

---

# NetIQ Identity Manager

## 安裝指南 - Linux

2018 年 2 月

## 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	11
關於 NetIQ Corporation	13
<b>I 介紹</b>	<b>15</b>
<b>1 Identity Manager 的元件綜覽</b>	<b>17</b>
<b>2 建立和維護 Identity Manager 環境</b>	<b>19</b>
2.1 Designer for Identity Manager	19
2.2 Analyzer for Identity Manager	19
2.3 iManager	20
<b>3 在 Identity Manager 環境中管理資料</b>	<b>21</b>
3.1 瞭解資料同步	21
3.2 瞭解稽核、報告及法規遵循	21
3.3 瞭解用於同步化身分資料的元件	22
3.3.1 Identity Vault	22
3.3.2 Identity Manager 引擎	22
3.3.3 遠端載入器	22
3.3.4 Identity Reporting	22
<b>4 佈建使用者以進行安全的存取</b>	<b>25</b>
4.1 瞭解 Identity Manager 中的證明程序	25
4.2 瞭解 Identity Manager 中的自助服務程序	26
4.3 瞭解管理使用者佈建的元件	26
4.3.1 使用者應用程式和 Roles Based Provisioning Module	27
4.3.2 Identity Applications 管理	28
4.3.3 Identity Manager 儀表板	28
<b>II 規劃安裝 Identity Manager</b>	<b>31</b>
<b>5 規劃綜覽</b>	<b>33</b>
5.1 規劃核對清單	33
5.2 瞭解 Identity Manager 通訊	34
5.3 瞭解安裝檔案	35
5.4 目錄結構	36
5.5 預設安裝位置	36
5.6 安裝的元件版本	37
5.7 建議的安裝情境和伺服器設定	38
5.7.1 將事件傳送到稽核服務，而不在 Identity Manager 中報告	38
5.7.2 將事件傳送到 Identity Manager 並產生報告	38
5.7.3 在將事件推入 Identity Manager 前先將其傳送至外部服務	39
5.7.4 建議的伺服器設定	39
5.7.5 選取 Identity Manager 的作業系統平台	40

5.8	瞭解授權和啟用	41
5.9	準備安裝	42
5.9.1	確保 Identity Manager 的高可用性	42
5.9.2	Linux 伺服器上的最低空間要求	43
5.9.3	在 SLES 12 SP2 或更新版本的伺服器上安裝 Identity Manager	43
5.9.4	在 RHEL 7.3 或更新版本的伺服器上安裝 Identity Manager	44
5.10	瞭解語言支援	46
5.10.1	已翻譯的元件和安裝程式	47
5.10.2	關於語言支援的特殊考量	47
5.11	下載安裝檔案	48
<b>III</b>	<b>安裝 Sentinel Log Management for Identity Governance and Administration</b>	<b>49</b>
<b>6</b>	<b>規劃安裝 SLM for IGA</b>	<b>51</b>
6.1	安裝 SLM for IGA 的核對清單	51
6.2	系統要求	51
<b>7</b>	<b>安裝 SLM for IGA</b>	<b>53</b>
7.1	標準安裝	53
7.2	自訂安裝	53
<b>IV</b>	<b>安裝和設定 Identity Manager 引擎、Identity Applications 及 Identity Reporting</b>	<b>55</b>
<b>8</b>	<b>規劃安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting</b>	<b>57</b>
8.1	安裝 Identity Manager 元件的核對清單	57
8.2	瞭解安裝程式	58
8.2.1	Identity Manager 引擎	58
8.2.2	Identity Manager 遠端載入器伺服器	58
8.2.3	Identity Manager 擴送代理程式	58
8.2.4	iManager Web 管理	58
8.2.5	Identity Applications	59
8.2.6	Identity Reporting	59
8.3	規劃安裝 Identity Manager 引擎	59
8.3.1	安裝 Identity Manager 引擎的考量	59
8.3.2	隨 Identity Manager 引擎一起安裝驅動程式的考量	60
8.3.3	在叢集環境中安裝 Identity Vault 的先決條件	60
8.3.4	Identity Manager 引擎、遠端載入器和 iManager 的系統要求	61
8.4	規劃安裝遠端載入器	62
8.4.1	遠端載入器安裝核對清單	63
8.4.2	瞭解遠端載入器	64
8.4.3	瞭解安裝程式	65
8.4.4	在同一個電腦上使用 32 位元和 64 位元遠端載入器	65
8.4.5	安裝遠端載入器的先決條件和考量	66
8.5	規劃安裝 Identity Applications	67
8.5.1	Identity Applications 的安裝核對清單	68
8.5.2	安裝 Identity Applications 的先決條件和考量	69
8.5.3	Identity Applications 的系統要求	75
8.6	規劃安裝 Identity Reporting	77
8.6.1	Identity Reporting 的安裝核對清單	77
8.6.2	安裝 Identity Reporting 各元件的先決條件	78
8.6.3	瞭解 Identity Reporting 各元件的安裝程序	79
8.6.4	Identity Reporting 的系統要求	80

<b>9</b>	<b>安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting</b>	<b>83</b>
9.1	安裝 Identity Manager 引擎	83
9.1.1	執行互動式安裝	83
9.1.2	以靜默模式安裝 Identity Manager 引擎	84
9.1.3	以非 root 使用者身分安裝 Identity Manager 引擎	84
9.2	安裝 Java 遠端載入器	87
9.3	安裝 Identity Applications	88
9.3.1	執行互動式安裝	88
9.3.2	以靜默模式安裝	88
9.3.3	以互動模式安裝 SSPR	89
9.3.4	以靜默模式安裝 SSPR	89
9.4	安裝 Identity Reporting	89
9.4.1	執行互動式安裝	90
9.4.2	以靜默模式安裝	90
<b>10</b>	<b>設定安裝的元件</b>	<b>91</b>
10.1	瞭解組態參數	91
10.2	執行組態	95
10.2.1	執行互動式組態	95
10.2.2	執行靜默組態	96
<b>11</b>	<b>完成安裝的最後步驟</b>	<b>97</b>
11.1	完成非 Root 使用者安裝	97
11.1.1	為密碼規則建立容器	97
11.1.2	新增電子郵件通知中的圖形支援	97
11.2	安裝後設定 Identity Vault	98
11.2.1	使用 ndsconfig 公用程式修改 eDirectory 網路樹和複本伺服器	98
11.2.2	使用 ndsmanage 公用程式管理例項	103
11.3	設定遠端載入器和驅動程式	105
11.3.1	與 Identity Manager 引擎建立安全連接	105
11.3.2	瞭解遠端載入器的組態參數	108
11.3.3	為驅動程式例項設定遠端載入器	115
11.3.4	為驅動程式例項設定 Java 遠端載入器	117
11.3.5	設定 Identity Manager 驅動程式以與遠端載入器配合使用	118
11.3.6	設定與 Identity Manager 引擎的雙向驗證	119
11.3.7	驗證組態	124
11.3.8	啟動遠端載入器中的驅動程式例項	124
11.3.9	停止遠端載入器中的驅動程式例項	125
11.4	設定 Identity Applications 的 Identity Vault	125
11.5	為叢集設定使用者應用程式驅動程式	126
11.6	完成 Identity Applications 的設定	126
11.6.1	執行 Identity Applications 組態公用程式	126
11.6.2	使用者應用程式參數	127
11.6.3	Reporting 參數	136
11.6.4	驗證參數	138
11.6.5	SSO 用戶端參數	141
11.6.6	CEF 稽核參數	145
11.7	啟動 Identity Applications	145
11.8	為叢集設定 OSP 和 SSPR	145
11.8.1	設定 SSPR 以支援叢集	145
11.8.2	在叢集節點上設定任務	146
11.9	設定執行時期環境	147
11.9.1	將資料收集服務驅動程式設定為從 Identity Applications 收集資料	147
11.9.2	移轉資料收集服務驅動程式	148
11.9.3	新增對自訂屬性和物件的支援	150

11.9.4	新增多個驅動程式集支援	152
11.9.5	將驅動程式設定為使用 SSL 在遠端模式下執行	153
11.10	設定 Identity Reporting	155
11.10.1	在「身分資料收集服務」頁面中手動新增資料來源	155
11.10.2	對 Oracle 資料庫執行報告	155
11.10.3	手動產生資料庫綱要	155
11.10.4	清除資料庫檢查總數	156
11.10.5	部署 Identity Reporting 的 REST API	157
11.10.6	連接遠端 Remote PostgreSQL 資料庫	157
<b>V</b>	<b>安裝 Designer</b>	<b>159</b>
<b>12</b>	<b>規劃安裝 Designer</b>	<b>161</b>
12.1	Designer 安裝核對清單	161
12.2	安裝 Designer 的先決條件	161
12.3	Designer 的系統要求	161
<b>13</b>	<b>安裝 Designer</b>	<b>163</b>
<b>VI</b>	<b>安裝 Analyzer</b>	<b>165</b>
<b>14</b>	<b>規劃安裝 Analyzer</b>	<b>167</b>
14.1	Analyzer 的安裝核對清單	167
14.2	安裝 Analyzer 的先決條件	167
14.3	Analyzer 的系統要求	168
<b>15</b>	<b>安裝 Analyzer</b>	<b>169</b>
15.1	使用精靈安裝 Analyzer	169
15.2	以靜默模式安裝 Analyzer	170
15.3	將 XULrunner 新增至 Analyzer.ini 中	170
15.4	安裝 Analyzer 的稽核用戶端	171
<b>VII</b>	<b>在 Identity Manager 中設定單一登入存取</b>	<b>173</b>
<b>16</b>	<b>準備單一登入存取</b>	<b>175</b>
<b>17</b>	<b>在 Identity Manager 中使用 One SSO Provider 進行單一登入存取</b>	<b>177</b>
17.1	準備 eDirectory 以支援單一登入存取	177
17.2	修改單一登入存取的基本設定	177
17.3	將 Self Service Password Reset 設定為信任 OSP	178
<b>18</b>	<b>對 NetIQ Access Manager 使用 SAML 驗證進行單一登入</b>	<b>179</b>
18.1	瞭解協力廠商驗證和單一登入	179
18.2	建立和安裝 SSL 證書	179
18.2.1	為 Access Manager 建立 SSL 證書	180
18.2.2	在 Identity Manager 可信證書儲存區中安裝 Access Manager 證書	180
18.2.3	在 Access Manager 可信證書儲存區中安裝 SSL 伺服器證書	181
18.3	將 Identity Manager 設定為信任 Access Manager	181

18.4	將 Access Manager 設定為與 Identity Manager 配合運作	182
18.4.1	複製 Identity Manager 的中繼資料	182
18.4.2	建立 SAML 的屬性集	182
18.4.3	將 Identity Manager 新增為可信的服務提供者	183
18.5	更新 Access Manager 的登入頁面	183
<b>19</b>	<b>驗證是否可對 Identity Applications 進行單一登入存取</b>	<b>185</b>
<b>20</b>	<b>使用 SSL 進行安全通訊</b>	<b>187</b>
20.1	確保使用 SSL 連接的核對清單	187
20.2	建立金鑰儲存區和證書簽署要求	188
20.3	使用外部 CA 簽署的證書啟用 SSL	189
20.4	使用自行簽署的證書啟用 SSL	190
20.4.1	輸出證書管理中心	190
20.4.2	產生自行簽署的證書	191
20.5	在 Sentinel 與 Identity Manager 元件之間啟用 SSL	192
20.5.1	在 Sentinel 與 Identity Manager 引擎 / 遠端載入器之間啟用 SSL	193
20.5.2	在 Sentinel 與使用者應用程式之間啟用 SSL	194
20.6	更新應用程式伺服器的 SSL 設定	195
20.7	在組態公用程式中更新 SSL 設定	196
20.8	更新 Self Service Password Reset 的 SSL 設定	197
<b>VIII</b>	<b>安裝後任務</b>	<b>199</b>
<b>21</b>	<b>設定已連接系統</b>	<b>201</b>
21.1	建立和設定驅動程式集	201
21.1.1	建立驅動程式集	201
21.1.2	將預設密碼規則指定給驅動程式集	201
21.1.3	在 Identity Vault 中建立密碼規則物件	202
21.1.4	建立自訂密碼規則	203
21.1.5	在 Identity Vault 中建立預設通知集合物件	203
21.2	建立驅動程式	203
21.3	定義規則	204
<b>22</b>	<b>設定忘記密碼管理功能</b>	<b>205</b>
22.1	使用 Self Service Password Reset 進行忘記密碼管理	205
22.1.1	將 Identity Manager 設定為使用 Self Service Password Reset	205
22.1.2	為 Identity Manager 設定 Self Service Password Reset	206
22.1.3	鎖定 SSPR 組態	206
22.2	使用外部系統進行忘記密碼管理	207
22.2.1	指定外部忘記密碼管理 WAR 檔案	207
22.2.2	測試外部忘記密碼 組態	208
22.2.3	設定應用程式伺服器之間的 SSL 通訊	208
22.3	針對分散式環境或叢集環境更新儀表板中的 SSPR 連結	208
<b>23</b>	<b>管理驅動程式活動</b>	<b>209</b>
23.1	停止和啟動 Identity Manager 驅動程式	209
23.1.1	停止驅動程式	209
23.1.2	啟動驅動程式	210

<b>24 啟用 Identity Manager</b>	<b>213</b>
24.1 安裝產品啟用身分證明	213
24.2 檢閱 Identity Manager 和驅動程式的產品啟用	214
24.3 啟用 Identity Manager 驅動程式	214
24.4 啟用特定的 Identity Manager 元件	214
24.4.1 啟用 Designer	215
24.4.2 啟用 Analyzer	215
24.4.3 啟用 Sentinel Log Management for IGA	215
 <b>IX 升級 Identity Manager</b>	 <b>217</b>
<b>25 升級 Identity Manager 的準備工作</b>	<b>219</b>
25.1 Identity Manager 的升級核對清單	219
25.2 瞭解升級程序	220
25.3 支援的升級路徑	221
25.3.1 從 Identity Manager 4.6.x 版本升級	221
25.3.2 從 Identity Manager 4.5.x 版本升級	222
25.4 備份目前組態	224
25.4.1 輸出 Designer 專案	225
25.4.2 輸出驅動程式的組態	226
 <b>26 升級 Identity Manager 的元件</b>	 <b>227</b>
26.1 升級順序	227
26.2 升級 Designer	227
26.3 升級 Identity Manager 引擎	228
26.3.1 升級 Identity Vault	228
26.3.2 升級 Identity Manager 引擎	228
26.3.3 升級遠端載入器	229
26.3.4 升級 iManager	230
26.4 升級 Identity Manager 驅動程式	232
26.4.1 建立新驅動程式	232
26.4.2 以套件中的內容取代現有內容	232
26.4.3 保留目前內容並透過套件新增新內容	233
26.5 升級 Identity Applications	233
26.5.1 瞭解升級程式	234
26.5.2 升級的先決條件和注意事項	234
26.5.3 系統要求	235
26.5.4 升級 PostgreSQL 資料庫	235
26.5.5 升級 Identity Applications 的驅動程式套件	238
26.5.6 升級 Identity Applications	238
26.5.7 升級後任務	239
26.6 升級 Identity Reporting	242
26.6.1 升級的先決條件和注意事項	243
26.6.2 升級 Identity Reporting 的驅動程式套件	243
26.6.3 升級 Sentinel Log Management for IGA	243
26.6.4 升級作業系統	244
26.6.5 升級 Identity Reporting	244
26.6.6 Reporting 的升級後步驟	245
26.6.7 驗證 Identity Reporting 的升級	245
26.7 升級 Analyzer	245
26.8 將新伺服器新增至驅動程式集	246
26.8.1 將新伺服器新增至驅動程式集	246
26.8.2 從驅動程式集移除舊的伺服器	246
26.9 將自訂規則還原至驅動程式	247



26.9.1	使用 Designer 將自訂規則還原至驅動程式	247
26.9.2	使用 iManager 將自訂規則還原至驅動程式	248
<b>27</b>	<b>從 Advanced Edition 切換到 Standard Edition</b>	<b>249</b>
<b>X</b>	<b>將 Identity Manager 資料移轉至新安裝中</b>	<b>251</b>
<b>28</b>	<b>移轉 Identity Manager 的準備工作</b>	<b>253</b>
28.1	用於執行移轉的核對清單	253
28.2	在移轉期間停止和啟動 Identity Manager 驅動程式	254
<b>29</b>	<b>將 Identity Manager 移轉至新伺服器</b>	<b>255</b>
29.1	Identity Manager 的移轉核對清單	255
29.2	準備用於移轉的 Designer 專案	256
29.3	複製驅動程式集的伺服器特定資訊	256
29.3.1	在 Designer 中複製伺服器特定資訊	257
29.3.2	在 iManager 中變更伺服器特定資訊	257
29.3.3	變更使用者應用程式的伺服器特定資訊	258
29.4	將 Identity Manager 引擎移轉至新伺服器	258
29.5	移轉使用者應用程式驅動程式	258
29.5.1	輸入新的基礎套件	258
29.5.2	升級現有的基礎套件	259
29.5.3	部署移轉的驅動程式	259
29.6	升級 Identity Applications	259
29.7	完成 Identity Applications 的移轉	260
29.7.1	準備 Oracle 資料庫以執行 SQL 檔案	260
29.7.2	衝洗瀏覽器快取	261
29.7.3	更新 SharedPagePortlet 的最大逾時設定	261
29.7.4	停用群組的自動查詢設定	261
29.8	移轉 Identity Reporting	262
29.8.1	從事件稽核服務移轉至 Sentinel Log Management for IGA	262
29.8.2	設定新 Reporting 伺服器	265
29.8.3	建立資料同步規則	265
<b>30</b>	<b>解除安裝 Identity Manager 的元件</b>	<b>267</b>
30.1	從 Identity Vault 中移除物件	267
30.2	解除安裝 Identity Manager 引擎	267
30.3	解除安裝 Identity Applications	268
30.4	解除安裝 Identity Reporting 元件	268
30.4.1	刪除報告驅動程式	268
30.4.2	解除安裝 Identity Reporting	269
30.4.3	解除安裝 Sentinel	269
30.5	解除安裝 Designer	269
30.6	解除安裝 Analyzer	269
<b>31</b>	<b>疑難排解</b>	<b>271</b>
31.1	使用者應用程式和 RBPM 安裝疑難排解	271
31.2	登入疑難排解	272
31.3	解除安裝疑難排解	273

<b>A</b>	<b>使用 Identity Vault 的多個例項</b>	<b>275</b>
A.1	瞭解 eDirectory 中的 Identity Manager 物件	275
A.2	在伺服器上複製 Identity Manager 需要的物件	275
A.3	使用範圍過濾來管理不同伺服器上的使用者	277
A.4	瞭解 Identity Vault 安裝套件中的 Linux 套件	278
<b>B</b>	<b>SLES 12 SP2 上簡單的 Identity Manager 叢集部署解決方案</b>	<b>281</b>
B.1	先決條件	281
B.2	安裝程序	282
B.2.1	設定 iSCSI 伺服器	282
B.2.2	在所有節點上設定 iSCSI 啟動器	283
B.2.3	分割共享儲存	283
B.2.4	安裝 HA Extension	283
B.2.5	設定 Softdog 監視程式	284
B.2.6	設定 HA 叢集	284
B.2.7	在叢集節點上安裝並設定 eDirectory 和 Identity Manager	285
B.2.8	設定 eDirectory 資源	285
B.2.9	eDirectory 和共享儲存子資源的原始值	286
B.2.10	變更位置條件約束分數	287
<b>C</b>	<b>Tomcat 應用程式伺服器上的範例 Identity Applications 叢集部署解決方案</b>	<b>289</b>
C.1	先決條件	290
C.2	安裝程序	290

# 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：	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
美國和加拿大：	1-888-323-6768
電子郵件：	<a href="mailto:info@netiq.com">info@netiq.com</a>
網站：	<a href="http://www.netiq.com">www.netiq.com</a>

## 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：	<a href="http://www.netiq.com/support/contactinfo.asp">www.netiq.com/support/contactinfo.asp</a>
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：	<a href="mailto:support@netiq.com">support@netiq.com</a>
網站：	<a href="http://www.netiq.com/support">www.netiq.com/support</a>

## 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](http://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](mailto: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](http://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 19 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 21 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 25 頁)。

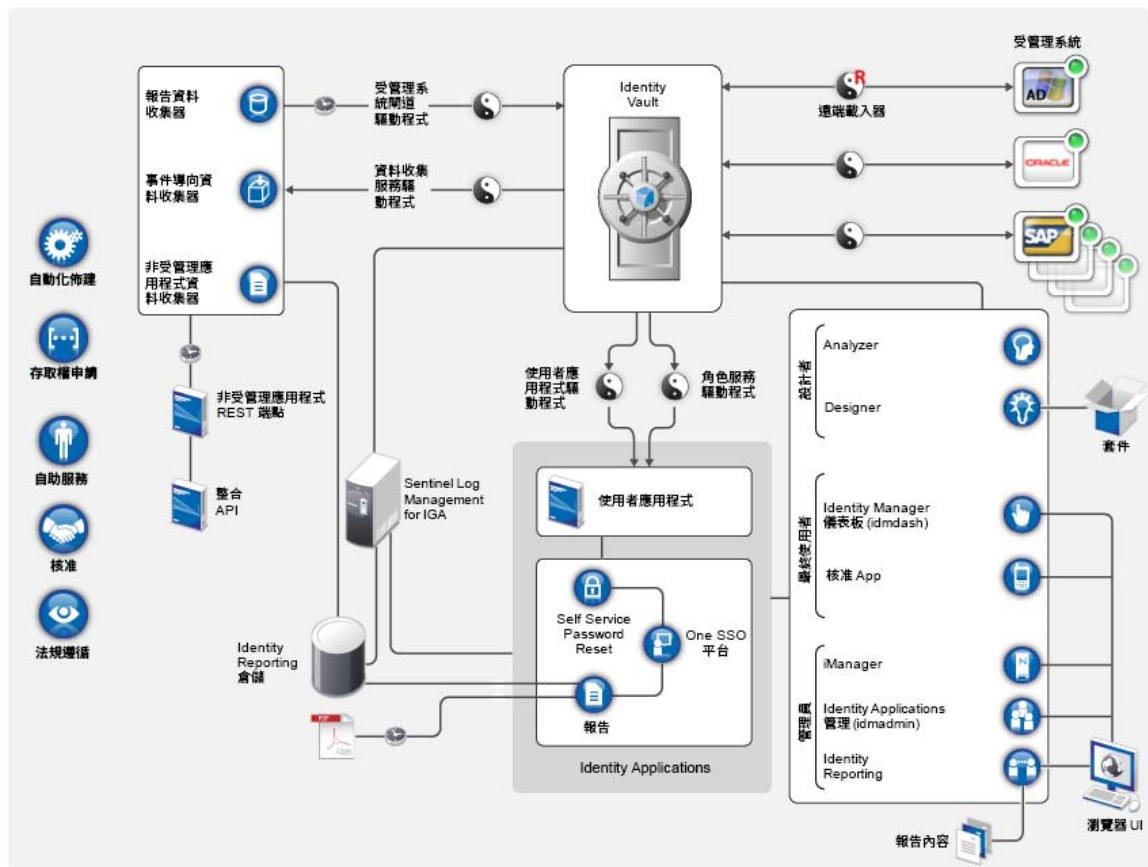
此部分介紹可協助您執行這些活動的各個 Identity Manager 元件。掌握這些知識之後，您便可以開始規劃產品安裝。若要瞭解這些元件如何是互連的，請參閱第 1 章「[Identity Manager 的元件綜覽](#)」(第 17 頁)。





