所做的工作是維護已註冊本地服務的記憶體內部資料庫。事實上，除非存在本地 SA，否則服務無法註冊到 SLP。用戶端可以探查僅包含 UA 程式庫的服務，但註冊時需要 SA，主要原因是 SA 必須定期重新宣示已註冊服務的存在，以確保將其註冊到監聽目錄代理程式。

服務代理程式透過以下方式將 DA 探查要求直接傳送至潛在的 DA 位址，來查找和快取目錄代理程式及其支援的範圍清單：

1. 檢查所有靜態設定的 DA 位址 (並將新位址新增至 SA 的已知 DA 快取中)。
2. 要求獲取來自 DHCP 的 DA 和範圍清單 (並將新位址新增至 SA 的已知 DA 快取中)。
3. 在已知的連接埠上多路廣播 DA 探查要求 (並將新位址新增至 SA 的已知 DA 快取中)。
4. 接收 DA 定期廣播的 DA 通告封包 (並將新位址新增至 SA 的已知 DA 快取中)。

使用者代理程式永遠會先查詢本地服務代理程式，這一點非常重要，因為本地服務代理程式的回應將決定使用者代理程式是否要繼續執行下一個探查階段 (在本案例中為 DHCP，請參閱「使用者代理程式」(第 58 頁) 中的步驟 3 和步驟 4)。

目錄代理程式

目錄代理程式的任務是提供所通告服務長期持久的快取，以及為使用者代理程式提供一個存取點來查閱服務。做為快取，DA 將會監聽 SA 以通告新服務，並會快取相應通知。不久後，DA 的快取就會變得更充實完整。目錄代理程式使用過期演算法來使快取項目過期。一個目錄代理程式啟動時，會從永

久儲存 (通常是硬碟) 中讀取其快取，然後開始根據演算法使項目過期。當有新的 DA 啟動或某個快取已被刪除時，之前的 DA 會偵測到此狀況，並向所有監聽 SA 發出傾印其本地資料庫的特殊通知，以使該 DA 能夠快速建立其快取。

在不存在任何目錄代理程式的情況下，UA 將會採用 SA 可以回應的一般多路廣播查詢，以與 DA 建立快取時所用的大致相同的方式，構建所要求服務的清單。此類查詢傳回的服務清單並不完整，與 DA 提供的服務清單相比，該清單的當地化程度要高得多，當網路中設定了多路廣播過濾 (許多網路管理員為了將廣播和多路廣播局限於本地子網路會進行此設定) 時尤其如此。

總而言之，一切都取決於使用者代理程式要在其中尋找給定範圍的目錄代理程式。

為 Identity Vault 設定 SLP

%systemroot%/slp.conf 檔案中的以下參數用於控制目錄代理程式探查：

```
net.slp.useScopes = comma-delimited scope list
net.slp.DAAddresses = comma-delimited address list
net.slp.passiveDADetection = <"true" or "false">
net.slp.activeDADetection = <"true" or "false">
net.slp.DAActiveDiscoveryInterval = <0, 1, or a number of seconds>
```

useScopes

指示 SA 將通告的範圍，以及當服務或用戶端應用程式執行的註冊或查詢中不存在特定範圍時，要對其執行查詢的範圍。由於 Identity Vault 一律會通告到預設範圍並從預設範圍查詢，此清單將會成為所有 Identity Vault 註冊和查詢的預設範圍清單。

DAAddresses

代表 DA 點分式十進位 IP 位址的逗號分隔清單，這些位址應優先於所有其他位址。如果這個包含已設定 DA 的清單不支援某個註冊或查詢的範圍，則 SA 和 UA 將採用多路廣播 DA 探查，除非此類探查被停用。

passiveDADetection

依預設，其值為 True。如果進行了相應的設定，目錄代理程式將定期透過已知連接埠在子網路上廣播其存在性。這些封包稱為 DAAdvert 封包。如果將此選項設定為 False，SA 將會忽略所有廣播 DAAdvert 封包。

activeDADetection

依預設，其值為 True。此參數允許 SA 定期廣播要求，以便所有 DA 都可使用導向 DAAdvert 封包做出回應。導向的封包不會廣播，而是做為這些要求的回應直接傳送給 SA。如果將此選項設定為 False，SA 將不會定期廣播 DA 探查要求。

DAActiveDirectoryInterval

代表一個 tri-state 參數。預設值為 1，該特殊值表示 SA 在啟始化時只應發出一個 DA 探查要求。將此選項設定為 0 相當於將 activeDADetection 選項設定為 false。任何其他值則為兩次探查廣播間隔的秒數。

正確使用這些選項可確保合理使用網路頻寬來進行服務通告。事實上，預設設定就能最佳化平均水準之網路的延展性。

7.2.3 改進 Identity Vault 效能

Identity Vault 的底層基礎架構 eDirectory 屬於 I/O 密集型應用程式，而不是處理器密集型應用程式。以下兩個因素可以提高 Identity Vault 的效能：使用更多的快取記憶體和更快的處理器。若要達到最佳效果，應在硬體允許的前提下，盡可能多快取目錄資訊資料庫 (DIB) 集。

儘管 eDirectory 在一個處理器上就能實現很好的延展性，但您不妨考慮使用多個處理器。增加處理器會改進使用者登入等方面的效能。此外，在多個處理器上啟用多個線串也能改進效能。

下表提供了根據 eDirectory 中的預期物件數進行伺服器設定的一般指導準則。

物件	記憶體	硬碟
100.000	384 MB	144 MB
1 百萬	4 GB	1.5 GB
1 千萬	2 GB 以上	15 GB

例如，一項 eDirectory 標準綱要的基本安裝，每 50,000 個使用者需要大約 74 MB 的磁碟空間。但是，若您要新增一組新的屬性或將每個現有的屬性填滿，則物件會增大。這些新增會影響磁碟空間、處理器、及記憶體的需求。此外，對處理器的要求還取決於電腦上可用的其他服務，以及電腦正在處理的驗證、讀取和寫入數。加密和索引等程序可能會消耗大量的處理器資源。

7.2.4 在 Identity Vault 伺服器上使用 IPv6 位址

Identity Vault 既支援 IPv4 位址，也支援 IPv6 位址。您可以在安裝 Identity Vault 時啟用 IPv6 位址。如果從以前的版本升級，則必須手動啟用 IPv6 位址。

Identity Vault 還支援雙 IP 堆疊、通道封裝和純 IPv6 轉換方法。它僅支援全域 IP 位址。例如：

- [::]
- [::1]
- [2015::12]
- [2015::12]:524

指定 IPv6 位址時必須用方括號 [ ] 將其括住。若要使用主機名稱而不使用 IP 位址，必須在 C:\Windows\System32\drivers\etc\hosts 檔案中指定主機名稱，並將它與 IPv6 位址關聯。

若要在 Windows 伺服器上使用 IPv6 位址，必須在安裝期間選取 **IPv6 優先設定**下的**啟用 IPv6** 核取方塊。此選項將為 IPv6 位址啟用 NCP、HTTP 和 HTTPS 通訊協定。如果您在安裝期間未啟用 IPv6 位址，後來又決定使用 IPv6 位址，則您必須重新執行安裝程式。如需詳細資訊，請參閱第 7.3 章 「安裝 Identity Vault」 (第 62 頁)。

您可以使用以下連結透過 IPv6 位址存取 iMontior：http://[2015::3]:8028/nds。

7.2.5 使用 LDAP 與 Identity Vault 通訊

當您安裝 Identity Vault 時，必須指定 LDAP 伺服器監控的連接埠，以使該伺服器能夠為 LDAP 要求提供服務。在預設組態中，用於純文字和 SSL/TLS 通訊的連接埠號分別設定為 389 和 636。

LDAP 簡單結合只需要有 DN 和密碼。該密碼採用純文字格式。如果您使用連接埠 389，則整個封包都採用純文字格式。由於連接埠 389 允許純文字傳輸，LDAP 伺服器將透過此連接埠為目錄的讀取和寫入要求提供服務。這種開放性足以建立環境信任，在其中不會發生詐騙現象，並且沒有人可以透過不當方式擷取封包。依預設，在安裝期間會停用此選項。

透過連接埠 636 建立的連接會被加密。TLS (以前稱為 SSL) 可管理加密。與連接埠 636 建立連接時，會自動例項化一個信號交換。如果信號交換失敗，則會拒絕連接。

附註：依預設，安裝程式會選取連接埠 636 來進行 TLS/SSL 通訊。此預設選擇可能會給您的 LDAP 伺服器造成問題。如果在安裝 eDirectory 之前主機伺服器上就已載入的服務使用了連接埠 636，則您必須指定另一個連接埠。低於 eDirectory 8.7 的安裝會將此衝突視為嚴重錯誤，並會卸載 nldap。在 eDirectory 8.7.3 以後的版本中，安裝程式會載入 nldap，在 dstrace.log 檔案中記錄一則錯誤訊息，然後會繼續執行，不過不會使用該安全連接埠。

在安裝過程中，您可以將 Identity Vault 設定為禁止純文字的密碼和其他資料。選取**需要 TLS 以與密碼簡單結合**選項可以阻止使用者傳送可辨認出的密碼。如果您不選取此設定，使用者將不知道其他人可以辨認出他們的密碼。這個不允許連接的選項僅適用於純文字連接埠。如果與連接埠 636 建立安全連接並使用簡單結合，則連接已經加密。將沒有人能夠檢視密碼、資料封包或結合要求。

請考慮以下情境：

啟用了「需要 TLS 以與密碼簡單結合」

Olga 正在使用一個要求輸入密碼的用戶端。在 Olga 輸入密碼後，用戶端連接到伺服器。但是，LDAP 伺服器不允許連接透過純文字連接埠結合到伺服器。任何人都能夠檢視 Olga 的密碼，但 Olga 卻無法取得結合的連接。

連接埠 636 已在使用中

您的伺服器正在執行 Active Directory。Active Directory 執行的某個 LDAP 程式使用了連接埠 636。您安裝 eDirectory。安裝程式偵測到連接埠 636 已在使用中，並且未為 NetIQ LDAP 伺服器指定連接埠號。LDAP 伺服器將會載入，並且看上去已執行。但是，由於 LDAP 伺服器不會複製或使用已開啟的連接埠，因此不會對任何複製的連接埠上的要求進行處理。

若要驗證是否已將連接埠 389 或 636 指定給 NetIQ LDAP 伺服器，請執行 ICE 公用程式。如果*廠商版本*欄位中未指定 NetIQ，則您必須為 eDirectory 重新設定 LDAP 伺服器，並選取其他連接埠。如需詳細資訊，請參閱《*NetIQ eDirectory Administration Guide*》(NetIQ eDirectory 管理指南) 中的「Verifying That the LDAP Server is Running」(驗證 LDAP 伺服器是否正在執行)。

Active Directory 正在執行

如果 Active Directory 正在執行，並且純文字連接埠 389 已開啟，則您可以對連接埠 389 執行 ICE 指令，並要求獲得廠商版本。報告將顯示 **Microsoft***。然後，您可以透過選取另一連接埠來重新設定 NetIQ LDAP 伺服器，以使 eDirectory LDAP 伺服器能夠為 LDAP 要求提供服務。

iMonitor 也可以報告連接埠 389 或 636 是否已開啟。如果 LDAP 伺服器未運作，可使用 iMonitor 來查看詳細資料。如需詳細資訊，請參閱《*NetIQ eDirectory Administration Guide*》(NetIQ eDirectory 管理指南) 中的「Verifying That the LDAP Server is Running」(驗證 LDAP 伺服器是否正在執行)。

7.2.6 在裝有管理公用程式的工作站上手動安裝 NICI

使用 iManager 等管理公用程式的每個工作站上都必須安裝 NICI。如需將 NICI 與 Identity Vault 配合使用的詳細資訊，請參閱 「安裝 Identity Vault 的先決條件」(第 52 頁)。

若要安裝 NICI，請使用預設位於 products\eDirectory\ 處理器類型 \windows\ *處理器類型*\nici *資料夾中的* NICI_wx64.msi 檔案。您可以使用引導式程序 (精靈) 或靜默安裝方式執行該檔案。

7.2.7 安裝 NMAS 用戶端軟體

您要使用 NetIQ Modular Authentication Service (NMAS) 登入方法的每個用戶端工作站上都必須安裝 NMAS 用戶端軟體。登入方法是在安裝 Identity Vault 時指定的。

1. 使用管理員帳戶登入 用戶端工作站。
2. 從安裝目錄 (預設為 Win:\products\eDirectory\ 處理器類型 \nmas\) *執行* nmasinstall.exe 程式。
3. 按一下 **NMAS 用戶端元件**。
4. (選擇性) 選取 「NICI」選項以安裝 NICI 元件。
5. 按一下 「**確定**」。
6. 安裝程序完成後，重新啟動用戶端工作站。

7.3 安裝 Identity Vault

安裝程式可引導您完成 Identity Vault 的組態設定。安裝程式會自動預設為精靈模式。但是，您也可以執行靜默安裝。

本節假設您要將 eDirectory 用做 Identity Vault 的基礎結構。

當您啟動安裝程式時，它會檢查 Novell International Cryptographic Infrastructure (NICI) 和 Novell Client for Windows 是否已安裝。安裝程式會視需要安裝或更新這些元件。如果在已裝有 Novell Client 的電腦上安裝 Identity Vault，eDirectory 將使用現有的 Novell Client。在沒有 Novell Client 的情況下，您可以安裝 Identity Vault

如需 NICI 的詳細資訊，請參閱 《*Novell International Cryptographic Infrastructure Administration Guide*》 (Novell International Cryptographic Infrastructure 管理指南)。如需 Client 的詳細資訊，請參閱 Novell Client for Windows 文件。

安裝程式可以安裝 NetIQ Module Authentication Service (NMAS) 的伺服器元件。在安裝期間，您必須指定要與 NMAS 配合使用的登入方法。此外，必須在您要使用 NMAS 登入方法的每個用戶端工作站上安裝 NMAS 用戶端軟體。

附註：

- 從 eDirectory 8.8 開始，可以對所有公用程式使用區分大小寫的密碼。
- 容器名稱可以包含句點 (點)。如需在容器名稱中使用點號的資訊，請參閱第 7.1.2 節「安裝 Identity Vault 的先決條件和考量」(第 52 頁)。

7.3.1 使用精靈安裝 Identity Vault

1 以管理使用者身分登入您要安裝 eDirectory 的電腦。
2 導覽至 \products\eDirectory\x64\ 目錄。
3 執行 eDirectory_910_windows_x86_64.exe 檔案。
4 在基本索引標籤中指定以下詳細資料：
   - 如果您選取了新網路樹，請指定以下詳細資料：
      - **網路樹名稱**：指定 Identity Vault 的網路樹名稱。
      - **伺服器 FDN**：指定伺服器 FDN。

      附註：雖然 Identity Vault 允許您為 NCP 伺服器物件設定最多包含 256 個字元的 FDN，但建議您將該變數限制為一個小得多的值，因為 Identity Vault 會依據此物件的長度建立其他更長的物件。

      - **網路樹管理員**：指定 Identity Vault 的管理員名稱。
      - **管理員密碼**：指定管理員密碼。
   - 如果選取了現有網路樹，請指定以下詳細資料：
      - **IP 位址**：指定 Identity Vault 現有網路樹的 IP 位址。
      - **連接埠號碼**：指定現有網路樹的連接埠號碼。預設值為 524。
      - **伺服器 FDN**：指定伺服器 FDN。
      - **網路樹管理員**：指定 Identity Vault 的現有管理員名稱。
      - **管理員密碼**：指定管理員密碼。
5 (視情況而定) 在進階索引標籤中指定以下詳細資料：
   - 若要在 Identity Vault 伺服器上使用 IPv6 位址，請選取**啟用 IPv6**。

      附註：NetIQ 建議您啟用此選項。若要在安裝後啟用 IPv6 位址，必須再次執行安裝程式。

   - 若要啟用增強型背景驗證 (EBA)，請選取**啟用 EBA**。
   - 指定 HTTP 純文字連接埠和安全連接埠。預設值分別為 8028 和 8030。
   - 指定 LDAP 純文字連接埠和安全連接埠。預設值分別為 389 和 636。
6 在安裝位置欄位中，指定 Identity Vault 的安裝位置。
7 在 **DIB 位置**欄位中，指定 DIB 檔案所在的位置。
8 按一下安裝，繼續安裝過程。

7.3.2 以靜默方式安裝和設定 Identity Vault

若要支援以靜默 (或無人管理) 方式安裝或設定 Identity Vault，您可以使用 response.ni 檔案，該檔案與 Windows.ini 檔案類似，其中包含了一些區段和鍵。

附註：您必須安裝並設定 NetIQ SecreStore (ss)。如需詳細資訊，請參閱第 7.4.1 節「將 SecretStore 新增至 Identity Vault 綱要」(第 70 頁)。

編輯 response.ni 檔案

您可以使用 ASCII 文字編輯器來建立和編輯 response.ni 檔案。該 response 檔案可協助您：

- 提供所有必要的使用者輸入執行完全無人管理的安裝。
- 定義元件的預設組態。
- 在安裝期間略過所有提示。

NetIQ 在安裝套件的 products\eDirectory\x64\windows\x64\NDSonNT 資料夾中提供了一個 response.ni 檔案。該檔案包含參數的預設設定。您必須在 NWI:NDS 區段中編輯 eDirectory 例項的值。

附註：當您編輯 response.ni 檔案時，請不要在每個鍵值組中的鍵、值和等號 (「=」) 之間包含空格。

警告：在 response.ni 檔案中為無人管理安裝指定管理員使用者身分證明。為了防止管理員身分證明洩露，您應該在完成安裝或設定後永久性刪除該檔案。

以下章節描述了 response.ni 檔案中的必要區段和鍵：

- 「NWI:NDS」(第 64 頁)
- 「NWI:NMAS (NMAS 方法)」(第 66 頁)
- 「eDir:HTTP (連接埠)」(第 67 頁)
- 「Novell:Languages:1.0.0 (語言設定)」(第 67 頁)
- 「Initialization」(第 68 頁)
- 「NWI:SNMP」(第 68 頁)
- 「EDIR:SLP」(第 68 頁)
- 「Novell:ExistingTree:1.0.0」(第 68 頁)
- 「Selected Nodes」(第 69 頁)
- 「Novell:NOVELL_ROOT:1.0.0」(第 69 頁)

NWI:NDS

Upgrade Mode

指定是否要以升級模式執行安裝程式。有效值為 False、True 和 Copy。

Mode

指定要執行的安裝類型：

- 如果指定 **full**，則您既可以安裝，也可以設定 Identity Vault。如果您想進行全新安裝並設定 Identity Vault，或者只想升級並設定所需的檔案，請指定此值。
- 如果指定 **install**，則您可以安裝全新版本的 Identity Vault，或升級所需的檔案。
- 如果指定 **configure**，則您可以修改 Identity Vault 設定。如果您只是執行所需檔案的升級，則安裝程式只會設定升級的檔案。

附註：

- 如果指定 *configure*，請切勿變更 [Initialization] 區段中 ConfigurationMode 鍵的 RestrictNodeRemove 值。
- 如果指定 *full*，則您在解除安裝 Identity Vault 時，將無法分別選取取消設定和解除安裝選項。

New Tree

指定此次安裝的是新網路樹還是次要伺服器。有效值為 Yes 和 No。例如，如果您要安裝新網路樹，請指定 Yes。如需指定現有網路樹的值的詳細資訊，請參閱 「Novell:ExistingTree:1.0.0」(第 68 頁)。

Tree Name

如果要執行全新安裝，請指定想要安裝之網路樹的名稱。若要安裝次要伺服器，請指定要向其新增該伺服器的網路樹。

Server Name

指定要在 Identity Vault 中安裝之伺服器的名稱。

Server Container

指定網路樹中要新增伺服器物件的容器物件。伺服器物件包含 Identity Vault 伺服器特定的所有組態詳細資料。如果您要安裝全新版本的 Identity Vault，安裝程式將會建立包含伺服器物件的此容器。

Server Context

指定伺服器物件的完整可辨識名稱 (DN) (伺服器名稱) 以及容器物件。例如，如果 Identity Vault 伺服器為 EDIR-TEST-SERVER，容器為 Netiq，則指定 EDIR-TEST-SERVER.Netiq。

Admin Context

指定網路樹中要新增管理員物件的容器物件。例如 Netiq。新增至網路樹中的任何使用者都有一個使用者物件，其中包含該使用者特定的所有詳細資料。如果您要安裝全新版本的 Identity Vault，安裝程式將會建立包含伺服器物件的此容器。

Admin Login Name

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。例如 Admin。安裝程式將使用此帳戶在網路樹中執行所有操作。

Admin Password

指定管理員物件的密碼。例如 netiq123。如果您要安裝全新版本的 Identity Vault，安裝程式將為管理員物件設定此密碼。

NDS Location

指定本地系統中要安裝 Identity Vault 程式庫和二進位檔案的路徑。當您設定 Identity Vault 元件時，它們將查閱此安裝位置來獲取相關檔案。依預設，安裝程式會將檔案放置在 C:\Novell\NDS 中。

DataDir

指定本地系統中要安裝 DIB 檔案的路徑。依預設，安裝程式會將檔案放置在 C:\Novell\NDS\DIBFiles 中。

如果在您的環境中，DIB 資料檔案所需的空間超過了預設位置的可用空間，則您可能需要指定其他路徑。

Installation Location

(選擇性) 指定安裝程式在向 NDS 位置複製檔案時使用的路徑。例如 [Novell:DST:1.0.0_Location] 或 Path=file://C:\Novell\NDS。預設值為 C:\Novell\NDS，這與「NDS Location」的預設值相同。安裝程式在向指定的 NDS 和 DataDir 位置複製檔案時將會使用此路徑。

System Location

(選擇性) 指定您要安裝 Identity Vault 伺服器的電腦上的系統資料夾路徑。例如 [Novell:SYS32_DST:1.0.0_Location] 或 Path=file:/C:\Windows\system32。在安裝期間，安裝程式需要存取該系統資料夾以複製 DLL，還需要存取系統特定的檔案。

Require TLS

(選擇性) 指定 Identity Vault 在接收純文字格式的 LDAP 要求時，是否需要使用輸送層安全性 (TLS) 通訊協定。

LDAP TLS Port

(選擇性) 指定 Identity Vault 要用來監聽純文字格式 LDAP 要求的連接埠。

LDAP SSL Port

(選擇性) 指定 Identity Vault 應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。

Install as Service

指示安裝程式將 eDirectory 安裝為一項服務。您必須指定 Yes。

Prompt

指定是否要讓安裝程式提示您來決定網路樹名稱和伺服器名稱等事項。例如，在採用靜默或無人管理安裝模式時，請指定 False。

NWI:NMAS (NMAS 方法)

Identity Vault 支援在安裝和升級期間使用多種 NMAS 方法。您必須在 response.ni 檔案中指定 NDS NMAS 方法。如果未指定任何 NMAS 方法，安裝程式預設會安裝 NDS 方法。但是，如果您要建立明確的清單，則必須包含 NDS。

Choices

指定要安裝的 NMAS 方法數量。例如 5。

Methods

指定要安裝的 NMAS 方法類型。請使用逗號分隔多個類型。例如 CertMutual,Challenge Response,DIGEST-MD5,NDS。

安裝程式在選擇要安裝的 NMAS 方法時會對比確切的字串 (區分大小寫)，因此，您必須完全依照以下所列格式指定值：

- CertMutual

- Challenge Response - 代表 NetIQ 處理安全回應 NMAS 方法。
- DIGEST-MD5
- Enhanced Password
- Entrust
- GSSAPI - 代表 eDirectory 的 SASL GSSAPI 機制。向 Identity Vault 的驗證是使用 Kerberos 票證透過 LDAP 進行的。
- NDS - 預設的登入方法。REQUIRED.
- NDS Change Password
- Simple Password
- Universal Smart Card
- X509 Advanced Certificate
- X509 Certificate

當您在 response 檔案中指定 NMAS 方法後，Identity Vault 將會在安裝時顯示狀態訊息，而不提示使用者輸入資料。

eDir:HTTP (連接埠)

Identity Vault 將在預先設定的 HTTP 連接埠上監聽透過 Web 進行的存取活動。例如，iMonitor 會透過 Web 介面存取 Identity Vault，而這些介面需要指定特定連接埠來存取相應的應用程式。使用以下選項可以針對特定的連接埠設定 Identity Vault：

Clear Text HTTP Port

為純文字 HTTP 操作指定連接埠號。

SSL HTTP Port

為使用 SSL 通訊協定的 HTTP 操作指定連接埠號。

Novell:Languages:1.0.0 (語言設定)

在安裝期間，您可以指定 Identity Vault 的地區設定和顯示語言：英語、法語或日語。這些值相互排斥。

LangID4

代表英語。例如 LangID4=true。

LangID6

表示法語。

LangID9

代表日語。

附註：

- 請不要對多種語言指定 true。
- 您還可以指定安裝程式在整個安裝過程中用來顯示訊息的語言。如需詳細資訊，請參閱「Initialization」(第 68 頁)。

Initialization

Response.ni 檔案的 [Initialization] 區段指定安裝程序的設定。

DisplayLanguage

指定安裝過程中用於顯示訊息的語言。例如 DisplayLanguage=en_US。

InstallationMode

指定執行安裝程序的方式。例如，若要執行靜默或無人管理安裝，請指定 silent。

SummaryPrompt

指定是否要讓安裝程式提示您檢閱安裝設定的摘要。例如，在採用靜默或無人管理安裝模式時，請指定 false。

prompt

指定是否要讓安裝程式提示您來決定某些事項。例如，在採用靜默或無人管理安裝模式時，請指定 false。

NWI:SNMP

大多數 Windows 伺服器都已設定並會執行 SNMP。在安裝 Identity Vault 時，您必須停止 SNMP 服務，並在安裝程序完成後重新啟動這些服務。在手動安裝期間，程式會提示您在繼續安裝之前先停止 SNMP 服務。

如果希望安裝程式在靜默或無人管理安裝期間不發出提示，直接停止 SNMP 服務，請在 response.ni 檔案的 [NWI:SNMP] 區段中指定 Stop Service=yes。

EDIR:SLP

在安裝或升級期間，Identity Vault 使用服務位置通訊協定 (SLP) 服務識別子網路中的其他伺服器或網路樹。如果您的伺服器上已安裝 SLP 服務，您可以將它們取代為目前 Identity Vault 版本隨附的服務版本，或者使用您自己的 SLP 服務。

Need to uninstall service

指定是否要解除安裝伺服器上已安裝的所有 SLP 服務。預設值為 true。

Need to remove files

指定是否要移除伺服器上已安裝的所有 SLP 服務檔案。預設值為 true。

Novell:ExistingTree:1.0.0

安裝程式提供了相應的選項，供您以無人管理模式在網路中安裝主要或次要伺服器。安裝程式使用三個不同的鍵來決定是要安裝新網路樹，還是在現有網路樹中安裝次要伺服器。

附註：New Tree 鍵位於 NWI:NDS 區段中。如需詳細資訊，請參閱 「NWI:NDS」(第 64 頁)。

ExistingTreeYes

有效值為 True 和 False。例如，如果您要安裝新網路樹，請指定 False。

ExistingTreeNo

有效值為 True 和 False。例如，如果您要安裝新網路樹，請指定 True。

如果您要執行靜默或無人管理安裝，並且不希望程式提示您來決定有關主要或次要伺服器安裝的事項，請在 response.ni 檔案的 Existing Tree 區段中指定 prompt=false。

Selected Nodes

response.ni 檔案的此區段列出了 Identity Vault 中安裝的元件，以及包含元件詳細資訊之設定檔資料庫中的資訊，其中包括來源位置、目的地複製位置和元件版本。設定檔資料庫中的這些詳細資料已編譯成 .db 檔案，Identity Vault 版本中隨附了此檔案。

如果您要執行靜默或無人管理安裝，並且不希望程式提示您來決定目的地複製位置或版本詳細資料等事項，請在 response.ni 檔案的 [Selected Nodes] 區段中指定 prompt=false。

您的 response 檔案必須包含此區段。請使用與範例 response.ni 檔案中提供的完全相同的鍵和值。

Novell:NOVELL_ROOT:1.0.0

Response.ni 檔案的此區段包含安裝過程中顯示的影像和狀態的設定。例如，您可以設定安裝程式對檔案寫入衝突和檔案複製決策等情況做出回應的方式。您還可以指定是否顯示影像。大多數影像包含所安裝 Identity Vault 版本和元件的資訊、歡迎螢幕、授權檔案、自訂選項、指示目前正在安裝元件的狀態訊息、完成百分比，等等。有些特意內嵌 eDirectory 的應用程式可能不希望 eDirectory 顯示這些影像。

如果您要執行靜默或無人管理安裝，並且不希望程式提示您來決定目的地複製位置或版本詳細資料等事項，請在 response.ni 檔案的此區段中指定 prompt=false。

您的 response 檔案應包含此區段。請使用範例 response.ni 檔案中提供的鍵和值。

執行靜默或無人管理安裝

在開始之前，請查看執行靜默或無人管理安裝的先決條件。如需詳細資訊，請參閱 第 7.1.2 節「安裝 Identity Vault 的先決條件和考量」(第 52 頁)。此外，請建立要用做安裝樣板的 response.ni 檔案。如需詳細資訊，請參閱 「編輯 response.ni 檔案」(第 64 頁)。

附註：為了確保作業系統不會顯示安裝、升級或組態的狀態視窗，請在指令中使用 nopleasewait 選項。

---

1. 建立新的 response.ni 檔案，或編輯現有的 response 檔案。如需 response 檔案中各值的詳細資訊，請參閱 「編輯 response.ni 檔案」(第 64 頁)。
2. 使用管理員帳戶登入您要安裝 Identity Vault 的電腦。
3. 在啟用**以管理員身分執行**選項的情況下開啟指令提示符。
4. 在指令行中輸入以下指令：

   ```
   path_to_installation_files\windows\eDirectory\x64\NDSonNT>install.exe /silent /nopleasewait /
   template=Response file
   ```

   例如：

   ```
   D:\builds\eDirectory\windows\eDirectory\x64\NDSonNT>install.exe /silent /
   nopleasewait /template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
   ```

執行靜默組態

1 建立新的 response.ni 檔案，或編輯現有的 response 檔案。如需 response 檔案中各值的詳細資訊，請參閱 「編輯 response.ni 檔案」 (第 64 頁)。

2 使用管理員帳戶登入您要安裝 Identity Vault 的電腦。

3 在啟用**以管理員身分執行**選項的情況下開啟指令提示符。

4 在指令行中輸入以下指令：

```
Windows Drive\Program Files\Common Files\novell>install.exe /silent /restrictnoderemove /
nopleasewait /template=Response file
```

例如：

```
c:\Program Files\Common Files\novell>install.exe /silent /restrictnoderemove /nopleasewait /
template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
```

執行含組態設定的靜默安裝

在開始之前，請查看執行靜默或無人管理安裝的先決條件。如需詳細資訊，請參閱 第 7.1.2 節 「安裝 Identity Vault 的先決條件和考量」 (第 52 頁)。此外，請建立要用做安裝樣板的 response.ni 檔案。

1 建立新的 response.ni 檔案，或編輯現有的 response 檔案。如需 response 檔案中各值的詳細資訊，請參閱 「編輯 response.ni 檔案」 (第 64 頁)。

2 使用管理員帳戶登入您要安裝 Identity Vault 的電腦。

3 在啟用**以管理員身分執行**選項的情況下開啟指令提示符。

4 在指令行中輸入以下指令：

```
Unzipped Location\windows\eDirectory\x64\NDSonNT>install.exe /silent /nopleasewait /
template=Response file
```

例如：

```
D:\builds\eDirectory\windows\eDirectory\x64\NDSonNT>install.exe /silent /
nopleasewait /template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
```

7.4 安裝後設定 Identity Vault

安裝 Identity Vault 之後，您可能需要針對 Identity Vault 執行某些組態任務。

7.4.1 將 SecretStore 新增至 Identity Vault 綱要

必須擴充 Identity Vault 綱要以支援 SecretStore 功能。Identity Applications 需要使用 SecretStore 來連接 Identity Vault。

1 若要擴充 Identity Vault 的綱要，請輸入以下指令：

```
ice -S SCH -f C:\NetIQ\eDirectory\sssv3.sch -D LDAP -s serverIP -d adminDN
```

例如：

```
ice -S SCH -f C:\NetIQ\eDirectory\sssv3.sch -D LDAP -s 192.168.0.1 -d cn=admin,o=administrators
```

2 若要在 Windows 伺服器上設定 SecretStore，請完成以下步驟：

2a 導覽至 C:\NetIQ\eDirectory 目錄。

2b 輸入以下指令：

```
ssscfg.exe -c
```

2c 指定 SecretStore 的組態設定，然後關閉該公用程式。

2d 執行 NDSCons.exe。

2e 在該公用程式中，為 ssncp.dlm 模組指定 auto。

2f 關閉此公用程式。

如需詳細資訊，請參閱《*NetIQ eDirectory Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html)》(NetIQ eDirectory 管理指南) 中的「SecretStore Configuration for eDirectory Server」(適用於 eDirectory 伺服器的 SecretStore 組態)。

7.4.2 使用特定的地區設定進行 Identity Vault 設定

若要使用特定的地區設定進行 Identity Vault 設定，必須在執行組態設定前，先將 LC_ALL 和 LANG 輸出為該特定地區設定。例如，在 ndsconfig 公用程式中輸入以下指令：

```
export LC_ALL=ja
export LANG=ja
```

7.4.3 管理 eDirectory 例項

您可以建立、啟動和停止 Identity Vault 中的伺服器例項。您還可以檢視所設定例項的清單。

列出 Identity Vault 例項

可以使用 DHost iConsole 來檢視伺服器例項的組態檔案路徑、完全可辨識名稱和連接埠，以及所指定使用者的例項狀態 (使用中或非使用中)。

在 Identity Vault 中建立新例項

可使用 DHost 公用程式在 eDirectory 中建立新的例項。

在 Identity Vault 中設定和取消設定例項

可使用 DHost 公用程式在 Identity Vault 中設定和取消設定例項。

針對 Identity Vault 中的例項呼叫公用程式

您可以針對例項執行 DSTrace 等公用程式。

1 導覽至 C:\NetIQ\eDirectory 目錄。

2 執行 NDCCons.exe。

3 在 **NetIQ eDirectory 服務**主控台中，導覽至 dstrace.dlm。

4 按一下「**啟動**」。

在 Identity Vault 中啟動和停止例項

您可以啟動或停止您所設定的一或多個例項。

若要啟動某個例項：

1 導覽至 C:\NetIQ\eDirectory 目錄。

2 執行 NDCCons.exe。

3 導覽至某個例項，然後按一下**啟動**。

若要停止某個例項：

1 導覽至 C:\NetIQ\eDirectory 目錄。

2 執行 NDCCons.exe。

3 導覽至某個例項，然後按一下**停止**。

8 規劃安裝引擎、驅動程式和外掛程式

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

- 第 8.1 節「Identity Manager 引擎、驅動程式和外掛程式的安裝核對清單」(第 73 頁)
- 第 8.2 節「瞭解安裝程式」(第 74 頁)
- 第 8.3 節「安裝 Identity Manager 引擎的先決條件和考量」(第 74 頁)
- 第 8.4 節「Identity Manager 引擎的系統要求」(第 75 頁)

附註：此安裝程式還可以安裝遠端載入器。如需詳細資訊，請參閱第 10.2 節「安裝遠端載入器」(第 92 頁)。

8.1 Identity Manager 引擎、驅動程式和外掛程式的安裝核對清單

NetIQ 建議您在開始執行安裝程序之前先檢閱以下步驟。

	核對清單項目
❑	1. 瞭解 Identity Manager 各元件之間的互動。如需詳細資訊，請參閱第 1 章 「Identity Manager 的元件綜覽」(第 19 頁)。
❑	2. 確定要為 Identity Manager 的元件使用哪些伺服器。如需詳細資訊，請參閱第 5.3 節「建議的安裝情境和伺服器設定」(第 39 頁)。
❑	3. 檢閱關於安裝 Identity Manager 引擎的考量，以確保電腦符合先決條件。如需詳細資訊，請參閱第 8.3 節「安裝 Identity Manager 引擎的先決條件和考量」(第 74 頁)。
❑	4. 檢閱將要代管 Identity Manager 引擎的電腦需要符合的硬體和軟體要求。如需詳細資訊，請參閱「iManager 伺服器的系統要求」(第 128 頁)。
❑	5. 瞭解在安裝 Identity Manager 引擎後，哪些驅動程式會自動啟動。如需詳細資訊，請參閱第 8.3.2 節「隨 Identity Manager 引擎一起安裝驅動程式的考量」(第 75 頁)。
❑	6. 瞭解安裝程式中的選項。如需詳細資訊，請參閱第 8.2 節「瞭解安裝程式」(第 74 頁)。
❑	7. (視情況而定) 如需 Identity Manager 引擎的引導式安裝程序 (精靈)，請參閱第 9 節「安裝引擎、驅動程式和 iManager 外掛程式」(第 77 頁)。
❑	8. (視情況而定) 若要透過一個指令安裝元件，請參閱第 9.2 節「執行靜默安裝」(第 78 頁)。
❑	9. (視情況而定) 若要安裝遠端載入器，請參閱第 10.2 節「安裝遠端載入器」(第 92 頁)。
❑	10. 啟動遠端載入器中的驅動程式例項。如需詳細資訊，請參閱第 10.3 章 「設定遠端載入器和驅動程式」(第 96 頁)。

	核對清單項目
❑	11. 安裝其餘的 Identity Manager 元件，包括 Identity Applications 和 Identity Reporting。

8.2 瞭解安裝程式

為方便起見，此安裝程式綑綁了多個元件，這些元件提供了 Identity Manager 解決方案的基礎架構。您可以選擇將所有元件安裝在同一個伺服器上，或者安裝在不同的伺服器上。如需伺服器要求的詳細資訊，請參閱每個元件相應的規劃安裝引擎、驅動程式和外掛程式、各驅動程式的指南，以及最新的《版本說明》。

安裝程式提供了以下用於安裝元件的選項：

Identity Manager 伺服器

安裝 Identity Manager 引擎、綱要、NetIQ Audit 代理程式和 XDAS (分散式稽核服務)。

已連接系統伺服器 (32 位元、64 位元、.NET)

在載入器中安裝遠端載入器服務和驅動程式例項。借助遠端載入器，您可以在未代管 Identity Vault 和 Identity Manager 引擎的已連接系統上執行 Identity Manager 驅動程式。在安裝程式中，您可以選取要在已連接系統上隨遠端載入器一起安裝的驅動程式。

擴送代理程式

安裝 JDBC 擴送驅動程式的擴送代理程式。JDBC 擴送驅動程式使用擴送代理程式來建立多個 JDBC 擴送驅動程式例項。擴送代理程式依據擴送驅動程式中連接物件的組態載入 JDBC 驅動程式例項。如需詳細資訊，請參閱 《NetIQ Identity Manager Driver for JDBC Fan-Out Implementation Guide》 (NetIQ Identity Manager Driver for JDBC Fan-Out 實作指南)。

Identity Manager 的 iManager 外掛程式

安裝 iManager 外掛程式，這些外掛程式可讓您使用 iManager 來管理具有結構化全域組態值 (GCV) 的 Identity Manager 驅動程式。

驅動程式

Identity Manager 驅動程式可在多種類型的目錄、資料庫和業務應用程式以及 Identity Vault 之間同步化身分資訊。您可以將驅動程式設定為單向或雙向同步化資料。

在安裝程式中，您可以選取要隨其餘元件一起安裝的驅動程式。您可能需要在未代管 Identity Manager 引擎的伺服器上安裝一些驅動程式。在這種情況下，您還需要在該伺服器上安裝遠端載入器服務。

8.3 安裝 Identity Manager 引擎的先決條件和考量

本節提供安裝 Identity Manager 引擎和驅動程式的資訊。

- 第 8.3.1 節「安裝 Identity Manager 引擎的考量」(第 75 頁)
- 第 8.3.2 節「隨 Identity Manager 引擎一起安裝驅動程式的考量」(第 75 頁)

8.3.1 安裝 Identity Manager 引擎的考量

在安裝 Identity Manager 引擎之前，請檢閱以下考量：

- 在安裝 Identity Manager 引擎之前，您必須安裝 Identity Vault。此外，Identity Vault 必須包含至少具有一個組織單位、一個使用者和一個 iManager 伺服器的網路樹。
- 在代管 Identity Vault 的伺服器上安裝 Identity Manager 引擎。安裝程式將會根據 Identity Vault 的版本安裝 32 位元或 64 位元 Identity Manager。
- (視情況而定) 若要在 Identity Manager 引擎所在的同一個電腦上安裝遠端載入器，請務必選取對這兩個元件都提供支援的作業系統。如需遠端載入器系統要求的詳細資訊，請參閱第 10.1.6 節「安裝遠端載入器的先決條件和考量」(第 88 頁)。

8.3.2 隨 Identity Manager 引擎一起安裝驅動程式的考量

許多變數會影響安裝 Identity Manager 引擎之伺服器的效能，其中包括伺服器上執行的驅動程式數量。NetIQ 提供了以下建議，供您在規劃驅動程式的安裝位置時加以參考：

- 一般而言，伺服器上執行的驅動程式數量取決於驅動程式對伺服器施加的負載。有些驅動程式需要處理大量的物件，而有些驅動程式則不然。
- 如果您計劃讓每個驅動程式同步化數百萬個物件，則請限制伺服器上的驅動程式數量。例如，只部署 10 個以下此類驅動程式。
- 如果您計劃讓每個驅動程式同步化 100 個或更少的物件，則或許可以在伺服器上執行 10 個以上的驅動程式。
- 若要建立伺服器效能基線以協助確定最佳驅動程式數量，可以使用 iManager 中的狀態監控工具。如需狀態監控工具的詳細資訊，請參閱《*NetIQ Identity Manager Driver Administration Guide*》(NetIQ Identity Manager 驅動程式管理指南) 中的「Monitoring Driver Health」(監控驅動程式狀態)。

如需在安裝後啟用 Identity Manager 驅動程式的詳細資訊，請參閱第 30.6 節「啟用 Identity Manager」(第 310 頁)。

8.4 Identity Manager 引擎的系統要求

本節提供要安裝 Identity Manager 引擎的伺服器的最低要求。請務必檢閱安裝的先決條件和注意事項，特別是與作業系統有關的內容。

類別	要求
處理器	1 GHz
磁碟空間	◆ 300 MB ◆ 每 50,000 個使用者需要 150 MB 的額外磁碟空間
記憶體	◆ Identity Manager 引擎需要 2 GB ◆ Identity Manager 驅動程式需要 2 GB

類別	要求
作業系統 (已認證)	以下 64 位元作業系統之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 NetIQ 建議您在安裝 Identity Manager 之前，依照製造商的自動更新機制來套用最新的作業系統修補程式。 **附註：***已認證*指作業系統已進行全面測試且受支援。
作業系統 (受支援)	已認證作業系統的最新版 Service Pack **附註：***受支援*指作業系統尚未進行測試，但預期可正常運作。
虛擬化系統	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 及更新版本 ◆ 包含 Hyper-V 的 Windows Server 2012 R2 Virtualization (受支援) NetIQ 允許您在為執行 NetIQ 產品的作業系統提供官方支援的企業級虛擬化系統上執行 Identity Manager。只要虛擬化系統的廠商為這些作業系統提供官方支援，NetIQ 就支援在這些系統上執行整個 Identity Manager 堆疊。
其他軟體	◆ NetIQ eDirectory 9.1 ◆ iManager 3.1

9 安裝引擎、驅動程式和 iManager 外掛程式

本章介紹 Identity Manager 引擎、驅動程式、iManager 外掛程式和遠端載入器的安裝程序。您可以將這些元件安裝在同一個伺服器上，也可以安裝在不同的伺服器上。例如，您可能想將一個驅動程式安裝在某個連接的系統上，而不是 Identity Manager 引擎所在的那個伺服器上。在此情況下，您還要在這個連接的系統上安裝遠端載入器。

NetIQ 提供引導式安裝程序和靜默安裝模式。

- 第 9.1 節「使用精靈安裝元件」(第 77 頁)
- 第 9.2 節「執行靜默安裝」(第 78 頁)
- 第 9.3 節「在具有多個 Identity Vault 例項的伺服器上安裝」(第 79 頁)
- 第 9.4 節「停止和啟動 Identity Manager 驅動程式」(第 81 頁)

9.1 使用精靈安裝元件

安裝程式將引導您完成 Identity Manager 引擎的組態設定。安裝程式會自動預設為精靈模式。

若要進行安裝準備工作，請參閱第 8.1 節「Identity Manager 引擎、驅動程式和外掛程式的安裝核對清單」(第 73 頁)。另請參閱版本隨附的《版本說明》。若要執行無人管理安裝，請參閱第 9.2 節「執行靜默安裝」(第 78 頁)。

附註：是要以管理員還是非管理員使用者身分執行安裝，應該依您安裝 Identity Vault 時使用的方法而定。

9.1.1 以管理使用者身分安裝

本節介紹以管理使用者身分使用安裝精靈來安裝 Identity Manager 引擎的引導式程序。安裝程式的路徑為 \products\idm\windows\setup\idm_install.exe。

若要以管理使用者身分安裝 Identity Manager 引擎：

1. 以管理員身分登入要安裝 Identity Manager 引擎的電腦。
2. 在包含安裝檔案的目錄中，找到並執行 idm_install.exe。
3. 接受授權合約，然後按下一步。
4. 在「選取元件」視窗中，指定要安裝的元件。

   如需選項的詳細資訊，請參閱第 8.2 節「瞭解安裝程式」(第 74 頁)。
5. (選擇性) 若要為個別元件選取特定的驅動程式，請完成以下步驟：
   - **5a** 按一下自訂選定的元件，然後按下一步。
   - **5b** 展開要安裝的元件下方的驅動程式。
   - **5c** 選取要安裝的驅動程式。
6. 按一下「下一步」。

7 在「啟動通知」視窗中，按一下**確定**。如需詳細資訊，請參閱第 30.6 節「啟用 Identity Manager」(第 310 頁)。

8 對於「驗證」，請指定在 eDirectory 中有權延伸綱要的使用者帳戶及其密碼。以 LDAP 格式指定使用者名稱。例如 cn=admin,o=company。

9 在「安裝前摘要」中驗證設定。

10 按一下「**安裝**」。

11 啟用 Identity Manager。如需詳細資訊，請參閱第 30.6 節「啟用 Identity Manager」(第 310 頁)。

12 若要建立和設定驅動程式物件，請參閱該驅動程式的具體指南。如需詳細資訊，請造訪 Identity Manager 驅動程式文件網站。

13 (選擇性) 關於預設安裝位置，請參閱安裝記錄。例如 C:\Users\Admin1\AppData\Local\Temp\1\idmInstall.log。

9.2 執行靜默安裝

若要以靜默模式安裝 Identity Manager，請建立內含完成安裝所需參數的 properties 檔案。Identity Manager 媒體包含一個範例內容檔案，其路徑為 \products\idm\windows\setup\silent.properties。

若要執行靜默安裝：

1 在安裝目錄中，建立一個 properties 檔案或編輯範例 silent.properties 檔案。

2 使用文字編輯器在該檔案中指定以下參數：

EDITION_INPUT_RESULTS

指定 Identity Manager 伺服器的版本。例如，Advanced Edition 或 Standard Edition。安裝程式會使用此資訊設定指定的 Identity Manager 版本。

EDIR_USER_NAME

指定 Identity Vault 管理員帳戶的 LDAP 可辨識名稱。例如 c=admin,o=netiq。安裝程式使用此帳戶將 Identity Manager 引擎連接到 Identity Vault。

您可能需要將此參數新增至範例 silent.properties 檔案中。

EDIR_USER_PASSWORD

指定 Identity Vault 管理員帳戶的密碼。例如 netiq123。您可能需要將此參數新增至範例 silent.properties 檔案中。

如果不想在檔案中包含密碼，請將該欄位保留空白。這樣，安裝程式就會從 EDIR_USER_PASSWORD 環境變數中讀取該值。請確保指定了 EDIR_USER_PASSWORD 環境變數。

METADIRECTORY_SERVER_SELECTED

指定是否要安裝 Identity Manager 伺服器和驅動程式。

CONNECTED_SYSTEM_SELECTED

指定是否要安裝 32 位元遠端載入器服務和驅動程式。可以在同一個伺服器上安裝 32 位元和 64 位元版本。

FANOUTAGENT_SELECTED

指定是否要安裝 JDBC 驅動程式的擴送代理程式。

X64_CONNECTED_SYSTEM_SELECTED

指定是否要安裝 64 位元遠端載入器服務和驅動程式。可以在同一個伺服器上安裝 32 位元和 64 位元版本。

WEB_ADMIN_SELECTED

適用於您先前已安裝 iManager 的情況。

指定是否要安裝 iManager 外掛程式。

UTLITIES_SELECTED

指定是否要安裝公用程式和遠端載入器的系統元件。

DOT_NET_REMOTELOADER_SELECTED

指定是否要在 Windows 伺服器上安裝 .NET 遠端載入器服務和驅動程式。

EDIR_NDS_CONF

指定 Identity Vault 組態檔案的路徑。

如果您有多個 Identity Vault 例項，請指定每個例項的相應值。

EDIR_IP_ADDRESS

指定 Identity Vault 的 IP 位址。

如果您有多個 Identity Vault 例項，請指定每個例項的位址。

EDIR_NCP_PORT

指定 Identity Vault 的連接埠號。

如果您有多個 Identity Vault 例項，請指定每個例項的連接埠。

3 若要執行靜默安裝，請從 properties 檔案所在的目錄執行以下指令： install.exe -i silent -f *檔案名稱* .properties

4 (選擇性) 關於預設安裝位置，請參閱安裝記錄。例如 C:\Users\Admin1\AppData\Local\Temp\1\idmInstall.log。

9.3 在具有多個 Identity Vault 例項的伺服器上安裝

Identity Manager 支援以管理使用者身分在靜默模式下執行此安裝。此程序需要您為要安裝 Identity Manager 的每個 Identity Vault 例項建立一個 silent.properties 檔案。

若要在靜默模式下安裝 Identity Manager，請執行以下步驟：

1 檢閱第 8 章 「規劃安裝引擎、驅動程式和外掛程式」 (第 73 頁) 中的先決條件和系統要求。

2 依照第 9.2 節 「執行靜默安裝」 (第 78 頁) 中的說明操作。

   2a 確認 silent.properties 檔案包含以下設定：

```
EDITION_INPUT_RESULTS=Advanced Edition
EDIR_USER_NAME=cn=admin_name,o=organization_name
EDIR_USER_PASSWORD=identity_vault_password
METADIRECTORY_SERVER_SELECTED=true
CONNECTED_SYSTEM_SELECTED=false
X64_CONNECTED_SYSTEM_SELECTED=false
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
FANOUTAGENT_SELECTED=false
EDIR_NCP_PORT=<ncp_port>
EDIR_NDS_CONF=</path/to/edir/conf>
EDIR_IP_ADDRESS=ip_address_for_identity_vault

# For Customization use the following properties
CUSTOM_SELECTED=true
# engine custom list engine and drivers jdbc and delim
CHOSEN_INSTALL_FEATURE_LIST_SERVER=ENGINE,JDBC,DELIM,additional_value
```

2b 您可以包括以下額外的值以自訂引擎清單：

- Server_DRIVERS
- AD
- EBSHR
- EBSTCA
- EBSUM
- DELIM
- EDIR
- BIEDIR
- JDBC
- JMS
- LDAP
- NXSET
- 備註
- PS
- REMEDY
- SAPUMJ
- SAPHR
- SAPBL
- SAPPORTAL
- SOAP
- REST
- SFORCE
- SENTREST
- BLACK
- BANNER
- GOOGLE
- AR

- NPUM
- TSS
- RACF
- AFC2
- UAD
- RRSD

3 (視情況而定) 若要驗證安裝是否成功，請在安裝記錄檔案中尋找下面幾行。例如 C:\Users\Admin1\AppData\Local\Temp\1\idmInstall.log 檔案。

```
NDS schema extension complete.
exitValue=0
Schema extended
SCHEMA_EXTENDED=true
==== UpdateIDMConfigureStatus ============================
stateFile: C:\IDM\Uninstall_Identity_Manager\idmconfigure_state.conf
INSTALL_SUCCESS: SUCCESS
enter loop:
==== Complete ============================================
INSTALL_SUCCESS=SUCCESS
```

9.4 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，以確保安裝或升級程序能夠修改或取代正確的檔案。本節將介紹以下活動：

- 第 9.4.1 節「停止驅動程式」(第 81 頁)
- 第 9.4.2 節「啟動驅動程式」(第 82 頁)

9.4.1 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 來停止驅動程式」(第 81 頁)
- 「使用 iManager 來停止驅動程式」(第 82 頁)

使用 Designer 來停止驅動程式

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 iManager 來停止驅動程式

1 在 iManager 中，選取 **Identity Manager > Identity Manager 綜覽**。
2 瀏覽並選取網路樹中的位置，來搜尋「驅動程式集」物件，然後按一下搜尋圖示。
3 按一下「驅動程式集」物件。
4 按一下「**驅動程式**」>「**停止所有驅動程式**」。
5 對每個「驅動程式集」物件，重複步驟 2 到步驟 4。
6 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：
   - **6a** 在 iManager 中，選取 **Identity Manager > Identity Manager 綜覽**。
   - **6b** 瀏覽並選取網路樹中的位置，來搜尋「驅動程式集」物件，然後按一下搜尋圖示。
   - **6c** 按一下「驅動程式集」物件。
   - **6d** 在驅動程式圖示的右上角按一下「**編輯內容**」。
   - **6e** 在「驅動程式組態」頁面的「**啟動選項**」下，選取「**手動**」，然後按一下「**確定**」。
   - **6f** 對網路樹中的每一個驅動程式，重複步驟 6a 到步驟 6e。

9.4.2 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 來啟動驅動程式」（第 82 頁）
- 「使用 iManager 來啟動驅動程式」（第 82 頁）

使用 Designer 來啟動驅動程式

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 iManager 來啟動驅動程式

1 在 iManager 中，選取「**Identity Manager**」>「**Identity Manager 綜覽**」。
2 瀏覽並選取網路樹中的位置，來搜尋「驅動程式集」物件，然後按一下搜尋圖示。
3 按一下「驅動程式集」物件。
4 按一下「**驅動程式**」>「**啟動所有驅動程式**」，來同時啟動所有驅動程式。

或

在驅動程式圖示的右上角，按一下「**啟動驅動程式**」來個別地啟動每一個驅動程式。

5 如果有多個驅動程式，請重複步驟 2 到步驟 4。

6 設定驅動程式啟動選項：

   6a 在 iManager 中，選取「**Identity Manager**」> 「**Identity Manager 綜覽**」。

   6b 瀏覽至網路樹中要搜尋驅動程式集物件的位置並加以選取，然後按一下搜尋圖示 ▶。

   6c 按一下「驅動程式集」物件。

   6d 在驅動程式圖示的右上角按一下「**編輯內容**」。

   6e 在「驅動程式組態」頁面的「**啟動選項**」下，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**」。

   6f 對每個驅動程式重複步驟 6b 到步驟 6e。

7 測試驅動程式來驗證規則是否如設計般運作。

   iManager 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 安裝和管理遠端載入器

本章介紹如何安裝遠端載入器、.NET 遠端載入器或 Java 遠端載入器，以及在載入器中設定驅動程式例項。

遠端載入器的安裝程式與 Identity Manager 引擎綑綁在一起。這些檔案位於 Identity Manager 安裝套件的 \products\idm 目錄中。依預設，安裝程式會在 C:\Netiq 中安裝元件。

NetIQ 建議您在開始之前檢閱安裝程序。如需詳細資訊，請參閱第 10.1.1 節「遠端載入器安裝核對清單」(第 85 頁)。

10.1 規劃安裝遠端載入器

本節提供的資訊可協助您為安裝 .NET 遠端載入器做好準備。

- 第 10.1.1 節「遠端載入器安裝核對清單」(第 85 頁)
- 第 10.1.2 節「瞭解遠端載入器」(第 86 頁)
- 第 10.1.3 節「瞭解 Java 遠端載入器」(第 88 頁)
- 第 10.1.4 節「瞭解安裝程式」(第 88 頁)
- 第 10.1.5 節「在同一個電腦上使用 32 位元和 64 位元遠端載入器」(第 88 頁)
- 第 10.1.6 節「安裝遠端載入器的先決條件和考量」(第 88 頁)
- 第 10.1.7 節「遠端載入器的系統要求」(第 90 頁)

10.1.1 遠端載入器安裝核對清單

NetIQ 建議您完成以下核對清單中的步驟：

	核對清單項目
❑	1. 瞭解 Identity Manager 各元件之間的互動。如需詳細資訊，請參閱第 1 章「Identity Manager 的元件綜覽」(第 19 頁)。
❑	2. 確定要為 Identity Manager 的元件使用哪些伺服器。如需詳細資訊，請參閱第 5.3 節「建議的安裝情境和伺服器設定」(第 39 頁)。
❑	3. 確保 Identity Manager 引擎已安裝。如需詳細資訊，請參閱第 9 章「安裝引擎、驅動程式和 iManager 外掛程式」(第 77 頁)
❑	4. 檢閱關於安裝遠端載入器的考量，以確保電腦符合先決條件。如需詳細資訊，請參閱第 10.1.6 節「安裝遠端載入器的先決條件和考量」(第 88 頁)。
❑	5. 檢閱將要代管遠端載入器的電腦需要符合的硬體和軟體要求。如需詳細資訊，請參閱第 10.1.7 節「遠端載入器的系統要求」(第 90 頁)。

	核對清單項目
❑	6. (視情況而定) 若要在未代管 Identity Manager 引擎的伺服器上安裝遠端載入器，請確保您能與該引擎建立安全連接。如需詳細資訊，請參閱第 10.3.1 節「與 Identity Manager 引擎建立安全連接」(第 97 頁)。
❑	7. 確定是要安裝 32 位元還是 64 位元版本的遠端載入器。如需詳細資訊，請參閱第 10.1.5 節「在同一個電腦上使用 32 位元和 64 位元遠端載入器」(第 88 頁)。
❑	8. 安裝遠端載入器： ◆ 若要執行引導式安裝，請參閱第 10.2.1 節「使用精靈安裝遠端載入器」(第 92 頁)。 ◆ 若要執行靜默安裝，請參閱第 10.2.5 節「執行遠端載入器的靜默安裝」(第 96 頁)。
❑	9. (視情況而定) 若要安裝 .NET 遠端載入器，請參閱第 10.2.4 節「安裝 .NET 遠端載入器」(第 95 頁)。
❑	10. 檢閱用於設定驅動程式例項的參數。如需詳細資訊，請參閱第 10.3.2 節「瞭解遠端載入器的組態參數」(第 99 頁)。
❑	11. 若要設定遠端載入器中的驅動程式例項，請參閱下列其中一節： ◆ 第 10.3.3 節「為驅動程式例項設定遠端載入器」(第 107 頁) ◆ 第 10.3.4 節「為驅動程式例項設定 Java 遠端載入器」(第 110 頁) ◆ 第 10.3.5 節「為驅動程式例項設定 .NET 遠端載入器」(第 111 頁)
❑	12. 準備遠端載入器的驅動程式。如需詳細資訊，請參閱第 10.3.6 節「設定 Identity Manager 驅動程式以與遠端載入器配合使用」(第 113 頁)。
❑	13. 啟動遠端載入器中的驅動程式例項。如需詳細資訊，請參閱第 10.4.1 節「啟動遠端載入器中的驅動程式例項」(第 123 頁)。
❑	14. (視情況而定) 若要設定遠端載入器與 Identity Manager 引擎間的雙向驗證，請參閱第 10.3.7 節「設定與 Identity Manager 引擎的雙向驗證」(第 114 頁)。
❑	15. 驗證遠端載入器和驅動程式是否可與 Identity Manager 引擎和已連接系統通訊。如需詳細資訊，請參閱第 10.3.8 節「驗證組態」(第 122 頁)。
❑	16. 安裝其餘的 Identity Manager 元件，包括 Identity Applications 和 Identity Reporting。

10.1.2 瞭解遠端載入器

借助遠端載入器，您可以在未代管 Identity Vault 和 Identity Manager 引擎的已連接系統上執行 Identity Manager 驅動程式。.NET 遠端載入器只在 Windows 系統上運作。

遠端載入器可以透過 JNI 代管平台特定檔案中包含的 Identity Manager 應用程式 shim，並且還可代管適用於各種平台的 JAR 檔案中包含的較常見 Identity Manager 應用程式 shim。遠端載入器可以在任何平台上執行。但是，平台特定的 shim 必須在其原生平台上執行。

瞭解 Shim

遠端載入器使用 shim 來與受管理系統上的應用程式通訊。*Shim* 是一或多個檔案，其中包含的程式碼可以處理在 Identity Vault 與應用程式之間同步化的事件。在使用遠端載入器之前，您必須設定應用程式 shim，以與 Identity Manager 引擎進行安全地連接。此外，您還必須設定遠端載入器和 Identity Manager 驅動程式。

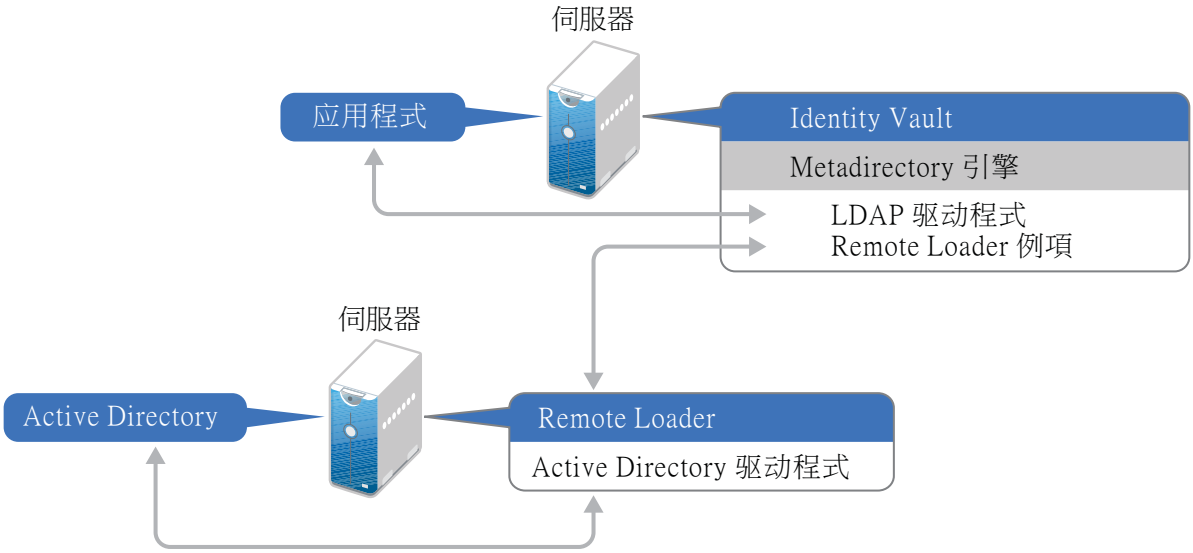
如需詳細資訊，請參閱第 10.3 章 「設定遠端載入器和驅動程式」 (第 96 頁)。

確定何時使用遠端載入器

您可以在同一個伺服器上安裝 Identity Manager 引擎、Identity Vault 和驅動程式 shim。Identity Manager 引擎做為 eDirectory 程序的一部分執行。Identity Manager 驅動程式可以在 Identity Manager 所在的伺服器上執行。它們也可以做為 Identity Manager 引擎所屬程序的一部分執行。但是，對於以下情況，您可能希望 Identity Manager 驅動程式在代管 Identity Manager 引擎的伺服器上做為獨立程序執行。

- 防止 Identity Vault 在驅動程式 shim 發生任何例外時受到影響。
- 透過將驅動程式指令負載卸載到遠端應用程式或資料庫，來改進執行 Identity Manager 引擎的伺服器效能。
- 在未代管 Identity Manager 引擎的伺服器上執行更多驅動程式。

針對這些情況，遠端載入器在 Identity Manager 引擎與驅動程式之間提供了一個通訊通道。例如，您在 Identity Manager 引擎和 Identity Vault 所在的同一個伺服器上安裝了 LDAP 驅動程式。然後，您在裝有遠端載入器的另一個伺服器上安裝了 Active Directory (AD) 驅動程式。若要使這些驅動程式能夠存取應用程式並與 Identity Vault 通訊，請依下圖所示，在兩部伺服器上都安裝遠端載入器：



NetIQ 建議您盡可能對您的驅動程式使用遠端載入器組態。即使應用程式位於 Identity Manager 引擎所在的同一個伺服器上，也應該使用遠端載入器。

10.1.3 瞭解 Java 遠端載入器

Java 遠端載入器是一個 Java 應用程式。您可以將 Java 遠端載入器與任何公開支援的 Java 版本配合使用。

若要設定驅動程式的 Java 遠端載入器，請參閱第 10.3.4 節「為驅動程式例項設定 Java 遠端載入器」(第 110 頁)。

10.1.4 瞭解安裝程式

為方便起見，此安裝程式綑綁了多個元件，這些元件提供了 Identity Manager 解決方案的基礎架構。您可以選擇將所有元件安裝在同一個伺服器上，或者安裝在不同的伺服器上。除了遠端載入器以外，您還可以選取要在連接的系統上安裝的驅動程式。此安裝套件提供適用於 Windows 作業系統的 .NET 遠端載入器選項。

10.1.5 在同一個電腦上使用 32 位元和 64 位元遠端載入器

依預設，安裝程式會偵測作業系統的版本，然後安裝相應版本的遠端載入器。您可以在 64 位元作業系統上安裝 32 位元和 64 位元遠端載入器：

- 如果您要升級 64 位元作業系統上安裝的 32 位元遠端載入器，升級程序會將 32 位元遠端載入器升級至最新版本，並且還會安裝 64 位元遠端載入器。
- 如果您選擇在同一台電腦上安裝 32 位元和 64 位元遠端載入器，則稽核事件將僅會透過 64 位元遠端載入器產生。如果 64 位元遠端載入器在 32 位元遠端載入器之前安裝，則事件會記錄到 32 位元快取中。

10.1.6 安裝遠端載入器的先決條件和考量

NetIQ 建議您在安裝遠端載入器之前檢閱以下考量：

- 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。
- 可以在安裝了 Identity Manager 引擎的同一台電腦上安裝遠端載入器。
- 可以在同一台電腦上安裝 32 位元和 64 位元遠端載入器。
- 可以在不支援原生遠端載入器的平台上安裝 Java 遠端載入器。如需受支援平台的詳細資訊，請參閱第 10.1.7 節「遠端載入器的系統要求」(第 90 頁)。
- (視情況而定) 若要將 Identity Manager 連接到 Active Directory，您必須在屬於成員伺服器或網域控制器的伺服器上安裝遠端載入器和適用於 Active Directory 的驅動程式。不需要在連接的系統所在的同一個伺服器上安裝 eDirectory 和 Identity Manager。遠端載入器會將來自 Active Directory 的所有事件傳送至 Identity Manager 伺服器。然後，遠端載入器會接收來自 Identity Manager 伺服器的任何資訊，並將其傳遞給連接的應用程式。
- NetIQ 建議您盡可能對您的驅動程式使用遠端載入器組態。即使連接的系統位於 Identity Manager 伺服器引擎所在的同一個伺服器上，也應該使用遠端載入器。

  在遠端載入器組態中執行驅動程式 shim 具有以下優勢：

  - 在驅動程式 shim 之間實現記憶體與處理隔離，從而改進效能並增強 Identity Manager 解決方案監控能力。
  - 修補和升級驅動程式 shim 時不會影響到 eDirectory 或其他驅動程式。

    - 保護 eDirectory 不受驅動程式 shim 中可能發生的嚴重問題的影響。
    - 將驅動程式 shim 的負載分散到其他伺服器。
- 以下驅動程式支援遠端載入器功能：
    - Active Directory
    - Access Review
    - ACF2
    - Azure Active Directory
    - 標題頁
    - Blackboard
    - 資料收集服務
    - 分隔文字
    - GoogleApps
    - REST
    - GroupWise 2014 (適用於 32 位元遠端載入器)
    - JDBC
    - JMS
    - LDAP
    - Linux 設定
    - Lotus Notes
    - 受管理系統閘道
    - 手動任務服務
    - Null and Loopback
    - Office 365
    - Oracle EBS HRMS
    - Oracle EBS TCA
    - Oracle EBS User Management
    - PeopleSoft 5.2
    - Privileged User Management
    - 補救
    - SalesForce.com
    - SAP 業務邏輯
    - SAP 入口網站
    - SAP HR (不受 Java 遠端載入器的支援)
    - SAP User Management (不受 Java 遠端載入器的支援)
    - ServiceNow
    - Integration Module V2.0 for Sentinel
    - SharePoint
    - SOAP

    - 最高機密
    - 工作順序
- 以下驅動程式不支援遠端載入器：
    - 雙向 eDirectory
    - eDirectory
    - 授權服務
    - 角色服務
    - 使用者應用程式

如需 Identity Manager 遠端載入器的詳細資訊，請參閱「The Many Faces of Remote Loader in Identity Manager」(Identity Manager 中遠端載入器的多面孔)。

10.1.7 遠端載入器的系統要求

本節提供要安裝遠端載入器、.NET 遠端載入器和 Java 遠端載入器的伺服器的最低要求。

遠端載入器 32 位元和 64 位元

類別	要求
處理器	1 GHz 處理器
記憶體	512 MB
作業系統 (已認證)	以下 64 位元作業系統之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 對於 32 位元作業系統： ◆ Windows Server 2008 SP2 **重要：**Lotus Notes Client 僅受工作站平台的支援。在 Windows XP、Windows 7 和 8 及 SLED 32 位元上執行的遠端載入器僅支援用於 Lotus Notes 驅動程式整合。在一般的 Identity Manager 安裝中，遠端載入器僅受伺服器平台的支援。 NetIQ 建議您在安裝 Identity Manager 之前，依照製造商的自動更新機制來套用最新的作業系統修補程式。 **附註：***已認證*指作業系統已進行全面測試且受支援。
作業系統 (受支援)	已認證作業系統的最新版 Service Pack **附註：***受支援*指作業系統尚未進行測試，但預期可正常運作。

類別	要求
虛擬化系統	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 及更新版本 ◆ 包含 Hyper-V 的 Windows Server 2012 R2 Virtualization (受支援) NetIQ 允許您在為執行 NetIQ 產品的作業系統提供官方支援的企業級虛擬化系統上執行 Identity Manager。只要虛擬化系統的廠商為這些作業系統提供官方支援，NetIQ 就支援在這些系統上執行整個 Identity Manager 堆疊。