# 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圖。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 19 頁)
- ◆ 第 2.2 節「Analyzer for Identity Manager」(第 19 頁)
- ◆ 第 2.3 節「iManager」(第 20 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
- ◆ 擴送代理程式
- ◆ 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 )、系統 ( 例如 PeopleSoft 和 Lotus Notes ) 及作業系統 ( 例如 UNIX 與 Linux ) 中，建立新的使用者帳戶和移除現有的帳戶。例如，當您將新員工新增至 SAP HR 系統時，Identity Manager 可以自動在 Active Directory 中建立新的使用者帳戶、在 Lotus Notes 中建立新帳戶，以及在 Linux NIS 帳戶管理系統中建立新帳戶。

## 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 瞭解用於同步化身資料的元件

- [第 3.3.1 節「Identity Vault」\(第 22 頁\)](#)
- [第 3.3.2 節「Identity Manager 引擎」\(第 22 頁\)](#)
- [第 3.3.3 節「遠端載入器」\(第 22 頁\)](#)
- [第 3.3.4 節「Identity Reporting」\(第 22 頁\)](#)

### 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 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。

如需遠端載入器的詳細資訊，請參閱[第 8.4.2 節「瞭解遠端載入器」\(第 64 頁\)](#)。

### 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 23 頁)
- ◆ 「資料收集服務」(第 23 頁)
- ◆ 「受管理系統閘道驅動程式」(第 23 頁)

## Identity Manager 的 Identity Reporting

身分資訊倉儲將其資訊儲存在 Sentinel Log Management for Identity Governance and Administration (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。它允許存取所有現有的 **Catlog Administrator** 和使用者應用程式功能。從 **Identity Manager 4.6** 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

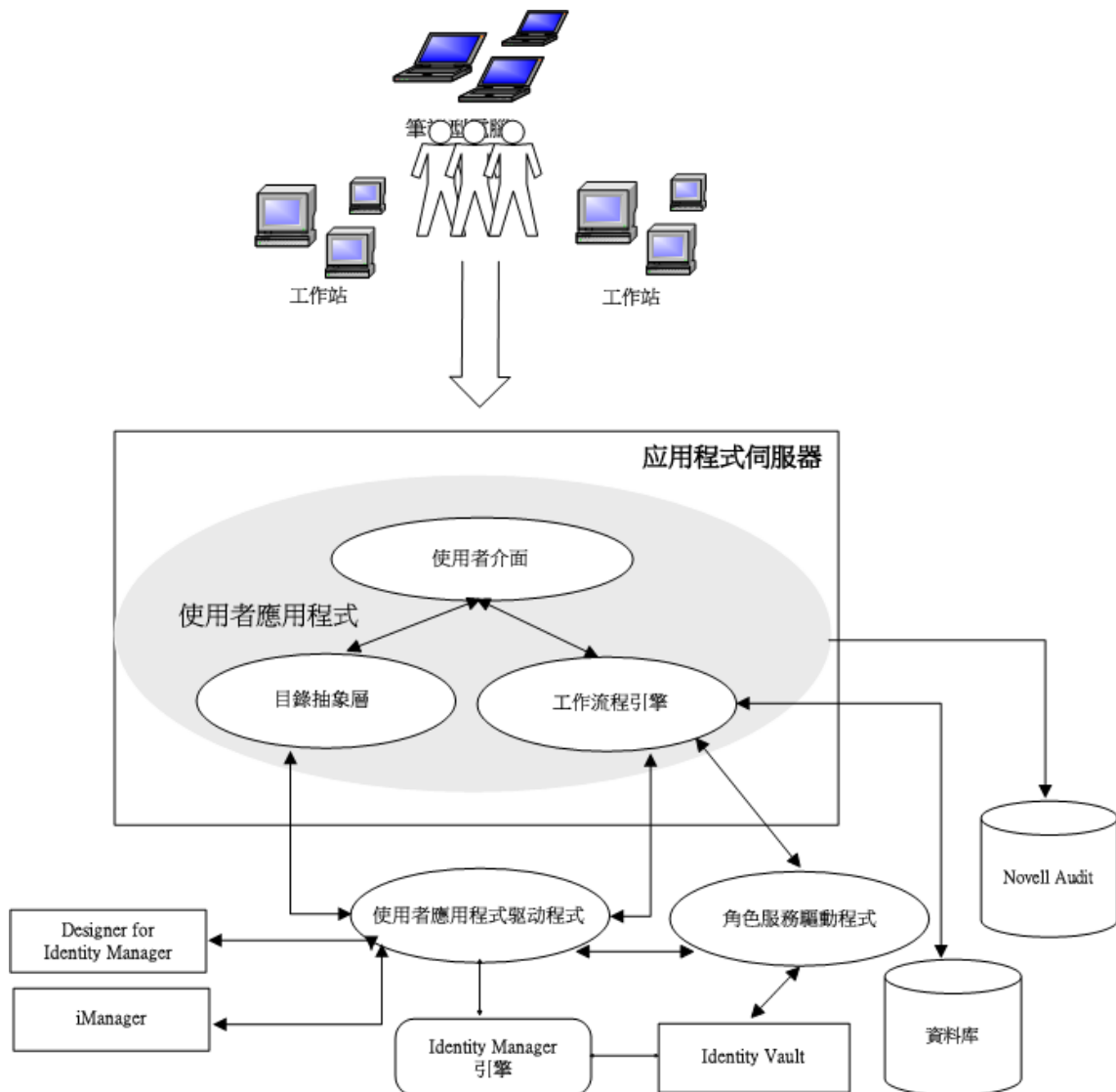
本節說明下列元件的用途：

- ◆ [第 4.3.1 節「使用者應用程式和 Roles Based Provisioning Module」](#)（第 27 頁）
- ◆ [第 4.3.2 節「Identity Applications 管理」](#)（第 28 頁）
- ◆ [第 4.3.3 節「Identity Manager 儀表板」](#)（第 28 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)。





# 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」 \(第 33 頁\)](#)





# 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 33 頁)
- 第 5.2 節「瞭解 Identity Manager 通訊」(第 34 頁)
- 第 5.3 節「瞭解安裝檔案」(第 35 頁)
- 第 5.4 節「目錄結構」(第 36 頁)
- 第 5.5 節「預設安裝位置」(第 36 頁)
- 第 5.6 節「安裝的元件版本」(第 37 頁)
- 第 5.7 節「建議的安裝情境和伺服器設定」(第 38 頁)
- 第 5.8 節「瞭解授權和啟用」(第 41 頁)
- 第 5.9 節「準備安裝」(第 42 頁)
- 第 5.10 節「瞭解語言支援」(第 46 頁)
- 第 5.11 節「下載安裝檔案」(第 48 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
<input type="checkbox"/>	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 15 頁)。
<input type="checkbox"/>	2. (視情況而定) 在 Red Hat Enterprise Linux 7.x 環境中安裝元件時，請確保伺服器上有正確的程式庫。如需詳細資訊，請參閱第 5.9.4 節「在 RHEL 7.3 或更新版本的伺服器上安裝 Identity Manager」(第 44 頁)。
<input type="checkbox"/>	3. 確保您已獲得執行 Identity Manager 的授權。如需詳細資訊，請參閱第 5.8 節「瞭解授權和啟用」(第 41 頁)。
<input type="checkbox"/>	4. 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 5.2 節「瞭解 Identity Manager 通訊」(第 34 頁)。
<input type="checkbox"/>	5. 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 5.10 節「瞭解語言支援」(第 46 頁)。
<input type="checkbox"/>	6. 確保您有 Identity Manager 的安裝檔案。如需詳細資訊，請參閱第 5.11 節「下載安裝檔案」(第 48 頁)。

	核對清單項目
<input type="checkbox"/>	7. (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 5.9.1 節「確保 Identity Manager 的高可用性」(第 42 頁)。
<input type="checkbox"/>	8. 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。
<input type="checkbox"/>	9. 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，請參閱每個元件的系統要求。 <ul style="list-style-type: none"> <li>◆ 第 8.3.4 節「Identity Manager 引擎、遠端載入器和 iManager 的系統要求」(第 61 頁)</li> <li>◆ 第 8.5.3 節「Identity Applications 的系統要求」(第 75 頁)</li> <li>◆ 第 8.6.4 節「Identity Reporting 的系統要求」(第 80 頁)</li> <li>◆ 第 12.3 節「Designer 的系統要求」(第 161 頁)</li> <li>◆ 第 14.3 節「Analyzer 的系統要求」(第 168 頁)</li> </ul> <p>附註：NetIQ 建議您記下在安裝期間建立的每個帳戶。</p>
<input type="checkbox"/>	10. 啟用 Identity Manager 的元件。如需詳細資訊，請參閱第 24 節「啟用 Identity Manager」(第 213 頁)。

## 5.2 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
465	Identity Reporting	用於與 SMTP 郵件伺服器進行通訊
524	Identity Vault	用於 NetWare 核心協定 (NCP) 通訊
636	Identity Vault	用於透過 TLS/SSL 與 Identity Manager 的元件進行 LDAP 通訊
5432	Identity Applications	用於與 Identity Applications 資料庫進行通訊
7707	Identity Reporting	受管理系統閘道驅動程式使用該連接埠來與 Identity Vault 通訊
8000	遠端載入器	驅動程式例項使用該連接埠進行 TCP/IP 通訊 附註：應該為每個遠端載入器例項指定唯一的連接埠。
8005	Identity Applications	Tomcat 使用該連接埠來監聽關閉指令
8009	Identity Applications	Tomcat 使用該連接埠透過 AJP 通訊協定 (而不是 HTTP) 來與 Web 連接器通訊
8028	Identity Vault	用於進行 HTTP 純文字通訊和 NCP 通訊

埠號碼	元件電腦	連接埠用途
8030	Identity Vault	用於進行 HTTPS 通訊和 NCP 通訊
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 <b>附註：</b> 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	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
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

## 5.3 瞭解安裝檔案

下表列出了可用於該版本的檔案：

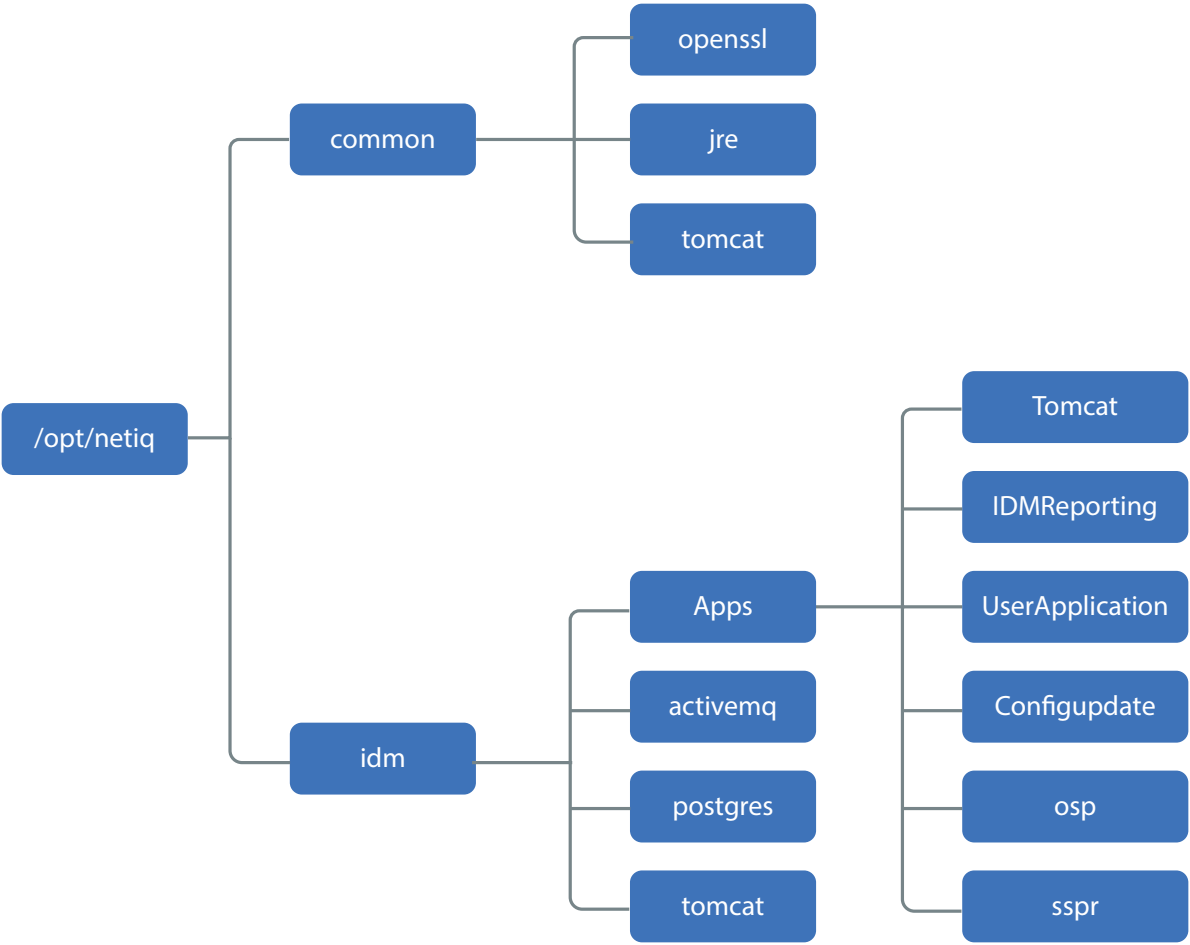
檔名	描述
Identity_Manager_4.7_Linux.iso	包含以下 Identity Manager 元件： <ul style="list-style-type: none"> <li>◆ Identity Manager 引擎</li> <li>◆ 遠端載入器服務</li> <li>◆ 擴送代理程式</li> <li>◆ Designer</li> <li>◆ iManager Web 管理</li> <li>◆ Identity Reporting</li> <li>◆ Identity Applications</li> <li>◆ Analyzer</li> </ul>
SentinelLogManagementForIGA8.1.1.0.tar.gz	包含 Sentinel Log Management for IGA。
Identity_Manager_4.7_Linux_Designer.tar.gz	包含 Designer for Identity Manager。
Identity_Manager_4.7_Linux_Analyzer.tar.gz	包含 Analyzer for Identity Manager。

附註：Identity\_Manager\_4.7\_Linux.iso 檔案還封裝了執行 Identity Manager 所需的支援軟體和元件，例如 Oracle JRE、PostgreSQL、ActiveMQ 和 Apache Tomcat。

## 5.4 目錄結構

安裝程序會建立以下目錄結構：

- /opt/netiq 目錄是目錄結構的起始點。其他每個檔案和目錄都在此目錄下。
- common 目錄包含支援軟體。此軟體會在需要它的元件之間共享。
- idm 目錄包含元件特定的子目錄，其中包括用於安裝和設定元件的二進位檔案。



## 5.5 預設安裝位置

安裝程序會將元件放在以下預先定義的位置。

Identity Manager 元件	預設安裝路徑
Identity Manager 引擎	/opt/novell/eDirectory/lib/dirxml
遠端載入器	/opt/novell/dirxml/bin/x86_64

Identity Manager 元件	預設安裝路徑
擴送代理程式	/opt/novell/dirxml/fanoutagent
Designer	/root/designer
iManager	/var/opt/novell/iManager
使用者應用程式	/opt/netiq/idm/apps/UserApplication
Identity Applications	/opt/netiq/idm/apps
組態更新公用程式	/opt/netiq/idm/apps/configupdate
Identity Reporting	/opt/netiq/idm/apps/IDMReporting
SLM for IGA	/opt/novell/sentinel
Analyzer	/root/analyzer

支援元件	預設安裝路徑
Oracle JRE	/opt/netiq/common/jre
Apache Tomcat	/opt/netiq/idm/tomcat
PostgreSQL	/opt/netiq/idm/postgres
Apache ActiveMQ	/opt/netiq/idm/activemq

系統將在 /var/opt/netiq/idm/log 目錄中產生安裝記錄檔案。

## 5.6 安裝的元件版本

此版本中提供以下版本的元件和支援軟體：

Identity Manager 元件	版本
Identity Vault	9.1
附註：如果您要升級至 Identity Manager 4.7，請確定 Identity Vault 已升級至 9.1 版本。	
Identity Manager 引擎、遠端載入器、擴送代理程式	4.7
Designer	4.7
iManager	3.1
One SSO Provider	6.2.1
Self-Service Password Reset	4.2.0.4
Identity Applications	4.7
Identity Reporting	6.0

Identity Manager 元件	版本
SLM for IGA	8.1.1.0

支援元件	版本
Oracle Java Development Kit (JRE)	1.8.0_162
Apache Tomcat	8.5.27
PostgreSQL	9.6.6
Apache ActiveMQ	5.15.2

## 5.7 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 5.7.1 節「將事件傳送到稽核服務，而不在 Identity Manager 中報告」](#) (第 38 頁)
- ◆ [第 5.7.2 節「將事件傳送到 Identity Manager 並產生報告」](#) (第 38 頁)
- ◆ [第 5.7.3 節「在將事件推入 Identity Manager 前先將其傳送至外部服務」](#) (第 39 頁)
- ◆ [第 5.7.4 節「建議的伺服器設定」](#) (第 39 頁)
- ◆ [第 5.7.5 節「選取 Identity Manager 的作業系統平台」](#) (第 40 頁)

### 5.7.1 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
2. Identity Manager 引擎、驅動程式和 iManager 外掛程式
3. (選擇性) iManager
4. Designer
5. SSPR
6. Identity Applications
7. (選擇性) Analyzer

### 5.7.2 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. Sentinel Log Management for IGA

2. Identity Manager 引擎、驅動程式和 iManager 外掛程式
3. ( 選擇性 ) iManager
4. Designer
5. SSPR
6. Identity Applications
7. Identity Reporting
8. ( 選擇性 ) Analyzer

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

在此情境中，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 Manager 引擎、驅動程式和 iManager 外掛程式
3. ( 選擇性 ) iManager
4. Designer
5. SSPR
6. Identity Applications
7. Identity Reporting
8. ( 選擇性 ) Analyzer

### 5.7.4 建議的伺服器設定

查看以下注意事項以協助您規劃安裝：

元件粘性

元件	獨立安裝	附註
Identity Manager 引擎	是	
Identity Applications	是	必須具有自己的 OSP。必須將 Identity Applications 和 OSP 安裝在同一部電腦上。
Identity Reporting	是	可以具有自己的 OSP。安裝或升級 Identity Reporting 時，安裝程式支援本地或遠端安裝的 OSP。
OSP	否	對於 Identity Applications，安裝程式不支援遠端安裝的 OSP 伺服器。必須將 OSP 和 Identity Applications 安裝在同一部電腦上。
SSPR	是	安裝程式支援獨立安裝和升級 SSPR。
Identity Applications 資料庫	是	
Reporting 資料庫	是	

元件	獨立安裝	附註
Sentinel Log Management for IGA	是	

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

電腦設定	元件設定
一體機 (建議僅用於展示 /POC 設定)	在一部電腦上安裝和設定所有元件 ( <b>Identity Manager</b> 引擎、 <b>Identity Applications</b> 、 <b>Identity Reporting</b> 、 <b>OSP</b> 、 <b>SSPR</b> 、 <b>Identity Applications</b> 資料庫和 <b>Identity Reporting</b> 資料庫)，並在另一部電腦上安裝和設定 <b>Sentinel Log Management for IGA</b> 。
<b>分散式設定</b>	
伺服器 1	<ul style="list-style-type: none"> <li>Identity Vault</li> <li>Identity Manager 引擎</li> </ul>
伺服器 2	Identity Applications 和 OSP (可以叢集化)
伺服器 3	Identity Reporting (OSP)
伺服器 4	SSPR
伺服器 5 和 6	Identity Manager 資料庫，用於： <ul style="list-style-type: none"> <li>Identity Applications</li> <li>Identity Reporting</li> </ul>
伺服器 7	Sentinel Log Management for IGA

### 5.7.5 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
openSUSE	Analyzer Designer
Red Hat Linux Server (RHEL)	Identity Applications Identity Manager 引擎 Identity Reporting iManager 遠端載入器 Sentinel Log Management for IGA



平台	元件
SUSE Linux Enterprise Desktop (SLED)	Designer
SUSE Linux Enterprise Server (SLES)	Analyzer
	Designer
	Identity Applications
	Identity Manager 引擎
	Identity Reporting
	iManager
	遠端載入器
	Sentinel Log Management for IGA

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 161 頁 )
- 「規劃安裝 [Identity Manager 引擎](#)、[Identity Applications](#) 和 [Identity Reporting](#)」 ( 第 57 頁 )

## 5.8 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 24 節「啟用 [Identity Manager](#)」( 第 213 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。

## 5.9 準備安裝

本節列出了將用於代管 **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 5.9.1 節「確保 Identity Manager 的高可用性」](#) (第 42 頁)
- ◆ [第 5.9.2 節「Linux 伺服器上的最低空間要求」](#) (第 43 頁)
- ◆ [第 5.9.3 節「在 SLES 12 SP2 或更新版本的伺服器上安裝 Identity Manager」](#) (第 43 頁)
- ◆ [第 5.9.4 節「在 RHEL 7.3 或更新版本的伺服器上安裝 Identity Manager」](#) (第 44 頁)

### 5.9.1 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** 透過叢集或監管程式叢集 (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 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 5.7.4 節「建議的伺服器設定」](#) (第 39 頁)

在叢集中執行 **Identity Vault**

[第 8.3.3 節「在叢集環境中安裝 Identity Vault 的先決條件」](#) (第 60 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**)。

---

若需要更多相關資訊 ...	請參閱 ...
在叢集中執行 Identity Applications	<a href="#">「為叢集設定 OSP 和 SSPR」 (第 145 頁)</a> <a href="#">「在叢集環境中安裝 Identity Applications 的先決條件」 (第 74 頁)</a> <a href="#">「為叢集啟用許可權索引」 (第 71 頁)</a> <a href="#">「為 Identity Applications 準備叢集」 (第 74 頁)</a> <a href="#">「為叢集設定使用者應用程式驅動程式」 (第 126 頁)</a> <a href="#">第 22.3 節「針對分散式環境或叢集環境更新儀表板中的 SSPR 連結」 (第 208 頁)</a>

## 5.9.2 Linux 伺服器上的最低空間要求

Identity Manager 元件有最低空間要求。

表格 5-1(第 43 頁) 包含不同元件所需的最低安全空間：

表格 5-1 最低安全空間要求

路徑	元件	所需的最低安全空間
/opt	IDM	3 GB
/var	IDM	5 GB，用於包含 100,000 個物件的 dib
/etc	IDM	5 MB
/opt	iManager	700 MB
/var	iManager	3 GB
/etc	iManager	10 MB
/opt	Identity Applications 伺服器	5 GB
/var	Identity Applications 伺服器	100 MB

安裝期間，請確定 /temp 資料夾以執行權限掛接，有 5 GB 可用空間且具有寫入許可權。

## 5.9.3 在 SLES 12 SP2 或更新版本的伺服器上安裝 Identity Manager

- ◆ 若要使用個別元件安裝程式或整合式安裝程式進行 Identity Manager 元件的引導式安裝，您的 SLES 12 SP2 或更新版本伺服器上必須已安裝特定的套件。
  - ◆ libXtst6-32bit-1.2.1-4.4.1.x86\_64
  - ◆ libXrender1-32bit
  - ◆ libXi6-32bit
- ◆ (視情況而定) 在 SLES 12 SP3 環境中安裝 Identity Manager 元件時，請確定已安裝 glibc-32bit-\*x86\_64.rpm，其中 \* 表示 RPM 的最新版本。

---

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

---

## 5.9.4 在 RHEL 7.3 或更新版本的伺服器上安裝 Identity Manager

若要在執行 Red Hat Enterprise Linux 7.3 或更新版本作業系統的伺服器上安裝 Identity Manager，請確定伺服器符合一組特定的先決條件。

- ◆ 「先決條件」 (第 44 頁)
- ◆ 「執行先決條件檢查」 (第 44 頁)
- ◆ 「確認伺服器上已安裝相依程式庫」 (第 44 頁)
- ◆ 「建立安裝媒體的儲存庫」 (第 45 頁)

### 先決條件

NetIQ 建議您檢閱以下先決條件：

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

當任何公用程式嘗試解析到 `ndsd` 伺服器時，下面的範例會出現問題：

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

以下為 `/etc/hosts` 中正確的範例項目：

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

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

- ◆ 在伺服器上安裝適當的程式庫。如需詳細資訊，請參閱「[確認伺服器上已安裝相依程式庫](#)」 (第 44 頁)。

### 執行先決條件檢查

您可以針對每個 Identity Manager 元件產生不符合先決條件的報告。執行 `./ll-rhel-Prerequisite.sh` 程序檔，位於安裝套件的 `<Identity Manager 版次擷取位置>install/utilities` 目錄中。

### 確認伺服器上已安裝相依程式庫

在 64 位元平台上，RHEL 所需的程式庫因所選安裝方法的不同而異。請依列出的順序安裝相依程式庫或 rpm。

---

**附註：**若要新增 `ksh` 檔案，您可以輸入以下指令：

```
yum -y install ksh
```

---

- ◆ `glibc-*.i686.rpm`

- ◆ libstdc++-\*.i686.rpm
- ◆ libgcc-\*.i686.rpm
- ◆ compat-libstdc++-33-\*.x86\_64.rpm
- ◆ compat-libstdc++-33-\*.i686.rpm
- ◆ libXtst-\*.i686.rpm
- ◆ libXrender-\*.i686.rpm

## 建立安裝媒體的儲存庫

如果您的 RHEL 7.x 伺服器需要用於存放安裝媒體的儲存庫，您可以手動建立一個儲存庫。

---

### 附註：

- ◆ RHEL 伺服器還必須裝有相應的程式庫。如需詳細資訊，請參閱「[確認伺服器上已安裝相依程式庫](#)」(第 44 頁)。
  - ◆ 在安裝 Identity Manager 之前，請務必安裝 unzip rpm。這適用於所有 Linux 平台。
- 

### 若要設定用於安裝的儲存庫：

- 1 在本地伺服器中建立掛接點。  
例如：`/mnt/rhel (mkdir -p /mnt/rhel)`
- 2 如果您使用安裝媒體，則可以使用以下指令來掛接：  

```
# mount -o loop /dev/sr0 /mnt/rhel
```

  
或  
使用以下指令將 RHEL 7 安裝 ISO 掛接到 `/mnt/rhel` 這樣的目錄中：  

```
# mount -o loop RHEL7.x.iso /mnt/rhel
```

  
下載並掛接 RHEL 7.4 iso。  
例如：`mount -o loop <所下載 rhel*.iso 的路徑> /mnt/rhel`
- 3 將所掛接目錄的根目錄中的 `media.repo` 檔案複製到 `/etc/yum.repos.d/`，並設定所需的許可權。  
例如：  

```
# cp /mnt/rhel/media.repo /etc/yum.repos.d/rhel7dvd.repo
# chmod 644 /etc/yum.repos.d/rhel7dvd.repo
```
- 4 編輯新 repo 檔案，將 `gpgcheck=0` 設定變更為 1，並新增以下內容：  

```
enabled=1
baseurl=file:///mnt/rhel/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

  
最後，新 repo 檔案內容將與下文類似（不過 `mediaid` 會因 RHEL 版本而異）：

```
[InstallMedia]
name=DVD for Red Hat Enterprise Linux 7.1 Server
mediaid=1359576196.686790
metadata_expire=-1
gpgcheck=1
cost=500
enabled=1
baseurl=file:///mnt/rhel
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

- 5 若要安裝 32 位元套件，請將 `/etc/yum.conf` 檔案中的 `exactarch=1` 變更為 `exactarch=0`。
- 6 若要在 RHEL 7.x 上安裝 Identity Manager 所需的套件，請建立 `install.sh` 檔案，並將以下內容新增至其中：

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

PKGS="ksh gettext.x86_64 libXrender.i686 libXau.i686 libxcb.i686 libX11.i686 libXext.i686
libXi.i686 libXtst.i686 glibc.x86_64 libstdc++.i686 libstdc++.x86_64 libgcc.x86_64"

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

---

**附註：**由於安裝媒體中未包含 `compat-libstdc++-33-*.i686.rpm` 和 `compat-libstdc++-33-*.x86_64.rpm`，因此需要從 [Red Hat](#) 入口網站下載該 rpm。

例如：若要安裝 `compat-libstdc++-33-*.x86_64.rpm`，請執行以下指令：

```
yum -y install compat-libstdc++-33-*.x86_64.rpm
```

---

- 7 執行在步驟 8 或步驟 7 (視 RHEL 版本而定) 中建立的 `install.sh` 檔案。
- 8 若要確認是否符合先決條件，請執行第 6.3.2 節中所述的程序檔。
- 9 安裝 Identity Manager 4.7。

## 5.10 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。

若要以特定語言執行安裝程式，請在設定檔中或透過指令行設定 `LANG` 變數。

## 5.10.1 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
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。

## 5.10.2 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。
- ◆ 安裝 Designer 時，必須安裝 gettext 公用程式。GNU gettext 公用程式提供了國際化多語訊息架構。
- ◆ 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。

## 5.11 下載安裝檔案

若要安裝 Identity Manager 元件，請從 NetIQ 下載網站下載以下安裝檔案：

- ◆ **Identity Manager 引擎、Identity Applications 和 Identity Reporting：**

Identity\_Manager\_4.7\_Linux.iso

- ◆ **Sentinel Log Management for Identity Governance and Administration：**

SentinelLogManagementForIGA8.1.1.0.tar.gz

- ◆ **Designer：** Identity\_Manager\_4.7\_Linux\_Designer.tar.gz

- ◆ **Analyzer：** Identity\_Manager\_4.7\_Linux\_Analyzer.tar.gz

若要下載安裝檔案：

- 1 造訪 NetIQ 下載網站。
- 2 按一下要下載的檔案旁邊的下載按鈕。
- 3 按照畫面上的提示，將檔案下載到您電腦上的目錄中。





# 安裝 Sentinel Log Management for Identity Governance and Administration

本部分引導您完成安裝 Identity Manager 的預設稽核服務 SLM for IGA 的過程。

SLM for IGA 的安裝程式會執行以下功能：

- ◆ 安裝並選擇性設定服務
- ◆ 建立可對服務執行管理任務的使用者帳戶 (**admin**)
- ◆ 建立服務用來與資料庫互動的資料庫管理員帳戶 (**dbauser**)



# 6 規劃安裝 SLM for IGA

本章提供安裝 Identity Manager 的預設稽核服務 SLM for IGA 的準備指南。

- ◆ 第 6.1 節「安裝 SLM for IGA 的核對清單」(第 51 頁)
- ◆ 第 6.2 節「系統要求」(第 51 頁)

## 6.1 安裝 SLM for IGA 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
<input type="checkbox"/>	1. 安裝前檢閱系統要求，以確認電腦符合要求。如需詳細資訊，請參閱第 6.2 節「系統要求」(第 51 頁)。
<input type="checkbox"/>	2. (視情況而定) 對於執行 RHEL 7.4 作業系統的電腦，請確定您已安裝一組適當的程式庫。
<input type="checkbox"/>	3. 決定是要執行 SLM for IGA 的標準安裝還是一般安裝。如需詳細資訊，請參閱第 7 節「安裝 SLM for IGA」(第 53 頁)。

## 6.2 系統要求

本節提供要安裝的伺服器的最低要求。如需詳細資訊，請存取 [NetIQ Sentinel 技術資訊網站](#)。

此外，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	4 - 8 顆 CPU 核心
磁碟空間	200 GB
記憶體	24 GB
作業系統 (已認證)	以下 64 位元作業系統之一 (最低版本)： <ul style="list-style-type: none"><li>◆ SLES 12 SP2</li><li>◆ RHEL 7.3</li></ul> <p>附註：已認證指作業系統已進行全面測試且受支援。</p>
作業系統 (受支援)	已認證作業系統的最新版 Service Pack <p>附註：受支援指作業系統尚未進行測試，但預期可正常運作</p>



# 7 安裝 SLM for IGA

可以使用標準或自訂安裝來安裝 Sentinel Log Management for Identity Governance and Administration (IGA)。

## 7.1 標準安裝

1 從 NetIQ 下載網站下載 SentinelLogManagementForIGA8.1.1.0.tar.gz。

2 導覽至要擷取檔案的目錄。

3 執行以下指令來擷取檔案

```
tar -zxvf SentinelLogManagementForIGA8.1.1.0.tar.gz
```

4 導覽至 SentinelLogManagementforIGA 目錄。

5 若要安裝 SLM for IGA，請執行以下指令：

```
./install.sh
```

6 指定要用於安裝的語言，然後按 Enter。

7 輸入 y 以接受授權合約。

安裝作業會利用幾秒鐘的時間來載入安裝套件。

8 收到提示時，請指定 1 以繼續標準安裝。

安裝會繼續使用安裝程式中包含預設的試用版授權金鑰。在試用期間或試用期結束後，您可以隨時以購買的授權金鑰取代試用版授權。

9 指定管理員使用者 (admin) 的密碼。

10 再次確認密碼。

此密碼用於 admin、dbauser 及 appuser。

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

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

```
https://<IP_Address/DNS_SLM for IGA_server>:8443/SLM for IGA/views/main.html
```

其中，<IP\_Address/DNS\_SLM for IGA\_server> 是 SLM for IGA 伺服器的 IP 位址或 DNS 名稱，8443 是 SLM for IGA 伺服器的預設連接埠。

## 7.2 自訂安裝

1 從 NetIQ 下載網站下載 SentinelLogManagementForIGA8.1.1.0.tar.gz。

2 導覽至要擷取檔案的目錄。

3 執行以下指令來擷取檔案

```
tar -zxvf SentinelLogManagementForIGA8.1.1.0.tar.gz
```

- 4 導覽至 SentinelLogManagementforIGA 目錄。
- 5 執行以下指令：  
`./install.sh`
- 6 輸入 y 以接受授權合約並繼續安裝。  
安裝作業會利用幾秒鐘的時間來載入安裝套件。
- 7 指定 2 以執行 SLM for IGA 的自訂組態。
- 8 輸入 1 以使用預設的試用版授權金鑰。  
或  
輸入 2 以輸入為 SLM for IGA 購買的授權金鑰。
- 9 指定管理員使用者 (admin) 的密碼，並再次確認密碼。
- 10 指定資料庫使用者 (dbauser) 的密碼，並再次確認密碼。  
dbauser 帳戶是 SLM for IGA 用來與資料庫互動的身分。您在此處輸入的密碼可用來執行資料庫維護工作，包括在忘記或遺失管理員密碼時重設管理員密碼。
- 11 指定應用程式使用者 (appuser) 的密碼，並再次確認密碼。
- 12 透過輸入所需的連接埠號碼變更連接埠指定。  
例如，Web 伺服器的預設連接埠為 8443。若要修改 Web 伺服器的連接埠號碼，請指定 4。為 Web 伺服器輸入新的連接埠值，例如，8643。
- 13 變更連接埠後，請指定 8 來完成作業。
- 14 輸入 1，僅以內部資料庫來驗證使用者。  
或  
如果您已在網域中設定 LDAP 目錄，請輸入 2 以利用 LDAP 目錄驗證來驗證使用者。  
預設值為 1。
- 15 當系統提示您啟用 FIPS 140-2 模式時，請輸入 n。
- 16 當系統提示您啟用可擴充儲存時，請輸入 n。

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

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

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

其中，<IP\_Address/DNS\_SLM for IGA\_server> 是 SLM for IGA 伺服器的 IP 位址或 DNS 名稱，<port> 是 SLM for IGA 伺服器的連接埠。

# IV

## 安裝和設定 Identity Manager 引擎、Identity Applications 及 Identity Reporting

本部分引導您完成安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting 元件的過程。開始安裝前，請先評估您要實作 Identity Manager 的方式。您可以將各 Identity Manager 元件安裝在同一部伺服器上，也可以安裝在不同的伺服器上。如需詳細資訊，請參閱第 5.7.4 節「建議的伺服器設定」(第 39 頁)。

可以採用互動模式或靜默模式安裝和設定元件。安裝程式提供了不同階段來安裝和設定元件。如需詳細資訊，請參閱第 8.2 節「瞭解安裝程式」(第 58 頁)。安裝及組態程序檔 `install.sh` 和 `configure.sh` 均位於 Identity Manager 安裝套件 `.iso` 影像檔的根目錄中。依預設，安裝程式將在預設位置安裝元件。如需詳細資訊，請參閱第 5.5 節「預設安裝位置」(第 36 頁)。

---

**附註：**您應該從掛接 `.iso` 的位置執行 `install.sh`。從自訂位置執行 `install.sh` 將導致失敗。

---

NetIQ 建議您在開始安裝前先查看先決條件和系統要求。如需詳細資訊，請參閱第 8 章「規劃安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting」(第 57 頁)。

- ◆ 第 8 章「規劃安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting」(第 57 頁)
- ◆ 第 9 章「安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting」(第 83 頁)
- ◆ 第 10 章「設定安裝的元件」(第 91 頁)
- ◆ 第 11 章「完成安裝的最後步驟」(第 97 頁)





# 8 規劃安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting

本章提供安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting 元件的先決條件、注意事項及所需的系統設定。首先，請參閱核對清單，以瞭解安裝程序。

- ◆ 第 8.1 節「安裝 Identity Manager 元件的核對清單」(第 57 頁)
- ◆ 第 8.2 節「瞭解安裝程式」(第 58 頁)
- ◆ 第 8.3 節「規劃安裝 Identity Manager 引擎」(第 59 頁)
- ◆ 第 8.4 節「規劃安裝遠端載入器」(第 62 頁)
- ◆ 第 8.5 節「規劃安裝 Identity Applications」(第 67 頁)
- ◆ 第 8.6 節「規劃安裝 Identity Reporting」(第 77 頁)

## 8.1 安裝 Identity Manager 元件的核對清單

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
<input type="checkbox"/>	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 15 頁)。
<input type="checkbox"/>	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 5.7 節「建議的安裝情境和伺服器設定」(第 38 頁)。
<input type="checkbox"/>	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「規劃安裝 Identity Manager 引擎」(第 59 頁)。
<input type="checkbox"/>	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「Identity Manager 引擎、遠端載入器和 iManager 的系統要求」(第 61 頁)。
<input type="checkbox"/>	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 60 頁)。
<input type="checkbox"/>	6. (視情況而定)對於執行 RHEL 7.3 或更新版本的電腦，請確定您已安裝一組適當的程式庫。
<input type="checkbox"/>	7. 若要安裝 Identity Manager 引擎，請參閱以下章節之一： <ul style="list-style-type: none"><li>◆ 第 9.1.1 節「執行互動式安裝」(第 83 頁)</li><li>◆ 第 9.1.2 節「以靜默模式安裝 Identity Manager 引擎」(第 84 頁)</li></ul>
<input type="checkbox"/>	8. (視情況而定)若要安裝遠端載入器，請參閱第 8.4 節「規劃安裝遠端載入器」(第 62 頁)。
<input type="checkbox"/>	9. (視情況而定)如果您是以非 root 身分執行安裝，請更新驅動程式集，以在電子郵件通知中支援圖形。如需詳細資訊，請參閱第 11.1.2 節「新增電子郵件通知中的圖形支援」(第 97 頁)。

	核對清單項目
<input type="checkbox"/>	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 11.3 章「設定遠端載入器和驅動程式」(第 105 頁)。

## 8.2 瞭解安裝程式

Identity Manager 安裝程式分不同階段來進行 Identity Manager 元件的安裝和設定。根據安裝期間選取的是 Identity Manager Advanced Edition 還是 Standard Edition，安裝的元件將有所不同。例如，如果選取 Identity Manager Advanced Edition，將顯示以下選項：

- ◆ Identity Manager 引擎
- ◆ Identity Manager 遠端載入器服務
- ◆ Identity Manager 擴送代理程式
- ◆ iManager Web 管理
- ◆ Identity Reporting
- ◆ Identity Applications

可以在安裝 Identity Manager 元件之後立即設定元件，也可以稍後設定。Identity Manager 提供兩個組態選項：一般和自訂。

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

如需元件範圍組態的詳細資料，請參閱第 10.1 節「瞭解組態參數」(第 91 頁)。

下列章節說明使用安裝程式提供的每個安裝選項可以安裝的元件：

### 8.2.1 Identity Manager 引擎

安裝 Identity Vault、Identity Manager 引擎和 Identity Manager 驅動程式。

### 8.2.2 Identity Manager 遠端載入器伺服器

在遠端載入器中安裝遠端載入器服務和驅動程式例項。使用遠端載入器可以在未代管 Identity Vault 和 Identity Manager 引擎的已連接系統上執行 Identity Manager 驅動程式。

### 8.2.3 Identity Manager 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。擴送代理程式根據擴送驅動程式中的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)。

### 8.2.4 iManager Web 管理

安裝 iManager Web 管理主控台和 iManager 外掛程式。

## 8.2.5 Identity Applications

此安裝選項將安裝用於提供 Identity Applications 基礎架構的數個元件。

- ◆ Identity Manager 儀表板
- ◆ Identity Manager 管理主控台
- ◆ 使用者應用程式
- ◆ 使用者應用程式驅動程式 (UAD)
- ◆ 角色與資源服務驅動程式 (RRSD)

安裝程式會在內部安裝驗證服務，以支援透過單一登入存取 Identity Applications 和 Identity Reporting 的功能。安裝程式還會安裝密碼管理服務來協助您設定 Identity Manager，以允許使用者重設其密碼。

安裝程序會部署使用者應用程式驅動程式以及角色與資源服務驅動程式。

## 8.2.6 Identity Reporting

此安裝選項將安裝用於提供 Identity Reporting 基礎架構的數個元件。

- ◆ Identity Reporting
- ◆ 受管理系統閘道 (MSGW) 驅動程式
- ◆ 資料收集服務驅動程式 (DCS)

Identity Reporting 會與 SLM for IGA 通訊來進行稽核。為了記錄事件，Identity Reporting 需要使用隨 SLM for IGA 一併安裝的 SIEM 資料庫。

安裝程序會部署 MSGW 和 DCS 驅動程式。

## 8.3 規劃安裝 Identity Manager 引擎

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 59 頁)
- ◆ [第 8.3.2 節「隨 Identity Manager 引擎一起安裝驅動程式的考量」](#) (第 60 頁)
- ◆ [第 8.3.3 節「在叢集環境中安裝 Identity Vault 的先決條件」](#) (第 60 頁)
- ◆ [第 8.3.4 節「Identity Manager 引擎、遠端載入器和 iManager 的系統要求」](#) (第 61 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：

- ◆ 安裝程式將根據 Identity Vault 的版本安裝 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 8.4.5 節「安裝遠端載入器的先決條件和考量」](#) (第 66 頁)。
- ◆ (視情況而定) 如果您以非 root 使用者身分安裝 Identity Manager 引擎，安裝程序將不會安裝 NetIQ Sentinel 平台代理、Linux 帳戶驅動程式或遠端載入器。您必須單獨安裝這些元件。

---

**附註：**若要支援透過非 root 使用者身分安裝的引擎執行稽核，請安裝 Novell Audit 平台代理程式的最新修補程式。如需詳細資訊，請與[技術支援](#)團隊聯絡。

---

## 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 24 章「[啟用 Identity Manager](#)」(第 213 頁)。

## 8.3.3 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)。

## 8.3.4 Identity Manager 引擎、遠端載入器和 iManager 的系統要求

下表列出了執行安裝的元件範圍最低系統要求：

附註：BTRFS 檔案系統不支援 Identity Vault。

類別	Identity Vault	Identity Manager 引擎	遠端載入器 (64 位元)	iManager
處理器	1 GHz	1 GHz	1 GHz	1 GHz
磁碟空間	<ul style="list-style-type: none"> <li>Identity Vault 需要 300 MB</li> <li>每 50,000 個使用者需要 150 MB 的額外磁碟空間</li> </ul>	<ul style="list-style-type: none"> <li>1 GB</li> <li>每 50,000 個使用者需要 150 MB 的額外磁碟空間</li> </ul>		200 MB
記憶體	2 GB	<ul style="list-style-type: none"> <li>Identity Manager 引擎需要 2 GB</li> <li>Identity Manager 驅動程式需要 2 GB</li> </ul>	512 MB	512 MB
作業系統 (已認證)	以下 64 位元作業系統之一：	以下 64 位元作業系統之一：	以下 64 位元作業系統之一：	以下 64 位元作業系統之一：
附註：已認證指作業系統已進行全面測試且受支援。	<ul style="list-style-type: none"> <li>SLES 12 SP3</li> <li>SLES 12 SP2</li> <li>RHEL 7.4</li> <li>RHEL 7.3</li> </ul>	<ul style="list-style-type: none"> <li>SLES 12 SP3</li> <li>SLES 12 SP2</li> <li>RHEL 7.4</li> <li>RHEL 7.3</li> </ul>	<ul style="list-style-type: none"> <li>SLES 12 SP3</li> <li>SLES 12 SP2</li> <li>RHEL 7.4</li> <li>RHEL 7.3</li> </ul>	<ul style="list-style-type: none"> <li>SLES 12 SP3</li> <li>SLES 12 SP2</li> <li>RHEL 7.4</li> <li>RHEL 7.3</li> </ul>
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。				
作業系統 (受支援)	已認證作業系統的最新版 Service Pack	已認證作業系統的最新版 Service Pack	已認證作業系統的最新版 Service Pack	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	Identity Vault	Identity Manager 引擎	遠端載入器 (64 位元)	iManager
虛擬化系統 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。	<ul style="list-style-type: none"> <li>Hyper-V Server 2012 R2</li> <li>VMWare ESX 5.0 及更新版本</li> <li>包含 Hyper-V 的 Windows Server 2012 R2 Virtualization (受支援)</li> </ul>	<ul style="list-style-type: none"> <li>Hyper-V Server 2012 R2</li> <li>VMWare ESX 5.0 及更新版本</li> <li>包含 Hyper-V 的 Windows Server 2012 R2 Virtualization (受支援)</li> </ul>	<ul style="list-style-type: none"> <li>Hyper-V Server 2012 R2</li> <li>VMWare ESX 5.0 及更新版本</li> <li>包含 Hyper-V 的 Windows Server 2012 R2 Virtualization (受支援)</li> </ul>	
軟體	eDirectory 9.1	Identity Manager 引擎 4.7	遠端載入器 4.7	iManager 3.1
Java (Oracle 的 Java Runtime Environment (JRE))	JRE 1.8.0_162	JRE 1.8.0_162	JRE 1.8.0_162	JRE 1.8.0_162
網頁瀏覽器				以下任意瀏覽器 (最低版本) : <ul style="list-style-type: none"> <li>Google Chrome 61</li> <li>Mozilla Firefox 51</li> </ul>
應用程式伺服器				iManager 隨附的 Apache Tomcat 8.5.27
預設連接埠				8080、8443 及 9009