.NET 遠端載入器

.NET 遠端載入器專用於與以 Windows 為基礎的伺服器配合使用。

類別	要求
處理器	Pentium* III 600MHz 處理器
記憶體	512 MB
作業系統 (已認證)	以下 64 位元作業系統之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 對於 32 位元作業系統： ◆ Windows Server 2008 SP2 NetIQ 建議您在安裝 Identity Manager 之前，依照製造商的自動更新機制來套用最新的作業系統修補程式。 **附註：***已認證*指作業系統已進行全面測試且受支援。
作業系統 (受支援)	已認證作業系統的最新版 Service Pack **附註：***受支援*指作業系統尚未進行測試，但預期可正常運作。
虛擬化系統	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.5 ◆ 包含 Hyper-V 的 Windows Server 2012 R2 Virtualization (受支援) NetIQ 允許您在為執行 NetIQ 產品的作業系統提供官方支援的企業級虛擬化系統上執行 Identity Manager。只要虛擬化系統的廠商為這些作業系統提供官方支援，NetIQ 就支援在這些系統上執行整個 Identity Manager 堆疊。
.NET Framework	4.x

Java 遠端載入器

Java 遠端載入器可以在裝有相容 JRE 和 Java Sockets 的任何連接的系統上執行。

類別	要求
處理器	Pentium* III 600MHz (最低要求)
記憶體	遠端載入器需要 512 MB
JRE	Java8u162 (最低要求) **附註：**您可以將 Java 遠端載入器與任何公開支援的 Java 版本配合使用。
平台代理程式	PA v2011.1r6

10.2 安裝遠端載入器

遠端載入器主控台使用 rlconsole.exe 來與 dirxml_remote.exe 互動，後者是一個可執行檔，可使 Identity Manager 引擎伺服器能夠與執行的 Identity Manager 驅動程式通訊。

- 第 10.2.1 節「使用精靈安裝遠端載入器」(第 92 頁)
- 第 10.2.2 節「執行遠端載入器的靜默安裝」(第 93 頁)
- 第 10.2.3 節「安裝 Java 遠端載入器」(第 94 頁)
- 第 10.2.4 節「安裝 .NET 遠端載入器」(第 95 頁)
- 第 10.2.5 節「執行遠端載入器的靜默安裝」(第 96 頁)

10.2.1 使用精靈安裝遠端載入器

安裝程式將引導您完成遠端載入器的組態設定。本節介紹使用安裝精靈安裝遠端載入器的引導式程序。安裝程式位於 \products\idm\windows\setup\ 目錄中。

若要進行安裝準備工作，請參閱第 10.1.1 節「遠端載入器安裝核對清單」(第 85 頁)。另請參閱版本隨附的《版本說明》。若要執行無人管理安裝，請參閱第 9.2 節「執行靜默安裝」(第 78 頁)。

附註：是要以管理員還是非管理員使用者身分執行安裝，應該依您安裝 Identity Vault 時使用的方法而定。

若要安裝「遠端載入器」：

1. 登入您要安裝遠端載入器的電腦。

   附註：您可以使用非管理員使用者身分安裝 Java 遠端載入器。

2. 導覽至 \products\idm\windows\setup\ 目錄。
3. 執行 idm_install.exe 程式。
4. 接受授權合約，然後按下一步。
5. 在選取元件視窗中，指定要安裝的遠端載入器元件。

   如需選項的詳細資訊，請參閱第 8.2 節「瞭解安裝程式」(第 74 頁)。

6 (選擇性) 若要為個別元件選取特定的驅動程式，請完成以下步驟：

   6a 按一下自訂選定的元件，然後按下一步。

   6b 展開要安裝的元件下方的驅動程式。

   6c 選取要安裝的驅動程式。

7 按一下「下一步」。

8 在啟動通知視窗中，按一下確定。

9 對於「驗證」，請指定在 eDirectory 中有權延伸綱要的使用者帳戶及其密碼。以 LDAP 格式指定使用者名稱。例如 cn=admin,o=company。

10 在「安裝前摘要」中驗證設定。

11 按一下「安裝」。

12 啟用 Identity Manager。如需詳細資訊，請參閱第 30.6 節「啟用 Identity Manager」(第 310 頁)。

13 設定遠端載入器，以便與驅動程式和 Identity Manager 連接。如需詳細資訊，請參閱第 10.3 章「設定遠端載入器和驅動程式」(第 96 頁)。

14 若要建立和設定驅動程式物件，請參閱該驅動程式的具體指南。如需詳細資訊，請造訪 Identity Manager 驅動程式文件網站。

15 (選擇性) 關於預設安裝位置，請參閱安裝記錄檔案。例如 C:\Users\Admin1\AppData\Local\Temp\1\idmInstall.log。

10.2.2 執行遠端載入器的靜默安裝

若要以靜默模式安裝遠端載入器，請建立包含完成安裝所需參數的 properties 檔案。Identity Manager 媒體中包含了一個範例 properties 檔案。依預設，該範例內容檔案位於 \products\idm\windows\setup\ 目錄中。

若要執行靜默安裝：

1 登入您要安裝遠端載入器的電腦。

2 導覽至 \products\idm\windows\setup\ 目錄。

3 建立一個 properties 檔案，或編輯範例 silent.properties 檔案。

4 在該檔案中指定以下參數：

   CONNECTED_SYSTEM_SELECTED

   指定是否要安裝 32 位元遠端載入器服務和驅動程式。可以在同一個伺服器上安裝 32 位元和 64 位元版本。

   X64_CONNECTED_SYSTEM_SELECTED

   指定是否要安裝 64 位元遠端載入器服務和驅動程式。可以在同一個伺服器上安裝 32 位元和 64 位元版本。

   UTLITIES_SELECTED

   指定是否要安裝公用程式和遠端載入器的系統元件。

   DOT_NET_REMOTELOADER_SELECTED

   指定是否要安裝 .NET 遠端載入器服務和驅動程式。

5 若要執行靜默安裝，請從指令提示符執行以下指令：

   install.exe -i silent -f *檔案名稱* .properties

10.2.3 安裝 Java 遠端載入器

Identity Manager 會使用 Java 遠端載入器，在一部伺服器上執行的 Identity Manager 引擎與其他位置 (該位置未執行 rdxml) 執行的 Identity Manager 驅動程式之間交換資料。您可以在裝有相容 JRE (最低為 1.8.0) 和 Java 通訊端的任何受支援 Windows 平台上安裝 Java 遠端載入器 dirxml_jremote。

1 在代管 Identity Manager 引擎的伺服器上，複製位於預設位置的應用程式 Shim .iso 或 .jar 檔案。例如，C:\NetIQ\idm\NDS\lib 目錄。

2 登入您要安裝 Java 遠端載入器的電腦 (目標電腦)。

3 驗證目標電腦是否裝有受支援版本的 JRE。

4 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) 如果您已取得 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 products\idm\java_remoteloader)。

   4b (視情況而定) 如果您已從 NetIQ 下載網站下載了 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 C:\NetIQ\idm。

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，使用 7-Zip 或受支援的軟體解壓縮 .tar.gz 檔案。

8 將 CLASSPATH 環境變數設定至存在於 lib 資料夾中的所有 jar。如果您有特定於任何驅動程式的相依 jar，請將這些 jar 檔案複製到 lib 資料夾，然後也將 CLASSPATH 環境變數設定至這些 jar。

   例如，進行如下設定：

```
CLASSPATH=E:\RL\JAVARL\lib\activation.jar;E:\RL\JAVARL\lib\commondrivershim.jar;E:\RL\JAVARL\l
ib\delimitedtextshim.jar;E:\RL\JAVARL\lib\delimitedtextutil.jar;E:\RL\JAVARL\lib\dirxml.jar;E:
\RL\JAVARL\lib\dirxml_misc.jar;E:\RL\JAVARL\lib\dirxml_remote.jar;E:\RL\JAVARL\lib\jco3environ
ment.jar;E:\RL\JAVARL\lib\mail.jar;E:\RL\JAVARL\lib\mapdb.jar;E:\RL\JAVARL\lib\nxsl.jar;E:\RL\
JAVARL\lib\shimwrapper.jar;E:\RL\JAVARL\lib\xds.jar;E:\RL\JAVARL\lib\xp.jar
```

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

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。

   dirxml_jremote.tar.gz jar 檔案包含此檔案。如需詳細資訊，請參閱第 10.3 章 「設定遠端載入器和驅動程式」(第 96 頁)。

12 使用以下指令啟動遠端載入器：

   12a 若要指定遠端載入器密碼：

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

例如，

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

12b 若要啟動遠端載入器：

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

例如，

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

12c 若要停止遠端載入器：

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

例如，

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

10.2.4 安裝 .NET 遠端載入器

若要以管理使用者身分安裝 .NET 遠端載入器：

1. 以管理員身分登入要安裝 .NET 遠端載入器的電腦。
2. 若要存取安裝程式，請完成下列其中一個步驟：
   - **2a** (視情況而定) 如果您已取得 Identity Manager 安裝套件的 .iso 影像檔，請導覽至包含 .Net 遠端載入器安裝檔案的目錄 (預設為 \products\idm\windows\setup\ 目錄)。
   - **2b** (視情況而定) 如果您已從 NetIQ 下載網站下載了 .NET 遠端載入器安裝檔案，請完成以下步驟：
     - 導覽至所下載影像的 .tgz 檔案。
     - 將該檔案的內容擷取到本地電腦上的某個資料夾中。
3. 執行安裝目錄中的 idm_install.exe 程式。
4. 接受授權合約，然後按下一步。
5. 在「選取元件」視窗中，指定「.NET 遠端載入器」。

   如需選項的詳細資訊，請參閱第 8.2 節「瞭解安裝程式」(第 74 頁)。
6. (選擇性) 若要為個別元件選取特定的驅動程式，請完成以下步驟：
   - **6a** 按一下自訂選定的元件，然後按下一步。
   - **6b** 展開要安裝的元件下方的驅動程式。
   - **6c** 選取要安裝的驅動程式。
7. 按一下「下一步」。
8. 在啟動通知視窗中，按一下確定。

9 選取 .NET 遠端載入器在您電腦上的安裝目錄。

10 查看「摘要」頁面，然後按一下**安裝**以完成安裝。

10.2.5 執行遠端載入器的靜默安裝

若要以靜默模式安裝遠端載入器，請建立包含完成安裝所需參數的內容檔案。Identity Manager 媒體包含一個範例內容檔案，其路徑為 \products\idm\windows\setup\silent.properties。

若要執行靜默安裝：

1 在安裝目錄中，建立一個 properties 檔案或編輯範例 silent.properties 檔案。

2 使用文字編輯器在該檔案中指定以下參數：

CONNECTED_SYSTEM_SELECTED

指定是否要安裝 32 位元遠端載入器服務和驅動程式。可以在同一個伺服器上安裝 32 位元和 64 位元版本。

X64_CONNECTED_SYSTEM_SELECTED

指定是否要安裝 64 位元遠端載入器服務和驅動程式。可以在同一個伺服器上安裝 32 位元和 64 位元版本。

UTLITIES_SELECTED

指定是否要安裝公用程式和遠端載入器的系統元件。

DOT_NET_REMOTELOADER_SELECTED

指定是否要在 Windows 伺服器上安裝 .Net 遠端載入器服務和驅動程式。

3 若要執行靜默安裝，請執行以下指令：

install.exe -i silent -f *檔案名稱* .properties

4 (選擇性) 關於預設安裝位置，請參閱安裝記錄檔案。例如 C:\Users\Admin1\AppData\Local\Temp\1\idmInstall.log。

10.3 設定遠端載入器和驅動程式

遠端載入器可以代管 .dll、.so 或 .jar 檔案中包含的 Identity Manager 應用程式 shim。Java 遠端載入器只代管 Java 驅動程式 Shim。它不能載入或代管原生 (C++) 驅動程式 Shim。

在使用遠端載入器之前，您必須設定應用程式 shim，以與 Identity Manager 引擎進行安全地連接。此外，您還必須設定遠端載入器和 Identity Manager 驅動程式。如需 shim 的詳細資訊，請參閱「瞭解 Shim」(第 87 頁)。

- 第 10.3.1 節「與 Identity Manager 引擎建立安全連接」(第 97 頁)
- 第 10.3.2 節「瞭解遠端載入器的組態參數」(第 99 頁)
- 第 10.3.3 節「為驅動程式例項設定遠端載入器」(第 107 頁)
- 第 10.3.4 節「為驅動程式例項設定 Java 遠端載入器」(第 110 頁)
- 第 10.3.5 節「為驅動程式例項設定 .NET 遠端載入器」(第 111 頁)
- 第 10.3.6 節「設定 Identity Manager 驅動程式以與遠端載入器配合使用」(第 113 頁)
- 第 10.3.7 節「設定與 Identity Manager 引擎的雙向驗證」(第 114 頁)
- 第 10.3.8 節「驗證組態」(第 122 頁)

10.3.1 與 Identity Manager 引擎建立安全連接

您必須確保資料能夠在遠端載入器與 Identity Manager 引擎之間安全傳輸。NetIQ 建議使用輸送層安全性 / 安全通訊端層 (TLS/SSL) 通訊協定來通訊。若要支援 TLS/SSL 連接，您需要有金鑰儲存區檔案或 KMO 中儲存的相應自行簽署證書。本節說明如何建立、輸出和儲存該證書。

附註：請在代管 Identity Manager 引擎與代管遠端載入器的伺服器上使用相同的 SSL 版本。如果伺服器上的 SSL 與遠端載入器上的 SSL 版本不相符，伺服器將會傳回 SSL3_GET_RECORD：錯誤的版本號碼錯誤訊息。此訊息僅用於警告目的，伺服器與遠端載入器之間的通訊並不會中斷。不過，該錯誤可能會造成困擾。

瞭解通訊程序

遠端載入器會開啟用戶端通訊端，並監聽來自遠端介面 Shim 的連接。遠端介面 shim 和遠端載入器會執行 SSL 信號交換，以建立安全通道。然後，遠端介面 shim 會向遠端載入器進行驗證。如果遠端介面 shim 驗證成功，遠端載入器會向遠端介面 shim 進行驗證。僅在雙方都確認自己是與有授權之實體建立通訊時，才會發生同步化傳輸。

用於在驅動程式與 Identity Manager 引擎之間建立 SSL 連接的程序取決於驅動程式類型：

- **對於原生驅動程式** (例如 Active Directory 驅動程式)，請指向 base64 編碼的證書。如需詳細資訊，請參閱 「管理自行簽署的伺服器證書」(第 97 頁)。
- **對於 Java 驅動程式**，您必須建立金鑰儲存區。如需詳細資訊，請參閱 「使用 SSL 連接時建立金鑰儲存區檔案」(第 99 頁)。
- **對於 .NET 驅動程式**，請指向 base64 編碼的證書。如需詳細資訊，請參閱 「管理自行簽署的伺服器證書」(第 97 頁)。

附註：遠端載入器允許在遠端載入器與 Identity Manager 伺服器上代管的遠端介面 shim 之間使用自訂連接方法。若要設定自訂連接模組，請參閱該模組隨附的文件中關於應該和允許在連接字串中指定何值的資訊。

管理自行簽署的伺服器證書

您可以建立並輸出自行簽署的伺服器證書，以確保在遠端載入器與 Identity Manager 引擎之間進行安全通訊。如需額外的安全保障，您可以依照 Suite B 指定為 SSL 通訊設定較強的加密。此通訊需要使用 ECDSA (Elliptic Curve Digital Signature Algorithm，橢圓曲線數位簽名演算法) 證書來加密資料。啟用 Suite B 時，遠端載入器使用 TLS 1.2 做為通訊協定。如需 Suite B 的詳細資訊，請參閱「Suite B Cryptography」(Suite B 加密法)。

您可以輸出新建立的證書，也可以使用現有證書。

附註：當伺服器加入網路樹時，eDirectory 會建立下列預設證書：

- SSL CertificateIP

- SSL CertificateDNS
- 符合 Suite B 要求的證書

---

1 登入 NetIQ iManager。

2 若要建立新證書，請完成以下步驟：

   2a 按一下 **NetIQ Certificate Server > 建立伺服器證書**。

   2b 選取擁有該證書的伺服器。

   2c 指定證書的綽號。例如 remotecert。

   附註：NetIQ 建議不要在證書綽號中使用空格。例如，應使用 remotecert 而不使用 remote cert。

   同時，請記下證書綽號。此綽號在驅動程式的遠端連接參數中將用做 KMO 名稱。

   2d 選取證書建立方法，然後按下一步。

   您可以選擇以下選項：

   - **標準：**此選項會使用可能的最大金鑰大小建立伺服器證書物件，並使用您的組織 CA 簽署公用金鑰證書。
   - **自訂：**此選項會使用您指定的設定建立伺服器證書物件。它可讓您為伺服器證書物件設定一些自訂設定。選取此選項可建立 ECDSA 證書以用於 Suite B 通訊。
   - **輸入：**此選項會使用 PKCS12 (PFX) 檔案中的金鑰和證書建立伺服器證書物件。您可以用此選項搭配 「輸出」功能來備份與還原 「伺服器證書」物件，或將 「伺服器證書」物件移到別的伺服器。

   2e 指定證書參數。

   2f 接受其餘的證書預設值。

   2g 檢閱摘要，按一下完成，然後按一下關閉。

3 若要輸出證書，請完成以下步驟：

   3a 在 iManager 中，導覽至角色與任務 > **NetIQ 證書存取 > 伺服器證書**。

   3b 瀏覽並選取已建立的證書或伺服器建立的證書 (例如 SSL CertificateDNS)。

   3c 按一下 「輸出」。

   3d 從下拉式功能表中選取 **OU=organization CA.O=TREEANAME** 做為 **CA 證書**。

   3e 從下拉式功能表中選取 **BASE64 > 輸出格式**。

   附註：如果遠端載入器要在 Windows 2012 R2 64 位元伺服器上執行，證書必須採用 Base64 格式。如果您使用 DER 格式，遠端載入器將無法連接到 Identity Manager 引擎。

   3f 按下一步。

   3g 按一下 「儲存」，然後按一下 「關閉」。

使用 SSL 連接時建立金鑰儲存區檔案

若要在 Java 驅動程式與 Identity Manager 引擎之間使用 SSL 連接，您必須建立一個金鑰儲存區。金鑰儲存區是包含加密金鑰和證書 (選擇性) 的 Java 檔案。如果要在遠端載入器與 Identity Manager 引擎之間使用 SSL，並且您使用的是 Java shim，那麼，您需要建立一個金鑰儲存區檔案。以下章節說明了如何建立金鑰儲存區檔案：

- 「在任何平台上建立金鑰儲存區」(第 99 頁)
- 「建立 KeyStore」(第 99 頁)

在任何平台上建立金鑰儲存區

若要在平台上建立金鑰儲存區，可以在指令行輸入下列指令：

keytool -import -alias trustedroot -file self-signed_certificate_name -keystore filename -storepass keystorepass

檔案名稱可以是任意名稱。例如 rdev_keystore。

建立 KeyStore

執行預設位於 c:\novell\remoteloader\jre\bin 目錄中的 Keytool 公用程式。

10.3.2 瞭解遠端載入器的組態參數

若要使遠端載入器能夠與代管 Identity Manager 應用程式 shim 的驅動程式例項配合使用，您必須對該驅動程式例項進行設定。例如，您必須指定該例項的連接和連接埠設定。您可以透過指令行或遠端載入器主控台來指定設定。例項執行後，您便可以使用指令行修改組態參數，或者指示遠端載入器執行某個功能。例如，您可能想要開啟追蹤視窗或卸載遠端載入器。

本節提供關於組態參數的資訊。這些說明將會指出，當例項正在執行時，是否可以從指令行傳送參數來更新遠端載入器。

如需設定新驅動程式例項的詳細資訊，請參閱第 10.3.3 節「為驅動程式例項設定遠端載入器」(第 107 頁)。

遠端載入器中驅動程式例項的組態參數

您可以在指令行或組態檔案中設定驅動程式例項。NetIQ 提供了 config8000.txt 範例檔案，以協助您設定要與應用程式 shim 配合使用的遠端載入器和驅動程式。該範例檔案預設位於 C:\novell\remoteloader\<architecture(64bit/32bit>\ 或 C:\Novell\remoteloader.NET 目錄中。例如，該組態檔案可能包含以下幾行：

```
-commandport 8000
-connection "port=8090"
-trace 4
-tracefile ./trace8000.log
-class com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver
```

使用以下參數：

-assembly

(視情況而定) 使用 .NET 遠端載入器時，請指定驅動程式 .dll 所在的路徑。請確定組態檔案包含此參數。例如：

```
-assembly C:\Novell\remoteloader.NET\DXMLMADDriver.dll
```

-description *值* (-desc *值*)

(選擇性) 以字串格式指定簡短描述 (例如 SAP)，應用程式將在追蹤視窗的標題中使用該描述，並將其用於稽核記錄。例如：

```
-description SAP
```

```
-desc SAP
```

-class *名稱* (-cl *名稱*)

(視情況而定) 使用 Java 驅動程式時，指定要代管之 Identity Manager 應用程式 shim 的 Java 類別名稱。此選項指示應用程式使用 Java 金鑰儲存區來讀取證書。例如：

-class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim-cl
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim

附註：

- 如果您指定了 -module 選項，則不能使用此選項。
- 如果您使用定位字元做為 -class 選項中的分隔符，遠端載入器將不會自動啟動，您必須手動來啟動它。若要讓遠端載入器正常啟動，您可以使用空格字元，而不要使用定位字元。
- 如需可為此選項指定之名稱的詳細資訊，請參閱「瞭解 Java -class 參數的名稱」(第 106 頁)。

-commandport *連接埠號* (-cp *連接埠號*)

指定驅動程式例項用於進行控制操作的 TCP/IP 連接埠。例如 -commandport 8001 或 -cp 8001。預設值為 8000。

若要在同一個伺服器上將多個驅動程式例項與遠端載入器配合使用，請為每個例項指定不同的連接埠和指令埠。

如果驅動程式例項代管了一個應用程式 shim，則指令埠為另一個例項用於與代管 shim 之例項進行通訊的連接埠。如果驅動程式例項將指令傳送到某個代管應用程式 shim 的例項，則指令埠為代管例項監聽的連接埠。

如果要從指令行將此參數傳送到代管應用程式 shim 的例項，則指令埠代表代管例項監聽的連接埠。您可以在遠端載入器執行時傳送此指令。

-config *檔案名稱*

指定驅動程式例項的組態檔案。例如：

```
-config config.txt
```

組態檔案可以包含除 config 之外的任何指令行選項。在指令行上指定的選項會優先於組態檔案中指定的選項。

您可以在遠端載入器執行時傳送此指令。

-connection " *參數* " (-conn " *參數* ")

指定用於連接到代管 Identity Manager 引擎並執行 Identity Manager 遠端介面 shim 之伺服器的設定。預設連接方法為使用 SSL 的 TCP/IP。

若要在同一個伺服器上將多個驅動程式例項與遠端載入器配合使用，請為每個例項指定不同的連接埠和指令埠。

請使用以下語法輸入連接設定：

```
-connection "parameter parameter parameter"
```

例如：

```
-connection "port=8091 fromaddress=198.51.100.0 rootfile=server1.pem keystore=ca.pem
localaddress=198.51.100.0 hostname=198.51.100.0 kmo=remote driver cert"
```

請使用以下參數指定 TCP/IP 連接的設定：

address=*IP 位址*

(選擇性) 指定遠端載入器是否監聽特定的本地 IP 位址。如果代管遠端載入器的伺服器具有多個 IP 位有效值包括：

- address=address number
- address='localhost'

例如：

```
address=198.51.100.0
```

如果您未指定任何值，遠端載入器將會監聽所有本地 IP 位址。

fromaddress=*IP 位址*

指定遠端載入器接受其連接的伺服器。應用程式會忽略來自其他位址的連接。請指定伺服器的 IP 位址或 DNS 名稱。例如：

```
fromaddress=198.51.100.0
```

```
fromaddress=testserver1.company.com
```

handshaketimeout= *毫秒數*

(視情況而定) 當來自 Identity Manager 引擎的其他有效連接發生信號交換逾時時適用。為遠端載入器與 Identity Manager 引擎之間的信號交換指定逾時期間，以毫秒為單位。例如：

```
handshaketimeout=1000
```

您可以指定大於或等於零的整數。零表示連接永不逾時。預設值為 1000 毫秒。

hostname= *伺服器*

指定要執行遠端載入器之伺服器的 IP 位址或名稱。例如：

```
hostname=198.51.100.0
```

secureprotocol=*TLS 版本*

指定遠端載入器用於連接 Identity Manager 引擎的 TLS 通訊協定版本。例如：

```
secureprotocol=TLSv1_2
```

Identity Manager 支援 TLSv1 和 TLSv1_2。遠端載入器預設使用 TLSv1_2。若要使用 TLSv1，請在參數中指定此版本。

enforceSuiteB=*true/false*

(視情況而定) 僅當您希望遠端載入器使用 Suite B 加密演算法與 Identity Manager 引擎通訊時才適用。

若要對通訊使用 Suite B，請指定 true。只有 TLS 1.2 通訊協定支援此通訊。

如果您嘗試將啟用 Suite B 的引擎與不支援 TLSv1.2 的遠端載入器進行連接，信號交握將會失敗，並且無法建立通訊。例如，遠端載入器 4.5.3 就不支援 TLS v1.2。

useMutualAuth=*true/false*

(視情況而定) 僅當您想讓遠端載入器與 Identity Manager 引擎透過驗證可信證書管理中心 (CA) 核發的公用金鑰證書或數位證書或者自行簽署的證書來相互驗證時適用。例如：

```
useMutualAuth=true
```

keystore= ***檔案名稱***

指定 Java 金鑰儲存區的檔案名稱，該金鑰儲存區包含遠端介面 shim 所用證書之發行者的可信根證書。例如：

```
keystore=keystore filename
```

通常，您可指定代管遠端介面 shim 之網路樹的證書管理中心。

kmo= ***名稱***

指定包含用於 SSL 連接的金鑰和證書之金鑰資料物件的金鑰名稱。例如：

```
kmo=remote driver cert
```

localaddress=*IP 位址*

指定要將用戶端連接的通訊端與之相結合的 IP 位址。例如：

```
localaddress=198.51.100.0
```

port= ***連接埠號***

指定遠端載入器會在其上監聽來自遠端介面 shim 之連接的 TCP/IP 連接埠。若要指定預設連接埠，請輸入 port=8090。

rootfile= ***可信證書名稱***

指定包含遠端介面 Shim 所用證書核發者可信根證書的檔案名稱。證書檔案必須為 Base 64 格式 (PEM)。例如：

```
rootfile=trustedcert
```

通常，該檔案是代管遠端介面 shim 之網路樹的證書管理中心。

storepass= ***密碼***

指定您為 keystore 參數輸入的 Java 金鑰儲存區密碼。例如：

```
storepass=mypassword
```

若要讓遠端載入器與 Java 驅動程式通訊，請使用以下語法指定金鑰值組：

keystore=*keystorename* storepass=*password*

-datadir *目錄* (-dd *目錄*)

指定遠端載入器使用的資料檔案所在目錄。例如：

```
-datadir C:\novell\remoteloader
```

當您使用此指令時，遠端載入器會將其目前目錄切換為指定的目錄。系統將在此資料目錄中建立不帶明確指定路徑的追蹤檔案和其他檔案。

-help (-h)

指示應用程式顯示說明。

-java (-j)

(視情況而定) 指定您要為 Java 驅動程式 shim 例項設定密碼。

附註：如果您未同時指定 -class 值，請將此選項與 -setpasswords 選項配合使用。

-javadebugport *連接埠號* (-jdp *連接埠號*)

指示例項在指定的連接埠上啟用 Java 除錯。例如：

```
-javadebugport 8080
```

在開發 Identity Manager 應用程式 shim 時可以使用此指令。您可以在遠端載入器執行時傳送此指令。

-javaparam *參數* (-jp *參數*)

指定 Java 環境的參數。請使用以下語法輸入 Java 環境參數：

```
-javaparam parameter
-jp parameter
-jp parameter
```

附註：請勿對 Java 遠端載入器使用此參數。

若要為個別參數指定多個值，請用引號將該參數括住。例如：

```
-javaparam DHOST_JVM_MAX_HEAP=512M
-jp DHOST_JVM_MAX_HEAP=512M
-jp "DHOST_JVM_OPTIONS=-Dfile.encoding=utf-8 -Duser.language=en"
```

可以使用以下參數設定 Java 環境：

DHOST_JVM_ADD_CLASSPATH

指定 JVM 要在其中搜尋套件 (.jar) 和類別 (.class) 檔案的其他路徑。

DHOST_JVM_INITIAL_HEAP

以十進位位元組數字指定啟始 (最小) JVM 堆積大小。指定一個數值，後面跟著代表位元組類型的 G、M 或 K。例如：

```
100M
```

如果您未指定位元組類型，大小的單位將預設為位元組。使用此參數的效果與使用 Java -Xms 指令相同。

此參數優先於驅動程式集屬性選項。增加啟始堆積大小可以改善啟動時間和生產量效能。

DHOST_JVM_MAX_HEAP

以十進位位元組數字指定最大 JVM 堆積大小。指定一個數值，後面跟著代表位元組類型的 G、M 或 K。例如：

```
100M
```

如果您未指定位元組類型，大小的單位將預設為位元組。

此參數優先於驅動程式集屬性選項。

DHOST_JVM_OPTIONS

指定在啟動驅動程式的 JVM 例項時要使用的引數。請使用空格來分隔各個選項字串。例如：

```
-Xnoagent -Xdebug -Xrunjdwp: transport=dt_socket,server=y, address=8000
```

驅動程式集屬性選項優先於此參數。此環境變數附加在驅動程式集屬性選項的末尾。如需有效選項的詳細資訊，請參閱 JVM 文件。

-module " *名稱* " (-m " *名稱* ")

(視情況而定) 使用原生驅動程式時，指定包含您要代管之 Identity Manager 應用程式 shim 的模組。此選項指示應用程式使用 rootfile 證書。例如，針對原生驅動程式，輸入下列其中一項：

```
-module "c:\Novell\RemoteLoader\ADDriver.dll"
-m "c:\Novell\RemoteLoader\ADDriver.dll"
```

附註：

- 如果您指定了 -class 選項，則不能使用此選項。
- 如果您使用定位字元做為 -module 選項中的分隔符，遠端載入器將不會自動啟動，您必須手動來啟動它。若要讓遠端載入器正常啟動，您可以使用空格字元，而不要使用定位字元。

-password *值* (-p *值*)

在您發出的指令會變更設定或影響例項操作的情況下，指定驅動程式例項的密碼。對於指令所針對的例項，您指定的密碼必須與使用 setpasswords 指定的第一個密碼相同。例如：

```
-password netiq4
```

如果您在發出指令時未傳送該密碼，驅動程式例項會提示您提供該密碼。

您可以在遠端載入器執行時傳送此指令。

-service *值* (-serv *值*)

指定是否要將某個例項設定為 Win32 服務。有效值為 install 和 uninstall，以及代管應用程式 shim 所需的其他參數。例如，您必須包含 -module，此外，還可能需要包含 -commandport 和連接設定。

此指令只會將例項安裝為服務或將其解除安裝，不會啟動該服務。

您可以在遠端載入器執行時傳送此指令。不過，您不能在 rdxml 或 Java 遠端載入器上使用此指令。

-setpasswords *遠端載入器密碼 選擇性密碼* (-sp *遠端載入器密碼 選擇性密碼*)

指定驅動程式例項的密碼，以及與遠端載入器通訊之遠端介面 shim 的 Identity Manager 驅動程式物件密碼。

您不需要指定密碼，遠端載入器會提示您輸入密碼。但是，如果指定了遠端載入器的密碼，那麼還必須指定與 Identity Manager 引擎伺服器上遠端介面 shim 關聯之 Identity Manager 驅動程式物件的密碼。若要指定密碼，請使用以下語法：

-setpasswords *Remote_Loader_password driver_object_password*

例如：

-setpasswords netiq4 idmobject6

附註：使用此選項可為驅動程式例項設定指定的密碼，但不會載入 Identity Manager 應用程式 shim 或與其他例項通訊。

追蹤檔案設定

(視情況而定) 在代管 Identity Manager 應用程式 shim 的情況下，為追蹤檔案指定設定，該檔案中包含遠端載入器和此例項驅動程式所傳送的資訊訊息。

將以下參數新增至組態檔案：

-trace *整數* (-t *整數*)

指定要在追蹤視窗中顯示的訊息層級。例如：

-trace 3

遠端載入器的追蹤層級與代管 Identity Manager 引擎的伺服器上使用的追蹤層級對應。

-tracefile *檔案路徑* (-tf *檔案路徑*)

指定用於記錄追蹤訊息的檔案所在的路徑。必須為特定電腦上執行的每個驅動程式例項指定唯一的追蹤檔案。例如：

-tracefile c:\temp\trace.txt

如果 -trace 參數大於零，應用程式便會將訊息寫入該檔案。系統無需開啟追蹤視窗即可將訊息寫入該檔案。

-tracefilemax *大小* (-tf *大小*)

指定此例項的追蹤檔案大小限制。請以 K、M 或 G (位元組類型的縮寫) 為單位指定該值。例如：

- -tracefilemax 1000K
- -tf 100M
- -tf 10G

附註：

- 遠端載入器啟動時，如果追蹤檔案資料大於指定的最大值，在所有 10 個檔案都完成換用之前，追蹤檔案資料會一直大於指定的最大值。
- 將此選項新增至組態檔案後，應用程式將為追蹤檔案使用指定的名稱，並最多包含 9 個「換用」檔案。換用檔案使用主追蹤檔案名稱為基本名稱，後面會加上 _n，其中 n 是從 1 到 9 的數字。

-tracechange *整數* (-tc *整數*)

(視情況而定) 如果您有一個現有的驅動程式例項在代管應用程式 shim，此參數用於指定新的資訊訊息層級。追蹤層級對應 Identity Manager 伺服器上使用的追蹤層級。例如：

-trace 3

您可以在遠端載入器執行時傳送此指令。

-tracefilechange *檔案路徑* **(-tfc** *檔案路徑* **)**

(視情況而定) 如果您有一個現有的驅動程式例項在代管應用程式 shim，此參數指示該例項使用追蹤檔案，或關閉已在使用的檔案並變更為使用此新檔案。例如：

```
-tracefilechange \temp\newtrace.txt
```

您可以在遠端載入器執行時傳送此指令。

證書密碼設定

(視情況而定) 僅當組態檔案中的 useMutualAuth 設定為 true 時。

-keystorepassword (-ksp)

僅指定對 Java 遠端載入器驅動程式啟用雙向驗證所用的金鑰儲存區密碼。

-keypassword (-kp)

指定對 Java 和原生遠端載入器驅動程式啟用雙向驗證所用的金鑰密碼。

-unload (-u)

指示卸載驅動程式例項。如果遠端載入器正在做為 Win32 服務執行，則此指令會停止該服務。

您可以在遠端載入器執行時傳送此指令。

-window *值* **(-w)** *值*

指示應用程式開啟或關閉某個驅動程式例項的追蹤視窗。有效值為 on 和 off。例如：

```
-window on
```

您可以在遠端載入器執行時傳送此指令。您不能對 Java 遠端載入器使用此指令。

-wizard (-wiz)

啟動遠端載入器的組態精靈。您也可以不指定指令行參數，直接執行 dirxml_remote.exe 來啟動該精靈。

如果您執行此指令並指定了組態檔案 (-config 選項)，精靈會使用組態檔案中的值啟動。您可以使用該精靈變更組態，而無需直接編輯組態檔案。例如：

```
-wizard -config config.txt
```

您不能對 Java 遠端載入器使用此指令。

瞭解 Java -class 參數的名稱

當您使用 -class 參數設定遠端載入器和 Java 遠端載入器的驅動程式例項時，必須指定要代管之 Identity Manager 應用程式 shim 的 Java 類別名稱。

Java 類別名稱	驅動程式
com.novell.nds.dirxml.driver.dcsshim.DCSShim	Driver for Data Collection Service
com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver	Delimited Text Driver
be.opns.dirxml.driver.ars.arsremedydrivershim.ARSDriverShim	補救 ARS 的驅動程式
com.novell.nds.dirxml.driver.entitlement.EntitlementServiceDriver	Entitlements Service Driver
com.novell.gw.dirxml.driver.rest.shim.GWdriverShim	GroupWise 2014 驅動程式

Java 類別名稱	驅動程式
com.novell.idm.drivers.idprovider.IDProviderShim	ID Provider Driver
com.novell.nds.dirxml.driver.jdbc.JDBCDriverShim	JDBC 驅動程式
com.novell.nds.dirxml.driver.jms.JMSDriverShim	JMS 驅動程式
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim	LDAP Driver
com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim	迴路驅動程式
com.novell.nds.dirxml.driver.ebs.user.EBSUserDriver	Oracle User Management Driver
com.novell.nds.dirxml.driver.ebs.hr.EBSHRDriver	Oracle HR Driver
com.novell.nds.dirxml.driver.ebs.tca.EBSTCADriver	Oracle TCA Driver
com.novell.nds.dirxml.driver.msgateway.MSGatewayDriverShim	受管理系統閘道驅動程式
com.novell.nds.dirxml.driver.manualtask.driver.ManualTaskDriver	手動任務驅動程式
com.novell.nds.dirxml.driver.nisdriver.NISDriverShim	NIS 驅動程式
com.novell.nds.dirxml.driver.notes.NotesDriverShim	Notes 驅動程式
com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim	PeopleSoft 驅動程式
com.netiq.nds.dirxml.driver.pum.PUMDriverShim	Privileged User Management Driver
com.novell.nds.dirxml.driver.salesforce.SFDriverShim	Salesforce Driver
com.novell.nds.dirxml.driver.SAPHRShim.SAPDriverShim	SAP HR Driver
com.novell.nds.dirxml.driver.sap.portal.SAPPortalShim	SAP Portal Driver
com.novell.nds.dirxml.driver.sapumshim.SAPDriverShim	SAP 使用者管理驅動程式
com.novell.nds.dirxml.driver.soap.SOAPDriver	SOAP 驅動程式
com.novell.idm.driver.ComposerDriverShim	使用者應用程式
com.novell.nds.dirxml.driver.workorder.WorkOrderDriverShim	WorkOrder Driver

10.3.3 為驅動程式例項設定遠端載入器

遠端載入器可以代管 .dll、.so 或 .jar 檔案中包含的 Identity Manager 應用程式 shim。遠端載入器需要有相應的組態檔案 (例如 LDAPShim.txt) 才能執行。遠端載入器主控台公用程式 (簡稱主控台) 可協助您管理 伺服器上執行的所有 Identity Manager 驅動程式例項。您可以啟動、停止、新增、移除和編輯每個遠端載入器例項。遠端載入器的安裝程式也會安裝主控台。

如果您要進行升級，主控台會偵測並輸入現有的驅動程式例項。若要自動輸入某個驅動程式，其組態檔案必須儲存在遠端載入器目錄 (預設位於 c:\novell\remoteloader) 中。這樣，您便可以使用主控台來管理遠端驅動程式。

您可以使用指令行或遠端載入器主控台來設定遠端載入器，以識別驅動程式。如需使用指令行的詳細資訊，請參閱第 10.3.2 節「瞭解遠端載入器的組態參數」(第 99 頁)。

本節提供關於以下活動的指示：

- 「在遠端載入器中建立新驅動程式例項」(第 108 頁)
- 「在遠端載入器中修改現有驅動程式例項」(第 109 頁)

在遠端載入器中建立新驅動程式例項

1 開啟遠端載入器主控台。

附註：如果您在安裝期間選擇了建立主控台的捷徑，請使用桌面上的 Identity Manager 遠端載入器主控台圖示。否則，請執行預設位於 C:\novell\remoteloader*nn*bit 中的 rlconsole.exe。

---

2 若要在此伺服器上新增驅動程式的例項，請按一下**新增**。

3 在**描述**中，提供一個簡短名稱用來表示該例項。

主控台將在**組態檔案**的預設值中使用此資訊。

4 對於**驅動程式**，請選取 Java 類別名稱。

附註：若要使用 Active Directory 驅動程式，請選取 **ADDriver.dll**。如需每個驅動程式之類別名稱的詳細資訊，請參閱「瞭解 Java -class 參數的名稱」(第 106 頁)。

---

5 對於**組態檔案**，請指定遠端載入器用來儲存其組態參數的檔案路徑。預設值為 C:\novell\remoteloader*nn*bit*Description*-config.txt。

6 指定遠端載入器和驅動程式物件的密碼。

7 (選擇性) 若要在遠端載入器與 Identity Manager 引擎伺服器之間使用 TLS/SSL 連接，請完成以下步驟：

7a 選取**使用 SSL 連接**。

附註：NetIQ 建議在 Identity Manager 引擎伺服器和遠端載入器上使用相同的 SSL 版本。如果伺服器上的 SSL 與遠端載入器上的 SSL 版本不相符，伺服器將會傳回「SSL3_GET_RECORD：錯誤的版本號碼」錯誤訊息。此訊息僅用於警告目的，伺服器與遠端載入器之間的通訊並不會中斷。不過，該錯誤可能會造成困擾。

7b 對於**可信的根檔案** (base64 格式檔案)，請指定從 eDirectory 網路樹的組織證書管理中心輸出的自行簽署證書。如需詳細資訊，請參閱第 10.3.1 節「與 Identity Manager 引擎建立安全連接」(第 97 頁)與第 10.3.2 節「瞭解遠端載入器的組態參數」(第 99 頁)。

8 (選擇性) 若要設定遠端載入器的追蹤檔案，請完成以下步驟：

附註：NetIQ 建議僅在對問題進行疑難排解時使用追蹤功能。啟用追蹤功能會降低遠端載入器的效能。請不要在線上環境中啟用追蹤功能。

8a 對於**追蹤層級**，請指定大於零的值，來定義遠端載入器和驅動程式傳送的將在追蹤視窗中顯示的資訊訊息層級。主控台已預先定義值 1 至 4。若要建立自己的訊息類型，請指定 5 或更大的值。

最常用的設定是追蹤層級 3，它會提供關於一般處理、XML 文件和遠端載入器訊息。

8b 對於**追蹤檔案**，請指定要用來記錄追蹤訊息的檔案路徑。例如 C:\novell\remoteloader\64bit\Test-Delimited-Trace.log。

必須為特定電腦上執行的每個驅動程式例項指定唯一的追蹤檔案。僅當追蹤層級大於零時，追蹤訊息才會寫入追蹤檔案。

8c 對於**存放所有追蹤記錄所允許的最大磁碟空間 (MB)**，請指定此例項的追蹤檔案最多約可佔用多少磁碟空間。

9 (選擇性) 若要讓遠端載入器在電腦啟動時自動啟動，請選取**建立此驅動程式例項的遠端載入器服務**。

附註：如果遠端載入器與 Identity Manager 引擎建立連接時因 handshaketimeout 導致 SSL 連接失敗，請將預設 handshaketimeout 變數更新為 10000，並重新啟動驅動程式和遠端載入器。

---

10 (選擇性) 若要修改 Java 組態的參數，請完成以下步驟：

10a 選擇 **進階**。

10b 對於**類別路徑**，請指定 JVM 要在其中搜尋套件 (.jar) 和類別 (.class) 檔案的路徑。

此參數的作用與 java -classpath 指令相同。

10c 對於 **JVM 選項**，請指定在啟動驅動程式的 JVM 例項時要使用的選項。

10d 指定 JVM 例項的啟始和最大堆積大小 (以 MB 為單位)。

10e 對於 Suite B 通訊，指定 enforceSuiteB=true。只有 TLS 1.2 通訊協定支援此通訊。

如需詳細資訊，請參閱第 10.3.1 節「與 Identity Manager 引擎建立安全連接」(第 97 頁)與第 10.3.2 節「瞭解遠端載入器的組態參數」(第 99 頁)。

10f 按一下**確定**。

11 (選擇性) 若要允許遠端載入器在連接 Identity Manager 引擎時使用安全通訊協定，請在遠端載入器組態檔案中指定安全通訊協定版本。例如： secureprotocol=TLSv1_2

如需詳細資訊，請參閱第 10.3.2 節「瞭解遠端載入器的組態參數」(第 99 頁)。

附註：如果您已在驅動程式上設定安全通訊協定版本，請跳過此步驟。

---

12 (選擇性) 若要允許遠端載入器使用 Suite B 指定的通訊協定進行通訊，請在遠端載入器組態檔案中指定 enforceSuiteB=true。只有 TLS 1.2 通訊協定支援此通訊。

如需詳細資訊，請參閱第 10.3.2 節「瞭解遠端載入器的組態參數」(第 99 頁)。

附註：如果您已在驅動程式上啟用 Suite B 通訊，請跳過此步驟。

---

13 按一下**確定**。

在遠端載入器中修改現有驅動程式例項

1. 在遠端載入器主控台上，從**描述**欄中選取驅動程式例項。
2. 按一下「**停止**」。
3. 輸入遠端載入器的密碼，然後按一下**確定**。
4. 按一下「**編輯**」。
5. 修改組態資訊。如需每個參數的詳細資訊，請參閱「在遠端載入器中建立新驅動程式例項」(第 108 頁)。
6. 若要儲存變更，請按一下「**確定**」。

10.3.4 為驅動程式例項設定 Java 遠端載入器

Java 遠端載入器只代管 Java 驅動程式 Shim。它不能載入或代管原生 (C++) 驅動程式 Shim。

1 在文字編輯器中建立一個新檔案。

   NetIQ 提供了 config8000.txt 範例檔案，以協助您設定要與應用程式 shim 配合使用的遠端載入器和驅動程式。該範例檔案預設位於 C:\novell\remoteloader\<architecture(64bit\32bit>\ 或 C:\Novell\remoteloader.NET 目錄中。

2 將以下參數新增至新組態檔案：
   - -description (選擇性)
   - -class 或 -module

     例如 -class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim
   - -commandport
   - 連接參數：
     - port (強制)
     - address
     - fromaddress
     - handshaketimeout
     - rootfile
     - keystore
     - localaddress
     - hostname
     - kmo
     - secureprotocol
     - enforceSuiteB
     - useMutualAuth
   - -java (視情況而定)
   - -javadebugport
   - -password
   - -service
   - -setpasswords
   - 追蹤檔案參數 (選擇性)：
     - -trace
     - -tracefile
     - -tracefilemax

   附註：如需參數的詳細資訊，請參閱第 10.3.2 節「瞭解遠端載入器的組態參數」(第 99 頁)。

3 儲存新組態檔案。

   若要讓遠端載入器在電腦啟動時自動啟動，請將該檔案儲存到 \jremote 目錄。

4 啟

5 在提示符處，輸入 -config *filename*，其中，*filename* 是新組態檔案的名稱。例如：

```
dirxml_jremote -config <configFile> -service
```

如此會啟動 Java 遠端載入器服務並開啟追蹤視窗。

6 (選擇性) 若要停止驅動程式服務，請移至「服務」，然後停止該服務。

10.3.5 為驅動程式例項設定 .NET 遠端載入器

遠端載入器可以代管 .dll 檔案中包含的 Identity Manager 應用程式 shim。遠端載入器需要有相應的組態檔案 (例如 LDAPShim.txt) 才能執行。遠端載入器主控台公用程式 (簡稱主控台) 可協助您管理 伺服器上執行的所有 Identity Manager 驅動程式例項。您可以啟動、停止、新增、移除和編輯每個遠端載入器例項。遠端載入器的安裝程式也會安裝主控台。

如果您要進行升級，主控台會偵測並輸入現有的驅動程式例項。若要自動輸入某個驅動程式，其組態檔案必須儲存在遠端載入器目錄 (預設位於 c:\novell\remoteloader) 中。網路 . 這樣，您便可以使用主控台來管理遠端驅動程式。

您可以使用指令行或遠端載入器主控台來設定遠端載入器，以識別驅動程式。如需使用指令行的詳細資訊，請參閱第 10.3.2 節「瞭解遠端載入器的組態參數」(第 99 頁)。

本節提供關於以下活動的指示：

- 「在 .NET 遠端載入器中建立新驅動程式例項」(第 111 頁)
- 「在 .NET 遠端載入器中修改現有驅動程式例項」(第 112 頁)

在 .NET 遠端載入器中建立新驅動程式例項

1 開啟遠端載入器主控台。

附註：如果您在安裝期間選擇了建立主控台的捷徑，請使用桌面上的 Identity Manager 遠端載入器主控台圖示。否則，請執行預設位於 C:\novell\remoteloader.net 中的 rlconsole.exe。

---

2 若要在此伺服器上新增驅動程式的例項，請按一下**新增**。

3 在**描述**中，提供一個簡短名稱用來表示該例項。

主控台將在**組態檔案**的預設值中使用此資訊。

4 對於**驅動程式**，請選取相應的 driver.dll。

5 對於**組態檔案**，請指定遠端載入器用來儲存其組態參數的檔案路徑。預設值為 C:\novell\remoteloader.net*Description*-config.txt。

6 指定遠端載入器和驅動程式物件的密碼。

7 (選擇性) 若要在遠端載入器與 Identity Manager 引擎伺服器之間使用 TLS/SSL 連接，請完成以下步驟：

7a 選取**使用 SSL 連接**。

附註：NetIQ 建議在 Identity Manager 引擎伺服器和遠端載入器上使用相同的 SSL 版本。如果伺服器上的 SSL 與遠端載入器上的 SSL 版本不相符，伺服器將會傳回「SSL3_GET_RECORD：錯誤的版本號碼」錯誤訊息。此訊息僅用於警告目的，伺服器與遠端載入器之間的通訊並不會中斷。不過，該錯誤可能會造成困擾。

7b 對於**可信的根檔案** (base64 格式檔案)，請指定從 eDirectory 網路樹的組織證書管理中心輸出的自行簽署證書。如需詳細資訊，請參閱第 10.3.1 節「與 Identity Manager 引擎建立安全連接」(第 97 頁)與第 10.3.2 節「瞭解遠端載入器的組態參數」(第 99 頁)。

8 (選擇性) 若要設定遠端載入器的追蹤檔案，請完成以下步驟：

附註：NetIQ 建議僅在對問題進行疑難排解時使用追蹤功能。啟用追蹤功能會降低遠端載入器的效能。請不要在線上環境中啟用追蹤功能。

8a 對於**追蹤層級**，請指定大於零的值，來定義遠端載入器和驅動程式傳送的將在追蹤視窗中顯示的資訊訊息層級。主控台已預先定義值 1 至 4。若要建立自己的訊息類型，請指定 5 或更大的值。

最常用的設定是追蹤層級 3，它會提供關於一般處理、XML 文件和遠端載入器訊息。

8b 對於**追蹤檔案**，請指定要用來記錄追蹤訊息的檔案路徑。例如 C:\novell\remoteloader.net\Test-Delimited-Trace.log。

必須為特定電腦上執行的每個驅動程式例項指定唯一的追蹤檔案。僅當追蹤層級大於零時，追蹤訊息才會寫入追蹤檔案。

8c 對於**存放所有追蹤記錄所允許的最大磁碟空間 (MB)**，請指定此例項的追蹤檔案最多約可佔用多少磁碟空間。

9 (選擇性) 若要讓遠端載入器在電腦啟動時自動啟動，請選取**建立此驅動程式例項的遠端載入器服務**。

附註：如果遠端載入器與 Identity Manager 引擎建立連接時因 handshaketimeout 導致 SSL 連接失敗，請將預設 handshaketimeout 變數更新為 10000，並重新啟動驅動程式和遠端載入器。

---

10 (選擇性) 若要允許遠端載入器在連接 Identity Manager 引擎時使用安全通訊協定，請在遠端載入器組態檔案中指定安全通訊協定版本。例如： secureprotocol=TLSv1_2

如需詳細資訊，請參閱第 10.3.2 節「瞭解遠端載入器的組態參數」(第 99 頁)。

附註：如果您已在驅動程式上設定安全通訊協定版本，請跳過此步驟。

---

11 (選擇性) 若要允許遠端載入器使用 Suite B 指定的通訊協定進行通訊，請在遠端載入器組態檔案中指定 enforceSuiteB=true。只有 TLS 1.2 通訊協定支援此通訊。

如需詳細資訊，請參閱第 10.3.2 節「瞭解遠端載入器的組態參數」(第 99 頁)。

附註：如果您已在驅動程式上啟用 Suite B 通訊，請跳過此步驟。

---

12 按一下**確定**。

在 .NET 遠端載入器中修改現有驅動程式例項

1 在遠端載入器主控台上，從**描述**欄中選取驅動程式例項。

2 按一下「**停止**」。

3 輸入遠端載入器的密碼，然後按一下**確定**。

4 按一下「**編輯**」。

5 修改組態資訊。如需每個參數的詳細資訊，請參閱「在 .NET 遠端載入器中建立新驅動程式例項」(第 111 頁)。

6 若要儲存變更，請按一下「**確定**」。

10.3.6 設定 Identity Manager 驅動程式以與遠端載入器配合使用

您可以設定新驅動程式，或者啟用現有驅動程式以與遠端載入器通訊。您必須設定 Identity Manager 應用程式 shim 以與遠端載入器配合使用。

附註：本節會提供設定驅動程式以使它們與遠端載入器通訊的一般資訊。如需驅動程式特定的資訊，請參閱 Identity Manager 驅動程式文件網站上的相關驅動程式執行指南。

若要在 Designer 或 iManager 中新增新驅動程式物件或修改現有驅動程式物件，您必須設定用於啟用遠端載入器的驅動程式例項的設定。如需本節中所用參數的詳細資訊，請參閱「瞭解遠端載入器的組態參數」(第 99 頁)。

1 在綜覽中，選取 Identity Manager 驅動程式物件。

2 在驅動程式物件的內容中，完成以下步驟：

   2a 對於驅動程式模組，請選取連接至遠端載入器。

   2b 對於驅動程式物件密碼，請指定遠端載入器用於向 Identity Manager 引擎伺服器驗證自身的密碼。

   此密碼必須與遠端載入器中定義的驅動程式物件密碼相符。

   2c 對於遠端載入器連接參數，請指定連接到遠端載入器所需的資訊。請使用下列語法：

   hostname=*xxx.xxx.xxx.xxx* port=*xxxx* kmo=*certificatename* localaddress=*xxx.xxx.xxx.xxx*

   其中

   hostname

   指定代管遠端載入器的伺服器的 IP 位址。例如 hostname=192.168.0.1。

   port

   指定遠端載入器監聽的連接埠。預設值為 8090。

   kmo

   指定包含用於 SSL 連接的金鑰和證書之金鑰資料物件的金鑰名稱。例如 kmo=remotecert。

   localaddress

   如果在代管 Identity Manager 引擎的伺服器上設定了多個 IP 位址，請指定來源 IP 位址。

   2d 對於遠端載入器密碼，請指定 Identity Manager 引擎 (或遠端載入器 shim) 向遠端載入器進行驗證時需要使用的密碼。

3 定義一個具有同等安全性的使用者。

4 按下一步，然後按一下完成。

10.3.7 設定與 Identity Manager 引擎的雙向驗證

您可以設定雙向驗證，以確保在遠端載入器與 Identity Manager 引擎之間進行安全通訊。雙向驗證使用證書而非密碼進行信號交握。遠端載入器與 Identity Manager 引擎透過交換並驗證可信證書管理中心 (CA) 核發的公用金鑰證書或數位證書或者自行簽署的證書來相互驗證。如果雙向驗證成功，遠端載入器會向引擎進行驗證。當遠端載入器與 Identity Manager 引擎建立了信任關係，雙方均確信它們是在與授權實體通訊後，才會出現同步流量。

若要設定雙向驗證，請執行以下任務：

- 「輸出 Identity Manager 引擎和遠端載入器的證書」(第 114 頁)
- 「啟用驅動程式以進行雙向驗證」(第 117 頁)

輸出 Identity Manager 引擎和遠端載入器的證書

為了讓雙向驗證正常運作，您需要有引擎的伺服器證書和遠端載入器的用戶端證書。您可以從 eDirectory 輸出證書，也可以輸入來自協力廠商的證書。在大多數情況下，您會從 eDirectory 輸出伺服器證書，這樣不需要花費額外的費用。在某些情況下，您可能想要輸出遠端載入器的協力廠商用戶端證書。

- 「從 eDirectory 輸出證書」(第 114 頁)
- 「為遠端載入器輸出協力廠商證書」(第 116 頁)

從 eDirectory 輸出證書

Identity Vault 中的證書物件稱為金鑰材料物件 (KMO)。此物件可安全地包含證書和資料，包括與用於 SSL 連接的證書關聯的公用金鑰和私密金鑰。要使用雙向驗證，您需要兩個 KMO，一個用於引擎，一個用於遠端載入器。

您可以輸出現有的 KMO，也可以建立新的 KMO，然後將其輸出。建立用戶端 KMO 與建立伺服器 KMO 的程序不同。

建立 KMO

在建立用戶端 KMO 之前，必須先建立伺服器 KMO。若要建立 KMO，請執行下列步驟：

1. 登入 NetIQ iManager。
2. 在左側窗格中，選取 **NetIQ 證書伺服器 > 建立伺服器證書**。
3. 選取擁有您所建立證書的伺服器。
4. 指定證書的綽號。

   例如，為伺服器證書指定 serverkmo，為用戶端證書指定 clientkmo。
5. 在證書建立方法中選取自訂，然後按下一步。
6. 保留預設的組織證書管理中心選擇，然後按下一步。
7. (視情況而定) 如果您要建立用戶端 KMO。
   - **7a** 選取啟用延伸金鑰使用。
   - **7b** 選取自訂，然後選取使用者驗證。
   - **7c** 按下一步。

附註：對於伺服器 KMO，請保留預設選擇，然後按下一步。

8 指定 KMO 的有效期間。

確定 iManager 系統時間與您的 Identity Manager 元件以及連接的應用程式保持同步。

9 檢閱摘要，按一下完成，然後按一下關閉。

10 重複以上步驟以建立用戶端 KMO。

輸出 KMO

從 eDirectory 輸出引擎和遠端載入器將用於相互驗證的 KMO。

若要為 Identity Manager 引擎輸出 KMO，請執行 DirXML 指令行 (dxcmd) 公用程式：

```
dxcmd -user <admin DN> -password <password of admin> -exportcerts <kmoname> <server|client>
<java|native|dotnet> <output dir>
```

其中

- user 用於指定對驅動程式具有管理權限的使用者名稱。
- password 用於指定對驅動程式具有管理權限的使用者的密碼。
- exportcerts 用於從 eDirectory 輸出證書和私密金鑰 / 公用金鑰。您必須指定要輸出伺服器證書還是用戶端證書、將使用證書的驅動程式類型，以及指令將用於儲存此資訊的目的地資料夾。

例如，dxcmd -user admin.sa.system -password novell -exportcerts serverkmo server java 'C:\certs'

此指令會在 C:\certs 目錄中產生 serverkmo_server.ks 檔案。預設金鑰儲存區密碼和金鑰密碼是 dirxml。

執行用於為遠端載入器輸出 KMO 的 dxcmd 指令時，請注意以下事項：

- dxcmd 公用程式在 LDAP 模式下執行。第一次使用該公用程式時，它會提示您指定信任來自 eDirectory 的證書的選項。依據您的環境，您可以選擇僅針對目前的工作階段或針對目前和將來的工作階段信任該證書、信任所有證書，或者選取不信任證書。
- 如果遠端載入器要在 Identity Manager 伺服器上執行，請以 LDAP 或點格式執行該指令。如果遠端載入器安裝在單獨的伺服器上，請僅以 LDAP 格式執行指令。
- 在指令中指定 -host 參數可解析能夠向 Identity Manager 伺服器驗證的伺服器 IP 位址或主機名稱。

使用以下語法執行指令：

dxcmd -dnform ldap -host < 主機 IP 位址 > -user < 管理員 DN> -password < 管理員密碼 > -exportcerts <KMO 名稱 > <client> <java|native|dotnet> < 輸出目錄 >

表格 10-1 不同類型驅動程式的範例

驅動程式類型	指令	輸出
Java 驅動程式	`dxcmd -dnform ldap -host 194.99.90.218 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client java 'C:\certs'`	C:\certs 目錄中的 clientkmo_client.ks 檔案 金鑰儲存區的預設密碼為 dirxml。 預設私密金鑰密碼是 dirxml。
原生驅動程式	`dxcmd -dnform ldap -host 194.99.90.218 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client native 'C:\certs'`	C:\certs 目錄中的 clientkmo_clientcert.pem、clientkmo_clientkey.pem 和 trustedcert.b64 檔案。 預設金鑰密碼是 dirxml。
.NET 驅動程式	`dxcmd -dnform ldap -host 194.99.90.218 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client dotnet 'C:\certs'`	C:\certs 目錄中的 clientkmo_clientcert.pfx 和 trustedcert.b64 檔案。 clientkmo_clientcert.pfx 的預設金鑰密碼是 dirxml。

為遠端載入器輸出協力廠商證書

若要將協力廠商證書與遠端載入器配合使用，您需要將證書輸出為 .pfx 檔案以及 Base 64 格式的可信根檔案，然後將 .pfx 證書轉換為驅動程式使用的格式。例如，原生驅動程式需要 .pem 格式的私密金鑰和證書金鑰，而 Java 驅動程式需要 .jks 格式的金鑰儲存區。.NET 驅動程式使用 .pfx 格式的檔案。因此，您需要為 .NET 驅動程式轉換檔案。

原生驅動程式

完成以下步驟：

1. 從 .pfx 檔案中取回 .pem 格式的私密金鑰。

   輸入一條指令，例如 openssl pkcs12 -in servercert.pfx -out serverkey.pem

2. 從 .pfx 檔案中取回 .pem 格式的證書金鑰。

   輸入一條指令，例如 openssl pkcs12 -in servercert.pfx -out servercert.pem

Java 驅動程式

透過 .pfx 檔案建立 Java 金鑰儲存區。輸入以下指令：

```
keytool -importkeystore -srckeystore servercert.pfx -srcstoretype pkcs12 -destkeystore servercert.jks -deststoretype JKS
```

此指令會提示您輸入來源金鑰儲存區密碼 (srckeystore passwd) 和目的地金鑰儲存區密碼 (dest keystorepasswd)。請輸入相應的密碼。

最後一個步驟是依據驅動程式類型，在遠端載入器組態檔案中指定資訊。如需詳細資訊，請參閱啟用驅動程式以進行雙向驗證。

啟用驅動程式以進行雙向驗證

若要啟用驅動程式通訊以進行雙向驗證，請執行以下任務：

- 「使用 KMO 或金鑰儲存區設定驅動程式」（第 117 頁）
- 「新增新的遠端載入器驅動程式例項」（第 120 頁）
- 「為驅動程式例項設定遠端載入器」（第 122 頁）

使用 KMO 或金鑰儲存區設定驅動程式

您可以在 Designer 或 iManager 中使用 KMO 或金鑰儲存區來設定驅動程式。

Designer

在 Designer 中使用 KMO 或金鑰儲存區設定驅動程式之前，務必依如下方式完成基本驅動程式組態：

1. 在 Designer 中開啟您的專案。
2. 在模型產生器檢視的選擇區中，選取您要建立的驅動程式。
3. 將驅動程式的圖示拖曳到模型產生器檢視上。
4. 依照安裝精靈中的步驟操作。
5. 在「遠端載入器」視窗中，選取是。
   - **5a** **主機名稱：**指定用於執行驅動程式遠端載入器服務的伺服器主機名稱或 IP 位址。例如，輸入 192.168.0.1 做為主機名稱。如果未指定此參數的值，則該值預設為 localhost。
   - **5b** **埠：**指定用於為此驅動程式安裝和執行遠端載入器的連接埠號碼。預設連接埠號碼為 8090。
6. 按下一步。
7. 依照精靈中的其餘指示操作，直到完成驅動程式的安裝。
8. 檢閱為了建立驅動程式將要完成的任務摘要，然後按一下完成。

若要使用 KMO 或金鑰儲存區修改驅動程式組態

1. 在 Designer 的大綱檢視中，以滑鼠右鍵按一下驅動程式。
2. 選取「內容」。
3. 在導覽窗格中，選取驅動程式組態。
4. 在驗證中，選取啟用雙向驗證並指定下列參數：

   KMO

   指定伺服器 KMO 的名稱。

   其他參數

   指定 rootfile 及其絕對路徑。

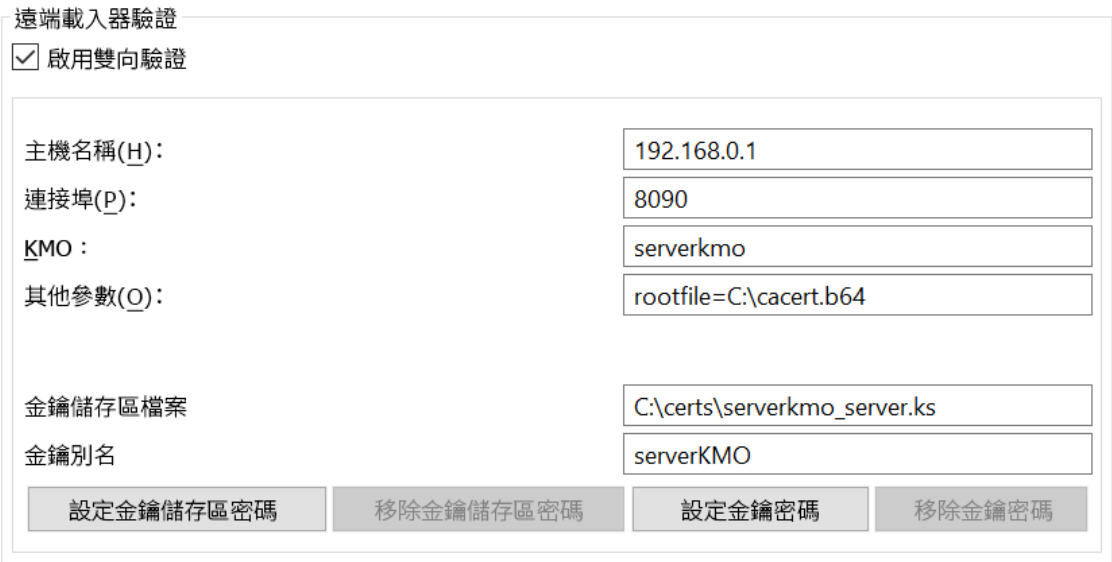
   金鑰儲存區檔案

   指定金鑰儲存區檔案的絕對路徑。

   金鑰別名

   指定伺服器 KMO 的名稱。

圖 10-1 在 Designer 中啟用雙向驗證的組態範例



5 設定金鑰儲存區密碼。

6 設定金鑰密碼。

附註：依預設，金鑰儲存區密碼和金鑰密碼均設為 dirxml。

您也可以使用 dxcmd 指令來設定金鑰儲存區和金鑰密碼。

```
dxcmd -user <administrative_user> -password <admin_password>
```

1. 選取驅動程式操作。
2. 選取要設定金鑰儲存區和金鑰密碼的驅動程式。
3. 選取密碼操作。
4. 選取設定雙向驗證的金鑰儲存區密碼，然後輸入金鑰儲存區密碼。
5. 選取設定雙向驗證的金鑰密碼，然後輸入金鑰密碼。

---

iManager

若要在 iManager 中修改組態：

1 啟動 iManager。

2 在 **Identity Manager 管理**中，選取 **Identity Manager 綜覽**。

3 在綜覽中，選取 Identity Manager 驅動程式集。

4 針對要設定的驅動程式選取編輯內容。

5 在驅動程式組態中，指定下列參數：

5a 在驅動程式模組中，選取連接至遠端載入器。

5b 在遠端載入器連接參數中，指定下列連接詳細資料：

```
KMO=<server_KMO_name>
rootfile=<absolute path to the file>
```

例如，

```
KMO=serverkmo
rootfile=C:\cacert.b64
```

5c 設定應用程式密碼。

5d 選取啟用雙向驗證。

5e 若要使用金鑰儲存區方法，請指定下列各項：

金鑰別名

指定伺服器 KMO 的名稱，並設定金鑰密碼。

例如：serverKMO

KeyStore 檔案

指定金鑰儲存區檔案的絕對路徑，並設定金鑰儲存區密碼。

例如：C:\certs\serverkmo_server.ks

5f 按一下「套用」，然後按一下「確定」。

圖 10-2 在 iManager 中啟用雙向驗證的組態範例

附註：啟用雙向驗證時，無需設定遠端載入器密碼和驅動程式物件密碼。

新增新的遠端載入器驅動程式例項

1 以滑鼠右鍵按一下 **Identity Manager 遠端載入器主控台**應用程式，並選取**以管理員身分執行**。

2 按一下**新增**以新增新的遠端載入器例項。

3 指定**描述**，並選取驅動程式類型。

4 指定用於連接遠端載入器和 Identity Manager 引擎的**連接埠**。

5 為您的遠端載入器例項指定**指令連接埠**。

6 選取**雙向驗證**並指定所需的驅動程式類型：

- **Java 驅動程式：**瀏覽包含證書的金鑰儲存區檔案的路徑。該金鑰儲存區檔案必須至少包含一個公用 / 私密金鑰組。

  金鑰儲存區檔案

  指定要用於驗證的 Java 金鑰儲存區檔案的路徑。金鑰儲存區檔案包含加密金鑰和證書。例如，「從 eDirectory 輸出證書」（第 114 頁）中透過 dxcmd 在 C:\certs\ 目錄下建立的 clientkmo_client.ks。