## 8.4 規劃安裝遠端載入器

本節提供的資訊可協助您為安裝遠端載入器和 Java 遠端載入器做好準備。

- 第 8.4.1 節「遠端載入器安裝核對清單」(第 63 頁)
- 第 8.4.2 節「瞭解遠端載入器」(第 64 頁)
- 第 8.4.3 節「瞭解安裝程式」(第 65 頁)
- 第 8.4.4 節「在同一個電腦上使用 32 位元和 64 位元遠端載入器」(第 65 頁)
- 第 8.4.5 節「安裝遠端載入器的先決條件和考量」(第 66 頁)

## 8.4.1 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
<input type="checkbox"/>	1. 瞭解 Identity Manager 各元件之間的互動。如需詳細資訊，請參閱第 3.3.3 節「遠端載入器」(第 22 頁)。
<input type="checkbox"/>	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 5.7 節「建議的安裝情境和伺服器設定」(第 38 頁)。
<input type="checkbox"/>	3. 確保 Identity Manager 引擎已安裝。
<input type="checkbox"/>	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 8.4.5 節「安裝遠端載入器的先決條件和考量」(第 66 頁)。
<input type="checkbox"/>	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 8.3.4 節「Identity Manager 引擎、遠端載入器和 iManager 的系統要求」(第 61 頁)。
<input type="checkbox"/>	6. (視情況而定)對於執行 RHEL 7.3 或更新版本作業系統的電腦，請確定您已安裝一組適當的程式庫。如需詳細資訊，請參閱第 5.9.4 節「在 RHEL 7.3 或更新版本的伺服器上安裝 Identity Manager」(第 44 頁)。
<input type="checkbox"/>	7. (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 11.3.1 節「與 Identity Manager 引擎建立安全連接」(第 105 頁)。
<input type="checkbox"/>	8. 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 8.4.4 節「在同一個電腦上使用 32 位元和 64 位元遠端載入器」(第 65 頁)。
<input type="checkbox"/>	9. 確定應使用遠端載入器還是 Java 遠端載入器。如需詳細資訊，請參閱「瞭解 Java 遠端載入器」(第 65 頁)。
<input type="checkbox"/>	10. 安裝「遠端載入器」。如需詳細資訊，請參閱第 9 章「安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting」(第 83 頁)。
<input type="checkbox"/>	11. (視情況而定)若要安裝 Java 遠端載入器，請參閱第 9.2 節「安裝 Java 遠端載入器」(第 87 頁)。
<input type="checkbox"/>	12. 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 11.3.2 節「瞭解遠端載入器的組態參數」(第 108 頁)。
<input type="checkbox"/>	13. 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： <ul style="list-style-type: none"><li>◆ 第 11.3.3 節「為驅動程式例項設定遠端載入器」(第 115 頁)</li><li>◆ 第 11.3.4 節「為驅動程式例項設定 Java 遠端載入器」(第 117 頁)</li></ul>
<input type="checkbox"/>	14. 準備遠端載入器的驅動程式。如需詳細資訊，請參閱第 11.3.5 節「設定 Identity Manager 驅動程式以與遠端載入器配合使用」(第 118 頁)。
<input type="checkbox"/>	15. 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 11.3.8 節「啟動遠端載入器中的驅動程式例項」(第 124 頁)。
<input type="checkbox"/>	16. (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 11.3.6 節「設定與 Identity Manager 引擎的雙向驗證」(第 119 頁)。



	核對清單項目
<input type="checkbox"/>	17. 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 11.3.7 節「驗證組態」(第 124 頁)。
<input type="checkbox"/>	18. 安裝其餘的 Identity Manager 元件，包括 Designer 和 Analyzer。

## 8.4.2 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。

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 (例如，Linux 上的 .iso 檔案)。

### 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 11.3 章「設定遠端載入器和驅動程式」(第 105 頁)。

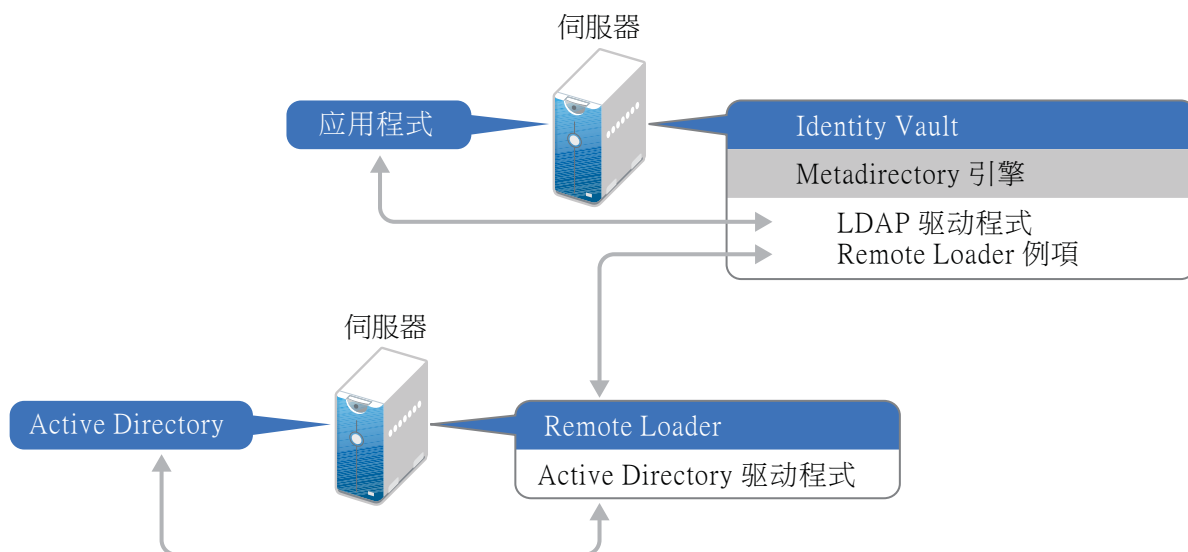
### 確定何時使用遠端載入器

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。

## 瞭解 Java 遠端載入器

在裝有原生遠端載入器不支援的 Linux 伺服器的電腦上，Java 遠端載入器可提供載入驅動程式 shim 的彈性。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。

若要開啟該應用程式，請執行名為 `dirxml_jremote` 的外圍程序程序檔。如需詳細資訊，請參閱第 11.3.4 節「為驅動程式例項設定 Java 遠端載入器」（第 117 頁）。

### 8.4.3 瞭解安裝程式

Identity Manager 引擎安裝程式可以安裝 32 位元和 / 或 64 位元版本的遠端載入器。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。

### 8.4.4 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。

## 8.4.5 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：

- ◆ 務必先安裝 Identity Manager 引擎，然後再安裝遠端載入器。

如果您未安裝 Identity Manager 引擎就已安裝遠端載入器，則必須先安裝 novell-openssl-9.1.0-0.x86\_64.rpm，之後再開始 Identity Manager 引擎的組態。

1. 導覽至以下位置：

<location where you have mounted the Identity\_Manager\_4.7\_Linux.iso>/IDM/packages/OpenSSL/x86\_64/

2. 使用以下指令安裝 novell-openssl-9.1.0-0.x86\_64.rpm：

```
rpm -ivh novell-openssl-9.1.0-0.x86_64.rpm
```

- ◆ 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 8.3.4 節「Identity Manager 引擎、遠端載入器和 iManager 的系統要求」(第 61 頁)。
- ◆ 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 不會影響 Identity Vault 或其他驅動程式。
- ◆ 保護 Identity Vault 免受驅動程式 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：
  - ◆ 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

## 8.5 規劃安裝 Identity Applications

Identity Applications 安裝包含以下元件：

- ◆ Identity Manager 儀表板
- ◆ Identity Manager 管理介面
- ◆ 使用者應用程式
- ◆ 角色與資源服務驅動程式
- ◆ 使用者應用程式驅動程式

本部分內容包含以下資訊：

- ◆ 第 8.5.1 節「Identity Applications 的安裝核對清單」(第 68 頁)
- ◆ 第 8.5.2 節「安裝 Identity Applications 的先決條件和考量」(第 69 頁)
- ◆ 第 8.5.3 節「Identity Applications 的系統要求」(第 75 頁)

## 8.5.1 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
<input type="checkbox"/>	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 27 頁)。
<input type="checkbox"/>	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 5.7.4 節「建議的伺服器設定」(第 39 頁)。
<input type="checkbox"/>	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 5.7 節「建議的安裝情境和伺服器設定」(第 38 頁)。
<input type="checkbox"/>	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 8.3.4 節「Identity Manager 引擎、遠端載入器和 iManager 的系統要求」(第 61 頁)。
<input type="checkbox"/>	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 8.5.2 節「安裝 Identity Applications 的先決條件和考量」(第 69 頁)。
<input type="checkbox"/>	6. (視情況而定)對於執行 SLES 12 SP2 或更新版本作業系統的電腦，請確定您已安裝引導式安裝所需的一組適當的程式庫。如需詳細資訊，請參閱第 5.9.3 節「在 SLES 12 SP2 或更新版本的伺服器上安裝 Identity Manager」(第 43 頁)。
<input type="checkbox"/>	7. (視情況而定)對於執行 RHEL 7.3 或更新版本作業系統的電腦，請確定您已安裝一組適當的程式庫。如需詳細資訊，請參閱第 5.9.4 節「在 RHEL 7.3 或更新版本的伺服器上安裝 Identity Manager」(第 44 頁)。
<input type="checkbox"/>	8. 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，請參閱第 8.5.3 節「Identity Applications 的系統要求」(第 75 頁)。
<input type="checkbox"/>	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。 <ul style="list-style-type: none"><li>◆ 若要瞭解該資料庫，請參閱「安裝 Identity Applications 資料庫的先決條件」(第 71 頁)。</li><li>◆ 若要安裝該資料庫，請參閱第 9 章「設定 Identity Applications 的資料庫」(第 72 頁)。</li></ul>
<input type="checkbox"/>	10. 安裝 Identity Applications。如需詳細資訊，請參閱下列其中一節： <ul style="list-style-type: none"><li>◆ 第 9.1.1 節「執行互動式安裝」(第 83 頁)</li><li>◆ 第 9.1.2 節「以靜默模式安裝 Identity Manager 引擎」(第 84 頁)</li></ul>
<input type="checkbox"/>	11. 若要執行安裝程序中的最後幾個任務，請參閱第 11 章「完成安裝的最後步驟」(第 97 頁)。
<input type="checkbox"/>	12. 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 19 章「驗證是否可對 Identity Applications 進行單一登入存取」(第 185 頁)。

	核對清單項目
<input type="checkbox"/>	13. ( 選擇性 ) 若要開始使用 Identity Applications，請參閱《 <a href="#">NetIQ Identity Manager - Administrator's Guide to the Identity Applications</a> 》(NetIQ Identity Manager - Identity Applications 管理員指南)。

## 8.5.2 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 69 頁 )
- ◆ 「Identity Applications 的組態和使用考量」( 第 70 頁 )
- ◆ 「指定許可權索引的位置」( 第 70 頁 )
- ◆ 「為叢集啟用許可權索引」( 第 71 頁 )
- ◆ 「安裝 Identity Applications 資料庫的先決條件」( 第 71 頁 )
- ◆ 「設定 Identity Applications 的資料庫」( 第 72 頁 )
- ◆ 「在叢集環境中安裝 Identity Applications 的先決條件」( 第 74 頁 )
- ◆ 「為 Identity Applications 準備叢集」( 第 74 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：
  - ◆ Identity Manager 引擎
  - ◆ 遠端載入器
- ◆ ( 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 )。
- ◆ 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。
- ◆ 依預設，安裝程序會將程式檔案放在 /opt/netiq/idm 目錄中。如果您打算將使用者應用程式安裝在非預設位置，在開始執行安裝程序之前，新目錄必須符合以下要求：
  - ◆ 該目錄存在並且可寫入。
  - ◆ 非 root 使用者可對該目錄進行寫入操作。
- ◆ 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。

- ◆ (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。
  - ◆ 必須使用 **Identity Manager 4.6** 或更新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。**iManager** 外掛程式封裝於 **Identity Manager** 引擎安裝中。

## 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 134 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。
- ◆ 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。

## 指定許可權索引的位置

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

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/perminindex
```

例如：

```
com.netiq.idm.cis.indexdir = /opt/netiq/idm/apps/tomcat/temp/perminindex
```

- 4 儲存然後關閉該檔案。
- 5 刪除暫存目錄中現有的 `perminindex` 資料夾。
- 6 啟動 **Tomcat**。

## 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.clustering** 內容設定為 **true**。

例如：

```
<property>  
  
<key>com.netiq.idm.cis.clustering</key>  
  
<value>true</value>  
  
</property>
```

5. 按一下「確定」。

## 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 73 頁)或「設定 Oracle 資料庫」(第 72 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。

## 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「[Identity Applications 的系統要求](#)」(第 75 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 71 頁)。

- ◆ 「設定 **Oracle** 資料庫」(第 72 頁)
- ◆ 「設定 **SQL Server** 資料庫」(第 73 頁)

## 設定 Oracle 資料庫

本節介紹為使用者應用程式使用 **Oracle** 資料庫時可用的組態選項。如需受支援 **Oracle** 版本的詳細資訊，請參閱「[Identity Applications 的系統要求](#)」(第 75 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
```

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

### 設定管理員使用者帳戶

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

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

其中，*idmuser* 代表使用者帳戶。

## 設定 SQL Server 資料庫

本節介紹為使用者應用程式使用 **SQL Server** 資料庫時可用的組態選項。如需受支援 **SQL Server** 版本的詳細資訊，請參閱「[Identity Applications 的系統要求](#)」(第 75 頁)。

### 設定字元集

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

### 設定管理員使用者帳戶

安裝 **Microsoft SQL Server** 後，請使用 **SQL Server Management Studio** 之類的應用程式建立一個資料庫和資料庫使用者。該資料庫使用者帳戶必須擁有以下權限：

- ◆ CREATE TABLE
- ◆ DELETE
- ◆ INSERT

- ♦ SELECT
- ♦ UPDATE

---

附註：建議使用 JDBC JAR 版本 sqjjdbc42.jar。

---

## 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。

## 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 74 頁）
- ♦ [「設定工作流程引擎 ID 的系統內容」](#)（第 75 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 75 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 8.5.2 節 [「安裝 Identity Applications 的先決條件和考量」](#)（第 69 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。

## 8.5.3 Identity Applications 的系統要求

本節提供要安裝 Identity Applications 及其支援架構 (包括 PostgreSQL、Tomcat、OSP 和 SSPR) 的伺服器的最低要求。

類別	要求
處理器	1 GHz
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)

類別	要求
作業系統 ( 已認證 )	<p>以下 64 位元作業系統之一：</p> <ul style="list-style-type: none"> <li>◆ SLES 12 SP3</li> <li>◆ SLES 12 SP2</li> <li>◆ RHEL 7.4</li> <li>◆ RHEL 7.3</li> </ul> <p>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。</p> <p><b>附註：</b> <i>已認證</i>指作業系統已進行全面測試且受支援。</p>
作業系統 ( 受支援 )	<p>已認證作業系統的最新版 Service Pack</p> <p><b>附註：</b> <i>受支援</i>指作業系統尚未進行測試，但預期可正常運作。</p>
虛擬化系統	<ul style="list-style-type: none"> <li>◆ Hyper-V Server 2012 R2</li> <li>◆ VMWare ESX 5.5 及更新版本</li> </ul> <p>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。</p>
資料庫	<ul style="list-style-type: none"> <li>◆ PostgreSQL 9.6.6</li> <li>◆ Oracle 12c</li> <li>◆ MySQL 2016</li> </ul> <p><b>附註：</b>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。</p>
應用程式伺服器	Apache Tomcat 8.5.27
Java	<p>Java Development Kit (JDK)</p> <p>或</p> <p>Sun (Oracle) 提供的 Java Runtime Environment (JRE) 1.8.0_162 或更新版本</p>
連接埠	8180
網頁瀏覽器	<p>以下任意瀏覽器 ( 最低版本 )：</p> <ul style="list-style-type: none"> <li>◆ Apple Safari 9</li> <li>◆ Google Chrome 61 或更新版本</li> <li>◆ Microsoft Edge 20.10240.17146.0</li> <li>◆ Microsoft Internet Explorer 11.0.10240.17443</li> </ul> <p><b>附註：</b>此「相容檢視」選項在 Internet Explorer 瀏覽器中不受支援。</p> <ul style="list-style-type: none"> <li>◆ Mozilla FireFox 51 或更新版本</li> </ul> <p><b>附註：</b>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。</p>
稽核	Platform Agent 2011.1r6 ( 最低版本 )

類別	要求
目錄服務	NetIQ eDirectory 9.1

## 8.6 規劃安裝 Identity Reporting

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

- ◆ 第 8.6.1 節「Identity Reporting 的安裝核對清單」(第 77 頁)
- ◆ 第 8.6.2 節「安裝 Identity Reporting 各元件的先決條件」(第 78 頁)
- ◆ 第 8.6.3 節「瞭解 Identity Reporting 各元件的安裝程序」(第 79 頁)
- ◆ 第 8.6.4 節「Identity Reporting 的系統要求」(第 80 頁)

### 8.6.1 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
<input type="checkbox"/>	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 22 頁)。
<input type="checkbox"/>	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 5.7 節「建議的安裝情境和伺服器設定」(第 38 頁)。
<input type="checkbox"/>	3. 檢閱安裝 Identity Reporting 的考量。如需詳細資訊，請參閱第 8.6.2 節「安裝 Identity Reporting 各元件的先決條件」(第 78 頁)。
<input type="checkbox"/>	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 8.6.4 節「Identity Reporting 的系統要求」(第 80 頁)。
<input type="checkbox"/>	5. (視情況而定)對於執行 RHEL 7.3 或更新版本作業系統的電腦，請確定您已安裝一組適當的程式庫。
<input type="checkbox"/>	6. (視情況而定)確定已安裝 Identity Applications。如果已安裝 Advanced Edition，則必須執行此步驟。如需詳細資訊，請參閱第 8 章「規劃安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting」(第 57 頁)。
<input type="checkbox"/>	7. 安裝 Sentinel。如需詳細資訊，請參閱第 7 節「安裝 SLM for IGA」(第 53 頁)
<input type="checkbox"/>	8. 安裝 Identity Reporting。如需詳細資訊，請參閱下列其中一節： <ul style="list-style-type: none"> <li>◆ 第 9.1.1 節「執行互動式安裝」(第 83 頁)</li> <li>◆ 第 9.1.2 節「以靜默模式安裝 Identity Manager 引擎」(第 84 頁)</li> </ul>
<input type="checkbox"/>	9. 完成 Identity Reporting 的設定。如需詳細資訊，請參閱第 11.10 章「設定 Identity Reporting」(第 155 頁)。
<input type="checkbox"/>	10. 設定驅動程式的環境。如需詳細資訊，請參閱第 11.9 節「設定執行時期環境」(第 147 頁)。

## 8.6.2 安裝 Identity Reporting 各元件的先決條件

NetIQ 建議您在開始安裝前先查看以下資訊。

- ◆ 「Identity Reporting 的先決條件」 (第 78 頁)
- ◆ 「Identity Reporting 的身分稽核事件」 (第 78 頁)

### Identity Reporting 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 元件的支援且已設定版本：
  - ◆ Identity Applications，包括使用者應用程式驅動程式 (僅適用於 Advanced Edition)
  - ◆ Sentinel 安裝在單獨的 Linux 電腦上。
- ◆ 請不要將 Identity Reporting 安裝在叢集環境中的伺服器上。
- ◆ 若要針對 Oracle 資料庫執行報告，必須確定已複製 ojdbc8.jar。如需詳細資訊，請參閱第 11.10.2 節「對 Oracle 資料庫執行報告」 (第 155 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.sh 檔案中修改 JRE 對應的 JAVA\_OPTS 或 CATALINA\_OPTS 項目。

### 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	<p>選擇使用 <b>SSPR</b> 的稽核旗標：啟動 <b>SSPR 組態編輯器</b> &gt; 稽核組態 &gt; 選取以下稽核旗標之一：</p> <ul style="list-style-type: none"> <li>◆ 驗證</li> <li>◆ 變更密碼</li> <li>◆ 解除鎖定密碼</li> <li>◆ 復原密碼</li> <li>◆ 入侵者嘗試</li> <li>◆ 入侵者鎖定</li> <li>◆ 入侵者鎖定使用者</li> </ul> <p>選取使用 <b>iManager</b> 的稽核旗標：轉到 <b>iManager 角色與任務</b> &gt; <b>eDirectory 稽核</b> &gt; 稽核組態 &gt; <b>Novell Audit</b> 選取以下稽核旗標之一：</p> <ul style="list-style-type: none"> <li>◆ 變更密碼</li> <li>◆ 驗證密碼</li> <li>◆ 登入</li> <li>◆ 登出</li> </ul>
所有其他報告事件	轉到 <b>NetIQ Identity Manager UserApp</b> > 管理 > 記錄 > 啟用稽核服務

### 8.6.3 瞭解 Identity Reporting 各元件的安裝程序

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：

- ◆ 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
- ◆ 部署 Identity Reporting 正常運作所需的驅動程式、受管理系統閘道和資料收集服務。
- ◆ 為 Identity Reporting 設定 PostgreSQL 資料庫

## 8.6.4 Identity Reporting 的系統要求

本節提供要安裝 Identity Reporting 的伺服器的最低要求。

此外，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  <b>附註：</b> 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： <ul style="list-style-type: none"><li>◆ SLES 12 SP3</li><li>◆ SLES 12 SP2</li><li>◆ RHEL 7.4</li><li>◆ RHEL 7.3</li></ul> 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。 <b>附註：</b> 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  <b>附註：</b> 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	<ul style="list-style-type: none"><li>◆ Hyper-V Server 2012 R2</li><li>◆ VMWare ESX 5.5 及更新版本</li></ul> 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	<ul style="list-style-type: none"><li>◆ PostgreSQL 9.6.6</li><li>◆ Oracle 12.2.01</li></ul>
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



類別	要求
網頁瀏覽器	<p>以下任意瀏覽器 ( 最低版本 ) :</p> <p><b>Desktop</b></p> <ul style="list-style-type: none"> <li>◆ Apple Safari 9</li> <li>◆ Google Chrome 61 或更新版本</li> <li>◆ Microsoft Internet Explorer 11</li> <li>◆ Mozilla FireFox 51 或更新版本</li> </ul> <p><b>iPad</b></p> <ul style="list-style-type: none"> <li>◆ Apple Safari 9</li> <li>◆ Google Chrome 61 或更新版本</li> </ul> <p><b>附註：</b>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。</p>
稽核	Sentinel Log Management for IGA



# 9 安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting

本章引導您完成安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting 元件的必需元件的過程。

可以使用互動模式或靜默模式進行安裝。安裝程式將提供建立靜默內容檔案的選項。您可以將多個元件的安裝選項記錄在內容檔案中，然後使用該檔案在您環境中的其他伺服器上執行靜默安裝。靜默安裝程式會從該檔案中讀取相應的值來執行安裝。

可以在安裝 Identity Manager 元件之後立即設定元件，也可以稍後設定。

安裝程式會將元件安裝在第 5.5 節「預設安裝位置」(第 36 頁)中所述的預先定義位置。

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 章「規劃安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting」(第 57 頁)。

## 9.1 安裝 Identity Manager 引擎

可以使用以下方法來安裝 Identity Manager 引擎：

- 第 9.1.1 節「執行互動式安裝」(第 83 頁)
- 第 9.1.2 節「以靜默模式安裝 Identity Manager 引擎」(第 84 頁)
- 第 9.1.3 節「以非 root 使用者身分安裝 Identity Manager 引擎」(第 84 頁)