  金鑰別名

  指定金鑰儲存區檔案中將用於產生對稱式金鑰的公用 / 私密金鑰組名稱。例如，clientkmo。

  金鑰儲存區密碼

  指定用於載入 金鑰儲存區檔案的密碼。

  私密金鑰密碼

  指定金鑰儲存區中儲存的私密金鑰的密碼。Identity Manager 使用此金鑰來加密 SSL 通訊。

  圖 10-3 新增 Java 遠端載入器例項的範例

- **原生驅動程式：**瀏覽用於驗證的證書所在金鑰檔案的路徑。該金鑰檔案必須為 Base 64 格式。

  金鑰檔

  指定用於驗證的金鑰所在檔案的路徑。例如，透過 dxcmd 在 C:\certs\ 目錄下建立的 clientkmo_clientkey.pem 檔案。

  金鑰密碼

  指定用於驗證的私密金鑰的密碼。

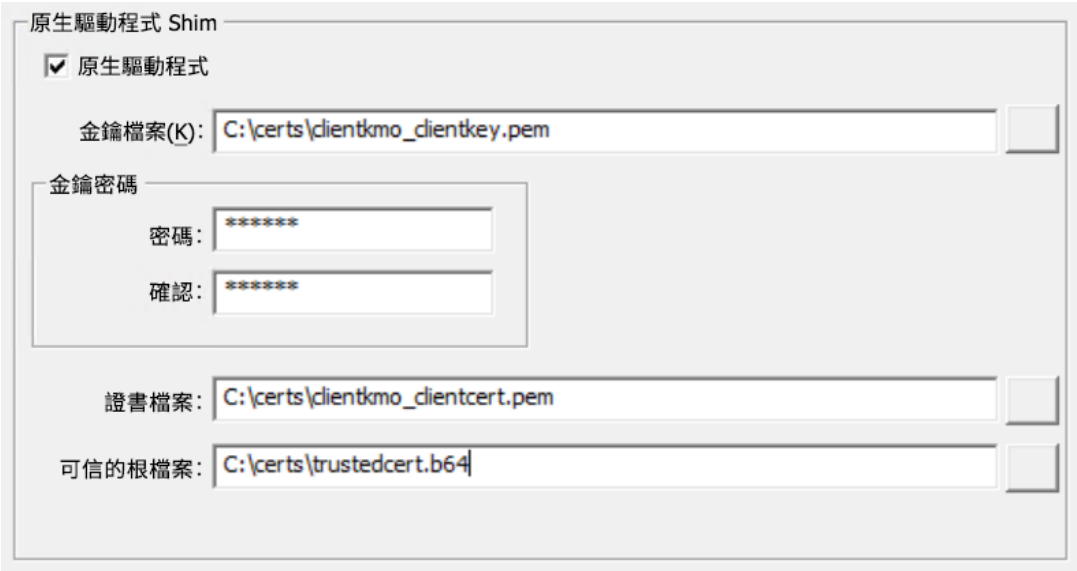
證書檔案

指定儲存證書的檔案。證書檔案必須為 Base 64 格式 . 例如，「從 eDirectory 輸出證書」(第 114 頁) 中透過 dxcmd 在 C:\certs\ 目錄下建立的 clientkmo_clientcert.pem 檔案。

可信的根檔案

指定包含遠端介面 Shim 所用證書核發者可信根證書的檔案名稱。該可信根檔案必須為 Base 64 格式。例如，「從 eDirectory 輸出證書」(第 114 頁) 中透過 dxcmd 在 C:\certs\ 目錄下建立的 trustedcert.b64 檔案。

圖 10-4 新增原生遠端載入器例項的範例



- **.Net 驅動程式**：瀏覽用於驗證的證書所在金鑰檔案的路徑。

金鑰檔

指定用於驗證的金鑰所在檔案的路徑。例如，「從 eDirectory 輸出證書」(第 114 頁) 中透過 dxcmd 在 C:\certs\ 目錄下建立的 clientkmo_clientcert.pfx。

金鑰密碼

指定用於驗證的私密金鑰的密碼。

可信的根檔案

指定包含遠端介面 Shim 所用證書核發者可信根證書的檔案名稱。該可信根檔案必須為 Base 64 格式。例如，「從 eDirectory 輸出證書」(第 114 頁) 中透過 dxcmd 在 C:\certs\ 目錄下建立的 trustedcert.b64 檔案。

圖 10-5 新增 .Net 遠端載入器例項的範例

如需使用 dxcmd 工具為此驅動程式產生的輸出檔案的詳細資訊，請參閱表格 10-1 「不同類型驅動程式的範例」(第 116 頁)。

為驅動程式例項設定遠端載入器

您必須在遠端載入器組態檔案中設定驅動程式例項。務必在驅動程式的遠端載入器組態檔案中，指定儲存金鑰儲存區檔案、金鑰檔案、證書檔案和根檔案的目錄的絕對路徑。

1 在遠端載入器主控台上，從**描述**欄中選取驅動程式例項。
2 按一下「**停止**」。
3 輸入遠端載入器的密碼，然後按一下**確定**。
4 按一下**編輯**，並執行「新增新的遠端載入器驅動程式例項」(第 120 頁) 中的步驟 6
5 按一下**確定**。

10.3.8 驗證組態

如需啟動和停止遠端載入器的詳細資訊，請參閱第 10.4 章 「啟動和停止遠端載入器」(第 123 頁)。

1 使用 iManager 啟動驅動策 ｛C
2 使用以下任一方式管理遠端載入器：

遠端載入器使用者介面

1. 以滑鼠右鍵按一下 **Identity Manager 遠端載入器** 主控台，並選取**以管理員身分執行**。
2. 您可以使用遠端載入器介面**啟動**、**停止**、**新增**、**移除**，以及執行其他操作。

附註：若要將遠端載入器做為服務執行，請選取**為此驅動程式例項建立遠端載入器服務**。如果取消選取此選項，會將遠端載入器做為應用程式執行。

遠端載入器主控台

導覽至遠端載入器安裝位置，然後在指令提示符處執行以下指令：

1. 若要啟動或載入遠端載入器例項：

   對於 Java 遠端載入器：

```
dirxml_jremote -config <configuration_filename> -ksp <keystore_password> -kp
<keypassword>
```

```
dirxml_jremote -config <configuration_filename>
```

對於原生遠端載入器：

```
dirxml_remote -config <configuration_filename> -ksp <keystore_password> -kp
<keypassword>
```

```
dirxml_remote -config <configuration_filename>
```

對於 .Net 遠端載入器：

```
RemoteLoader.exe  -config <configuration_filename> -ksp <keystore_password> -kp
<keypassword>
```

```
RemoteLoader.exe  -config <configuration_filename>
```

2. 若要停止或卸載遠端載入器例項，請在上一條指令的末尾附加 -u。例如

   對於 Java 遠端載入器：

```
dirxml_jremote -config <configuration_filename> -u
```

   對於原生遠端載入器：

```
dirxml_remote -config <configuration_filename> -u
```

   對於 .Net 遠端載入器：

```
RemoteLoader.exe  -config <configuration_filename> -u
```

附註：若要將遠端載入器例項做為服務執行，請使用以下指令：

```
dirxml_remote -config config.txt -service install
```

10.4 啟動和停止遠端載入器

遠端載入器做為服務或精靈，有時必須重新啟動。本節介紹如何停止和啟動遠端載入器。

- 第 10.4.1 節「啟動遠端載入器中的驅動程式例項」(第 123 頁)
- 第 10.4.2 節「停止遠端載入器中的驅動程式例項」(第 124 頁)

10.4.1 啟動遠端載入器中的驅動程式例項

您可以將每個平台設定為在主機電腦啟動時自動啟動驅動程式例項。您也可以手動啟動例項。

- 「自動啟動驅動程式例項」(第 123 頁)
- 「使用主控台啟動驅動程式例項」(第 124 頁)

自動啟動驅動程式例項

您可以將遠端載入器的驅動程式例項設定為在主機電腦啟動時自動啟動。

1 開啟遠端載入器主控台。

如果您在安裝期間建立了遠端載入器主控台的捷徑，請使用桌面上的 Identity Manager 遠端載入器主控台圖示。否則，請執行預設位於 C:\novell\remoteloader*nn*bit 中的 rlconsole.exe。

2 選取一個驅動程式例項，然後按一下**編輯**。

3 選取**建立此驅動程式例項的遠端載入器服務**。

4 儲存變更，然後關閉主控台。

使用主控台啟動驅動程式例項

1 開啟遠端載入器主控台。

如果您在安裝期間建立了遠端載入器主控台的捷徑，請使用桌面上的 Identity Manager 遠端載入器主控台圖示。否則，請執行預設位於 C:\novell\remoteloader*nn*bit 中的 rlconsole.exe。

2 選取驅動程式例項，然後按一下**啟動**。

10.4.2 停止遠端載入器中的驅動程式例項

每個平台都提供了不同的方法來停止遠端載入器中的驅動程式例項。如需本節中所用參數的詳細資訊，請參閱「瞭解遠端載入器的組態參數」(第 99 頁)。

附註：若要停止驅動程式例項，您必須具有足夠的權限，或指定遠端載入器密碼。例如，遠端載入器正在做為 Windows 服務執行。您具有足夠的權限停止它。您輸入密碼，但意識到它是錯誤的。此時，遠端載入器仍會停止，因為遠端載入器實際上並不「接受」密碼，而是會忽略密碼，原因是在這種情況下，密碼是多餘的。如果做為應用策 ' 茂 D 服務執行遠端載入器，則會使用該密碼。

若要停止某個驅動程式例項：

遠端載入器

使用遠端載入器主控台。

如果您在安裝期間建立了遠端載入器主控台的捷徑，請使用桌面上的 Identity Manager 遠端載入器主控台圖示。否則，請執行預設位於 C:\novell\remoteloader*nn*bit 中的 rlconsole.exe。

Java 遠端載入器

輸入 dirxml_jremote -config *檔案名稱* -u 指令。例如：

```
dirxml_jremote -config config.txt -u
```

11 安裝 iManager

本章將引導您完成安裝 iManager 所需元件的程序。安裝程式可以安裝以下元件：

- iManager (伺服器版本)
- iManager Workstation (用戶端版本)
- Java
- Novell 國際密碼基礎結構 (NICI)
- Tomcat

安裝檔案位於 Identity Manager 安裝套件 .iso 影像檔中的 \products\iManager\installs\ *伺服器平台* \ 目錄內。依預設，安裝程式會在 C:\Novell 中安裝元件。

NetIQ 建議您在開始之前檢閱安裝程序。如需詳細資訊，請參閱第 11.1 章 「規劃安裝 iManager」(第 125 頁)。

11.1 規劃安裝 iManager

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

- 第 11.1.1 節 「iManager 的安裝核對清單」(第 125 頁)
- 第 11.1.2 節 「瞭解 iManager 的伺服器版本和用戶端版本」(第 126 頁)
- 第 11.1.3 節 「瞭解 iManager 外掛程式的安裝」(第 126 頁)
- 第 11.1.4 節 「安裝 iManager 的先決條件和考量」(第 127 頁)
- 第 11.1.5 節 「iManager 伺服器的系統要求」(第 128 頁)
- 第 11.1.6 節 「iManager Workstation (用戶端版本) 的系統要求」(第 129 頁)

11.1.1 iManager 的安裝核對清單

NetIQ 建議您在開始安裝前先檢閱以下步驟：

	核對清單項目
❑	1. 瞭解 Identity Manager 各元件之間的互動。如需詳細資訊，請參閱第 1 章 「Identity Manager 的元件綜覽」(第 19 頁)。
❑	2. 確定要為 Identity Manager 的元件使用哪些伺服器。如需詳細資訊，請參閱第 5.3 節 「建議的安裝情境和伺服器設定」(第 39 頁)。
❑	3. 瞭解 iManager 與 iManager Workstation 之間的差別。如需詳細資訊，請參閱第 11.1.2 節 「瞭解 iManager 的伺服器版本和用戶端版本」(第 126 頁)。

	核對清單項目
❑	4. 為確定電腦符合安裝 iManager 伺服器和 iManager Workstation 的先決條件，請查看以下注意事項： ◆ 對於 iManager 伺服器，請參閱「安裝 iManager 伺服器的注意事項」(第 128 頁) ◆ 對於 iManager Workstation，請參閱「安裝 iManager Workstation 的注意事項」(第 128 頁)
❑	5. 存取 iManager 的安裝檔案。依預設，這些檔案位於 Identity Manager 安裝套件 .iso 影像檔中的 \products\iManager\installs\ *伺服器平台* \ 目錄內。 您也可以從 NetIQ 下載網站下載安裝檔案。搜尋 iManager 產品，選取所需的 iManager 版本，然後將 win.zip 檔案下載到您伺服器上的某個目錄中。例如 iMan_31_win.zip。
❑	6. (選擇性) 若要瞭解外掛程式的安裝程序，請參閱第 11.1.3 節「瞭解 iManager 外掛程式的安裝」(第 126 頁)。
❑	7. (選擇性) 若要檢閱安裝 iManager 後可以執行的動作，請參閱第 11.3 章「iManager 的安裝後任務」(第 135 頁)。
❑	8. 若要安裝 iManager 和 iManager Workstation，請參閱下列小節： ◆ 對於圖形使用者介面安裝，請參閱第 11.2.1 節「安裝 iManager 和 iManager Workstation」(第 130 頁) ◆ 若要執行靜默安裝，請參閱第 11.2.2 節「以靜默模式安裝 iManager」(第 133 頁)

11.1.2 瞭解 iManager 的伺服器版本和用戶端版本

您必須在可存取 eDirectory 網路樹的伺服器上安裝 iManager。若要在工作站而非伺服器上安裝 iManager，您需要使用 iManager 的用戶端版本，即 **iManager Workstation**。使用下列準則，判斷哪個版本最適用於您的環境，或者您的 eDirectory 管理政策是否可透過安裝兩個版本來獲益：

- 如果您有單一管理員都是從相同用戶端工作站來管理 eDirectory，則可採用 iManager 工作站。完全獨立的 iManager 工作站不需要進行很多設定。它會在載入或卸載時自動啟動和停止所需的資源。iManager Workstation 可在各種 Windows 用戶端工作站上安裝及執行，不需要依賴伺服器型 iManager，並且可與您在網路上安裝的所有其他 iManager 版本並存。

  iManager 外掛程式不會自動在 iManager 實例之間同步。如果您有多位管理員且使用自訂的外掛程式，則必須在每位管理員的用戶端工作站上安裝 iManager 工作站和這些外掛程式。
- 如果您從多個用戶端工作站上管理 eDirectory，或有多位管理員，則可以安裝 iManager 伺服器，以便在任一相連的工作站上都能使用。此外，只需在每台 iManager 伺服器上安裝一次自訂的外掛程式。

11.1.3 瞭解 iManager 外掛程式的安裝

根據預設，不會在 iManager 伺服器之間複製外掛程式模組。您必須在每個 iManager 伺服器上安裝所需的外掛程式模組。

在執行全新安裝時，安裝程式會預先選取「一般」外掛程式。進行升級時，只預選要更新的外掛程式。您可以置換預設選擇，並新增要下載的新外掛程式。不過，NetIQ 建議您在升級時不要取消選取以前預先選取的任何外掛程式。一般而言，您應該每次都升級隨先前 iManager 版本一起安裝的外掛程式。此外，較新版本的外掛程式可能會與先前的 iManager 版本不相容。

iManager 的基礎外掛程式僅做為完整 iManager 軟體下載的一部分 (例如，eDirectory 管理外掛程式) 提供。除非這些外掛程式有特定的更新，否則您只能將它們隨整個 iManager 產品一併下載和安裝。

安裝程式使用 XML 描述子檔案 iman_mod_desc.xml 來識別可供下載的外掛程式。該檔案的預設 URL 為 http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml。不過，您可以將安裝程式指向替代的網路 URL。例如，您可能要將 iManager 安裝在阻止安裝程式存取預設 URL 的代理或防火牆後面。

重要：您必須使用最新的 iManager SDK 來重新編譯要在新安裝版本環境中使用的所有自訂外掛程式。

如需下載和安裝外掛程式的指示，請參閱下列其中一節中的步驟：

- **圖形使用者介面安裝**：第 11.2.1 節「安裝 iManager 和 iManager Workstation」(第 130 頁)
- **靜默安裝**：第 11.2.2 節「以靜默模式安裝 iManager」(第 133 頁)

如需自訂外掛程式下載和安裝程序的詳細資訊，請參閱《*NetIQ iManager Installation Guide*》(NetIQ iManager 安裝指南) 中的「Downloading and Installing Plug-in Modules」(下載和安裝外掛程式模組)。

11.1.4 安裝 iManager 的先決條件和考量

本節提供關於安裝伺服器和工作站版本 iManager 的資訊。

- 「安裝 iManager 的一般注意事項」(第 127 頁)
- 「安裝 iManager 伺服器的注意事項」(第 128 頁)
- 「安裝 iManager Workstation 的注意事項」(第 128 頁)

安裝 iManager 的一般注意事項

在安裝 iManager 之前，請檢閱以下考量：

- Identity Manager 4.7 支援 eDirectory 9.1。請使用 iManager 3.1。如需詳細資訊，請參閱《iManager 3.1 Installation Guide》(iManager 3.1 安裝指南)。
- 如果您打算讓 10 位以上的管理員定期同時在 iManager 中工作，請不要在其他 Identity Manager 元件所在的同一個伺服器上安裝 iManager。
- 如果您只打算指定一位管理員，則可以在 Identity Manager 引擎所在的同一個伺服器上安裝 iManager。
- 如果 iManager 伺服器安裝程式偵測到以前安裝的 iManager 版本，您可以停止安裝程序，或者移除現有的 iManager、JRE 和 Tomcat 安裝。
- 因為 iManager 工作站是獨立的環境，所以您可以在相同工作站上安裝多種版本，包含較舊版本的 Mobile iManager。但是，您不應嘗試同時執行它們。如果您需要使用不同的版本，請執行一個版本、關閉它，再執行其他版本。
- 您不能從包含空格的路徑執行 iManager Workstation。例如 C:\NetIQ\iManager Workstation\working。
- 您必須對 Windows 伺服器擁有管理員存取權。
- 若要在 eDirectory 網路樹中建立角色服務 (RBS) 集合，您必須具有等同於管理員的權限。

- 若要執行 iManager eDirectory RBS 組態精靈，您必須具有等同於管理員的權限。
- 若要管理包含多個 iManager 版本的同一個 eDirectory 網路樹，您必須將 RBS 集合更新到最新的 iManager 版本。

安裝 iManager 伺服器的注意事項

若要使用 Microsoft Internet Information Services (IIS) 或 Apache HTTP Server，您必須手動將 iManager 與這些 Web 伺服器基礎架構進行整合。iManager 預設使用 Tomcat。

安裝 iManager Workstation 的注意事項

NetIQ 建議您在 Windows 用戶端上安裝 iManager Workstation 之前檢閱以下考量：

- 若要讓 Internet Explorer 針對您的 LAN 使用代理伺服器，您必須在**工具** > **網際網路選項** > **連線** > **區域網路設定**下指定**近端網址不使用 Proxy**。
- 若要執行低於 4.91 的 Novell Client 版本，必須在啟動 iManager Workstation 之前在工作站上安裝 NetIQ Modular Authentication Service (NMAS) 用戶端。
- 如果您從任何名稱中包含 temp 或 tmp 的目錄所在路徑 (例如 c:\programs\temp\imanager) 執行 iManager Workstation，系統將不會安裝 iManager 外掛程式。正確的做法是從 C:\imanager 或非暫存目錄執行 iManager Workstation。
- 首次在 Windows 工作站上執行 iManager Workstation 時，請使用屬於工作站管理員群組成員的帳戶。

11.1.5 iManager 伺服器的系統要求

本節提供要安裝 iManager 的伺服器的最低要求。如需 iManager 伺服器版本的詳細資訊，請參閱第 11.1.2 節「瞭解 iManager 的伺服器版本和用戶端版本」(第 126 頁)。

類別	要求
處理器	1 GHz
磁碟空間	200 MB
記憶體	512 MB (建議 1024 MB) iManager 外掛程式需要 80 MB
作業系統 (已認證)	下列作業系統之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 NetIQ 建議您在安裝 Identity Manager 之前，依照製造商的自動更新機制來套用最新的作業系統修補程式。 **附註：***已認證*指作業系統已進行全面測試且受支援。 您不能在 Solaris 平台上安裝 iManager。不過，iManager 還是可以管理並使用 Solaris 上執行的一些應用程式和資源，例如 eDirectory。

類別	要求
作業系統 (受支援)	已認證作業系統的最新版 Service Pack **附註：***受支援*指作業系統尚未進行測試，但預期可正常運作。
作業系統 HotFix	NetIQ 建議您依照製造商的自動更新機制，套用最新的作業系統修補程式。
網頁瀏覽器	以下任意瀏覽器 (最低版本)： ◆ Google Chrome 61 ◆ Mozilla Firefox 51
應用程式伺服器	Tomcat 8.5.27 **附註：**在 Windows 伺服器上，您可以手動將現有 IIS 或 Apache Web 伺服器基礎架構與 iManager 進行整合。
目錄服務	NetIQ eDirectory 9.1 (最低版本)
預設連接埠	8080、8443 及 9009

11.1.6 iManager Workstation (用戶端版本) 的系統要求

本節提供要安裝 iManager Workstation 的伺服器的最低要求。如需 iManager 用戶端版本的詳細資訊，請參閱第 11.1.2 節「瞭解 iManager 的伺服器版本和用戶端版本」(第 126 頁)。

類別	要求
處理器	1 GHz
磁碟空間	200 MB
記憶體	256 MB (建議 521 MB)
作業系統 (已認證)	下列作業系統之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 NetIQ 建議您在安裝 Identity Manager 之前，依照製造商的自動更新機制來套用最新的作業系統修補程式。 **附註：***已認證*指作業系統已進行全面測試且受支援。
作業系統 (受支援)	已認證作業系統的最新版 Service Pack **附註：***受支援*指作業系統尚未進行測試，但預期可正常運作。
網頁瀏覽器	以下任意瀏覽器 (最低版本)： ◆ Google Chrome 61 ◆ Mozilla Firefox 51
作業系統 HotFix	NetIQ 建議您依照製造商的自動更新機制，套用最新的作業系統修補程式。
應用程式伺服器	iManager Workstation 隨附的 Tomcat 8.5.27

類別	要求
Java	iManager Workstation 隨附的 JRE 1.8.0_162
預設連接埠	8080、8443 及 9009

11.2 安裝 iManager 伺服器和 iManager Workstation

本節介紹 iManager 的安裝程序。若要進行安裝準備工作，請檢閱第 11.1.4 節「安裝 iManager 的先決條件和考量」(第 127 頁)中提供的先決條件和系統要求。

若要檢閱完整安裝程序，請參閱「規劃安裝 iManager」(第 125 頁)。

- 第 11.2.1 節「安裝 iManager 和 iManager Workstation」(第 130 頁)
- 第 11.2.2 節「以靜默模式安裝 iManager」(第 133 頁)

11.2.1 安裝 iManager 和 iManager Workstation

本節提供在 Windows 伺服器和用戶端上安裝 iManager 與 iManager Workstation 的步驟。若要進行安裝準備工作，請檢閱先決條件和系統要求：

- **iManager**：「安裝 iManager 伺服器的注意事項」(第 128 頁)。
- **iManager Workstation** ：「安裝 iManager Workstation 的注意事項」(第 128 頁)。
- 另請參閱版本隨附的 《版本說明》。

安裝 iManager 伺服器

以下程序描述如何使用安裝精靈在 Windows 伺服器上安裝 iManager 伺服器版本。若要執行靜默模式的無人管理安裝，請參閱第 11.2.2 節「以靜默模式安裝 iManager」(第 133 頁)。

如果 iManager 伺服器安裝程式偵測到以前安裝的 iManager 版本，可能會提供選項讓您選擇是停止安裝程序，還是移除現有的 iManager、JRE 和 Tomcat 安裝。當安裝程式移除之前安裝的 iManager 版本時，會將目錄結構備份至舊的 *TOMCAT_HOME* 目錄，以保留先前建立的任何自訂內容。

若要安裝 iManager 伺服器：

1. 以具有管理員權限的使用者身分登入您要安裝 iManager 的電腦。
2. (視情況而定) 如果您已取得 Identity Manager 安裝套件的 .iso 影像檔，請導覽至包含 iManager 安裝檔案的目錄 (預設為 \products\iManager\installs\win 目錄)。
3. (視情況而定) 如果您已從 NetIQ 下載網站下載了 iManager 安裝檔案，請完成以下步驟：
   - **3a** 找到 win.zip 檔案。例如，iMan_310_win_x86_64.zip。
   - **3b** 將 win.zip 檔案的內容擷取到本地電腦上的某個資料夾中。
4. 執行 iManagerInstall.exe。
5. (選擇性) 若要檢視安裝程式的除錯輸出，請在啟動安裝程式後立即按住 Ctrl 鍵，直到出現主控台視窗再放開。如需除錯的詳細資訊，請參閱 《*NetIQ iManager Administration Guide*》 (NetIQ iManager 管理指南) 中的「Troubleshooting」(疑難排解)。
6. 在 iManager 歡迎視窗中選取一種語言，然後按一下**確定**。

7 在簡介視窗中，按下一步。

8 接受授權合約，然後按下一步。

9 (視情況而定) 如果已在伺服器上隨 iManager 一併安裝了某個版本的 JVM 或 Tomcat 或其他支援元件，請在偵測摘要視窗中完成以下步驟：

9a 在安裝以下元件的下方，驗證列出的元件版本是否與您要安裝的版本相符。

9b (選擇性) 如果安裝程式未列出您要安裝的版本，請瀏覽至安裝資料夾中的相應元件。

10 按一下「下一步」。

11 在取得連接埠輸入視窗中，指定 Tomcat 伺服器執行時必須使用的連接埠號，然後按下一步。

依照預設，HTTP 連接埠值與 SSL 連接埠值分別為 8080 和 8443。但是，如果有其他服務或 Tomcat 伺服器正在使用預設連接埠，您可以指定其他連接埠。

12 指定您希望 TLS 證書使用的證書公用金鑰演算法，然後按下一步。依預設，公用金鑰演算法設定為 **RSA**。

- **RSA**：此證書使用 2048 位元 RSA 金鑰組。如果選取 **RSA**，則允許四個加密層級。依預設，加密層級已設為「無」。
  - **無**：可使用任何加密類型。
  - **低**：可使用 56 位元或 64 位元加密。
  - **中**：可使用 128 位元加密。
  - **高**：可使用高於 128 位元的加密。
- **ECDSA 256**：此證書使用含曲線 secp256r1 的 ECDSA 金鑰組。如果選取 **ECDSA 256**，則只允許一個加密層級：
  - **僅 SUITEB 128**：可使用 128 位元加密。

如需加密的詳細資訊，請參閱《NetIQ iManager Administration Guide》(NetIQ iManager 管理指南)。

13 (選擇性) 若要對 iManager 使用 IPv6 位址，請在啟用 **IPv6** 視窗中按一下是。

您也可以在安裝 iManager 後啟用 IPv6 位址。如需詳細資訊，請參閱第 11.3.2 節「安裝後設定 iManager 以使用 IPv6 位址」(第 137 頁)。

14 按一下「下一步」。

15 在選擇安裝資料夾視窗中，指定用於儲存安裝檔案的資料夾，然後按下一步。

預設安裝位置是 C:\Program Files\Novell。

16 (選擇性) 若要在安裝過程中下載並安裝外掛程式，請完成以下步驟：

16a 在選取要下載並安裝的外掛程式視窗中，選取所需的外掛程式。

16b (選擇性) 若要從其他網路位置下載外掛程式，請指定相應的網路 **URL**。

使用替換 URL 下載外掛程式時，您必須確認 URL 內容以及該外掛程式是否適合自己使用。依預設，安裝程式將從以下網址下載外掛程式：http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml。如需詳細資訊，請參閱第 11.1.3 節「瞭解 iManager 外掛程式的安裝」(第 126 頁)。

16c 按一下「下一步」。

16d (視情況而定) 安裝程式可能會顯示以下訊息：

```
No new or updated plug-ins found. All plug-ins are downloaded or updated or the iManager
download server is unavailable.
```

如果出現此錯誤，則表明存在下列一種或多種情況：

- 下載網站中沒有提供任何更新的外掛程式。
- 網際網路連接有問題。請檢視您的連接並再試一次。
- 與描述元檔案 (http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml) 的連接失敗。此 URL 指向可用 iManager 外掛程式的 XML 描述子檔案。
- iManager 安裝是在不允許連接到上面所述 URL 的代理後面執行。

16e (選擇性) 若要從本地目錄安裝外掛程式，請在「從磁碟選取要安裝的外掛程式」視窗中，指定包含相應 .npm 外掛程式檔案的目錄路徑。

執行此步驟可以安裝先前下載的外掛程式或自訂外掛程式。預設路徑為 \ *擷取位置* \products\iManager\plugins。不過，您也可以指定任何有效路徑。

16f 按一下「下一步」。

17 (選擇性) 在取得使用者名稱和網路樹名稱視窗中，指定一個授權使用者，以及此使用者將要管理的 eDirectory 網路樹名稱。

附註：

- 如果 eDirectory 使用的連接埠不是預設連接埠 524，您可以指定 eDirectory 伺服器的 IP 位址或 DNS 名稱，再加上連接埠號。請不要使用 localhost。例如，若要指定 IPv6 位址，請輸入 https://[2001:db8::6]:1080/nps/servlet/webacc?taskId=fw.Startup&forceMaster=true。
- NetIQ 不建議將這些設定留白。如果您將這些欄位留白，iManager 會允許任何使用者安裝外掛程式及變更 iManager 伺服器設定。您也可以在完成安裝程序後指定授權使用者。如需詳細資訊，請參閱第 11.3.3 節「指定 eDirectory 的授權使用者」(第 137 頁)。
- 安裝程式不會向 eDirectory 驗證指定的使用者身分證明。

---

18 按一下「下一步」。

19 閱讀「安裝前摘要」頁面，然後按一下安裝。

20 安裝完成後，安裝完成視窗將會顯示安裝程序成功的相關訊息。

附註：儘管安裝成功，安裝完成視窗仍可能會顯示以下錯誤訊息：

```
The installation of iManager version is complete, but some errors occurred during the install.
Please see the installation log Log file path for details. Press "Done" to quit the installer.
```

---

21 (視情況而定) 如果安裝程式顯示了步驟 20 中所示的錯誤訊息，請完成以下步驟：

21a 記下錯誤訊息中顯示的記錄檔案路徑。

21b 在安裝完成視窗中按一下完成。

21c 開啟記錄檔案。

21d (視情況而定) 如果您在記錄檔案中發現以下錯誤，則可以忽略該錯誤訊息。安裝成功，iManager 可正常運作。

```
Custom Action: com.novell.application.iManager.install.InstallDLLs
Status: ERROR
Additional Notes: ERROR - class com.novell.application.iManager.install.InstallDLLs
NonfatalInstallException C:\WINDOWS\system32\msvcr71.dll (The process cannot access the
file because it is being used by another process)
```

21e (視情況而定) 如果記錄檔案中未包含步驟 21d 中所列的錯誤，NetIQ 建議您重試安裝。

22 按一下「完成」。

23 iManager 啟始化完成後，按一下「開始使用」頁面中的第一個連結，然後登入。如需詳細資訊，請參閱《*NetIQ iManager Administration Guide*》(NetIQ iManager 管理指南) 中的「Accessing iManager」(存取 iManager)。

安裝 iManager Workstation

iManager 工作站是獨立的環境。您可以在相同工作站上安裝多個版本 (包括舊版的 Mobile iManager)。不過，您不應嘗試同時執行不同的版本。如果您需要使用不同的版本，請執行一個版本、關閉它，再執行其他版本。

附註：您不能從包含空格的路徑執行 iManager Workstation。例如 C:\NetIQ\iManager Workstation\working。

若要安裝 iManager Workstation：

1 (視情況而定) 如果您已取得 Identity Manager 安裝套件的 .iso 影像檔，請導覽至包含 iManager 安裝檔案的目錄 (預設為 \products\iManager\installs\win\ 目錄)。

2 (視情況而定) 如果您已從 NetIQ 下載網站下載了 iManager 安裝檔案，請完成以下步驟：

   2a 找到 win.zip 檔案。例如 iMan_31_workstation_win.zip。

   2b 將 win.zip 檔案的內容擷取到本地電腦上的某個資料夾中。

3 從 imanager\bin 資料夾執行 iManager.bat 檔案。

4 在 iManager 登入視窗中，指定一個授權使用者的身分證明，以及此使用者要管理的 eDirectory 網路樹。

   如需存取 iManager 的詳細資訊，請參閱《*NetIQ iManager Administration Guide*》(NetIQ iManager 管理指南) 中的「Accessing iManager」(存取 iManager)。

5 (選擇性) 若要啟用 IPv6 位址，請完成以下步驟：

   1. 開啟 *User_Install_Directory*\Tomcat\conf\catalina.properties 檔案。
   2. 在 catalina.properties 檔案中設定下列組態項目：

      ```
      java.net.preferIPv4Stack=false
      java.net.preferIPv4Addresses=true
      ```

   3. 重新啟動 Tomcat 服務。

11.2.2 以靜默模式安裝 iManager

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。在此模式下，InstallAnywhere 會使用預設 install.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。

若要進行安裝準備工作，請檢閱先決條件和系統要求：

- **iManager 伺服器**：「安裝 iManager 伺服器的注意事項」(第 128 頁).
- **iManager Workstation** ：「安裝 iManager Workstation 的注意事項」(第 128 頁)。
- 另請參閱版本隨附的《版本說明》。

編輯 Properties 檔案以進行自訂的靜默安裝

如需更多用於安裝模組的控制項，可以自訂無訊息安裝程序。

1 開啟 install.properties 檔案。依預設，該檔案位於適用於各作業系統環境的 Identity Manager 安裝套件 *.iso* 影像檔中的 products/iManager 目錄內。

附註：如果您先前已在伺服器上安裝了目前版本的 iManager，則此時可以使用安裝程式之前產生的 installer.properties 檔案。該檔案預設位於 log 目錄中，包含您在安裝期間指定的值。

---

2 在該 properties 檔案中，新增以下參數和值：

$PLUGIN_INSTALL MODE$

指定用於控制是否安裝外掛程式的內容。新增下列其中一個值：

- DISK - (預設值) 指示安裝程式從本地磁碟安裝外掛程式。
- NET - 指示安裝程式從網路中安裝外掛程式。
- BOTH - 指示安裝程式既從磁碟也從網路中安裝外掛程式。
- SKIP - 不安裝外掛程式。

$PLUGIN_DIR$

指定本地磁碟中外掛程式的替代路徑。預設路徑為 *\installer_root_directory*iManager\installs\ *平台路徑*\plugin。

安裝程式將會安裝 plugin 目錄中的所有模組，子目錄中的模組除外。

$PLUGIN_INSTALL_URL$

指定安裝程式可從中下載外掛程式的網路 URL。依預設，該 URL 為 http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml。如果您指定了其他 URL，則必須驗證 URL 內容，並驗證外掛程式是否適用於您。如需詳細資訊，請參閱第 11.1.3 節「瞭解 iManager 外掛程式的安裝」(第 126 頁)。

$LAUNCH_BROWSER$

指定在安裝程序完成後，是否讓安裝程式啟動 gettingstarted.html 檔案。

$USER_INSTALL_DIR$

指定 iManager 的安裝路徑。

USER_INPUT_ENABLE_IPV6

指定是否要讓 iManager 使用 IPv6 位址。依預設，安裝程式會將此值設定為 yes。

3 對於要下載並安裝的每個外掛程式模組，請指定 MANIFEST.MF 檔案中的模組 ID 和版本。該檔案位於 .npm (外掛程式模組) 的 META-INF/ 資料夾中。例如：

```
$PLUGIN_MODULE_ID_1$=eDirectoryBackupAndRestore

$PLUGIN_VERSION_1$=2.7.20050517

$PLUGIN_MODULE_ID_2$=ldap

$PLUGIN_VERSION_2$=2.7.20050517
```

附註：

- 如果您未指定任何模組，安裝程式將會安裝最常安裝的模組，這些模組在下載網站上的 iman_mod_desc.xml 檔案中標記為「selected」。
- 如果您未定義模組版本，安裝程式將會安裝與 .npm 名稱相符的任何模組。

執行 iManager 的靜默安裝

您可以使用 install.properties 檔案中的預設值以靜默模式安裝 iManager。依預設，該檔案位於各作業系統環境的 Identity Manager 安裝套件 .iso 影像檔中的 *products*\iManager 目錄內。*products*\iManager 目錄應該也包含安裝可執行檔。

1. 在主控台視窗中，移至下載的 install.properties 檔案所在的目錄。
2. 在指令行中，輸入下列其中一個指令：

```
iManagerInstall.exe -i silent
```

11.3 iManager 的安裝後任務

安裝 iManager 後，您可以修改組態設定，例如，啟用 IPv6 位址，或者變更 eDirectory 網路樹的授權使用者。此外，NetIQ 建議您取代安裝程序建立的自行簽署證書。

- 第 11.3.1 節「取代 iManager 的暫存自行簽署證書」(第 135 頁)
- 第 11.3.2 節「安裝後設定 iManager 以使用 IPv6 位址」(第 137 頁)
- 第 11.3.3 節「指定 eDirectory 的授權使用者」(第 137 頁)

11.3.1 取代 iManager 的暫存自行簽署證書

獨立 iManager 安裝會包含暫時性的自我簽署證書，以供 Tomcat 使用。證書的有效期為一年。NetIQ 提供此證書的目的是協助您啟動並執行系統，以便在安裝 iManager 後可立即安全地使用該產品。NetIQ 和 OpenSSL 不建議將自行簽署的證書用於測試以外的目的，相反，您應該用安全的證書取代暫存證書。

Tomcat 將自行簽署的證書儲存在使用 Tomcat (JKS) 格式檔案的金鑰儲存區中。通常，您是透過輸入私密金鑰來取代該證書的。但是，用於修改 Tomcat 金鑰儲存區的 keytool 無法輸入私密金鑰。該工具只能使用自行產生的金鑰。

本節說明如何使用 NetIQ Certificate Server 在 eDirectory 中產生公用金鑰 / 私密金鑰組，以及如何取代暫存證書。如果您正在使用 eDirectory，則可以使用 NetIQ Certificate Server 安全地產生、追蹤、儲存和撤銷證書，而無需再採用其他工具。

取代 iManager 自行簽署的證書

本節介紹如何在 eDirectory 中建立金鑰組，並透過 PKCS#12 檔案輸出公用金鑰、私密金鑰和根證書管理中心 (CA) 金鑰。其中包括修改 Tomcat 的 server.xml 組態檔案，以使用 PKCS12 指令，並使組態指向實際的 P12 檔案而不是使用預設的 JKS 金鑰儲存區。

此程序使用下列檔案：

- C:\Program Files\Novell\Tomcat\conf\ssl\.keystore，用於存放暫存金鑰組
- C:\Program Files\Novell\jre\lib\security\cacerts，用於存放可信的根證書
- C:\Program Files\Novell\Tomcat\conf\server.xml，用於設定 Tomcat 的證書用法

若要取代自行簽署的證書：

1. 若要建立新證書，請完成以下步驟：
   - **1a** 登入 iManager。
   - **1b** 按一下 **NetIQ Certificate Server** > 建立伺服器證書。
   - **1c** 選取相應的伺服器。
   - **1d** 指定伺服器的綽號。
   - **1e** 接受其餘的證書預設值。
2. 若要輸出伺服器證書，請完成以下步驟：
   - **2a** 在 iManager 中，選取目錄管理 > 修改物件。
   - **2b** 瀏覽並選取 Key Material Object (KMO) 物件。
   - **2c** 按一下證書 > 輸出。
   - **2d** 指定密碼。
   - **2e** 將伺服器證書儲存為 PKCS#12 (.pfx)。
3. 若要將 .pfx 檔案轉換為 .pem 檔案，請完成以下步驟：

   附註：系統上預設不會安裝 OpenSSL。不過，您可以從 OpenSSL 網站下載所需的版本。

   - **3a** 輸入一個指令，例如 openssl pkcs12 -in newtomcert.pfx -out newtomcert.pem。
   - **3b** 指定您在步驟 2 中為證書指定的相同密碼。
   - **3c** 為新的 .pem 檔案指定密碼。

     如果您想使用相同密碼也可以。
4. 若要將 .pem 檔案轉換為 .p12 檔案，請完成以下步驟：
   - **4a** 輸入一個指令，例如 openssl pkcs12 -export -in newtomcert.pem -out newtomcert.p12 -name "New Tomcat"。
   - **4b** 指定您在步驟 3 中為證書指定的相同密碼。
   - **4c** 為新的 .p12 檔案指定密碼。

     如果您想使用相同密碼也可以。
5. 將 .p12 檔案複製到 Tomcat 證書位置 (預設為 C:\Program Files\Novell\Tomcat\conf\ssl\)。
6. 使用 services.msc 啟動程序檔停止 Tomcat 服務。
7. 為確保 Tomcat 使用新建立的 .p12 證書檔案，請將 keystoreType、keystoreFile 和 keystorePass 變數新增至 Tomcat 的 server.xml 檔案中。例如：

```
<Connector className="org.apache.coyote.http11.Http11AprProtocol"
 port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
 acceptCount="100" debug="0" scheme="https" secure="true"
 useURIValidationHack="false" disableUploadTimeout="true">
   <Factory className="org.apache.coyote.tomcat7.CoyoteServerSocketFactory"
 clientAuth="false" protocol="TLS" keystoreType="PKCS12"
 keystoreFile="C:\Program Files\Novell\Tomcat\conf\ssl\newtomcert.p12" keystorePass="password"
/>
```

或，

```
<Connector className="org.apache.coyote.http11.Http11NioProtocol"
 port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
 acceptCount="100" debug="0" scheme="https" secure="true"
 useURIValidationHack="false" disableUploadTimeout="true">
   <Factory className="org.apache.coyote.tomcat7.CoyoteServerSocketFactory"
 clientAuth="false" protocol="TLS" keystoreType="PKCS12"
 keystoreFile="C:\Program Files\Novell\Tomcat\conf\ssl\newtomcert.p12" keystorePass="password"
/>
```

如果金鑰儲存區類型設定為 PKCS12，則您必須指定證書檔案的整個路徑，因為 Tomcat 不再預設為使用 Tomcat 主路徑。

8 使用 services.msc 啟動程序檔啟動 Tomcat 服務。

11.3.2 安裝後設定 iManager 以使用 IPv6 位址

安裝 iManager 後，您可以設定 iManager，讓其使用 IPv6 位址。

1. 開啟安裝目錄中的 catalina.properties 檔案。依預設，該檔案位於 *installation_directory*\Tomcat\conf 中。
2. 在 properties 檔案中設定以下組態項目：

   ```
   java.net.preferIPv4Stack=false
   ```

   ```
   java.net.preferIPv4Addresses=true
   ```

3. 重新啟動 Tomcat。

11.3.3 指定 eDirectory 的授權使用者

安裝 iManager 後，您可以修改授權使用者的身分證明，以及此使用者要管理的相應 eDirectory 網路樹名稱。如需詳細資訊，請參閱《*NetIQ iManager Administration Guide*》(NetIQ iManager 管理指南) 中的「iManager Authorized Users and Groups」(iManager 授權使用者和群組)。

1 登入 iManager。

2 在「設定」檢視窗中，選取 **iManager 伺服器** > **設定 iManager** > **安全性**。

3 更新使用者身分證明和網路樹名稱。

IV 安裝 Identity Applications

此部分將會引導您完成安裝 Identity Applications 所需元件和架構的程序：

- Identity Applications 管理
- Identity Applications 儀表板
- 角色與資源服務驅動程式
- 使用者應用程式
- 使用者應用程式驅動程式

依預設，安裝程式將在 C:\NetIQ\idm\apps 中安裝這些元件。

在安裝期間以及安裝之後，Identity Applications 需要存取其他 Identity Manager 元件。NetIQ 建議您在開始之前檢閱安裝程序。如需詳細資訊，請參閱第 15.1 章 「規劃安裝 Identity Applications」 (第 165 頁)。

12 為 Identity Manager 安裝 PostgreSQL 和 Tomcat

本章您將安裝大多數 Identity Manager 元件所用的以下應用程式伺服器和資料庫程式：

- Apache Tomcat
- PostgreSQL

安裝檔案位於 Identity Manager 安裝套件的 \products\CommonApplication\ 目錄中。依預設，安裝程式將在 C:\NetIQ\idm\apps\ 中安裝應用程式。

NetIQ 建議您在開始之前檢閱安裝程序。如需詳細資訊，請參閱第 12.1.1 節「Tomcat 和 PostgreSQL 的安裝核對清單」(第 141 頁)。

12.1 規劃安裝 PostgreSQL 和 Tomcat

從 Identity Manager 4.6 起，NetIQ 僅支援將 Apache Tomcat 用做應用程式伺服器。如果您的公司提供受支援版本的 Tomcat，您便可將其與 Identity Manager 配合使用。

此外，為方便起見，NetIQ 將 Tomcat 和 PostgreSQL 捆綁在同一個安裝程式中。使用此安裝程式，您無需分別下載即可安裝這些應用程式。除了 NetIQ Identity Manager 文件中所述的內容外，NetIQ 不會另外提供這些元件的更新或其管理、組態或調整資訊。

- 第 12.1.1 節「Tomcat 和 PostgreSQL 的安裝核對清單」(第 141 頁)
- 第 12.1.2 節「瞭解 PostgreSQL 和 Tomcat 的安裝程序」(第 142 頁)
- 第 12.1.3 節「安裝 PostgreSQL 的先決條件」(第 142 頁)
- 第 12.1.4 節「安裝 Tomcat 的先決條件」(第 143 頁)
- 第 12.1.5 節「PostgreSQL 的系統要求」(第 143 頁)
- 第 12.1.6 節「Tomcat 的系統要求」(第 143 頁)

12.1.1 Tomcat 和 PostgreSQL 的安裝核對清單

NetIQ 建議您完成以下核對清單中的步驟：

	核對清單項目
❑	1. 瞭解 Identity Manager 各元件之間的互動。如需詳細資訊，請參閱以下各節： ◆ 第 4.4 節「使用 Identity Manager 中的自助式密碼管理」(第 31 頁) ◆ 第 4.5 節「在 Identity Manager 中使用單一登入存取」(第 33 頁)
❑	2. 確定要為 Identity Manager 的元件使用哪些伺服器。如需詳細資訊，請參閱第 5.3.4 節「建議的伺服器設定」(第 41 頁)。

	核對清單項目
❑	3. 確定安裝 Tomcat 或 PostgreSQL 前是否應安裝 NetIQ Sentinel。如需詳細資訊，請參閱第 5.3 節「建議的安裝情境和伺服器設定」(第 39 頁)。 **附註：**僅支援在 Linux 伺服器上安裝 Sentinel。若要安裝 Sentinel，您的環境中必須有一部 Linux 伺服器。
❑	4. 檢閱關於安裝應用程式的考量，以確保電腦符合要求： ◆ 第 12.1.4 節「安裝 Tomcat 的先決條件」(第 143 頁) ◆ 第 12.1.3 節「安裝 PostgreSQL 的先決條件」(第 142 頁)
❑	5. 安裝應用程式： ◆ 若要執行引導式安裝，請參閱第 12.2.1 節「使用精靈安裝 PostgreSQL 和 Tomcat」(第 144 頁)。 ◆ 若要執行靜默安裝，請參閱第 12.2.2 節「以靜默模式為 Identity Manager 安裝 Tomcat 和 PostgreSQL」(第 146 頁)。
❑	6. 安裝其餘的 Identity Manager 元件。

12.1.2 瞭解 PostgreSQL 和 Tomcat 的安裝程序

您可以選擇安裝其中一個應用程式，或者兩者均安裝。例如，如果伺服器上已有受支援版本的 PostgreSQL，您可能就不需要安裝該應用程式。在進行個別安裝時，請注意以下事項：

PostgreSQL

安裝程序會安裝 Identity Applications 的資料庫，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。綱要資訊是在您安裝 Identity Applications 時新增。

如果伺服器上已在執行受支援版本的 PostgreSQL，安裝程式會提示您提供預設 postgres 使用者的密碼。然後，程式將會建立 idmadmin 使用者，並為其指定與 postgres 相同的密碼。

安裝程序結束後，安裝程式將會啟動資料庫例項。當您安裝使用該資料庫的其他 Identity Manager 元件 (例如使用者應用程式) 時，該例項必須處於執行中狀態。

您不需要使用 PostgreSQL 做為 Identity Applications 的資料庫。

Tomcat

安裝程序將會建立 IDM Apps Tomcat 服務。為了支援 Tomcat 應用程式伺服器，安裝程式還會安裝 Apache ActiveMQ 和 Oracle JRE。這些項目可協助 Tomcat 傳送電子郵件通知。

安裝程式在完成後不會啟動 Tomcat。在您安裝其他 Identity Manager 元件 (例如 Identity Reporting) 之前，Tomcat 必須處於停止狀態。

12.1.3 安裝 PostgreSQL 的先決條件

在規劃 PostgreSQL 的安裝之前，請檢閱以下考量：

- 您可以在執行舊版資料庫程式的環境中安裝 Identity Manager 綑綁的 PostgreSQL 版本。為了確保新安裝不會覆寫以前的版本，請為安裝檔案指定一個不同的目錄。

- Identity Applications 要求其使用的資料庫 (例如 PostgreSQL) 符合一些先決條件。如需詳細資訊，請參閱 「安裝 Identity Applications 資料庫的先決條件」 (第 171 頁)。
- 您不能安裝多個版本的 PostgreSQL，因為 PostgreSQL 的服務帳戶無法處理兩個例項。請在安裝此版本的 PostgreSQL 之前先解除安裝舊版本。

12.1.4 安裝 Tomcat 的先決條件

在規劃 Tomcat 的安裝之前，請檢閱以下考量：

- 您可以將 Tomcat 和 PostgreSQL 安裝在同一個伺服器上，也可以安裝在不同的伺服器上。
- 安裝程序將會安裝受支援版本的 Oracle JRE 和 Apache ActiveMQ。
- 安裝程序還會安裝 Apache Log4j 服務在稽核 Tomcat 事件時需要使用的檔案。
- 您可以使用自己的 Tomcat 安裝程式，而不使用 Identity Manager 安裝套件中提供的安裝程式。但是，若要將 Apache Log4j 服務與您的 Tomcat 版本配合使用，請確保已安裝相應的檔案。如需詳細資訊，請參閱 第 13.1.4 節 「使用 Apache Log4j 服務記錄登入」 (第 150 頁)。為 OSP、Identity Applications 和 Identity Reporting 使用 Tomcat 時，需要符合此項要求。
- 為了使用 ActiveMQ 保證電子郵件通知的傳送，請安裝 MQServer。
- Identity Applications 要求執行它們的 Tomcat 應用程式伺服器符合一些先決條件。如需詳細資訊，請參閱 「應用程式伺服器的先決條件和考量」 (第 169 頁)。
- 安裝程序會在 setenv.bat 檔案 (預設位於 c:\NetIQ\idm\apps\tomcat\bin 目錄) 中設定 JRE 位置。當您在 Tomcat 上安裝 Identity Applications 和 Identity Reporting 時，安裝程序會更新 setenv.bat 檔案中的 JAVA_OPTs 或 CATALINA_OPTS 項目。

12.1.5 PostgreSQL 的系統要求

PostgreSQL 對電腦的要求與 Identity Applications 的要求相同。如需詳細資訊，請參閱 「Identity Applications 的系統要求」 (第 172 頁)。另請參閱最新版 Identity Manager 的 《版本說明》，以及 PostgreSQL 文件。

12.1.6 Tomcat 的系統要求

Tomcat 對電腦的要求與 Identity Applications 的要求相同。如需詳細資訊，請參閱 第 15.1.4 節 「Identity Applications 的系統要求」 (第 172 頁)。另請參閱最新版 Identity Manager 的 《版本說明》，以及 Apache 文件。

12.2 安裝 PostgreSQL 和 Tomcat

本節將引導您完成安裝 Tomcat 和 PostgreSQL 的程序。

- 第 12.2.1 節 「使用精靈安裝 PostgreSQL 和 Tomcat」 (第 144 頁)
- 第 12.2.2 節 「以靜默模式為 Identity Manager 安裝 Tomcat 和 PostgreSQL」 (第 146 頁)

12.2.1 使用精靈安裝 PostgreSQL 和 Tomcat

以下程序介紹如何使用引導式程序在 Windows 平台上安裝 Tomcat 和 PostgreSQL。若要執行靜默模式的無人管理安裝，請參閱第 12.2.2 節「以靜默模式為 Identity Manager 安裝 Tomcat 和 PostgreSQL」(第 146 頁)。

若要進行安裝準備工作，請檢閱以下章節中列出的考量和系統要求：

- 第 12.1.4 節「安裝 Tomcat 的先決條件」(第 143 頁)
- 第 12.1.3 節「安裝 PostgreSQL 的先決條件」(第 142 頁)
- 該版本隨附的《版本說明》

附註：無論您要安裝 PostgreSQL 還是使用 PostgreSQL 的現有版本，都必須指定資料庫的密碼。但是，此安裝程式不支援含有 " 或 $ 字元的密碼。若要使用這些特殊字元，請在完成安裝程序後變更密碼。

若要執行引導式安裝：

1. 以管理員身分登入要安裝這些應用程式的電腦。
2. 確保規劃的安裝路徑不包含使用以下任一名稱的目錄：
   - tomcat
   - postgres
   - activemq
   - jre

   附註：安裝 Standard Edition 時，必須安裝 ActiveMQ。否則，當您登入 Identity Reporting 後，Reporting 頁面不會載入。您也可以在完成 PostgreSQL 安裝後將 activemq-all-5.15.2 jar 檔案複製到 C:\NetIQ\idm\apps\tomcat\lib 目錄中，然後重新啟動 Tomcat。

   ---
3. (視情況而定) 如果您已取得 Identity Manager 安裝套件的 .iso 影像檔，請導覽至包含安裝檔案的 \products\CommonApplication\postgre_tomcat_install 目錄。
4. (視情況而定) 如果您已從 NetIQ 下載網站下載了安裝檔案，請完成以下步驟：
   - **4a** 導覽至所下載影像的 win.zip 檔案。
   - **4b** 將該檔案的內容擷取到本地電腦上的某個目錄中。
5. 從包含安裝檔案的目錄中執行 TomcatPostgreSQL.exe。
6. 在安裝程式中，指定要用於安裝的語言，然後按一下**確定**。
7. 檢閱簡介資訊，然後按**下一步**。
8. 接受授權合約，然後按**下一步**。
9. 指定您要安裝 Tomcat、PostgreSQL，還是兩者都安裝。
10. 若要完成引導式程序，請指定以下參數的值：
    - **Tomcat 的上層資料夾**

      僅在安裝 Tomcat 時適用。

      指定要用來安裝 Tomcat 檔案的目錄。
    - **Tomcat 詳細資料**

僅在安裝 Tomcat 時適用。

代表 Tomcat 所需的連接埠。

Tomcat 關閉連接埠

指定您要用於完全關閉所有 Web 應用程式和 Tomcat 的連接埠。預設值為 8005。

Tomcat http 連接埠

指定您希望 Tomcat 伺服器在與用戶端電腦通訊時使用的連接埠。預設值為 8080。SSL 通訊的預設連接埠為 8443。

Tomcat 重新導向連接埠

(視情況而定) 如果您未使用 TLS/SSL 通訊協定，請指定應用程式伺服器用來重新導向需要 SSL 傳輸之要求的連接埠。預設值為 8443。

Tomcat ajp 連接埠

(選擇性) 指定您希望應用程式伺服器在透過 AJP 通訊協定 (而不是 http) 與 Web 連接器通訊時使用的連接埠。預設值為 8009。

當您希望應用程式伺服器管理 Web 應用程式中包含的靜態內容，並且 / 或者您想要利用應用程式伺服器的 SSL 處理時，請使用此參數。

- **PostgreSQL 的上層資料夾**

  僅在安裝 PostgreSQL 時適用。

  代表要用來安裝 PostgreSQL 檔案的目錄。

- **PostgreSQL 詳細資料**

  僅在安裝 PostgreSQL 時適用。

  代表 Identity Applications 的 PostgreSQL 資料庫設定。

附註：如果伺服器上已在執行受支援版本的 PostgreSQL，安裝程式會提示您提供預設 postgres 使用者的密碼。然後，程式將會建立 idmadmin 使用者，並為其指定與 postgres 相同的密碼。

此安裝程式不支援含有 " 或 $ 字元的密碼。

資料庫名稱

指定資料庫的名稱。預設值為 idmuserappdb。

資料庫管理員

指定 idmadmin 帳戶，這是一個可以建立資料庫表、檢視和其他產出工件的資料庫管理員。

此帳戶與預設的 postgres 使用者不同。

管理員使用者的密碼

指定資料庫管理員和預設 postgres 使用者的密碼。

此安裝程式不支援含有 " 或 $ 字元的密碼。

PostgreSQL 連接埠

指定代管 Postgres 資料庫之伺服器的連接埠。預設值為 5432。

11 檢閱安裝前摘要。

12 啟動安裝程序。

13 安裝程序完成後，按一下*完成*。

12.2.2 以靜默模式為 Identity Manager 安裝 Tomcat 和 PostgreSQL

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。在此模式下，InstallAnywhere 會使用預設 silent.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。若要執行引導式安裝，請參閱第 12.2.1 節「使用精靈安裝 PostgreSQL 和 Tomcat」(第 144 頁)。

若要進行安裝準備工作，請檢閱以下章節中列出的考量和系統要求：

- 第 12.1.4 節「安裝 Tomcat 的先決條件」(第 143 頁)
- 第 12.1.3 節「安裝 PostgreSQL 的先決條件」(第 142 頁)
- 「保護靜默安裝所用的密碼」(第 146 頁)
- 該版本隨附的 《版本說明》

保護靜默安裝所用的密碼

如果您不想在 postgresq_tomcat-silent.properties 檔案中指定用於安裝的密碼，可以改為在環境中設定密碼。在這種情況下，靜默安裝程式將從環境中讀取密碼，而不是從 postgresq_tomcat-silent.properties 檔案中讀取。如此可以提高安全性。

您必須為安裝指定以下密碼：

- NETIQ_DB_PASSWORD
- NETIQ_DB_PASSWORD_CONFIRM

使用 set 指令。例如：

```
set NETIQ_DB_PASSWORD_CONFIRM=myPassWord
```

該安裝程式不支援含有 " 或 $ 字元的密碼。若要使用這些特殊字元，請在安裝 PostgreSQL 後變更密碼。

以靜默模式安裝 Tomcat 和 PostgreSQL

1. 登入您要安裝應用程式的電腦。
2. (視情況而定) 如果您已取得 Identity Manager 安裝套件的 .iso 影像檔，請導覽至包含安裝檔案的 \products\CommonApplication\postgre_tomcat_install 目錄。
3. (視情況而定) 如果您已從 NetIQ 下載網站下載了安裝檔案，請完成以下步驟：
   - **3a** 導覽至所下載影像的 win.zip 檔案。
   - **3b** 將該檔案的內容擷取到本地電腦上的某個目錄中。
4. 若要指定安裝參數，請完成以下步驟：
   - **4a** 確定 postgresq_tomcat-silent.properties 檔案與安裝的可執行檔位於同一目錄中。
   - **4b** 在文字編輯器中，開啟 postgresq_tomcat-silent.properties 檔案。
   - **4c** 指定參數值。如需參數的描述，請參閱步驟 10 (第 144 頁)。
   - **4d** 儲存然後關閉該檔案。
5. 若要啟動安裝程序，請輸入以下指令：

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

附註：如果 postgresq_tomcat-silent.properties 檔案不在安裝程序檔所在的目錄中，您必須指定該檔案的完整路徑。該程序檔會將所需的檔案解包到暫存目錄，然後啟動靜默安裝。

13 安裝單一登入元件

本章將介紹如何安裝 One SSO Provider (OSP)，以支援 Identity Applications 和 Identity Reporting 的單一登入存取。

安裝檔案位於 Identity Manager 安裝套件的 products\CommonApplication\osp_install 目錄中。依預設，安裝程式將在 C:\NetIQ\idm\apps\osp 中安裝元件。

NetIQ 建議您在開始之前檢閱安裝程序。

13.1 為 Identity Manager 規劃安裝單一登入

本節提供安裝 One SSO Provider (OSP) 所需的先決條件、注意事項和系統設定資訊。

- 第 13.1.1 節「單一登入元件的核對清單」(第 149 頁)
- 第 13.1.2 節「安裝 One SSO Provider 的先決條件」(第 150 頁)
- 第 13.1.3 節「One SSO Provider 的系統要求」(第 150 頁)
- 第 13.1.4 節「使用 Apache Log4j 服務記錄登入」(第 150 頁)

13.1.1 單一登入元件的核對清單

NetIQ 建議您完成以下核對清單中的步驟：

	核對清單項目
❑	1. 瞭解 Identity Manager 各元件之間的互動。如需詳細資訊，請參閱第 4.5 節「在 Identity Manager 中使用單一登入存取」(第 33 頁)。
❑	2. 確定要為 Identity Manager 的元件使用哪些伺服器。如需詳細資訊，請參閱第 5.3 節「建議的安裝情境和伺服器設定」(第 39 頁)。
❑	3. 確保已安裝 Tomcat。如需詳細資訊，請參閱第 12.2 章 「安裝 PostgreSQL 和 Tomcat」(第 143 頁)。
❑	4. (視情況而定) 若要使用 Apache Log4j 服務來記錄 Tomcat 中的事件，請確保您有相應的檔案。如需詳細資訊，請參閱第 13.1.4 節「使用 Apache Log4j 服務記錄登入」(第 150 頁)。
❑	5. 安裝 OSP ： ◆ 若要執行引導式安裝，請參閱第 13.2.1 節「使用精靈安裝 One SSO Provider」(第 151 頁)。 ◆ 若要執行靜默安裝，請參閱第 13.2.2 節「以靜默模式安裝 One SSO Provider」(第 153 頁)。
❑	6. 安裝 Self Service Password Reset (SSPR) 以管理 Identity Applications 的使用者密碼。如需詳細資訊，請參閱第 14.2 節「為 Identity Manager 安裝密碼管理功能」(第 157 頁)。

	核對清單項目
❑	7. 安裝 Identity Applications 並將其設定為使用單一登入存取。如需詳細資訊，請參閱第 15.5 節「安裝 Identity Applications」(第 181 頁)。

13.1.2 安裝 One SSO Provider 的先決條件

以下 Identity Manager 元件需要使用 OSP 來驗證使用者。

- Identity Applications
- Identity Reporting

NetIQ 建議您在安裝 OSP 之前檢閱以下考量：

- 若要執行 OSP，您可以使用自己的 Tomcat 安裝程式，而不使用 Identity Manager 安裝套件中提供的安裝程式。但是，若要將 Apache Log4j 服務與您的 Tomcat 版本配合使用，請確保已安裝相應的檔案。如需詳細資訊，請參閱第 13.1.4 節「使用 Apache Log4j 服務記錄登入」(第 150 頁)。
- OSP 需要使用信任證書來確保 Identity Applications 和報告元件能夠與驗證伺服器通訊。安裝程序會自動在 osp.jks 檔案中建立用於 TLS/SSL 的證書。您還可以讓安裝程序為 eDirectory 的 SAML 宣示建立可信根證書。

附註：這些證書將在建立之日的兩年後過期。原始證書過期後，您必須建立新證書。如需詳細資訊，請參閱「驗證伺服器」(第 215 頁) 與第 VIII 部分「在 Identity Manager 中設定單一登入存取」(第 277 頁)。

13.1.3 One SSO Provider 的系統要求

OSP 需要使用 Apache Tomcat 應用程式伺服器。Tomcat 的版本必須為 Identity Applications 所需的版本。

所有其他伺服器要求與 Identity Applications 的伺服器要求相符。如需詳細資訊，請參閱第 15.1.3 節「安裝 Identity Applications 的先決條件和考量」(第 167 頁) 和此版本的最新 《版本說明》。

13.1.4 使用 Apache Log4j 服務記錄登入

您可以使用 Apache Log4j 或 java.util.logging 服務來記錄 Tomcat 中發生的事件。Identity Manager 安裝套件中的 Tomcat 安裝程式包含執行 Log4j 所需的檔案。但如果您安裝了自己的 Tomcat 版本，若要使用 Apache 記錄服務，則需要以下檔案：

- log4j-1.2.16.jar
- tomcat-juli-adapters.jar
- tomcat-juli.jar

若要將這些檔案新增至 Tomcat 安裝中，請完成以下步驟：

1 從 Apache 網站下載 Tomcat 8.5.x 的「JULI」檔案：
   - tomcat-juli.jar
   - tomcat-juli-adapters.jar
2 從 Apache 網站下載 log4j-1.2.16.jar 檔案。
3 將以下檔案放在 $TOMCAT_HOME\lib 目錄中：
   - log4j-1.2.16.jar
   - tomcat-juli-adapters.jar
4 將 tomcat-juli.jar 檔案放在 $TOMCAT_HOME\bin 目錄中。
5 為 CATALINA_OPTS 中的 -Dlog4j.configuration 指定值，或者在 $TOMCAT_HOME\lib 目錄中建立 log4j.properties 檔案。

13.2 為 Identity Manager 安裝單一登入

- 第 13.2.1 節「使用精靈安裝 One SSO Provider」(第 151 頁)
- 第 13.2.2 節「以靜默模式安裝 One SSO Provider」(第 153 頁)
- 第 13.2.3 節「設定單一登入存取」(第 154 頁)

13.2.1 使用精靈安裝 One SSO Provider

以下程序介紹如何使用安裝精靈在 Windows 平台上安裝 OSP。若要執行靜默模式的無人管理安裝，請參閱第 13.2.2 節「以靜默模式安裝 One SSO Provider」(第 153 頁)。若要進行安裝準備工作，請檢閱第 13.1.1 節「單一登入元件的核對清單」(第 149 頁) 中列出的先決條件和系統要求。

1 以管理員身分登入要安裝 OSP 的伺服器。
2 停止 Tomcat 伺服器。
3 (視情況而定) 如果您已取得 Identity Manager 安裝套件的 .iso 影像檔，請導覽至包含 OSP 安裝檔案的目錄 (預設為 products\CommonApplication\osp_install 目錄)。
4 (視情況而定) 如果您已下載 OSP 安裝檔案，請完成以下步驟：
   - **4a** 導覽至所下載影像的 win.zip 檔案。
   - **4b** 將該檔案的內容擷取到本地電腦上的某個目錄中。
5 從包含安裝檔案的目錄中執行 osp-install-win.exe 檔案。
6 閱讀並接受授權合約，然後按下一步。
7 指定安裝檔案的路徑。
8 使用以下參數完成引導式程序：
   - **Tomcat 詳細資料**

     代表 Tomcat 伺服器的主目錄。例如 C:\NetIQ\idm\apps\tomcat\。安裝程序會將 OSP 的一些檔案新增至此資料夾中。
   - **Tomcat Java 主目錄**

     代表 Tomcat 伺服器上 Java 的主目錄。例如，C:\NetIQ\idm\jre。安裝程序會將 OSP 的一些檔案新增至該目錄中。

- 應用程式位址

  代表使用者連接至 Tomcat 伺服器上的 OSP 時所需的 URL 設定。例如，https://myserver.mycompany.com:8543。

  通訊協定

  指定您要使用 *http* 還是 *https*。若要使用安全通訊端層 (SSL) 進行通訊，請指定 https。

  主機名稱

  指定要安裝 OSP 的伺服器的 DNS 名稱或 IP 位址。請不要使用 localhost。

  連接埠

  指定您希望伺服器在與用戶端電腦通訊時使用的連接埠。

- 登入螢幕自訂

  指定要在使用者登入螢幕上顯示的自訂名稱。預設值為 **Identity Access**。

附註：僅支援 Latin1 標準字元集。

- 驗證詳細資料

  代表與包含可以登入應用程式之使用者清單的驗證伺服器相連接需要符合的要求。如需驗證伺服器的詳細資訊，請參閱第 4.5.1 節「瞭解使用 One SSO Provider 進行驗證的方法」(第 33 頁)。

  LDAP 主機

  指定 LDAP 驗證伺服器的 DNS 名稱或 IP 位址。請不要使用 localhost。

  LDAP 連接埠

  指定您希望 LDAP 驗證伺服器在與 Identity Manager 通訊時使用的連接埠。例如，指定 389 做為非安全連接埠，或者為 SSL 連接指定 636。

  使用 SSL

  指定是否要為 Identity Vault 與驗證伺服器之間的連接使用安全通訊端層通訊協定。

  JRE 可信證書儲存區 (cacerts) 檔案

  僅當您要對 LDAP 連接使用 SSL 時才適用。

  指定證書的路徑。例如，C:\NetIQ\idm\apps\jre\lib\security\cacerts。

  JRE 可信證書儲存區密碼

  僅當您要對 LDAP 連接使用 SSL 時才適用。

  指定 cacerts 檔案的密碼。

  管理員 DN

  僅在安裝新的驗證伺服器時適用。

  指定 LDAP 驗證伺服器管理員帳戶的 DN。例如 cn=admin,ou=sa,o=system。

  管理密碼

  僅在安裝新的驗證伺服器時適用。

  指定 LDAP 驗證伺服器管理員帳戶的密碼。

  使用者容器

  僅在安裝新的驗證伺服器時適用。

  指定 LDAP 驗證伺服器中要用來儲存可以登入 Access Review 之使用者帳戶的容器。例如 o=data。

管理員容器

僅在安裝新的驗證伺服器時適用。

指定 LDAP 驗證伺服器中要用來儲存管理員帳戶的容器。例如 ou=sa,o=system。

Identity Vault

指定您的 Identity Vault。

金鑰儲存區密碼

僅在安裝新的驗證伺服器時適用。

指定要為 LDAP 驗證伺服器的新金鑰儲存區建立的密碼。

該密碼必須至少包含六個字元。

- 稽核詳細資料 (OSP)

代表用於稽核驗證伺服器中發生的 OSP 事件的設定。

(視情況而定) ***為 OSP 啟用稽核***

指定是否要將 OSP 事件傳送到稽核伺服器。

如果選取此設定，您還需指定稽核記錄快取的位置。

稽核記錄快取資料夾

僅當為 OSP 啟用了稽核時才適用。

指定要用於稽核之快取目錄的位置。例如 C:\NetIQ\idm\naudit\jcache。

指定現有證書 / 產生證書

指出您要使用 NAudit 伺服器的現有證書，還是建立新的證書。

輸入公用金鑰

僅當您要使用現有證書時才適用。

列出您希望 NAudit 服務用來驗證稽核訊息的自訂公用金鑰證書。

輸入 RSA 金鑰

僅當您要使用現有證書時才適用。

指定您希望 NAudit 服務用來驗證稽核訊息的自訂私密金鑰檔案所在的路徑。

9 若要安裝 SSPR，請繼續第 14 部分「安裝密碼管理元件」(第 155 頁)。

如需設定忘記密碼管理的詳細資訊，請參閱第 15.7.8 節「設定忘記密碼管理功能」(第 199 頁)。

13.2.2 以靜默模式安裝 One SSO Provider

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。

1 以管理員身分登入要安裝這些元件的電腦。

2 停止 Tomcat。

3 (視情況而定) 如果您已取得 Identity Manager 安裝套件的 .iso 影像檔案，請導覽至包含 OSP 安裝檔案的目錄 (預設為 osp 目錄)。

4 (視情況而定) 如果您已從 NetIQ 下載網站下載了安裝檔案，請完成以下步驟：

4a 導覽至所下載影像的 .zip 檔案。

4b 將該檔案的內容擷取到本地電腦上的某個資料夾中。

5 將 osp.configure.properties 檔案複製到您有權寫入的位置，然後編輯此檔案。

如需安裝設定的詳細資訊，請參閱步驟 7 和步驟 8 (第 151 頁)。

6 若要執行靜默安裝，請執行以下指令：

osp-install-win.exe -i silent -f *path_to_silent.properties_file*

在此指令中，請指定檔案的絕對路徑。例如：

osp-install-win.exe -i silent -f *c:\NetIQ\idm\apps\osp\osp.silent.properties*

7 安裝 SSPR。如需詳細資訊，請參閱第 14 部分「安裝密碼管理元件」(第 155 頁)。

13.2.3 設定單一登入存取

安裝 OSP 之後，需要立即執行一些動作來設定單一登入存取。但是，最終的組態程序需要您先安裝 Identity Applications。如需詳細資訊，請參閱第 VIII 部分「在 Identity Manager 中設定單一登入存取」(第 277 頁)。

附註：在靜默模式下設定 One SSO Provider 時，請務必在 osp.silent.properties 檔案中指定正確的安裝、Java、Tomcat 和 SSL 金鑰儲存區資料夾路徑。例如，

安裝資料夾：USER_INSTALL_DIR=C:\NetIQ\idm\apps\osp

Tomcat 資料夾：NETIQ_TOMCAT_HOME=C:\NetIQ\idm\apps\tomcat

Windows：NETIQ_TOMCAT_HOME=C:\NetIQ\idm\apps\tomcat

Java 資料夾：NETIQ_JAVA_HOME=C:\NetIQ\idm\apps\jre

SSL 金鑰儲存區資料夾：USER_INSTALL_DIR=C:\NetIQ\idm\apps\jre\lib\security\cacerts

---

14 安裝密碼管理元件

本章將介紹如何安裝 Self Service Password Reset (SSPR)，該工具可協助您將 Identity Manager 設定為允許使用者重設其密碼。

SSPR 與 Identity Applications、Identity Reporting 和 OSP 相整合，可確保需要修改密碼的使用者無需執行任何額外動作，就能導向至相應的網頁。在使用者完成其自助活動後，SSPR 會將使用者重新導向至他們最初嘗試存取的應用程式。

附註：Identity Manager 4.6 及以上版本使用 SSPR 做為主要的密碼管理工具。

Identity Manager 不要求安裝 SSPR。您可以使用其他方法來重設使用者密碼，但可能需要修改 Identity Manager 的一些組態設定。如需詳細資訊，請參閱第 15.7.8 節「設定忘記密碼管理功能」(第 199 頁)。

安裝檔案位於 \products\CoomonApplication\sspr_install 目錄中。依預設，安裝程式將在 C:\NetIQ\idm\apps\sspr 中安裝 SSPR 元件。

NetIQ 建議您在開始之前檢閱安裝程序。

14.1 為 Identity Manager 規劃安裝密碼管理功能

本節提供安裝 Self Service Password Reset (SSPR) 所需的先決條件、注意事項和系統設定資訊。

- 第 14.1.1 節「安裝密碼管理元件的核對清單」(第 155 頁)
- 第 14.1.2 節「安裝 Self Service Password Reset 的先決條件」(第 156 頁)
- 第 14.1.3 節「Self Service Password Reset 的系統要求」(第 156 頁)
- 第 14.1.4 節「針對密碼事件使用 Apache Log4j 服務」(第 156 頁)

14.1.1 安裝密碼管理元件的核對清單

NetIQ 建議您完成以下核對清單中的步驟：

	核對清單項目
❑	1. 瞭解 Identity Manager 各元件之間的互動。如需詳細資訊，請參閱第 4.4 節「使用 Identity Manager 中的自助式密碼管理」(第 31 頁)。
❑	2. 確定要為 Identity Manager 的元件使用哪些伺服器。如需詳細資訊，請參閱第 5.3 節「建議的安裝情境和伺服器設定」(第 39 頁)。
❑	3. 確保已安裝 Tomcat。如需詳細資訊，請參閱第 12.2 章「安裝 PostgreSQL 和 Tomcat」(第 143 頁)。

	核對清單項目
❑	4. (視情況而定) 若要使用 Apache Log4j 服務來記錄 Tomcat 中的事件，請確保您有相應的檔案。如需詳細資訊，請參閱第 13.1.4 節「使用 Apache Log4j 服務記錄登入」(第 150 頁)。
❑	5. 安裝 SSPR ： ◆ 若要執行引導式安裝，請參閱第 14.2.1 節「使用精靈安裝 Self Service Password Reset」(第 157 頁)。 ◆ 若要執行靜默安裝，請參閱第 14.2.2 節「以靜默模式安裝 Self Service Password Reset」(第 160 頁)。
❑	6. 安裝 Identity Applications，並將其設定為使用單一登入存取和密碼管理。如需詳細資訊，請參閱第 15.5 章「安裝 Identity Applications」(第 181 頁)。

14.1.2 安裝 Self Service Password Reset 的先決條件

NetIQ Self Service Password Reset (SSPR) 的安裝應該符合 Identity Applications 的伺服器要求，並且安裝時需注意以下事項：

- SSPR 要求使用 TSL/SSL 通訊協定進行通訊。
- SSPR 要求使用受支援版本的 Tomcat 應用程式伺服器。如需詳細資訊，請參閱第 12.1.4 節「安裝 Tomcat 的先決條件」(第 143 頁) 和此版本的最新 《版本說明》。
- NetIQ 建議您檢閱 *《NetIQ Self Service Password Reset Administration Guide》* (NetIQ Self Service Password Reset 管理指南) 中列出的先決條件和要求。

14.1.3 Self Service Password Reset 的系統要求

SSPR 需要使用 Apache Tomcat 應用程式伺服器。Tomcat 的版本必須為 Identity Applications 所需的版本。

所有其他伺服器要求與 Identity Applications 的伺服器要求相符。如需詳細資訊，請參閱第 15.1.3 節「安裝 Identity Applications 的先決條件和考量」(第 167 頁) 和此版本的最新 《版本說明》。

14.1.4 針對密碼事件使用 Apache Log4j 服務

您可以使用 Apache Log4j 或 java.util.logging 服務來記錄 Tomcat 中發生的事件。Identity Manager 安裝套件中的 Tomcat 安裝程式包含執行 Log4j 所需的檔案。但如果您安裝了自己的 Tomcat 版本，若要使用 Apache 記錄服務，則需要以下檔案：

- log4j-1.2.16.jar
- tomcat-juli-adapters.jar
- tomcat-juli.jar

若要將這些檔案新增至 Tomcat 安裝中，請完成以下步驟：

1 從 Apache 網站下載 Tomcat 8.5.x 的「JULI」檔案：
   - tomcat-juli.jar
   - tomcat-juli-adapters.jar

2 從 Apache 網站下載 log4j-1.2.16.jar 檔案。

3 將以下檔案放在 $TOMCAT_HOME\lib 目錄中：

- log4j-1.2.16.jar
- tomcat-juli-adapters.jar

4 將 tomcat-juli.jar 檔案放在 $TOMCAT_HOME/bin 目錄中。

5 為 CATALINA_OPTS 中的 -Dlog4j.configuration 指定值，或者在 $TOMCAT_HOME\lib 目錄中建立 log4j.properties 檔案。

14.2 為 Identity Manager 安裝密碼管理功能

本節介紹 SSPR 的安裝程序。您可以將這些程式安裝在安裝了 OSP 元件的同一部伺服器上，也可以安裝在不同的伺服器上。

- 第 14.2.1 節「使用精靈安裝 Self Service Password Reset」(第 157 頁)
- 第 14.2.2 節「以靜默模式安裝 Self Service Password Reset」(第 160 頁)
- 第 14.2.3 節「安裝後任務」(第 160 頁)
- 第 14.2.4 節「為叢集設定 OSP 和 SSPR」(第 162 頁)

附註：如果您使用舊的忘記密碼管理方法，則不需要安裝 SSPR。如需詳細資訊，請參閱第 4.4.2 節「瞭解舊密碼管理提供程式」(第 32 頁)。

14.2.1 使用精靈安裝 Self Service Password Reset

以下程序介紹如何使用安裝精靈在 Windows 平台上安裝 SSPR。若要執行靜默模式的無人管理安裝，請參閱第 14.2.2 節「以靜默模式安裝 Self Service Password Reset」(第 160 頁)。若要進行安裝準備工作，請檢閱第 14.1.1 節「安裝密碼管理元件的核對清單」(第 155 頁) 中列出的先決條件和系統要求。

1 以管理員身分登入要安裝 SSPR 的伺服器。

2 停止 Tomcat 伺服器。

3 (視情況而定) 如果您已取得 Identity Manager 安裝套件的 .iso 影像檔，請導覽至包含 SSPR 安裝檔案的目錄 (預設為 products\CommonApplication\sspr_install 目錄)。

4 (視情況而定) 如果您已下載 SSPR 安裝檔案，請完成以下步驟：

   4a 導覽至所下載影像的 win.zip 檔案。

   4b 將該檔案的內容擷取到本地電腦上的某個目錄中。

5 從包含安裝檔案的目錄中執行 sspr-install-win.exe 檔案。

6 閱讀並接受授權合約，然後按下一步。

7 指定安裝檔案的路徑。

8 使用以下參數完成引導式程序：

- **Tomcat 詳細資料**

  代表 Tomcat 伺服器的主目錄。例如 C:\NetIQ\idm\apps\tomcat。安裝程序會將 SSPR 的一些檔案新增至此資料夾。

- **Tomcat 連接**

  代表使用者連接至 Tomcat 伺服器上的 SSPR 時所需的 URL 設定。例如，https://myserver.mycompany.com:8080。

附註：如果存在以下考量，您還必須選取連接至外部驗證伺服器，並指定外個伺服器的值：

- 您要安裝 SSPR。
- OSP 與 SSPR 在不同的受支援應用程式伺服器例項上執行。

通訊協定

指定您要使用 *http* 還是 *https*。若要使用安全通訊端層 (SSL) 進行通訊，請指定 https。

主機名稱

指定要安裝 SSPR 的伺服器的 DNS 名稱或 IP 位址。請不要使用 localhost。

連接埠

指定您希望伺服器在與用戶端電腦通訊時使用的連接埠。

連接至外部驗證伺服器

指定是否要用不同的 Tomcat 例項來代管驗證伺服器 (OSP)。驗證伺服器包含可登入 SSPR 的使用者清單。

如果選取此設定，則還要指定驗證伺服器的通訊協定、主機名稱和連接埠值。

- **Tomcat Java 主目錄**

  代表 Tomcat 伺服器上 Java 的主目錄。例如，C:\NetIQ\idm\jre。安裝程序會將 OSP 的一些檔案新增至該目錄中。

- **驗證詳細資料**

  代表與包含可以登入應用程式之使用者清單的驗證伺服器相連接需要符合的要求。如需驗證伺服器的詳細資訊，請參閱第 4.5.1 節「瞭解使用 One SSO Provider 進行驗證的方法」(第 33 頁)。

LDAP 主機

指定 LDAP 驗證伺服器的 DNS 名稱或 IP 位址。請不要使用 localhost。

LDAP 連接埠

指定您希望 LDAP 驗證伺服器在與 Identity Manager 通訊時使用的連接埠。例如，指定 389 做為非安全連接埠，或者為 SSL 連接指定 636。

使用 SSL

指定是否要為 Identity Vault 與驗證伺服器之間的連接使用安全通訊端層通訊協定。

JRE 可信證書儲存區 (cacerts) 檔案

僅當您要對 LDAP 連接使用 SSL 時才適用。

指定證書的路徑。例如，C:\NetIQ\idm\apps\jre\lib\security\cacerts。

JRE 可信證書儲存區密碼

僅當您要對 LDAP 連接使用 SSL 時才適用。

指定 cacerts 檔案的密碼。

管理員 DN

僅在安裝新的驗證伺服器時適用。

指定 LDAP 驗證伺服器管理員帳戶的 DN。例如 cn=admin,ou=sa,o=system。

管理密碼

僅在安裝新的驗證伺服器時適用。

指定 LDAP 驗證伺服器管理員帳戶的密碼。

使用者容器

僅在安裝新的驗證伺服器時適用。

指定 LDAP 驗證伺服器中要用來儲存可以登入 Access Review 之使用者帳戶的容器。例如 o=data。

管理員容器

僅在安裝新的驗證伺服器時適用。

指定 LDAP 驗證伺服器中要用來儲存 Access Review 管理員帳戶的容器。例如 ou=sa,o=system。

金鑰儲存區密碼

僅在安裝新的驗證伺服器時適用。

指定要為 LDAP 驗證伺服器的新金鑰儲存區建立的密碼。

該密碼必須至少包含六個字元。

- **SSPR 詳細資料**

代表設定 SSPR 時需要使用的設定。

組態密碼

指定要為管理員建立的用於設定 SSPR 的密碼。

依預設，SSPR 沒有組態密碼。若不指定該密碼，任何能夠登入 SSPR 的使用者皆可修改組態設定。

SSPR 重新導向 URL

指定在 SSPR 中完成密碼變更或處理安全問題等動作後，用戶端將重新導向到的絕對 URL。例如，轉到儀表板。

請使用以下格式：通訊協定 :// 伺服器 : 連接埠 / 路徑。例如，http://*IDM_userapp_ 伺服器 _IP: 連接埠號碼* /idmdash/#/landing。

- 驗證伺服器詳細資料

代表您要建立的供 SSPR 服務在連接到伺服器上 OSP 用戶端時使用的密碼。該密碼又稱為用戶端密碼。

若要在安裝後修改此密碼，請使用 RBPM 組態公用程式。

- 稽核詳細資料 **(SSPR)**

代表用於稽核驗證伺服器中發生的 SSPR 事件的設定。

(視情況而定) ***為 SSPR 啟用稽核***

指定是否要將 SSPR 事件傳送到稽核伺服器。

如果選取此設定，您還需指定 syslog 伺服器的設定。

Syslog 主機名稱

僅當為 SSPR 啟用了稽核時才適用。

指定代管 syslog 伺服器之伺服器的 DNS 或 IP 位址。請不要使用 localhost。

Syslog 連接埠

僅當為 SSPR 啟用了稽核時才適用。

指定代管 syslog 伺服器之伺服器的連接埠。

9 若要將 Identity Applications 和 Identity Reporting 設定為使用 SSPR，請繼續第 15 章 「安裝 Identity Applications」(第 165 頁)。

10 在組態更新公用程式中，更新 SSO 用戶端參數。如需更多資訊，請參閱「Self Service Password Reset」(第 222 頁)。

如需設定忘記密碼管理的詳細資訊，請參閱第 15.7.8 節 「設定忘記密碼管理功能」(第 199 頁)。

14.2.2 以靜默模式安裝 Self Service Password Reset

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。

1 以管理員身分登入要安裝這些元件的電腦。

2 停止 Tomcat。

3 (視情況而定) 如果您已取得 Identity Manager 安裝套件的 .iso 影像檔案，請導覽至包含 SSPR 安裝檔案的目錄 (預設為 sspr 目錄)。

4 (視情況而定) 如果您已從 NetIQ 下載網站下載了安裝檔案，請完成以下步驟：

   4a 導覽至所下載影像的 .zip 檔案。

   4b 將該檔案的內容擷取到本地電腦上的某個資料夾中。

5 針對 SSPR 安裝編輯 sspr-silent.properties 檔案。依預設，該檔案與安裝程序檔位於同一目錄中。

如需安裝設定的詳細資訊，請參閱步驟 7 (第 157 頁) 和步驟 8 (第 157 頁)。

6 若要執行靜默安裝，請執行以下指令：

```
sspr-install-win.exe -i silent -f path_to_silent.properties_file
```

7 在組態更新公用程式中，更新 SSO 用戶端參數。如需更多資訊，請參閱「Self Service Password Reset」(第 222 頁)。

14.2.3 安裝後任務

確定無錯安裝

安裝 SSPR 後，您便可修改組態設定，例如變更預設設定檔的 LDAP 群組 DN 的管理員許可權，或變更轉遞 URL。此外，NetIQ 還建議您驗證安裝程序建立的 URL，並視需要進行變更。

1 若要開啟 SSPR 登入頁面，請在瀏覽器中輸入以下 URL ：

   protocol://server:port/web-context

   例如，

   http://192.168.0.1:8080/sspr/

2 在 SSPR 登入頁面的右上角，從清單中選取**組態編輯器**。

3 指定組態密碼，然後按一下**登入**。

4 在樹狀檢視中選取**預設設定**，並確定在 **LDAP 廠商預設設定**清單中選取了 **NetIQ IDM/OAuth 整合**。

5 在樹狀檢視中，按一下 **LDAP > LDAP 目錄 > 預設 > 連接 > LDAP 證書**，然後按一下**從伺服器輸入**以輸入證書。

(視情況而定) 在同一頁面上按一下**測試 LDAP 設定檔**，確定可以存取所有已設定的 LDAP 伺服器。

6 在樹狀檢視中，按一下**模組 > 已驗證 > 管理**，並確定已將管理員許可權指定給預設設定檔的 LDAP 群組 DN。

如果執行的是 SSPR 全新安裝，則該清單為空。您需要在 iManager 中建立一個新群組，並將 admin 使用者新增至該群組。

7 在樹狀檢視中，按一下**設定 > 應用程式 > 應用程式**，並確定**轉遞 URL** 設定為 http://*<Server:Port>*/idmdash/#/landing。

例如 http:/192.168.0.1:8080/idmdash/#/landing。

8 在樹狀檢視中，按一下**設定 > 使用者介面 > 外觀**，然後將**介面主題**變更為 **Micro Focus (mdefault)** (如果尚未指定)。

9 在樹狀檢視中，按一下**設定 > 單一登入 (SSO) 用戶端 > OAuth**，然後驗證是否為以下參數指定了正確的值：

OAuth 登入 URL

指定 OAuth 伺服器登入的 URL。當使用者登入時，此 URL 會將使用者重新導向以向 OSP 進行驗證。

例如 http://192.168.0.1:8080/osp/a/idm/auth/oauth2/grant

OAuth 代碼解析服務 URL

指定 OAuth 代碼解析服務的 URL。SSPR 使用此 Web 服務 URL 來解析 OAuth 身分伺服器傳回的產出工件。

例如 http://192.168.0.1:8080/osp/a/idm/auth/oauth2/authcoderesolve

OAuth 設定檔服務 URL

指定 Identity Manager 所提供用於傳回使用者屬性資料的 Web 服務 URL。

例如 http://192.168.0.1:8080/osp/a/idm/auth/oauth2/getattributes

OAUTH Web 服務伺服器證書

(視情況而定) 如果已啟用 HTTPS，請輸入 OAuth Web 服務伺服器的證書。

OAuth 用戶端 ID

指定 OAuth 用戶端的用戶端 ID。例如，sspr.

OAuth 共享機密

指定 OAuth 共享機密的密碼。此密碼在 OSP 和 SSPR 應用程式之間共享。

OAuth 使用者名稱 //DN 登入屬性

指定 SSPR 用來申請 OAuth 伺服器在本地驗證使用者的使用者屬性。例如 name。

10 在頁面右上角按一下 以儲存組態。

11 在 SSPR 登入頁面的右上角，從清單中選取**組態管理器**。

12 按一下**限制組態**。

將通用密碼規則指定給使用者容器

若要將通用密碼規則指定給使用者容器：

1 登入 iManager。
2 選取角色與任務 > 密碼規則，然後選取密碼規則。
3 若要選取具有管理權限的使用者：
   3a 按一下通用密碼 > 組態選項 > 通用密碼取回。
   3b 選取允許管理員取回密碼或允許以下使用者取回密碼，然後按一下確定。
   例如，cn=uaadmin,ou=sa,o=data
4 按一下規則指定，然後將容器指定給該使用者所在的容器。
   例如，o=data 或管理使用者。

授予對 pwmResponseSet 屬性的權限

已驗證其權限的使用者可以依據與使用者連接相關聯的許可權執行操作。已驗證的使用者需要對自己的使用者項目擁有以下權限：

- [項目權限] 的瀏覽權限
- pwmResponseSet 的讀取、比較和寫入權限

若要授予對 pwmResponseSet 屬性的權限，請執行以下步驟：

1 登入 iManager。
2 按一下。
3 按一下 iManager 伺服器 > 設定 iManager。
4 按一下其他 > 啟用 [this]。
5 按一下。
6 在樹狀檢視中，選取目錄中所有使用者的頂層容器。
7 按一下目前層級核取方塊，然後按一下動作 > 修改託管者。
8 在清單中按一下 [This]，然後按一下新增託管者。
9 按一下「套用」。
10 針對 [This] 託管者按一下指定的權限。
11 按一下新增內容，然後選取在綱要中顯示所有內容核取方塊。
12 從清單中選取 pwmResponseSet。
   確定已選取「寫入」、「比較」、「讀取」和「繼承」選項。
13 按一下完成。

14.2.4 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

執行以下步驟以設定已安裝在單獨電腦上的 SSPR ：

1 檢閱第 14.1.1 節「安裝密碼管理元件的核對清單」(第 155 頁) 中的先決條件和系統要求。

2 依照第 14.2.1 節「使用精靈安裝 Self Service Password Reset」(第 157 頁) 中的說明操作，並務必在安裝期間執行以下步驟。

   a. 在應用程式伺服器連接頁面中，選取**連接至外部驗證伺服器**，並提供安裝了負載平衡器的伺服器的 DNS 名稱。

   b. 在驗證詳細資料頁面中，提供 Identity Manager 引擎伺服器的 IP 位址和連接埠。CA 證書的密碼為「changeit」。

   c. 完成 SSPR 安裝後，更新 SSL 設定。如需詳細資訊，請參閱第 29.8 節「更新 Self Service Password Reset 的 SSL 設定」(第 306 頁)。

3 若要在叢集的第一個節點中更新 SSPR 資訊，請啟動 C:\NetIQ\idm\apps\UserApplication\configupdate.bat 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，請參閱第 15.7.8 節「設定忘記密碼管理功能」(第 199 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 203 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：

   C:NetIQ\idm\apps\jre\bin\keytool -genkey -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： C:NetIQ\idm\apps\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：

   C:NetIQ\idm\apps\jre\bin\keytool -list -v -keystore osp.jks -storepass changeit

6 備份位於 C:\NetIQ\idm\apps\osp 中的原始 osp.jks 檔案，並將新的 osp.jks 檔案複製到此位置。新 osp.jks 檔案是在步驟 3 中建立的。

7 將第一個節點上位於 C:\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。

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.bat 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.bat 檔案中新增 JVM 內容「-Djava.net.preferIPv4Stack=true」。

9b 在第一個節點上的 setenv.bat 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。

10 在使用者應用程式中啟用叢集。如需更多資訊，請參閱步驟 10 (第 192 頁)。

11 為叢集啟用許可權索引。如需更多資訊，請參閱第 15.4.2 節「為叢集啟用許可權索引」(第 178 頁)。

12 啟用 Tomcat 叢集。如需詳細資訊，請參閱第 15.4.3 節「準備 Identity Applications 的應用程式伺服器」(第 179 頁) 中的「步驟 9」。

13 在所有節點上重新啟動 Tomcat。

14 為叢集設定使用者應用程式驅動程式。如需更多資訊，請參閱第 15.6.2 節「為叢集設定使用者應用程式驅動程式」(第 193 頁)。

15 安裝 Identity Applications

本章將引導您完成安裝 Identity Applications 所需元件和架構的程序：

- Identity Applications 管理
- Identity Applications 儀表板
- 角色與資源服務驅動程式
- 使用者應用程式
- 使用者應用程式驅動程式

依預設，安裝程式將在 C:\NetIQ\idm\apps 中安裝這些元件。

在安裝期間以及安裝之後，Identity Applications 需要存取其他 Identity Manager 元件。NetIQ 建議您在開始之前檢閱安裝程序。如需詳細資訊，請參閱第 15.1 章 「規劃安裝 Identity Applications」 (第 165 頁)。

15.1 規劃安裝 Identity Applications

Identity Applications 安裝包含以下元件：

- Identity Manager 儀表板
- Identity Manager 管理主控台
- 使用者應用程式
- 角色與資源服務驅動程式 (RRSD)
- 使用者應用程式驅動程式 (UAD)

安裝不包含 Identity Applications 所需的以下兩個驅動程式：使用者應用程式驅動程式，以及角色與資源服務驅動程式。

附註：從技術上講，Identity Reporting 可視為一種身分應用程式，因為該元件也使用 SSPR 和 OSP，並且您是透過 RBPM 組態公用程式來修改設定的。不過，Identity Reporting 有自己的安裝程式，可安裝在單獨的伺服器上，並且使用不同的資料庫。如需詳細資訊，請參閱第 16.5 節「Identity Reporting 的系統要求」(第 228 頁)。

- 第 15.1.1 節 「Identity Applications 的安裝核對清單」 (第 166 頁)
- 第 15.1.2 節 「瞭解 Identity Applications 的安裝程式」 (第 167 頁)
- 第 15.1.3 節 「安裝 Identity Applications 的先決條件和考量」 (第 167 頁)
- 第 15.1.4 節 「Identity Applications 的系統要求」 (第 172 頁)

15.1.1 Identity Applications 的安裝核對清單

NetIQ 建議您在開始安裝程序之前先檢閱以下步驟：

	核對清單項目
❑	1. 瞭解 Identity Manager 各元件之間的互動。如需詳細資訊，請參閱第 4.3.1 節「使用者應用程式和 Roles Based Provisioning Module」(第 29 頁)。
❑	2. 確定要為 Identity Manager 的元件使用哪些伺服器。如需詳細資訊，請參閱第 5.3.4 節「建議的伺服器設定」(第 41 頁)。
❑	3. 決定在安裝 Identity Applications 之前是否應安裝 Sentinel。如需詳細資訊，請參閱第 5.3 節「建議的安裝情境和伺服器設定」(第 39 頁)。
❑	4. 確保 Identity Manager 引擎已安裝。如需安裝引擎的詳細資訊，請參閱第 8 章「規劃安裝引擎、驅動程式和外掛程式」(第 73 頁)。
❑	5. 檢閱關於安裝 Identity Applications 及其支援架構的考量，以確保您的伺服器符合先決條件。如需詳細資訊，請參閱第 15.1.3 節「安裝 Identity Applications 的先決條件和考量」(第 167 頁)。
❑	6. 檢閱代管 Identity Applications 及其架構的電腦需要符合的硬體和軟體要求。如需詳細資訊，請參閱「Identity Applications 的系統要求」(第 172 頁)。
❑	7. 確保 eDirectory 在預設 LDAP 連接埠 389 和 636 上執行，以免收到關於綱要無效的錯誤訊息。您可以在安裝後手動延伸 eDirectory 綱要。如需詳細資訊，請參閱第 15.2.1 節「將使用者應用程式綱要做為記錄應用程式新增至稽核伺服器中」(第 173 頁)。
❑	8. 在 eDirectory Identity Vault 中建立一個使用者應用程式管理員帳戶。如需詳細資訊，請參閱第 15.2.2 節「向 Identity Vault 管理員和使用者應用程式管理員帳戶指定權限」(第 174 頁)。
❑	9. 在本地電腦或連接的伺服器上為 Identity Applications 安裝並設定資料庫。 ◆ 若要瞭解該資料庫，請參閱「安裝 Identity Applications 資料庫的先決條件」(第 171 頁)。 ◆ 若要安裝該資料庫，請參閱第 15.3 章「設定 Identity Applications 的資料庫」(第 175 頁)。
❑	10. 在本地電腦上或叢集中準備一個應用程式伺服器。 ◆ 若要瞭解相關要求，請參閱「應用程式伺服器的先決條件和考量」(第 169 頁)。 ◆ 若要準備叢集，請參閱第 15.4 章「準備 Identity Applications 的環境」(第 178 頁)。 ◆ 若要安裝應用程式伺服器，請參閱第 15.4.3 節「準備 Identity Applications 的應用程式伺服器」(第 179 頁)。
❑	11. (視情況而定) 若要使用 Apache Log4j 服務來記錄 Tomcat 中的事件，請確保您有相應的檔案。如需詳細資訊，請參閱第 13.1.4 節「使用 Apache Log4j 服務記錄登入」(第 150 頁)。
❑	12. 檢閱 Identity Applications 安裝套件的內容，以確定您的環境需要哪些檔案。如需詳細資訊，請參閱第 15.1.2 節「瞭解 Identity Applications 的安裝程式」(第 167 頁)。
❑	13. 建立並部署使用者應用程式驅動程式及角色與資源服務驅動程式。如需詳細資訊，請參閱第 15.6 章「建立和部署 Identity Applications 的驅動程式」(第 192 頁)。
❑	14. 安裝 Identity Applications。如需詳細資訊，請參閱第 15.5 章「安裝 Identity Applications」(第 181 頁)。

	核對清單項目
❑	15. 若要執行安裝程序中的最後幾個任務，請參閱第 15.7 章 「完成 Identity Applications 的安裝」 (第 194 頁)。
❑	16. 確保您已正確設定 Identity Applications 和單一登入設定。如需詳細資訊，請參閱第 28 章 「驗證是否可對 Identity Applications 進行單一登入存取」 (第 293 頁)。
❑	17. (選擇性) 若要開始使用 Identity Applications，請參閱 《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》 (NetIQ Identity Manager - Identity Applications 管理員指南)。

15.1.2 瞭解 Identity Applications 的安裝程式

Identity Applications 的安裝檔案位於安裝套件的 \products\UserApplication\ 目錄中。

安裝程式 (IdmUserApp.exe) 會執行以下操作：

- 指定現有的應用程式伺服器版本，以供使用。
- 指定要使用的現有資料庫版本。該資料庫用於儲存 Identity Applications 的資料和組態資訊。
- 設定 JDK 的證書檔案，以便 Tomcat 上執行的 Identity Applications 能夠安全地與 Identity Vault 和使用者應用程式驅動程式通訊。
- 設定使用者應用程式的 Java Web 應用程式歸檔 (WAR) 檔案，並將其部署到 Tomcat。
- 透過 Sentinel 稽核用戶端實現記錄功能 (如果您選擇如此)。
- 允許您輸入現有萬能金鑰，以還原特定的 Identity Applications 安裝，以及為叢集提供支援。

15.1.3 安裝 Identity Applications 的先決條件和考量

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。如需設定使用者應用程式環境的詳細資訊，請參閱 《*NetIQ Identity Manager - Identity Applications 使用者指南*》。

- 「Identity Applications 的安裝考量」 (第 167 頁)
- 「Identity Applications 的組態和使用考量」 (第 169 頁)
- 「應用程式伺服器的先決條件和考量」 (第 169 頁)
- 「在叢集環境中安裝 Identity Applications 的先決條件」 (第 170 頁)
- 「安裝 Identity Applications 資料庫的先決條件」 (第 171 頁)

Identity Applications 的安裝考量

在安裝 Identity Applications 時，請注意以下事項。

- 需要以下 Identity Manager 元件的支援版本：
  - Designer
  - Identity Vault
  - Identity Manager 引擎

- 遠端載入器
- One SSO Provider

如需這些元件所需版本和修補程式的詳細資訊，請參閱最新的 《版本說明》。

- 確認 Identity Vault 包括已建立且部署的使用者應用程式及角色與資源服務驅動程式。如需詳細資訊，請參閱第 15.6 章 「建立和部署 Identity Applications 的驅動程式」(第 192 頁)。
- 在安裝 Identity Applications 之前，請安裝以下架構項目：
  - 在本地電腦上安裝一個應用程式伺服器。如需詳細資訊，請參閱「應用程式伺服器的先決條件和考量」(第 169 頁)。
  - 在本地電腦或連接的伺服器上安裝一個資料庫。如需詳細資訊，請參閱「安裝 Identity Applications 資料庫的先決條件」(第 171 頁)。
- (選擇性) NetIQ 建議為 Identity Manager 各元件之間的通訊啟用安全通訊端層 (SSL) 通訊協定。若要使用 SSL 通訊協定，必須在您的環境中啟用 SSL，並在安裝期間指定 **https**。如需啟用 SSL 的資訊，請參閱 《*NetIQ Analyzer for Identity Manager Administration Guide*》 (NetIQ Analyzer for Identity Manager 管理指南) 中的「Configuring Security in the Identity Applications」(設定 Identity Applications 中的安全性)。
- 在建立角色與資源驅動程式之前，建立使用者應用程式驅動程式。角色與資源驅動程式會參考使用者應用程式驅動程式中的角色儲存區容器 (RoleConfig.AppConfig)。
- 角色與資源服務驅動程式無法與遠端載入器配合使用，因為該驅動程式使用 jClient。
- 將 JAVA_HOME 環境變數設定為指向您打算與 Identity Applications 配合使用的 JDK。若要置換 JAVA_HOME，請在安裝期間手動指定路徑。
- 依預設，安裝程序會將程式檔案放在 C:\NetIQ\idm 目錄中。

  如果您打算在非預設位置安裝使用者應用程式，則新目錄必須存在且可寫入。
- 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。
- (視情況而定) 如果您打算使用外部密碼管理，您的環境必須符合以下要求：
  - 為要部署 Identity Applications 和 IDMPwdMgt.war 檔案的 Tomcat 啟用安全通訊端層 (SSL) 通訊協定。
  - 請確定您的防火牆已開放 SSL 連接埠。

  如需為 Tomcat 啟用 SSL 的詳細資訊，請參閱第 29.8 節「更新 Self Service Password Reset 的 SSL 設定」(第 306 頁)。

  如需 IDMPwdMgt.war 檔案的詳細資訊，請參閱第 15.7.8 節「設定忘記密碼管理功能」(第 199 頁)。
- (選擇性) 若要從受管理系統擷取授權，請安裝一或多個 Identity Manager 驅動程式。
  - 您必須使用受 Identity Manager 3.6.1、4.0 或更高版本支援的驅動程式。如需安裝驅動程式的詳細資訊，請參閱 NetIQ Identity Manager 驅動程式文件網站中的相應驅動程式指南。
  - 若要管理驅動程式，您必須事先已安裝 Designer 或 iManager 的相應外掛程式。如需詳細資訊，請參閱第 11.1.3 節「瞭解 iManager 外掛程式的安裝」(第 126 頁)。

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。

- 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。如需在安裝期間設定索引的詳細資訊，請參閱「其他」(第 212 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。
- 在未登入 Identity Applications 的情況下，使用者無法以訪客或匿名使用者的身分存取 Identity Applications。系統將提示使用者登入使用者介面。如需詳細資訊，請參閱第 VIII 部分「在 Identity Manager 中設定單一登入存取」(第 277 頁)。
- 為確保 Identity Manager 強制執行通用密碼功能，請將 Identity Vault 設定為使用「NMAS 登入」做為使用者首次登入時要執行的程序。將 NDSD_TRY_NMASLOGIN_FIRST 連帶字串值 true 新增至 HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Environment 登錄機碼。
- (視情況而定) 若要執行報告，您的環境中必須已安裝 Identity Reporting 的元件。如需詳細資訊，請參閱《Administrator Guide to NetIQ Identity Reporting》(NetIQ Identity Reporting 管理員指南)。
- 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，必須在環境中安裝並設定 Identity Reporting 和稽核服務，以擷取事件。此外，您還必須對 Identity Applications 進行設定以支援稽核。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)。

應用程式伺服器的先決條件和考量

若要使用 Identity Applications，需要安裝 Tomcat，同時需注意以下事項：

- Tomcat 必須在與 Java Development Kit (JDK) 或 Java Runtime Environment (JRE) 配合執行。如需受支援版本的詳細資訊，請參閱「Identity Applications 的系統要求」(第 172 頁)。
- 將 JAVA_HOME 環境變數設定為指向您打算與使用者應用程式配合使用的 JDK。若要置換 JAVA_HOME，請在安裝期間手動指定路徑。
- (視情況而定) 您可以使用自己的 Tomcat 安裝程式，而不使用 Identity Manager 安裝套件中提供的安裝程式。但是，若要將 Apache Log4j 服務與您的 Tomcat 版本配合使用，請確保已安裝相應的檔案。如需詳細資訊，請參閱第 13.1.4 節「使用 Apache Log4j 服務記錄登入」(第 150 頁)。
- (視情況而定) 若要保留您數位簽名的文件，必須在 Tomcat 應用程式伺服器上安裝 Identity Applications，並使用 Novell Identity Audit。數位簽名文件不會與工作流程資料一起儲存在「使用者應用程式」資料庫中，而是儲存在記錄資料庫中。此外，您還必須啟用記錄才能保留這些文件。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「Setting Up Logging in the Identity Applications」(在 Identity Applications 中設定記錄)。

- (視情況而定) 在需要記錄大量使用者資料或者目錄伺服器包含大量物件的環境中，您可能需要使用多個部署了 Identity Applications 的應用程式伺服器。如需進行效能最佳化設定的詳細資訊，請參閱 《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》 (NetIQ Identity Manager - Identity Applications 管理員指南) 中的「Tuning the Performance of the Applications」(調整應用程式的效能)。
- (視情況而定) 如果您使用 Tomcat 應用程式伺服器，在完成安裝程序之前，請不要啟動該伺服器。
- (視情況而定) 若要使用外部密碼管理，您必須執行以下操作來啟用安全通訊端層 (SSL) 通訊協定：
  - 為要部署 Identity Applications 和 IDMPwdMgt.war 檔案的 Tomcat 啟用 SSL。
  - 請確定您的防火牆已開放 SSL 連接埠。

  如需 IDMPwdMgt.war 檔案的詳細資訊，請參閱設定忘記密碼管理功能 和 《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》(NetIQ Identity Manager - Identity Applications 管理員指南)。
- 安裝程序不會修改 Tomcat 伺服器上的 JAVA_HOME 或 JRE_HOME 項目。依預設，Tomcat 的便捷安裝程式會將 setenv.bat 檔案放在 C:\NetIQ\idm\apps\tomcat\bin\ 目錄中。安裝程式還會在該檔案中設定 JRE 位置。

在叢集環境中安裝 Identity Applications 的先決條件

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。
- 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。

如需在叢集環境中設定 Identity Applications 的詳細資訊，請參閱第 15.4 章 「準備 Identity Applications 的環境」(第 178 頁)。

安裝 Identity Applications 資料庫的先決條件

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，必須建立一個 JDBC 驅動程式。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。
- 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 不支援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 177 頁) 或第 15.3.1 節「設定 Oracle 資料庫」(第 175 頁)。
- 為了避免在移轉期間發生重複鍵錯誤，請使用區分大小寫的定序。如果發生重複鍵錯誤，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。
- 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。

15.1.4 Identity Applications 的系統要求

本節介紹安裝 Identity Applications 的最低要求。

類別	要求
處理器	1 GHz

類別	要求
磁碟空間	1 GB **附註：**為支援應用程式的內容 (例如資料庫和應用程式伺服器記錄) 提供足夠空間。
記憶體	4 GB
作業系統 (已認證)	以下 64 位元作業系統之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 對於 32 位元作業系統： ◆ Windows Server 2008 SP2 NetIQ 建議您在安裝 Identity Manager 之前，依照製造商的自動更新機制來套用最新的作業系統修補程式。 **附註：***已認證*指作業系統已進行全面測試且受支援。
作業系統 (受支援)	已認證作業系統的最新版 Service Pack **附註：***受支援*指作業系統尚未進行測試，但預期可正常運作。
虛擬化系統	◆ VMWare ESX 5.5 及更新版本 NetIQ 允許您在為執行 NetIQ 產品的作業系統提供官方支援的企業級虛擬化系統上執行 Identity Manager。只要虛擬化系統的廠商為這些作業系統提供官方支援，NetIQ 就支援在這些系統上執行整個 Identity Manager 堆疊。
資料庫	◆ PostgreSQL 9.6.6 ◆ Orcale 12c ◆ MsSQL 2016, 2014 **附註：**請勿在 Tomcat 的類別路徑中包含 PostgreSQL 版本 (例如 9.6.6)。如果指定這些版本，系統可能不會載入首頁影像。
網頁瀏覽器	以下任意瀏覽器 (最低版本)： ◆ Google Chrome 61 ◆ Mozilla Firefox 51 **附註：**必須在瀏覽器中啟用 Cookie。
應用程式伺服器	Apache Tomcat 8.5.27
Java	JRE 1.8.0_162
連接埠	8180

15.2 為 Identity Applications 準備 Identity Vault

本節的內容可協助您為安裝 Identity Applications 做好準備。應用程式在名為 Roles Based Provisioning Module (RBPM) 的架構上執行。當您安裝 Identity Manager 引擎時，安裝程序會自動安裝 netiq-DXMLuad-4.7.0-0.noarch，該程式會安裝使用者應用程式驅動程式和角色與服務驅動程式，並延伸 eDirectory 綱要以便與 RBPM 互動。

安裝檔案位於 Identity Manager 安裝套件 .iso 影像檔中的 products\UserApplication\ 目錄下。

- 第 15.2.1 節「將使用者應用程式綱要做為記錄應用程式新增至稽核伺服器中」(第 173 頁)
- 第 15.2.2 節「向 Identity Vault 管理員和使用者應用程式管理員帳戶指定權限」(第 174 頁)

15.2.1 將使用者應用程式綱要做為記錄應用程式新增至稽核伺服器中

如果稽核伺服器要將使用者應用程式做為記錄應用程式使用，則您必須將 dirxml.lsc 檔案複製到該伺服器上。本節內容僅適用於 Novell Identity Audit。

1. 找到 dirxml.lsc 檔案。

   安裝後，此檔案位於 Identity Manager 使用者應用程式安裝目錄中，例如 C:\NetIQ\idm\apps\UserApplication。
2. 使用網頁瀏覽器存取裝有 Novell Identity Audit 外掛程式的 iManager，然後以管理員身分登入。
3. 導覽至**角色與任務 > 稽核與記錄**，然後選取**記錄伺服器選項**。
4. 瀏覽至網路樹中的「記錄服務」容器，選取相應的稽核安全記錄伺服器，然後按一下**確定**。
5. 在**記錄應用程式**索引標籤中，選取相應的容器名稱，然後按一下**新增記錄應用程式**連結。
6. 在「新增記錄應用程式」對話方塊中完成以下步驟：
   - **6a** 對於「記錄應用程式名稱」，請指定對環境而言有意義的任意名稱。
   - **6b** 對於「輸入 LSC 檔案」，請瀏覽至 dirxml.lsc 檔案。
   - **6c** 按一下「**確定**」。
7. 按一下「**確定**」，以完成您的 Audit 伺服器組態。
8. 確保將「記錄應用程式」中的狀態設定為**開啟** (狀態下面的圓圈應該為綠色)。
9. 重新啟動 Audit 伺服器，以啟用新記錄應用程式設定。

15.2.2 向 Identity Vault 管理員和使用者應用程式管理員帳戶指定權限

Identity Vault 管理員是有權設定 Identity Vault 的使用者。這是可與其他管理使用者類型共享的邏輯角色。

Identity Vault 管理員需要以下權限：

- 對使用者應用程式驅動程式及其包含的所有物件的「監督者」權限。若要實現此目的，可在驅動程式容器層級設定權限，並將這些權限設為可繼承。
- 對透過目錄抽象層使用者實體定義所定義的任何使用者的「監督者輸入」權限。這應該包括對 objectClass 以及與 DirXML-EntitlementRecipient、srvprvEntityAux 和 srvprvUserAux 輔助類別關聯的任何屬性的「寫入屬性」權限。

- 對容器物件 cn=DefaultNotificationCollection, cn=Security 的「監督者」權限。此物件儲存用於自動佈建電子郵件的電子郵件伺服器設定。它可以包含對電子郵件伺服器自身進行驗證所用的 SecretStore 身分證明。
- 對容器物件 cn=Authorized Login Methods, cn=Security 的「監督者」權限。在安裝使用者應用程式期間，系統會在此容器中建立 SAML 聲明物件。
- 在安裝使用者應用程式之前，請確定您對 cn=Security 容器擁有「監督者」權限。在安裝使用者應用程式期間，系統會在 cn=Security 容器下建立 cn=RBPMTrustedRootContainer 容器。

  或者，您可以手動建立 cn=RBPMTrustedRootContainer,cn=Security 容器 (建立名為 Trusted Root Container 的物件，並在其 Security 容器中包含 NDSPKI:Trusted Root 物件類別)，然後指定對該容器的「監督者」權限。

您必須在 Identity Vault 中手動建立使用者應用程式管理員帳戶，以便正確安裝 Roles Based Provisioning Module。該使用者應用程式管理員帳戶必須是頂層容器的託管者，並且必須對該容器擁有「監督者」權限。

在建立使用者應用程式管理員帳戶時，必須向此新使用者容器指定密碼規則。如需詳細資訊，請參閱《*Password Management Administration Guide*》(密碼管理管理指南) 中的「Creating Password Policies」(建立密碼規則)。

若要為使用者應用程式管理員帳戶建立許可權，請在 LDAP 資料交換格式 (LDIF) 檔案中執行以下指令：

```
dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 1#subtree#[Root]#[Entry Rights]
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#description
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#directReports
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#mail
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#manager
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#photo
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#srvprvQueryList
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#srvprvUserPrefs
```

```
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#telephoneNumber
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#title

dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 17#subtree#%%RBPM_USER_APP_ADMIN_DN%%#[Entry Rights]
ACL: 35#subtree#%%RBPM_USER_APP_ADMIN_DN%%#[All Attributes Rights]
```

15.3 設定 Identity Applications 的資料庫

Identity Applications 的資料庫支援多種任務，例如，儲存組態資料和工作流程活動的資料。您必須先安裝並設定資料庫，然後才能安裝應用程式。如需受支援資料庫的詳細資訊，請參閱第 15.1.4 節「Identity Applications 的系統要求」(第 172 頁)。如需使用者應用程式資料庫考量的詳細資訊，請參閱「安裝 Identity Applications 資料庫的先決條件」(第 171 頁)。

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

- 第 15.3.1 節「設定 Oracle 資料庫」(第 175 頁)
- 第 15.3.2 節「設定 PostgreSQL 資料庫」(第 177 頁)
- 第 15.3.3 節「設定 SQL Server 資料庫」(第 177 頁)

15.3.1 設定 Oracle 資料庫

本節介紹為使用者應用程式使用 Oracle 資料庫時可用的組態選項。如需受支援 Oracle 版本的詳細資訊，請參閱「Identity Applications 的系統要求」(第 172 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';

預期輸出為： 12.1.0.2

設定字元集

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

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

```
select * from nls_database_parameters;
```

如果資料庫未設定為使用 UTF-8，系統將會回應以下資訊：

```
NLS_CHARACTERSET
WE8MSWIN1252
```

否則，系統會回應以下資訊，確認資料庫已設定為使用 UTF-8：

```
NLS_CHARACTERSET
AL32UTF8
```

附註：建議使用 JDBC JAR 版本 ojdbc6.jar。

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

設定管理員使用者帳戶

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

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

其中，*idmuser* 代表使用者帳戶。

15.3.2 設定 PostgreSQL 資料庫

為方便起見，NetIQ 提供了一個 PostgreSQL 安裝程式，該程式完全支援 Identity Manager 中的架構服務和應用程式。該安裝程式可引導您完成組態程序。如需詳細資訊，請參閱第 12.2 章 「安裝 PostgreSQL 和 Tomcat」(第 143 頁)。

15.3.3 設定 SQL Server 資料庫

本節介紹為使用者應用程式使用 SQL Server 資料庫時可用的組態選項。如需受支援 SQL Server 版本的詳細資訊，請參閱「Identity Applications 的系統要求」(第 172 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

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

- CREATE TABLE
- DELETE
- INSERT
- SELECT
- UPDATE

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

15.4 準備 Identity Applications 的環境

當 Identity Applications 在叢集中執行時，會因更高的可用性而受益良多。此外，它們還支援 HTTP 工作階段複製和工作階段容錯移轉。也就是說，如果正在執行一個工作階段的某個節點發生失敗，則無需使用者進行干預，該工作階段就能在叢集中的另一個伺服器上繼續。

本節提供關於準備環境 (包括叢集環境)，以供 Identity Applications 正常執行的指示。必須結合第 15.5.2 節「使用引導式程序安裝 Identity Applications」(第 182 頁)中的說明來完成本節中的步驟。

如需叢集環境要求的詳細資訊，請參閱第 15.1.3 節「安裝 Identity Applications 的先決條件和考量」(第 167 頁)和第 15.1.4 節「Identity Applications 的系統要求」(第 172 頁)。

- 第 15.4.1 節「指定許可權索引的位置」(第 178 頁)
- 第 15.4.2 節「為叢集啟用許可權索引」(第 178 頁)
- 第 15.4.3 節「準備 Identity Applications 的應用程式伺服器」(第 179 頁)
- 第 15.4.4 節「為 Identity Applications 準備叢集」(第 180 頁)

15.4.1 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 C:\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 = C:\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。

15.4.2 為叢集啟用許可權索引

本節提供為叢集啟用許可權索引的說明。

1. 在叢集的第一個節點中登入 iManager，然後導覽至**檢視物件**。
2. 在**系統**下，導覽至包含 **使用者應用程式驅動程式**的驅動程式集。
3. 選取 **AppConfig** > **AppDefs** > **組態**。
4. 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>
   ```

5. 按一下「**確定**」。

15.4.3 準備 Identity Applications 的應用程式伺服器

您應準備好將要執行 Identity Applications 的 Tomcat。為方便起見，NetIQ 在安裝套件中提供了 Apache Tomcat。如需在叢集環境中使用應用程式的詳細資訊，另請參閱第 15.4.4 節「為 Identity Applications 準備叢集」(第 180 頁)。

Identity Manager 的 .iso 安裝檔案中包含一個用於安裝 Tomcat (或者 PostgreSQL) 的程式。如需詳細資訊，請參閱第 12.2 章 「安裝 PostgreSQL 和 Tomcat」(第 143 頁)。

您可以使用自己的 Tomcat 安裝程式，而不使用安裝套件中提供的便捷安裝程式。但是，如果您要使用其他安裝程式，則必須執行一些額外的步驟才能使 Tomcat 配合 Identity Applications 正常運作。

在啟動安裝程序之前，請確保此 Identity Applications 版本支援您要安裝的元件版本。如需詳細資訊，請參閱第 15.1.3 節「安裝 Identity Applications 的先決條件和考量」(第 167 頁)。

1 將 Apache Tomcat 做為一項服務安裝在您的伺服器上。

   如需詳細資訊，請參閱「Tomcat Setup」(Tomcat 安裝)。

2 在裝有 Tomcat 的同一個伺服器上安裝以下元件。

   - **Java Runtime Environment (JRE)**：如需詳細資訊，請參閱《Java Platform Installation Guide》(Java 平台安裝指南)。

- **Apache ActiveMQ**：如需詳細資訊，請參閱 ActiveMQ。
- **PostgreSQL**：如需詳細資訊，請參閱 PostgreSQL 手冊。

3 將 activemq-all-5.15.2 jar 檔案複製到 *C:\NetIQ\idm\apps\activemq* 資料夾。

4 將以下檔案複製到 *C:\NetIQ\idm\apps\tomcat\bin* 資料夾，以用於記錄。
   - log4j.jar
   - log4j.properties
   - tomcat-juli-adapters.jar

5 在 setenv.bat 檔案中設定以下內容。

```
JAVA_HOME
JRE_HOME
PATH (set Java path)
JAVA_OPTS="-Xms1024m -Xmx1024m"
```

6 將 postgresql-9.4.1212jdbc42.jar 檔案複製到 C:\NetIQ\idm\apps\tomcat\bin 資料夾。

7 (視情況而定) 在叢集環境中，開啟叢集第一個節點上的 server.xml 檔案 (預設位於 \TOMCAT_INSTALLED_HOME\conf\ 目錄中)，取消註解下面一行：

   <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>

   對叢集中的所有節點執行此操作。

   對於進階 Tomcat 叢集組態，請依照 Apache Tomcat 相關文件中的步驟操作。

15.4.4 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 180 頁)
- 「設定工作流程引擎 ID 的系統內容」(第 180 頁)
- 「為叢集中的每個使用者應用程式使用相同的萬能金鑰」(第 180 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。

如需在叢集環境中安裝產品所需符合之先決條件的詳細資訊，請參閱第 15.1.3 節「安裝 Identity Applications 的先決條件和考量」(第 167 頁)。

設定工作流程引擎 ID 的系統內容

在叢集中代管 Identity Applications 的每個伺服器都可以執行一個工作流程引擎。為確保叢集和工作流程引擎的效能，叢集中的每個伺服器都應使用相同的分割區名稱和分割區 UDP 群組。此外，叢集中的每個伺服器都必須使用唯一的工作流程引擎 ID 啟動，因為工作流程引擎的叢集化獨立於 Identity Applications 的快取架構運作。

為確保工作流程引擎正常執行，您必須設定 Tomcat 的系統內容。

1 對叢集中的每個 Identity Applications 伺服器建立一個新 JVM 系統內容。
2 將系統內容命名為 com.novell.afw.wf. *引擎 ID*，其中的引擎 ID 是一個唯一值。

為叢集中的每個使用者應用程式使用相同的萬能金鑰

Identity Applications 使用萬能金鑰來加密敏感性資料。叢集中的所有 Identity Applications 都必須使用相同的萬能金鑰。本節的內容可協助您確保叢集中的所有 Identity Applications 都使用相同的萬能金鑰。

如需建立萬能金鑰的詳細資訊，請參閱步驟 6 (第 182 頁) 中的**安全性 - 萬能金鑰**。如需加密 Identity Applications 中敏感性資料的詳細資訊，請參閱《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》(NetIQ Identity Manager - Identity Applications 管理員指南) 中的「Encrypting Sensitive Identity Applications Data」(加密 Identity Applications 敏感性資料)。

1 在叢集中的第一個節點上安裝使用者應用程式。
2 在安裝程式的「安全性 - 萬能金鑰」視窗中，記下將要包含 Identity Applications 新萬能金鑰的 master-key.txt 檔案所在的位置。依預設，該檔案位於安裝目錄中。
3 在叢集中的其餘節點上安裝 Identity Applications。
4 在「安全性 - 萬能金鑰」視窗中，按一下**是**，然後按**下一步**。
5 在「輸入萬能金鑰」視窗中，複製在步驟 2 中建立之文字檔案中的萬能金鑰。

15.5 安裝 Identity Applications

本節提供關於為使用者應用程式和 RBPM 安裝及設定應用程式伺服器的指示。您必須為應用程式伺服器使用正確的 Java 環境版本。

如需 Tomcat 和 Java 要求的詳細資訊，請參閱第 15.1.4 節「Identity Applications 的系統要求」(第 172 頁)。

- 第 15.5.1 節「Identity Applications 的安裝核對清單」(第 181 頁)
- 第 15.5.2 節「使用引導式程序安裝 Identity Applications」(第 182 頁)
- 第 15.5.3 節「安裝後步驟」(第 187 頁)
- 第 15.5.4 節「停用阻止 HTML 框架設定以將 Identity Manager 與 SSPR 整合」(第 189 頁)
- 第 15.5.5 節「驗證使用者內容」(第 190 頁)
- 第 15.5.6 節「啟動 Identity Applications」(第 191 頁)

15.5.1 Identity Applications 的安裝核對清單

使用以下核對清單來逐步完成 Identity Applications 的安裝程序。

	核對清單項目
❑	1. (視情況而定) 檢閱在叢集環境中的 Tomcat 上安裝 Identity Applications 的注意事項。如需詳細資訊，請參閱「瞭解 Tomcat 環境中的叢集群組」(第 180 頁)。
❑	2. 安裝受支援版本的應用程式伺服器和 Java 開發套件或執行時期環境。如需詳細資訊，請參閱第 15.1.4 節「Identity Applications 的系統要求」(第 172 頁)。
❑	3. 確認 Tomcat 的設定正確。如需詳細資訊，請參閱第 15.4.3 節「準備 Identity Applications 的應用程式伺服器」(第 179 頁)。
❑	4. 設定資料庫的資料來源檔案和 JDBC 提供者。
❑	5. 安裝 Identity Applications。如需詳細資訊，請參閱第 15.5.2 節「使用引導式程序安裝 Identity Applications」(第 182 頁)。
❑	6. 為 Identity Applications 設定 Tomcat。如需詳細資訊，請參閱第 15.5.3 節「安裝後步驟」(第 187 頁)。
❑	7. 部署並啟動 Identity Applications。如需詳細資訊，請參閱「啟動 Identity Applications」(第 191 頁)。

15.5.2 使用引導式程序安裝 Identity Applications

以下程序介紹如何使用安裝精靈安裝 Identity Applications。

若要進行安裝準備工作，請檢閱第 15.5.1 節「Identity Applications 的安裝核對清單」(第 181 頁) 中列出的活動。另請參閱版本隨附的 《版本說明》。

附註：

- 安裝程式不會儲存您在完成精靈各視窗中的操作時輸入的值。如果按上一步返回前一個視窗，則必須重新輸入組態值。
- 安裝程式將建立 *novlua* 使用者帳戶，並為此使用者設定 Tomcat 中的許可權。例如，services.msc 程序檔會使用此使用者帳戶來執行 Tomcat。

若要使用引導式程序安裝：

1. 以管理使用者身分登入要安裝 Identity Applications 的電腦。
2. 停止 Tomcat。
3. (視情況而定) 如果您已取得 Identity Manager 安裝套件的 .iso 影像檔，請導覽至包含安裝檔案的目錄 (預設為 products\UserApplication\ 目錄)。
4. (視情況而定) 如果您已下載安裝檔案，請完成以下步驟：
   - **4a** 導覽至所下載影像的 win.zip 檔案。
   - **4b** 將該檔案的內容擷取到本地電腦上的某個目錄中。
5. 從包含安裝檔案的目錄中執行 IdmUserApp.exe 檔案。

6 使用以下參數完成引導式程序：

- **應用程式伺服器平台**

  代表用於執行 Identity Applications 的 Tomcat。必須已安裝 Tomcat。

- **安裝資料夾**

  代表安裝程式要在其中建立應用程式檔案的目錄路徑。

- **資料庫平台**

  代表使用者應用程式資料庫的平台。該資料庫軟體必須已安裝好。但您無需在安裝期間建立資料庫綱要。

  為方便起見，NetIQ 提供了 PostgreSQL。

- **資料庫主機和連接埠**

  代表代管使用者應用程式資料庫之伺服器的設定。

  附註：在叢集環境中，必須為叢集中的每個成員指定相同的資料庫設定。

  主機

  指定伺服器的名稱或 IP 位址。

  連接埠

  指定您希望伺服器在與使用者應用程式通訊時使用的連接埠。

- **資料庫使用者名稱與密碼**

  代表與執行使用者應用程式資料庫相關的設定。

  附註：

  - 如果您在安裝此 Identity Manager 版本的過程中安裝了 PostgreSQL，則安裝程序已經建立了資料庫和資料庫管理員。依預設，安裝的資料庫為 idmuserappdb，資料庫使用者為 idmadmin。指定您在安裝 PostgreSQL 時使用的相同值。
  - 在叢集環境中，必須為叢集中的每個成員指定相同的資料庫名稱、使用者名稱和密碼。

  資料庫名稱或 SID

  根據資料庫平台指定資料庫的名稱。依預設，資料庫名稱為 idmuserappdb。

  - 對於 PostgreSQL 或 SQL Server 資料庫，請指定名稱。
  - 對於 Oracle 資料庫，請指定您為資料庫例項建立的安全識別碼 (SID)。

  資料庫使用者名稱

  指定使用者應用程式用來存取和修改資料庫中資料的帳戶名稱。

  資料庫密碼

  提供所指定使用者名稱的密碼。

  資料庫驅動程式 JAR 檔案

  指定資料庫平台的 JAR 檔案。

  資料庫廠商會提供驅動程式 JAR 檔案，該檔案代表資料庫伺服器的簡易用戶端 JAR。例如，對於 PostgreSQL，可以指定預設位於 C:\NetIQ\idm\apps\Postgres 資料夾中的 postgresql-9.4-1212.jdbc42.jar。

  NetIQ 不支援協力廠商提供的驅動程式 JAR 檔案。

- **資料庫管理員**

選擇性

代表資料庫管理員的名稱和密碼。

此欄位會自動列出您為「資料庫使用者名稱和密碼」指定的使用者帳戶和密碼。若要使用該帳戶，請不要進行任何變更。

資料庫管理員

(選擇性) 指定可建立資料庫表、檢視和其他產出工件的資料庫管理員帳戶。

密碼

(選擇性) 指定資料庫管理員的密碼。

- 建立資料庫表格

指示是要在安裝過程中還是在安裝後設定新的或現有的資料庫。

立即建立表格

安裝程式將在安裝過程中建立資料庫表。

應用程式啟動時建立表格

安裝程式會發出在使用者應用程式首次啟動時建立表格的指示。

將 SQL 寫入檔案

產生一個 SQL 程序檔，資料庫管理員可以執行該程序檔來建立資料庫。如果您選擇此選項，則還必須為**綱要檔案**指定名稱。該項設定在 **SQL 輸出檔案**組態中指定。

如果您沒有在環境中建立或修改某個資料庫的許可權，則可以選取此選項。如需使用該檔案產生表格的詳細資訊，請參閱第 15.7.2 節「手動建立資料庫綱要」(第 195 頁)。

- 新資料庫或現有資料庫

指定您要使用現有的空資料庫還是在現有資料庫中建立新表。請注意以下事項：

- 新的資料庫

  如果使用新的資料庫，請按一下**新資料庫**。選取此選項之前，請確認資料庫存在。

- 現有資料庫

  如果資料庫是現有的且具有來自先前安裝的使用者應用程式表，請選取**現有資料庫**。

  如果現有資料庫在 Oracle 平台上執行，則您必須在更新綱要之前準備好 Oracle。

選取資料庫類型後，需要指定應在何時建立資料庫表。「建立資料庫表格」螢幕可讓您選擇是要在安裝時還是在應用程式啟動時建立表格。此外，您也可以在安裝時建立綱要檔案，資料庫管理員以後會使用該檔案來建立表格。

如果要產生綱要檔案，請選取「將 SQL 寫入檔案」按鈕，並在「綱要輸出檔案」欄位中提供檔案名稱。

- 測試資料庫連接

指定您是希望安裝程式在連接到資料庫後直接建立表格，還是建立 .sql 檔案。

當您按**下一步**或按 **Enter** 鍵後，安裝程式會嘗試建立連接。

附註：如果資料庫連接失敗，您可以繼續安裝。但在安裝後，您必須手動建立表格並連接到資料庫。如需詳細資訊，請參閱「手動建立用於產生資料庫綱要的 SQL 檔案」(第 195 頁)。

- **Java 安裝**

代表用於啟動安裝程式的 JRE 檔案所在的路徑。例如，C:\NetIQ\idm\jre。

- ***應用程式伺服器*組態**

代表 Tomcat 的安裝檔案路徑。例如，C:\NetIQ\idm\jre。安裝程序會將一些檔案新增至此資料夾中。

- **IDM 組態**

  代表 URL 中所用 Identity Applications 網路位置的設定以及工作流程引擎的設定。

  應用程式網路位置

  指定代表 Tomcat 組態的名稱、應用程式 WAR 檔案以及 URL 網路位置中的名稱。

  安裝程序檔將建立伺服器組態，然後依照您在安裝 Tomcat 時建立的名稱為該組態命名。例如 IDMProv。

  重要：NetIQ 建議您記下指定的應用程式網路位置。當您從瀏覽器啟動 Identity Applications 時，會在 URL 中用到此應用程式名稱。

- **選取稽核記錄類型**

  指出要啟用 CEF 還是 Sentinel Log Management for IGA。指定是或否。

- **稽核記錄**

  僅當您對「選取稽核記錄類型」指定了「是」時才適用。

  指出要啟用的記錄類型。

  如需設定記錄的詳細資訊，請參閱 *《User Application Administration Guide》*（使用者應用程式管理指南）。

  Sentinel Log Management for IGA

  透過適用於使用者應用程式的 Novell 或 NetIQ 用戶端啟用記錄。

  附註：如果您選擇此選項，則還必須指定用戶端伺服器的主機名稱或 IP 位址，以及記錄快取的路徑。

  CEF

  讓使用者應用程式透過 CEF 來記錄事件。

  附註：如果您選擇此選項，則還必須指定 syslog 伺服器的主機名稱或 IP 位址，以及 syslog 連接埠。

- **安全性 - 萬能金鑰**

  指出是否要輸入現有的萬能金鑰。使用者應用程式使用萬能金鑰來存取加密的資料。指定是或否。

  在以下情況下，您可能需要輸入萬能金鑰：

  - 在叢集中安裝了第一個 Identity Applications 例項之後。叢集中的每個使用者應用程式例項都必須使用相同的萬能金鑰。如需詳細資訊，請參閱「為叢集中的每個使用者應用程式使用相同的萬能金鑰」（第 180 頁）。
  - 您要將安裝從預備系統移轉至線上系統，並希望保留對預備系統所用資料庫的存取能力。
  - 您要還原使用者應用程式，並想要存取以前的使用者應用程式版本所儲存的加密資料。

  是

  指定您要輸入現有的萬能金鑰。

否

指定您要讓安裝程式建立該金鑰。

依預設，安裝程序會將加密萬能金鑰寫入安裝目錄中的 master-key.txt 檔案。

- **輸入萬能金鑰**

  僅當您對「安全性 - 萬能金鑰」指定了「是」時才適用。

  指定您要使用的萬能金鑰。您可以從 master-key.txt 檔案中複製萬能金鑰。

- **應用程式伺服器連接**

  代表使用者連接 Tomcat 上的 Identity Applications 時所需的 URL 設定。例如 https:myserver.mycompany.com:8080。

附註：如果 OSP 在其他 Tomcat 應用程式伺服器例項上執行，則還必須選取**連接至外部驗證伺服器**，並指定 OSP 伺服器的值。

通訊協定

指定您要使用 *http* 還是 *https*。若要使用安全通訊端層 (SSL) 進行通訊，請指定 https。

主機名稱

指定代管 OSP 之伺服器的 DNS 名稱或 IP 位址。請不要使用 localhost。

連接埠

指定您希望伺服器在與用戶端電腦通訊時使用的連接埠。

連接至外部驗證伺服器

指定是否要用不同的 Tomcat 例項來代管驗證伺服器 (OSP)。驗證伺服器包含可登入 SSPR 的使用者清單。

如果選取此設定，則還要指定驗證伺服器的**通訊協定**、**主機名稱**和**連接埠**值。

- **驗證伺服器詳細資料**

  指定您希望 Identity Applications 在連接到驗證伺服器時使用的密碼。該密碼又稱為用戶端密碼。安裝程序會建立此密碼。

7 在「設定更新」視窗中進行 Identity Applications 的設定。

7a 瀏覽 **Identity Vault DN**。

7b 按一下**確定**。

附註：

- 確認使用者應用程式及角色與資源服務驅動程式已建立且部署到 Identity Vault。如需詳細資訊，請參閱「Identity Applications 的安裝考量」(第 167 頁)。
- 如果按一下**取消**，您將回到「應用程式伺服器連接」視窗。
- 安裝使用者應用程式後，您可以修改 configureupdate.bat 檔案中的大部分設定。如需指定設定值的詳細資訊，請參閱第 15.8 章「完成 Identity Applications 的設定」(第 204 頁)。

---

8 (視情況而定) 在使用圖形使用者介面進行安裝時，若要立即設定 Identity Applications，請在「設定 IDM」視窗中完成以下步驟：

8a 按一下是，然後按下一步。

8b 在「Roles Based Provisioning Module 組態」中，按一下顯示進階選項。

8c 視需要修改設定。

附註：

- 如需指定值的詳細資訊，請參閱第 15.8 章「完成 Identity Applications 的設定」(第 204 頁)。
- 在線上環境中，所有管理員指定均受授權限制。NetIQ 會在稽核資料庫中收集監控資料，以確保線上環境遵循法規。此外，NetIQ 還建議只對一位使用者授予安全性管理員許可權。

8d 按一下「確定」。

9 按下一步。

10 在「安裝前摘要」視窗中按一下安裝。

11 (選擇性) 檢閱安裝記錄檔案。若要瞭解基本安裝的結果，請參閱 C:\NetIQ\idm\apps\UserApplication\logs\ 目錄中的 user_application_install_log.log 檔案。

如需 Identity Applications 組態的資訊，請參閱 C:\NetIQ\idm\apps\UserApplication 目錄中的 NetIQ-Custom-Install.log 檔案。

12 (選擇性) 如果您使用的是外部密碼管理 WAR，請手動將該 WAR 複製到安裝目錄，以及執行外部密碼 WAR 功能的遠端應用程式伺服器部署目錄中。

13 依照第 15.7 章「完成 Identity Applications 的安裝」(第 194 頁) 所述繼續執行安裝後任務。

15.5.3 安裝後步驟

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

- 「為叢集設定使用者應用程式驅動程式」(第 187 頁)
- 「將 preferIPv4Stack 內容傳遞至 JVM」(第 187 頁)
- 「檢查伺服器的狀態」(第 187 頁)
- 「監控狀態統計資料」(第 188 頁)
- 「建立複合索引」(第 188 頁)
- 「設定 Identity Application 以拒絕用戶端發起的 SSL 重新交涉」(第 189 頁)

如果您使用了 Tomcat 的便捷安裝程式，Identity Manager 的安裝程式將為您設定 Tomcat。如果您安裝了自己的 Tomcat 程式，請注意以下問題：

- 您可以修改 Tomcat 服務，以提高其執行效率。如需詳細資訊，請參閱 *So You Want High Performance* (如何提高效能)。
- 您可能需要新增對記錄事件的支援。如需詳細資訊，請參閱第 13.1.4 節「使用 Apache Log4j 服務記錄登入」(第 150 頁)。

為叢集設定使用者應用程式驅動程式

如需更多資訊，請參閱第 15.6.2 節「為叢集設定使用者應用程式驅動程式」(第 193 頁)。

將 preferIPv4Stack 內容傳遞至 JVM

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

如果不使用此選項，可能會發生以下錯誤：

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

您還可能會看到此錯誤：

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

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

檢查伺服器的狀態

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

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

監控狀態統計資料

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

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

  例如，

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

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

  例如，

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

  若要存取 JVM 中線串的堆疊追蹤，請將堆疊參數設定為 **True**。

  例如，

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

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

例如，

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

- **快取資訊**：讀取使用者應用程式的快取資訊。
  例如，

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

- **叢集資訊**：讀取與叢集相關的資訊。
  例如，

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

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

建立複合索引

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

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

以下指令可協助您使用 ndsindex 公用程式來建立複合索引：

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

例如，若要依職位對使用者排序，請執行以下指令：

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

您也可以使用轉換輸出公用程式建立複合索引。

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

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