### 9.1.1 執行互動式安裝

- 1 從 NetIQ 下載網站下載 Identity\_Manager\_4.7\_Linux.iso。
- 2 掛接下載的 .iso。
- 3 從 .iso 檔案的根目錄中，執行以下指令：  
`./install.sh`
- 4 通讀授權合約。
- 5 輸入 y 以接受授權合約。
- 6 決定要安裝的 Identity Manager 伺服器版本。輸入 y 將安裝 Advanced Edition，輸入 n 將安裝 Standard Edition。
- 7 選取 Identity Manager 引擎並繼續安裝。
- 8 設定安裝的元件。如需詳細資訊，請參閱第 10 章「設定安裝的元件」(第 91 頁)。

## 9.1.2 以靜默模式安裝 Identity Manager 引擎

- 1 從 NetIQ 下載網站下載 Identity\_Manager\_4.7\_Linux.iso。
- 2 掛接下載的 .iso。
- 3 從 .iso 的根目錄中，執行以下指令：  

```
./create_silent_props.sh
```
- 4 輸入 y 以確認建立檔案。
- 5 若要安裝 JRE，請輸入 y。
- 6 若要升級現有的 Identity Manager 元件，請輸入 y。
- 7 決定要安裝的 Identity Manager 伺服器版本。輸入 y 將安裝 Advanced Edition，輸入 n 將安裝 Standard Edition。
- 8 選取元件的組態模式。如需詳細資訊，請參閱第 10 章「設定安裝的元件」(第 91 頁)。
- 9 指定要安裝的元件。
- 10 執行以下指令以執行靜默安裝：  

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

  
例如，  

```
./install.sh -s -f /mnt/silent.properties
```

，其中，/mnt/silent.properties 是靜默內容檔案的儲存位置。

## 9.1.3 以非 root 使用者身分安裝 Identity Manager 引擎

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

1. 確定已安裝 NCI。如需詳細資訊，請參閱「安裝 NCI」(第 84 頁)。
2. 以非 root 使用者身分安裝 Identity Vault。如需詳細資訊，請參閱「以非 root 使用者身分安裝 Identity Vault」(第 85 頁)。
3. 以非 root 使用者身分安裝 Identity Manager 引擎。如需詳細資訊，請參閱「以非 root 使用者身分安裝引擎」(第 86 頁)。

### 安裝 NCI

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

- 1 從掛接的 iso 中，導覽至 /IDVault/setup/ 目錄。
- 2 執行以下指令：  

```
rpm -ivh nci64-3.1.0-0.00.x86_64.rpm
```
- 3 驗證 NCI 是否設定為伺服器模式。輸入以下指令：  

```
/var/opt/novell/nci/set_server_mode
```

  
必須執行此步驟，以確保 Identity Vault 組態不會失敗。

## 以非 root 使用者身分安裝 Identity Vault

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

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

---

**附註：**若要指定自訂安裝路徑，也可以使用 root 使用者身分登入。

---

- 2 從掛接的 iso 中，導覽至 /IDVault/ 目錄。
- 3 建立一個新目錄，然後將 eDir\_NonRoot.tar.gz 檔案複製到該目錄。例如，/home/user/install/eDirectory。

- 4 使用下列指令來解壓縮檔案：

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

- 5 (視情況而定) 若要手動輸出環境變數的路徑，請輸入以下指令：

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

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

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

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

- 6 (視情況而定) 若要使用 ndspath 程序檔輸出環境變數的路徑，必須將 ndspath 程序檔放在公用程式的前面。完成以下步驟：

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

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

- 6b 使用以下指令輸出目前外圍程序中的路徑：

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

- 6c 照常執行公用程式。

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

執行此步驟後，每當您登入或者開啟新外圍程序時，都可以直接啟動公用程式。

- 7 若要設定 Identity Vault，請完成下列其中一個步驟：

- 7a 若要執行 ndsconfig 公用程式，請在指令行中輸入以下文字：

```
ndsconfig new [-t treename] [-n server_context] [-a admin_FDN] [-w  
admin_password] [-i] [-S server_name] [-d path_for_dib] [-m module] [e] [-L ldap_port] [-l  
SSL_port] [-o http_port] -O https_port [-p IP address:[port]] [-c] [-b port_to_bind] [-B  
interface1@port1, interface2@port2,...] [-D custom_location] [--config-file  
configuration_file]
```

例如：

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

---

附註：

- ◆ 必須指定介於 1024 和 65535 之間的連接埠號。您不能假定預設連接埠 524 適用於任何 eDirectory 應用程式。
- ◆ 這項連接埠規格限制可能會對以下類型的應用程式造成負面影響：
  - ◆ 未提供指定目標伺服器連接埠的選項的應用程式。
  - ◆ 使用 NCP 並以 root 身分在連接埠 524 上執行的舊版應用程式。
- ◆ 您可以在 -B 和 -P 選項中指定 IPv6 位址。若要指定 IPv6 位址，必須將地址包含在方括號 [] 中。例如 -B [2015::4]:636。

---

**7b** 使用 ndsmanage 公用程式設定一個新例項。如需詳細資訊，請參閱「在 Identity Vault 中建立新例項」(第 104 頁)。

## 以非 root 使用者身分安裝引擎

當您使用此方法時，將無法安裝以下元件：

- ◆ **遠端載入器**：若要以非 root 使用者身分安裝遠端載入器，請使用 Java 遠端載入器。如需詳細資訊，請參閱「安裝 Java 遠端載入器」(第 87 頁)。
- ◆ **Linux 帳戶驅動程式**：需要根特權才能運作。

---

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

---

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

- 1 以安裝 Identity Vault 時使用的非 root 使用者身分登入。  
該使用者帳戶必須對非 root Identity Vault 安裝的目錄和檔案具有寫入存取權。
- 2 導覽至掛接 Identity\_Manager\_4.7\_Linux.iso 的位置。
- 3 從掛接位置導覽至 /IDM 目錄。
- 4 執行下列指令：  
./idm-nonroot-install.sh
- 5 根據以下資訊完成此安裝：

### 非 root eDirectory 安裝的基礎目錄

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

### 延伸 eDirectory 綱要

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

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

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

完成安裝之後，執行 `/opt/novell/eDirectory/bin/idm-install-schema` 程式，以對其他 **eDirectory** 例項延伸綱要。

- 6 若要完成安裝程序，請繼續第 11.1 節「完成非 **Root** 使用者安裝」(第 97 頁)。
- 7 啟用 **Identity Manager**。如需詳細資訊，請參閱第 24 章「啟用 **Identity Manager**」(第 213 頁)。
- 8 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](#)。

## 9.2 安裝 Java 遠端載入器

一般來說，您會在作業系統與原生遠端載入器不相容的電腦上安裝 **Java** 遠端載入器 **dirxml\_jremote**。不過，**Java** 遠端載入器也可以在您可能安裝了原生遠端載入器的同一部伺服器上執行。**Identity Manager** 會使用 **Java** 遠端載入器，在一部伺服器上執行的 **Identity Manager** 引擎與其他位置 (該位置未執行 **rdxml**) 執行的 **Identity Manager** 驅動程式之間交換資料。您可以在裝有任何公開支援的 **Java** 版本的任何受支援 **Linux** 電腦上安裝 **dirxml\_jremote**。

- 1 在代管 **Identity Manager** 引擎的伺服器上，複製預設位於 `/opt/novell/eDirectory/lib/dirxml/classes` 目錄中的應用程式 **Shim .iso** 或 **.jar** 檔案。
- 2 登入您要安裝 **Java** 遠端載入器的電腦 (目標電腦)。
- 3 驗證目標電腦是否裝有受支援版本的 **JRE**。
- 4 若要存取安裝程式，請完成下列其中一個步驟：
  - 4a (視情況而定) 如果您已取得 **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 (預設在 `products/IDM/java_remoteloader` 中)。
  - 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 `/usr/idm` 中。
- 6 將下列其中一個檔案複製到目標電腦上的所需位置：
  - ♦ **dirxml\_jremote.tar.gz**
  - ♦ **dirxml\_jremote\_mvs.tar**如需 **mvs** 的資訊，請將 **dirxml\_jremote\_mvs.tar** 檔案解包，然後參閱 **usage.html** 文件。
- 7 在目標電腦上，解壓縮並擷取 **.tar.gz** 檔案。  
例如，輸入 `gunzip dirxml_jremote.tar.gz` 或 `tar -xvf dirxml_jremote_dev.tar`。
- 8 將您在步驟 1 中從 `dirxml/classes` 目錄複製的應用程式 **shim** 的 **.iso** 或 **.jar** 檔案放在 **lib** 目錄下。

- 9 若要自訂 `dirxml_jremote` 程序檔，以便能夠透過 `RDXML_PATH` 環境變數存取 Java 可執行檔，請完成下列其中一個步驟：
  - 9a 輸入下列其中一個指令，以設定環境變數 `RDXML_PATH`：
    - ◆ `set RDXML_PATH=path`
    - ◆ `export RDXML_PATH`
  - 9b 編輯 `dirxml_jremote` 程序碼，並在執行 Java 的程序碼行上，將路徑預增至 Java 執行檔。
- 10 必須在 `dirxml_jremote` 程序檔中指定 `jar` 檔案的位置。這些檔案位於 `dirxml_jremote.tar.gz` 解壓縮目錄的 `lib` 子目錄中。例如，`/lib/*.jar`。
- 11 設定範例組態檔案 `config8000.txt`，使其可用於您的應用程式 `shim`。

依預設，該範例檔案位於 `/opt/novell/dirxml/doc` 目錄中。如需詳細資訊，請參閱第 11.3 章「設定遠端載入器和驅動程式」(第 105 頁)。

## 9.3 安裝 Identity Applications

可以使用以下方法來安裝 Identity Applications：

- ◆ 第 9.3.1 節「執行互動式安裝」(第 88 頁)
- ◆ 第 9.3.2 節「以靜默模式安裝」(第 88 頁)
- ◆ 第 9.3.3 節「以互動模式安裝 SSPR」(第 89 頁)
- ◆ 第 9.3.4 節「以靜默模式安裝 SSPR」(第 89 頁)

### 9.3.1 執行互動式安裝

- 1 從 NetIQ 下載網站下載 `Identity_Manager_4.7_Linux.iso`。
- 2 掛接下載的 `.iso`。
- 3 從 `.iso` 檔案的根目錄中，執行以下指令：

```
./install.sh
```
- 4 通讀授權合約。
- 5 輸入 `y` 以接受授權合約。
- 6 決定要安裝的 Identity Manager 伺服器版本。輸入 `y` 將安裝 Advanced Edition，輸入 `n` 將安裝 Standard Edition。
- 7 選取 Identity Applications 並繼續安裝。
- 8 設定安裝的元件。如需詳細資訊，請參閱第 10 章「設定安裝的元件」(第 91 頁)。

### 9.3.2 以靜默模式安裝

- 1 從 NetIQ 下載網站下載 `Identity_Manager_4.7_Linux.iso`。
- 2 掛接下載的 `.iso`。
- 3 從 `.iso` 的根目錄中，執行以下指令：

```
./create_silent_props.sh
```
- 4 輸入 `y` 以確認建立檔案。



- 5 若要安裝 JRE，請輸入 y。
- 6 決定要安裝的 Identity Manager 伺服器版本。輸入 y 將安裝 Advanced Edition，輸入 n 將安裝 Standard Edition。
- 7 選取元件的組態模式。如需詳細資訊，請參閱第 10 章「設定安裝的元件」(第 91 頁)。
- 8 選取 Identity Applications 並繼續安裝。
- 9 執行以下指令以執行靜默安裝：  

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

  
例如，  

```
./install.sh -s -f /mnt/silent.properties
```

，其中，/mnt/silent.properties 是靜默內容檔案的儲存位置。

### 9.3.3 以互動模式安裝 SSPR

如果要在分散式環境中安裝 Identity Applications 和 SSPR，安裝程式會為您提供單獨安裝 SSPR 的選項。

- 1 從 NetIQ 下載網站下載 Identity\_Manager\_4.7\_Linux.iso。
- 2 掛接下載的 .iso。
- 3 從 .iso 檔案的根目錄中，導覽至 SSPR 目錄。
- 4 執行以下指令：  

```
./install.sh
```
- 5 通讀授權合約。
- 6 輸入 y 以接受授權合約。
- 7 設定安裝的元件。如需詳細資訊，請參閱第 10 章「設定安裝的元件」(第 91 頁)。

### 9.3.4 以靜默模式安裝 SSPR

- 1 從 NetIQ 下載網站下載 Identity\_Manager\_4.7\_Linux.iso。
- 2 掛接下載的 .iso。
- 3 從 .iso 檔案的根目錄中，導覽至 SSPR 目錄。
- 4 執行以下指令：  

```
./install.sh -s sspr_silentinstall.properties
```

## 9.4 安裝 Identity Reporting

可以使用以下方法來安裝 Identity Reporting：

- 第 9.4.1 節「執行互動式安裝」(第 90 頁)
- 第 9.4.2 節「以靜默模式安裝」(第 90 頁)

## 9.4.1 執行互動式安裝

- 1 從 NetIQ 下載網站下載 Identity\_Manager\_4.7\_Linux.iso。
- 2 掛接下載的 .iso。
- 3 從 .iso 檔案的根目錄中，執行以下指令：  
`./install.sh`
- 4 通讀授權合約。
- 5 輸入 y 以接受授權合約。
- 6 決定要安裝的 Identity Manager 伺服器版本。輸入 y 將安裝 Advanced Edition，輸入 n 將安裝 Standard Edition。
- 7 指定 Identity Reporting 並繼續安裝。
- 8 設定安裝的元件。如需詳細資訊，請參閱第 10 章「設定安裝的元件」(第 91 頁)。

## 9.4.2 以靜默模式安裝

- 1 從 NetIQ 下載網站下載 Identity\_Manager\_4.7\_Linux.iso。
- 2 掛接下載的 .iso。
- 3 從 .iso 的根目錄中，執行以下指令：  
`./create_silent_props.sh`
- 4 輸入 y 以確認建立檔案。
- 5 若要安裝 JRE，請輸入 y。
- 6 決定要安裝的 Identity Manager 伺服器版本。輸入 y 將安裝 Advanced Edition，輸入 n 將安裝 Standard Edition。
- 7 選取元件的組態模式。如需詳細資訊，請參閱第 10 章「設定安裝的元件」(第 91 頁)。
- 8 指定 Identity Reporting 並繼續安裝。
- 9 執行以下指令以執行靜默安裝：  
`./install.sh -s -f <location of the silent properties file>`  
例如，  
`./install.sh -s -f /mnt/silent.properties`，其中，/mnt/silent.properties 是靜默內容檔案的儲存位置。

# 10 設定安裝的元件

本章引導您完成設定第 9 章「安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting」(第 83 頁)中所安裝 Identity Manager 元件的過程。您可以採用互動模式(主控台)或靜默模式執行組態。

在開始組態過程前，必須查看每個元件的組態選項。如需詳細資訊，請參閱第 10.1 節「瞭解組態參數」(第 91 頁)。

## 10.1 瞭解組態參數

本節定義設定 Identity Manager 安裝需要指定的參數。您可以在安裝元件後立即使用安裝程式來設定元件，也可以稍後再設定。

附註：

- 如果採用一般組態模式設定 Identity Applications 和 Identity Reporting，則無法連接至安裝在其他機器上的資料庫。
- 安裝程序不允許您啟用稽核。必須單獨為 Identity Manager 元件啟用稽核。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)。

---

### 參數 一般組態

---

#### Identity Manager 引擎

通用密碼	指定是否要設定通用密碼。
Identity Vault 管理員名稱	指定網路樹中管理員物件的相對可辨識名稱 (RDN)，該管理員至少對要新增此伺服器的網路位置擁有完整權限。

#### Identity Applications

通用密碼	指定是否要設定通用密碼。
Identity Vault 管理員名稱	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。
主機名稱 (小寫 FQDN)	指定伺服器完全合格的可辨識名稱或預設 IP 位址。
應用程式伺服器 DNS/IP 位址	指定 Tomcat 伺服器的 IP 位址。
Identity Applications 管理員名稱	指定 Identity Applications 管理員帳戶的名稱。

#### Identity Reporting

通用密碼	指定是否要設定通用密碼。
Identity Vault 管理員名稱	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。

---

---

## 參數 一般組態

---

主機名稱 ( 小寫 FQDN)	指定伺服器完全合格的可辨識名稱或預設 IP 位址。
連接至外部 One SSO 伺服器	指定是否要連接至不同的 One SSO 伺服器。
應用程式伺服器 DNS/IP 位址	指定 Tomcat 伺服器的 IP 位址。
One SSO 伺服器 DNS/IP 位址	指定安裝了單一登入服務的伺服器的 IP 位址。
Identity Reporting 管理員名稱	指定 Identity Reporting 的管理員名稱。預設值為 <code>cn=uaadmin,ou=sa,o=data</code> 。

---

---

## 參數 自訂組態

---

### Identity Manager 引擎

Identity Vault 網路樹名稱	為 Identity Vault 指定新的網路樹。網路樹名稱必須符合以下要求： <ul style="list-style-type: none"><li>◆ 網路樹名稱在網路中必須是唯一的。</li><li>◆ 網路樹名稱的長度必須為 2 至 32 個字元。</li><li>◆ 網路樹名稱只能包含字母 (A-Z)、數字 (0-9)、連字號 (-) 和底線 (_) 之類的字元。</li></ul>
Identity Vault 管理員名稱	指定網路樹中管理員物件的相對可辨識名稱 (RDN)，該管理員至少對要新增此伺服器的網路位置擁有完整權限。
Identity Vault 管理員密碼	指定管理員物件的密碼。例如， <i>password</i> 。
NDS var 資料夾位置	指定此 Identity Vault 例項在此伺服器上的路徑。預設路徑為 <code>/var/opt/novell/eDirectory</code> 。
NDS 資料位置	指定本地系統中要安裝目錄資訊資料庫 (DIB) 檔案的路徑。DIB 檔案是您的 Identity Vault 資料庫檔案。預設位置為 <code>/var/opt/novell/eDirectory/data/dib</code> 。
NCP 連接埠	指定 Identity Vault 用來與 Identity Manager 各元件通訊的 NetWare 核心協定 (NCP) 連接埠。預設值為 524。
LDAP 非 SSL 連接埠	指定 Identity Vault 要用來監聽純文字格式 LDAP 要求的連接埠。預設值為 389。
LDAP SSL 連接埠	指定 Identity Vault 用來監聽使用安全通訊端層 (SSL) 通訊協定之 LDAP 要求的連接埠。預設值為 636。
Identity Vault HTTP 連接埠	指定 HTTP 堆疊以純文字格式運作所需使用的連接埠。預設值為 8028。
Identity Vault HTTPS 連接埠	指定 HTTP 堆疊採用 TLS/SSL 通訊協定運作所需使用的連接埠。預設值為 8030。
含路徑的 NDS 組態檔案	指定 Identity Vault 組態檔案的位置。預設值為 <code>/etc/opt/novell/eDirectory/conf/nds.conf</code> 。
Identity Vault 驅動程式集名稱	為新的 Identity Manager 驅動程式集物件指定名稱。
Identity Vault 驅動程式集部署網路位置	指定要在其中建立驅動程式集物件的容器的 LDAP DN。

---

---

## 參數 自訂組態

---

### Identity Applications

主機名稱 (小寫 FQDN)	指定伺服器完全合格的可辨識名稱或預設 IP 位址。  <b>附註：</b> 確定以小寫字元指定 FQDN。另外，必須將代管元件的伺服器設定為使用小寫 FQDN。
Identity Vault 主機名稱 /IP 位址	指定安裝了 Identity Vault 的伺服器的 IP 位址。
Identity Vault 管理員名稱	指定網路樹中管理員物件的相對可辨識名稱 (RDN)，該管理員至少對要新增此伺服器的網路位置擁有完整權限。
Identity Vault 管理員密碼	指定管理員物件的密碼。例如， <i>password</i> 。
應用程式伺服器 DNS/IP 位址	指定 Tomcat 伺服器的 IP 位址。
OSP 自訂登入畫面名稱	指定將顯示在 OSP 登入畫面上的名稱。
SSPR 組態密碼	<i>僅當將通用密碼設定為否時才適用。</i>  指定 Identity Applications 用於進行密碼管理的密碼。
OAuth 金鑰儲存區密碼	<i>僅當將通用密碼設定為否時才適用。</i>  指定您要建立以用於在 OAuth 伺服器上載入新金鑰儲存區的密碼。
使用者搜尋容器 DN	指定 Identity Vault 中所有使用者物件的預設容器。
管理員搜尋容器 DN	指定資料組織中存放 Identity Manager 所有資料物件的位置。管理員應該確保所有使用者都有權存取此容器和所有子容器。
應用程式伺服器 HTTPS 連接埠	指定 Tomcat 伺服器在與用戶端電腦通訊時使用的 HTTPS 連接埠。預設值為 8543。
One SSO 伺服器 SSL 連接埠	指定單一登入服務要使用的連接埠。預設值為 8543。
Identity Application One SSO 服務密碼	<i>僅當將通用密碼設定為否時才適用。</i>  指定 Identity Applications 使用的單一登入用戶端的密碼。
Identity Applications 管理員名稱	指定 Identity Applications 管理員帳戶的名稱。
LDAP 非 SSL 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。
Identity Vault 驅動程式集名稱	指定 Identity Vault 的驅動程式集名稱。
Identity Vault 驅動程式集部署網路位置	指定要在其中建立驅動程式集物件的容器的 LDAP DN。
資料庫平台	指定 Identity Applications 所需的資料庫。
在目前伺服器上設定 PostgreSQL	指定是否要在同一部伺服器上設定 PostgreSQL 資料庫。
Identity Applications 資料庫連接埠	指定 Identity Applications 的資料庫連接埠。
Identity Applications 資料庫名稱	指定資料庫的名稱。預設值為 <i>idmuserappdb</i> 。
Identity Applications 資料庫使用者名稱	指定 Identity Applications 資料庫管理員的使用者名稱

---

---

## 參數 自訂組態

---

Identity Application 資料庫 JDBC jar 檔案	指定資料庫平台的 JAR 檔案。
建立綱要	做為安裝程序的一部分，指出要在何時建立資料庫綱要。可用選項有 <b>現在</b> 、 <b>啟動</b> 和 <b>檔案</b> 。
建立新資料庫或從現有資料庫升級 / 移轉	指定是要建立新資料庫，還是從現有資料庫升級。
使用自訂容器做為根容器	<p>指定是否要使用自訂容器做為根容器。依預設，安裝程式會建立 <b>o=data</b> 並選取它做為使用者容器，然後指定密碼規則和所需的託管者權限。</p> <p>若要建立自訂容器，請選擇是。</p>
自訂容器 LDIF 檔案路徑	<p>僅當將自訂容器設定為是時適用。</p> <p>為自訂容器指定 LDIF 檔案的路徑。</p>
根容器	指定根容器。預設值為 <b>o=data</b> 。
群組搜尋根容器 DN	指定群組搜尋根容器的 DN。
<b>Identity Reporting</b>	
主機名稱 (小寫 FQDN)	<p>指定伺服器完全合格的可辨識名稱或預設 IP 位址。</p> <p><b>附註：</b>確定以小寫字元指定 FQDN。另外，必須將代管元件的伺服器設定為使用小寫 FQDN。</p>
Identity Vault 主機名稱 /IP 位址	指定安裝了 Identity Vault 的伺服器的 IP 位址。
LDAP SSL 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。
Identity Vault 管理員名稱	指定網路樹中管理員物件的相對可辨識名稱 (RDN)，該管理員至少對要新增此伺服器的網路位置擁有完整權限。
Identity Vault 管理員密碼	指定管理員物件的密碼。例如， <i>password</i> 。
應用程式伺服器 DNS/IP 位址	指定 Tomcat 伺服器的 IP 位址。
OSP 自訂登入畫面名稱	指定將顯示在 OSP 登入畫面上的名稱。
使用者搜尋容器 DN	指定 Identity Vault 中所有使用者物件的預設容器。
管理員搜尋容器 DN	指定資料組織中存放 Identity Manager 所有資料物件的位置。管理員應該確保所有使用者都有權存取此容器和所有子容器。
應用程式伺服器 HTTPS 連接埠	指定 Tomcat 伺服器在與用戶端電腦通訊時使用的 HTTPS 連接埠。預設值為 8543。
One SSO 伺服器 DNS/IP 位址	指定安裝了單一登入服務的伺服器的 IP 位址。
One SSO 伺服器 SSL 連接埠	指定單一登入服務要使用的連接埠。預設值為 8543。
Identity Reporting 資料庫名稱	指定 Identity Reporting 的資料庫名稱。預設值為 <b>idmrptdb</b> 。
Identity Reporting 資料庫使用者	指定允許 Identity Reporting 存取和修改資料庫中資料的管理帳戶。預設值為 <b>rptadmin</b> 。

---

---

## 參數 自訂組態

---

Identity Reporting 資料庫主機	指定需要在其中建立資料庫的伺服器的 DNS 名稱或 IP 位址。
Identity Reporting 資料庫連接埠	指定用於連接資料庫的連接埠。預設連接埠為 5432。
Identity Application 資料庫 JDBC jar 檔案	指定資料庫平台的 JAR 檔案。
Identity Reporting 資料庫帳戶密碼	指定 Identity Reporting 的資料庫帳戶密碼。
建立綱要	<p>做為安裝程序的一部分，指出要在何時建立資料庫綱要。可用選項有現在、啟動和檔案。</p> <p>如果為資料庫綱要建立選項選取啟動或檔案，則必須手動將資料來源新增至「身分資料收集服務」頁面。如需詳細資訊，請參閱第 11.10.1 節「在「身分資料收集服務」頁面中手動新增資料來源」(第 155 頁)。</p> <p>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。對於遠端安裝的 PostgreSQL 資料庫，請驗證該資料庫是否在執行中。若要連接至遠端 PostgreSQL 資料庫，請參閱第 11.10.6 節「連接遠端 Remote PostgreSQL 資料庫」(第 157 頁)。如果要連接至 Oracle 資料庫，請確定已建立 Oracle 資料庫例項。如需詳細資訊，請參閱 Oracle 文件。</p> <p>如果為資料庫綱要建立選項選取啟動或檔案，則必須在組態後手動建立表並連接至資料庫。如需詳細資訊，請參閱第 11.10.3 節「手動產生資料庫綱要」(第 155 頁)。</p>
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。
SMTP 伺服器連接埠	指定 SMTP 伺服器的連接埠號。預設埠為 465。
為 Identity Reporting 建立 MSGW 和 DCS 驅動程式	指定是否要建立 MSGW 和 DCS 驅動程式。

---

## 10.2 執行組態

下列各節提供有關設定 Identity Manager 元件的資訊。

### 10.2.1 執行互動式組態

- 1 導覽至掛接 Identity\_Manager\_4.7\_Linux.iso 的位置。
- 2 執行下列指令：  
./configure.sh
- 3 決定是要執行一般組態還是自訂組態。組態選項將因您選取要設定的元件而異。
- 4 若要設定元件，請參閱第 10.1 節「瞭解組態參數」(第 91 頁)中的資訊。

## 10.2.2 執行靜默組態

1 導覽至掛接 Identity\_Manager\_4.7\_Linux.iso 的位置。

2 執行下列指令：

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

例如，

```
./configure.sh -s -f /mnt/silent.properties
```

其中，/mnt/silent.properties 是靜默內容檔案的儲存位置。

3 若要設定元件，請參閱第 10.1 節「瞭解組態參數」(第 91 頁)中的資訊。



# 11

## 完成安裝的最後步驟

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 11.1 節「完成非 Root 使用者安裝」(第 97 頁)
- ◆ 第 11.2 節「安裝後設定 Identity Vault」(第 98 頁)
- ◆ 第 11.3 節「設定遠端載入器和驅動程式」(第 105 頁)
- ◆ 第 11.4 節「設定 Identity Applications 的 Identity Vault」(第 125 頁)
- ◆ 第 11.5 節「為叢集設定使用者應用程式驅動程式」(第 126 頁)
- ◆ 第 11.6 節「完成 Identity Applications 的設定」(第 126 頁)
- ◆ 第 11.7 節「啟動 Identity Applications」(第 145 頁)
- ◆ 第 11.8 節「為叢集設定 OSP 和 SSPR」(第 145 頁)
- ◆ 第 11.9 節「設定執行時期環境」(第 147 頁)
- ◆ 第 11.10 節「設定 Identity Reporting」(第 155 頁)

### 11.1 完成非 Root 使用者安裝

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

#### 11.1.1 為密碼規則建立容器

Identity Manager 需要 Identity Vault 中的密碼規則物件。但是，非 root 使用者身分安裝程序不會建立密碼規則的容器。

- 1 在 iManager 中登入 Identity Manager 網路樹。
- 2 導覽至 eDirectory 中的安全性容器。

#### 11.1.2 新增電子郵件通知中的圖形支援

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

- 1 在 Designer 中登入您的專案。
- 2 在「大綱」窗格中，展開 Identity Vault。
- 3 以滑鼠右鍵按一下驅動程式集。
- 4 選取內容 > Java。
- 5 對於 JVM 選項，輸入以下內容：

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

例如：

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

- 6 按一下**確定**。
- 7 部署對驅動程式集進行的變更：
  - 7a 以滑鼠右鍵按一下**驅動程式集**。
  - 7b 選取**即時 > 部署**。
  - 7c 選取**部署**。
- 8 重新啟動 Identity Vault。

## 11.2 安裝後設定 Identity Vault

在安裝 Identity Vault 後，您可以使用 `ndsconfig` 公用程式來設定目錄，並使用 `ndsmanage` 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。

### 11.2.1 使用 `ndsconfig` 公用程式修改 eDirectory 網路樹和複本伺服器

安裝 Identity Vault 之後，您便可使用 `ndsconfig` 公用程式來設定 Identity Vault。若要使用 `ndsconfig` 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 11.2 章「安裝後設定 Identity Vault」(第 98 頁)。

在使用 `ndsconfig` 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 `ndsconfig` 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 `ndsconfig` 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)。

## 瞭解 **ndsconfig** 公用程式參數

Ndsconfig 公用程式支援以下參數：

### **new**

建立新的 網路樹。如果您未在指令行中指定參數，該公用程式將會提示您為缺少的每個參數輸入值。

### **def**

建立新的 網路樹。如果您未在指令行中指定參數，**ndsconfig** 將為缺少的每個參數套用預設值。

### **add**

將伺服器新增至現有網路樹中。此外，當您在現有網路樹中設定 **Identity Vault** 後，它還會新增 LDAP 和 SAS 服務。

### **rm**

從網路樹移除伺服器物件及目錄服務。

---

**附註：**此選項不會移除金鑰資料物件。您必須手動移除這些物件。

---

### **upgrade**

將 **eDirectory** 升級至更高的版本。

### **-i**

指示公用程式在您設定新網路樹時，不要檢查是否存在同名的網路樹。系統中可以存在多個同名的網路樹。

### **-t 網路樹名稱**

指定要新增伺服器的網路樹名稱。該值最多可包含 **32** 個字元。如果未指定網路樹名稱，**ndsconfig** 將採用 **/etc/opt/novell/eDirectory/conf/nds.conf** 檔案指定之 **n4u.nds.treename** 參數中的名稱。預設的網路樹名稱為 **\$LOGNAME-\$HOSTNAME-NDStree**。

### **-n 伺服器網路位置**

指定要在其中新增伺服器物件的伺服器網路位置。該值最多可包含 **64** 個字元。如果未指定網路位置，**ndsconfig** 將採用 **/etc/opt/novell/eDirectory/conf/nds.conf** 檔案指定之 **n4u.nds.server-context** 組態參數中的網路位置。必須輸入已指定的伺服器網路位置。預設網路位置為 **org**。

### **-d DIB 路徑**

指定資料庫檔案將存放的目錄路徑。

### **-r**

強制新增該伺服器的複本，而不管已有多少個伺服器新增至該伺服器。

### **-L LDAP 連接埠**

指定 LDAP 伺服器上的 TCP 連接埠號。如果預設連接埠 **389** 已在使用中，該公用程式會提示您指定一個新連接埠。

### **-I SSL 連接埠**

指定 LDAP 伺服器上的 SSL 連接埠號。如果預設連接埠 **636** 已在使用中，該公用程式會提示您指定一個新連接埠。

### **-a 管理員 FDN**

指定對要在其中建立伺服器物件和目錄服務的網路位置擁有「監督者」權限之使用者物件的完全可辨識名稱。必須輸入已指定的 **admin** 名稱。該值最多可包含 **64** 個字元。預設值為 **admin.org**。

### **-e**

對 LDAP 物件啟用純文字密碼。

### **-m 模組名稱**

指定要安裝或設定之模組的名稱。如果您正在設定新網路樹，則只能指定 **ds** 模組。在設定 **ds** 模組後，可以使用 **add** 指令新增 **NMAS**、**LDAP**、**SAS**、**SNMP**、**HTTP** 服務和 **NetIQ SecretStore (ss)**。如果未指定模組名稱，則會安裝所有模組。

---

**附註：**如果您不想在透過 **nds-install** 指令升級 **eDirectory** 期間設定 **SecretStore**，請向此選項傳遞 **no\_ss** 值。例如，輸入 **ndsinstall '-m no\_ss'**。

---

### **-o**

指定 **HTTP** 純文字連接埠號。

### **-O**

指定 **HTTP** 安全連接埠號。

### **-p IP 位址 :[ 連接埠 ]**

指定遠端主機的 **IP** 位址，該遠端主機存放要新增此伺服器的分割區複本。在將次要伺服器新增至網路樹（使用 **add** 指令）時，請使用此選項。預設連接埠號碼為 **524**。這可以避免進行 **SLP** 查閱，因而有助於加快查閱網路樹的速度。

### **-R**

將您要向其新增伺服器的分割區複製到本地伺服器上。此選項會禁止將複本新增至本地伺服器。

### **-c**

防止在執行 **ndsconfig** 期間出現提示，例如，提示是否要繼續操作，或者在發生衝突時提示重新輸入連接埠號，等等。如果未在指令行上傳遞強制參數，該公用程式仍會提示您輸入這些參數。

### **-w 管理員密碼**

此選項允許傳遞純文字格式的管理員使用者密碼。

---

**附註：**NetIQ 不建議在注重密碼安全性的環境中使用此選項。

---

### **-E**

為您要嘗試新增的伺服器啟用加密複製。

### **-j**

指示公用程式在安裝 **Identity Vault** 之前跳過或置換狀態檢查選項。

### **-b 要結合的連接埠**

指定特定例項應監聽的預設連接埠號。這會設定 **n4u.server.tcp-port** 和 **n4u.server.udp-port** 上的預設連接埠號。如果您使用 **-b** 選項指定了 **NCP** 連接埠，則公用程式會假設該連接埠是預設連接埠，並相應地更新 **TCP** 和 **UDP** 參數。

---

附註：-b 和 -B 選項是互斥的參數。

---

### **-B interface1@port1,interface2@port2,...**

指定連接埠號以及 IP 位址或介面。例如 -B eth0@524、-B 100.1.1.2@524、-B[2015::3]@524。

---

附註：

- ◆ -b 和 -B 選項是互斥的參數。
  - ◆ 若要指定 IPv6 位址，必須將位址包含在方括號 ([ ]) 中。
- 

### **--config-file 組態檔案**

指定用於儲存 nds.conf 組態檔案的絕對路徑和檔案名稱。例如，若要在 /etc/opt/novell/eDirectory/directory 中儲存組態檔案，請輸入以下指令：

```
--config-file /etc/opt/novell/eDirectory/nds.conf
```

### **-P LDAP\_URL(s)**

允許 LDAP URL 設定 LDAP 伺服器物件上的 LDAP 介面。請使用逗號分隔多個 URL。例如：

```
-P ldap://1.2.3.4:389,ldaps://1.2.3.4:636,ldap://[2015::3]:389
```

---

附註：

- ◆ 若要指定 IPv6 位址，必須將位址包含在方括號 ([ ]) 中。例如 ldap://[2015::3]:389。
  - ◆ 如果在進行啟始組態設定時未指定 LDAP URL，您可以在完成啟始設定後，使用 ldapconfig 指令或 iManager 將其新增至 ldapInterfaces 屬性中。
- 

### **-D path\_for\_data**

在指定的路徑中建立 data、dib 和 log 目錄。

### **set valuelist**

設定您為 Identity Vault 指定之可設定參數的值。在設定網路樹之前，可以使用此選項設定開機參數。

變更組態參數後，必須重新啟動 ndsd 才能使新值生效。對於以下組態參數，無需重新啟動 ndsd：

- ◆ n4u.nds.inactivity-synchronization-interval
- ◆ n4u.nds.synchronization-restrictions
- ◆ n4u.nds.janitor-interval
- ◆ n4u.nds.backlink-interval
- ◆ n4u.nds.drl-interval
- ◆ n4u.nds.flatcleaning-interval
- ◆ n4u.nds.server-state-up-threshold
- ◆ n4u.nds.heartbeat-schema
- ◆ n4u.nds.heartbeat-data

## get help paramlist

顯示您為 Identity Vault 指定之可設定參數的說明字串。如果您未指定參數清單，該公用程式會列出所有可設定參數的說明字串。

## 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
```

## 將新網路樹新增至 Identity Vault 中

當您在 Identity Vault 中建立新網路樹時，ndsconfig 公用程式可以引導您完成組態設定，或者，您也可以輸入一個指令來指定所有參數值。如果您的 Identity Vault 伺服器原本就支援 IPv6 位址，您可以為新網路樹指定 IPv6 位址。

- 1 (視情況而定) 若要讓 ndsconfig 公用程式提示您為 Identity Vault 中的新網路樹指定參數，請輸入以下指令：

```
ndsconfig new [-t tree_name] [-n server_context] [-a admin_FDN]
```

例如：

```
ndsconfig new -t corp-tree -n o=company -a cn=admin.o=company
```

- 2 (視情況而定) 若要透過在指令行中指定所有參數的方式在 Identity Vault 中建立新網路樹，請輸入以下文字：

```
ndsconfig new [-t 網路樹名稱] [-n 伺服器網路位置] [-a 管理員 FDN] [-i] [-S 伺服器名稱] [-d DIB 路徑] [-m 模組] [-e] [-L LDAP 連接埠] [-l SSL 連接埠] [-o HTTP 連接埠] [-O HTTPS 連接埠] [-p IP 位址[:連接埠]] [-R] [-c] [-w 管理員密碼] [-b 要結合的連接埠] [-B interface1@port1,interface2@port2,...] [-D 自訂位置] [--config-file 組態檔案]
```

或

```
ndsconfig def [-t 網路樹名稱] [-n 伺服器網路位置] [-a 管理員 FDN] [-w 管理員密碼] [-c] [-i] [-S 伺服器名稱] [-d DIB 路徑] [-m 模組] [-e] [-L LDAP 連接埠] [-l SSL 連接埠] [-o HTTP 連接埠] [-O HTTPS 連接埠] [-D 自訂位置] [--config-file 組態檔案]
```

## 將伺服器新增至現有網路樹

若要将伺服器新增至現有網路樹，請輸入以下指令：

```
ndsconfig add [-t tree_name] [-n server_context] [-a admin_FDN] [-i] [-S server_name] [-d path_for_dib] [-m module] [-e] [-L ldap_port] [-l ssl_port] [-o http_port] [-O https_port] [-p IP_address[:port]] [-R] [-c] [-w admin_password] [-b port_to_bind] [-B interface1@port1,interface2@port2,...] [-D custom_location] [--config-file configuration_file]
```

例如：

```
ndsconfig add -t corp-tree -n o=company -a cn=admin.o=company -S srv1
```

## 從伺服器中移除 Identity Vault 及其資料庫

- 1 導覽至預設位於 `/var/opt/novell/eDirectory/data/` 中的 `dsreports` 目錄。
- 2 刪除您先前使用 iMonitor 建立的 HTML 檔案。
- 3 使用 `ndsconfig` 公用程式輸入以下指令：

```
ndsconfig rm [-a admin_FDN] [-w admin_password] [-p IP_address:[port]] [-c]
```

## 從網路樹中移除 eDirectory 伺服器物件和目錄服務

要從網路樹中移除 伺服器物件，請輸入以下指令：

```
ndsconfig rm -a Admin_FDN
```

## 設定多個 Identity Vault 例項

您可以在一個主機上設定多個 Identity Vault 例項。使用 `ndsconfig` 公用程式設定多個例項的方法類似於多次設定一個例項。每個例項應具有唯一的例項識別碼，如下所述：

- ◆ 不同的資料和記錄檔案位置。使用 `--config-file`、`-d` 和 `-D` 選項。
- ◆ 例項要監聽的唯一連接埠號。使用 `-b` 和 `-B` 選項。
- ◆ 例項的唯一伺服器名稱。使用 `-S 伺服器名稱` 選項。

如需詳細資訊，請參閱《[NetIQ eDirectory Installation Guide](#)》(NetIQ eDirectory 安裝指南) 中的「[Using ndsconfig to Configure Multiple Instances of eDirectory](#)」(使用 `ndsconfig` 設定多個 eDirectory 例項)。

---

附註：

- ◆ 在 Identity Vault 組態設定期間，預設的 NCP 伺服器名稱會設定為主機伺服器名稱。當設定多個例項時，您必須變更 NCP 伺服器名稱。使用 `ndsconfig` 指令行選項 `-S 伺服器名稱` 可以指定其他伺服器名稱。若要設定多個例項 (無論是在相同的網路樹還是不同的網路樹中)，NCP 伺服器名稱都應該是唯一的。
  - ◆ 所有例項共享同一個伺服器金鑰 (NICI)。
- 

## 11.2.2 使用 ndsmanage 公用程式管理例項

使用 `ndsmanage` 公用程式可以建立、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

您可以使用 `ndsmanage` 公用程式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)。該公用程式支援以下參數：

#### **ndsmanage**

列出您設定的所有例項。

## **ndsmanage -a|--all**

列出所有使用 Identity Vault 特定安裝版本之使用者的例項。

## **ndsmanage 使用者名稱**

列出指定使用者設定的例項。

## **在 Identity Vault 中建立新例項**

- 1 在指令行中輸入 **ndsmanage**。
- 2 輸入 **c**。
- 3 依照指令提示符中的指示建立新例項。

## **在 Identity Vault 中設定和取消設定例項**

若要設定例項，請輸入以下指令：

```
ndsconfig new -t treename -n server_context -a admin_FDN -b port_to_bind -D path_for_data
```

例如：

```
ndsconfig new -t mytree -n o=netiq -a cn=admin.o=company -b 1524 -D  
/home/mary/inst1/var --config-file /home/mary/inst1/nds.conf
```

---

**附註：**Linux 作業系統限制在裝入的檔案系統上建立通訊端。對於 eDirectory，NetIQ 建議將 var 目錄放置在本地檔案系統上 (結合 -D 選項使用 **ndsconfig**)，而 DIB 目錄可以採用任何檔案系統 (結合 -d 選項使用 **ndsconfig**)。

---

若要取消設定某個例項：

- 1 在指令行中輸入 **ndsmanage**。
- 2 選取要取消設定的例項。
- 3 輸入 **d**。

## **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。例如，您想要對監聽連接埠 1524 的例項 1 執行 **DSTrace** 公用程式，其組態檔案位於 `/home/mary/inst1/nds.conf` 目錄，並且其 DIB 檔案位於 `/home/mary/inst1/var` 目錄中。您可以輸入下列其中一個指令：

```
ndstrace --config-file /home/mary/inst1/nds.conf
```

或

```
ndstrace -h 192.168.0.1:1524
```

如果您未指定例項識別碼，該公用程式會顯示您的所有例項。然後，您便可以選取一個例項。



## 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。

1 (視情況而定) 若要透過引導式程序啟動或停止單個例項，請完成以下步驟：

1a 在指令行中輸入 `ndsmanage`。

1b 選取要啟動或停止的例項。

1c 輸入 `s` 或 `k` 相應地啟動或停止該例項。

2 (視情況而定) 若要啟動或停止單個例項，請輸入：

```
ndsmanage start --config-file configuration_file_of_the_instance
```

或

```
ndsmanage stop --config-file configuration_file_of_the_instance
```

3 (視情況而定) 若要啟動或停止所有例項，請輸入：

```
ndsmanage startall
```

或

```
ndsmanage stopall
```

## 11.3 設定遠端載入器和驅動程式

遠端載入器可以代管 `.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 64 頁)。

- 第 11.3.1 節「與 Identity Manager 引擎建立安全連接」(第 105 頁)
- 第 11.3.2 節「瞭解遠端載入器的組態參數」(第 108 頁)
- 第 11.3.3 節「為驅動程式例項設定遠端載入器」(第 115 頁)
- 第 11.3.4 節「為驅動程式例項設定 Java 遠端載入器」(第 117 頁)
- 第 11.3.5 節「設定 Identity Manager 驅動程式以與遠端載入器配合使用」(第 118 頁)
- 第 11.3.6 節「設定與 Identity Manager 引擎的雙向驗證」(第 119 頁)
- 第 11.3.7 節「驗證組態」(第 124 頁)
- 第 11.3.8 節「啟動遠端載入器中的驅動程式例項」(第 124 頁)
- 第 11.3.9 節「停止遠端載入器中的驅動程式例項」(第 125 頁)

### 11.3.1 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 106 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 107 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。您可以利用此選項搭配「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。

**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 107 頁）
- ◆ 「在 Linux 上建立金鑰儲存區」（第 107 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。

### 在 Linux 上建立金鑰儲存區

在 Linux 環境中，請使用 create\_keystore 檔案，這是一個會呼叫 Keytool 公用程式的外圍程序程序檔。該檔案已隨 rdxml 一起安裝，預設位於安裝目錄 /dirxml/bin 目錄中。\\dirxml\\java\_remoteloader 目錄下的 dirxml\_remote.tar.gz 檔案中也包含 create\_keystore 檔案。

在指令行輸入下列指令：

```
create_keystore self-signed_certificate_name keystorename
```

例如，輸入下列其中一項

```
create_keystore tree-root.b64 mystore
create_keystore tree-root.der mystore
```

Create\_keystore 程序檔會為金鑰儲存區密碼指定一個硬式編碼密碼「dirxml」。因為只有公用證書和公用金鑰儲存在金鑰儲存區中，所以這不是安全性風險。

## 11.3.2 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。您可以透過指令行在組態檔案中指定設定。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 11.3.3 節「為驅動程式例項設定遠端載入器」（第 115 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。依預設，該範例檔案位於 /opt/novell/dirxml/doc 目錄中。例如，該組態檔案可能包含以下幾行：

```
-commandport 8000
-connection "port=8090 rootfile=/dirxmlremote/root.pem"
-module $DXML_HOME/dirxmlremote/libcskeldrv.so.0.0.0
-trace 3
```

使用以下參數：

#### **-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 114 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 /var/opt/novell/dirxml/rdxml/data
```

使用此指令後，rdxml 程序會將其目前目錄變更為指定的目錄。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。若要為 Linux JVM 指定多個類別路徑，請在各路徑之間插入一個冒號。

### **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。



### **-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。

### **-piddir 目錄 (-pd 目錄)**

指定遠端載入器程序使用的程序 ID 檔案 (pidfile) 所在目錄的路徑。例如：

```
-piddir /var/opt/novell/dirxml/rdxml/data
```