```
dn: cn=osg-nw5-7, o=Novell

changetype: modify

add: indexDefinition

indexDefinition: 0$sntitleindex$0$0$0$1$Title$surname
```

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

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

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

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

15.5.4 停用阻止 HTML 框架設定以將 Identity Manager 與 SSPR 整合

本節介紹為將 Identity Manager 整合到不是由 Identity Manager 4.5 部署的現有 SSPR 4.2 環境所需使用的組態。SSPR 提供了一個可設定的選項**阻止 HTML 框架**，使用該選項後，對於包含 iframe html 原始程式碼的任何應用程式，使用者均可在 Inline 框架中檢視 SSPR。如果您選取此選項，SSPR 將不會包含在應用程式的指定 iFrame 中。若要為 Identity Manager 停用此選項，請執行以下步驟：

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. 以 SSPR 管理員身分登入。
3. 按一下頁面頂部的**組態編輯器**，然後指定 OSP 組態密碼。
4. 按一下**設定 > 安全性 > 永遠顯示進階設定**，然後執行以下動作：
   - **4a** 瀏覽至**阻止 HTML 框架**，取消選取**已啟用**，然後按一下**儲存**以儲存設定。
   - **4b** 在確認視窗中，按一下**確定**。

15.5.5 驗證使用者內容

若要讓使用者能夠使用 Identity Applications，必須確定已將具有必要權限的使用者內容新增至包含您所有系統使用者的容器中。您可以使用 iManager 驗證這些內容。在 iManager 中執行下列步驟來驗證這些設定：

1. 使用 Identity Vault IP 位址做為樹狀結構，以管理員身分登入 iManager。
2. 在**樹狀結構**面板中，選取設定了 Identity Applications 的樹狀結構。
3. 針對包含所有系統使用者的容器按一下**指定的權限**。
4. 驗證下列內容是否具有清單中的必要權限：
   - 描述
   - 網際網路電子郵件地址
   - 登入程序檔
   - 列印工作組態
   - 電話號碼
   - 職位
   - 直屬下屬
   - 管理者

- 相片
- srvprvQueryList
- srvprvUserPrefs

如果缺少任何內容，請按一下新增內容。

4a 從清單中選取所需的內容，然後按一下完成。

4b 選取內容的必要權限，然後按一下完成。

圖 15-1 將內容新增至使用者容器中

15.5.6 啟動 Identity Applications

本節提供關於啟動 Identity Applications 以及首次登入應用程式伺服器的指示。若為叢集環境，請在主要節點上開始執行該程序。Identity Applications 應該已安裝好，可供部署。如需安裝後任務的詳細資訊，請參閱第 15.7 章 「完成 Identity Applications 的安裝」(第 194 頁)。

可以使用 services.msc 啟動程序檔來啟動 Tomcat 服務。此檔案也可用於停止和重新啟動 Tomcat 服務。

完成這些步驟之後，如果瀏覽器未顯示使用者應用程式頁面，請檢查終端機主控台上是否有錯誤訊息，並參閱第 37 章 「疑難排解」(第 369 頁)。

若要啟動 Identity Applications：

1. 啟動 Identity Applications 的資料庫。如需詳細資訊，請參閱資料庫文件。
2. 若要讓使用者應用程式執行報告，請將 Djava.awt.headless=true 旗標新增至 Tomcat 的啟動程序檔中。例如：

   JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8 -Dsun.jnu.encoding=UTF-8 -server -Xms1024m -Xmx1024m -XX:MaxPermSize=512m

   附註：如果您執行的是 X11 Windows 系統，則不需要執行此步驟。

3. 啟動 Identity Applications 安裝到的 Tomcat。

附註：在叢集中，只能在主要節點上啟動。

4 在指令行中，將工作目錄切換為安裝目錄。

5 執行啟動程序檔。

6 若要實現與使用者應用程式驅動程式通訊的功能，請完成以下步驟：

   6a 登入 iManager。

   6b 在左側導覽框架中的**角色與任務 > Identity Manager** 下，按一下 **Identity Manager 綜覽**。

   6c 在內容檢視窗中，指定包含使用者應用程式驅動程式的驅動程式集，然後按一下**搜尋**。

   6d 在顯示驅動程式集及其關聯驅動程式的圖形中，按一下使用者應用程式驅動程式對應的紅白圖示。

   6e 按一下**啟動驅動程式**。

   驅動程式啟動後會嘗試與使用者應用程式「交換信號」。如果應用程式伺服器未在執行，或者 WAR 尚未成功部署，驅動程式會傳回錯誤。否則，驅動程式狀態會變更為陰陽符號，表明驅動程式現已啟動。

7 若要啟動角色與資源服務驅動程式，請重複步驟 6 中的程序。

8 若要啟動並登入使用者應用程式，請在網頁瀏覽器中輸入以下 URL：

   `http://hostname:port/ApplicationName`

   hostname

   代表應用程式伺服器的名稱 (Tomcat)。例如 myserver.domain.com

   port

   代表應用程式伺服器的連接埠號。例如 8180。

   ApplicationName

   代表您在安裝應用程式期間提供應用程式伺服器組態資訊時指定的名稱。例如 IDMProv。

9 在使用者應用程式抵達頁面的右上角，按一下**登入**。

10 (視情況而定) 若要在叢集群組中啟用使用者應用程式，請完成以下步驟：

   10a 按一下**管理**。

   10b 在應用程式組態入口網站中，按一下**快取**。

   10c 在「快取管理」視窗中，對**叢集已開啟**選取 **True**。

   10d 按一下「**儲存**」。

   10e 然後重新啟動伺服器。

   10f (視情況而定) 若要使用本地設定，請對叢集中的每個伺服器重複此程序。

15.6 建立和部署 Identity Applications 的驅動程式

RBPM 的安裝程序會新增用於建立 Identity Applications 驅動程式的檔案。驅動程式組態支援允許您執行下列工作：

- 將一個使用者應用程式驅動程式與一個角色與資源服務驅動程式相關聯。
- 將一個使用者應用程式與一個使用者應用程式驅動程式相關聯。

在嘗試設定驅動程式之前，請確定 Designer 的「套件目錄」中包含所有必要的套件。在建立新的 Identity Manager 專案時，使用者介面會自動提示您將幾個套件輸入至新的專案中。

- 第 15.6.1 節「建立「使用者應用程式」驅動程式」(第 192 頁)
- 第 15.6.2 節「為叢集設定使用者應用程式驅動程式」(第 193 頁)
- 第 15.6.3 節「建立角色與資源服務驅動程式」(第 193 頁)
- 第 15.6.4 節「部署使用者應用程式的驅動程式」(第 194 頁)

15.6.1 建立「使用者應用程式」驅動程式

使用者應用程式驅動程式不僅是一個執行時期元件，也是目錄物件 (構成使用者應用程式的執行時期產出工件) 的儲存包裝程式。它負責儲存應用程式特定的環境組態資料。該驅動程式還會在 Identity Vault 中的重要資料值變更時通知目錄抽象層。收到此通知後，目錄抽象層會更新其快取。

1. 在 Designer 中開啟您的專案。
2. 在**模型產生器 > 佈建**檢視窗上的調色盤中，選取**使用者應用程式**。
3. 將「**使用者應用程式**」的圖示拖曳至「**模型產生器**」檢視窗中。
4. 在驅動程式組態精靈中，選取**使用者應用程式基礎**，然後按**下一步**。
5. 收到安裝多個其他套件的提示時，按一下**確定**。
6. (選擇性) 指定驅動程式的名稱。

   按一下「**下一步**」。
7. 在連接參數視窗中，指定使用者應用程式管理員的 ID 和密碼。
8. 指定使用者應用程式伺服器的主機和連接埠。
9. 指定使用者應用程式伺服器的應用程式網路位置。
10. (選擇性) 若要允許佈建管理員以其他人 (佈建管理員已指定為其代理) 的名義啟動工作流程，請對**允許啟始者覆寫功能**選取**是**。
11. 在**確認安裝任務**視窗中，按一下**完成**。

15.6.2 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 iManager 例項。
2. 在導覽框架中，選取 **Identity Manager**。
3. 選取 **Identity Manager 綜覽**。
4. 使用搜尋網頁顯示「Identity Manager 綜覽」，以瞭解包含使用者應用程式驅動程式的驅動程式集。
5. 按一下驅動程式圖示右上角的圓形狀態指示器：
6. 選取**編輯內容**。
7. 對於**驅動程式參數**，請將**主機**變更為發送器的主機名稱或 IP 位址。
8. 按一下**確定**。

15.6.3 建立角色與資源服務驅動程式

使用者應用程式使用角色與資源服務驅動程式來管理資源的後端處理。例如，它會管理所有資源申請、啟動資源申請的工作流程以及啟始資源申請的佈建程序。

1 在 Designer 中開啟您的專案。
2 在模型產生器 > 佈建檢視窗上的調色盤中，選取角色服務。
3 將「角色服務」的圖示拖曳至「模型產生器」檢視窗中。
4 在驅動程式組態精靈中，選取角色與資源服務基礎，然後按下一步。
5 (視情況而定) 如果這是 Designer 中安裝的第一個驅動程式，請按一下確定以安裝 **Common Settings Advanced Edition** 套件。
   - **5a** 指定使用者應用程式伺服器的 URL。
   - **5b** 指定使用者應用程式管理員的 eDirectory DN。
   - **5c** 指定使用者應用程式佈建服務帳戶的 LDAP DN。該帳戶可以與使用者應用程式管理員的帳戶相同，也可以不同。

     如果角色或資源佈建申請是由此服務帳戶發起，則系統會略過與此角色或資源關聯的所有核准或佈建工作流程。
6 (選擇性) 指定驅動程式的名稱。
7 按一下「下一步」。
8 在「使用者應用程式 / 工作流程連接」視窗中，指定使用者群組基礎容器 DN，以及您剛才建立的使用者應用程式驅動程式。

   由於該驅動程式尚未部署，瀏覽功能將不會顯示您剛才設定的使用者應用程式驅動程式。您可能需要輸入該驅動程式的 DN。
9 指定使用者應用程式的 URL。
10 指定使用者應用程式管理員帳戶的 LDAP DN

   使用者應用程式管理員帳戶將會向使用者應用程式進行驗證，以啟動核准工作流程。如需詳細資訊，請參閱第 15.2.2 節「向 Identity Vault 管理員和使用者應用程式管理員帳戶指定權限」(第 174 頁)。
11 指定使用者應用程式管理員帳戶的密碼。
12 按一下「下一步」。
13 在「確認安裝任務」視窗中，按一下完成。

15.6.4 部署使用者應用程式的驅動程式

使用者應用程式和角色與資源服務驅動程式只有在部署之後才能使用。

附註：複製 eDirectory 環境時，必須確保複製本包含 Identity Manager 的 NCP 伺服器物件。Identity Manager 只能做為伺服器的本地複製本。因此，如果次要伺服器不包含伺服器物件，角色與資源服務驅動程式可能將無法正常啟動。

若要部署驅動程式：

1 在 Designer 中開啟您的專案。

2 在模型產生器或大綱檢視窗中，選取「驅動程式集」。

3 按一下即時 > 部署。

15.7 完成 Identity Applications 的安裝

本節提供您在安裝 Identity Applications 及其架構後可能需要執行之活動的指示：

- 第 15.7.1 節「在叢集環境中檢查伺服器的狀態」(第 194 頁)
- 第 15.7.2 節「手動建立資料庫綱要」(第 195 頁)
- 第 15.7.3 節「手動將 Identity Applications 和 Identity Reporting 證書輸入到 Identity Vault 中」(第 196 頁)
- 第 15.7.4 節「記錄萬能金鑰」(第 196 頁)
- 第 15.7.5 節「設定 Identity Applications 的 Identity Vault」(第 196 頁)
- 第 15.7.6 節「變更使用者應用程式的預設網路位置名稱」(第 197 頁)
- 第 15.7.7 節「重新設定 Identity Applications 的 WAR 檔案」(第 199 頁)
- 第 15.7.8 節「設定忘記密碼管理功能」(第 199 頁)

15.7.1 在叢集環境中檢查伺服器的狀態

如需詳細資訊，請參閱「檢查伺服器的狀態」(第 187 頁)

15.7.2 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 195 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 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。

7 重新啟動 Tomcat。

手動建立用於產生資料庫綱要的 SQL 檔案

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

1 停止 Tomcat。

2 登入代管 Identity Applications 資料庫的伺服器。

3 刪除現有的資料庫。

4 建立一個與您在步驟 3 中刪除的資料庫同名的新資料庫。

5 在文字編輯器中，開啟 NetIQ-Custom-Install.log 檔案 (預設位於 Identity Applications 的安裝根目錄中)。例如：

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

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

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

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

8 在終端機中，貼上您複製的指令字串。

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

---

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

10 執行指令。

11 (視情況而定) 如果安裝程序產生了一個 SQL 檔案，而不是在資料庫中填入資料，請將該檔案提供給資料庫管理員，讓其將該檔案輸入至資料庫伺服器。如需詳細資訊，請參閱 「使用 SQL 檔案產生資料庫綱要」(第 195 頁)。

12 在資料庫管理員輸入該 SQL 檔案後，啟動 Tomcat。

15.7.3 手動將 Identity Applications 和 Identity Reporting 證書輸入到 Identity Vault 中

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

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

  ```
  keytool -importkeystore -alias <User Application certificate alias> -srckeystore  <backup
  cacert> -srcstorepass changeit -destkeystore C:\NetIQ\eDirectory\jre\lib\security\cacerts
  ```

- 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。

15.7.4 記錄萬能金鑰

NetIQ 建議您在安裝後，立即複製加密的萬能金鑰，並將其記錄在安全的位置。如果此安裝是在叢集的第一個成員上進行，當您在叢集的其他成員上安裝 Identity Applications 時，請使用這個加密的萬能金鑰。

警告：請永遠保存一份加密萬能金鑰。如果遺失了萬能金鑰，您需要使用加密的萬能金鑰來重新取得加密資料的存取權。例如，在設備發生故障後，您可能需要用到該金鑰。

15.7.5 設定 Identity Applications 的 Identity Vault

Identity Applications 必須能夠與 Identity Vault 中的物件互動。

為了提高 Identity Applications 的效能，eDirectory 管理員應為 manager、ismanager 和 srvprvUUID 屬性建立值索引。如果沒有為這些屬性建立索引值，Identity Applications 使用者可能會遭遇效能不佳問題，在叢集環境中尤為突出。

透過在 RBPM 組態公用程式中選取「進階」>「建立 eDirectory 索引」，即可在安裝期間自動建立這些值索引。如需使用 Index Manager 建立值索引的詳細資訊，請參閱《*NetIQ eDirectory Administration Guide*》(NetIQ eDirectory 管理指南)。

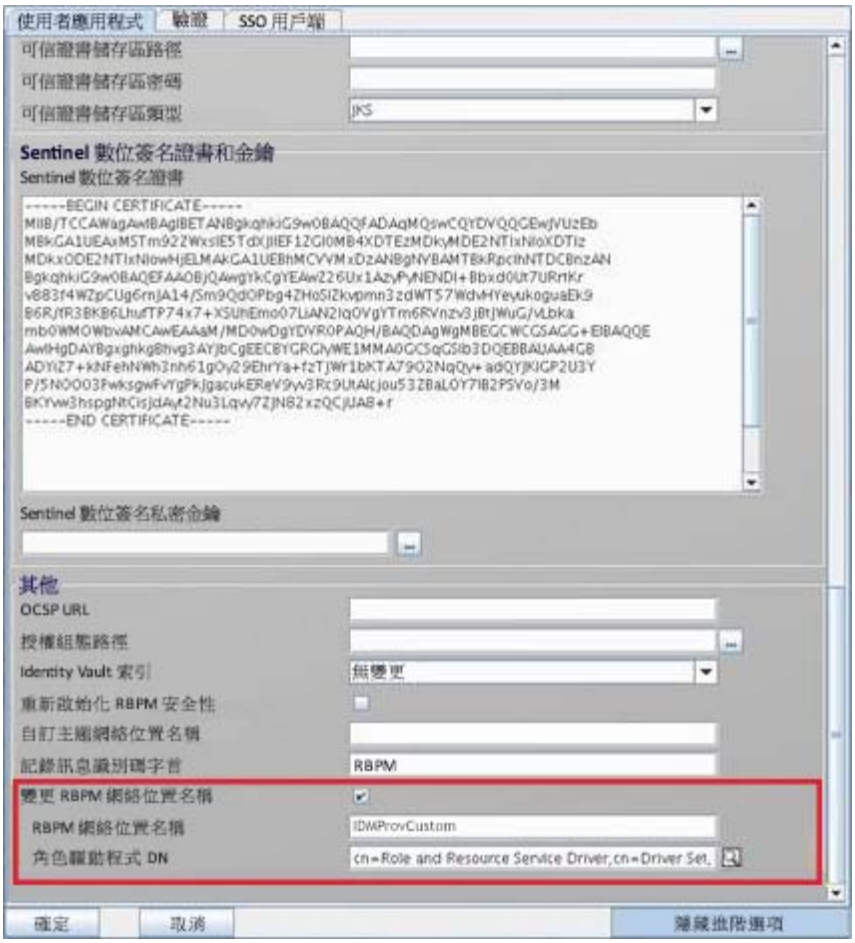
15.7.6 變更使用者應用程式的預設網路位置名稱

如果不使用預設網路位置名稱，您可以依據組織的要求建立新網路位置。您可以透過執行下列動作來變更網路位置名稱：

1. 使用 services.msc 檔案停止 Tomcat 服務。
2. 導覽至 C:\NetIQ\idm\apps\UserApplication 中的使用者應用程式目錄。
3. 在圖形使用者介面模式下啟動 configupdate 公用程式。

   確定 configupdate.bat.properties 檔案中的 use_console 選項設定為 false。
4. 在**使用者應用程式**索引標籤中按一下**顯示進階選項**，然後執行以下步驟：
   - **4a** 選取**變更 RBPM 網路位置名稱**。
   - **4b** 在 **RBPM 網路位置名稱**中指定自訂網路位置名稱。例如 IDMProvCustom。
   - **4c** 瀏覽至角色驅動程式 DN 並加以選取。例如 cn=Role and Resource Service Driver,cn=Driver Set,o=system。

4d 按一下「確定」。



5 驗證 war 檔案是否已重新命名。

- 導覽至 Tomcat webapps 資料夾，檢查 IDMProvCustom.war 項目是否已更新。
- 導覽至 \TOMCAT_INSTALLED_HOME\conf 中的 ism-configuration properties 檔案，檢查 portal.context 項目是否指定了新的網路位置名稱。

6 使用 C:\NetIQ\idm\apps\UserApplication 中的 update-context.bat 檔案將資料庫更新為採用新網路位置名稱。

執行以下指令以執行 update-context.bat 檔案。

```
ua:C:\NetIQ\idm\apps\UserApplication # vi update-context.bat
```

螢幕上應該會顯示以下項目：

```
# copy and paste or execute this script before changing context name

# Substitute your new context where indicated

#
```

```
C:\NetIQ\idm\jre\bin\java -Xms256m -Xmx256m  -Dwar.context.name=[New Context Here] -
Ddriver.dn=[UA Driver DN] -jar C:\NetIQ\idm\apps\UserApplication\liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase  --driver=org.postgresql.Driver  --
classpath=
C:\NetIQ\idm\apps\postgres\postgresql-9.4.1212.jdbc42.jar:
C:\NetIQ\idm\apps\tomcat\webapps\IDMProv.war --changeLogFile=UpdateProducerId.xml   --
url="jdbc:postgresql://localhost:5432/idmuserappdb?compatible=true" --contexts="prov,updatedb"
--logLevel=debug --username=******** --password=******** update
```

例如，如果您使用的是 PostgreSQL 資料庫，請執行以下程序檔：

```
C:\NetIQ\idm\apps\jre\bin\java -Xms256m -Xmx256m  -Dwar.context.name=IDMProvCustom  -
Ddriver.dn= cn=Role and Resource Service Driver,cn=driverset1,o=system -jar
C:\NetIQ\idm\apps\UserApplication\liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase  --driver=org.postgresql.Driver  --
classpath=
C:\NetIQ\idm\apps\postgres\postgresql-9.4.1212.jdbc42.jar:
C:\NetIQ\idm\apps\tomcat\webapps\IDMProv.war --changeLogFile=UpdateProducerId.xml   --
url="jdbc:postgresql://<Database Server:5432/idmuserappdb?compatible=true" --
contexts="prov,updatedb" --logLevel=debug -–username=dbadmin --password=******** update
```

其中

-Dwar.context.name=IDMProvCustom 指定新網路位置。

-Ddriver.dn ="cn=User Application Driver,cn=driverset1,o=system" 指定使用者應用程式驅動程式 DN。

--username=dbadmin 指定可建立資料庫表、檢視和其他產出工件的資料庫管理員使用者名稱。

重要：對於其他受支援的資料庫，請不要變更程序檔中的資料庫驅動程式詳細資料。

---

7 驗證資料庫表是否使用了新的網路位置名稱。

表名稱	要檢查的欄
PORTALPRODUCERS	producerid
PORTALPRODUCERREGISTRY	producerid
PORTALREGISTRY	producerid
PORTALPORTLETSETTINGS	producerid
PORTALPORTLETHANDLES	producerid
PROFILEGROUPPREFERENCES	elementid

例如，執行以下 SQL 指令可在 PORTALPRODUCERS 表中驗證新網路位置名稱：

```
Select * from PORTALPRODUCERS;
```

該指令應該只傳回新網路位置名稱。

8 使用 services.msc 檔案啟動 Tomcat 服務。

15.7.7 重新設定 Identity Applications 的 WAR 檔案

若要更新 Identity Applications 的 WAR 檔案，請執行 RBPM 組態公用程式。

1 透過執行 configupdate.bat 來執行安裝目錄中的公用程式。

   如需公用程式參數的詳細資訊，請參閱第 15.8 章 「完成 Identity Applications 的設定」(第 204 頁)。

2 將新的 WAR 檔案部署到您的應用程式伺服器上。

   對於 Tomcat 單一伺服器，這些變更將套用至所部署的 WAR。

15.7.8 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 199 頁)
- 「使用舊提供程式進行忘記密碼管理」(第 201 頁)
- 「使用外部系統進行忘記密碼管理」(第 202 頁)
- 「針對分散式環境或叢集環境更新儀表板中的 SSPR 連結」(第 203 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 199 頁)
- 「為 Identity Manager 設定 Self Service Password Reset」(第 200 頁)
- 「鎖定 SSPR 組態」(第 200 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，請參閱第 15.8.1 節「執行 Identity Applications 組態公用程式」(第 204 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。如需組態密碼的詳細資訊，請參閱第 14.2 章 「為 Identity Manager 安裝密碼管理功能」(第 157 頁)。

1 使用您在安裝期間指定的組態密碼登入 SSPR。

2 在「設定」頁面中，修改密碼規則和處理安全回應問題的設定。如需設定 SSPR 設定預設值的詳細資訊，請參閱《*NetIQ Self Service Password Reset Administration Guide*》(NetIQ Self Service Password Reset 管理指南) 中的「Configuring Self Service Password Reset」(設定 Self Service Password Reset)。

3 鎖定 SSPR 組態檔案 (SSPRConfiguration.xml)。如需鎖定組態檔案的詳細資訊，請參閱「鎖定 SSPR 組態」(第 200 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。

使用舊提供程式進行忘記密碼管理

您也可以不使用 SSPR，而是使用 Identity Manager 中的舊提供程式實現忘記密碼管理功能。如果您選擇使用舊提供程式，則不需要安裝 SSPR。但是，您需要為使用者重新指定許可權，使其能夠存取密碼管理的共享頁面。本節提供執行以下活動的步驟：

- 「設定舊提供程式以進行忘記密碼管理」(第 201 頁)
- 「重新指定對密碼管理頁面的許可權」(第 202 頁)

如需舊提供程式的詳細資訊，請參閱第 4.4.2 節「瞭解舊密碼管理提供程式」(第 32 頁)。如需共享頁面和許可權的詳細資訊，請參閱《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》(NetIQ Identity Manager - Identity Applications 管理員指南) 中的「Page Administration」(頁面管理)。

設定舊提供程式以進行忘記密碼管理

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，請參閱第 15.8.1 節「執行 Identity Applications 組態公用程式」(第 204 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**使用者應用程式 (舊版)**。

5 對於**忘記密碼**，請指定**內部**。

6 導覽至 **SSO 用戶端 > Self Service Password Reset**。

7 **OSP 重新導向 URL** 設定應該為空白。

8 儲存變更，然後關閉公用程式。

重新指定對密碼管理頁面的許可權

在安裝期間，Identity Applications 的設定預設為 SSPR。必須為允許存取密碼管理共用頁面的使用者、群組或容器指定或重新指定許可權。為使用者指定對某個容器頁面或共享頁面的檢視許可權後，使用者便可以存取該頁面，並在可用頁面清單中看到該頁面。

1 確保 Identity Manager 使用的是舊提供程式。如需詳細資訊，請參閱「設定舊提供程式以進行忘記密碼管理」(第 201 頁)。

2 以應用程式管理員身分登入使用者應用程式。例如，以 uaadmin 身分登入。

3 導覽至**管理 > 網頁管理**。

4 在共享頁面面板中，導覽至密碼管理。
5 選取您要指定對其的許可權的頁面。例如「變更密碼」或「密碼處理安全回應」。
6 在右側面板中，按一下指定權限。
7 在檢視中，選取要為其指定對該頁面權限的使用者、群組或容器。
8 (選擇性) 若要確保只有應用程式管理員才能存取指定的頁面，請選取檢視權限設定為僅限於管理者身分。
9 按一下「儲存」。
10 對您要設定的每個頁面執行步驟 5 至步驟 9。
11 選取首頁圖示以返回儀表板。
12 導覽至應用程式，然後選取 ⚙。
13 在管理應用程式頁面中，以 UserApp PwdMgt 的連結取代指向 SSPR 的連結。

   如需詳細資訊，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 203 頁) 和 *Identity Applications 說明*。
14 登出系統，然後重新啟動 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 202 頁)
- 「測試外部忘記密碼 組態」(第 203 頁)
- 「設定應用程式伺服器之間的 SSL 通訊」(第 203 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此值，現在想要修改設定，則可以使用 RBPM 組態公用程式，或者以管理員身分在使用者應用程式中進行變更。

1 (視情況而定) 若要在 RBPM 組態公用程式中修改設定，請完成以下步驟：
   1a 登入安裝了 Identity Applications 的伺服器。
   1b 執行 RBPM 組態公用程式。如需詳細資訊，請參閱第 15.8.1 節「執行 Identity Applications 組態公用程式」(第 204 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 203 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。

15.8 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.bat) 的檔案位於 Identity Applications 的某個安裝子目錄 (C:\NetIQ\idm\apps\UserApplication) 中。

附註：在叢集中，所有叢集成員的組態設定都必須相同。

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。

- 第 15.8.1 節「執行 Identity Applications 組態公用程式」(第 204 頁)
- 第 15.8.2 節「使用者應用程式參數」(第 204 頁)
- 第 15.8.3 節「Reporting 參數」(第 214 頁)
- 第 15.8.4 節「驗證參數」(第 215 頁)
- 第 15.8.5 節「SSO 用戶端參數」(第 218 頁)
- 第 15.8.6 節「CEF 稽核參數」(第 222 頁)

15.8.1 執行 Identity Applications 組態公用程式

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

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

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

附註：您可能需要花幾分鐘時間等待公用程式啟動。

15.8.2 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 205 頁)
- 「Identity Vault DN」(第 206 頁)
- 「Identity Vault 使用者身分」(第 208 頁)
- 「Identity Vault 使用者群組」(第 209 頁)
- 「Identity Vault 證書」(第 209 頁)
- 「電子郵件伺服器組態」(第 210 頁)

- 「可信金鑰儲存區」(第 211 頁)
- 「NetIQ Sentinel 數位簽名證書與金鑰」(第 212 頁)
- 「其他」(第 212 頁)
- 「容器物件」(第 213 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.bat 檔案變更此設定。
- 此容器必須包含您在安裝使用者應用程式驅動程式時指定的使用者應用程式管理員。否則，指定的帳戶將無法執行工作流程。

群組容器 DN

必需

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

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

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

使用者應用程式驅動程式

必需

指定使用者應用程式驅動程式的可辨識名稱。

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

使用者應用程式管理員

必需

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

- 如果您已啟動代管使用者應用程式的 Tomcat，則無法使用 configupdate.bat 檔案變更此設定。
- 若要在部署使用者應用程式後變更此指定，請在使用者應用程式的管理 > 安全性頁面中進行變更。

- 此使用者帳戶有權使用使用者應用程式的管理索引標籤來管理入口網站。
- 如果使用者應用程式管理員參與 iManager、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.bat 檔案變更此設定。
- 此容器必須包含您在安裝使用者應用程式驅動程式時指定的使用者應用程式管理員。否則，指定的帳戶將無法執行工作流程。

使用者搜尋範圍

指定 Identity Vault 使用者在搜尋容器時可以探查的範圍深度。

使用者物件類別

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

登入屬性

指定代表使用者登入名稱的 LDAP 屬性。例如，cn。

命名屬性

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

使用者成員資格屬性

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

Identity Vault 使用者群組

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

僅當您選取了顯示進階選項時，公用程式才會顯示這些設定。

群組容器 DN

必需

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

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

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

群組容器範圍

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

群組物件類別

指定 LDAP 群組的物件類別。通常，該類別為 groupofNames。

群組成員資格屬性

(選擇性) 指定使用者的群組成員資格。請勿在此名稱中使用空格。

使用動態群組

指定是否要使用動態群組。

您還必須指定動態群組物件類別的值。

動態群組物件類別

僅當您選取了使用動態群組時才適用。

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

Identity Vault 證書

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

金鑰儲存區路徑

必需

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

- 在環境中，您必須指定 RBPM 的安裝目錄。預設值會設定為正確的位置。
- Identity Applications 的安裝程式將會修改金鑰儲存區檔案。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。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「Enabling Support for Digital Signatures」(啟用數位簽名支援)，以及 *Identity Applications 說明*中的「管理透過電子郵件進行的核准」。

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。例如 http://localhost:8080/IDMProv/images。

對電子郵件簽名

指定是否要將數位簽名新增至外送郵件。

如果啟用此選項，則還必須指定金鑰儲存區和簽名金鑰的設定。

金鑰儲存區路徑

僅當您啟用了對電子郵件簽名時才適用。

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

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

金鑰儲存區密碼

僅當您啟用了對電子郵件簽名時才適用。

指定金鑰儲存區檔案的密碼。例如，changeit。

簽名金鑰的別名

僅當您啟用了對電子郵件簽名時才適用。

指定簽章金鑰在金鑰儲存區中的別名。例如，idmapptest。

簽名金鑰密碼

僅當您啟用了對電子郵件簽名時才適用。

指定用於保護包含簽名金鑰的檔案的密碼。例如，changeit。

可信金鑰儲存區

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

可信儲存區路徑

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

可信儲存區密碼

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

這個密碼會根據萬能金鑰進行加密。

可信證書儲存區類型

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

NetIQ Sentinel 數位簽名證書與金鑰

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

Sentinel 數位簽名證書

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

Sentinel 數位簽名私密金鑰

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

其他

僅當您選取了顯示進階選項時，公用程式才會顯示這些設定。

OCSP URI

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

OCSP URI 會在線上更新可信證書的狀態。

授權組態路徑

指定授權組態檔案的完全合格名稱。

Identity Vault 索引

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

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

伺服器 DN

僅當您要建立或刪除 Identity Vault 索引時才適用。

指定要在其中建立或移除索引的 eDirectory 伺服器。

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

重新啟始化 RBPM 安全性

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

IDMReport URL

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

自訂主題網路位置名稱

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

記錄訊息識別碼字首

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

變更 RBPM 網路位置名稱

指定是否要變更 RBPM 的網路位置名稱。

您還必須指定角色與資源驅動程式的新名稱和 DN。

RBPM 網路位置名稱

僅當您選取了變更 RBPM 網路位置名稱時才適用。

指定 RBPM 的新網路位置名稱。

角色驅動程式 DN

僅當您選取了變更 RBPM 網路位置名稱時才適用。

指定角色與資源驅動程式的 DN。

容器物件

這些參數僅在安裝期間適用。

此區段可協助您定義容器物件的值，或建立新的容器物件。

已選定

指定您要使用的容器物件類型。

容器物件類型

指定容器：地域性、國家 / 地區、組織單位、組織或網域。

您也可以在 iManager 中定義自己的容器，然後將其新增至「新增新容器物件」之下。

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。

15.8.3 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 214 頁)
- 「報告保留值」(第 214 頁)

- 「修改地區設定」(第 215 頁)
- 「職能組態」(第 215 頁)

電子郵件傳送組態

本節定義用於傳送通知的值。

SMTP 伺服器主機名稱

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

SMTP 伺服器連接埠

指定 SMTP 伺服器的連接埠號。

SMTP 使用 SSL

指定是否要使用 TLS/SSL 通訊協定來與電子郵件伺服器通訊。

伺服器需要驗證

指定是否要對電子郵件伺服器通訊使用驗證。

SMTP 使用者名稱

指定要用來進行驗證的電子郵件地址。

您必須指定一個值。如果伺服器不需要驗證，則可指定無效的位址。

SMTP 使用者密碼

僅當您指定了伺服器需要驗證時才適用。

指定 SMTP 使用者帳戶的密碼。

預設電子郵件地址

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

報告保留值

本節定義用於儲存已完成報告的值。

報告單位，報告生命期間

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

報告的位置

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

修改地區設定

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

職能組態

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

新增驗證來源

指定您要為報告功能新增的驗證來源類型。驗證來源可以是

- **預設值**
- **LDAP 目錄**
- **檔案**

15.8.4 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 215 頁)
- 「驗證組態」(第 216 頁)
- 「驗證方法」(第 216 頁)
- 「密碼管理」(第 217 頁)
- 「Sentinel 數位簽名證書和金鑰」(第 218 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。

OAuth 伺服器正在使用 TLS/SSL

指定驗證伺服器是否使用 TLS/SSL 通訊協定進行通訊。

選擇性 TLS/SSL 可信證書儲存區檔案

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

選擇性 TLS/SSL 可信證書儲存區密碼

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

指定用於載入 TLS/SSL 驗證伺服器之金鑰儲存區檔案的密碼。

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

驗證組態

本節定義驗證伺服器的設定。

管理員容器的 LDAP DN

必需

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

重複的解析命名屬性

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

將驗證來源限制為網路位置

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

工作階段逾時 (分鐘)

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

存取記號生命期間 (秒)

指定 OSP 存取記號保持有效的秒數。預設值是 60 秒。

重新整理記號生命期間 (小時)

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

驗證方法

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

方法 ：

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

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

對應屬性名稱

*僅當您指定了 **Kerberos** 或 **SAML** 時才適用。*

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

中繼資料 URL

*僅當您指定了 **SAML** 時才適用。*

指定 OSP 用來將驗證要求重新導向至 SAML 的 URL。

密碼管理

本節定義可讓使用者透過自助操作形式修改其密碼的值。

密碼管理提供程式

指定要使用的密碼管理系統類型。

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

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》* (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。

15.8.5 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。

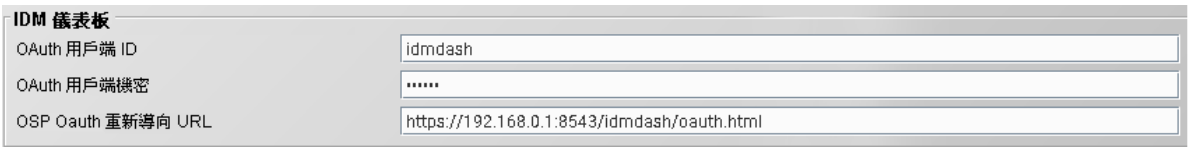
該索引標籤預設會顯示基本選項。若要查看所有設定，請按一下**顯示進階選項**。此索引標籤包含以下幾組設定：

- 「IDM 儀表板」(第 218 頁)
- 「IDM 管理員」(第 219 頁)
- 「RBPM」(第 219 頁)
- 「報告」(第 220 頁)
- 「IDM 資料收集服務」(第 221 頁)
- 「DCS 驅動程式」(第 221 頁)
- 「Self Service Password Reset」(第 222 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。

圖 15-2 IDM 儀表板



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

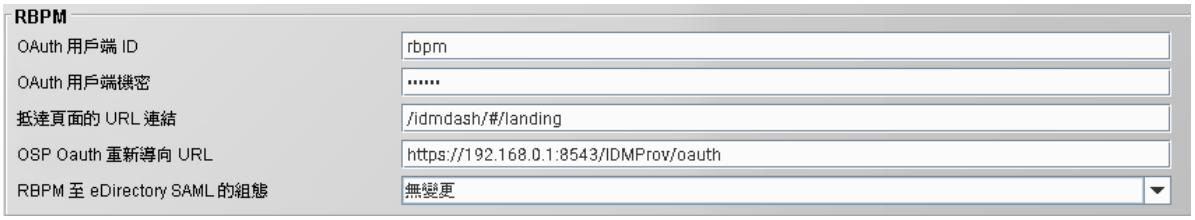
指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。

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。

圖 15-3 *RBPM*



OAuth 用戶端 ID

必需

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

OAuth 用戶端密碼

必需

指定使用者應用程式單一登入用戶端的密碼。

抵達頁面的 URL 連結

必需

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

OSP OAuth 重新導向 URL

必需

指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。

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

RBPM 至 eDirectory SAML 的組態

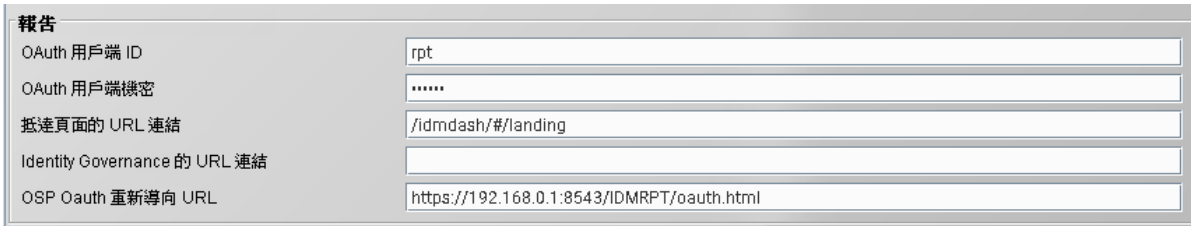
必需

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

報告

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

圖 15-4 *報告*



OAuth 用戶端 ID

必需

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

OAuth 用戶端密碼

必需

指定 Identity Reporting 單一登入用戶端的密碼。

抵達頁面的 URL 連結

必需

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

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

OSP OAuth 重新導向 URL

必需

指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。

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

IDM 資料收集服務

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

OAuth 用戶端 ID

必需

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

OAuth 用戶端密碼

必需

指定 Identity Manager 資料收集服務單一登入用戶端的密碼。

OSP OAuth 重新導向 URL

必需

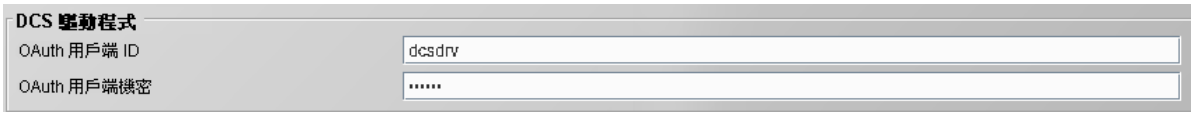
指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。

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

DCS 驅動程式

本節定義用於管理資料收集服務驅動程式的值。

圖 15-5



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。

15.8.6 CEF 稽核參數

本節定義用於管理 CEF 稽核參數的值。

傳送稽核事件

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

目的地主機

指定稽核伺服器的 DNS 名稱或 IP 位址。

目的地連接埠

指定稽核伺服器的連接埠。

網路協定

指定稽核伺服器用來接收 CEF 事件的網路通訊協定。

使用 TLS

僅當您要使用 TCP 做為網路通訊協定時適用。

指定稽核伺服器是否設定為將 TLS 與 TCP 搭配使用。

中間事件儲存目錄

指定在將 CEF 事件傳送到稽核伺服器之前快取目錄的位置。

附註：請確定對快取目錄設定了 novlua 許可權。否則，您將不能存取 IDMDash 和 IDMProv 應用程式，並且系統也不會在快取目錄中記錄 OSP 事件。例如，您可以使用 chown novlua:novlua /<directorypath> 指令來變更該目錄的許可權和擁有權，其中，<directorypath> 是快取檔案目錄路徑。

V 安裝 Identity Reporting

此部分將引導您完成安裝執行報告所需元件的程序。安裝程序包含應用程式所需的全部元件：

- NetIQ Identity Reporting
- Identity Manager Managed System Gateway Driver (MSGW 驅動程式)
- Identity Manager Driver for Data Collection Service (DCS 驅動程式)

安裝檔案位於 Identity Manager 安裝套件 .iso 影像檔中的 \products\Reporting 目錄下。依預設，安裝程式會在 C:\NetIQ\idm\apps\IDMReporting 中安裝元件。

為方便起見，Identity Manager 安裝套件中包含了 Sentinel Log Management for IGA (Sentinel) 做為內建稽核服務。如需詳細資訊，請參閱 《NetIQ Identity Manager Setup Guide for Linux》 (NetIQ Identity Manager 安裝指南 - Linux) 中的 「Installing Sentinel Log Management for Identity Governance and Administration」 (安裝 Sentinel Log Management for Identity Governance and Administration)。

NetIQ 建議您在開始之前檢閱安裝程序。如需詳細資訊，請參閱第 16 章 「規劃安裝 Identity Reporting」 (第 225 頁)。

16 規劃安裝 Identity Reporting

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

- 第 16.1 節「Identity Reporting 的安裝核對清單」(第 225 頁)
- 第 16.2 節「瞭解 Identity Reporting 各元件的安裝程序」(第 226 頁)
- 第 16.3 節「安裝 Identity Reporting 各元件的先決條件」(第 226 頁)
- 第 16.4 節「Identity Reporting 的身分稽核事件」(第 227 頁)
- 第 16.5 節「Identity Reporting 的系統要求」(第 228 頁)

16.1 Identity Reporting 的安裝核對清單

NetIQ 建議您完成以下核對清單中的步驟：

	核對清單項目
❑	1. 瞭解 Identity Manager 各元件之間的互動。如需詳細資訊，請參閱第 3.3.4 節「Identity Reporting」(第 24 頁)。
❑	2. 確定要為 Identity Manager 的元件使用哪些伺服器。如需詳細資訊，請參閱第 5.3 節「建議的安裝情境和伺服器設定」(第 39 頁)。
❑	3. 檢閱安裝 Identity Reporting 的考量。如需詳細資訊，請參閱第 16.3 節「安裝 Identity Reporting 各元件的先決條件」(第 226 頁)。
❑	4. 檢閱將要代管 Identity Reporting 的電腦需要符合的硬體和軟體要求。如需詳細資訊，請參閱第 16.5 節「Identity Reporting 的系統要求」(第 228 頁)。
❑	5. 確保您已安裝 Identity Applications。如需詳細資訊，請參閱第 15.1 章「規劃安裝 Identity Applications」(第 165 頁)。
❑	6. 若要稽核事件，請在 Linux 伺服器上安裝 Sentinel。如需詳細資訊，請參閱《NetIQ Identity Manager Setup Guide for Linux》(NetIQ Identity Manager 安裝指南 - Linux) 中的「Installing Sentinel Log Management for Identity Governance and Administration」(安裝 Sentinel Log Management for Identity Governance and Administration)。
❑	7. 確保要安裝 Identity Reporting 的伺服器上已裝有諸如 Tomcat 的應用程式伺服器。如需詳細資訊，請參閱第 12.2 章「安裝 PostgreSQL 和 Tomcat」(第 143 頁)。
❑	8. (視情況而定) 若要使用 Apache Log4j 服務來記錄 Tomcat 中的事件，請確保您有相應的檔案。如需詳細資訊，請參閱第 13.1.4 節「使用 Apache Log4j 服務記錄登入」(第 150 頁)。
❑	9. 安裝 Identity Reporting： ◆ 若要執行引導式安裝，請參閱第 17.1 節「使用引導式程序安裝 Identity Reporting」(第 231 頁)。 ◆ 若要以靜默模式安裝 Reporting，請參閱第 17.2 節「以靜默模式安裝 Identity Reporting」(第 235 頁)。

	核對清單項目
❑	10. 完成 Identity Reporting 的設定。如需詳細資訊，請參閱第 18 章 「設定 Identity Reporting」 (第 239 頁)。
❑	11. 設定受管理系統閘道驅動程式和資料收集服務驅動程式。如需詳細資訊，請參閱第 19.1 節 「設定 Identity Reporting 的驅動程式」 (第 241 頁)。
❑	12. 部署並啟動驅動程式。如需詳細資訊，請參閱第 19.2 節 「部署並啟動 Identity Reporting 的驅動程式」 (第 246 頁)。
❑	13. 設定驅動程式的環境。如需詳細資訊，請參閱第 19.3 節 「設定執行時期環境」 (第 251 頁)。
❑	14. 設定 Identity Manager 和 eDirectory，以向驅動程式傳送資料。如需詳細資訊，請參閱第 19.4 節 「設定驅動程式的稽核旗標」 (第 258 頁)。

16.2 瞭解 Identity Reporting 各元件的安裝程序

您可以將 Sentinel、Identity Reporting 和 Reporting 驅動程式安裝在同一台伺服器上。但是，由於工作負載的原因，NetIQ 建議將 Sentinel 和 Reporting 安裝在不同的伺服器上。

如果進行全新安裝，安裝程式將在該資料庫中建立表格並驗證連接性。程式還會安裝 PostgreSQL JDBC 驅動程式的 JAR 檔案，並自動使用此檔案建立資料庫連接。

如果您已將您的資料 (例如 SIEM) 從 EAS 移轉至 PostgreSQL 資料庫，則安裝程式將連接到現有資料庫。

Identity Reporting 的安裝程式會執行以下功能：

- 允許您選擇應用程式伺服器平台
- 將用戶端 WAR 檔案 (DCS 和 Reporting) 部署到 Tomcat，該檔案中包含用於執行報告的使用者介面元件
- 部署核心 WAR 檔案 (DCS 和 Reporting)，其中包含執行報告所需的核心 REST 服務
- 部署 API WAR 檔案，其中包含執行報告所需 REST 服務的文件
- 部署 API WAR 檔案，其中包含執行報告所需的 Identity Manager 資料收集服務
- 設定 Identity Reporting 的驗證服務
- 設定 Identity Reporting 的電子郵件傳送系統
- 設定 Identity Reporting 的核心報告服務
- 為 Identity Reporting 建立使用者帳戶 (**idmrptsrv** 和 **idmrptuser**)
- 建立用來與 Sentinel 互動的使用者帳戶 (**appuser** 和 **rptuser**)

16.3 安裝 Identity Reporting 各元件的先決條件

在安裝 Identity Reporting 時，請注意以下先決條件和事項：

- 需要以下 Identity Manager 元件的受支援且已設定版本：
  - Identity Applications，包括使用者應用程式驅動程式

- Sentinel 安裝在單獨的 Linux 電腦上。
- Driver for Data Collection Service
- 受管理系統閘道服務的驅動程式

如需這些元件所需版本和修補程式的詳細資訊，請參閱最新的 《版本說明》。如需安裝驅動程式的詳細資訊，請參閱第 19 章 「管理執行報告所需的驅動程式」(第 241 頁)。

- 請不要將 Identity Reporting 安裝在叢集環境中的伺服器上。
- 如果您要使用本地資料庫以外的資料庫，則應在 Identity Reporting 安裝期間於其他伺服器上建立資料庫，並指定詳細資料。
- (視情況而定) 若要針對 Oracle 12c 資料庫執行報告，您必須安裝相應的 JDBC 檔案。如需詳細資訊，請參閱第 18.1 節 「對 Oracle 資料庫執行報告」(第 239 頁)。
- (視情況而定) 您可以使用自己的 Tomcat 安裝程式，而不使用 Identity Manager 安裝套件中提供的安裝程式。但是，若要將 Apache Log4j 服務與您的 Tomcat 版本配合使用，請確保已安裝相應的檔案。如需詳細資訊，請參閱第 13.1.4 節「使用 Apache Log4j 服務記錄登入」(第 150 頁)。
- 為您要授予報告功能存取權的所有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 引擎的伺服器與代管倉儲的伺服器的時間戳記不同，則此問題可能會影響到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。
- 安裝程序會在 Tomcat 的 setenv.bat 檔案中修改 JRE 對應的 JAVA_OPTs 或 CATALINA_OPTS 項目。

  依預設，Tomcat 的便捷安裝程式會將 setenv.bat 檔案放在 C:\NetIQ\idm\apps\tomcat\bin 目錄中。安裝程式還會在該檔案中設定 JRE 位置。

16.4 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 **選取使用 iManager 的稽核旗標：**轉到 **iManager 角色與任務** > **eDirectory 稽核** > > **稽核組態** > **Novell Audit** > 選取以下稽核旗標之一： ◆ 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**

16.5 Identity Reporting 的系統要求

本節提供要安裝 Identity Reporting 元件的伺服器的最低要求。

類別	要求
處理器	1 GHz 處理器
磁碟空間	1 GB **附註：**為支援應用程式的內容 (例如資料庫和應用程式伺服器記錄) 提供足夠空間。
記憶體	512 MB (建議 4 GB)
作業系統 (已認證)	以下 64 位元作業系統之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 NetIQ 建議您在安裝 Identity Manager 之前，依照製造商的自動更新機制來套用最新的作業系統修補程式。

類別	要求
作業系統 (受支援)	已認證作業系統的最新版 Service Pack **附註：***受支援*指作業系統尚未進行測試，但預期可正常運作。
虛擬化系統	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.5 及更新版本 ◆ 包含 Hyper-V 的 Windows Server 2012 R2 Virtualization (受支援) NetIQ 允許您在為執行 NetIQ 產品的作業系統提供官方支援的企業級虛擬化系統上執行 Identity Manager。只要虛擬化系統的廠商為這些作業系統提供官方支援，NetIQ 就支援在這些系統上執行整個 Identity Manager 堆疊。
資料庫	◆ PostgreSQL 9.6.6 ◆ Oracle 12c ◆ MsSQL 2014、2016
應用程式伺服器	Apache Tomcat 8.5.27
Java	Java Development Kit (JDK) 或 Sun (Oracle) 提供的 Java Runtime Environment (JRE) 1.8.0_162 或更新版本
網頁瀏覽器	以下任意瀏覽器 (最低版本)： **Desktop** ◆ Apple Safari 9 ◆ Apple Safari 5.1.7 for Windows ◆ Google Chrome 61 ◆ Microsoft Internet Explorer 11 ◆ Mozilla Firefox 51 **iPad** ◆ Apple Safari 9 ◆ Google Chrome 61 **附註：**必須在瀏覽器中啟用 Cookie。如果停用 Cookie，該產品將不會正常運作。
稽核	Sentinel Log Management for IGA

17 安裝 Identity Reporting

本章介紹 Identity Reporting 的安裝程序。

- 第 17.1 節「使用引導式程序安裝 Identity Reporting」(第 231 頁)
- 第 17.2 節「以靜默模式安裝 Identity Reporting」(第 235 頁)
- 第 17.3 節「手動產生資料庫綱要」(第 236 頁)
- 第 17.4 節「連接遠端 Remote PostgreSQL 資料庫」(第 237 頁)

17.1 使用引導式程序安裝 Identity Reporting

以下程序介紹如何使用安裝精靈安裝 Identity Reporting。若要執行靜默模式的無人管理安裝，請參閱第 17.2 節「以靜默模式安裝 Identity Reporting」(第 235 頁)。

若要進行安裝準備工作，請檢閱第 16.5 節「Identity Reporting 的系統要求」(第 228 頁) 中列出的先決條件和系統要求。另請參閱版本隨附的《版本說明》。

1. 登入您要安裝 Identity Reporting 的電腦。
2. 停止 Tomcat。
3. (視情況而定) 如果您已取得 Identity Manager 安裝套件的 .iso 影像檔，請導覽至包含 Identity Reporting 安裝檔案的目錄 (預設位於 \products\Reporting 目錄中)。
4. (視情況而定) 如果您已從 NetIQ 下載網站下載了 Identity Reporting 安裝檔案，請完成以下步驟：
   - **4a** 導覽至所下載影像的 .tgz 檔案。
   - **4b** 將該檔案的內容擷取到本地電腦上的某個資料夾中。
5. 從包含安裝檔案的目錄中執行 rpt-install-win.exe 檔案。
6. 在安裝程式中，指定要用於安裝的語言，然後按一下**確定**。
7. 查看「簡介」文字，然後按**下一步**。
8. 接受授權合約，然後按**下一步**。
9. 使用以下參數完成引導式程序：
   - 安裝資料夾

     指定安裝程式要在其中建立應用程式檔案 (包括安裝記錄檔案、輔助程式程序檔和組態程序檔) 的目錄路徑。
   - **Reporting 安裝**

     代表要將 Identity Reporting 新增至的環境及其設定。為 **Identity Manager** 指定以下值：

     ***Identity Vault** 伺服器*

     指定 eDirectory 伺服器的主機名稱。

安全 LDAP 連接埠

指定您要用於透過 SSL 與 eDirectory 伺服器建立 LDAP 連接的連接埠。預設埠為 636。

佈建主目錄

指定 Identity Manager 佈建主目錄位置。這可以是完整的應用程式伺服器 URL，也可以是 URL 的相對路徑。

- 應用程式伺服器詳細資料

代表要執行 Identity Reporting 的 Tomcat。該應用程式伺服器必須已安裝好。

次要

指定目前安裝是否位於叢集的次要節點上。

Tomcat 根資料夾

指定 Tomcat 例項的路徑。例如 C:\NetIQ\idm\apps\tomcat。

Java JRE 基礎資料夾

指定 Java JRE 基礎資料夾位置。

該路徑包含組態更新公用程式檔案，用於在安裝 Identity Reporting 後啟動此公用程式。

- 應用程式位址

表示代管 Identity Reporting 的伺服器的設定。

通訊協定

指定您要使用 *http* 還是 *https*。若要使用 SSL 進行通訊，請指定 https。

主機名稱

指定 Tomcat 的 DNS 名稱或 IP 位址。請不要使用 localhost。

連接埠

指定您希望 Tomcat 在與 Identity Reporting 應用程式通訊時使用的連接埠。

連接至外部驗證伺服器

指定是否要用不同的 Tomcat 例項來代管驗證伺服器 (OSP)。驗證伺服器包含可登入 Identity Reporting 的使用者清單。

如果選取此設定，請指定驗證伺服器的通訊協定、主機名稱和連接埠值。

- 驗證伺服器詳細資料

指定 Identity Reporting 服務的密碼。

Identity Manager 使用此密碼來連接驗證伺服器上的 OSP 用戶端。

- 資料庫詳細資料

代表 Reporting 資料庫的設定，包括您是要讓安裝程序建立資料庫，還是產生一個 SQL 檔案以便稍後再建立資料庫。

資料庫名稱

依據您的要求指定資料庫名稱：

- 執行全新安裝時，請指定 Reporting 資料庫的名稱。例如，idmrptdb 或 SIEM。
- 如果您要從 EAS 移轉，請指定 EAS 資料庫的名稱，例如 SIEM。

資料庫主機

依據您的要求指定資料庫主機：

- 執行全新安裝時，請指定需要在其中建立資料庫的伺服器的 DNS 名稱或 IP 位址。
- 如果您要從 EAS 移轉，請指定代管 SIEM 資料庫的伺服器的 DNS 名稱或 IP 位址。

資料庫類型

選取要使用的資料庫。

如果選取 **Oracle**，請指定以下詳細資料：

- **JDBC 驅動程式 jar**

  指定 Oracle JDBC 驅動程式 jar 檔案的路徑。例如 C:\oracle\ojdbc7.jar。

  如需詳細資訊，請參閱第 18.1 節「對 Oracle 資料庫執行報告」(第 239 頁)。

- **JDBC 驅動程式類別名稱**

  指定 JDBC 驅動程式的類別。

- **JDBC 驅動程式類型**

  指定 JDBC 驅動程式的類型。

如果選取 **PostgresSQL**，請按下一步。

共享密碼

可讓您為所有 Reporting 使用者指定一個用於連接資料庫的密碼。

指定每個使用者的密碼

可讓您為每個 Reporting 使用者指定用於連接資料庫的唯一密碼。需要為 idm_rpt_data_password、idm_rpt_cfg_password 和 idmrptuserpassword 指定密碼。

資料庫連接埠

指定用於連接資料庫的連接埠。預設連接埠為 5432。

立即設定資料庫或在啟動時設定

指出您可以選取以下資料庫登入設定：讓安裝程式立即建立資料庫，或在啟動 Reporting 期間建立。此外，您還必須指定以下值：

- **DBA 使用者 ID**

  指定 SIEM 資料庫伺服器管理帳戶的名稱。例如，*postgres.*

- **DBA 密碼**

  指定資料庫管理帳戶的密碼。

- **測試資料庫連接：**指定是否要讓安裝程式測試您為資料庫指定的值。

  當您按下一步或 **Enter** 鍵後，安裝程式會嘗試建立連接。

附註：如果資料庫連接失敗，您可以繼續安裝。但在安裝後，您必須手動建立表格並連接到資料庫。如需詳細資訊，請參閱第 17.3 節「手動產生資料庫綱要」(第 236 頁)。

產生 SQL 供日後使用

指示安裝程式產生資料庫管理員將用於在您完成安裝程序後建立資料庫的 SQL 檔案。若要在安裝後建立資料庫，請參閱第 17.3 節「手動產生資料庫綱要」(第 236 頁)。

- 預設語言

指定您希望 Identity Reporting 在搜尋時使用的語言。

- **Identity Vault 身分證明**

  代表 Identity Reporting 用於連接 Identity Vault 的設定。

  Identity Vault 管理員

  指定 LDAP 管理員的可辨識名稱。例如，cn=admin。Identity Vault 中必須已存在此使用者。

  Identity Vault 管理員密碼

  指定 Identity Vault 管理員的密碼。

  金鑰儲存區路徑

  指定 Tomcat 在執行時所用 JRE 金鑰儲存區 (cacerts) 檔案的完整路徑。

  金鑰儲存區密碼

  指定金鑰儲存區檔案的密碼。

  報告管理員角色容器 DN

  指定儲存報告管理員角色的容器 DN。

  報告管理員使用者 DN

  指定 Identity Vault 中有權執行 Identity Reporting 管理任務的現有使用者帳戶。

- 「使用者應用程式」驅動程式

  表示應用程式驅動程式、驅動程式集和驅動程式集容器的名稱。

  使用者應用程式驅動程式

  指定使用者應用程式驅動程式的名稱。

  驅動程式集名稱

  指定驅動程式集的名稱。

  驅動程式集容器

  指定驅動程式集容器的名稱。

- 電子郵件傳送

  代表傳送報告通知之 SMTP 伺服器的設定。若要在安裝後修改這些設定，請使用 RBPM 組態公用程式。

  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。

  SMTP 伺服器

  指定 Identity Reporting 用來傳送通知之 SMTP 電子郵件主機的 IP 位址或 DNS 名稱。請不要使用 localhost。

  SMTP 伺服器連接埠

  指定 SMTP 伺服器的連接埠號。預設埠為 465。

  對 SMTP 使用 SSL

  指定是否要使用 SSL 通訊協定來與 SMTP 伺服器通訊。

  需要伺服器驗證

  指定是否要對與 SMTP 伺服器的通訊使用驗證。此外，您還必須指定以下值：

  - ***SMTP 使用者名稱***

指定 SMTP 伺服器登入帳戶的名稱。

- ***SMTP 密碼***

  指定 SMTP 伺服器登入帳戶的密碼。

- **報告詳細資料**

  代表報告定義及已完成報告的設定。

  保留已完成報告的時間

  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，請輸入 6 然後選取月。

  報告定義的位置

  指定要用來儲存報告定義的路徑。

  例如，C:\NetIQ\idm\apps\IdentityReporting。

10 在「安裝前摘要」視窗中按一下**安裝**。

17.2 以靜默模式安裝 Identity Reporting

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，系統會使用 .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。若要執行引導式安裝，請參閱「使用引導式程序安裝 Identity Reporting」(第 231 頁)。

若要進行安裝準備工作，請檢閱第 16.5 節「Identity Reporting 的系統要求」(第 228 頁)中列出的先決條件和系統要求。另請參閱版本隨附的 《版本說明》。

1 (視情況而定) 若不想在 .properties 檔案中為靜默安裝指定用於安裝的管理員密碼，請使用 export 或 set 指令。例如： set NOVL_ADMIN_PWD=*myPassWord*

靜默安裝程序將會從環境中讀取密碼，而不是從 .properties 檔案中讀取。

指定以下密碼：

NOVL_DB_RPT_USER_PASSWORD

指定 SIEM 資料庫管理員的密碼。

NOVL_IDM_SRV_PWD

指定用於執行報告之資料庫綱要與物件擁有者的密碼。

NOVL_IDM_USER_PWD

指定對報告資料擁有唯讀存取權之 idmrptuser 的密碼。

NOVL_ADMIN_PWD

(視情況而定) 若要在登入時啟用子容器搜尋，請指定 LDAP 管理員的密碼。

NOVL_SMTP_PASSWORD

(視情況而定) 若要對電子郵件通訊使用驗證，請指定預設 SMTP 電子郵件使用者的密碼。

2 若要指定安裝參數，請完成以下步驟：

2a 確保 .properties 檔案位於安裝可執行檔所在的目錄中。

為方便起見，NetIQ 提供了兩個 .properties 檔案 (這些檔案預設位於 .iso 影像的 products\Reporting 目錄中) ：

- rpt_installonly.properties，使用預設安裝設定
- rpt_configonly.properties，用於自訂安裝設定

2b 在文字編輯器中，開啟 .properties 檔案。

2c 指定參數值。如需參數的描述，請參閱步驟 9 (第 231 頁)。

附註：用於安裝 Standard Edition 的 .properties 檔案中僅包含該版本所需的參數。

2d 儲存然後關閉該檔案。

3 若要啟動安裝程序，請輸入以下指令：

rpt-install.exe -i silent -f *properties 檔案的路徑*

附註：如果 .properties 檔案不在安裝程序檔所在的目錄中，則您必須指定該檔案的完整路徑。該程序檔會將所需的檔案解包到暫存目錄，然後啟動靜默安裝。

17.3 手動產生資料庫綱要

您可以在安裝後重新建立資料庫表格，而無需重新安裝。本節的內容可協助您建立資料庫綱要。

1 使用 services.msc 檔案停止 Tomcat。

2 (視情況而定) 建立一個新資料庫。

如果您的資料庫在其他伺服器上執行，則必須連接至該資料庫伺服器。對於遠端安裝的 PostgreSQL 資料庫，請驗證該資料庫伺服器是否在執行中。若要連接至遠端 PostgreSQL 資料庫，請參閱第 17.4 節「連接遠端 Remote PostgreSQL 資料庫」(第 237 頁)。如果要連接至 Oracle 資料庫，請確定已在該資料庫伺服器中建立 Oracle 資料庫例項。如需詳細資訊，請參閱 Oracle 文件。

3 使用 C:\NetIQ\idm\apps\IdentityReporting\sql 中的下列 SQL 將所需角色新增至資料庫中。

- **PostgreSQL：**create_dcs_roles_and_schemas.sql 和 create_rpt_roles_and_schemas.sql
- **Oracle：**create_dcs_roles_and_schemas-orcale.sql 和 create_rpt_roles_and_schemas-orcale.sql

4 若要建立 IDM_RPT_DATA、IDM_RPT_CFG 和 IDMRPTUSER 角色：

- **PostgreSQL：**依給定順序執行以下指令：

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

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

- **Oracle：**依給定順序執行以下指令：

```
begin
CREATE_DCS_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_DATA>');
end;

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

5 將 get_formatted_user_dn 函數新增至 IDM_RPT_DATA 綱要中。

   5a 以資料庫管理員使用者的身分登入資料庫。

   5b 從 C:\NetIQ\idm\apps\IdentityReporting\sql 中新增 get_formatted dn 函數。

   對於 PostgreSQL，請尋找 get_formatted_user_dn.sql；對於 Oracle，請尋找 get_formatted_user_dn-oracle.sql。

6 清除位於 C:\NetIQ\idm\apps\IdentityReporting\sql 中的下列 .sql 檔案的資料庫檢查總數：

   - 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

   6a 在每個 SQL 的起始處附加下行：

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

   修改後的內容應該類似如下：

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

   6b 執行相應使用者的每個 SQL。

7 將變更提交到資料庫。

8 使用 services.msc 檔案啟動 Tomcat。

17.4 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，請將以下項目新增至 C:\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，請將以下項目新增至 C:\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。

18 設定 Identity Reporting

安裝 Identity Reporting 後，您仍可以執行 configupdate.bat 檔案來修改許多安裝內容。

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。

- 第 18.1 節「對 Oracle 資料庫執行報告」(第 239 頁)
- 第 18.2 節「部署 Identity Reporting 的 REST API」(第 239 頁)
- 第 18.3 節「連接遠端 Remote PostgreSQL 資料庫」(第 239 頁)

18.1 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。但是，您必須將一個 Oracle JDBC 檔案新增至應用程式伺服器的程式庫中。

1. 從 Oracle 網站下載 ojdbc7.jar 檔案。
2. 將該檔案複製到 Tomcat 伺服器的相應位置 (*tomcat_lib* 中的 common/lib 目錄)。

如需受支援 Oracle 資料庫的詳細資訊，請參閱第 16.5 節「Identity Reporting 的系統要求」(第 228 頁)。

18.2 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。

在臨時環境或生產環境中操作時，請從 Tomcat 上的環境中手動刪除 rptdoc war 檔案和資料夾。

18.3 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，請將以下項目新增至 C:\NetIQ\idm\apps\postgres\data\postgresql.conf 檔案中：

   ```
   listen_addresses = '*'
   ```

   如果伺服器上有多個介面，可以指定要監聽的特定介面。
2. 將用戶端驗證項目新增至 pg_hba.conf 檔案中。

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

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

例如，192.168.104.24/26 trust

這僅適用於 IPv4 位址。對於 IPv6 位址，請新增以下項目：

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

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

pg_hba.conf 檔案支援以下用戶端驗證格式。

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

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

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

3 測試遠端連接。

3a 重新啟動遠端 PostgreSQL 伺服器。

3b 使用使用者名稱和密碼從遠端登入伺服器。

19 管理執行報告所需的驅動程式

Identity Reporting 需要以下驅動程式：

- Identity Manager Managed System Gateway Driver
- Identity Manager Driver for Data Collection Service

您可以使用 Designer 隨附的套件管理工具來安裝和設定這些驅動程式。此程序包括以下活動：

- 第 19.1 節「設定 Identity Reporting 的驅動程式」(第 241 頁)
- 第 19.2 節「部署並啟動 Identity Reporting 的驅動程式」(第 246 頁)
- 第 19.3 節「設定執行時期環境」(第 251 頁)
- 第 19.4 節「設定驅動程式的稽核旗標」(第 258 頁)

19.1 設定 Identity Reporting 的驅動程式

本節的內容可協助您安裝和設定 Identity Reporting 的受管理系統閘道驅動程式及資料收集服務驅動程式。

附註：本節假設您已安裝並設定 RBPM 的使用者應用程式驅動程式及角色與資源驅動程式。如需詳細資訊，請參閱第 15.6 章 「建立和部署 Identity Applications 的驅動程式」(第 192 頁)。

- 第 19.1.1 節「安裝 Identity Reporting 的驅動程式套件」(第 241 頁)
- 第 19.1.2 節「設定受管理系統閘道驅動程式」(第 242 頁)
- 第 19.1.3 節「設定資料收集服務的驅動程式」(第 243 頁)
- 第 19.1.4 節「設定 Identity Reporting 以從 Identity Applications 收集資料」(第 245 頁)

19.1.1 安裝 Identity Reporting 的驅動程式套件

在嘗試設定驅動程式之前，必須先安裝「套件目錄」中所有必要的驅動程式套件。當您在 Designer 中建立新的 Identity Manager 專案時，使用者介面會自動提示您將幾個套件輸入至新專案中。您不需要在安裝期間輸入這些套件，但為了使 Identity Reporting 正常運作，您必須在某個時間安裝這些套件。

1. 在 Designer 中開啟您的專案。
2. 選取**套件目錄 > 輸入套件**。
3. 在「選取套件」對話方塊中，按一下**全部選取**，然後按一下**確定**。

   Designer 會在「**套件目錄**」下新增數個新的套件資料夾。這些套件資料夾與 Designer 中「模型產生器」檢視窗右側調色盤中的一些物件相對應。
4. 按一下「**儲存**」。

19.1.2 設定受管理系統閘道驅動程式

1 在 Designer 中開啟您的專案。

2 在模型產生器檢視窗上的調色盤中，選取服務 > 受管理系統閘道。

3 將受管理系統閘道的圖示拖曳至模型產生器檢視窗中。

4 在驅動程式組態精靈中，選取受管理系統閘道基礎，然後按下一步。

5 在「選取強制功能」視窗中，選取強制功能，然後按下一步。

6 (視情況而定) 如果應用程式提示您選取一個名為進階 Java 類別的額外套件，請選取該套件，然後按一下確定。

7 (選擇性) 指定要為驅動程式使用的名稱。

8 按一下「下一步」。

9 對於「連接參數」，請指定 Identity Reporting 用來向驅動程式要求獲取資料的值。

   如果指定了多個 IP 位址，您仍然是使用同一個連接埠號來監聽所有介面。例如，如果您指定了 192.168.0.1,127.0.0.1 位址和 9000 連接埠，則驅動程式會使用以下設定：

   ```
   192.168.0.1:9000
   127.0.0.1:9000
   ```

10 (選擇性) 若要啟用端點追蹤，請選取 **true**，然後指定追蹤檔案的位置。

11 按一下「下一步」。

12 (選擇性) 若要將驅動程式連接到遠端載入器，請完成以下步驟：

   12a 在「遠端載入器」視窗中，選取是。

   12b 指定您要使用之遠端載入器的設定。

13 按一下「下一步」。

14 檢閱「確認安裝任務」視窗中的資訊，然後按一下完成。

15 (選擇性) 若要設定驅動程式的其他設定，請在「模型產生器」檢視窗中完成以下步驟：

   15a 在用於將受管理系統閘道驅動程式連接到驅動程式集的行上按一下滑鼠右鍵，然後按一下內容。

   15b 在「內容」對話方塊中，選取驅動程式組態 > 啟動選項。

   15c 選取手動做為啟動選項，然後按一下套用。

   15d 選取驅動程式參數索引標籤。

   15e (選擇性) 在驅動程式選項索引標籤中，修改驅動程式、連接和端點追蹤的設定。

   您可能需要在連接參數和驅動程式參數下選取顯示才能顯示這些設定。

   15f (選擇性) 若要讓驅動程式在發行者通道上傳送週期性狀態訊息，請按一下發行者選項索引標籤，然後為發行者活動訊號間隔指定一個值 (以分鐘為單位)。

   如果在指定的間隔內發行者通道上未出現流量，則驅動程式會傳送新的活動訊號。

   15g 按一下「套用」。

16 (選擇性) 若要指定伺服器的全域組態值，請完成以下步驟：

   16a 在導覽窗格中，選取 **GCV**。

   16b 指定全域組態值，例如：

查詢各驅動程式集的受管理系統

定義受管理系統閘道驅動程式的操作範圍。如果設定為 **true**，驅動程式將會傳回各驅動程式集的受管理系統資訊。否則，範圍限制為本地驅動程式集。

將端點要求資料新增至查詢

指定是否將端點要求資料新增至驅動程式傳送的查詢中。這些資料將會新增為操作資料節點。

端點要求資料節點名稱

指定要新增至查詢之操作資料的節點名稱。節點屬性將包含關於該要求的詳細資料。

16c 按一下「套用」。

17 (選擇性) 若要檢閱已安裝的套件，請在導覽窗格中按一下套件。

除非您要解除安裝特定的套件，否則不需要變更操作設定。

18 按一下「確定」。

19 啟用訂閱者通道，以使 Identity Reporting 能夠正常運作。

19.1.3 設定資料收集服務的驅動程式

1 在 Designer 中開啟您的專案。

2 在模型產生器檢視窗上的調色盤中，選取服務 > 資料收集服務。

3 將資料收集服務的圖示拖曳至模型產生器檢視窗中。

4 在驅動程式組態精靈中，選取資料收集服務基礎，然後按下一步。

5 在「選取強制功能」視窗中，選取強制功能，然後按下一步。

6 選取要套用的選擇性功能，然後按下一步。

7 (視情況而定) 如果應用程式提示您選取一個名為 **LDAP 程式庫**的額外套件，請完成以下步驟：

7a 選取該套件，然後按一下確定。

7b (選擇性) 若要在「安裝 LDAP 程式庫」頁面上設定所有驅動程式的全域連接設定檔，請選取是。

8 按一下「下一步」。

9 (選擇性) 指定要為驅動程式使用的名稱。

10 按一下「下一步」。

11 對於「連接參數」，請指定 Identity Reporting 用來向驅動程式要求獲取資料的值。

例如，指定用於驗證的報告管理員使用者和密碼。

如果指定了多個 IP 位址，您仍然是使用同一個連接埠號來監聽所有介面。例如，如果您指定了 192.168.0.1,127.0.0.1 位址和 9000 連接埠，則驅動程式會使用以下設定：

```
192.168.0.1:9000
127.0.0.1:9000
```