Pidfile 主要由 SysV-style init 程序檔使用。預設值為 */var/run*。如果執行遠端載入器的使用者權限不足，無法開啟 */var/run* 中的 pidfile 以進行讀取和寫入，那麼，預設值將是目前的目錄。

此參數類似於 **-datadir**。

### **-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 /home/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。

## **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

---

Java 類別名稱	驅動程式
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
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

### 11.3.3 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。為使遠端載入器能夠在 Linux 電腦上執行，應用程式需要每個驅動程式例項都有相應的組態檔案 (例如 LDAPShim.txt)。您也可以使用指令行選項建立或編輯組態檔案。

依預設，遠端載入器使用 TLS/SSL 通訊協定透過 TCP/IP 連接到 Identity Manager 引擎。此連接的預設 TCP/IP 連接埠為 8090。您可以在同一個伺服器上執行多個驅動程式例項來與遠端載入器配合工作。每個例項代管一個獨立的 Identity Manager 應用程式 shim 例項。若要在同一個伺服器上使用遠端載入器的多個例項，請為每個例項指定不同的連接埠和指令埠。

---

附註：

- ◆ 組態檔案可以包含除 `-config` 之外的任何指令行選項。
  - ◆ 將參數新增至組態檔案時，可以使用參數的完整格式或簡寫格式。例如，可以使用 `-description` 或 `-desc`。
  - ◆ 以下程序先列出完整格式，然後在括號中列出簡寫格式。例如，`-description 值 (-desc 值)`。
  - ◆ 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 108 頁)。
- 

若要建立組態檔案：

- 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。依預設，該範例檔案位於 `/opt/novell/dirxml/doc` 目錄中。

- 2 將以下組態參數新增至該檔案：

- ◆ `-description` (選擇性)
- ◆ `-commandport`
- ◆ 連接參數：
  - ◆ `port` (強制)
  - ◆ `address`
  - ◆ `fromaddress`
  - ◆ `handshaketimeout`
  - ◆ `rootfile`
  - ◆ `keystore`
  - ◆ `localaddress`
  - ◆ `hostname`
  - ◆ `kmo`
  - ◆ `secureprotocol`
  - ◆ `enforceSuiteB`
  - ◆ `useMutualAuth`
- ◆ 追蹤檔案參數 (選擇性)：
  - ◆ `-trace`
  - ◆ `-tracefile`
  - ◆ `-tracefilemax`
- ◆ `-javaparam`
- ◆ `-class` 或 `-module`

如需指定這些參數的值的詳細資訊，請參閱第 11.3.2 節「[瞭解遠端載入器的組態參數](#)」(第 108 頁)。

- 3 儲存檔案。

若要在電腦啟動時自動啟動遠端載入器，請將該檔案儲存到 `/etc/opt/novell/dirxml/rdxml` 目錄中。

## 11.3.4 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。

若要在 Linux 平台上設定 Java 遠端載入器的新例項，請完成以下步驟。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 108 頁)。

- 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。依預設，該範例檔案位於 /opt/novell/dirxml/doc 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.Idap.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
- ◆ -keypassword
- ◆ -keystorepassword ( 僅適用於 Java 驅動程式 )
- ◆ 追蹤檔案參數 ( 選擇性 )：
  - ◆ -trace
  - ◆ -tracefile
  - ◆ -tracefilemax

- 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 /etc/opt/novell/dirxml/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 filename
```

## 11.3.5 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 108 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。

## 11.3.6 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 119 頁)
- ◆ 「啟用驅動程式以進行雙向驗證」(第 121 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 119 頁)
- ◆ 「為遠端載入器輸出協力廠商證書」(第 121 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

若要建立伺服器 KMO：

- 1 登入 NetIQ iManager。
- 2 在左側窗格中按一下 **NetIQ 證書伺服器**，然後選取伺服器證書。
- 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，serverkmo。
- 5 在證書建立方法中選取標準，然後按下一步。
- 6 檢閱摘要，按一下完成，然後按一下關閉。

若要建立用戶端 KMO：

- 1 登入 NetIQ iManager。
- 2 在左側窗格中按一下 **NetIQ 證書伺服器**，然後選取伺服器證書。
- 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，clientkmo
- 5 在證書建立方法中選取自訂，然後按下一步。

- 6 將預設的組織證書管理中心保留不變，然後按下一步。
- 7 取消選取啟用擴充金鑰使用，然後按下一步。
- 8 接受其餘的證書預設值。
- 9 檢閱摘要，按一下完成，然後按一下關閉。

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>
<javalnative|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 '/home/certs'

此指令會在 /home/certs/ 目錄中產生 serverkmo\_server.ks 檔案。金鑰儲存區的預設密碼為 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 11-1 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 192.168.0.1 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client java '/home/certs'	/home/certs/ 目錄中的 clientkmo_client.ks 檔案  金鑰儲存區的預設密碼為 dirxml。



## 為遠端載入器輸出協力廠商證書

若要将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。

### Java 驅動程式

透過 .pfx 檔案建立 Java 金鑰儲存區。輸入一條指令，例如 `keytool -importkeystore -srckeystore servercert.pfx -srcstoretype pkcs12 -destkeystore servercert.jks -deststoretype JKS`。

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 121 頁）
- ◆ 「為驅動程式例項設定遠端載入器」（第 123 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。

在 Designer 中，您可以在初始驅動程式建立過程中設定驅動程式，也可以在建立驅動程式後再設定。

若要在 Designer 中設定驅動程式：

- 1 在 Designer 中開啟您的專案。
- 2 在「模型產生器」檢視窗的選擇區中，選取您要建立的驅動程式。
- 3 將驅動程式的圖示拖曳至「模型產生器」檢視窗中。
- 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 `hostname=192.168.0.1`。如果未為此參數指定值，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。
  - 5c **KMO**：指定包含遠端載入器用於 SSL 連接的金鑰和證書的 KMO 金鑰名稱。例如，輸入 `kmo=serverkmo`。如果您要設定使用 KMO 進行的雙向驗證，則必須為此參數指定值。您還需要在「其他參數」區段指定根檔案參數的值。
  - 5d **其他參數**：指定您要使用的遠端載入器的設定。可以在此參數中包括有關雙向驗證通訊的資訊。指定的所有參數都必須使用金鑰值組格式，如下所示：`paraName1=paraValue1 paraName2=paraValue2`

例如，對於金鑰儲存區，請使用以下語法：

```
UseMutualAuth=true keystore='/home/certs/serverkmo_server.ks' storepass='dirxml' keypass='dirxml' key='serverkmo'
```

例如，對於 KMO，請使用以下語法：

```
useMutualAuth=true rootFile='/home/cacert.b64'
```

**5e 遠端密碼：**指定遠端載入器密碼。

**5f 驅動程式密碼：**指定驅動程式密碼。

**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。

或者，您可以在建立驅動程式之後，透過執行以下步驟來設定驅動程式：

**1** 在 **Designer** 的「大綱」檢視窗中，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** 選取**驗證**。

**5** 在 **遠端載入器驗證**區段下方，指定設定遠端載入器與 **Identity Manager** 引擎間的雙向驗證所需的資訊。

對於 **KOM**，請使用以下語法：

```
hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true kmo=certificatename rootFile=<absolute path to the file>
```

例如：

```
hostname=192.168.0.1 port=8090 useMutualAuth=true kmo=serverkmo rootFile='/home/cacert.b64'
```

對於金鑰儲存區，請使用以下語法：

```
hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true keystore=<absolute path to the keystore file> storepass=<keystore password> key=<alias name> keypass= <password for the key>
```

例如：

```
hostname=192.168.0.1 port=8097 useMutualAuth=true keystore='/home/certs/serverkmo_server.ks' storepass='dirxml' key='serverkmo' keypass='dirxml'
```

**若要在 iManager 中修改組態：**

**1** 啟動 **iManager**。

**2** 在綜覽中，選取 **Identity Manager** 驅動程式物件。

**3** 在驅動程式物件的內容中，完成以下步驟：

**3a** 對於**驅動程式模組**，請選取**連接至遠端載入器**。

**3b** 對於**驅動程式物件密碼**，請指定遠端載入器用於向引擎驗證的密碼。

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。

**3c** 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。

對於 **KOM**，請使用以下語法：

```
hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true kmo=certificatename rootFile=<absolute path to the file>
```

例如：

```
hostname=192.168.0.1 port=8090 useMutualAuth=true kmo=serverkmo rootFile='/home/cacert.b64'
```

對於金鑰儲存區，請使用以下語法：

```
hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true keystore=<absolute path to the  
keystore file> storepass=<keystore password> key=<alias name> keypass= <password for the  
key>
```

例如：

```
hostname=192.168.0.1 port=8097 useMutualAuth=true keystore='/home/certs/  
serverkmo_server.ks' storepass='dirxml' key='serverkmo' keypass='dirxml'
```

**3d** ( 選擇性 ) 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所需的密碼。

**3e** 按一下「套用」，然後按一下「確定」。

## 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檔案、證書檔案和根檔案的目錄的絕對路徑。

修改驅動程式的遠端載入器組態檔案，以包括用於啟用雙向驗證的內容。該檔案位於 `/opt/novell/dirxml/doc` 目錄中。

若要修改組態：

**1** 登入安裝了驅動程式和遠端載入器的伺服器。

**2** 停止遠端載入器。

例如，輸入以下指令：

```
rdxml -config /home/drivershim.conf -u
```

**3** 根據遠端載入器類型提供金鑰儲存區或金鑰密碼：

**Java 遠端載入器：**

使用以下語法指定金鑰儲存區密碼和金鑰密碼的組合：

```
dirxml_jremote -config /home/drivershim.conf -ksp <keystorepassword> -kp <keypassword>
```

例如，

```
dirxml_jremote -config /home/drivershim.conf -ksp dirxml -kp dirxml
```

**原生遠端載入器：**

使用以下語法指定金鑰密碼：

```
dirxml_jremote -config /home/drivershim.conf -kp <keypassword>
```

例如，

```
dirxml_jremote -config /home/drivershim.conf -kp dirxml
```

**4** 在文字編輯器中開啟驅動程式的遠端載入器組態檔案。

**5** 將啟用雙向驗證所需的內容新增至該檔案。

◆ 例如，對於 Java 驅動程式，請新增以下項目：

```
-connection "port=8090 useMutualAuth=true keystore='/home/certs/clientkmo_client.ks'  
key='clientkmo'
```

- ◆ 例如，對於原生驅動程式，請新增以下項目：

```
-connection "useMutualAuth=true port=8090 rootfile='/home/certs/trustedcert.b64'  
certfile='/home/certs/clientkmo_clientcert.pem' keyfile='/home/certs/  
clientkmo_clientkey.pem' certform=PEM keyform=PEM"
```

- 6 儲存然後關閉該檔案。
- 7 重新啟動驅動程式。

## 11.3.7 驗證組態

1. 啟動遠端載入器。例如：

```
dirxml_remote -config config.txt
```

2. 使用 **iManager** 啟動遠端介面 **shim**。
3. 確認遠端載入器運作正常。
4. 停止遠端載入器。例如：

```
dirxml_remote -config config.txt -u
```

## 11.3.8 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。

NetIQ 可讓您以兩種方式啟動遠端載入器的驅動程式例項：

- ◆ 「自動啟動驅動程式例項」(第 124 頁)
- ◆ 「使用指令行啟動驅動程式例項」(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電腦啟動時自動啟動。請將您的組態檔案放置在 `/etc/opt/novell/dirxml/rdxml` 目錄中。

### 使用指令行啟動驅動程式例項

對於遠端載入器，二進位元件 `rdxml` 支援指令行功能。依預設，此元件位於 `/usr/bin/` 目錄中。

- 1 啟
- 2 (視情況而定) 若要指定用於向 **Identity Manager** 引擎驗證驅動程式例項的密碼，請輸入以下指令之一：
  - ◆ 遠端載入器：`rdxml -config filename -keystorepassword <keystore pass> -keypassword <key pass>`
  - ◆ **Java** 遠端載入器：`dirxml_jremote -config filename -keystorepassword <keystore pass> -keypassword <key pass>`
- 3 (視情況而定) 如果在遠端載入器的驅動程式例項與 **Identity Manager** 引擎之間啟用了雙向驗證，請輸入以下指令之一來指定證書密碼：
  - ◆ 遠端載入器：`rdxml -config filename -keystorepassword <keystore pass> -keypassword <key pass>`

- ◆ **Java 遠端載入器**：`dirxml_jremote -config filename -keypassword <key pass>`

4 若要啟動驅動程式例項，請輸入以下指令：

`rdxml -config 檔案名稱`

5 登入 iManager，然後啟動驅動程式。

6 確認遠端載入器正在正常運作。

使用 `ps` 指令或追蹤檔案確定指令和連接埠是否正在監聽。

遠端載入器僅會在與 Identity Manager 引擎伺服器上的遠端介面 `shim` 通訊時，載入 Identity Manager 應用程式 `shim`。這表示，如果遠端載入器與伺服器的通訊中斷，應用程式 `shim` 將會關閉。

## 11.3.9 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。

---

附註：

- ◆ 如果執行了遠端載入器的多個例項，請包含 `-cp command port` 選項，以確保遠端載入器能夠停止相應的例項。
  - ◆ 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。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。如果您將遠端載入器做為應用程式而非服務執行，它將會使用該密碼。
- 

若要停止某個驅動程式例項：

### 遠端載入器

輸入 `rdxml -config 檔案名稱 -u` 指令。例如：

`rdxml -config config.txt -u`

### 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`

## 11.4 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)。

## 11.5 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。

## 11.6 完成 Identity Applications 的設定

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

依預設，用於執行組態公用程式 (configupdate.sh) 的檔案位於 /opt/netiq/idm/apps/configupdate 目錄中：

---

附註：

- ◆ 您應該只從 configupdate 目錄執行 configupdate.sh。從自訂位置執行 configupdate.sh 將導致失敗。
  - ◆ 在叢集中，所有叢集成員的組態設定都必須相同。
- 

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 11.6.1 節「執行 Identity Applications 組態公用程式」](#) (第 126 頁)
- ◆ [第 11.6.2 節「使用者應用程式參數」](#) (第 127 頁)
- ◆ [第 11.6.3 節「Reporting 參數」](#) (第 136 頁)
- ◆ [第 11.6.4 節「驗證參數」](#) (第 138 頁)
- ◆ [第 11.6.5 節「SSO 用戶端參數」](#) (第 141 頁)
- ◆ [第 11.6.6 節「CEF 稽核參數」](#) (第 145 頁)

### 11.6.1 執行 Identity Applications 組態公用程式

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

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

---

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

---

2 儲存並關閉 `configupdate.sh`。

3 在指令提示符處，執行以下指令來執行組態公用程式：

`./configupdate.sh`

---

**附註：**您可能需要花幾分鐘時間等待公用程式啟動。

---

## 11.6.2 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 127 頁)
- ◆ 「**Identity Vault DN**」(第 128 頁)
- ◆ 「**Identity Vault 使用者身分**」(第 130 頁)
- ◆ 「**Identity Vault 使用者群組**」(第 131 頁)
- ◆ 「**Identity Vault 證書**」(第 132 頁)
- ◆ 「**電子郵件伺服器組態**」(第 132 頁)
- ◆ 「**可信金鑰儲存區**」(第 134 頁)
- ◆ 「**NetIQ Sentinel 數位簽名證書與金鑰**」(第 134 頁)
- ◆ 「**其他**」(第 134 頁)
- ◆ 「**容器物件**」(第 136 頁)

## Identity Vault 設定

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

### Identity Vault 伺服器

*必需*

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

### LDAP 連接埠

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

### LDAP 安全連接埠

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

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



## Identity Vault 管理員

*必需*

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

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

## Identity Vault 管理員密碼

*必需*

指定與 LDAP 管理員關聯的密碼。這個密碼會根據萬能金鑰進行加密。

## 使用公用匿名帳戶

指定未登入的使用者是否能夠存取 LDAP 公用匿名帳戶。

## 安全管理員連接

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

---

**附註：**此選項可能會對效能造成負面影響。

---

## 安全使用者連接

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

---

**附註：**此選項可能會對效能造成負面影響。

---

## Identity Vault DN

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

### 根容器 DN

*必需*

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

### 使用者容器 DN

*必需*

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

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

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



## 群組容器 DN

### 必需

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

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

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

## 使用者應用程式驅動程式

### 必需

指定使用者應用程式驅動程式的可辨識名稱。

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

## 使用者應用程式管理員

### 必需

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

- ◆ 如果您已啟動代管使用者應用程式的 Tomcat，則無法使用 `configupdate.sh` 檔案變更此設定。
- ◆ 若要在部署使用者應用程式後變更此指定，請在使用者應用程式的**管理 > 安全性**頁面中進行變更。
- ◆ 此使用者帳戶有權使用使用者應用程式的**管理**索引標籤來管理入口網站。
- ◆ 如果使用者應用程式管理員參與 *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.sh` 檔案變更此設定。
- ◆ 此容器必須包含您在安裝使用者應用程式驅動程式時指定的使用者應用程式管理員。否則，指定的帳戶將無法執行工作流程。

## 使用者搜尋範圍

指定 Identity Vault 使用者在搜尋容器時可以探查的範圍深度。

## 使用者物件類別

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

## 登入屬性

指定代表使用者登入名稱的 LDAP 屬性。例如，`cn`。

## 命名屬性

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

## 使用者成員資格屬性

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

# Identity Vault 使用者群組

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

僅當您選取了顯示進階選項時，公用程式才會顯示這些設定。

## 群組容器 DN

*必需*

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

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

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

## 群組容器範圍

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

## 群組物件類別

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

## 群組成員資格屬性

(選擇性) 指定使用者的群組成員資格。請勿在此名稱中使用空格。

## 使用動態群組

指定是否要使用動態群組。

您還必須指定動態群組物件類別的值。

## 動態群組物件類別

*僅當您選取了使用動態群組時才適用。*

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

# Identity Vault 證書

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

## 金鑰儲存區路徑

*必需*

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

- ◆ 在環境中，您必須指定 RBPM 的安裝目錄。預設值會設定為正確的位置。
- ◆ Identity Applications 的安裝程式將會修改金鑰儲存區檔案。在 Linux 上，使用者必須具有寫入此檔案的許可權。

## 金鑰儲存區密碼

*必需*

指定金鑰儲存區檔案的密碼。預設值為「changeit」。

# 電子郵件伺服器組態

本節定義用於啟用電子郵件通知的值，您可以使用電子郵件通知來進行基於電子郵件的核准。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，/opt/netiq/idm/apps/jre/lib/security/cacerts。

### 金鑰儲存區密碼

*僅當您啟用了對電子郵件簽名時才適用。*

指定金鑰儲存區檔案的密碼。例如，changeit。

## 簽名金鑰的別名

*僅當您啟用了對電子郵件簽名時才適用。*

指定簽章金鑰在金鑰儲存區中的別名。例如，`idmapptest`。

## 簽名金鑰密碼

*僅當您啟用了對電子郵件簽名時才適用。*

指定用於保護包含簽名金鑰的檔案的密碼。例如，`changeit`。

## 可信金鑰儲存區

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

### 可信儲存區路徑

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

### 可信儲存區密碼

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

這個密碼會根據萬能金鑰進行加密。

### 可信證書儲存區類型

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

## NetIQ Sentinel 數位簽名證書與金鑰

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

### Sentinel 數位簽名證書

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

### Sentinel 數位簽名私密金鑰

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

## 其他

僅當您選取了**顯示進階選項**時，公用程式才會顯示這些設定。

### OCSP URI

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

OCSP URI 會在線上更新可信證書的狀態。



## 授權組態路徑

指定授權組態檔案的完全合格名稱。

## Identity Vault 索引

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。

## 11.6.3 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 136 頁)
- ◆ 「報告保留值」(第 137 頁)
- ◆ 「修改地區設定」(第 137 頁)
- ◆ 「職能組態」(第 137 頁)

## 電子郵件傳送組態

本節定義用於傳送通知的值。

### SMTP 伺服器主機名稱

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

### SMTP 伺服器連接埠

指定 SMTP 伺服器的連接埠號。

### SMTP 使用 SSL

指定是否要使用 TLS/SSL 通訊協定來與電子郵件伺服器通訊。



## 伺服器需要驗證

指定是否要對電子郵件伺服器通訊使用驗證。

## SMTP 使用者名稱

指定要用來進行驗證的電子郵件地址。

您必須指定一個值。如果伺服器不需要驗證，則可指定無效的位址。

## SMTP 使用者密碼

*僅當您指定了伺服器需要驗證時才適用。*

指定 SMTP 使用者帳戶的密碼。

## 預設電子郵件地址

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

## 報告保留值

本節定義用於儲存已完成報告的值。

### 報告單位，報告生命期間

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

### 報告的位置

指定要用來儲存報告定義的路徑。例如 /opt/netiq/IdentityReporting。

## 修改地區設定

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

## 職能組態

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

### 新增驗證來源

指定您要為報告功能新增的驗證來源類型。驗證來源可以是

- ◆ 預設值
- ◆ LDAP 目錄
- ◆ 檔案

## 11.6.4 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 138 頁)
- ◆ 「驗證組態」(第 138 頁)
- ◆ 「驗證方法」(第 139 頁)
- ◆ 「密碼管理」(第 139 頁)
- ◆ 「Sentinel 數位簽名證書和金鑰」(第 140 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。

## 11.6.5 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 141 頁)
- ◆ 「IDM 管理員」(第 142 頁)
- ◆ 「RBPM」(第 142 頁)
- ◆ 「報告」(第 143 頁)
- ◆ 「IDM 資料收集服務」(第 143 頁)
- ◆ 「DCS 驅動程式」(第 144 頁)
- ◆ 「Self Service Password Reset」(第 144 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 11-1 IDM 儀表板

IDM 儀表板	
OAuth 用戶端 ID	<input type="text" value="idmdash"/>
OAuth 用戶端機密	<input type="password" value="*****"/>
OSP OAuth 重新導向 URL	<input type="text" value="https://192.168.0.1:8543/idmdash/oauth.html"/>

#### OAuth 用戶端 ID

必需

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

#### OAuth 用戶端密碼

必需

指定儀表板的單一登入用戶端的密碼。

#### OSP OAuth 重新導向 URL

必需

指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。

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

## IDM 管理員

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

### OAuth 用戶端 ID

*必需*

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

### OAuth 用戶端密碼

*必需*

指定 Identity Manager 管理員單一登入用戶端的密碼。

### OSP OAuth 重新導向 URL

*必需*

指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。

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

## RBPM

本節定義使用者在存取使用者應用程式時需要使用的 URL 值。

圖 11-2 RBPM

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

### OAuth 用戶端 ID

*必需*

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

### OAuth 用戶端密碼

*必需*

指定使用者應用程式單一登入用戶端的密碼。

### 抵達頁面的 URL 連結

*必需*

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

### OSP OAuth 重新導向 URL

*必需*

指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。

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

## RBPM 至 eDirectory SAML 的組態

*必需*

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

## 報告

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

圖 11-3 報告

報告	
OAuth 用戶端 ID	<input type="text" value="rpt"/>
OAuth 用戶端機密	<input type="text" value="....."/>
抵達頁面的 URL 連結	<input type="text" value="/idmdash/#/landing"/>
Identity Governance 的 URL 連結	<input type="text"/>
OSP OAuth 重新導向 URL	<input type="text" value="https://192.168.0.1:8543/IDMRPT/oauth.html"/>

### OAuth 用戶端 ID

*必需*

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

### OAuth 用戶端密碼

*必需*

指定 Identity Reporting 單一登入用戶端的密碼。

### 抵達頁面的 URL 連結

*必需*

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

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

### OSP OAuth 重新導向 URL

*必需*

指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。

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

## IDM 資料收集服務

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

### OAuth 用戶端 ID

*必需*

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

## OAuth 用戶端密碼

*必需*

指定 Identity Manager 資料收集服務單一登入用戶端的密碼。

## OSP OAuth 重新導向 URL

*必需*

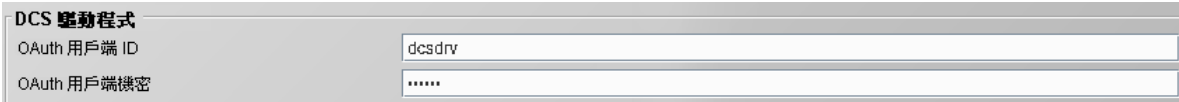
指定在驗證完成後，驗證伺服器要將瀏覽器用戶端重新導向到的絕對 URL。

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

## DCS 驅動程式

本節定義用於管理資料收集服務驅動程式的值。

圖 11-4



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

## OAuth 用戶端 ID

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

## OAuth 用戶端密碼

指定資料收集服務驅動程式單一登入用戶端的密碼。

## Self Service Password Reset

本節定義使用者存取 SSPR 所需 URL 的值。

## OAuth 用戶端 ID

*必需*

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

## OAuth 用戶端密碼

*必需*

指定 SSPR 單一登入用戶端的密碼。

## 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。



## 11.6.6 CEF 稽核參數

本節定義用於管理單一登入用戶端的 CEF 稽核參數的值。

### 傳送稽核事件

指定是否要使用 CEF 來稽核事件。

### 目的地主機

指定稽核伺服器的 DNS 名稱或 IP 位址。

### 目的地連接埠

指定稽核伺服器的連接埠。

### 網路協定

指定稽核伺服器用來接收 CEF 事件的網路通訊協定。

### 使用 TLS

*僅當您要使用 TCP 做為網路通訊協定時適用。*

指定稽核伺服器是否設定為將 TLS 與 TCP 搭配使用。

### 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。

---

## 11.7 啟動 Identity Applications

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