12 按一下「下一步」。

13 對於 **Identity Vault 註冊**，請指定 Identity Vault 的設定。

您必須指定 IP 位址。請勿指定用於 Identity Vault 註冊的 localhost 位址。

14 (選擇性) 若要註冊受管理系統閘道驅動程式，請完成以下步驟：

14a 對於受管理系統閘道註冊，請按一下是。

14b 指定驅動程式的 DN，以及 LDAP 管理員的使用者和密碼。

附註：由於您剛才設定的受管理系統閘道驅動程式尚未部署，瀏覽功能將不會顯示該驅動程式，因此，您可能需要輸入該驅動程式的 DN。

---

15 按一下「下一步」。

16 (選擇性) 若要將驅動程式連接到遠端載入器，請完成以下步驟：

16a 在「遠端載入器」視窗中，選取是。

16b 指定您要使用之遠端載入器的設定。

17 按一下「下一步」。

18 對於範圍組態，請指定資料收集服務驅動程式的角色。

19 檢閱「確認安裝任務」視窗中的資訊，然後按一下完成。

20 (選擇性) 若要設定驅動程式的其他設定，請在「模型產生器」檢視窗中完成以下步驟：

20a 在用於將資料收集服務驅動程式連接到驅動程式集的行上按一下滑鼠右鍵，然後按一下內容。

20b 在「內容」對話方塊中，選取驅動程式組態 > 啟動選項。

20c 選取手動做為啟動選項，然後按一下套用。

20d 選取驅動程式參數索引標籤。

在驅動程式會接收到大量事件的環境中，NetIQ 建議將每個檔案的批次數設定為不超過 5 的數值。如果將此參數設定為大於 5 的值，驅動程式將無法有效率地處理事件。

20e (選擇性) 在驅動程式選項索引標籤中，修改驅動程式、連接和註冊的設定。

在測試環境中，您可能需要使用較小的數字，以確保事件得到正確處理。但是，在線上環境中，您或許要使用較大的數字，以免系統不必要地處理事件。

IP 位址

指定代管 Identity Reporting 之伺服器的 IP 位址。

連接埠

指定 Identity Reporting 用來建立 REST 連接的連接埠號。

通訊協定

指定用於存取 Identity Reporting 的通訊協定。如果您選取 HTTPS，則還必須指定是否要信任伺服器的證書。

名稱

指定在 Identity Reporting 中用於參考 Identity Vault 的名稱。

描述

指定 Identity Vault 的簡短描述。

位址

指定 Identity Vault 的 IP 位址。

例如 192.168.0.1

附註：您必須指定 IP 位址。請勿指定用於 Identity Vault 註冊的「localhost」位址。

註冊受管理系統閘道

指定是否要註冊受管理系統閘道驅動程式。

受管理系統閘道驅動程式 DN (LDAP)

以斜線格式指定受管理系統閘道驅動程式的 DN。

受管理系統閘道驅動程式組態模式

指定是要在本地還是在遠端設定驅動程式。

使用者 DN (LDAP)

指定驅動程式應用來向受管理系統閘道驅動程式進行驗證的使用者 LDAP DN。Identity Vault 中必須存在此 DN。

密碼

指定該使用者的密碼。

提交事件的時間間隔

在將某個事件提交到 DCS (以及 Identity Reporting 的資料庫) 之前，該事件可在持續性層中保留的最長時間，以分鐘為單位。

20f (視情況而定) 若要從 Identity Applications 收集資料，請指定 **SSO 服務支援**的值。如需詳細資訊，請參閱第 19.1.4 節「設定 Identity Reporting 以從 Identity Applications 收集資料」(第 245 頁)。

20g 按一下「**套用**」。

21 若要設定 DN，請完成以下步驟：

21a 在導覽功能表中，選取**引擎控制值**。

21b 對於 **DN 語法屬性值的合法格式**設定，請選取 **True**。

21c 按一下「**套用**」。

22 (選擇性) 若要指定伺服器的全域組態值，請完成以下步驟：

22a 在導覽窗格中，選取 **GCV**。

22b 對於**顯示覆寫選項**，請選取**顯示**。

22c 修改用於置換全域組態值的設定。

22d 按一下「**套用**」。

23 按一下「**確定**」。

19.1.4 設定 Identity Reporting 以從 Identity Applications 收集資料

若要讓 Identity Reporting 從 Identity Applications 收集資料，必須將 DCS 驅動程式設定為支援單一登入程序。

1 在 Designer 中開啟您的專案。

2 在**大綱**檢視窗中，於資料收集服務驅動程式上按一下滑鼠右鍵，然後按一下**內容**。

3 按一下**驅動程式組態 > 驅動程式參數**。

4 按一下**顯示連接參數 > 顯示**。

5 按一下 **SSO 服務支援 > 是**。

6 指定單一登入功能的參數：

SSO 服務位址

必需

指定向 OSP 發出記號之驗證伺服器的相對 URL。例如，10.10.10.48。

此值必須與您在 RBPM 組態公用程式中為 **OSP 伺服器主機識別碼**指定的值相符。如需詳細資訊，請參閱 「驗證伺服器」 (第 215 頁)。

SSO 服務連接埠

必需

指定驗證伺服器的連接埠。預設值為 8180。

此值必須與您在 RBPM 組態公用程式中為 **OSP 伺服器 TCP 連接埠**指定的值相符。如需詳細資訊，請參閱 「驗證伺服器」 (第 215 頁)。

SSO 服務用戶端 ID

必需

指定用來供驗證伺服器識別 DCS 驅動程式單一登入用戶端的名稱。預設值為 dcsdrv。

此值必須與您在 RBPM 組態公用程式中為 **OSP 用戶端 ID** 指定的值相符。如需詳細資訊，請參閱 「報告」 (第 220 頁)。

SSO 服務用戶端密碼

必需

指定 DCS 驅動程式單一登入用戶端的密碼。

此值必須與您在 RBPM 組態公用程式中為 **OSP 用戶端密碼**指定的值相符。如需詳細資訊，請參閱 「報告」 (第 220 頁)。

通訊協定

指定服務用戶端在與驗證伺服器通訊時，應使用 http (非安全) 通訊協定還是 https (安全) 通訊協定。

7 按一下 「**套用**」，然後按一下 「**確定**」。

8 (視情況而定) 如果您在部署驅動程式後變更了這些設定，則必須部署並重新啟動驅動程式。如需詳細資訊，請參閱第 19.2 節 「部署並啟動 Identity Reporting 的驅動程式」 (第 246 頁)。

9 對環境中的每個 DCS 驅動程式重複此程序。

19.2 部署並啟動 Identity Reporting 的驅動程式

Identity Reporting 需要以下驅動程式：

- Identity Manager Managed System Gateway Driver
- Identity Manager Driver for Data Collection Service

此程序包括以下活動：

- 第 19.2.1 節 「部署驅動程式」 (第 247 頁)
- 第 19.2.2 節 「驗證受管理系統是否正在運作中」 (第 247 頁)
- 第 19.2.3 節 「啟動 Identity Reporting 的驅動程式」 (第 249 頁)

如需安裝和設定這些驅動程式的詳細資訊，請參閱第 19.1 節 「設定 Identity Reporting 的驅動程式」 (第 241 頁)。

19.2.1 部署驅動程式

您必須為 Identity Reporting 部署兩個驅動程式。

1 在 Designer 中開啟您的專案。
2 在模型產生器或大綱檢視窗中，於您要部署的驅動程式集上按一下滑鼠右鍵。
3 選取即時 > 部署。
4 指定所選驅動程式的 Identity Vault 身分證明。

19.2.2 驗證受管理系統是否正在運作中

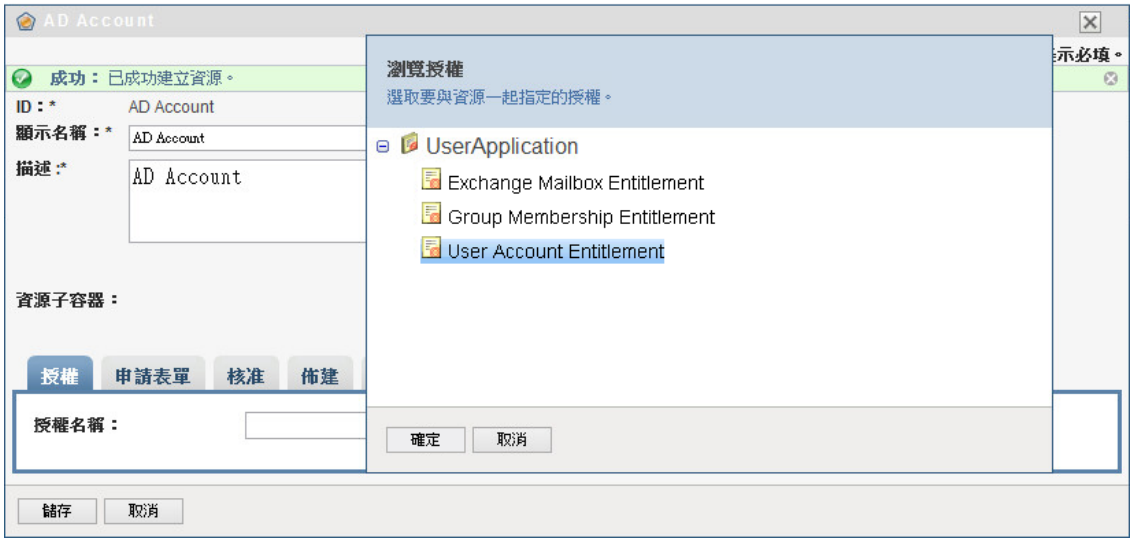
在啟動受管理系統閘道驅動程式和資料收集服務驅動程式之前，您應該確認基礎受管理系統是否已正確設定。此程序將會協助您排除環境中與報告驅動程式組態無關的問題。

例如，若要對 Active Directory 環境中的問題進行疑難排解，您可能需要透過在使用者應用程式中指定資源來測試某個 Active Directory 授權。

附註：如需 Active Directory 驅動程式的詳細資訊，請參閱 *《NetIQ Identity Manager Driver for Active Directory Implementation Guide》* (NetIQ Identity Manager Driver for Active Directory 執行指南)。

以下步驟示範了一種確認 Active Directory 是否已正確設定的方法：

1 確保使用者應用程式和 Identity Reporting 在同一伺服器上執行。
2 在 iManager 中，驗證使用者應用程式驅動程式及角色與資源服務驅動程式是否正在執行，然後確保受管理系統的驅動程式正在執行。
3 若要驗證使用者應用程式是否能夠從 Active Directory 擷取資訊，請以使用者應用程式管理員身分登入使用者應用程式。
4 在「資源目錄」中，為 Active Directory 帳戶建立一個新資源：
5 將該資源與 Active Directory 驅動程式中的某個授權相結合，例如使用者帳戶授權。



使用者應用程式可以從驅動程式擷取該授權。

6 由於這個特定的資源隸屬於帳戶，因此，請對該資源進行設定，以指定一個帳戶值。

7 選取該帳戶值，然後按一下新增。

8 建立另一個要指定群組的資源。

9 將該資源與適用於群組的授權相結合。具體而言，就是將這個特定的資源對應到群組成員資格授權。

10 設定此資源，讓使用者能夠在申請時指定授權值，並允許使用者為單個指定申請選取多個值。

11 驗證授權是否已成功建立。

此時，您可以看到，受管理系統 (本案例中為 Active Directory) 的基礎架構在正常運作。這可以協助您對以後可能出現的任何問題進行疑難排解。

19.2.3 啟動 Identity Reporting 的驅動程式

本節提供關於啟動受管理系統閘道驅動程式及資料收集服務驅動程式的指示。

1 開啟 iManager。

2 在受管理系統閘道驅動程式上按一下滑鼠右鍵，然後按一下**啟動驅動程式**。

3 在資料收集服務驅動程式上按一下滑鼠右鍵，然後按一下**啟動驅動程式**。

4 驅動程式啟動後，檢查主控台是否顯示了伺服器主控台中的額外資訊。例如：

```
21:22:56,399 INFO  [LogEvent] [DCS_Driver_Registration_Add] DCS Driver DN
TREE\novell\TestDrivers\Data Collection Service Driver; DCS-Report Driver
d44571a5708446bad65832481bb401d
```

5 以報告管理員身分登入 Identity Reporting。

6 在左側導覽窗格中，按一下**綜覽**。

7 驗證**組態**區段是否報告 Identity Vault 已設定。

8 在導覽窗格中，按一下 **Identity Vault**。

9 驗證「Identity Vault」頁面是否提供了關於資料收集服務驅動程式和受管理系統閘道驅動程式的詳細資料。受管理系統閘道驅動程式狀態應指出該驅動程式已啟始化。

此時，您可以查看身分資訊倉儲的內容，以詳細瞭解所儲存的關於 Identity Vault 的豐富資料，以及企業中的受管理系統。

10 若要檢視身分資訊倉儲中的資料，請使用諸如 PGAdmin for PostgreSQL 之類的資料庫管理工具來查看 SIEM 資料庫的內容。查看 SIEM 資料庫時，您應該會看到以下綱要：

idm_rpt_cfg

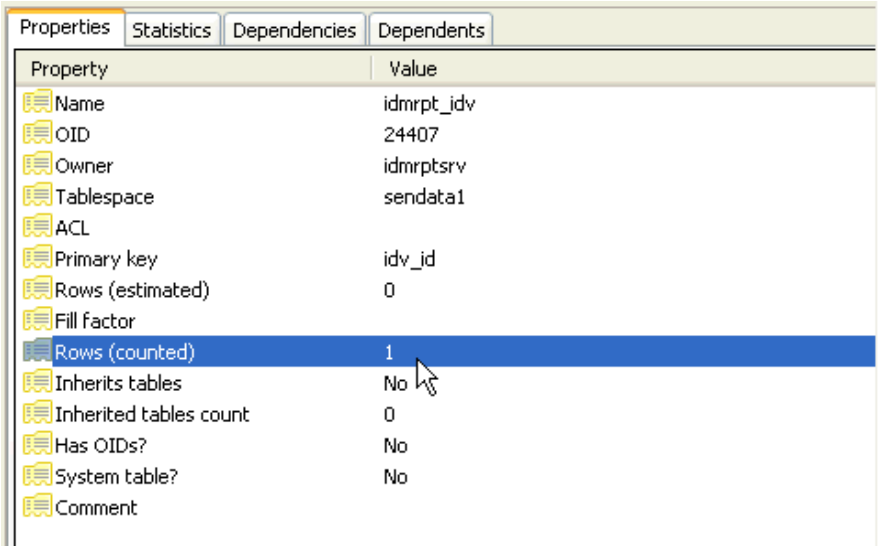
包含報告組態資料，例如報告定義和排程。Identity Reporting 的安裝程式會將此綱要新增至資料庫。

idm_rpt_data

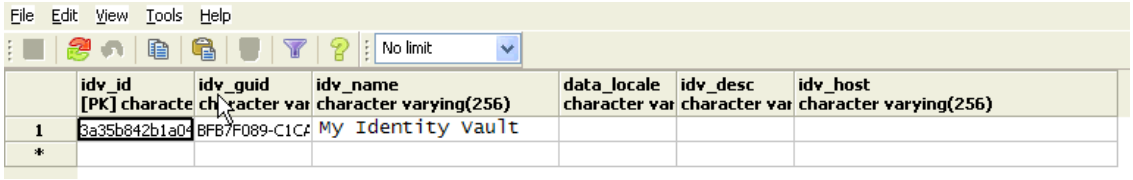
包含受管理系統閘道驅動程式和資料收集服務驅動程式所收集的資訊。Identity Reporting 的安裝程式會將此綱要新增至資料庫。

11 若要檢視驅動程式收集的資料，請展開 **idm_rpt_data > 表格 > idmrpt_idv**。

12 驗證新資料收集服務驅動程式的這個表格中是否已新增了一列：



13 驗證此表格的資料是否顯示了 Identity Vault 名稱：



如果您在此表格中看到了這個新列，則表示驅動程式註冊程序已成功。

19.3 設定執行時期環境

本節提供為確保執行時期環境正常運作，您應執行的一些額外組態步驟。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：

- 第 19.3.1 節「將資料收集服務驅動程式設定為從 Identity Applications 收集資料」(第 251 頁)
- 第 19.3.2 節「移轉資料收集服務驅動程式」(第 252 頁)
- 第 19.3.3 節「新增對自訂屬性和物件的支援」(第 254 頁)
- 第 19.3.4 節「新增多個驅動程式集支援」(第 256 頁)
- 第 19.3.5 節「將驅動程式設定為使用 SSL 在遠端模式下執行」(第 257 頁)

如果一或多個驅動程式出現了難以理解的問題，請參閱《Administrator Guide to NetIQ Identity Reporting》(NetIQ Identity Reporting 管理員指南) 中的「Troubleshooting」(疑難排解)。

19.3.1 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) 如果您的專案尚不包含資料收集服務驅動程式，請將該驅動程式輸入至您的專案。如需詳細資訊，請參閱第 15.6 章「建立和部署 Identity Applications 的驅動程式」(第 192 頁)。
4. (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：
   - **4a** 下載最新的 DCS 驅動程式修補程式檔案。
   - **4b** 將該修補程式檔案擷取到伺服器上的某個位置。
   - **4c** 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
     change this
     ```

   - **4d** 重新啟動 eDirectory。
   - **4e** 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，請參閱第 16.3 節「安裝 Identity Reporting 各元件的先決條件」(第 226 頁)。
   - **4f** 在 Designer 中重新部署並重新啟動 DCS 驅動程式。
5. 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**。
6. 按一下**驅動程式組態**。

7 按一下**驅動程式參數**索引標籤。

8 按一下**顯示連接參數**，然後選取**顯示**。

9 按一下 **SSO 服務支援**，然後選取**是**。

10 指定 Reporting Module 的 IP 位址和連接埠。

11 指定 SSO 服務用戶端的密碼。預設密碼為 driver。

12 按一下「**套用**」，然後按一下「**確定**」。

13 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**。

14 按一下**部署**。

15 收到重新啟動 DCS 驅動程式的提示時，按一下**是**。

16 按一下「**確定**」。

19.3.2 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 iManager。

2 在資料收集服務驅動程式的**綜覽**面板中，選取**從 Identity Vault 移轉**。

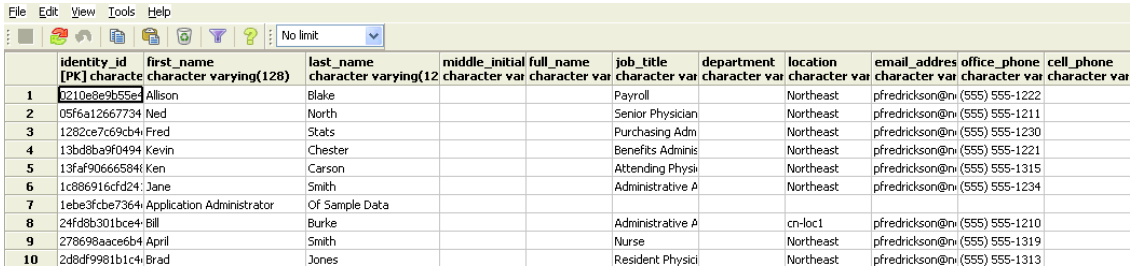
3 選取包含相關資料的組織，然後按一下**啟動**。

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。

---

4 等待移轉程序完成。

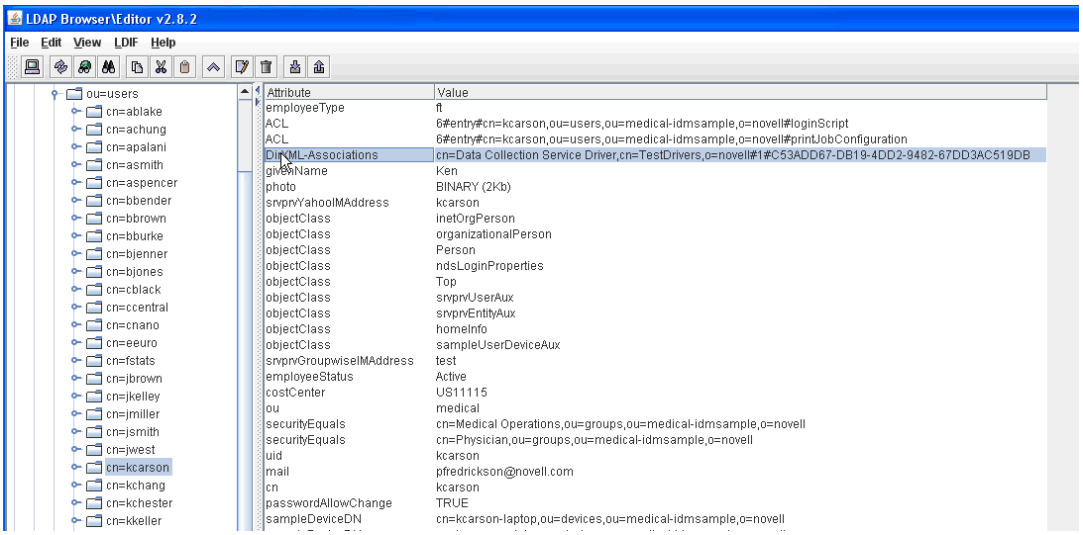
5 確保 **idmrpt_identity** 和 **idmrpt_acct** 表格 (提供關於 Identity Vault 中身分和帳戶的資訊) 中包含以下類型的資訊：



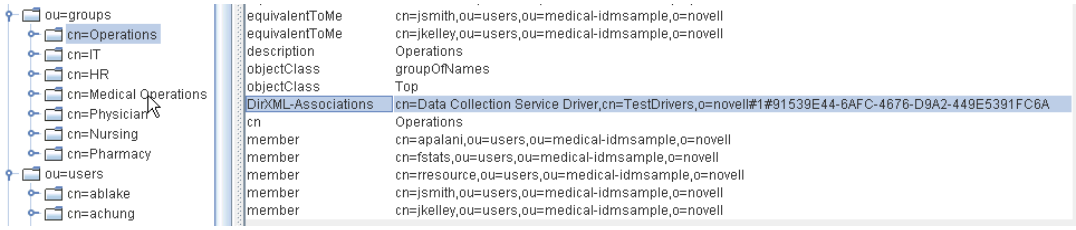
	identity_id [PK] characte	first_name character varying(128)	last_name character varying(12	middle_initial character var	full_name character var	job_title character var	department character var	location character var	email_addres character var	office_phone character var	cell_phone character var
1	0210e8e9b55e4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

6 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：



7 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 Operati	Medical Operati	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。

8 (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

9 (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。

19.3.3 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 254 頁)
- 「包含資料庫中的名稱和描述」(第 255 頁)
- 「將延伸屬性新增至已知物件類型」(第 255 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 (ldmrptIdentity.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。

19.3.4 新增多個驅動程式集支援

新的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。

  如果您還使用了資料收集服務驅動程式做為此次要伺服器上的主要驅動程式，該驅動程式將無法察覺到需要報告的物件變更。若要在此伺服器上設定資料收集服務驅動程式，請參閱第 19.1.3 節「設定資料收集服務的驅動程式」(第 243 頁)。
- **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。

19.3.5 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 iManager 中建立伺服器證書。
   - **1a** 在角色與任務檢視窗中，按一下 **NetIQ Certificate Server > 建立伺服器證書**。
   - **1b** 瀏覽到裝有受管理系統閘道驅動程式的伺服器物件並選取它。
   - **1c** 指定證書綽號。
   - **1d** 選取標準建立方法，然後按下一步。
   - **1e** 按一下「完成」，然後按一下「關閉」。
2. 使用 iManager 輸出伺服器證書。
   - **2a** 在角色與任務檢視窗中，按一下 **NetIQ 證書存取 > 伺服器證書**。
   - **2b** 選取步驟 1 (第 257 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 257 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 或更高版本。

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 iManager 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 **Identity Manager 綜覽**中，按一下包含受管理系統閘道驅動程式的驅動程式集。

4b 按一下驅動程式狀態圖示，然後選取**編輯內容 > 驅動程式組態**。

4c 將**顯示連接參數**設定為 true，並將**驅動程式組態模式**設定為「遠端」。

4d 輸入金鑰儲存區檔案的完整路徑和密碼。

4e 儲存驅動程式並將其重新啟動。

5 使用 iManager 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 **Identity Manager 綜覽**中，按一下包含受管理系統閘道驅動程式的驅動程式集。

5b 按一下驅動程式狀態圖示，然後選取**編輯內容 > 驅動程式組態**。

5c 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」。

5d 輸入金鑰儲存區的完整路徑、密碼以及在步驟 1c (第 257 頁) 中指定的別名。

5e 儲存驅動程式並將其重新啟動。

19.4 設定驅動程式的稽核旗標

本節概述了受管理系統閘道驅動程式和資料收集服務驅動程式的建議稽核設定。

- 第 19.4.1 節「在 Identity Manager 中設定稽核旗標」(第 258 頁)
- 第 19.4.2 節「在 eDirectory 中設定稽核旗標」(第 259 頁)

19.4.1 在 Identity Manager 中設定稽核旗標

NetIQ 建議您在 Identity Manager 中設定驅動程式的稽核旗標。這些旗標適用於 Novell 稽核 (不適用於 XDAS)。

若要在 iManager 中設定旗標，請移至**驅動程式集內容 > 記錄層級 > 記錄特定事件**。

類別	建議的旗標
Metadirectory 引擎事件	◆ Metadirectory 引擎警告
狀態事件	◆ 成功 附註：按使用者列出的關連資源指定事件報告需要「成功」旗標。如果您希望能夠執行此報告或其自訂版本，則需要啟用「成功」旗標。 ◆ 錯誤 ◆ 嚴重
操作事件	◆ 修改 ◆ 新增關聯 ◆ 檢查密碼 ◆ 新增值 ◆ 新增 ◆ 重新命名 ◆ 移除關聯 ◆ 檢查物件密碼 ◆ 清除屬性 ◆ 移除值 ◆ 取得具名密碼 ◆ 移除 ◆ 移動 ◆ 變更密碼 ◆ 新增值 (在 Modify 上) ◆ 重設屬性
轉換事件	◆ 密碼重設 ◆ 使用者代理程式申請 ◆ 密碼同步化
身分證明佈建事件	◆ 設定 SSO 身分證明 ◆ 清除 SSO 身分證明 ◆ 設定 SSO 通關密語

19.4.2 在 eDirectory 中設定稽核旗標

NetIQ 建議您在 eDirectory 中設定驅動程式的稽核旗標。這些旗標適用於 Novell 稽核 (不適用於 XDAS)。

若要在 iManager 中設定旗標，請移至 **eDirectory 稽核 > 稽核組態 > Novell 稽核**。

類別	建議的旗標
全域	◆ 不要傳送複製事件
中繼	◆ *(選取所有旗標)*
物件	◆ 新增內容 ◆ 允許登入 ◆ 變更密碼 ◆ 變更安全性等於 ◆ 建立 ◆ 刪除 ◆ 刪除內容 ◆ 登入 ◆ 登出 ◆ 修改 RDN ◆ 移動 (來源) ◆ 移動 (目的地) ◆ 移除 ◆ 重新命名 ◆ 還原 ◆ 搜尋 ◆ 驗證密碼
屬性	◆ *(選取所有旗標)*
代理程式	◆ DS 已重新載入 ◆ 本地代理程式已開啟 ◆ 本地代理程式已關閉 ◆ NLM 已載入
其他	◆ 產生 CA 金鑰 ◆ 已重新認證公用金鑰

類別	建議的旗標
LDAP	◆ LDAP 結合 ◆ LDAP 結合回應 ◆ LDAP 修改 ◆ LDAP 修改回應 ◆ LDAP 密碼修改 ◆ LDAP 取消結合 ◆ LDAP 刪除 ◆ LDAP 刪除回應 ◆ LDAP 修改 DN ◆ LDAP 修改 DN 回應 ◆ LDAP 搜尋 ◆ LDAP 搜尋回應 ◆ LDAP 新增 ◆ LDAP 新增回應

VI 安裝 Designer

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

重要：請確定包含 Designer 安裝程式的目錄名稱沒有空格。如果目錄名稱包含空格，則安裝 Designer 期間不會安裝 NICI。例如，目錄名稱不能是 Designer Install，但可以是 DesignerInstall。

NetIQ 建議您在開始之前檢閱安裝程序。如需詳細資訊，請參閱第 20 章 「規劃安裝 Designer」 (第 265 頁)。

20 規劃安裝 Designer

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

- 第 20.1 節「Designer 安裝核對清單」(第 265 頁)
- 第 20.2 節「安裝 Designer 的先決條件」(第 266 頁)
- 第 20.3 節「Designer 的系統要求」(第 266 頁)

20.1 Designer 安裝核對清單

NetIQ 建議您在開始安裝前先檢閱以下步驟：

	核對清單項目
❑	1. 檢閱產品架構資訊，以瞭解 Identity Manager 各元件之間的互動。如需詳細資訊，請參閱第 1 章「Identity Manager 的元件綜覽」(第 19 頁)。
❑	2. 確定要為 Identity Manager 的元件使用哪些伺服器。如需詳細資訊，請參閱第 5.3 節「建議的安裝情境和伺服器設定」(第 39 頁)。
❑	3. 檢閱關於安裝 Designer 的考量，以確保電腦符合先決條件。如需詳細資訊，請參閱第 20.2 節「安裝 Designer 的先決條件」(第 266 頁)。
❑	4. 確保您要安裝 Designer 的電腦符合指定的軟體和硬體要求。如需詳細資訊，請參閱第 20.3 節「Designer 的系統要求」(第 266 頁)。
❑	5. 若要安裝 Designer，請參閱下列其中一節： ◆「執行 Windows 可執行檔」(第 269 頁) ◆「使用靜默安裝程序」(第 269 頁)
❑	6. 安裝其餘的 Identity Manager 元件。
❑	7. (選擇性) 若要啟動 Identity Manager 解決方案的一個專案，請參閱 *《NetIQ Designer for Identity Manager Administration Guide》*(NetIQ Designer for Identity Manager 管理指南)。

20.2 安裝 Designer 的先決條件

本節提供關於安裝 Designer 的考量和系統要求。

在安裝或升級 Designer 之前，請檢閱以下考量：

- 在安裝 Designer 之前，必須先安裝 32 位元 Novell International Cryptographic Infrastructure (NICI) 套件。
- 您不能為 Designer 3.0 或更高版本使用 Designer 2.1*x* 工作空間，因為舊版工作空間與較新版本的 Designer 不相容。Designer 將專案和組態資訊儲存在**工作空間**中。例如，在 **Windows 10** 和 **Windows 7** 上，Designer 4.x 工作空間預設會安裝在 %UserProfile%\designer_workspace 目錄中。

20.3 Designer 的系統要求

本節提供要安裝 Designer 的伺服器的最低要求。請務必檢閱安裝的先決條件和注意事項，特別是與作業系統有關的內容。

類別	要求
處理器	1 GHz
磁碟空間	1 GB
記憶體	1 GB
作業系統 (已認證)	以下 64 位元作業系統之一 (最低版本)： **伺服器** ◆ Windows Server 2016 ◆ Windows Server 2012 R2 **桌面** ◆ Windows 10 ◆ Windows 8
作業系統 (受支援)	已認證作業系統的最新版 Service Pack **附註：***受支援*指作業系統尚未進行測試，但預期可正常運作。
虛擬化系統	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 及更新版本 ◆ 包含 Hyper-V 的 Windows Server 2012 R2 Virtualization (受支援) NetIQ 允許您在為執行 NetIQ 產品的作業系統提供官方支援的企業級虛擬化系統上執行 Identity Manager。只要虛擬化系統的廠商為這些作業系統提供官方支援，NetIQ 就支援在這些系統上執行整個 Identity Manager 堆疊。

類別	要求
網頁瀏覽器	以下任意瀏覽器 (最低版本)： ◆ Internet Explorer 11 ◆ Chrome 61 ◆ Firefox 51

21 安裝 Designer

您可以根據具體的目標電腦，使用可執行檔、二進位檔案或採用文字模式安裝 Identity Manager Designer。您還可以執行靜默安裝。使用預設位於 \products\Designer\ 目錄中的安裝程式：

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

- 第 21.1 節「執行 Windows 可執行檔」(第 269 頁)
- 第 21.2 節「使用靜默安裝程序」(第 269 頁)
- 第 21.3 節「修改包含空格字元的安裝路徑」(第 270 頁)

21.1 執行 Windows 可執行檔

1. 使用管理員帳戶登入要安裝 Designer 的電腦。
2. 從 NetIQ 下載網站下載 Identity_Manager_4.7_Windows_Designer.zip。
3. 擷取 Identity_Manager_4.7_Windows_Designer.zip 檔案。
4. 執行 install.exe 檔案。
5. 依照精靈中的步驟操作，直到安裝程序完成。

21.2 使用靜默安裝程序

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

1. 使用管理員帳戶登入您要安裝 Designer 的電腦。
2. 導覽至包含安裝程式的目錄。
3. (選擇性) 若要設定 Designer 的安裝目錄和語言，請完成以下步驟。

   3a 開啟 designerInstaller.properties 檔案 (預設位於 *Path_to_unzipped_Designer_file*\products\Designer 目錄中)。

   3b 在該 properties 檔案中，修改以下參數的值：

   USER_INSTALL_DIR

   指定 Designer 安裝位置的路徑。例如：

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

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

   SELECTED_DESIGNER_LOCALE

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

   - zh_CN - 簡體中文

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

3c 儲存並關閉該 properties 檔案。

4 執行下列其中一個指令：

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

21.3 修改包含空格字元的安裝路徑

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

將

```
C:\designer installation
```

變更為

```
C:\designer\ installation
```

VII 安裝 Analyzer

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

安裝檔案位於 Identity Manager 安裝套件 .iso 影像檔中的 \products\Analyzer 目錄內。依預設，安裝程式會在 C:\NetIQ\Analyzer 中安裝元件。

NetIQ 建議您在開始之前檢閱安裝程序。如需詳細資訊，請參閱第 22.1 節「Analyzer 的安裝核對清單」(第 273 頁)。

22 規劃安裝 Analyzer

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

- 第 22.1 節「Analyzer 的安裝核對清單」(第 273 頁)
- 第 22.2 節「安裝 Analyzer 的系統要求」(第 273 頁)

22.1 Analyzer 的安裝核對清單

NetIQ 建議您在開始安裝程序之前先檢閱以下步驟：

	核對清單項目
❑	1. 瞭解 Identity Manager 各元件之間的互動。如需詳細資訊，請參閱第 1 章「Identity Manager 的元件綜覽」(第 19 頁)。
❑	2. 確定要為 Identity Manager 的元件使用哪些伺服器。如需詳細資訊，請參閱第 5.3 節「建議的安裝情境和伺服器設定」(第 39 頁)。
❑	3. 確保您的環境符合代管 Analyzer 的考量和要求。如需詳細資訊，請參閱第 22.2 節「安裝 Analyzer 的系統要求」(第 273 頁)。
❑	4. 若要安裝 Analyzer，請參閱以下章節： ◆ 若要使用安裝精靈，請參閱第 23.1 節「使用精靈安裝 Analyzer」(第 275 頁)。 ◆ 若要執行靜默安裝，請參閱第 23.2 節「以靜默模式安裝 Analyzer」(第 276 頁)
❑	5. (選擇性) 若要自動接收和顯示來自 Analyzer 的稽核事件，請安裝 XDAS 用戶端。如需詳細資訊，請參閱第 23.3 節「安裝 Analyzer 的稽核用戶端」(第 276 頁)。
❑	6. 若要啟用 Analyzer，請參閱「啟用 Analyzer」(第 312 頁)。
❑	7. (選擇性) 若要升級 Analyzer，請參閱第 32.7 節「升級 Analyzer」(第 343 頁)。

22.2 安裝 Analyzer 的系統要求

本節提供要安裝 Analyzer 的伺服器的最低要求。請務必檢閱安裝的先決條件和注意事項，特別是與作業系統有關的內容。

類別	要求
處理器	1 GHz
記憶體	512 MB (建議 4 GB)
視訊解析度	1024*768 (建議 1280*1025)

類別	要求
作業系統 (已認證)	以下 64 位元作業系統之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 NetIQ 建議您在安裝 Identity Manager 之前，依照製造商的自動更新機制來套用最新的作業系統修補程式。 **附註：***已認證*指作業系統已進行全面測試且受支援。
作業系統 (受支援)	已認證作業系統的最新版 Service Pack **附註：***受支援*指作業系統尚未進行測試，但預期可正常運作。
虛擬化系統	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 及更新版本 NetIQ 允許您在為執行 NetIQ 產品的作業系統提供官方支援的企業級虛擬化系統上執行 Identity Manager。只要虛擬化系統的廠商為這些作業系統提供官方支援，NetIQ 就支援在這些系統上執行整個 Identity Manager 堆疊。

23 安裝 Analyzer

本章將引導您完成安裝 Analyzer 及設定其環境的程序。

- 第 23.1 節「使用精靈安裝 Analyzer」(第 275 頁)
- 第 23.2 節「以靜默模式安裝 Analyzer」(第 276 頁)
- 第 23.3 節「安裝 Analyzer 的稽核用戶端」(第 276 頁)

23.1 使用精靈安裝 Analyzer

以下程序介紹如何使用安裝精靈安裝 Analyzer。若要執行靜默模式的無人管理安裝，請參閱第 23.2 節「以靜默模式安裝 Analyzer」(第 276 頁)。

若要進行安裝準備工作，請檢閱第 22.1 節「Analyzer 的安裝核對清單」(第 273 頁) 中列出的先決條件和系統要求。

1 登入要安裝 Analyzer 的電腦。
2 (視情況而定) 如果您已取得 Identity Manager 安裝套件的 .iso 影像檔，請導覽至包含 Analyzer 安裝檔案的目錄 (預設為 \products\Analyzer 目錄)。
3 (視情況而定) 如果您已下載 Analyzer 安裝檔案，請完成以下步驟：
   - 3a 導覽至所下載影像的 win.zip 檔案。
   - 3b 將該檔案的內容擷取到本地電腦上的某個資料夾中。
4 從 \products\Analyzer 目錄執行 install.exe 安裝程式：
5 依照精靈中的指示操作，直到完成 Analyzer 的安裝。
6 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。
7 按一下「完成」。
8 (選擇性) 若要在 Windows 電腦上為 Analyzer 設定角色服務，請開啟 gettingstarted.html 網站的連結 (預設位於 C:\Program Files (x86)\NetIQ\Tomcat\webapp\nps\help\en\install 目錄中)。

   您可以使用 iManager 來設定角色服務。
9 若要啟用 Analyzer，請參閱「啟用 Analyzer」(第 312 頁)。

23.2 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。在此模式下，InstallAnywhere 會使用預設 analzerInstaller.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 Program Files (x86)\NetIQ\Analyzer 目錄中安裝 Analyzer。

1 登入要安裝 Analyzer 的電腦。
2 (視情況而定) 如果您已取得 Identity Manager 安裝套件的 .iso 影像檔，請導覽至包含 Analyzer 安裝檔案的目錄 (預設為 \products\Analyzer 目錄)。
3 (視情況而定) 如果您已從 NetIQ 下載網站下載了 Analyzer 安裝檔案，請完成以下步驟：
   - **3a** 導覽至所下載影像的 win.zip 檔案。
   - **3b** 將該檔案的內容擷取到本地電腦上的某個資料夾中。
4 (選擇性) 若要指定非預設安裝路徑，請完成以下步驟：
   - **4a** 開啟預設位於 \products\Analyzer 目錄中的 analzerInstaller.properties 檔案。
   - **4b** 將以下文字新增至該 properties 檔案中：

     USER_INSTALL_DIR=*installation_path*
5 若要執行靜默安裝，請執行以下指令：

   install.exe -i silent -f analyzerInstaller.properties
6 若要啟用 Analyzer，請參閱 「啟用 Analyzer」(第 312 頁)。

23.3 安裝 Analyzer 的稽核用戶端

Analyzer 包含一個 XDAS 程式庫，當您向應用程式傳回資料更新時，該程式庫會自動產生來自「資料瀏覽器」編輯器的稽核事件。如需關於在來源應用程式中使用「資料瀏覽器」編輯器更新資料的詳細資訊，請參閱《*NetIQ Analyzer for Identity Manager Administration Guide*》(NetIQ Analyzer for Identity Manager 管理指南) 中的「Modifying Data」(修改資料)。

若要檢視這些稽核事件，請安裝可從 Analyzer 接收稽核事件的 XDAS 用戶端。「OpenXDAS Project」(OpenXDAS 專案) (http://openxdas.sourceforge.net) 中提供了關於 XDAS 的詳細資訊。

Analyzer 的下載套件中包含 Windows 版 XDAS 用戶端。不過，Analyzer 的安裝程式不會安裝 XDAS 用戶端。

1 安裝 Analyzer。
2 導覽至 OpenXDAS 安裝檔案。依預設，這些檔案位於 .iso 影像檔的 \products\Analyzer\openxdas\ *作業系統*目錄中。
3 啟動 XDAS 用戶端的安裝程式 (.msi 檔案)：
4 依照提示安裝 XDAS 用戶端。
5 安裝程序完成後，啟動 XDAS 用戶端，以自動接收並顯示來自 Analyzer 的稽核事件。

VIII 在 Identity Manager 中設定單一登入存取

依預設，Identity Manager 使用 OSP 提供 Identity Manager 中的單一登入存取。安裝 Identity Reporting 和 Identity Applications 時，您可以指定使用者驗證的基本設定。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 IDP 的驗證。例如，您可以使用 SAML 支援來自 NetIQ Access Manager 的驗證。如需 OSP 的詳細資訊，請參閱第 4.5 節「在 Identity Manager 中使用單一登入存取」(第 33 頁)。

24 準備單一登入存取

依預設，Identity Manager 使用 OSP 提供 Identity Manager 中的單一登入存取。安裝 Identity Reporting 和 Identity Applications 時，您可以指定使用者驗證的基本設定。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 IDP 的驗證。例如，您可以使用 SAML 支援來自 NetIQ Access Manager 的驗證。

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 Identity Manager 如何使用 OSP 提供單一登入存取。如需詳細資訊，請參閱第 4.5 節「在 Identity Manager 中使用單一登入存取」(第 33 頁)。
❑	2. 安裝 OSP。如需詳細資訊，請參閱第 14 部分「安裝密碼管理元件」(第 155 頁)。
❑	3. 安裝 Identity Applications。如需詳細資訊，請參閱第 IV 部分「安裝 Identity Applications」(第 139 頁)。
❑	4. (選擇性) 安裝 Identity Reporting。如需詳細資訊，請參閱第 V 部分「安裝 Identity Reporting」(第 223 頁)。
❑	5. 將 Identity Applications 設定為使用 OSP 進行單一登入存取。如需詳細資訊，請參閱第 25 章「在 Identity Manager 中使用 One SSO Provider 進行單一登入存取」(第 281 頁)。
❑	6. 安裝您要用於 Identity Manager 的驗證系統。例如 Access Manager 或 Kerberos。
❑	7. (視情況而定) 設定 Access Manager 和 OSP。如需詳細資訊，請參閱第 26 章「對 NetIQ Access Manager 使用 SAML 驗證進行單一登入」(第 283 頁)。
❑	8. 驗證單一登入設定。如需詳細資訊，請參閱第 28 章「驗證是否可對 Identity Applications 進行單一登入存取」(第 293 頁)。

25 在 Identity Manager 中使用 One SSO Provider 進行單一登入存取

若要提供對 Identity Applications 的單一登入存取，您必須在 RBPM 組態公用程式中完成一些設定。您應該事先準備好在安裝 OSP 後進行單一登入所需的證書和金鑰。

此程序假設您的環境將為 eDirectory、SSO 控制器和 OAuth 提供程式使用一個證書。如果您的組織需要更多分離層，請單獨為 OAuth 提供程式建立一個證書。

25.1 準備 eDirectory 以支援單一登入存取

在安裝 eDirectory 的過程中，您必須設定 Identity Vault，以支援對 Identity Applications 和 Identity Reporting 進行單一登入存取。

執行第 15.7.5 節「設定 Identity Applications 的 Identity Vault」(第 196 頁)中所述的步驟。如果您先前已將 eDirectory 綱要延伸為包含 SAML 綱要，並安裝了所需的 NMAS 方法，則不需要再次執行這些步驟，可以直接跳至建立可信根容器的小節。

25.2 修改單一登入存取的基本設定

在安裝 Identity Applications 時，您通常需要設定單一登入存取的基本設定。本節的內容可協助您確保這些設定適合您的環境。

1 執行 RBPM 組態公用程式。如需詳細資訊，請參閱第 15.8.1 節「執行 Identity Applications 組態公用程式」(第 204 頁)。

2 若要修改驗證設定，請完成以下步驟：

   2a 按一下**驗證**。

   2b (視情況而定) 若要指定實際的伺服器 DNS 名稱或 IP 位址，請變更 localhost 的所有例項。

   - 指定的位址必須能夠由所有用戶端解析。僅當對 Identity Manager 的所有存取 (包括透過瀏覽器存取) 都是從本地進行時，才應使用 localhost。
   - 此「公用」主機名稱或 IP 位址應該與您在安裝 OSP 時指定的 *PublicServerName* 值相同。如需詳細資訊，請參閱第 14.2 章 「為 Identity Manager 安裝密碼管理功能」(第 157 頁)。
   - 在分散式環境或叢集環境中，所有的 OAuth URL 值都應該相同。該 URL 應該透過 L4 交換器或負載平衡器協助實現用戶端存取。此外，必須在環境中的每個部署上安裝 osp.war 和組態檔案。

   2c 對於**管理員容器的 LDAP DN**，請按一下**瀏覽**按鈕，然後選取 Identity Vault 中包含 Identity Applications 管理員的容器。

2d 指定您在安裝 OSP 時建立的 OAuth 金鑰儲存區檔案。如需詳細資訊，請參閱第 14.2 章「為 Identity Manager 安裝密碼管理功能」(第 157 頁)。

請包含金鑰儲存區檔案路徑、金鑰儲存區檔案密碼、金鑰別名和金鑰密碼。預設的金鑰儲存區檔案為 osp.jks，預設的金鑰別名為 osp。

3 若要修改單一登入設定，請完成以下步驟：

3a 按一下 **SSO 用戶端**。

3b (視情況而定) 若要指定實際的伺服器 DNS 名稱或 IP 位址，請變更 localhost 的所有例項。

- 指定的位址必須能夠由所有用戶端解析。僅當對儀表板的所有存取 (包括透過瀏覽器的存取) 都將在本地進行時，才應使用 localhost。
- 此「公用」主機名稱或 IP 位址應該與您在安裝 OSP 時指定的 *PublicServerName* 值相同。如需詳細資訊，請參閱第 14.2 章「為 Identity Manager 安裝密碼管理功能」(第 157 頁)。
- 在分散式環境或叢集環境中，所有的 OAuth 重新導向 URL 值都應該相同。該 URL 應該透過 L4 交換器或負載平衡器協助實現用戶端存取。

3c (視情況而定) 如果使用非預設連接埠，請更新以下 Identity Manager 元件的連接埠號：

- Identity Applications 管理
- Identity Manager 儀表板
- Identity Reporting
- 使用者應用程式

4 按一下**確定**儲存所做的變更，然後關閉組態公用程式。

5 啟動 Tomcat。

25.3 將 Self Service Password Reset 設定為信任 OSP

為了使單一登入功能正常運作，您必須使用證書在 OSP 與 Self Service Password Reset (SSPR) 之間設定信任關係。您必須從 OSP 的金鑰儲存區檔案 osp.jks 中輸出證書。

輸出證書後，必須將它輸入至 SSPR 的金鑰儲存區檔案。SSPR 的預設金鑰儲存區檔案路徑為 C:\[Java_Home]\lib\security\cacerts。

如需設定安全通道的詳細資訊，請參閱《Self Service Password Reset Administration Guide》(Self Service Password Reset 管理指南) 中的「Setting Up a Secure Channel Between the Application Server and the LDAP Server」(在應用程式伺服器與 LDAP 伺服器之間設定安全通道)。

26 對 NetIQ Access Manager 使用 SAML 驗證進行單一登入

本章的內容可協助您設定 NetIQ Access Manager 和 OSP，以支援在 Identity Manager 中使用 SAML 2.0 驗證進行單一登入存取。在開始之前，請檢閱操作指示所依據的以下假設：

- 您已安裝新的受支援 Access Manager 版本。
- 您已安裝 Identity Manager 的新版本。
- 這兩項安裝的主機名稱組態都使用了 DNS 名稱。
- 這兩項安裝都使用 SSL 通訊協定進行通訊。
- 您必須為 Access Manager 設定一個使用 Identity Vault 做為 LDAP 使用者儲存區的叢集環境。如需詳細資訊，請參閱 《*NetIQ Access Manager Administration Guide*》 (NetIQ Access Manager 管理指南)。

26.1 瞭解協力廠商驗證和單一登入

您可以將 Identity Manager 設定為使用 SAML 2.0 驗證來與 NetIQ Access Manager 配合運作。憑藉此項功能，您可以使用密碼以外的技術，透過 Access Manager 登入 Identity Applications。例如，使用者可以透過使用者 (用戶端) 證書登入，例如用智慧卡登入。

Access Manager 會與 OSP 互動，以將使用者與 Identity Vault 中的 DN 對應。當使用者透過 Access Manager 登入 Identity Applications 時，Access Manager 可在 HTTP 標題中插入一個 SAML 宣示 (使用使用者的 DN 做為識別碼)，並將要求轉遞到 Identity Applications。Identity Applications 使用該 SAML 宣示來與 Identity Vault 建立 LDAP 連接。

當使用 SAML 宣示進行 Identity Applications 驗證時，允許基於密碼之單一登入驗證的附屬入口網站應用程式將不支援單一登入。

26.2 建立和安裝 SSL 證書

為了確保驗證順利完成，Access Manager 和 OSP 必須共享其 SSL 證書的可信根。本節的內容可協助您為 Access Manager 建立新證書，並確保可信證書儲存區包含正確的證書。

- 第 26.2.1 節「為 Access Manager 建立 SSL 證書」(第 284 頁)
- 第 26.2.2 節「在 Identity Manager 可信證書儲存區中安裝 Access Manager 證書」(第 284 頁)
- 第 26.2.3 節「在 Access Manager 可信證書儲存區中安裝 SSL 伺服器證書」(第 285 頁)

26.2.1 為 Access Manager 建立 SSL 證書

Access Manager 無法使用其預設 SSL 證書 test-connector 來與 Identity Manager 通訊。您必須建立一個證書標題欄位中包含主機名稱的證書，並將它指定給 Access Manager。

如需詳細資訊，請參閱《*NetIQ Access Manager Administration Console Guide*》(NetIQ Access Manager 管理主控台指南) 中的「Security and Certificate Management」(安全性和證書管理)。

1 開啟 Access Manager 的管理主控台。
2 按一下**安全性 > 證書**。
3 按一下「**新增**」。
4 指定新證書的名稱。例如 *hostname*_ssl。
5 按一下視窗右側的編輯按鈕。
6 對於**公用名稱**，請指定代管 Access Manager 之伺服器的 DNS 名稱，然後按一下**確定**。
7 對於**有效月數**，請指定不超過 99 的值。
8 對於**金鑰大小**，請指定 2048。
9 選取新建立的證書，然後按一下**動作 > 將證書新增至金鑰儲存區 ...**。
10 按一下**金鑰儲存區**右側的編輯按鈕。
11 選取 **SSL 連接器**，然後按一下**確定**。
12 按一下「**確定**」。
13 在 OSP 可信證書儲存區中安裝新證書。如需詳細資訊，請參閱第 26.2.2 節「在 Identity Manager 可信證書儲存區中安裝 Access Manager 證書」(第 284 頁)。

26.2.2 在 Identity Manager 可信證書儲存區中安裝 Access Manager 證書

OSP 可信證書儲存區必須包含 Access Manager 的安全性證書。

1 若要輸出新 SSL 證書，請完成以下動作：
   - 在 Access Manager 管理主控台的**安全性** > **可信的根**下，輸出 SSL 證書的根證書。將根證書命名為 **configCA**。
   - 輸出 SSL 伺服器證書。

     如需詳細資訊，請參閱《*NetIQ Access Manager Administration Console Guide*》(NetIQ Access Manager 管理主控台指南) 中的「Managing Trusted Roots and Trust Stores」(管理可信的根和可信證書儲存區)。
2 將輸出的證書複製到執行 OSP 的伺服器上。
3 使用 Java 隨附的 keytool 將該檔案輸入到 JRE 的 cacerts 金鑰儲存區中。

   例如，C:\NetIQ\idm\apps\jre\bin\keytool -importcert -trustcacerts -alias <NAM-cert> -keystore C:\NetIQ\idm\apps\jre\bin\security\cacerts -storepass <password> -file custom_location\<exported_file>
4 在 Access Manager 可信證書儲存區中安裝 OSP 證書。

   如需詳細資訊，請參閱第 26.2.3 節「在 Access Manager 可信證書儲存區中安裝 SSL 伺服器證書」(第 285 頁)。

26.2.3 在 Access Manager 可信證書儲存區中安裝 SSL 伺服器證書

Access Manager 可信證書儲存區必須包含 OSP 的安全性證書。如需詳細資訊，請參閱《*NetIQ Access Manager Administration Console Guide*》(NetIQ Access Manager 管理主控台指南) 中的「Managing Trusted Roots and Trust Stores」(管理可信的根和可信證書儲存區)。

獲取執行 OSP 的 Tomcat 例項要用於 SSL 的伺服器證書。

1 將代管 OSP 之 Tomcat 例項的 SSL 伺服器證書複製到安裝了 Access Manager 的伺服器上。
2 開啟 Access Manager 的管理主控台。
3 若要輸入證書，請按一下**安全性 > NIDP 可信證書儲存區**。
4 按一下**新增**。
5 從**新增**對話方塊 > **輸入**中選取「可信的根」。
6 選取要輸入的根證書，然後按一下**確定**。
7 確保 OSP 能夠識別來自 SAML 的驗證宣示。

   如需詳細資訊，請參閱第 26.4.2 節「建立 SAML 的屬性集」(第 286 頁)。

26.3 將 Identity Manager 設定為信任 Access Manager

對於驗證要求，Identity Manager 需要使用 SAML 中繼資料的 URL 來重新導向使用者。依預設，Access Manager 使用以下 URL 來儲存 SAML 中繼資料：

`https://server:port/nidp/saml2/metadata`

其中，*server*:*port* 代表 Access Manager 身分伺服器。

1 (選擇性) 若要檢視 SAML 中繼資料的 .xml 文件，請在瀏覽器中開啟該 URL。

   如果該 URL 未產生文件，請確保連結正確無誤。
2 在 OSP 伺服器上，執行 RBPM 組態公用程式。如需詳細資訊，請參閱第 15.8.1 節「執行 Identity Applications 組態公用程式」(第 204 頁)。
3 在公用程式中選取**驗證**。
4 對於**驗證方法**，請指定 **SAML 2.0**。
5 對於**中繼資料 URL**，請指定 OSP 用於將驗證要求重新導向到 Access Manager 之 SAML 中繼資料的 URL。

   例如 https://*server*:*port*/nidp/saml2/metadata
6 在**驗證伺服器**區段中的 **OAuth 伺服器主機識別碼**設定內，指定代管 OSP 之伺服器的 DNS 名稱。
7 按一下「**確定**」儲存變更。
8 重新啟動代管 OSP 的 Tomcat 例項。

26.4 將 Access Manager 設定為與 Identity Manager 配合運作

為了確保讓 Access Manager 將 Identity Manager 識別為可信的服務提供者，請將 OSP 的中繼資料文字新增至身分伺服器，並設定一個屬性集。此程序包括以下活動：

- 第 26.4.1 節「複製 Identity Manager 的中繼資料」(第 286 頁)
- 第 26.4.2 節「建立 SAML 的屬性集」(第 286 頁)
- 第 26.4.3 節「將 Identity Manager 新增為可信的服務提供者」(第 287 頁)

26.4.1 複製 Identity Manager 的中繼資料

Access Manager 需要 OSP 的中繼資料文字。您應該將中繼資料 .xml 檔案的內容複製到可在 Access Manager 身分伺服器上開啟的文件中。

1. 在瀏覽器中，導覽至 OSP 中繼資料的 URL。依預設，Identity Manager 使用以下 URL：

   `https://server:port/osp/a/idm/auth/saml2/spmetadata`

   其中，*server*:*port* 代表代管 OSP 的 Tomcat 伺服器。
2. 檢視 spmetadata.xml 檔案的頁面來源。
3. 將該檔案的內容複製到可在「將 Identity Manager 新增為可信的服務提供者」(第 287 頁) 中存取的文件中。

26.4.2 建立 SAML 的屬性集

為了確保 SAML 能夠在 Access Manager 與 OSP 之間執行宣示交換，請在 Access Manager 中建立一個屬性集。屬性集為交換提供通用命名規劃。OSP 會尋找用於識別宣示標題的屬性值。依預設，該屬性為 mail。

如需詳細資訊，請參閱《*NetIQ Access Manager Administration Guide*》(NetIQ Access Manager 管理指南) 中的「Configuring Attribute Sets」(設定屬性集)。

1. 開啟 Access Manager 的管理主控台。
2. 按一下**裝置 > 身分伺服器 > 共享設定 > 屬性集 > 新增**。
3. 指定屬性集的名稱。例如 IDM SAML Attributes。
4. 按**下一步**，然後按一下**新增**。
5. 對於**本地屬性**，請選取 **Ldap 屬性：mail [LDAP 屬性設定檔]**。
6. 對於**遠端屬性**，請指定 mail。
7. 按一下**確定**，然後按一下**完成**。

26.4.3 將 Identity Manager 新增為可信的服務提供者

設定 Access Manager，以將 Identity Manager 識別為可信的服務提供者。如需詳細資訊，請參閱《*NetIQ Access Manager Administration Guide*》(NetIQ Access Manager 管理指南) 中的「Creating a Trusted Service Provider for SAML 2.0」(為 SAML 2.0 建立可信的服務提供者)。

1 開啟 Access Manager 的管理主控台。
2 按一下**裝置 > 身分伺服器 > 編輯 > SAML 2.0**。
3 按一下**新增 > 服務提供者**。
4 對於**提供者類型**，請指定**一般**。
5 對於**來源**，請指定**中繼資料文字**。
6 在**文字**欄位中，貼上您在「複製 Identity Manager 的中繼資料」(第 286 頁) 中複製的 spmetadata.xml 檔案內容。
7 指定新 OSP 服務提供者的名稱。
8 按**下一步**，然後按一下**完成**。
9 在 **SAML 2.0** 索引標籤上，選取您在**步驟 7** 中建立的 OSP 服務提供者。
10 按一下**屬性**。
11 選取您在「建立 SAML 的屬性集」(第 286 頁) 中建立的屬性集。例如 IDM SAML Attributes。
12 將可用於 OSP 服務提供者集的屬性移至頁面左側的**驗證時傳送**面板中。

   移至**驗證時傳送**面板中的屬性是您要在驗證期間取得的屬性。
13 按兩次**確定**。
14 若要更新身分伺服器，請按一下**裝置 > 身分伺服器 > 更新 > 更新所有組態**。

26.5 更新 Access Manager 的登入頁面

Access Manager 的預設登入頁面使用 HTML iFrame 元素，這些元素與用於 Identity Applications 的元素相衝突。本節說明如何透過建立 Access Manager 的新登入方法和合約，來消除該衝突。本節提到的 .jsp 檔案預設位於 C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp 目錄中。

如需詳細資訊，請參閱《*NetIQ Access Manager Administration Guide*》(NetIQ Access Manager 管理指南) 中的「Customizing the Identity Server Login Page」(自訂身分伺服器登入頁面)。

1 依照 TID 7004020 和 TID 7018468 的內容修改 top.jsp 檔案。
2 (選擇性) 為進行備份，請複製並重新命名 login.jsp 檔案。例如，將其重新命名為 idm_login.jsp。
3 開啟 Access Manager 的管理主控台。
4 若要建立新的登入方法，請完成以下步驟：
   - **4a** 按一下**裝置 > 身分伺服器 > 編輯 > 本地 > 方法**。
   - **4b** 按一下**新增**，然後指定新方法的**顯示名稱**。例如 IDM Name/Password。
   - **4c** 對於**類別**，請指定 **Name/Password-Form**。
   - **4d** 對於**使用者儲存區**，請指定「Identity Vault」做為 LDAP 使用者儲存區。

4e 在內容區段中按一下新增，然後指定以下內容：

名稱	數值
JSP	idm_login
MainJSP	true

4f 按一下「確定」。

5 若要建立使用新登入方法的合約，請完成以下步驟：

5a 按一下合約 > 新增。

5b 在組態索引標籤中，指定新合約的顯示名稱。例如 IDM Name/Password。

5c 對於 **URI**，請指定 name/password/uri/idm。

5d 於方法下新增您在步驟 4 中建立的方法。例如 IDM Name/Password。

5e 在驗證卡索引標籤中，指定卡的 **ID**。例如 IDM_NamePassword。

5f 指定卡的影像。

5g 按一下「確定」。

6 若要指定系統處理新驗證合約方式的預設值，請完成以下步驟：

6a 在本地索引標籤上，按一下預設值。

6b 對於「使用者儲存區」，請指定「Identity Vault」做為 LDAP 使用者儲存區。

6c 對於驗證合約，請指定您在步驟 5 中建立的合約。例如 IDM Name/Password-Form。

6d 按一下「確定」。

7 若要更新身分伺服器，請按一下裝置 > 身分伺服器 > 更新 > 更新所有組態。

27 使用 Kerberos 進行單一登入

對於允許單一登入 (SSO) 的 Identity Applications，您可以使用 Kerberos 做為驗證方法。Kerberos 還允許使用者使用整合式 Windows 驗證登入應用程式。本章提供了設定 Active Directory 以使用 Kerberos 連接到 Identity Applications 的說明：

- 第 27.1 節「在 Active Directory 中設定 Kerberos 使用者帳戶」(第 289 頁)
- 第 27.2 節「設定 Identity Applications 伺服器」(第 290 頁)
- 第 27.3 節「將最終使用者瀏覽器設定為使用整合式 Windows 驗證」(第 292 頁)

27.1 在 Active Directory 中設定 Kerberos 使用者帳戶

請使用 Active Directory 管理工具來對 Kerberos 驗證設定 Active Directory。您需要為 Identity Applications 和 Identity Reporting 建立新的 Active Directory 使用者帳戶。該使用者帳戶名稱必須使用代管 Identity Applications 和 Identity Reporting 的伺服器的 DNS 名稱。

附註：對於網域或領域參考，請使用大寫格式。例如 @MYCOMPANY.COM。

---

1 以 Active Director 中的管理員身分，使用 Microsoft Management Console (MMC) 建立一個包含 Identity Applications 所在伺服器 DNS 名稱的新使用者帳戶。

   例如，如果 Identity Applications 伺服器的 DNS 名稱為 rbpm.mycompany.com，則可以使用以下資訊來建立使用者：

   名：rbpm

   使用者登入名稱：HTTP/rbpm.mycompany.com

   載入 Windows 前的登入名稱：rbpm

   設定密碼：指定相應的密碼。例如：Passw0rd。

   密碼永不過期：選取此選項。

   使用者必須在下次登入時變更密碼：不要選取此選項。

2 將新使用者與服務主體名稱 (SPN) 相關聯。

   2a 在 Active Directory 伺服器中開啟一個 cmd 外圍程序。

   2b 在指令提示符處，輸入以下指令：

   ```
   setspn -A HTTP/DNS_Identity_Applications_server@WINDOWS-DOMAIN userID
   ```

   例如：

   ```
   setspn -A HTTP/rbpm.mycompany.com@MYCOMPANY.COM rbpm
   ```

   2c 輸入 setspn -L *使用者 ID* 以驗證 setspn。

3 若要產生 keytab 檔案，請使用 ktpass 公用程式：

   3a 在指令行提示符處，輸入以下指令：

```
ktpass /out filename.keytab /princ servicePrincipalName /mapuser userPrincipalName /mapop
set /pass password /crypto ALL /ptype KRB5_NT_PRINCIPAL
```

例如：

```
ktpass /out rbpm.keytab /princ HTTP/rbpm.mycompany.com@MYCOMPANY.COM /mapuser rbpm  /mapop set
/pass Passw0rd /crypto All /ptype KRB5_NT_PRINCIPAL
```

重要：對於網域或領域參考，請使用大寫格式。例如，@MYCOMPANY.COM。

3b 將 rbpm.keytab 檔案複製到 Identity Applications 伺服器中。

4 以 Active Directory 中的管理員身分使用 MCC 建立一個最終使用者帳戶，以便為 SSO 做好準備。

若要支援單一登入，該終端使用者帳戶名稱必須與 eDirectory 使用者的某個屬性值相符。建立名稱類似於 cnano 的使用者，記住密碼，並確保不要選取**使用者必須在下次登入時變更密碼**。

5 (選擇性) 如果您已將報告元件安裝在單獨的伺服器上，請對 Identity Reporting 重複這些步驟。

6 將 Identity Applications 的伺服器設定為接受 Kerberos 組態。如需詳細資訊，請參閱第 27.2 節「設定 Identity Applications 伺服器」(第 290 頁)。

27.2 設定 Identity Applications 伺服器

您必須對 Identity Applications 伺服器進行設定，讓其使用您在 Active Directory 中建立的 Kerberos keytab 檔案和使用者帳戶。在繼續下一步之前，請務必完成第 27.1 節「在 Active Directory 中設定 Kerberos 使用者帳戶」(第 289 頁)中的操作。

附註：對於網域或領域參考，請使用大寫格式。例如 @MYCOMPANY.COM。

1 若要定義 Kerberos 組態的作業系統設定，請完成以下步驟：

1a 在代管 Identity Applications 的伺服器上的文字編輯器中，開啟 C:\Windows\krb5.ini 中的 krb5 檔案。

1b 將以下資訊新增至 krb5 檔案：

```
[libdefaults]
    default_realm = WINDOWS-DOMAIN
    kdc_timesync = 0
    forwardable = true
    proxiable = false
[realms]
    WINDOWS-DOMAIN = {
         kdc = FQDN Active Directory Server
         admin_server = FQDN Active  Directory Server
    }
[domain_realm]
    .your.domain = WINDOWS-DOMAIN
    your.domain = WINDOWS-DOMAIN
```

例如：

```
[libdefaults]
    default_realm = MYCOMPANY.COM
    kdc_timesync = 0
    forwardable = true
    proxiable = false
[realms]
    MYCOMPANY.COM = {
         kdc = myadserver.mycompany.com
         admin_server = myadserver.mycompany.com
    }
[domain_realm]
    .mycompany.com = MYCOMPANY.COM
    mycompany.com = MYCOMPANY.COM
```

1c 儲存變更並關閉 krb5 檔案。

2 (視情況而定) 若要定義 Tomcat 的 Kerberos 組態資訊，請完成以下步驟：

2a 在 Tomcat 應用程式伺服器上，建立包含以下內容的範例 Kerberos_login.config 檔案：

附註：novlua 使用者需要相應的許可權才能建立 Kerberos_login.config 檔案。

```
com.sun.security.jgss.krb5.accept {
    com.sun.security.auth.module.Krb5LoginModule required
    debug="true"
    refreshKrb5Config="true"
    useTicketCache="true"
ticketCache="c:\NetIQ\idm\apps\tomcat\kerberos\spnegoTicket.cache"
    doNotPrompt="true"
        principal="HTTP/DNS_Identity_Applications_server@WINDOWS-DOMAIN
"
    useKeyTab="true"
        keyTab="/absolute_path/filename.keytab"
    storeKey="true";
    };
```

Windows 伺服器上的範例如下所示：

```
keyTab="c:\\NetIQ\\idm\\apps\\tomcat\kerberos\\rbpm.keytab"
```

2b 在該檔案中為 principal 和 keyTab 指定值。例如：

```
principal="HTTP/rbpm.mycompany.com@MYCOMPANY.COM"
keyTab="/home/usr/rbpm.keytab"
```

- principal 的值必須與您為 Kerberos 指定的值相符。如需詳細資訊，請參閱步驟 3 (第 289 頁)。
- 提供 Identity Applications 伺服器上 keytab 檔案的絕對路徑。該檔案不一定位於 Identity Applications 的預設目錄中。

2c 使用以下指令行在 JVM java.security 檔案中參考 Kerberos_login.config 檔案：

```
login.config.url.1=file:c:\NetIQ\idm\apps\tomcat\kerberos\Kerberos_login.config
```

3 若要在 RBPM 組態公用程式中指定驗證方法，請完成以下步驟：

3a 開啟 Configupdate 公用程式。

3b 按一下**驗證**索引標籤。

3c 向下捲動至**驗證方法**區段。

3d 在方法欄位中，選取 **Kerberos**。

3e 在對應屬性名稱欄位中，指定 cn。

附註：如需 RBPM 組態公用程式的詳細資訊，請參閱第 15.8 章 「完成 Identity Applications 的設定」(第 204 頁)。

---

4 (選擇性) 如果您已將報告元件安裝在單獨的伺服器上，請對 Identity Reporting 重複這些步驟。

5 設定最終使用者用於存取 Identity Applications 的瀏覽器。如需詳細資訊，請參閱第 27.3 節 「將最終使用者瀏覽器設定為使用整合式 Windows 驗證」(第 292 頁)。

27.3 將最終使用者瀏覽器設定為使用整合式 Windows 驗證

最終使用者用於存取 Identity Applications 和 Identity Reporting 的瀏覽器也需要設定為使用整合式 Windows 驗證。本節提供將最終使用者電腦設定為使用整合式 Windows 驗證來支援單一登入存取的說明。

附註：必須對您要提供 Identity Applications 和 Identity Reporting 的單一登入存取的每部最終使用者電腦都重複此程序。

---

1 登入使用者將需要單一登入存取的電腦。

2 開啟 「網際網路選項」控制台。

3 按一下安全性。

4 按一下信任的網站 > 網站。

5 新增 Identity Applications 伺服器的 DNS 名稱。

   例如：rbpm.mycompany.com

6 按一下新增，然後按一下關閉。

7 按一下自訂等級 ...。

8 在使用者驗證下，選取使用目前的使用者名稱及密碼來自動登入。

9 按一下確定。

10 在 「網際網路選項」中，按一下進階。

11 在 「安全性」下，選取啟用整合的 **Windows** 驗證。

12 對您要提供 Identity Applications 和 Identity Reporting 的單一登入存取的每部最終使用者電腦都重複此程序。

28 驗證是否可對 Identity Applications 進行單一登入存取

在安裝 Identity Applications 並設定單一登入的設定後，您應該驗證是否能夠登入個別應用程式，並在不登出的情況下切換各個應用程式。依預設，應用程式會在 URL 連結中使用以下字尾：

- Identity Applications 管理： /idmadmin
- Identity Manager 儀表板： /idmdash
- 使用者應用程式：/IDMProv
- Identity Reporting ： /IDMRPT

若要自訂字尾，請使用 RBPM 組態公用程式。如需詳細資訊，請參閱第 15.8 章 「完成 Identity Applications 的設定」(第 204 頁)。

若要驗證單一登入功能：

1. 在 Identity Applications 伺服器上的新瀏覽器視窗中，輸入儀表板的 URL ：

   https://*server*:port/idmdash

   請不要登入儀表板。
2. 在瀏覽器中，導覽至使用者應用程式：

   https://*server*:port/*IDM-context*
3. 驗證使用者應用程式是否顯示步驟 1 中所示的相同登入頁面。
4. 登入使用者應用程式。
5. 按一下右上角的首頁圖示，然後驗證您是否不必再次登入即可存取儀表板。

29 使用 SSL 進行安全通訊

Identity Applications 和 Identity Reporting 使用 HTML 表單進行驗證。因此，登入程序可能會泄露使用者身分證明。NetIQ 建議您啟用 SSL 通訊協定來保護敏感性資訊。SSL 通訊協定可確保在 Identity Manager 各元件之間處理的通訊安全。

您應該準備好證書，以便將 Tomcat 伺服器設定為使用 SSL 進行通訊。可透過兩種方式取得證書：

- 外部可信的證書管理中心 (CA) 核發的證書
- 自行簽署的證書

29.1 確保使用 SSL 連接的核對清單

為確保在 Identity Applications、Identity Reporting、SSPR 和 OSP 之間使用安全連接，NetIQ 建議您執行以下核對清單中的步驟：

	核對清單項目
❑	1. 使用金鑰儲存區來儲存驗證證書。如需詳細資訊，請參閱第 29.2 節「建立金鑰儲存區和證書簽署要求」(第 295 頁)。
❑	2. (視情況而定) 可以在您的環境中使用自行簽署的證書或外部 CA 核發的證書。如需詳細資訊，請參閱第 29.4 節「使用自行簽署的證書啟用 SSL」(第 298 頁)。對於生產環境，則建議使用外部 CA 核發的證書。
❑	3. (視情況而定) 在線上環境中輸入簽署的證書。如需詳細資訊，請參閱第 29.3 節「使用外部 CA 簽署的證書啟用 SSL」(第 297 頁)。
❑	4. 設定驗證伺服器、Identity Applications 和 Identity Reporting，以支援 SSL 通訊。如需詳細資訊，請參閱第 29.6 節「更新應用程式伺服器的 SSL 設定」(第 303 頁) 與第 29.7 節「在組態公用程式中更新 SSL 設定」(第 304 頁)。

29.2 建立金鑰儲存區和證書簽署要求

金鑰儲存區是一個 Java 檔案，其中包含加密金鑰，有時還包含安全性證書。若要建立金鑰儲存區，可以使用 JRE 中隨附的 Java Keytool 公用程式。您可以建立 .jks 檔案，將證書產生到金鑰儲存區中。每個證書都與一個唯一的別名關聯。將金鑰儲存區放置在支援 Identity Applications 和 Identity Reporting 的應用程式伺服器的 conf 目錄中。

1 在指令提示符處，導覽至已部署 Identity Applications 的應用程式伺服器安裝的 conf 目錄。例如，C:\NetIQ\idm\apps\tomcat\conf。

   tomcat/conf 路徑是安裝於 Tomcat 上的 Identity Applications 的預設路徑。根據您安裝應用程式和 Tomcat 的方式，該路徑會有所不同。

2 使用以下指令設定用於建立金鑰儲存區的環境路徑：

```
cd C:\NetIQ\idm\apps\tomcat\conf
export PATH=C:\NetIQ\idm\apps\jre\bin:$PATH
```

3 使用以下指令建立金鑰儲存區：

```
keytool -genkey -alias keystore_name -keyalg RSA -keystore keystore_name.keystore -validity 3650 -keysize 2048
```

例如：

```
keytool -genkey -alias IDMkey -keyalg RSA -keystore IDMkey.keystore -validity 3650 -keysize 2048
```

4 出現提示時，依據以下注意事項指定參數值：

- 對於名字和姓氏，請指定伺服器的完全合格名稱。例如：

  MyTomcatServer.NetIQ.com

- 使用正確的拼字。如果拼錯了任何單字，當您從簽章管理中心產生簽署的證書時，將會看到錯誤。

5 (選擇性) 建立一個簡單的文字檔，用於儲存您為參數值提供的資訊副本。

儲存這些資訊有助於確保您在向簽章管理中心申請簽章，以及輸入證書時提供相同的資訊。

6 將金鑰儲存區檔案複製到已部署 Identity Manager 元件和 SSPR 的每個應用程式伺服器例項的 tomcat/conf 目錄中。

7 若要產生 CA 證書申請，請完成以下步驟：

7a 在 conf 目錄中，建立名為 your_request.csr 的簡單文字檔。例如 IDMcertrequest.csr。

7b 執行以下指令：

```
keytool -certreq -v -alias keystore_name -file your_request.csr -keypass keystore_password -keystore your.keystore -storepass your_password
```

例如，

```
keytool -certreq -v -alias IDMkey.keystore -file IDMcertrequest.csr -keypass IDMkeypass -keystore IDMkey.keystore -storepass IDMpass
```

當您執行該指令時，Keytool 公用程式會在 .csr 檔案中填入用於申請證書的相應資料。

8 (視情況而定) 若要取得簽署的證書，請將 .csr 檔案提交給有效的證書管理中心。

9 將證書複製到應用程式伺服器的組態目錄中。

例如，C:\NetIQ\idm\apps\tomcat\conf。

10 停止 Tomcat。

建立金鑰儲存區並產生 CA 證書申請後，請遵循以下程序將證書輸入金鑰儲存區：

- 對於外部 CA 簽署的證書，請參閱第 29.3 節「使用外部 CA 簽署的證書啟用 SSL」(第 297 頁)。
- 對於自行簽署的證書，請參閱第 29.4 節「使用自行簽署的證書啟用 SSL」(第 298 頁)。

29.3 使用外部 CA 簽署的證書啟用 SSL

對於生產環境，請使用有效證書管理中心核發的已簽署證書。本節說明如何將簽署的證書輸入至 Identity Applications 的預設 Tomcat 應用程式伺服器。

此程序假設您已從有效的證書管理中心取得了一個已簽署證書。如需詳細資訊，請參閱第 29.2 節「建立金鑰儲存區和證書簽署要求」(第 295 頁)。

若要使用簽署的證書和 SSL：

1. 將證書複製到應用程式伺服器的組態目錄中。例如，C:\NetIQ\idm\apps\tomcat\conf。
2. 若要將根證書轉換為 DER 格式，請完成以下步驟：
   - **2a** 連按兩下 conf 目錄中儲存的證書。
   - **2b** 在「證書」對話方塊中，按一下**證書路徑**。
   - **2c** 選取您從簽章管理中心收到的根證書。
   - **2d** 按一下**檢視證書**。
   - **2e** 按一下**詳細資料 > 複製到檔案**。
   - **2f** 在輸出證書精靈中，按**下一步**。
   - **2g** 選取**適用於 X.509 的 DER 編碼二進位檔案 (.CER)**，然後按**下一步**。
   - **2h** 建立一個新檔案以儲存設定了新格式的證書，並將該檔案儲存在應用程式伺服器的 conf 目錄中。

     例如，C:\NetIQ\idm\apps\tomcat\conf。
   - **2i** 按一下「**完成**」。
3. 若要輸入轉換後的證書，請完成以下步驟：
   - **3a** 在指令提示符處，導覽至應用程式伺服器的 conf 目錄。
   - **3b** 輸入以下指令：

     ```
     keytool -import -trustcacerts -alias root -keystore your.keystore -file yourRootCA.der
     ```

     例如：

     ```
     keytool -import -trustcacerts -alias root -keystore IDMkey.keystore -file IDMTESTREE.der
     ```

     附註：您必須指定 **root** 做為您的別名。

     輸入證書後，伺服器會顯示**證書已新增至金鑰儲存區**。
   - **3c** 使用以下指令驗證是否已將簽署的證書正確輸入到 conf 目錄中：

     ```
     keytool -list -v -alias root -keystore your.keystore
     ```

     例如：

     ```
     keytool -list -v -alias root -keystore IDMkey.keystore
     ```

     伺服器會列出您的證書。
4. 建議您將簽署的證書也輸入至 Java cacerts 位置。例如：

   ```
   keytool -import -trustcacerts -alias root -keystore C:\NetIQ\idm\jre\lib\security\cacerts -
   file IDMTESTREE.der
   ```

5 更新應用程式伺服器的 SSL 設定，請參閱第 29.6 節「更新應用程式伺服器的 SSL 設定」(第 303 頁)。

6 在組態公用程式中更新 SSL 設定。如需詳細資訊，請參閱第 29.7 節「在組態公用程式中更新 SSL 設定」(第 304 頁)。

7 更新 Self Service Password Reset 的 SSL 設定。如需詳細資訊，請參閱第 29.8 節「更新 Self Service Password Reset 的 SSL 設定」(第 306 頁)

8 重新啟動 Tomcat。

29.4 使用自行簽署的證書啟用 SSL

如果您想在測試環境中使用自行簽署的證書 (因為與有效管理中心簽署的證書相比，這種類型的證書更容易獲得)，請參閱本節。

- 第 29.4.1 節「輸出證書管理中心」(第 298 頁)
- 第 29.4.2 節「產生自行簽署的證書」(第 299 頁)

29.4.1 輸出證書管理中心

您可以使用 iManager 從 eDirectory 伺服器輸出證書管理中心 (CA)，以產生自行簽署的證書。

1 使用 eDirectory 管理員的使用者名稱和密碼登入 iManager。

2 按一下「**管理**」> 「**修改物件**」。

3 在安全性容器中，瀏覽至名為*網路樹名稱* CA.Security 的 CA 物件。例如 IDMTESTTREE CA.Security。

4 按一下「**確定**」。

5 按一下**證書** > **自行簽署的證書**。

6 選取要使用的自行簽署證書。

範例：**自行簽署的證書 RSA**

6a 核取**自行簽署的證書 RSA**。

6b 按一下**驗證**。

7 按一下「**輸出**」。

8 清除**輸出私密金鑰**。

9 按一下**輸出格式** > **DER**。

10 按一下「**下一步**」。

11 按一下**儲存輸出的證書**。

12 按一下**儲存檔案**。

iManager 會將該檔案儲存為*網路樹名稱* cert.der。例如 IDMTESTREE cert.der。

13 按一下「**關閉**」。

14 將證書複製到應用程式伺服器的組態目錄中 (cert.der)。

例如，C:\NetIQ\idm\apps\tomcat\conf。

15 若要輸入根證書，請完成以下步驟：

15a 在指令提示符處，使用以下指令導覽至應用程式伺服器的 conf 目錄：

```
keytool -import -trustcacerts -alias root -keystore <keystore file>.keystore -file
exported_certificate_filename.der
```

範例：

```
keytool -import -trustcacerts -alias root -keystore IDMkey.keystore -file cert.der
```

附註：您必須指定 **root** 做為您的別名。

輸入證書後，伺服器會顯示**證書已新增至金鑰儲存區**。

15b 建議您將根證書也輸入至 Java cacerts 位置。

例如：

```
keytool -import -trustcacerts -alias root -keystore C:\NetIQ\idm\jre\lib\security\cacerts
-file cert.der
```

15c 使用以下指令驗證是否已將簽署的證書正確輸入到 conf 目錄中：

```
keytool -list -v -alias root -keystore your.jks
```

例如，

```
keytool -list -v -alias root -keystore IDMkey.jks
```

伺服器會列出證書。

29.4.2 產生自行簽署的證書

在產生自行簽署的證書之前，請確保您有一個金鑰儲存區和證書要求檔案。如需詳細資訊，請參閱第 29.2 節「建立金鑰儲存區和證書簽署要求」(第 295 頁)

1. 登入 iManager。
2. 導覽至**證書伺服器 > 發放證書**。
3. 瀏覽至第 29.2 節「建立金鑰儲存區和證書簽署要求」(第 295 頁)的步驟 7 中建立的 .csr 檔案。

   範例： IDMcertrequest.csr
4. 按兩次「下一步」。
5. 對於證書類型，請按一下**未指定**。
6. 按兩次「下一步」。

   iManager 會將檔案儲存為 csr_request_name.der。範例： IDMcertrequest.der
7. 將證書複製到應用程式伺服器的組態目錄中 (IDMcertrequest.der) 。

   例如，C:\NetIQ\idm\apps\tomcat\conf。
8. 若要輸入產生的自行簽署證書，請完成以下步驟：

   8a 在指令提示符處，使用以下指令導覽至應用程式伺服器的 conf 目錄：

   ```
   keytool -import -alias keystore_name -keystore <keystore_file> -file
   <signed_certificate_filename>.der
   ```

   範例：

   ```
   keytool -import -alias IDMkey -keystore IDMkey.keystore -file IDMcertrequest.der
   ```

   附註：必須指定金鑰儲存區名稱做為別名。

輸入證書後，伺服器會顯示**證書已新增至金鑰儲存區**。

8b 建議您將自行簽署的證書也輸入至 Java cacerts 位置。

例如：

```
keytool -import -alias IDMkey -keystore
C:\NetIQ\idm\jre\lib\security\cacerts -file IDMcertrequest.der
```

8c 使用以下指令驗證是否已將簽署的證書正確輸入到 conf 目錄中：

```
keytool -list -v -alias keystore_name -keystore your.jks
```

例如，

```
keytool -list -v -alias IDMkey -keystore IDMkey.jks
```

伺服器會列出證書。

9 更新應用程式伺服器的 SSL 設定。如需詳細資訊，請參閱第 29.6 節「更新應用程式伺服器的 SSL 設定」(第 303 頁)。

10 在組態公用程式中更新 SSL 設定。如需詳細資訊，請參閱第 29.7 節「在組態公用程式中更新 SSL 設定」(第 304 頁)。

11 更新 Self Service Password Reset 的 SSL 設定。如需詳細資訊，請參閱第 29.8 節「更新 Self Service Password Reset 的 SSL 設定」(第 306 頁)

12 重新啟動 Tomcat。

29.5 在 Sentinel 與 Identity Manager 元件之間啟用 SSL

您可以建立並輸出自行簽署的伺服器證書，以確保在 Sentinel 與 Identity Manager 元件之間進行安全通訊。請使用有效證書管理中心核發的已簽署證書。

- 第 29.5.1 節「在 Sentinel 與 Identity Manager 引擎 / 遠端載入器之間啟用 SSL」(第 300 頁)
- 第 29.5.2 節「在 Sentinel 與使用者應用程式之間啟用 SSL」(第 302 頁)

29.5.1 在 Sentinel 與 Identity Manager 引擎 / 遠端載入器之間啟用 SSL

1 若要建立新證書，請完成以下步驟：

1a 登入 iManager。

1b 按一下 **NetIQ Certificate Server** > **建立伺服器證書**。

1c 選取相應的伺服器。

1d 指定伺服器的綽號。

1e 接受其餘的證書預設值。

2 若要將伺服器證書輸出為 .pfx 格式，請完成以下步驟：

2a 在 iManager 中，選取**目錄管理** > **修改物件**。

2b 瀏覽並選取 Key Material Object (KMO) 物件。

2c 按一下**證書** > **輸出**。

2d 指定密碼。

2e 將伺服器證書儲存為 PKCS#12。例如，certificate.pfx。

3 使用以下指令將所輸出證書中的私密金鑰擷取到 dxipkey.pem。

openssl pkcs12 -in certificate.pfx -nocerts -out dxipkey.pem –nodes

4 將證書擷取到 dxicert.pem 檔案。

openssl pkcs12 -in certificate.pfx -nokeys -out dxicert.pem

5 若要將步驟 1 中建立的 eDirectory 伺服器 CA 證書輸出為 Base64 格式，請完成以下步驟：

5a 在 iManager 中，導覽至**角色與任務** > **NetIQ 證書存取** > **使用者證書**。

5b 瀏覽並選取建立的證書。

5c 按一下「**輸出**」。

5d 從下拉式功能表中選取 **OU=organizationCA.O=TREENAME** 做為 **CA 證書**。

5e 從下拉式功能表中選取 **BASE64 > 輸出格式**。

5f 按**下一步**，然後儲存該證書。例如，cacert.b64。

6 使用以下指令將 CA 證書輸出到金鑰儲存區：

keytool -import -alias < 別名 > -file <b64 檔案 > -keystore < 金鑰儲存區檔案 > –noprompt

例如，

keytool -import -alias trustedroot -file cacert.b64 -keystore idmKeystore.ks –noprompt

7 若要將證書輸入到稽核連接器的可信證書儲存區，請完成以下步驟：

7a 以管理員身分登入 Sentinel 主要介面。

7b 在主要 ESM 顯示螢幕中，找到稽核伺服器。

7c 以滑鼠右鍵按一下**稽核伺服器**，然後按一下**編輯**。

7d 在「安全性」索引標籤中，選取**嚴格**。

附註：該選項預設設定為使用**開放**（不安全）模式，以允許初始連接。但是，當您在生產環境中使用它時，請務必將模式設定為**嚴格**。

7e 按一下**輸入**，然後導覽至您在步驟 6 中建立的證書。例如，idmkeystore.ks。

7f 依次按一下**開啟**和**儲存**。

7g 重新啟動稽核伺服器。

8 依據您的元件，將步驟 3 和步驟 4 中建立的私密金鑰與證書分別複製到以下位置：

元件	Windows 路徑
Identity Manager 引擎	C:\NetIQ\idm\NDS\DIBFiles
遠端載入器	遠端載入器安裝目錄： C:\NetIQ\idm\RemoteLoader 或 C:\NetIQ\idm\RemoteLoader\64bit 或 C:\NetIQ\idm\RemoteLoader\32bit
.NET 遠端載入器	C:\NetIQ\idm\RemoteLoader.NET
擴送代理程式	C:\NetIQ\idm\FanoutAgent

9 重新啟動 Identity Manager 服務。

29.5.2 在 Sentinel 與使用者應用程式之間啟用 SSL

1 若要建立新證書，請完成以下步驟：
   - **1a** 登入 iManager。
   - **1b** 按一下 **NetIQ 證書伺服器** > **建立使用者證書**。
   - **1c** 選取相應的使用者。
   - **1d** 為使用者指定綽號。
   - **1e** 在**建立方法**中選取**自訂**。
   - **1f** 接受其餘的證書預設值。
   - **1g** 按**下一步**。
   - **1h** 在**自訂延伸**中選取**新增 DER 編碼的延伸**。
   - **1i** 瀏覽到 \products\UserApplication\ext.der 自訂延伸。
   - **1j** (選擇性) 指定電子郵件地址。
   - **1k** 檢閱證書參數，然後按一下**完成**。
2 若要輸出使用者證書，請完成以下步驟：
   - **2a** 按一下 **NetIQ 證書存取** > **使用者證書**。
   - **2b** 選取在步驟 1 中輸入的使用者證書。
   - **2c** 選取有效的使用者證書，然後按一下**輸出**。
   - **2d** 指定密碼。
   - **2e** 將使用者證書儲存為 PKCS12。例如，certificate.pfx。
3 使用以下指令將所輸出證書中的私密金鑰擷取到 key.pem 檔案。

   openssl pkcs12 -in certificate.pfx -nocerts -out key.pem –nodes
4 將證書擷取到 cert.pem 檔案。

   openssl pkcs12 -in certificate.pfx -nokeys -out cert.pem

5 停止使用者應用程式。

6 將私密金鑰和證書新增至 configupdate 公用程式。

   6a 開啟 configupdate 公用程式。

   6b 按一下**顯示進階選項**。

   6c 在 **NetIQ Sentinel 數位簽名證書**欄位中，複製 cert.pem。

   6d 在 **NetIQ Sentinel 數位簽名私密金鑰**欄位中，導覽至私密金鑰 (key.pem) 的擷取位置，然後輸入金鑰。

   6e 儲存在 configupdate 公用程式中所做的變更。

7 重新啟動使用者應用程式。

8 若要將步驟 1 中建立的 eDirectory 伺服器 CA 證書輸出為 Base64 格式，請完成以下步驟：

   8a 在 iManager 中，導覽至**角色與任務** > **NetIQ 證書存取** > **使用者證書**。

   8b 選取建立的證書。

   8c 按一下**輸出**並清除「輸出私密金鑰」核取方塊。

   8d 從下拉式功能表中選取 **BASE64 > 輸出格式**。

   8e 按**下一步**，然後儲存該證書。例如，cacert.b64。

9 使用以下指令將 CA 證書輸出到金鑰儲存區：

   keytool -import -alias < 別名 > -file cacert.b64 -keystore < 金鑰儲存區檔案 > –noprompt

   例如，

   keytool -import -alias trustedroot -file cacert.b64 -keystore idmKeystore.ks –noprompt

10 若要將證書輸入到稽核連接器的可信證書儲存區，請完成以下步驟：

   10a 以管理員身分登入 Sentinel 主要介面。

   10b 在主要 ESM 顯示螢幕中，找到稽核伺服器。

   10c 以滑鼠右鍵按一下**稽核伺服器**，然後按一下**編輯**。

   10d 在**安全性**索引標籤中，選取**嚴格**。

   附註：該選項預設設定為使用**開放** (不安全) 模式，以允許初始連接。但是，當您在生產環境中使用它時，請務必將模式設定為**嚴格**。

   10e 按一下**輸入**，然後導覽至您在步驟 9 中建立的證書。例如，idmKeystore.ks。

   10f 依次按一下**開啟**和**儲存**。

   10g 重新啟動稽核伺服器。

11 重新啟動使用者應用程式。

29.6 更新應用程式伺服器的 SSL 設定

若要支援 SSL 通訊，需要對代管 Identity Applications 和 Identity Reporting 的應用程式伺服器進行設定。本節提供更新 Tomcat 應用程式伺服器 (即預設的應用程式伺服器) 的說明。

1 如果 Tomcat 正在執行，請將其停止。

2 設定 Tomcat 伺服器的 SSL 連接埠。

例如，SSL 的連接器連接埠為 8543。編輯位於 C:\NetIQ\idm\apps\tomcat\conf 目錄中的 server.xml 檔案。

```
<Connector port="8543" protocol="HTTP/1.1"
maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="path_to_keystore_file"
keystorePass="keystore_password" />
```

位於：

keystoreFile

指定預設位於 C:\NetIQ\idm\apps\tomcat\conf\userapp.keystore 目錄中的 userapp.keystore 檔案的路徑。

keystorePass

指定 userapp.keystore 檔案的密碼。

另外，請將 redirectPort 屬性更新為 8543，然後儲存 server.xml。

3 導覽至 Tomcat 的 conf 目錄 (預設為 C:\NetIQ\idm\apps\tomcat\conf)。

4 確定 conf 目錄中包含金鑰儲存區檔案。例如，idmapps.keystore。

如果您要在執行此程序後再建立金鑰儲存區檔案，請務必使用在此程序中提供的相同檔案名稱。如需詳細資訊，請參閱第 29.2 節「建立金鑰儲存區和證書簽署要求」(第 295 頁)。

5 在文字編輯器中開啟 conf 目錄中的 server.xml 檔案。

6 將以下內容新增至 server.xml 檔案：

```
<Connector port="port_number" protocol="HTTP/1.1" maxThreads="150" SSLEnabled="true"
scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile="path_to_file/
filename.keystore" keystorePass="password"
```

例如：

```
<Connector port="8543" protocol="HTTP/1.1" maxThreads="150" SSLEnabled="true" scheme="https"
secure="true" clientAuth="false" sslProtocol="TLS"
keystoreFile="C:\NetIQ\idm\apps\tomcat\conf\idmapps.keystore"
keystorePass="encrypted_password"
```

NetIQ 建議您在 keystorePass 中指定加密密碼，不要提供純文字密碼。如需在 SSL 通訊中使用純文字密碼和加密密碼的詳細資訊，請參閱「Securing Tomcat」(保護 Tomcat)。

7 啟動 Tomcat。

29.7 在組態公用程式中更新 SSL 設定

在安裝 Identity Applications 和 Identity Reporting 時，您應該指定 *https* 做為通訊方法。例如「*通訊協定*」*(第 185 頁)*。但是，在安裝後，您可以使用 RBPM 組態公用程式來確保應用程式使用 SSL 進行通訊。如需這些參數的詳細資訊，請參閱第 15.8 章「完成 Identity Applications 的設定」(第 204 頁)。

1 使用 services.msc 檔案停止 Tomcat。

2 導覽至預設位於 Identity Applications 安裝目錄中的 RBPM 組態公用程式。例如 C:\NetIQ\idm\apps\UserApplication。

3 在指令提示符處，執行組態公用程式 (configupdate.bat) ：

附註：您可能需要花幾分鐘時間等待公用程式啟動。

4 (視情況而定) 如果您在 configupdate 公用程式中設定了 SSL，請導覽至**驗證**索引標籤，並取代 **SSO 用戶端**索引標籤中提到的所有參考。

https://*<IP address>*:*<SSL Port number>*

例如，

https://*192.168.0.1*:*8543*

5 按一下**驗證**，然後修改以下設定：

OAuth 伺服器 TCP 連接埠

指定驗證伺服器的連接埠。

例如： 8543

OAuth 伺服器正在使用 TLS/SSL

指定您要讓驗證伺服器使用 TLS/SSL 通訊協定進行通訊。

選擇性 TLS/SSL 金鑰儲存區檔案

指定包含驗證伺服器可信證書之 Java JKS 金鑰儲存區檔案的路徑和檔案名稱。當驗證伺服器使用 TLS/SSL 通訊協定，並且驗證伺服器的可信證書不在 JRE 可信證書儲存區 (cacerts) 中時，此參數才適用。

選擇性 TLS/SSL 金鑰儲存區密碼

指定用於載入 TLS/SSL 驗證伺服器之金鑰儲存區檔案的密碼。

OAuth 金鑰儲存區檔案

指定要用於驗證的 Java JKS 金鑰儲存區檔案的路徑。該金鑰儲存區檔案必須至少包含一個公用金鑰 / 私密金鑰組。

OAuth 金鑰儲存區檔案密碼

指定用於載入 OAuth 金鑰儲存區檔案的密碼。

OAuth 使用之金鑰的金鑰別名

指定 OSP 金鑰儲存區檔案中將用來產生對稱式金鑰的公用金鑰 / 私密金鑰組的名稱。

OAuth 使用之金鑰的金鑰密碼

指定驗證伺服器使用的私密金鑰密碼。

6 按一下 **SSO 用戶端**。

7 更新所有 URL 設定，例如**抵達頁面的 URL 連結**和 **OAuth 重新導向 URL**。

這些設定指定驗證伺服器完成驗證後要將瀏覽器用戶端重新導向到的絕對 URL。

使用以下格式： https://DNS_name:sslport/path。例如，https:/nqserver.testsite:8543/landing/com.netiq.test。

8 儲存在組態公用程式中所做的變更。

9 使用 services.msc 檔案啟動 Tomcat。

29.8 更新 Self Service Password Reset 的 SSL 設定

若要修改 SSPR 的 SSL 設定，您必須登入應用程式。

1 在瀏覽器中，輸入您在組態公用程式中為抵達頁面指定的 https URL。例如 https://myserver.host:8543/landing。

2 使用 Identity Applications 的管理員身分證明登入。

   應用程式會顯示一則警告，指出您需要變更重新導向白名單 URL。

3 若要變更重新導向白名單 URL，請依照頁面上的指示操作。

4 導覽至**設定 > OAuth SSO**。

5 對於所有三個 URL，請指定 https 通訊協定和連接埠。

6 導覽至**設定 > 應用程式**。

7 對於所有三個 URL，請指定 https 通訊協定和連接埠。

8 按一下**儲存**，然後按一下**確定**。

9 驗證 Identity Applications 的所有 URL 現在是否都使用了 https 通訊協定。

疑難排解秘訣

更新 SSPR 的 SSL 設定後，如果您無法存取 SSPR 抵達頁面，請遵循以下步驟在 SSPRConfiguration.xml 檔案中更新所需的 URL。

1 導覽至位於以下路徑的 SSPRConfiguration.xml 檔案：

   ```
   C:\NetIQ\idm\apps\sspr\sspr_data
   ```

2 使用相應的 IP 位址和連接埠號碼更新所有 URL。

   ```
   https://<IP address>:<SSL Port number>
   ```

   範例：

   ```
   https://192.168.0.1:8543
   ```

30 安裝後任務

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

- 第 30.1 節「設定已連接系統」(第 307 頁)
- 第 30.2 節「建立和設定驅動程式集」(第 307 頁)
- 第 30.3 節「建立驅動程式」(第 309 頁)
- 第 30.4 節「定義規則」(第 310 頁)
- 第 30.5 節「管理驅動程式活動」(第 310 頁)
- 第 30.6 節「啟用 Identity Manager」(第 310 頁)

30.1 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。

30.2 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。

- 第 30.2.1 節「建立驅動程式集」(第 307 頁)
- 第 30.2.2 節「將預設密碼規則指定給驅動程式集」(第 308 頁)
- 第 30.2.3 節「在 Identity Vault 中建立密碼規則物件」(第 308 頁)
- 第 30.2.4 節「建立自訂密碼規則」(第 309 頁)
- 第 30.2.5 節「在 Identity Vault 中建立預設通知集合物件」(第 309 頁)

30.2.1 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)。

30.2.2 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，請參閱第 30.2.3 節「在 Identity Vault 中建立密碼規則物件」(第 308 頁)與第 30.2.4 節「建立自訂密碼規則」(第 309 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。

30.2.3 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，請從 Identity Manager 安裝套件的 install/utilities 目錄執行 ldapmodify.exe，以從檔案中輸入屬性。

30.2.4 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，請參閱第 30.2.3 節「在 Identity Vault 中建立密碼規則物件」(第 308 頁)。

30.2.5 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。

30.3 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 驅動程式網站上的相關驅動程式實作指南。

30.4 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。

30.5 管理驅動程式活動

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

30.6 啟用 Identity Manager

當您首次登入時，有些 Identity Manager 元件會自動啟用。其他元件則需要透過執行某個程序來啟用。

- 第 30.6.1 節「安裝產品啟用身分證明」(第 310 頁)
- 第 30.6.2 節「檢閱 Identity Manager 和驅動程式的產品啟用」(第 311 頁)
- 第 30.6.3 節「啟用 Identity Manager 驅動程式」(第 312 頁)
- 第 30.6.4 節「啟用特定的 Identity Manager 元件」(第 312 頁)

30.6.1 安裝產品啟用身分證明

NetIQ 建議使用 iManager 來安裝產品啟用身分證明。

附註：對於想要使用的每個驅動程式，請啟用包含驅動程式的驅動程式集。您可以使用認證來啟用任何網路樹。

1 在您購買授權之後，NetIQ 會向您傳送一封電子郵件，其中包含您的客戶 ID。在這封電子郵件中的「訂單詳細資料」區段有一個網站連結，您可以從該網站取得認證。按一下連結，前往該網站。

2 按一下授權下載連結，然後完成下列其中一個動作：
   - 開啟「產品啟用身分證明」檔案，然後將「產品啟用身分證明」的內容複製到簡貼簿。
   - 儲存「產品啟用身分證明」檔案。
   - 如果您選擇複製內容，請不要包含任何多餘的行或空格。您應該從身分證明的第一個破折號 (-) 開始複製 (----BEGIN PRODUCT ACTIVATION CREDENTIAL)，一直到身分證明的最後一個破折號 (-) (END PRODUCT ACTIVATION CREDENTIAL-----)。

3 登入 iManager。

4 選取「**Identity Manager**」> 「**Identity Manager 綜覽**」。

5 若要在樹狀結構中選取一個驅動程式集，請按一下瀏覽圖示 ()。

6 在 **Identity Manager 綜覽**頁面上，按一下包含要啟用之驅動程式的驅動程式集。

7 在**驅動程式集綜覽**頁面上，按一下**啟用** > **安裝**。

8 選取要在其中啟用 Identity Manager 元件的驅動程式集，然後按**下一步**。

9 (視情況而定) 如果您之前儲存了產品啟用身分證明檔案，請指定儲存的位置。

10 (視情況而定) 如果您之前複製了產品啟用身分證明檔案的內容，請將這些內容貼至文字區域中。

11 按一下「**下一步**」。

12 按一下「**完成**」。

附註：套用 Bundle Edition 啟用碼後，Identity Manager 不會顯示正確的 Identity Manager 版本。

30.6.2 檢閱 Identity Manager 和驅動程式的產品啟用

對於每個驅動程式集，您可以檢視已為 Identity Manager 引擎伺服器和 Identity Manager 驅動程式安裝的產品啟用身分證明。您也可以移除啟用身分證明。

附註：為驅動程式集安裝有效的產品啟用身分證明後，驅動程式名稱的旁邊可能仍然會顯示「需要啟用」。若如此，請重新啟動驅動程式。該訊息應該即會消失。

1 登入 iManager。

2 按一下「**Identity Manager**」 > 「**Identity Manager 綜覽**」。

3 若要在樹狀結構中選取一個驅動程式集，請使用瀏覽圖示 () 和搜尋圖示 ()。

4 在 **Identity Manager 綜覽**頁面上，按一下您要檢閱其啟用資訊的驅動程式集。

5 在**驅動程式集綜覽**頁面上，按一下**啟用 > 資訊**。

   您可以檢視啟用身分證明的文字，或者如果報告錯誤，則可以移除啟用身分證明。

30.6.3 啟用 Identity Manager 驅動程式

在啟用 Identity Manager 引擎時，還可以啟用以下驅動程式：

服務驅動程式	通用驅動程式
資料收集服務	Active Directory
ID 提供者	eDirectory 的雙向驅動程式
受管理系統閘道	eDirectory
角色與資源服務	GroupWise 2014
使用者應用程式	LDAP
	Lotus Notes

若要啟用其他 Identity Manager 驅動程式，您必須另外購買 Identity Manager 整合模組，其中可能會包含一或多個驅動程式。您會收到每個所購 Identity Manager 整合模組的產品啟用身分證明。在收到身分證明後，請執行第 30.6.1 節「安裝產品啟用身分證明」(第 310 頁)中所列的程序。如需驅動程式的詳細資訊，請造訪 Identity Manager 驅動程式文件網站。

30.6.4 啟用特定的 Identity Manager 元件

本節提供關於啟用 Identity Manager 特定元件的資訊。

- 「啟用 Designer」(第 312 頁)
- 「啟用 Analyzer」(第 312 頁)

啟用 Designer

您在啟用 Identity Manager 引擎或 Identity Manager 驅動程式時，還可以啟用 Designer。

啟用 Analyzer

當您啟動未獲授權的 Analyzer 透視功能時，Analyzer 將會開啟啟用頁面，您可以從中管理 Analyzer 的授權。

附註：如果您關閉「啟用」對話方塊，Analyzer 會一直保持鎖定狀態，直到您提供了授權將其啟用。當您準備好新增授權時，請在專案檢視中按一下**啟用 Analyzer**，以開啟「啟用」對話方塊。

1. 啟動 Analyzer。
2. 在 **Analyzer 啟用**視窗中，您可以新增授權，或存取 Customer Center 以獲得授權。
3. (視情況而定) 若要新增授權：
   - **3a** 按一下**新增授權**。
   - **3b** 在**授權**視窗中，輸入您從 NetIQ 客戶服務中心入口網站下載的啟用代碼，然後按一下**確定**。

4 (視情況而定) 若要存取 Customer Center 以獲得授權：

   4a 按一下**存取 Customer Center 以獲得授權**。

   4b 按一下**存取 Micro Focus Customer Center**。

   4c 瀏覽至 Analyzer 授權並加以選取。

   4d 複製啟用代碼，然後關閉客戶服務中心入口網站。

   4e 在**授權**視窗中輸入啟用代碼，然後按一下**確定**。

5 在 **Analyzer 啟用**視窗中，檢閱您剛才所安裝授權的詳細資料。

6 按一下**確定**開始使用 Analyzer。

IX 升級 Identity Manager

此部分提供升級 Identity Manager 各元件的資訊。若要將現有資料移轉至新伺服器，請參閱第 X 部分「將 Identity Manager 資料移轉至新安裝中」(第 351 頁)。如需升級與移轉之間差異的詳細資訊，請參閱第 31.2 節「瞭解升級和移轉」(第 319 頁)。

31 升級 Identity Manager 的準備工作

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

- 第 31.1 節「Identity Manager 的升級核對清單」(第 317 頁)
- 第 31.2 節「瞭解升級和移轉」(第 319 頁)
- 第 31.3 節「升級順序」(第 319 頁)
- 第 31.4 節「支援的升級路徑」(第 320 頁)
- 第 31.5 節「備份目前組態」(第 323 頁)

31.1 Identity Manager 的升級核對清單

若要執行升級，NetIQ 建議您完成以下核對清單中的步驟。

	核對清單項目
❑	1. 檢閱升級與移轉之間的差異。如需詳細資訊，請參閱第 31.2 節「瞭解升級和移轉」(第 319 頁)。
❑	2. 升級至 Identity Manager 4.5.6。您無法將低於 4.5.6 的版本升級或移轉至 4.7 版本。如需詳細資訊，請參閱《NetIQ Identity Manager 4.5 安裝指南》。
❑	3. 確保您已取得用於升級 Identity Manager 的最新安裝套件。請參閱第 5.5 節「下載安裝檔案」(第 43 頁)。
❑	4. 瞭解 Identity Manager 各元件之間的互動。如需詳細資訊，請參閱第 I 部分「介紹」(第 17 頁)。
❑	5. 確保您的電腦符合更高版本 Identity Manager 的硬體和軟體先決條件。如需詳細資訊，請參閱第 6 章「安裝注意事項」(第 45 頁) 和您要升級至的版本的《版本說明》。
❑	6. 備份目前的專案、驅動程式組態和資料庫。如需詳細資訊，請參閱第 31.5 節「備份目前組態」(第 323 頁)。
❑	7. 將 Designer 升級至最新版本。如需詳細資訊，請參閱第 32.1 節「升級 Designer」(第 327 頁)。
❑	8. 安裝或升級至 Identity Manager 的最新版 iManager。如需詳細資訊，請參閱下列其中一節： ◆ **安裝**：「安裝 iManager」(第 125 頁) ◆ **升級**：「升級 iManager」(第 328 頁)

	核對清單項目
❑	9. 在執行 Identity Manager 的伺服器上，將 eDirectory 升級至最新的版本和修補程式。 如果在已升級最新 64 位元遠端載入器的環境中升級 eDirectory 9.0 或更新版本，eDirectory 安裝會失敗，並且遠端載入器會停止運作。為了確保遠端載入器正常運作，請先執行以下步驟，然後再升級 eDirectory ： 1. 停止遠端載入器及其例項。 2. 解除安裝 novell-DXMLopensslx RPM。 3. 安裝 eDirectory 9.1 或更新版本。 升級 eDirectory 會停止 ndsd，進而停止所有驅動程式。如需詳細資訊，請參閱 《*NetIQ eDirectory Installation Guide*》 (NetIQ eDirectory 安裝指南)。
❑	10. 更新 iManager 外掛程式，使其與 iManager 的版本相符。如需詳細資訊，請參閱第 32.2.4 節「在升級或重新安裝後更新 iManager 外掛程式」(第 330 頁)。
❑	11. 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，請參閱第 9.4.1 節「停止驅動程式」(第 81 頁)。
❑	12. 升級 Identity Manager 引擎。如需詳細資訊，請參閱第 32.4 節「升級 Identity Manager 引擎」(第 331 頁)。 **附註：**若要將 Identity Manager 引擎移轉至新伺服器，可以使用目前 Identity Manager 伺服器上的相同 eDirectory 複製本。如需詳細資訊，請參閱第 35.4 節「將 Identity Manager 引擎移轉至新伺服器」(第 358 頁)。
❑	13. (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，請參閱第 32.3 節「升級遠端載入器」(第 331 頁)。
❑	14. (視情況而定) 如果使用的是套件，請在現有驅動程式上升級套件以獲取新規則。如需詳細資訊，請參閱第 32.8 節「升級 Identity Manager 驅動程式」(第 343 頁)。 僅當套件有更新版本提供，且某個驅動程式規則中包含新的功能，而您想將其新增至現有驅動程式時，才需要執行該操作。
❑	15. (視情況而定) 如果未安裝 OSP，請加以安裝。如需詳細資訊，請參閱第 13 部分「安裝單一登入元件」(第 149 頁)。
❑	16. (視情況而定) 如果未安裝 SSPR，請加以安裝。如需詳細資訊，請參閱第 14 部分「安裝密碼管理元件」(第 155 頁)。 **附註：**如果您目前使用的是舊密碼管理提供程式，請安裝 SSPR。如需詳細資訊，請參閱第 4.4.2 節「瞭解舊密碼管理提供程式」(第 32 頁)。
❑	17. 使用升級程式升級使用者應用程式、Identity Manager 儀表板、OSP、SSPR 和 Identity Reporting。如需詳細資訊，請參閱第 32.5 節「升級 Identity Applications 和 Identity Reporting」(第 332 頁)。 或者，您也可以手動升級這些元件。如需詳細資訊，請參閱第 X 部分「將 Identity Manager 資料移轉至新安裝中」(第 351 頁)。
❑	18. 升級 Identity Reporting 和關聯的驅動程式。如需詳細資訊，請參閱第 32.6 節「升級 Identity Reporting」(第 341 頁)。
❑	19. 啟動與 Identity Applications 和 Identity Manager 引擎關聯的驅動程式。如需詳細資訊，請參閱第 9.4.2 節「啟動驅動程式」(第 82 頁)。

	核對清單項目
❑	20. (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，請參閱第 32.9 節「將新伺服器新增至驅動程式集」(第 345 頁)。
❑	21. (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，請參閱第 32.10 節「將自訂規則還原至驅動程式」(第 346 頁)。
❑	22. 啟用升級後的 Identity Manager 解決方案。如需詳細資訊，請參閱第 30.6 節「啟用 Identity Manager」(第 310 頁)。

31.2 瞭解升級和移轉

當您要安裝現有 Identity Manager 安裝的更高版本時，通常可以執行**升級**程序。但是，如果新版 Identity Manager 沒有為現有資料提供升級路徑，則您必須執行移轉。NetIQ 將**移轉**定義為在新伺服器上安裝 Identity Manager，然後將現有資料移轉至此新伺服器的程序。

在產品評估期或者在啟用 Advanced Edition 之後，如果您不想在環境中使用 Advanced Edition 功能，可以**切換**至 Standard Edition。Identity Manager 可讓您透過一個簡單的程序從 Advanced Edition 切換至 Standard Edition。

從 Advanced Edition 切換到 Standard Edition

Identity Manager 允許您在產品試用期內或啟用 Advanced Edition 後從 Advanced Edition 切換到 Standard Edition。

重要：如果您已套用 Advanced Edition 啟用碼，則不需要切換至 Standard Edition，因為 Standard Edition 的所有功能在 Advanced Edition 中都有提供。僅當您不想在環境中使用任何 Advanced Edition 功能，並且要縮減 Identity Manager 部署時，才需要切換至 Standard Edition。如需詳細資訊，請參閱「從 Advanced Edition 切換到 Standard Edition」(第 349 頁)。

31.3 升級順序

必須依照以下順序來升級 Identity Manager 的各元件：

1. Designer
2. iManager
3. Sentinel Log Management for IGA
4. Identity Vault
5. Identity Manager 引擎 / 遠端載入器
6. iManager 外掛程式
7. Tomcat 和 PostgreSQL 元件
8. 單一登入 (One SSO Provider)
9. Self Service Password Reset
10. Identity Applications (適用於 Advanced Edition)

11. Identity Reporting
12. Analyzer

如需最新的受支援升級路徑資訊，請參閱 Identity Manager 4.6 文件網站中適用於您版本的版本說明。

31.4 支援的升級路徑

Identity Manager 4.7 支援從 4.6.x 和 4.5.x 版本升級。NetIQ 建議開始升級前先在您目前版本相應的版本說明中查看該資訊。

- 第 31.4.1 節「從 Identity Manager 4.6.x 版本升級」(第 320 頁)
- 第 31.4.2 節「從 Identity Manager 4.5.x 版本升級」(第 321 頁)

31.4.1 從 Identity Manager 4.6.x 版本升級

下表列出了 Identity Manager 4.6.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	4.6.x	1. 將作業系統升級至支援的版本。 2. 將 Identity Vault 升級至 9.1。 3. 將 Identity Manager 引擎升級至 4.7。
遠端載入器 / 擴送代理程式	4.6.x	安裝 4.7 版遠端載入器 / 擴送代理程式
Designer	4.6.x	1. 安裝 Designer 4.7。 2. 將工作空間從 NCP 轉換為 LDAP。 Designer 4.7 基於 LDAP 執行。使用此版本之前，請參閱《*NetIQ Identity Manager LDAP Designer 版本說明*》。
Identity Applications	4.6.x	升級 Identity Applications 前，請確定 Identity Vault 和 Identity Manager 引擎已分別升級至 9.1 和 4.7。 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。 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 4.7 版本。 4. 更新使用者應用程式驅動程式以及角色與資源驅動程式套件。 5. 將 Identity Applications 升級至 4.7。 6. 停止 Tomcat。

元件	基礎版本	升級後的版本
Identity Reporting	4.6.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。 3. 升級 SLM for IGA。 4. 更新資料收集服務和受管理服務閘道驅動程式套件。 5. 安裝 Identity Reporting 4.7。 6. 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您所用版本的版本說明中查看該資訊：

- 《NetIQ Identity Manager 4.6 Service Pack 2 Release Notes》 (NetIQ Identity Manager 4.5 Service Pack 4 版本說明)
- 《NetIQ Identity Manager 4.6 Service Pack 1 Release Notes》 (NetIQ Identity Manager 4.5 Service Pack 4 版本說明)
- NetIQ Identity Manager 4.6 版本說明

31.4.2 從 Identity Manager 4.5.x 版本升級

下表列出了 Identity Manager 4.5.x 版本的元件範圍升級路徑：

元件	基礎版本	中間步驟	升級後的版本
Identity Manager 引擎	裝有 eDirectory 8.8.8.x (其中 x 為 3 至 9) 的 Identity Manager 4.5.x (其中 x 為 0 至 5)	套用 4.5.6 修補程式	1. 將作業系統升級至支援的版本。 2. 將 Identity Vault 升級至 9.1。 3. 將 Identity Manager 引擎升級至 4.7。
遠端載入器 / 擴送代理程式	4.5.x (其中 x 為 0 至 5)	套用 4.5.6 修補程式	安裝 4.7 版遠端載入器 / 擴送代理程式。
Designer	4.5.x (其中 x 為 0 至 5)	套用 4.5.6 修補程式	1. 安裝 Designer 4.7。 2. 將工作空間從 NCP 轉換為 LDAP。 Designer 4.7 基於 LDAP 執行。使用此版本之前，請參閱 《*NetIQ Identity Manager LDAP Designer 版本說明*》。

元件	基礎版本	中間步驟	升級後的版本
Identity Applications	4.5.x (其中 x 為 0 至 5)	◆ 如果您使用的是 JBoss 或 Websphere，請移轉至 Tomcat 應用程式伺服器。 ◆ 套用 4.5.6 修補程式。	升級 Identity Applications 前，請確定 Identity Vault 和 Identity Manager 引擎已分別升級至 9.1 和 4.7。 1. 將作業系統升級至支援的版本。 2. 更新使用者應用程式驅動程式以及角色與資源驅動程式套件。 3. 將資料庫升級至支援的版本。 4. (視情況而定) 如果 SSPR 安裝在其他電腦上，請將該元件升級至 4.7 版本。 5. 將 Identity Applications 升級至 4.7。 6. 停止 Tomcat。
Identity Reporting	4.5.x (其中 x 為 0 至 5)	◆ 如果您使用的是 JBoss 或 Websphere，請移轉至 Tomcat 應用程式伺服器。 ◆ 套用 4.5.6 修補程式。	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。 3. 將事件稽核服務資料移轉至受支援版本的 PostgreSQL 或 Oracle 資料庫。 4. 安裝 SLM for IGA。 5. 更新資料收集服務和受管理服務閘道驅動程式套件。 6. 安裝 Identity Reporting 4.7。 7. 從 IDMDCS 頁面建立資料同步規則。

NetIQ 建議開始升級前先在您所用版本的版本說明中查看該資訊：

- 《NetIQ Identity Manager 4.5 Service Pack 6 Release Notes》 (NetIQ Identity Manager 4.5 Service Pack 4 版本說明)
- 《NetIQ Identity Manager 4.5 Service Pack 5 Release Notes》 (NetIQ Identity Manager 4.5 Service Pack 5 版本說明)
- 《NetIQ Identity Manager 4.5 Service Pack 4 Release Notes》 (NetIQ Identity Manager 4.5 Service Pack 4 版本說明)
- 《NetIQ Identity Manager 4.5 Service Pack 3 Release Notes》 (NetIQ Identity Manager 4.5 Service Pack 4 版本說明)
- 《NetIQ Identity Manager 4.5 Service Pack 2 Release Notes》 (NetIQ Identity Manager 4.5 Service Pack 4 版本說明)
- 《NetIQ Identity Manager 4.5 Service Pack 1 Release Notes》 (NetIQ Identity Manager 4.5 Service Pack 4 版本說明)
- 《NetIQ Identity Manager 4.5 版本說明》

31.5 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：

- 第 31.5.1 節「輸出 Designer 專案」(第 323 頁)
- 第 31.5.2 節「輸出驅動程式的組態」(第 324 頁)

31.5.1 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 323 頁)
- 「從 Identity Vault 建立新專案」(第 323 頁)

輸出目前的專案

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

1. 在 Designer 中開啟您的專案。
2. 在模型產生器中，請在 Identity Vault 上按一下滑鼠右鍵，然後選取「即時」> 「比較」。
3. 評估專案並調整差異，然後按一下「確定」。

   如需詳細資訊，請參閱《*NetIQ Designer for Identity Manager Administration Guide*》(NetIQ Designer for Identity Manager 管理指南) 中的「Using the Compare Feature When Deploying」(在部署時使用比較功能)。
4. 在工具列上選取「專案」> 「輸出」。
5. 按一下「全選」，以全選所有資源來加以輸出。
6. 選取專案的儲存位置及儲存格式，然後按一下「完成」。

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

從 Identity Vault 建立新專案

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

1. 安裝 Designer。
2. 啟動 Designer，然後為工作空間指定位置。
3. 選取是否要檢查線上更新，然後按一下「確定」。
4. 在「歡迎」頁上，按一下「執行 Designer」。
5. 在工具列上，選取「專案」> 「輸入專案」> 「Identity Vault」。
6. 指定專案名稱，然後針對專案使用預設位置或選取不同位置。
7. 按「下一步」。

8 指定以下用於連接 Identity Vault 的值：
   - **主機名稱**：代表 Identity Vault 伺服器的 IP 位址或 DNS 名稱
   - **使用者名稱**：代表用於向 Identity Vault 進行驗證的使用者 DN
   - **密碼**：代表驗證使用者的密碼
9 按「下一步」。
10 讓 Identity Vault 綱要和「預設通知集合」維持選取狀態。
11 展開「預設通知集合」，然後取消選取不需要的語言。
   「預設通知集合」會翻譯成多種語言。您可以輸入所有語言或只選取您使用的語言。
12 按一下「瀏覽」，然後瀏覽至要輸入的驅動程式集並加以選取。
13 針對此 Identity Vault 內的每個驅動程式集重複步驟 12，然後按一下「完成」。
14 專案輸入後按一下「確定」。
15 若您只有一個 Identity Vault，則所有作業已完成。如果您有多個 Identity Vault，請繼續進行步驟 16。
16 按一下工具列上的「即時」> 「輸入」。
17 對其他各個 Identity Vault 重複步驟 8 到步驟 14。

31.5.2 輸出驅動程式的組態

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

- 「使用 Designer 輸出驅動程式組態」（第 324 頁）
- 「使用 iManager 來建立驅動程式的輸出」（第 324 頁）

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。

使用 iManager 來建立驅動程式的輸出

1 在 iManager 中，選取「**Identity Manager**」> 「**Identity Manager 綜覽**」。
2 瀏覽並選取網路樹中的位置，來搜尋「驅動程式集」物件，然後按一下搜尋圖示 ▶。
3 按一下保存您要升級之驅動程式的「驅動程式集」物件。
4 按一下您要升級的驅動程式，然後按一下「輸出」。

5 按「下一步」，然後選取「輸出所有包含的規則 (無論是否連結至組態)」。

6 按「下一步」，然後按一下「另存新檔」。

7 選取「儲存至磁碟」，然後按一下「確定」。

8 按一下「完成」。

9 對每個驅動程式重複步驟 1 到步驟 8。

32 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。例如，您可能只想將 Designer 升級至最新版本，而不升級 iManager。本章還提供了可能需要在升級後執行的步驟。

- 第 32.1 節「升級 Designer」(第 327 頁)
- 第 32.2 節「升級 iManager」(第 328 頁)
- 第 32.3 節「升級遠端載入器」(第 331 頁)
- 第 32.4 節「升級 Identity Manager 引擎」(第 331 頁)
- 第 32.5 節「升級 Identity Applications 和 Identity Reporting」(第 332 頁)
- 第 32.6 節「升級 Identity Reporting」(第 341 頁)
- 第 32.7 節「升級 Analyzer」(第 343 頁)
- 第 32.8 節「升級 Identity Manager 驅動程式」(第 343 頁)
- 第 32.9 節「將新伺服器新增至驅動程式集」(第 345 頁)
- 第 32.10 節「將自訂規則還原至驅動程式」(第 346 頁)

32.1 升級 Designer

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. 從 Identity Manager 媒體啟動 Designer 安裝程式 (\products\Designer\install.exe)
4. 選取安裝 Designer 時要使用的語言，然後閱讀並接受授權合約。
5. 指定安裝 Designer 的目錄，然後在說明您已安裝 Designer 的訊息中按一下「是」。
6. 選擇捷徑應放在桌面上還是放在桌面功能表中。
7. 檢閱摘要，然後按一下安裝。
8. 檢閱《版本說明》，然後按下一步。
9. 選擇啟動 Designer，然後按一下「完成」。
10. 指定 Designer 工作空間的位置，然後按一下「確定」。
11. 在說明專案需要關閉和轉換的警告訊息中，按一下「確定」。
12. 在專案檢視窗中，展開專案，然後連按兩下專案需要轉換。
13. 檢閱專案轉換器精靈執行的步驟，然後按「下一步」。
14. 指定專案備份的名稱，然後按「下一步」。
15. 檢閱轉換期間執行的動作摘要，然後按一下「轉換」。
16. 在轉換完成後檢閱摘要，然後按一下「開啟」。

升級至最新版本的 Designer 後，必須從舊版本輸入所有 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 *《Designer for Identity Manager Administration Guide》*(Designer for Identity Manager 管理指南)。

32.2 升級 iManager

一般而言，iManager 升級程序會使用 configiman.properties 檔案中的現有組態值，例如，連接埠值和授權使用者。如果您以前修改了 server.xml 和 context.xml 組態檔案，NetIQ 建議在升級之前備份這些檔案。

如果您使用的是 eDirectory 9.1，請將 iManager 版本升級至 3.1。iManager 3.1 安裝檔案位於 <iso_extracted_directory>\products\iManager277\installs\win 目錄中。

升級程序包括以下活動：

- 第 32.2.1 節「在 Windows 上升級 iManager」(第 328 頁)
- 第 32.2.2 節「更新職能服務」(第 329 頁)
- 第 32.2.3 節「重新安裝或移轉 Plug-in Studio 的外掛程式」(第 330 頁)
- 第 32.2.4 節「在升級或重新安裝後更新 iManager 外掛程式」(第 330 頁)

32.2.1 在 Windows 上升級 iManager

如果 iManager Server 安裝程式偵測到以前安裝的 iManager 版本，可能會提示您升級已安裝版本。如果您選擇升級，安裝程式會將現有的 JRE 和 Tomcat 版本取代為最新版本。如此一來，iManager 也會升級為最新版本。

在升級 iManager 之前，請確保電腦符合先決條件和系統要求。如需詳細資訊，請參閱以下資訊來源：

- 更新隨附的 《版本說明》。
- 對於 iManager，請參閱「安裝 iManager 伺服器的注意事項」(第 128 頁)。
- 對於 iManager Workstation，請參閱「安裝 iManager Workstation 的注意事項」(第 128 頁)。

附註：升級程序使用舊版 iManager 中設定的 HTTP 連接埠值和 SSL 連接埠值。

若要在 Windows 上安裝 iManager 伺服器：

1. 以擁有管理員權限的使用者身分登入您要升級 iManager 的電腦。
2. (視情況而定) 如果您以前修改了 server.xml 和 context.xml 組態檔案，請在執行升級之前，在其他位置儲存這些檔案的備份副本。

   升級程序會取代這些組態檔案。
3. 在 NetIQ 下載網站上，選取所需的 iManager 版本，然後將 win.zip 檔案下載到伺服器上的某個目錄中。例如 iMan_277_win.zip。
4. 將該 win.zip 檔案擷取到 iManager 資料夾中。
5. 執行預設位於 extracted_directory\iManager\installs\win *資料夾中的* iManagerInstall.exe。
6. 在 iManager 歡迎視窗中選取一種語言，然後按一下**確定**。

7 在簡介視窗中，按下一步。

8 接受授權合約，然後按下一步。

9 (選擇性) 若要對 iManager 使用 IPv6 位址，請在啟用 **IPv6** 視窗中按一下是。

您也可以在升級 iManager 後啟用 IPv6 位址。如需詳細資訊，請參閱第 11.3.2 節「安裝後設定 iManager 以使用 IPv6 位址」(第 137 頁)。

10 按一下「下一步」。

11 系統出現升級提示時，請選取 **[升級]**。

12 (視情況而定) 檢閱偵測摘要視窗中的內容。

偵測摘要視窗列出了 iManager 在升級後會使用的最新版伺服器常式容器和 JVM 軟體。

13 按一下「下一步」。

14 閱讀安裝前摘要頁面，然後按一下安裝。

升級程序需費時數分鐘的時間。升級程序可能會新增 iManager 元件的新檔案或變更 iManager 組態。如需詳細資訊，請參閱升級目標版本的《版本說明》。

15 (視情況而定) 如果安裝完成視窗顯示以下錯誤訊息，請完成以下步驟：

```
The installation of iManager version is complete, but some errors occurred during the install.
Please see the installation log Log file path for details. Press "Done" to quit the installer.
```

15a 記下錯誤訊息中顯示的記錄檔案路徑。

15b 在安裝完成視窗中按一下完成。

15c 開啟記錄檔案。

15d (視情況而定) 如果您在記錄檔案中發現以下錯誤，則可以忽略該錯誤訊息。安裝成功，iManager 可正常運作。

```
Custom Action: com.novell.application.iManager.install.InstallDLLs
Status: ERROR
Additional Notes: ERROR - class com.novell.application.iManager.install.InstallDLLs
NonfatalInstallException C:\WINDOWS\system32\msvcr71.dll (The process cannot access the
file because it is being used by another process)
```

15e (視情況而定) 如果記錄檔案中未包含步驟 21d 中所列的錯誤，NetIQ 建議您重試安裝。

16 按一下「完成」。

17 iManager 啟始化完成後，按一下「開始使用」頁面中的第一個連結，然後登入。如需詳細資訊，請參閱《*NetIQ iManager Administration Guide*》(NetIQ iManager 管理指南) 中的「Accessing iManager」(存取 iManager)。

18 (視情況而定) 如果您在啟動升級程序之前建立了 server.xml 和 context.xml 組態檔案的備份副本，請將新的組態檔案取代為備份副本。

32.2.2 更新職能服務

當您首次使用 iManager 登入已包含角色服務 (RBS) 集合的 eDirectory 網路樹時，可能無法看到所有的角色資訊。這是正常行為，因為僅當您更新了某些外掛程式後，它們才能與最新版 iManager 配合運作。NetIQ 建議您將 RBS 模組更新為最新版本，這樣您就可以看到並使用 iManager 中的所有可用功能。「RBS 組態」表格會列出需要更新的 RBS 模組。

請注意，您的多種職能可能具有同一名稱。從 iManager 2.5 開始，某些外掛程式開發者變更了任務 ID 或模組名稱，但它們的顯示名稱卻保留不變。此問題導致有些角色看似重複，但事實上，兩個例項一個來自舊版本，另一個來自新版本。

附註：

- 在更新或重新安裝 iManager 時，安裝程式不會更新現有的外掛程式。若要手動更新外掛程式，請啟動 iManager 並導覽至**設定** > **外掛程式安裝** > **可用的 Novell 外掛程式模組**。如需詳細資訊，請參閱第 11.1.3 節「瞭解 iManager 外掛程式的安裝」(第 126 頁)。
- 不同的 iManager 安裝程式可能會在本地安裝不同數量的外掛程式。因此，在**角色服務** > **RBS 組態**頁面中，您可能會發現任一指定集合的模組報告都存在偏差。為了使不同 iManager 安裝的外掛程式數量保持一致，請務必在網路樹中的每個 iManager 例項上都安裝相同的外掛程式子集。

若要檢查並更新已過時的 RBS 物件：

1. 登入 iManager。
2. 在「設定」檢視窗中，選取「**職能服務**」> 「**RBS 組態**」。

   檢閱「2.*x* 集合」索引標籤頁面上的表格中有無過時的模組。
3. (選擇性) 若要更新某個模組，請完成以下步驟：

   3a 對於要更新的集合，選取**已過時**欄中的數字。

   Identity Manager 隨即會顯示已過時模組的清單。

   3b 選取要更新的模組。

   3c 按一下表格頂部的**更新**。

32.2.3 重新安裝或移轉 Plug-in Studio 的外掛程式

您可以將 Plug-in Studio 外掛程式移轉或複製到其他 iManager 例項中，以及新的或者更新的 iManager 版本中。

1. 登入 iManager。
2. 在 iManager 的「設定」檢視窗中，選取**角色服務** > **Plug-in Studio**。

   「內容」框架會顯示「已安裝的自訂外掛程式」清單，包括外掛程式隸屬之 RBS 集合的位置。
3. 選取您要重新安裝或移轉的外掛程式，然後按一下**編輯**。

   附註：一次只能編輯一個外掛程式。
4. 按一下「**安裝**」。
5. 對每個需要重新安裝或移轉的外掛程式重複上述步驟。

32.2.4 在升級或重新安裝後更新 iManager 外掛程式

升級或重新安裝 iManager 時，安裝程序不會更新現有外掛程式。確認外掛程式與正確的 iManager 版本相符。如需詳細資訊，請參閱第 11.1.3 節「瞭解 iManager 外掛程式的安裝」(第 126 頁)。

1. 開啟 iManager。
2. 導覽至**設定** > **外掛程式安裝** > **可用的 Novell 外掛程式模組**。
3. 更新外掛程式。

32.3 升級遠端載入器

如果您在執行遠端載入器，則需要升級遠端載入器的檔案。

附註：在升級 .Net 遠端載入器之前，請確定已在系統上成功安裝所有 Windows 更新。

---

1 建立遠端載入器組態檔案的備份。檔案的預設位置為 C:\...\RemoteLoader*remoteloadername*-config.txt。

2 驗證是否已停止驅動程式。如需指示，請參閱第 9.4.1 節「停止驅動程式」(第 81 頁)。

3 停止每一個驅動程式的遠端載入器服務或精靈。
   - **Windows：**在「遠端載入器主控台」中，選取遠端載入器例項，然後按一下「**停止**」。
   - **Java 遠端載入器：**dirxml_jremote -config *path_to_configfile* -u

4 使用 Windows 工作管理員停止 Icache 程序。

5 (視情況而定) 若要在 Windows 伺服器上執行靜默安裝，請確保 silent.properties 檔案包含安裝的遠端載入器檔案所在目錄的路徑。例如：

   ```
   X64_CONNECTED_SYSTEM_LOCATION=c:\novell\remoteloader\64bit
   ```

   安裝程式不會偵測先前已安裝版本的預設路徑。

6 執行遠端載入器的安裝程式。

   安裝程序會將檔案及二進位檔更新為目前版本。如需詳細資訊，請參閱第 III 部分「安裝 Identity Manager 引擎」(第 49 頁)。

7 完成安裝後，驗證組態檔案是否包含您的環境資訊。

8 (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，繼續進行步驟 9 (第 331 頁)。

9 啟動每一個驅動程式的遠端載入器服務或精靈。
   - **Java 遠端載入器：**dirxml_jremote -config *組態檔案的路徑*
   - **Windows：**在遠端載入器主控台中選取遠端載入器例項，然後按一下**啟動**。

32.4 升級 Identity Manager 引擎

當您升級 Identity Manager 引擎或個別更新 SAML 方法時，iMonitor 會顯示 SAML 方法的存在和不存在狀態旗標。您可以忽略不存在狀態旗標，因為 eDirectory 會正確使用更新後的方法。升級引擎時，升級程序會重新啟動 eDirectory，它會在內部負責使用更新後的 SAML 方法。如果您個別更新 SAML 方法，請手動重新啟動 eDirectory 伺服器以使用更新後的 SAML 方法。

開始升級前，請確定快取檔案中沒有任何事件。將 Identity Manager 引擎升級至 4.7 版本時，引擎安裝程式會清理現有的 MapDB 驅動程式工作快取檔案 (dx*)。不過，您必須在升級驅動程式後，手動移除現有的 MapDB 狀態快取檔案。否則，驅動程式可能無法啟動。以下 Identity Manager 驅動程式使用 MapDB 3.0.5：

- MS Azure
- JDBC
- DCS
- MSGW

- LDAP
- Salesforce
- ServiceNow

在升級遠端載入器和角色服務後，便可以升級 Identity Manager 引擎。升級程序會更新主機電腦上檔案系統中儲存的驅動程式 shim 檔案。

1 驗證是否已停止驅動程式。如需詳細資訊，請參閱第 9.4.1 節「停止驅動程式」(第 81 頁)。
2 透過 IDM *version*_Win:\products\idm\Windows\setup\idm_install.exe 啟動 Identity Manager 引擎的安裝程式。
3 選取要用於安裝的語言。
4 閱讀並接受授權合約。
5 若要更新 Identity Manager 引擎和驅動程式 shim 檔案，請選取以下選項：
   - **Identity Manager 伺服器**
   - **Identity Manager 的 iManager 外掛程式**
   - **驅動程式**
6 以 LDAP 格式指定擁有 eDirectory 管理權限的使用者和使用者密碼。
7 檢閱摘要，然後按一下「安裝」。
8 閱讀安裝摘要，然後按一下「完成」。

32.5 升級 Identity Applications 和 Identity Reporting

本節提供關於升級 Identity Applications 和支援軟體的資訊，其中包括更新以下元件的內容：

- Identity Manager 使用者應用程式
- One SSO Provider (OSP)
- Self-Service Password Reset (SSPR)
- Tomcat、JDK 和 ActiveMQ
- Identity Reporting

NetIQ 提供了一個升級程式來升級這些元件。此程式位於 Identity Manager 安裝套件的 products\CommonApplication\ 目錄中。導覽至包含 ApplicationUpgrade.exe 檔案的目錄。

升級後，元件會升級至以下版本：

- Tomcat – 8.5.27
- ActiveMQ – 5.15.2
- Java – 1.80_162
- One SSO Provider – 6.2.1
- Self-Service Password Reset – 4.2.0.4
- Identity Applications – 4.7.0
- Identity Reporting – 6.0.0

本節提供關於以下主題的資訊：

- 第 32.5.1 節「瞭解升級程式」(第 333 頁)
- 第 32.5.2 節「升級的先決條件和注意事項」(第 333 頁)
- 第 32.5.3 節「升級 PostgreSQL 資料庫」(第 334 頁)
- 第 32.5.4 節「系統要求」(第 336 頁)
- 第 32.5.5 節「升級 Identity Applications 的驅動程式套件」(第 336 頁)
- 第 32.5.6 節「使用引導式程序升級」(第 336 頁)
- 第 32.5.7 節「升級後任務」(第 339 頁)

32.5.1 瞭解升級程式

升級程序會從現有元件中讀取組態值。這些資訊包括 ism-configuration.properties、server.xml、SSPRConfiguration.xml 和其他組態檔案。升級程序會使用這些組態檔案在內部叫用各元件的升級程式。此外，此程式還會建立目前安裝的備份。

32.5.2 升級的先決條件和注意事項

執行升級前，請先檢閱以下注意事項：

- **Identity Manager 已升級至版本 4.5.6：**您不能從低於 4.5.6 的版本升級或移轉至版本 4.7。如需如何升級至 Identity Manager 4.5 的詳細資訊，請參閱《*NetIQ Identity Manager 安裝指南*》中的「升級 Identity Manager」。
- **系統要求：**升級程序至少需要 3 GB 可用磁碟空間，用於儲存目前的組態以及升級期間建立的暫存檔案。確認伺服器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。

  在 Windows 伺服器上，升級程式會將暫存檔案儲存在 %TEMP% 環境變數指定的目錄中。如果此目錄不能提供所需的空間，請將 TEMP 和 TMP 環境變數設定為檔案系統中具有足夠可用空間的某個目錄。如此會重新指示升級程式將檔案儲存到該目錄。

  若要將這些環境變數設定為不同的目錄，請在開始升級之前完成以下步驟：

  1. 開啟指令提示符並輸入以下指令：

     ```
     SET TMP=D:\custom_tmp
     SET TEMP=D:\custom_tmp
     ```

     其中，D:\custom_tmp 是具有足夠可用磁碟空間的目錄路徑。

     附註：對於叢集環境，請備份 Identity Applications 證書 (cacerts)。

  2. 從指令行啟動升級程式。
- **使用 Tomcat 做為應用程式伺服器：**此版本的 Identity Manager 僅支援使用 Tomcat 做為應用程式伺服器。

  附註：確定您已在之前的安裝期間使用便捷安裝程式安裝 Tomcat 應用程式伺服器。升級程序只允許您升級使用便捷安裝程式安裝的 Tomcat。

- **資料庫平台已升級：**此程式不會升級 Identity Applications 的資料庫平台。請手動將目前的資料庫版本升級至受支援的版本。若要升級 PostgreSQL 資料庫，請參閱「升級 PostgreSQL 資料庫」(第 334 頁)。

- **Identity Applications 和 Identity Reporting 驅動程式已升級：**確定您已升級 Identity Applications 和 Identity Reporting 的下列驅動程式。
  - 使用者應用程式驅動程式
  - 角色與資源驅動程式
  - 管理系統閘道驅動程式
  - 資料收集服務驅動程式

  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「Upgrading Installed Packages」(升級安裝的套件)。
- **管理員使用者擁有最高的存取權限：**向管理員使用者提供最高存取權限。
- **使用者帳戶控制設定已變更為「永不通知」：**移至**控制台 > 使用者帳戶**，然後將**使用者帳戶控制設定**變更為**永不通知**。
- **Self Service Password Reset：**若要從 SSPR 4.0 升級，請確定您已更新 CATALINA_OPTS 內容，並且 -Dsspr.application.Path 設定為儲存 SSPR 組態的資料夾。

  例如： set CATALINA_OPTS="-Dsspr.applicationPath=C:\sspr_data

  在升級前備份 SSPR LocalDB。若要輸出或下載 LocalDB，請執行以下步驟：
  1. 以管理員身分登入 SSPR 入口網站。
  2. 從下拉式功能表中導覽至**您的 ID > 組態管理員**。
  3. 按一下 **LocalDB**。
  4. 按一下**下載 LocalDB**。

32.5.3 升級 PostgreSQL 資料庫

重要：升級過程可能需要一段時間，時間長短取決於資料庫大小。因此，請相應規劃您的升級。

1. 停止伺服器上正在執行的 PostgreSQL 服務。
2. 重新命名 C:\Netiq\idm\apps 中的 postgres 目錄。

   例如，將 postgres 重新命名為 postgresql_9_3。
3. 安裝作業系統支援的 PostgreSQL 版本。

   選擇的位置必須與 PostgreSQL 的目前安裝位置不同。

   3a 掛接 Identity_Manager_4.7_Windows.iso 影像檔，並導覽至包含 PostgreSQL 安裝檔案的 products\CommonApplication\postgre_tomcat_install 目錄。

   3b 執行 TomcatPostgreSQL.exe 檔案來安裝 PostgreSQL 應用程式。

   安裝期間，請只選取 **PostgreSQL** 選項。

   附註：不要在 **PostgreSQL 詳細資料**頁面中提供任何資料庫詳細資料。確定取消選取了**建立資料庫登入帳戶**和**建立空資料庫**。
4. 停止新安裝的 PostgreSQL 服務。移至**服務**，搜尋 PostgreSQL 9.6 服務，然後停止該服務。

   附註：相應的使用者在提供有效的驗證資訊後，可以執行停止操作。

5 透過執行以下動作來變更新安裝的 PostgreSQL 目錄的許可權：

建立一個 postgres 使用者：

1. 移至控制台 > 使用者帳戶 > 使用者帳戶 > 管理帳戶。
2. 按一下新增使用者帳戶。
3. 在「新增使用者」頁面中，指定 postgres 做為使用者名稱，並提供該使用者的密碼。

為 postgres 使用者提供對現有和新安裝的 PostgreSQL 目錄的許可權：

1. 在 PostgreSQL 目錄上按一下滑鼠右鍵，然後移至內容 > 安全性 > 編輯。
2. 為該使用者選取完全控制，以提供完全許可權。
3. 按一下「套用」。

6 以 postgres 使用者的身分存取 PostgreSQL 目錄。

1. 以 postgres 使用者的身分登入伺服器。

   在登入之前，請驗證是否允許 postgres 使用者建立遠端連接，以確定此使用者可連接到 Windows 伺服器。
2. 開啟指令提示符，然後使用以下指令設定 PGPASSWORD ：

   ```
   set PGPASSWORD=<your pg password>
   ```
3. 切換至新安裝的 PostgreSQL 目錄。

   例如：C:\Users\postgres>cd C:\NetIQ\idm\apps1\postgresql962\bin。

7 從新 PostgreSQL 的 bin 目錄升級 PostgreSQL。執行以下指令，然後按一下 **Enter**。

```
pg_upgrade.exe --old-datadir "C:\NetIQ\idm\apps1\postgres\data" --new-datadir
"C:\NetIQ\idm\apps1\postgresql962\data" --old-bindir "C:\NetIQ\idm\apps1\postgres\bin" --new-
bindir "C:\NetIQ\idm\apps1\postgresql962\bin"
```

8 啟動升級後的 PostgreSQL 資料庫服務。

移至服務，搜尋 PostgreSQL 9.6 服務，然後啟動該服務。

附註：相應的使用者在提供有效的驗證資訊後，可以執行啟動操作。

---

9 停用舊 PostgreSQL 服務，以確定該服務不會自動啟動。

10 (選擇性) 從新安裝的 PostgreSQL 服務的 bin 目錄中刪除舊資料檔案。

1. 以 postgres 使用者的身分登入。
2. 導覽至 bin 目錄，並執行 analyze_new_cluster.bat 和 delete_old_cluster.bat 檔案。

   例如：C:\NetIQ\idm\apps1\postgresql961\bin

附註：僅當您想要刪除舊資料檔案時，才需要執行此步驟。

32.5.4 系統要求

升級程序會為所安裝元件的目前組態建立備份。確認伺服器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。

32.5.5 升級 Identity Applications 的驅動程式套件

本節介紹如何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的套件更新到最新版本。升級 Identity Applications 前必須先執行此任務。

1 在 Designer 中開啟目前的專案。
2 在套件目錄 > 輸入套件上按一下滑鼠右鍵。
3 選取相應的套件。例如，使用者應用程式驅動程式基礎套件。
4 按一下「確定」。
5 在開發人員檢視窗中，在該驅動程式上按一下滑鼠右鍵，然後按一下內容。
6 導覽至內容頁面中的套件索引標籤。
7 按一下右上角的新增套件 (+) 符號。
8 選取該套件，然後按一下確定。
9 部署並重新啟動驅動程式。
10 重複相同程序，以升級角色與資源服務驅動程式的套件。

附註：

- 確定使用者應用程式驅動程式以及角色與資源服務驅動程式連接至升級後的 Identity Manager。
- 如果您在升級使用者應用程式驅動程式套件時安裝了任何通知樣板，請將預設通知集合物件部署到您的 Identity Manager 伺服器。

32.5.6 使用引導式程序升級

以下程序介紹如何使用精靈升級 Identity Applications、OSP、SSPR、Tomcat、ActiveMQ 和 Identity Reporting。

1 登入要執行升級程序的伺服器。
2 掛接 .iso 影像檔，導覽至包含升級可執行檔的目錄 (預設位於 products\CommonApplication\ 目錄中)。
3 啟動升級程式。以滑鼠右鍵按一下 ApplicationUpgrade.exe 並選取以管理員身分執行。
4 在簡介頁面上，您可以檢視可升級的 Identity Manager 元件，然後按下一步。
5 閱讀並接受授權合約，然後按「下一步」。
6 檢閱已部署的應用程式頁面，然後按下一步。

   此頁面會列出目前安裝的元件及其版本。如果在該伺服器上部署了其他應用程式，則升級程序會顯示警告，指出升級後這些應用程式可能會無法正常運作。

   您必須手動從升級程序建立的備份還原它們。
7 若要繼續升級，請按下一步。

8 使用以下參數完成引導式程序。此程式會自動填入現有元件的值。確認為參數指定了正確的值。

- **One SSO Provider 安裝資料夾**

  代表升級程式要在其中建立 OSP 應用程式檔案的目錄路徑。如果該路徑不正確，請瀏覽到 OSP 的安裝路徑。

- **SSPR 安裝資料夾**

  代表升級程式要在其中建立 SSPR 應用程式檔案的目錄路徑。如果該路徑不正確，請瀏覽到 SSPR 的安裝路徑。

- **使用者應用程式安裝資料夾**

  代表升級程式要在其中建立使用者應用程式的應用程式檔案的目錄路徑。如果該路徑不正確，請瀏覽到使用者應用程式的安裝路徑。

- **資料庫連接**

  代表用於連接使用者應用程式資料庫的設定，Identity Applications 也會連接到此資料庫。升級程式會將這些詳細資料包含在使用者應用程式組態檔案中。

  資料庫平台

  代表使用者應用程式資料庫的平台。

  資料庫主機

  指定代管使用者應用程式的伺服器的名稱或 IP 位址。

  資料庫連接埠

  指定資料庫伺服器用於與使用者應用程式通訊的連接埠。

  資料庫驅動程式 JAR 檔案

  指定資料庫平台的 jar 檔案。

  資料庫廠商會提供驅動程式 JAR 檔案，即資料庫伺服器的 JAR。例如，對於 PostgreSQL，可以指定預設位於 C:\NetIQ\idm\apps\postgres 中的 postgresql-9.4-1212.jdbc42.jar。同樣，指定您資料庫平台的相應 jar 檔案。

- **(視情況而定) Reporting 資料庫連接**

  代表用於連接 Identity Reporting 資料庫的設定。

  資料庫主機

  指定代管使用者應用程式的伺服器的名稱或 IP 位址。

  資料庫連接埠

  指定資料庫伺服器用於與使用者應用程式通訊的連接埠。

  資料庫名稱

  指定資料庫的名稱。資料庫名稱預設為 idmrptdb。

- **(視情況而定) Reporting 資料庫身分證明**

  Reporting 資料庫使用者

  指定使用者應用程式用來存取和修改資料庫中資料的帳戶名稱。資料庫使用者名稱預設為 postgres。

  Reporting 資料庫密碼

  提供所指定使用者名稱的密碼。

  升級 Reporting 資料庫

  立即升級資料庫：升級程式會在升級過程中更新 Reporting 資料庫表的綱要。

在應用程式啟動時升級資料庫：升級程式會發出在升級後使用者應用程式首次啟動時為資料庫表格更新綱要的指示。

將 SQL 寫入檔案：產生一個 SQL 程序檔，資料庫管理員可以執行該程序檔來更新資料庫。如果您選擇此選項，則還必須為**綱要檔案**指定名稱。設定位於 **SQL 輸出**檔案組態中。如果您無權在您的環境中建立或修改資料庫，則可選取此選項。如需使用該檔案產生表的詳細資訊，請參閱第 15.7.2 節「手動建立資料庫綱要」(第 195 頁)。

資料庫驅動程式 JAR 檔案

指定資料庫平台的 jar 檔案。

資料庫廠商會提供驅動程式 JAR 檔案，即資料庫伺服器的 JAR。例如，對於 PostgreSQL，可以指定預設位於 C:\NetIQ\idm\apps\postgres 中的 postgresql-9.4-1212.jdbc42.jar。同樣，指定您資料庫平台的相應 jar 檔案。

- **升級資料庫**

立即升級資料庫

升級程式會在升級過程中為資料庫表格更新綱要。

在應用程式啟動時升級資料庫

升級程式會發出在升級後使用者應用程式首次啟動時為資料庫表格更新綱要的指示。

將 SQL 寫入檔案

產生一個 SQL 程序檔，資料庫管理員可以執行該程序檔來更新資料庫。如果您選擇此選項，則還必須為**綱要檔案**指定名稱。設定位於 **SQL 輸出**檔案組態中。如果您無權在您的環境中建立或修改資料庫，則可選取此選項。如需使用該檔案產生表的詳細資訊，請參閱第 15.7.2 節「手動建立資料庫綱要」(第 195 頁)。

- **資料庫管理員**

代表資料庫管理員的名稱和密碼。

資料庫使用者名稱

指定可建立資料庫表格、檢視和其他產出工件的資料庫管理員帳戶。

密碼

指定資料庫管理員的密碼。

- **Reporting 資料庫連接**

代表資料庫管理員的主機名稱和密碼。

資料庫使用者名稱

指定可建立資料庫表格、檢視和其他產出工件的資料庫管理員帳戶。

密碼

指定資料庫管理員的密碼。

9 檢閱**升級前摘要**頁面，然後按一下**安裝**。

升級程序會停止 Tomcat 服務並開始升級，完成此程序可能需要一段時間。

10 當升級過程完成時，檢閱 /tmp/rbpm_upgrade/ 中的升級記錄檔案，您需要手動更新數個組態，請參閱第 32.5.7 節「升級後任務」(第 339 頁)。

依據元件的安裝位置，安裝程序會在該位置建立備份目錄，並將時戳 (指示備份時間) 附加至備份目錄。

例如，

- Tomcat – C:\NetIQ\idm\apps\tomcat_backup_02262018_033634

- OSP 和 SSPR - C:\NetIQ\idm\apps\osp_sspr_backup_02262018_033634
- ActiveMQ - C:\NetIQ\idm\apps\activemq_backup_02262018_033634
- 使用者應用程式 - C:\NetIQ\idm\apps\UserApplication_backup_02262018_033634
- Identity Reporting - C:\NetIQ\idm\apps\IdentityReporting_backup_02262018_033634

32.5.7 升級後任務

升級 Identity Applications 後，請務必執行下列操作：

您還必須手動還原 Tomcat、SSPR、OSP 或 Identity Applications 的自訂設定。

針對所需元件執行升級後步驟：

- 「Java」(第 339 頁)
- 「Tomcat」(第 339 頁)
- 「Identity Applications」(第 340 頁)
- 「One SSO Provider」(第 341 頁)
- 「Self-Service Password Reset」(第 341 頁)
- 「Kerberos」(第 341 頁)

Java

對照舊 JRE 的位置，驗證新升級 JRE 位置中的證書： jre\lib\security\cacerts。手動將缺少的證書輸入到 cacerts 中。

1 使用 keytool 指令輸入 java cacerts ：

```
keytool -import -trustcacerts -file Cerificate_Path -alias ALIAS_NAME -keystore cacerts
```

附註：升級後，JRE 儲存在 Identity Applications 安裝位置。例如：C:\NetIQ\idm\apps\jre

2 驗證 JRE 主目錄位置是否為 tomcat\bin\setenv.bat。

3 啟動組態更新公用程式，並驗證您的 cacerts 路徑。

Tomcat

1 (視情況而定) 若要從升級程序先前建立的備份還原自訂檔案，請執行以下任務：

- 還原自訂的 https 證書。若要還原這些證書，請將所備份 server.xml 中的 Java Secure Socket Extension (JSSE) 內容複製到 \tomcat\conf 目錄下的新 server.xml 檔案中。
- 不要將所備份 Tomcat 目錄中的組態檔案複製到新 Tomcat 目錄中。應視需要在新版本預設組態的基礎上進行變更。如需詳細資訊，請造訪此 Apache 網站。

  驗證新 server.xml 檔案是否包含以下項目

```
<Connector port="8543" protocol="HTTP/1.1"
       maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
       clientAuth="false" sslProtocol="TLS"
       keystoreFile="path_to_keystore_file"
       keystorePass="keystore_password" />
<!--
      <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
 -->
```

或

```
<Connector port="8543" protocol="org.apache.coyote.http11.Http11NioProtocol"
       maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
       clientAuth="false" sslProtocol="TLS"
       keystoreFile="path_to_keystore_file"
       keystorePass="keystore_password" />
<!--
      <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
 -->
```

附註：在叢集環境中，手動取消備註 server.xml 中的 Cluster 標記，然後將第一個節點上的 osp.jks (位於 C:\netiq\idm\apps\osp_backup_<date> 中) 複製到所有節點上。

- 如果您自訂了金鑰儲存區檔案，請在新 server.xml 檔案中包括正確的路徑。
- 將 Identity Applications 證書輸入到 Identity Vault 中 (位於 C:\NetIQ\eDirectory\jre\lib\security\cacerts)。

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

  ```
  keytool -importkeystore -alias <User Application certificate alias> -srckeystore  <backup cacert> -srcstorepass changeit -destkeystore C:\NetIQ\eDirectory\jre\lib\security\cacerts
  ```

2 (視情況而定) 導覽至使用者應用程式，然後透過讀取備份的組態手動還原自訂設定。

Identity Applications

從升級期間建立的備份還原 Identity Applications 自訂組態。

如果您要從 4.5.6 版本升級 Identity Manager，則必須為要用於在 Identity Manager 儀表板中對使用者排序的每個屬性手動建立複合索引，請參閱 「建立複合索引」(第 188 頁)。

1 啟動 configupdate 公用程式 (configupdate.bat) 檔案。

  在 configupdate.bat.properties 檔案中，確定 use_console 的值設定為 false。

2 連接 Identity Vault 伺服器，並接受 eDirectory 證書。

3 在 **SSO 用戶端**索引標籤中，導覽至 **RBPM**，然後按一下**顯示進階選項**。

4 將 **RBPM 至 eDirectory SAML 組態**設定為「自動」。

One SSO Provider

logevent.conf 檔案中的 LogHost 項目預設設定為 localhost。

若要修改 LogHost 項目，請手動從升級期間建立的備份還原 OSP 自訂組態。

Self-Service Password Reset

升級 SSPR 後，使用組態更新公用程式來更新 SSO 用戶端參數。如需詳細資訊，請參閱 第 15.8.5 節「SSO 用戶端參數」(第 218 頁) 中的 「Self Service Password Reset」(第 222 頁)。

若要更新 SSPR 組態詳細資料，請執行以下步驟：

1. 以管理員身分登入 SSPR 入口網站。
2. 更新稽核伺服器詳細資料：
   - **2a** 導覽至**您的 ID > 組態編輯器**，指定組態密碼。
   - **2b** 選取**設定 > 稽核 > 稽核轉遞 > Syslog 稽核伺服器證書**。
   - **2c** 從伺服器輸入這些證書，然後按一下**儲存**。
3. 將 **LocalDB** 輸入 SSPR ：
   - **3a** 從下拉式功能表導覽至**您的 ID > 組態管理員**。
   - **3b** 按一下 **LocalDB**。
   - **3c** 按一下**輸入 (上傳) LocalDB 歸檔檔案**。
4. (視情況而定) 若要限制 SSPR 的組態：
   - **4a** 從清單中導覽至**您的 ID > 組態管理員**。
   - **4b** 按一下**限制組態**。
5. 設定 SSPR 的管理員許可權，請參閱第 14.2.3 節「安裝後任務」(第 160 頁)。

若要驗證升級是否成功，請啟動升級的元件。

例如，啟動 Identity Manager 儀表板，按一下**關於**。檢查應用程式顯示的是否為新版本，例如 **4.7.0**。

Kerberos

升級公用程式會在電腦上建立新的 Tomcat 資料夾。如果任何 Kerberos 檔案 (例如 keytab 和 Kerberos_login.config) 存放在舊 Tomcat 資料夾中，請從備份資料夾中將這些檔案複製到新 Tomcat 資料夾。

32.6 升級 Identity Reporting

Identity Reporting 中包含兩個驅動程式。此外，您需要將 NetIQ Event Auditing Service 中的內容移轉至 Sentinel Log Management for IGA。依照以下順序執行升級：

1. 升級資料收集服務的驅動程式套件。
2. 升級受管理系統閘道服務的驅動程式套件。
3. 移轉至 Sentinel Log Management for IGA
4. 升級 Identity Reporting

32.6.1 升級 Identity Reporting 的驅動程式套件

本節說明如何將受管理系統閘道驅動程式套件和資料收集服務驅動程式套件更新到最新版本。您必須先執行此任務，然後再升級 Identity Reporting。

1 在 Designer 中開啟目前的專案。
2 在**套件目錄 > 輸入套件**上按一下滑鼠右鍵。
3 選取相應的套件。例如，**受管理系統閘道基礎套件 2.0.0.20120509205929**。
4 按一下「**確定**」。
5 在開發人員檢視窗中，在該驅動程式上按一下滑鼠右鍵，然後按一下**內容**。
6 導覽至**內容**頁面中的**套件**索引標籤。
7 按一下右上角的**新增套件 (+)** 符號。
8 選取該套件，然後按一下**確定**。
9 完成驅動程式的組態程序。如需詳細資訊，請參閱以下各節：
   - 第 19.1.2 節「設定受管理系統閘道驅動程式」(第 242 頁)
   - 第 19.1.3 節「設定資料收集服務的驅動程式」(第 243 頁)
10 重複步驟 2 至步驟 9，以升級資料收集服務驅動程式套件。
11 確保受管理系統閘道驅動程式和資料收集服務驅動程式已連接到升級後的 Identity Manager。

32.6.2 升級 Identity Reporting

升級 Identity Reporting 前必須先升級 Identity Applications 和 SLM for IGA。若要從 4.0.2 或更高版本升級 Identity Reporting，請在舊版本的基礎上安裝新版本。如需詳細資訊，請參閱「安裝 Identity Reporting」(第 231 頁)。

32.6.3 變更對資料庫中 reportRunner 的參考

升級 Identity Reporting 後，請務必在第一次啟動 Tomcat 之前更新對資料庫中 reportRunner 的參考。

1 停止 Tomcat。
2 導覽至 Identity Reporting 安裝目錄，然後將 reportContent 資料夾重新命名為 ORG-reportContent。

   例如：C:\NetIQ\idm\apps\IdentityReporting
3 清理 Tomcat 資料夾下的臨時目錄和工作目錄。
4 登入 PostgreSQL 資料庫。
   4a 在下面的表中尋找 reportRunner 參考：
      - idm_rpt_cfg.idmrpt_rpt_params
      - idm_rpt_cfg.idmrpt_definition
   4b 發出以下 delete 陳述式：

```
DELETE FROM idm_rpt_cfg.idmrpt_rpt_params WHERE
rpt_def_id='com.novell.content.reportRunner';

DELETE FROM idm_rpt_cfg.idmrpt_definition WHERE def_id='com.novell.content.reportRunner';
```

5 啟動 Tomcat。

檢查記錄以確定使用正確的 reportRunner 是否可重新產生報告。

6 登入 Identity Reporting 並執行報告。

32.6.4 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。

32.7 升級 Analyzer

NetIQ 提供了 .zip 格式的修補程式檔案以協助您升級 Analyzer。在升級 Analyzer 之前，請確保電腦符合先決條件和系統要求。如需詳細資訊，請參閱更新隨附的 《版本說明》。

1 從 NetIQ 下載網站下載修補程式檔案，例如 analyzer_4.6_patch1_20121128.zip。
2 將該 .zip 檔案擷取到包含 Analyzer 安裝檔案 (例如外掛程式、解除安裝程序檔和其他 Analyzer 檔案) 的目錄。
3 重新啟動 Analyzer。
4 若要驗證您是否已成功套用新的修補程式，請完成以下步驟：
   4a 啟動 Analyzer。
   4b 按一下**說明 > 關於 Analyzer**。
   4c 檢查程式是否顯示了新版本，例如 **4.6 Update 1** 和版次 ID **20121128**。

32.8 升級 Identity Manager 驅動程式

NetIQ 透過**套件**而不是驅動程式組態檔案提供新驅動程式內容。您可以在 Designer 中管理、維護和建立套件。雖然 iManager 支援套件，但 Designer 不會保留您在 iManager 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「Managing Packages」(管理套件)。

附註：如果您將 3.*x* 版的使用者應用程式驅動程式升級至使用者應用程式 4.0.2 版套件，Designer 會安裝相同驅動程式規則的 3.*x* 版與 4.0 版。套件目錄中同時具有 3.*x* 與 4.0 規則可能會導致 Designer 無法正常運作。請刪除 3.*x* 版規則並保留 4.0 版規則。

您可透過以下方式將驅動程式升級至套件：

- 第 32.8.1 節「建立新驅動程式」(第 344 頁)
- 第 32.8.2 節「以套件中的內容取代現有內容」(第 344 頁)
- 第 32.8.3 節「保留目前內容並透過套件新增新內容」(第 344 頁)

32.8.1 建立新驅動程式

刪除現有驅動程式，然後建立包含套件的新驅動程式，是將驅動程式升級為套件的最簡便的方法。可以在這個新驅動程式中新增您需要的所有功能。相關步驟因驅動程式而異。如需指示，請參閱 Identity Manager 驅動程式文件網站中個別驅動程式的指南。驅動程式現在可如往常一樣運作，但其內容來自套件而不是驅動程式組態檔案。

32.8.2 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，請參閱第 31.5.2 節「輸出驅動程式的組態」(第 324 頁)。

2 在 Designer 中刪除驅動程式內儲存的所有物件。請刪除驅動程式內儲存的規則、過濾器、授權及所有其他項目。

附註：Designer 提供了自動輸入機制，用於輸入最新的套件。您不需要手動將驅動程式套件輸入至套件目錄。

如需詳細資訊，請參閱《*NetIQ Designer for Identity Manager Administration Guide*》(NetIQ Designer for Identity Manager 管理指南) 中的「Importing Packages into the Package Catalog」(將套件輸入至套件目錄)。

---

3 將最新的套件安裝到驅動程式中。

   以上步驟視驅動程式而定。如需指示，請參閱 Identity Manager 驅動程式文件網站中各驅動程式的指南。

4 將任何自訂規則還原至驅動程式。如需指示，請參閱第 32.10 節「將自訂規則還原至驅動程式」(第 346 頁)。

32.8.3 保留目前內容並透過套件新增新內容

您可以將驅動程式保留為目前狀態，並透過套件將新功能新增至驅動程式，只要套件中的功能與驅動程式的目前功能不重疊。

在安裝套件之前，請建立驅動程式組態檔案的備份。當您安裝套件時，它或許會覆寫現有規則，這可能會導致驅動程式停止運作。如果某個規則被覆寫，您可以輸入備份驅動程式組態檔案，然後重新建立該規則。

開始之前，確定所有自訂規則都具有與預設規則不同的規則名稱。以新的驅動程式檔案覆寫驅動程式組態時，就會覆寫現有規則。如果自訂規則的名稱不唯一，您將會遺失這些自訂規則。

若要透過套件將新內容新增至驅動程式：

1 建立驅動程式及其中所有自訂內容的備份。

   如需指示，請參閱第 31.5.2 節「輸出驅動程式的組態」(第 324 頁)。

附註：Designer 提供了自動輸入機制，用於輸入最新的套件。您不需要手動將驅動程式套件輸入至套件目錄。

如需詳細資訊，請參閱《*NetIQ Designer for Identity Manager Administration Guide*》(NetIQ Designer for Identity Manager 管理指南) 中的「Importing Packages into the Package Catalog」(將套件輸入至套件目錄)。

2 將套件安裝到驅動程式中。

如需指示，請參閱 Identity Manager 驅動程式文件網站中各驅動程式的指南。

3 將所需的套件新增到驅動程式中。以上步驟視驅動程式而定。

如需詳細資訊，請造訪 Identity Manager 驅動程式文件網站。

驅動程式即包含由套件新增的新功能。

32.9 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 iManager 更新驅動程式集。

32.9.1 將新伺服器新增至驅動程式集

若您使用的是 iManager，就必須將新伺服器新增至驅動程式集。Designer 包含的伺服器移轉精靈可為您執行此步驟。若您使用的是 Designer，請跳至第 35.3.1 節「在 Designer 中複製伺服器特定資訊」(第 357 頁)。若您使用的是 iManager，請完成下列程序：

1 在 iManager 中按一下 以顯示 Identity Manager 管理頁面。

2 按一下「**Identity Manager 綜覽**」。

3 瀏覽並選取保有驅動程式集的容器。

4 按一下驅動程式集名稱，以存取「驅動程式集綜覽」頁面。

5 按一下「**伺服器**」> 「**新增伺服器**」。

6 瀏覽至新的 Identity Manager 伺服器並加以選取，然後按一下「**確定**」。

32.9.2 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 345 頁)
- 「使用 iManager 從驅動程式集移除舊的伺服器」(第 346 頁)
- 「解除舊伺服器」(第 346 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 iManager 從驅動程式集移除舊的伺服器

1 在 iManager 中按一下 以顯示 Identity Manager 管理頁面。

2 按一下「**Identity Manager 綜覽**」。

3 瀏覽並選取保有驅動程式集的容器。

4 按一下驅動程式集名稱，以存取「驅動程式集綜覽」頁面。

5 按一下「**伺服器**」>「**遠端伺服器**」。

6 選取舊的 Identity Manager 伺服器，然後按一下「**確定**」。

解除舊伺服器

於此時，舊伺服器未代管任何驅動程式。如果不再需要此伺服器，則另外還必須完成以下步驟解除其職能：

1 從此伺服器上移除 eDirectory 複製本。

如需詳細資訊，請參閱《*NetIQ eDirectory Administration Guide*》(NetIQ eDirectory 管理指南) 中的「Deleting Replicas」(刪除複製本)。

2 從此伺服器上移除 eDirectory。

如需詳細資訊，請參閱 TID 10056593，從 NDS 網路樹永久移除伺服器。

32.10 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。

- 第 32.10.1 節「使用 Designer 將自訂規則還原至驅動程式」(第 346 頁)
- 第 32.10.2 節「使用 iManager 將自訂規則還原至驅動程式」(第 347 頁)

32.10.1 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，請參閱第 9.4.2 節「啟動驅動程式」(第 82 頁)。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。

32.10.2 使用 iManager 將自訂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 iManager 中，選取「**Identity Manager**」>「**Identity Manager 綜覽**」。

2 瀏覽並選取網路樹中的位置，來搜尋「驅動程式集」物件，然後按一下搜尋圖示 ▶。

3 按一下包含已升級驅動程式的「驅動程式集」物件。

4 按一下驅動程式圖示，然後選取您需要還原自訂規則的規則集。

5 按一下「**插入**」。

6 選取「**使用現有規則**」，然後瀏覽並選取自訂規則。

7 按一下「**確定**」，然後按一下「**關閉**」。

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 3 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，請參閱第 9.4.2 節「啟動驅動程式」(第 82 頁)。iManager 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。

33 從 Advanced Edition 切換到 Standard Edition

僅當您不想在環境中使用任何 Advanced Edition 功能，並且要縮減 Identity Manager 部署時，才應切換至 Standard Edition。

1 (視情況而定) 如果您已套用 Advanced Edition 啟用，請移除該啟用。
2 (視情況而定) 若要切換到 Standard Edition 評估模式：
   - **2a** 導覽至 C:\Novell\NDS\DIBFiles 中的 Identity Vault dib 目錄。
   - **2b** 建立一個新檔案，將其命名為 .idme，並在其中新增 2(數值)。
   - **2c** 重新啟動 eDirectory。
   - **2d** 繼續執行步驟 4。
3 (視情況而定) 如果您已採購 Standard Edition 啟用，請套用該啟用。
4 停止 Tomcat。
5 從 C:\NetIQ\idm\apps\tomcat\webapps 目錄中移除以下 WAR 檔案和 Webapps 資料夾：
   - IDMProv*
   - IDMRPT*
   - dash*
   - idmdash*
   - landing*
   - rra*
   - rptdoc*
6 將以下現有資料夾移到備份目錄：
   - IDMReporting
   - UserApplication
7 將 < 安裝資料夾 >/tomcat/conf 目錄中的 ism-configuration.properties 檔案複製到備份目錄。
8 從 Identity Manager 4.6 媒體安裝 Identity Reporting。
9 從 <*Reporting 安裝資料夾*>/bin 目錄啟動 configupdate.bat，然後指定以下參數的值：

   「**報告**」**索引標籤**：指定以下區段中的設定：
   - ID Vault
   - Identity Vault 使用者身分
   - 報告管理員
     - **報告管理員角色容器 DN**. 例如，ou=sa,o=data
     - **報告管理員**。例如，cn=uaadmin,ou=sa,o=data

「**驗證**」索引標籤：指定以下區段中的設定：

- 驗證伺服器
  - **OAuth 伺服器主機識別碼** . 例如，驗證伺服器的 IP 位址或 DNS 名稱 (如 192.99.17.22)
  - **OAuth 伺服器 TCP 連接埠**
  - **OAuth 伺服器正在使用 TLS/SSL**
- 驗證組態
  - **OAuth 金鑰儲存區檔案** . 例如，C:\NetIQ\idm\apps\osp\osp.jks
  - **OAuth 使用之金鑰的金鑰別名**
  - **OAuth 所用金鑰的金鑰密碼**
  - **工作階段逾時 (分鐘)**. 例如，60 分鐘。

「**SSO 用戶端**」索引標籤：指定以下區段中的設定：

- 報告
  - **抵達頁面的 URL 連結** . 例如，http://192.99.17.22:8180/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://192.99.179.202:8180/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 204 頁)。

10 儲存變更並結束組態公用程式。

11 啟動 Tomcat。

X 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 IX 部分「升級 Identity Manager」(第 315 頁)。如需升級與移轉之間差異的詳細資訊，請參閱第 31.2 節「瞭解升級和移轉」(第 319 頁)。

34 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。

34.1 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. 確定您應該執行升級，還是執行移轉。如需詳細資訊，請參閱第 31.2 節「瞭解升級和移轉」(第 319 頁)。
❑	2. 確保您已取得用於移轉 Identity Manager 資料的最新安裝套件。
❑	3. 瞭解 Identity Manager 各元件之間的互動。如需詳細資訊，請參閱第 I 部分「介紹」(第 17 頁)。
❑	4. 確保您的電腦符合更高版本 Identity Manager 的硬體和軟體先決條件。如需詳細資訊，請參閱第 6 章「安裝注意事項」(第 45 頁) 和您要升級至的版本的《版本說明》。
❑	5. 將 eDirectory 升級至 Identity Vault 的最新受支援版本。如需詳細資訊，請參閱第 7.1.2 節「安裝 Identity Vault 的先決條件和考量」(第 52 頁)。
❑	6. 將目前 Identity Manager 伺服器上的 eDirectory 複製本新增至新伺服器。如需詳細資訊，請參閱第 35.4 節「將 Identity Manager 引擎移轉至新伺服器」(第 358 頁)。
❑	7. 在新伺服器上安裝 Identity Manager。如需詳細資訊，請參閱「規劃安裝 Identity Manager」(第 35 頁)。
❑	8. (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，請參閱第 32.3 節「升級遠端載入器」(第 331 頁)。
❑	9. (視情況而定) 如果您是在舊伺服器上執行使用者應用程式，請更新該元件及其驅動程式。如需詳細資訊，請參閱第 35.1 節「Identity Manager 的移轉核對清單」(第 355 頁)。
❑	10. 將新伺服器新增至驅動程式集。如需詳細資訊，請參閱第 32.9.1 節「將新伺服器新增至驅動程式集」(第 345 頁)。
❑	11. 變更每個驅動程式的伺服器特定資訊。如需詳細資訊，請參閱第 35.3.1 節「在 Designer 中複製伺服器特定資訊」(第 357 頁)。
❑	12. (視情況而定) 如果您在使用 RBPM，請將使用者應用程式的伺服器特定資訊從舊伺服器更新為新伺服器。如需詳細資訊，請參閱第 35.3 節「複製驅動程式集的伺服器特定資訊」(第 356 頁)
❑	13. 將驅動程式更新為套件格式。如需詳細資訊，請參閱第 32.8 節「升級 Identity Manager 驅動程式」(第 343 頁)。
❑	14. (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，請參閱第 32.10 節「將自訂規則還原至驅動程式」(第 346 頁)。

	核對清單項目
❑	15. 從驅動程式集移除舊的伺服器。如需詳細資訊，請參閱第 32.9.2 節「從驅動程式集移除舊的伺服器」(第 345 頁)。
❑	16. 啟用升級後的 Identity Manager 解決方案。如需詳細資訊，請參閱第 30.6 節「啟用 Identity Manager」(第 310 頁)。

34.2 在移轉期間停止和啟動 Identity Manager 驅動程式

在升級或移轉 Identity Manager 時，您需要啟動和停止驅動程式，以確保升級或移轉程序能夠修改或取代正確的檔案。本節包括以下活動。如需詳細資訊，請參閱以下各節：

- 第 9.4.1 節「停止驅動程式」(第 81 頁)
- 第 9.4.2 節「啟動驅動程式」(第 82 頁)

35 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：

- 第 35.1 節「Identity Manager 的移轉核對清單」(第 355 頁)
- 第 35.2 節「準備用於移轉的 Designer 專案」(第 356 頁)
- 第 35.3 節「複製驅動程式集的伺服器特定資訊」(第 356 頁)
- 第 35.4 節「將 Identity Manager 引擎移轉至新伺服器」(第 358 頁)
- 第 35.5 節「移轉使用者應用程式驅動程式」(第 358 頁)
- 第 35.6 節「升級 Identity Applications」(第 360 頁)
- 第 35.7 節「完成 Identity Applications 的移轉」(第 360 頁)

35.1 Identity Manager 的移轉核對清單

NetIQ 建議您完成以下核對清單中的步驟。

	核對清單項目
❑	1. 備份 Identity Manager 解決方案的目錄和資料庫。
❑	2. 確保您已安裝最新版本的 Identity Manager 元件 (Identity Applications 除外)。如需詳細資訊，請參閱第 5.3.4 節「建議的伺服器設定」(第 41 頁) 和元件的最新 《版本說明》。 **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 15 章 「安裝 Identity Applications」(第 165 頁)。
❑	3. 執行 Identity Vault 狀態檢查，以確保綱要可正常延伸。請使用 TID 3564075 完成健康狀態檢查。
❑	4. 將現有的使用者應用程式驅動程式輸入到 Designer 中。
❑	5. 將 Designer 專案歸檔。它代表移轉前狀態的驅動程式。如需詳細資訊，請參閱第 35.2 節「準備用於移轉的 Designer 專案」(第 356 頁)。
❑	6. (視情況而定) 若要將 Identity Manager 引擎移轉至某個新伺服器，請將 eDirectory 複製本複製到這個新伺服器上。如需詳細資訊，請參閱第 35.4 節「將 Identity Manager 引擎移轉至新伺服器」(第 358 頁)。
❑	7. 在最新版 Designer 中建立一個新 Designer 專案，然後輸入使用者應用程式驅動程式，為移轉做好準備。
❑	8. 移轉使用者應用程式驅動程式。如需詳細資訊，請參閱第 35.5 節「移轉使用者應用程式驅動程式」(第 358 頁)。

	核對清單項目
❑	9. 建立新的角色與資源服務驅動程式。 您無法移轉現有的角色與資源服務驅動程式。如需詳細資訊，請參閱第 15.6.3 節「建立角色與資源服務驅動程式」(第 193 頁)。
❑	10. 將兩個驅動程式部署到 Identity Vault。如需詳細資訊，請參閱第 15.6.4 節「部署使用者應用程式的驅動程式」(第 194 頁)。
❑	11. 升級 Identity Applications。如需詳細資訊，請參閱第 32.5 節「升級 Identity Applications 和 Identity Reporting」(第 332 頁)。
❑	12. 確保您的瀏覽器不包含先前版本 Identity Manager 的內容。如需詳細資訊，請參閱第 35.7.1 節「衝洗瀏覽器快取」(第 360 頁)。
❑	13. (視情況而定) 恢復 SharedPagePortlet 的自訂設定。如需詳細資訊，請參閱第 35.7.3 節「更新 SharedPagePortlet 的最大逾時設定」(第 360 頁)。
❑	14. 確保在使用者未提供過濾參數時，搜尋群組選項不會顯示任何資訊。如需詳細資訊，請參閱第 35.7.4 節「停用群組的自動查詢設定」(第 361 頁)。

35.2 準備用於移轉的 Designer 專案

在移轉驅動程式之前，您需要執行一些設定步驟，以準備用於移轉的 Designer 專案。

附註：如果您沒有用於移轉的現有 Designer 專案，請使用**檔案 > 輸入 > 專案 (來自 Identity Vault)** 建立一個新專案。

1 啟動 Designer。
2 (視情況而定) 如果某個現有 Designer 專案包含要移轉的使用者應用程式，請備份該專案：
   - **2a** 在「專案」檢視窗中該專案的名稱上按一下滑鼠右鍵，然後選取**複製專案**。
   - **2b** 指定專案的名稱，然後按一下**確定**。
3 若要更新現有專案的綱要，請完成以下步驟：
   - **3a** 在「模型產生器」檢視窗中，選取「Identity Vault」。
   - **3b** 選取**即時 > 綱要 > 輸入**。
4 (選擇性) 若要驗證專案中 Identity Manager 的版本號碼是否正確，請完成以下步驟：
   - **4a** 在「模型產生器」檢視窗中，選取「Identity Vault」，然後按一下**內容**。
   - **4b** 在左側導覽功能表中，選取**伺服器清單**。
   - **4c** 選取一個伺服器，然後按一下**編輯**。

     Identity Manager 版本欄位應該會顯示最新版本。

35.3 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

您可以在 Designer 或 iManager 中這樣做。若您使用 Designer，則為自動程序。如果您使用 iManager，則需手動進行變更。若要從版本低於 3.5 的 Identity Manager 伺服器移轉至 3.5 或更高版本的 Identity Manager 伺服器，您應該使用 iManager。對於所有其他受支援的移轉路徑，您可以使用 Designer。

- 第 35.3.1 節「在 Designer 中複製伺服器特定資訊」(第 357 頁)
- 第 35.3.2 節「在 iManager 中變更伺服器特定資訊」(第 358 頁)
- 第 35.3.3 節「變更使用者應用程式的伺服器特定資訊」(第 358 頁)

35.3.1 在 Designer 中複製伺服器特定資訊

此程序會影響驅動程式集中儲存的所有驅動程式。

1. 在 Designer 中開啟您的專案。
2. 在「大綱」標籤中，在伺服器上按一下滑鼠右鍵，然後選取「移轉」。
3. 閱讀綜覽以查看移轉至新伺服器的項目，然後按「下一步」。
4. 從列出的可用伺服器中選取目標伺服器，然後按「下一步」。

   只有目前與驅動程式集沒有關聯且與來源伺服器的 Identity Manager 版本相同或更新的伺服器會被列出。
5. 選取以下選項之一：
   - **啟用目標伺服器：**將來源伺服器的設定複製到目標伺服器，並停用來源伺服器上的驅動程式。NetIQ 建議您使用此選項。
   - **將來源伺服器保持為啟用：**不要複製設定，並停用目標伺服器上的所有驅動程式。
   - **同時啟用目標和來源伺服器：**將來源伺服器的設定複製到目標伺服器，但不停用來源或目標伺服器上的驅動程式。不建議使用此選項。如果兩者的驅動程式皆啟動，則會將相同資訊寫入兩個不同佇列，這可能會造成資料損毀。
6. 按一下「移轉」。
7. 將變更的驅動程式部署至 Identity Vault。

   如需詳細資訊，請參閱《*NetIQ Designer for Identity Manager Administration Guide*》(NetIQ Designer for Identity Manager 管理指南) 中的「Deploying a Driver to an Identity Vault」(將驅動程式部署至 Identity Vault)。
8. 啟動驅動程式。

   如需詳細資訊，請參閱第 9.4.2 節「啟動驅動程式」(第 82 頁)。

35.3.2 在 iManager 中變更伺服器特定資訊

1 在 iManager 中按一下 以顯示 Identity Manager 管理頁面。
2 按一下「**Identity Manager 綜覽**」。
3 瀏覽並選取保有驅動程式集的容器。
4 按一下驅動程式集名稱，以存取「驅動程式集綜覽」頁面。
5 按一下驅動程式的右上角，然後按一下「**停止驅動程式**」。
6 按一下驅動程式的右上角，然後按一下「**編輯內容**」。
7 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。
8 按一下「**確定**」儲存所有變更。
9 按一下驅動程式的右上角以啟動驅動程式。
10 對驅動程式集中的每個驅動程式重複步驟 5 到步驟 9。

35.3.3 變更使用者應用程式的伺服器特定資訊

您必須重新設定使用者應用程式，以識別新伺服器。執行 configupdate.bat。

1 導覽至預設位於使用者應用程式安裝子目錄中的組態更新公用程式。
2 在指令提示符處，啟動組態更新公用程式 (configupdate.bat)。
3 依照第 15.8 章「完成 Identity Applications 的設定」(第 204 頁)所述指定值。

35.4 將 Identity Manager 引擎移轉至新伺服器

將 Identity Manager 引擎移轉至新伺服器時，您可以保留舊伺服器上目前所使用的 eDirectory 複製本。

1 在新伺服器上安裝受支援的 eDirectory 版本。
2 將目前 Identity Manager 伺服器上的 eDirectory 複製本複製到新伺服器上。

   如需詳細資訊，請參閱《*NetIQ eDirectory Administration Guide*》(NetIQ eDirectory 管理指南) 中的「Administering Replicas」(管理複製本)。
3 在新伺服器上安裝 Identity Manager 引擎。

   如需詳細資訊，請參閱第 III 部分「安裝 Identity Manager 引擎」(第 49 頁)。

35.5 移轉使用者應用程式驅動程式

在升級至新版 Identity Manager 或移轉至另一個伺服器時，您可能需要輸入使用者應用程式的新基礎套件，或升級現有套件。例如 **使用者應用程式基礎版本 2.2.0.20120516011608**。

當您開始處理 Identity Manager 專案時，Designer 會自動提示您將新套件輸入該專案。此時，您也可以手動輸入套件。

35.5.1 輸入新的基礎套件

1 在 Designer 中開啟您的專案。
2 在套件目錄 > 輸入套件上按一下滑鼠右鍵，然後選取相應的套件。
3 (視情況而定) 如果 「輸入套件」對話方塊未列出使用者應用程式基礎套件，請完成以下步驟：
   3a 按一下 「瀏覽」按鈕。
   3b 導覽至 *Designer 根目錄* /packages/eclipse/plugins/NOVLUABASE_ *最新套件的版本* .jar。
   3c 按一下 「確定」。
4 按一下 「確定」。

35.5.2 升級現有的基礎套件

1 在 Designer 中開啟您的專案。
2 在 「使用者應用程式驅動程式」上按一下滑鼠右鍵。
3 按一下驅動程式 > 內容 > 套件。

   如果基礎套件可以升級，應用程式會在升級欄中顯示一個核取記號。
4 按一下套件對應的選取操作。出現此項表示該套件可升級。
5 在下拉式清單中，按一下升級。
6 選取升級的目標版本。按一下 「確定」。
7 按一下 「套用」。
8 在各欄位中填入用於升級套件的適當資訊。然後按 「下一步」。
9 查看安裝摘要。然後按一下 「完成」。
10 關閉 「套件管理」頁面。
11 取消選取僅顯示適用的套件版本。

35.5.3 部署移轉的驅動程式

只有將使用者應用程式驅動程式部署到 Identity Vault 後，驅動程式移轉才真正完成。移轉後，專案所處的狀態只允許部署整個移轉的組態。您無法將任何定義輸入至移轉的組態。在部署整個移轉組態後，此限制即會解除，您便可以部署個別物件以及輸入定義。

1 在 Designer 中開啟專案，然後對移轉的物件執行專案檢查。

   如需詳細資訊，請參閱 《*NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications*》 (NetIQ Identity Manager - Identity Applications 管理員設計指南) 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 在大綱檢視窗中的使用者應用程式驅動程式上按一下滑鼠右鍵。
3 選取部署。
4 對驅動程式集中的每個使用者應用程式驅動程式重複此程序。

35.6 升級 Identity Applications

在執行 Identity Applications 的升級程式時，請務必注意以下事項：

- 使用先前的使用者應用程式所用的同一個資料庫。「先前安裝」是指您要從中移轉資料的安裝。在安裝程式中，指定現有資料庫做為資料庫類型。
- 您可為使用者應用程式網路位置指定其他名稱。
- 指定不同於先前安裝的安裝位置。
- 指向受支援版本的 Tomcat。
- 不要為資料庫使用不區分大小寫的定序。不支援不區分大小寫的定序。如果使用不區分大小寫的定序，在移轉期間可能會遇到重複鍵錯誤。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。
- 瞭解各密碼管理提供程式之間的差異。SSPR 是預設提供程式。若要使用 Identity Manager 的舊提供程式或者使用外部提供程式，您必須在升級後更新 Identity Applications 的組態。如需詳細資訊，請參閱第 4.4 節「使用 Identity Manager 中的自助式密碼管理」(第 31 頁)。

如需升級 Identity Applications 的詳細資訊，請參閱第 32.5 節「升級 Identity Applications 和 Identity Reporting」(第 332 頁)。

35.7 完成 Identity Applications 的移轉

在升級或移轉 Identity Applications 後，請完成移轉程序。

35.7.1 衝洗瀏覽器快取

在您登入 Identity Applications 之前，應該先衝洗瀏覽器上的快取。如果不衝洗快取，您可能會遇到一些執行時期錯誤。

35.7.2 使用舊提供程式或外部提供程式來管理密碼

依預設，Identity Manager 使用 SSPR 進行密碼管理。但是，為了使用現有的密碼規則，您可能需要使用 Identity Manager 內部的舊提供程式。或者，您也可以使用外部提供程式。如需為這些提供程式設定 Identity Manager 的詳細資訊，請參閱下列其中一節：

- 「使用舊提供程式進行忘記密碼管理」(第 201 頁)
- 「使用外部系統進行忘記密碼管理」(第 202 頁)

35.7.3 更新 SharedPagePortlet 的最大逾時設定

如果您之前自訂了 SharedPagePortlet 的任何預設設定或優先設定，那麼，這些自訂已經儲存到資料庫中，並且此設定將會被覆寫。因此，導覽至「身分自助服務」索引標籤可能並不總是反白顯示正確的共享頁面。為確保不會遇到此問題，請完成以下步驟：

1. 以使用者應用程式管理員身分登入。
2. 導覽至**管理 > 入口網站應用程式管理**。
3. 展開**共享頁面導覽**。

4 在左側的入口網站應用程式樹中，按一下共享頁面導覽。

5 在頁面的右側按一下設定。

6 確保最大逾時設定為 0。

7 按一下「儲存設定」。

35.7.4 停用群組的自動查詢設定

依預設，目錄抽象層中「群組」實體的「DNLookup 顯示」處於啟用狀態。這意味著，每次為群組指定開啟物件選擇器時，您無需搜尋，所有群組預設就會顯示。您應該變更此設定，因為用於搜尋群組的視窗在使用者輸入搜尋內容之前不應顯示任何結果。

您可以在 Designer 中取消核取執行自動查詢來變更此設定，如下所示：

36 解除安裝 Identity Manager 的元件

本章介紹解除安裝 Identity Manager 各元件的程序。解除安裝某些元件需要符合一些先決條件。在開始執行解除安裝程序之前，請務必檢閱每個元件的相關完整章節。

附註：在解除安裝 Identity Manager 元件之前，必須先停止所有服務，例如 Tomcat、PostgreSQL 和 ActiveMQ。

36.1 解除安裝 Identity Vault

在解除安裝 Identity Vault 之前，您必須瞭解 eDirectory 樹狀結構和複本佈置。例如，您應該知道網路樹中是否包含多個伺服器。

1 (視情況而定) 如果 eDirectory 網路樹中有多個伺服器，請完成以下步驟：

   1a (視情況而定) 如果安裝 eDirectory 的伺服器保留了任何主複製本，請在移除 eDirectory 之前，將複本環中的另一個伺服器升級為主伺服器。

   如需詳細資訊，請參閱《*NetIQ eDirectory Administration Guide*》(NetIQ eDirectory 管理指南) 中的「Managing Partitions and Replicas」(管理分割區和複製本)。

   1b (視情況而定) 如果安裝 eDirectory 的伺服器上的樹中保留了某個分割區的唯一副本，請將此分割區合併到母分割區中，或者將此分割區的複製本新增至另一個伺服器中，並使該伺服器成為主複製本持有者。

   如需詳細資訊，請參閱《*NetIQ eDirectory Administration Guide*》(NetIQ eDirectory 管理指南) 中的「Managing Partitions and Replicas」(管理分割區和複製本)。

   1c 對 eDirectory 資料庫執行狀態檢查。在繼續下一步之前，修復發生的所有錯誤。

   如需詳細資訊，請參閱《*NetIQ eDirectory Administration Guide*》(NetIQ eDirectory 管理指南) 中的「Keeping eDirectory Healthy」(維護 eDirectory 的健康)。

2 解除安裝 Identity Vault ：

   使用用於新增和移除程式的控制台公用程式。例如，在 Windows Server 2012 R2 上，按一下**程式和功能**。在 **NetIQ eDirectory** 上按一下滑鼠右鍵，然後按一下**解除安裝**。

3 (視情況而定) 如果 eDirectory 網路樹中有多個伺服器，請完成以下步驟：

   3a 刪除網路樹中左側的所有伺服器特定物件。

   3b 再次執行狀態檢查，以驗證是否已從網路樹中正確移除伺服器。

   如需詳細資訊，請參閱《*NetIQ eDirectory Administration Guide*》(NetIQ eDirectory 管理指南) 中的「Keeping eDirectory Healthy」(維護 eDirectory 的健康)。

36.2 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 網路樹具有完整權限的管理員身分登入 iManager。
3. 選取「分割區及複製本」> 「合併分割區」。
4. 瀏覽並選取作為分割區根物件的驅動程式集物件，然後按一下「確定」。
5. 等待合併程序完成，然後按一下「確定」。
6. 刪除驅動程式集物件。

   當您刪除驅動程式集物件時，刪除程序會刪除與該驅動程式集關聯的所有驅動程式物件。
7. 對於每一個位於 eDirectory 資料庫的驅動程式集物件，重複步驟 3 到步驟 6，直到它們全都刪除為止。
8. 重複步驟 1，以確保所有合併均已完成，而且所有物件均已刪除。

36.3 解除安裝 Identity Manager 引擎

當您安裝 Identity Manager 引擎時，安裝程序會在 Identity Manager 伺服器上新增一個解除安裝程序檔。使用此程序檔可以移除安裝期間建立的所有服務、套件和目錄。

附註：在解除安裝 Identity Manager 引擎之前，請準備 Identity Vault。如需詳細資訊，請參閱第 36.2 節「從 Identity Vault 中移除物件」(第 364 頁)。

若要在 Windows 伺服器上解除安裝 Identity Manager 引擎，請使用用於新增和移除程式的控制台公用程式。例如，在 Windows 2012 R2 上，按一下程式和功能。在 **Identity Manager** 上按一下滑鼠右鍵，然後按一下解除安裝。

36.4 解除安裝遠端載入器

當您安裝遠端載入器時，安裝程序會在伺服器上新增一個解除安裝程序檔。使用此程序檔可以移除安裝期間建立的所有服務、套件和目錄。

若要在 Windows 伺服器上解除安裝遠端載入器，請使用用於新增和移除程式的控制台公用程式。

36.5 解除安裝 Identity Applications

您必須解除安裝 Roles Based Provisioning Module (RBPM) 的每個元件，例如驅動程式和資料庫。

如果您需要解除安裝與 RBPM 相關聯的執行時期元件，解除安裝程式會自動將伺服器重新開機，除非您是以靜默模式在 Windows 上執行解除安裝程式。您必須手動將 Windows 伺服器重新開機。

附註：在解除安裝 RBPM 之前，請先解除安裝 Identity Manager 引擎。如需詳細資訊，請參閱第 36.3 節「解除安裝 Identity Manager 引擎」(第 364 頁)。

36.5.1 刪除 Roles Based Provisioning Module 的驅動程式

您可以使用 Designer 或 iManager 來刪除使用者應用程式驅動程式和角色與資源服務驅動程式。

1 停止使用者應用程式驅動程式以及角色與資源服務驅動程式。根據所用的元件完成下列其中一個動作：
   - **Designer：**在驅動程式行上按一下滑鼠右鍵，然後按一下「即時」> 「停止驅動程式」。
   - **iManager：**在「驅動程式集綜覽」頁面中，按一下驅動程式影像的右上角，然後按一下停止驅動程式。
2 刪除使用者應用程式驅動程式以及角色與資源服務驅動程式。根據所用的元件完成下列其中一個動作：
   - **Designer：**在驅動程式行上按一下滑鼠右鍵，然後按一下「刪除」。
   - **iManager：**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。

36.5.2 解除安裝 Identity Applications

必須從 Tomcat 中解除安裝使用者應用程式及其資料庫。此程序描述如何從 Tomcat 和 PostgreSQL 中移除使用者應用程式及其資料庫。如果您使用的是其他應用程式伺服器與資料庫，相關指示請參閱該產品的文件。

重要：請謹慎移除使用者應用程式，因為這會從安裝了使用者應用程式程序檔和支援檔案的資料夾中移除所有資料夾和檔案。移除這些檔案時，您有可能會無意中解除安裝 Tomcat 或 PostgreSQL。例如，安裝資料夾通常為 C:\NetIQ\idm\apps\UserApplication。此資料夾中還包含 Tomcat 和 PostgreSQL 的資料夾。

---

1 登入安裝了使用者應用程式的伺服器。
2 開啟用於新增和移除程式的控制台公用程式。例如，在 Windows Server 2012 R2 上，按一下程式和功能。
3 在 **Identity Manager** 使用者應用程式上按一下滑鼠右鍵，然後按一下解除安裝。

36.6 解除安裝 Identity Reporting 配件

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，請參閱第 36.6.1 節「刪除報告驅動程式」(第 366 頁)。

2. 刪除 Identity Reporting。如需詳細資訊，請參閱第 36.6.2 節「解除安裝 Identity Reporting」(第 366 頁)。
3. 刪除 Sentinel。如需詳細資訊，請參閱《NetIQ Identity Manager Setup Guide for Linux》(NetIQ Identity Manager 安裝指南 - Linux) 中的「Uninstalling Sentinel」(解除安裝 Sentinel)。

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。

36.6.1 刪除報告驅動程式

您可以使用 Designer 或 iManager 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。
   - **iManager：**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。
   - **iManager：**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。

36.6.2 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，請參閱第 36.6.1 節「刪除報告驅動程式」(第 366 頁)。

重要：在執行 Identity Reporting 解除安裝程式之前，請確保您已將產生的報告從 Reporting 安裝目錄複製到電腦上的其他位置，因為解除安裝程序會從 Reporting 安裝目錄中移除所有檔案和資料夾。例如，Reporting 安裝資料夾 C:\NetIQ\idm\apps\IDMReporting。

若要解除安裝 Identity Reporting，請使用用於新增和移除程式的控制台公用程式。例如，在 Windows Server 2012 R2 上，按一下程式和功能。在 **Identity Reporting** 上按一下滑鼠右鍵，然後按一下解除安裝。

36.7 解除安裝 Analyzer

1 關閉 Analyzer。
2 解除安裝 Analyzer。

   使用用於新增和移除程式的控制台公用程式。例如，在 Windows Server 2008 上，按一下程式和功能。在 **Analyzer for Identity Manager** 上按一下滑鼠右鍵，然後按一下解除安裝。

36.8 解除安裝 iManager

本節說明如何解除安裝 iManager 和 iManager Workstation。您無需依照特定順序來解除安裝 iManager 或關聯的協力廠商元件。NetIQ 建議您檢閱關於解除安裝其中任一元件的考量：

- 如果您解除安裝 Web 伺服器或伺服器常式容器，將無法執行 iManager。
- 在所有平台上，解除安裝程序都只會移除最初安裝的檔案，而不會移除應用程式在執行時建立的任何檔案。例如，Tomcat 執行時建立的記錄檔案和自動產生的組態檔案。
- 解除安裝程序不會移除建立的任何檔案，或者最初在安裝期間新增至目錄結構中，之後曾被修改的檔案。此動作可確保解除安裝程序不會無意中刪除資料。
- 解除安裝 iManager 不會對您在網路樹中設定的任何 RBS 組態造成影響。解除安裝程序不會移除記錄檔案或自訂內容。

重要：在解除安裝 iManager 之前，請備份您要保留的所有自訂內容或其他特殊 iManager 檔案。例如，自訂的外掛程式。

36.8.1 在 Windows 上解除安裝 iManager

若要解除安裝 iManager 的元件，請使用用於新增和移除程式的控制台公用程式。在解除安裝過程中，請注意以下事項：

- 控制台公用程式會將 Tomcat 和 NICI 與 iManager 分開列出。如果您不再使用這些程式，請將其解除安裝。
- 如果 eDirectory 和 iManager 安裝在同一個伺服器上，請不要解除安裝 NICI。eDirectory 需要 NICI 才能執行。
- 在解除安裝 iManager 時，程式會詢問您是否要移除所有的 iManager 檔案。如果您選取是，程式會移除這些檔案，包括所有自訂內容。但是，程式不會從 eDirectory 網路樹中移除 2.7 RBS 物件，並且綱要會保持不變。

36.8.2 解除安裝 iManager Workstation

若要解除安裝 iManager 工作站，請刪除您擷取檔案的目錄。

36.9 解除安裝 Designer

1. 關閉 Designer。
2. 根據作業系統解除安裝 Designer：

   使用用於新增和移除程式的控制台公用程式。例如，在 Windows Server 2008 上，按一下程式和功能。在 **Designer for Identity Manager** 上按一下滑鼠右鍵，然後按一下解除安裝。

37 疑難排解

本章提供對 Identity Manager 安裝問題進行疑難排解的實用資訊。如需 Identity Manager 疑難排解的詳細資訊，請參閱具體元件的指南。

37.1 使用者應用程式和 RBPM 安裝疑難排解

下表列出了您可能會遇到的問題，以及用於解決這些問題的建議動作。如果問題持續發生，請聯絡您的 NetIQ 代表。

問題	建議的動作
升級程序不會將預設的使用者應用程式管理帳戶設定為 cn=uaadmin.ou=sa.o=data。catalina.out 檔案中記錄了以下錯誤。 `AuthorizationManagerService [RBPM] Error occured calculating effective rights for attribute: nrfAccessMgrRevokeRole on object: cn=complianceAdmin,cn=System,cn=Level20,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=UserApplication,cn=Driver Set,o=system for trustee: cn=uaadmin,ou=sa,o=data.com.novell.srvprv.spi.security.IDMAuthorizationException: Error occured calculating effective rights for attribute: nrfAccessMgrRevokeRole on object: cn=complianceAdmin,cn=System,cn=Level20,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=UserApplication,cn=Driver Set,o=system for trustee: cn=uaadmin,ou=sa,o=data.at com.novell.idm.security.authorization.ldap.LdapRightsUtil.getPropertyRights(LdapRightsUtil.java:152) Unable to fetch roles from edirectory in the predefined time set.`	1. 導覽至 setenv.bat 檔案，然後在 CATALINA_OPTS 項目中將 -Dncpclient_req_timeout 內容的值變更為 *1150*。 2. 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。 從安裝目錄 (預設為 C:\NetIQ\idm\apps\UserApplication\) 執行以下指令： `configupdate.bat`
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 iManager 管理員帳戶不同。

問題	建議的動作
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 iManager)。
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**。 從安裝目錄 (預設為 C:\NetIQ\idm\apps\UserApplication\) 執行以下指令： `configupdate.bat`

37.2 解除安裝疑難排解

下表列出了您可能會遇到的問題，以及用於解決這些問題的建議動作。如果問題持續發生，請聯絡您的 NetIQ 代表。

問題	建議的動作
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。

37.3 登入疑難排解

下表列出了您可能會遇到的問題，以及用於解決這些問題的建議動作。如果問題持續發生，請聯絡您的 NetIQ 代表。

問題	建議的動作
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。

37.4 SSPR 頁面申請錯誤疑難排解

下表列出了您可能會遇到的問題，以及用於解決這些問題的建議動作。如果問題持續發生，請聯絡您的 NetIQ 代表。

問題	建議的動作
SSPR 報告頁面申請無序錯誤 如果在 SSPR 頁面中按上一步按鈕，則會出現此問題。SSPR 在 SSPR 錯誤記錄中顯示如下所示的錯誤順序訊息： `ERROR, password.pwm.servlet.TopServlet, 5035 ERROR_INCORRECT_REQUEST_SEQUENCE (expectedPageID=3, submittedPageID=4, url=<some sspr url>`	透過 **SSPR 組態管理器 > 設定 > 安全性 > Web 安全性**停用「上一步」按鈕。 **附註：**變更此設定不會影響到最終使用者。

如需驗證到或登入 Identity Applications 期間遇到的一般問題，請參閱《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》(NetIQ Identity Manager - Identity Applications 管理員指南)。

A Windows 上的範例 Identity Manager 叢集部署解決方案

本附錄提供如何在 Windows 2012 R2 平台上的叢集環境中設定 Identity Manager 的分步說明。

- 第 A.1 節「先決條件」(第 373 頁)
- 第 A.2 節「在 eDirectory 叢集上設定 NetIQ Identity Manager」(第 373 頁)
- 第 A.3 節「遠端載入器叢集化」(第 374 頁)

A.1 先決條件

Windows 2012 R2 平台上的叢集環境中正在執行 eDirectory 8.8.8 SP9 或 9.0.2 或更新版本的服務。如需設定 eDirectory 叢集的詳細資訊，請參閱《*NetIQ eDirectory Installation Guide*》(NetIQ eDirectory 安裝指南) 中的「Clustering eDirectory Services on Windows」(在 Windows 上將 eDirectory 服務叢集化)。

附註：eDirectory 不支援使用多個叢集節點進行負載平衡。eDirectory 叢集只是用於實現容錯移轉功能。

A.2 在 eDirectory 叢集上設定 NetIQ Identity Manager

本節假設您已設定 eDirectory 叢集。

請依照以下程序在 eDirectory 叢集環境中設定 Identity Manager。

1. 在主要節點上的**叢集管理員**中，將 eDirectory 叢集角色優先程度設定為**不自動啟動**。
2. 停止次要節點。
3. 在 Identity Manager 安裝精靈中，透過選取 **Metadirectory 伺服器**選項在主要節點上安裝 Identity Manager 引擎。

   重要：確認您是在本地儲存上安裝 Identity Manager 引擎。

   ---

4. Identity Manager 安裝精靈會在安裝期間停止 eDirectory 叢集角色。當此角色停止時，此角色的狀態可能會顯示為失敗。安裝後，請從**叢集管理員**中啟動 eDirectory 叢集角色。
5. 為 eDirectory 叢集角色設定必要的優先程度，並將次要節點設為主動節點。
6. 使用 DCLUSTER_INSTALL 指令在次要節點上安裝 Identity Manager 引擎。

   例如 idm_install.exe -DCLUSTER_INSTALL="true"

A.3 遠端載入器叢集化

1 在主要和次要叢集節點上安裝遠端載入器。

附註：對於主要和次要節點，請確認遠端載入器安裝在相同的共享儲存路徑上。

---

2 (視情況而定) 如果您與遠端載入器之間使用的是安全通訊，請將所有 SSL 證書都儲存在共享儲存中。

3 在建立遠端載入器叢集角色前，開啟遠端載入器主控台，然後選取**遠端載入器做為 Windows 服務**。

4 在**叢集管理員 > 角色**中，建立一個新的遠端載入器叢集角色。

指定該角色的以下資訊：

角色類型：一般服務

選取服務：遠端載入器例項會註冊為 Windows 服務。

名稱：叢集角色名稱

位址：指定唯一的 IP 位址

選取儲存：共享叢集儲存

複製登錄設定：

1. HKEY_LOCAL_MACHINE\SOFTWARE\Novell\RLConsole
2. HKEY_LOCAL_MACHINE\SOFTWARE\Novell\DirXML Remote Loader\Command port 8000

   指定您要叢集化的遠端載入器例項的登錄路徑。
3. HKEY_LOCAL_MACHINE\SOFTWARE\Novell\PassSync

附註：

- 每個叢集角色預設僅接受一項 Windows 服務。因此，請指定對每個遠端載入器例項而言唯一的指令連接埠和相應的登錄路徑。
- Windows 叢集不支援 Active Directory 驅動程式的密碼過濾器。

B 設定多伺服器環境

安裝 Identity Vault 之後，您可以設定目錄，並使用 DHost 公用程式來建立、啟動和停止伺服器例項。如果您的伺服器原本就支援 IPv6 位址，您還可以將 Identity Vault 設定為使用 IPv6 位址。

B.1 修改 eDirectory 網路樹和複本伺服器

安裝 Identity Vault 之後，您可以使用 DHost 公用程式來設定 Identity Vault。若要使用 DHost 公用程式，您必須具有管理員權限。當您配合引數使用此公用程式時，它會驗證所有引數，並提示輸入具有管理員權限之使用者的密碼。如果您不配合引數使用該公用程式，ndsconfig 將會顯示公用程式及可用選項的描述。

您還可以使用此公用程式來移除 eDirectory 複本伺服器，以及變更 eDirectory 伺服器的目前組態。如需詳細資訊，請參閱第 7.4 章 「安裝後設定 Identity Vault」(第 70 頁)。

使用 DHost 公用程式時，請注意以下事項：

- *treename*、*admin_FDN* 和 *server_FDN* 變數允許的最大字元數如下：
  - *treename*：32 個字元
  - *admin_FDN*：255 個字元
  - *server_FDN*：255 個字元
- 當您將伺服器新增至現有網路樹時，如果指定的網路位置在伺服器物件中不存在，則 DHost 公用程式會在新增該伺服器時建立該網路位置。
- 您可以在安裝 Identity Vault 後將 LDAP 和安全性服務新增至現有網路樹中。
- 若要在伺服器中啟用加密複製，請在用於向現有網路樹新增伺服器的指令中包含 -E 選項。如需加密複製的詳細資訊，請參閱《*NetIQ eDirectory Administration Guide*》(NetIQ eDirectory 管理指南) 中的「Encrypted Replication」(加密複製)。

如需使用 DHost 公用程式修改 eDirectory 的詳細資訊，請參閱《*NetIQ eDirectory Administration Guide*》(NetIQ eDirectory 管理指南)。

B.2 將新網路樹新增至 Identity Vault 中

在 Identity Vault 中建立新的網路樹時，如果您的 Identity Vault 伺服器原本就支援 IPv6 位址，則您可以為新網路樹指定 IPv6 位址。

B.3 將伺服器新增至現有網路樹

您可以透過執行 eDirectory 安裝程式，將伺服器新增至現有網路樹中。

B.4 從伺服器中移除 Identity Vault 及其資料庫

1 導覽至 dsreports 目錄。

2 刪除您先前使用 iMonitor 建立的 HTML 檔案。

B.5 從網路樹中移除 eDirectory 伺服器物件和目錄服務

使用 DHost 公用程式從網路樹中移除伺服器物件和目錄服務。如需詳細資訊，請參閱 《*NetIQ eDirectory Administration Guide*》 (NetIQ eDirectory 管理指南)。