```
systemctl restart netiq-tomcat
```

```
systemctl restart netiq-activemq
```

## 11.8 為叢集設定 OSP 和 SSPR

Identity Manager 支援 Tomcat 叢集環境中的 SSPR 組態。

### 11.8.1 設定 SSPR 以支援叢集

若要在叢集的第一個節點中更新 SSPR 資訊，請啟動 `/opt/netiq/idm/apps/configupdate/configupdate.sh` 中的組態公用程式。

在隨即開啟的視窗中，按一下 **SSO 用戶端 > Self Service Password Reset**，並為用戶端 ID、密碼和 **OSP OAuth 重新導向 URL** 參數輸入值。

## 11.8.2 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 22 節「設定忘記密碼管理功能」(第 205 頁)。
- 2 若要變更「變更我的密碼」連結，請參閱第 22.3 節「針對分散式環境或叢集環境更新儀表板中的 SSPR 連結」(第 208 頁)。
- 3 在叢集中的其他節點上，驗證「忘記密碼」連結和「變更我的密碼」連結是否已用 SSPR IP 位址更新。

---

**附註：**如果「變更密碼」和「忘記密碼」連結已用 SSPR IP 位址更新，則不需要執行其他變更。

---

- 4 在第一個節點中，停止 Tomcat，並使用以下指令指定負載平衡器伺服器的 DNS 名稱，以產生新 osp.jks 檔案：

```
/opt/netiq/common/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass <password> -keypass <password> -alias osp -validity 1800 -dname "cn=<loadbalancer IP/DNS>"
```

例如：/opt/netiq/common/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass changeit -keypass changeit -alias osp -validity 1800 -dname "cn=mydnsname"

---

**附註：**確認金鑰密碼與在 OSP 安裝期間提供的密碼相同。或者，可以使用組態更新公用程式並包括金鑰儲存區密碼來變更該密碼。

---

- 5 (視情況而定) 若要驗證 osp.jks 檔案是否已透過這些變更更新，請執行以下指令：  

```
/opt/netiq/common/jre/bin/keytool -list -v -keystore osp.jks -storepass changeit
```
- 6 備份位於 /opt/netiq/idm/apps/osp 中的原始 osp.jks 檔案，並將新 osp.jks 檔案複製到此位置。新 osp.jks 檔案是在步驟 3 中建立的。
- 7 將第一個節點上位於 /opt/netiq/idm/apps/osp 中的新 osp.jks 檔案複製到叢集中的所有其他使用者應用程式節點上。
- 8 在第一個節點中啟動組態公用程式，並在「SSO 用戶端」索引標籤下將所有 URL 設定 (例如抵達頁面的 URL 連結和 OAuth 重新導向 URL) 變更為負載平衡器 DNS 名稱。
  - 8a 儲存在組態公用程式中所做的變更。
  - 8b 若要在叢集的所有其他節點中反映此變更，請將第一個節點上位於 /TOMCAT\_INSTALLED\_HOME/conf 中的 ism-configuration properties 檔案複製到所有其他使用者應用程式節點。

---

**附註：**您之前已將第一個節點上的 ism.properties 檔案複製到叢集中的其他節點。如果您在安裝使用者應用程式期間指定了自訂安裝路徑，請在叢集節點中使用組態更新公用程式確保參考路徑正確。

此情境中，OSP 和使用者應用程式安裝在同一部伺服器上；因此，為重新導向 URL 使用了相同的 DNS 名稱。

如果 OSP 與使用者應用程式安裝在不同的伺服器上，請將 OSP URL 變更為指向負載平衡器的不同 DNS 名稱。請對安裝了 OSP 的所有伺服器執行此操作。這可確保所有 OSP 申請均透過負載平衡器傳發送到 OSP 叢集 DNS 名稱。這涉及到為 OSP 節點建立一個單獨的叢集。

---

- 9 在 `/TOMCAT_INSTALLED_HOME/bin/` 目錄下的 `setenv.sh` 檔案中執行以下動作：
- 9a 為確保成功進行 `mcast_addr` 繫結，JGroups 要求 `preferIPv4Stack` 內容設定為 `true`。為此，請在所有節點上的 `setenv.sh` 檔案中新增 JVM 內容「`-Djava.net.preferIPv4Stack=true`」。
  - 9b 在第一個節點上的 `setenv.sh` 檔案中新增「`-Dcom.novell.afw.wf.Engine-id=Engine`」。  
引擎名稱應該是唯一的。請提供安裝第一個節點時指定的名稱。如果之前未指定名稱，則預設名為「`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。
- 11 為叢集啟用許可權索引。如需更多資訊，請參閱「[為叢集啟用許可權索引](#)」(第 71 頁)。
- 12 在所有節點上重新啟動 Tomcat。
- 13 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 11.5 節「[為叢集設定使用者應用程式驅動程式](#)」(第 126 頁)。

## 11.9 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，您應執行的額外組態步驟的相關資訊。此外，本節還提供了一些疑難排解方法，以及關於特定用途資料庫表格的一些資訊。

此程序包括以下活動：

- [第 11.9.1 節「將資料收集服務驅動程式設定為從 Identity Applications 收集資料」](#) (第 147 頁)
- [第 11.9.2 節「移轉資料收集服務驅動程式」](#) (第 148 頁)
- [第 11.9.3 節「新增對自訂屬性和物件的支援」](#) (第 150 頁)
- [第 11.9.4 節「新增多個驅動程式集支援」](#) (第 152 頁)
- [第 11.9.5 節「將驅動程式設定為使用 SSL 在遠端模式下執行」](#) (第 153 頁)

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

### 11.9.1 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) 如果您尚未將 DCS 驅動程式升級至支援的修補程式版本，請完成以下步驟：

3a 下載最新的 DCS 驅動程式修補程式檔案。

3b 將該修補程式檔案擷取到伺服器上的某個位置。

3c 在終端機中，導覽至適用於您環境之修補程式 RPM 的擷取位置，然後執行以下指令：

```
rpm -Uvh novell-DXMLdcs.rpm
```

3d 重新啟動 Identity Vault。

3e 在 Designer 中，確保已安裝受支援版本的資料收集服務基礎套件。如果需要，請安裝最新版本，然後再繼續。如需軟體要求的詳細資訊，請參閱第 8.6.2 節「安裝 Identity Reporting 各元件的先決條件」(第 78 頁)。

3f 在 Designer 中重新部署並重新啟動 DCS 驅動程式。

4 在大綱檢視窗中，於 DCS 驅動程式上按一下滑鼠右鍵，然後選取內容。

5 按一下驅動程式組態。

6 按一下驅動程式參數索引標籤。

7 按一下顯示連接參數，然後選取顯示。

8 按一下 SSO 服務支援，然後選取是。

9 指定 Reporting Module 的 IP 位址和連接埠。

10 指定 SSO 服務用戶端的密碼。預設密碼為 driver。

11 按一下「套用」，然後按一下「確定」。

12 在模型產生器檢視窗中，於 DCS 驅動程式上按一下滑鼠右鍵，然後選取驅動程式 > 部署。

13 按一下部署。

14 收到重新啟動 DCS 驅動程式的提示時，按一下是。

15 按一下「確定」。

## 11.9.2 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] character character varying(128)	first_name character varying(128)	last_name character varying(128)	middle_initial character var	full_name character var	job_title character var	department character var	location character var	email_address character var	office_phone character var	cell_phone character var
1	1210e8e9b55e4	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	13fa90666584c	Ken	Carson			Attending Physici		Northeast	pfredrickson@n	(555) 555-1315	
6	1c886916cfd24	Jane	Smith			Administrative A		Northeast	pfredrickson@n	(555) 555-1234	
7	1e8e3fcb7364	Application Administrator	Of Sample Data								
8	24fd8b301bce4	Bill	Burke			Administrative A		cn-loc1	pfredrickson@n	(555) 555-1210	
9	278698aace6b4	April	Smith			Nurse		Northeast	pfredrickson@n	(555) 555-1319	
10	2d8df9981b1c4	Brad	Jones			Resident Physi		Northeast	pfredrickson@n	(555) 555-1313	

## 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：

Attribute	Value
employeeType	ft
ACL	6#entry#cn=karson,ou=users,ou=medical-idmsample,o=novell#loginScript
ACL	6#entry#cn=karson,ou=users,ou=medical-idmsample,o=novell#printJobConfiguration
DirXML-Associations	cn=Data Collection Service Driver,cn=TestDrivers,o=novell#1#C53ADD67-DB19-4DD2-9482-67DD3AC519DB
givenName	Ken
photo	BINARY (2Kb)
snrprvYahooIMAddress	karson
objectClass	inetOrgPerson
objectClass	organizationalPerson
objectClass	Person
objectClass	ndsLoginProperties
objectClass	Top
objectClass	snrprvUserAux
objectClass	snrprvEntityAux
objectClass	homeInfo
objectClass	sampleUserDeviceAux
snrprvGroupwiseIMAddress	test
employeeStatus	Active
costCenter	US11115
ou	medical
securityEquals	cn=Medical Operations,ou=groups,ou=medical-idmsample,o=novell
securityEquals	cn=Physician,ou=groups,ou=medical-idmsample,o=novell
uid	karson
mail	pfredrickson@novell.com
cn	karson
passwordAllowChange	TRUE
sampleDeviceDN	cn=karson-laptop,ou=devices,ou=medical-idmsample,o=novell

- 對於每個群組，驗證以下類型的資訊：

equivalentToMe	cn=jsmith,ou=users,ou=medical-idmsample,o=novell
equivalentToMe	cn=jkelly,ou=users,ou=medical-idmsample,o=novell
description	Operations
objectClass	groupOfNames
objectClass	Top
DirXML-Associations	cn=Data Collection Service Driver,cn=TestDrivers,o=novell#1#91539E44-6AFC-4676-D9A2-449E5391FC6A
cn	Operations
member	cn=apalani,ou=users,ou=medical-idmsample,o=novell
member	cn=fstats,ou=users,ou=medical-idmsample,o=novell
member	cn=rresource,ou=users,ou=medical-idmsample,o=novell
member	cn=jsmith,ou=users,ou=medical-idmsample,o=novell
member	cn=jkelly,ou=users,ou=medical-idmsample,o=novell

## 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_group boolean	dynamic_rule character var	nested_group boolean	idmrpt_valid_from timestamp without time zone	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 Resource	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Physician	Physician	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Operations	Operations	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Medical Operations	Medical Operations	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Nursing	Nursing	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1

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

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。

### 11.9.3 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 150 頁)
- ◆ 「包含資料庫中的名稱和描述」(第 151 頁)
- ◆ 「將延伸屬性新增至已知物件類型」(第 152 頁)

#### 將驅動程式設定為使用延伸物件

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

```

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

```

## 包含資料庫中的名稱和描述

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

例如：

```

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

```

下面是一個可顯示資料庫中這些物件和屬性值的 SQL 範例：

```

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

```

## 將延伸屬性新增至已知物件類型

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

以下 SQL 範例可顯示這些延伸屬性：

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

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

- ◆ nrfRole
- ◆ nrfResource
- ◆ 容器

---

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

---

- ◆ 群組
- ◆ nrfSod

您可以查看 idmrpt\_cat\_item\_types.idmrpt\_table\_name 欄，來瞭解延伸屬性與父表格或父物件之間的關聯。此欄描述如何將 idm\_rpt\_data.idmrpt\_ext\_item\_attr.cat\_item\_id 欄聯結到父表格的主鍵。

## 11.9.4 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。

如果您使用整合式安裝程序將另一個伺服器新增至網路樹中，則伺服器只會接收根及其自身驅動程式集分割區的副本。如果您還使用了資料收集服務驅動程式做為此次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。



- ◆ **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况：

- ◆ 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。

## 11.9.5 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 153 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 154 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 154 頁) 中指定的別名。
  - 5e 儲存驅動程式並將其重新啟動。

## 11.10 設定 Identity Reporting

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

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

- 第 11.10.1 節「在「身分資料收集服務」頁面中手動新增資料來源」(第 155 頁)
- 第 11.10.2 節「對 Oracle 資料庫執行報告」(第 155 頁)
- 第 11.10.3 節「手動產生資料庫綱要」(第 155 頁)
- 第 11.10.4 節「清除資料庫檢查總數」(第 156 頁)
- 第 11.10.5 節「部署 Identity Reporting 的 REST API」(第 157 頁)
- 第 11.10.6 節「連接遠端 Remote PostgreSQL 資料庫」(第 157 頁)

### 11.10.1 在「身分資料收集服務」頁面中手動新增資料來源

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

### 11.10.2 對 Oracle 資料庫執行報告

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

如需受支援 Oracle 資料庫的詳細資訊，請參閱第 8.6.4 節「Identity Reporting 的系統要求」(第 80 頁)。

### 11.10.3 手動產生資料庫綱要

若要在安裝後手動產生資料庫綱要，請對您的資料庫執行下列程序之一：

- 「針對 PostgreSQL 資料庫設定 Create\_rpt\_roles\_and\_schemas.sql 綱要」(第 155 頁)
- 「針對 Oracle 資料庫設定 Create\_rpt\_roles\_and\_schemas.sql 綱要」(第 156 頁)

#### 針對 PostgreSQL 資料庫設定 Create\_rpt\_roles\_and\_schemas.sql 綱要

- 1 使用位於 /mnt/reporting/sql 中的 create\_dcs\_roles\_and\_schemas.sql 和 create\_rpt\_roles\_and\_schemas.sql SQL，將必需的角色新增至資料庫。
  1. 以 postgres 使用者身分登入 PGAdmin。

2. 執行查詢工具。
3. 若要建立 `Create_rpt_roles_and_schemas` 和 `Create_dcs_roles_and_schemas` 程序，請將這些 SQL 中的內容複製到查詢工具，然後對連接的資料庫執行指令。
4. 若要建立 `IDM_RPT_DATA`、`IDM_RPT_CFG` 和 `IDMRPTUSER` 角色，請依給定順序執行以下指令：
 

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

Select CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>', '<Set pwd for
IDMRPTUSER>');
```
5. 若要建立 `IDM_RPT_DATA` 綱要，請將 `/mnt/Reporting/sql` 中 `get_formatted_user_dn.sql` 的內容複製到查詢工具，然後對連接的資料庫執行指令。

## 針對 Oracle 資料庫設定 `Create_rpt_roles_and_schemas.sql` 綱要

- 1 使用 `/mnt/Reporting/sql` 中的 `create_dcs_roles_and_schemas-oracle.sql` 和 `create_rpt_roles_and_schemas-oracle.sql`，將必需的角色新增至資料庫。
  1. 以資料庫管理員使用者身分登入 `SQL Developer`。
  2. 若要建立 `Create_rpt_roles_and_schemas` 和 `Create_dcs_roles_and_schemas` 程序，請將這些 SQL 中的內容複製到 `SQL Developer`，然後對連接的資料庫執行指令。
  3. 若要建立 `IDM_RPT_DATA`、`IDM_RPT_CFG` 和 `IDMRPTUSER` 角色，請依給定順序執行以下指令：
 

```
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;
```
  4. 若要建立 `IDM_RPT_DATA` 綱要，請將 `/mnt/Reporting/sql` 中 `get_formatted_user_dn-oracle.sql` 的內容複製到 `SQL Developer`，然後對連接的資料庫執行指令。

### 11.10.4 清除資料庫檢查總數

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

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

修改後的內容應該類似如下：

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

2b 以相應的使用者身分執行每個 .sql。

3 將變更提交到資料庫。

## 11.10.5 部署 Identity Reporting 的 REST API

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

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

## 11.10.6 連接遠端 Remote PostgreSQL 資料庫

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

1 在 postgresql.conf 檔案中變更監聽位址。

依預設，PostgreSQL 允許監聽 localhost 連接，不允許遠端 TCP/IP 連接。若要允許遠端 TCP/IP 連接，請將下面的項目新增至 /opt/netiq/idm/postgres/data/postgresql.conf 檔案中：

```
listen_addresses = '*'
```

如果伺服器上有多個介面，可以指定要監聽的特定介面。

2 將用戶端驗證項目新增至 pg\_hba.conf 檔案中。

依預設，PostgreSQL 只接受來自 localhost 的連接。它會拒絕遠端連接。透過套用存取控制規則來控制此行為，該規則允許使用者在提供有效密碼 (md5 關鍵字) 後從某個 IP 位址登入。若要接受遠端連接，請將下面的項目新增至 /opt/netiq/idm/postgres/data/pg\_hba.conf 檔案中。

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

例如，192.168.104.24/26 trust

這僅適用於 IPv4 位址。對於 IPv6 位址，請新增以下項目：

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

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

pg\_hba.conf 檔案支援以下用戶端驗證格式。

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

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

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

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

### **3** 測試遠端連接。

**3a** 重新啟動遠端 PostgreSQL 伺服器。

**3b** 使用使用者名稱和密碼從遠端登入伺服器。

# V 安裝 Designer

此部分將引導您完成安裝 Designer for Identity Manager 的程序。





# 12 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。

- ◆ 第 12.1 節「Designer 安裝核對清單」(第 161 頁)
- ◆ 第 12.2 節「安裝 Designer 的先決條件」(第 161 頁)
- ◆ 第 12.3 節「Designer 的系統要求」(第 161 頁)

## 12.1 Designer 安裝核對清單

NetIQ 建議您在開始安裝之前檢閱以下步驟。

	核對清單項目
<input type="checkbox"/>	1. 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 12.2 節「安裝 Designer 的先決條件」(第 161 頁)。
<input type="checkbox"/>	2. 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 12.3 節「Designer 的系統要求」(第 161 頁)。
<input type="checkbox"/>	3. 安裝 Designer。如需詳細資訊，請參閱第 13 節「安裝 Designer」(第 163 頁)。
<input type="checkbox"/>	4. (選擇性) 若要啟動 Identity Manager 解決方案的專案，請參閱《Understanding Designer for Identity Manager》(瞭解 Designer for Identity Manager)。

## 12.2 安裝 Designer 的先決條件

本節提供安裝 Designer 的先決條件和注意事項。

- ◆ 在執行 Linux 作業系統的電腦上安裝 Designer 之前，必須先安裝 GNU gettext 公用程式。這些公用程式提供了國際化和多語言訊息的架構。如需語言支援的詳細資訊，請參閱第 5.10 節「瞭解語言支援」(第 46 頁)。
- ◆ 在執行 RHEL 7.4 作業系統的電腦上安裝 Designer 之前，必須先安裝 gtk2-2.24.31-1.el7.x86\_64.rpm。例如，可以從作業系統廠商網站下載套件。

## 12.3 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

類別	要求
磁碟空間	1 GB
記憶體	1 GB
作業系統 (已認證)	<p>以下 64 位元作業系統之一：</p> <p><b>伺服器</b></p> <ul style="list-style-type: none"> <li>◆ SLES 12 SP3</li> <li>◆ SLES 12 SP2</li> <li>◆ RHEL 7.4</li> <li>◆ RHEL 7.3</li> <li>◆ openSUSE Leap 42.1</li> </ul> <p><b>桌面</b></p> <ul style="list-style-type: none"> <li>◆ SLED 12 SP3</li> <li>◆ SLED 12 SP2</li> </ul> <p><b>附註：</b> <i>已認證</i>指作業系統已進行全面測試且受支援。</p>
作業系統 (受支援)	<p>已認證作業系統的最新版 <b>Service Pack</b></p> <p><b>附註：</b> <i>受支援</i>指作業系統尚未進行測試，但預期可正常運作</p>
虛擬化系統	<ul style="list-style-type: none"> <li>◆ Hyper-V Server 2012 R2</li> <li>◆ VMWare ESX 5.5 或更新版本</li> </ul> <p>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 <b>Identity Manager</b>。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 <b>Identity Manager</b> 堆疊。</p>

# 13 安裝 Designer

本章介紹 Designer 的安裝過程。可以採用圖形使用者介面或主控台模式執行安裝。

若要安裝 Designer：

- 1 從 NetIQ 下載網站下載 Identity\_Manager\_Linux\_LDAP\_Designer.tar.gz。
- 2 導覽至要擷取檔案的目錄。
- 3 執行以下指令：  
`tar -zxvf Identity_Manager_Linux_LDAP_Designer.tar.gz`
- 4 執行以下指令之一來安裝 Designer。  
主控台：`./install`  
圖形使用者介面：`./install -i console`
- 5 依照提示操作並繼續安裝。





# 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。

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 14.1 節「**Analyzer** 的安裝核對清單」(第 167 頁)。



# 14 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 14.1 節「Analyzer 的安裝核對清單」(第 167 頁)
- ◆ 第 14.2 節「安裝 Analyzer 的先決條件」(第 167 頁)
- ◆ 第 14.3 節「Analyzer 的系統要求」(第 168 頁)

## 14.1 Analyzer 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
<input type="checkbox"/>	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 17 頁)。
<input type="checkbox"/>	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 5.7 節「建議的安裝情境和伺服器設定」(第 38 頁)。
<input type="checkbox"/>	3. 確保您的環境符合代管 Analyzer 的考量和要求。如需詳細資訊，請參閱以下各節： <ul style="list-style-type: none"><li>◆ 第 14.2 節「安裝 Analyzer 的先決條件」(第 167 頁)</li><li>◆ 第 14.3 節「Analyzer 的系統要求」(第 168 頁)</li></ul>
<input type="checkbox"/>	4. 若要安裝 Analyzer，請參閱以下章節： <ul style="list-style-type: none"><li>◆ 若要使用安裝精靈，請參閱第 15.1 節「使用精靈安裝 Analyzer」(第 169 頁)。</li><li>◆ 若要執行靜默安裝，請參閱第 15.2 節「以靜默模式安裝 Analyzer」(第 170 頁)</li></ul>
<input type="checkbox"/>	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 15.4 節「安裝 Analyzer 的稽核用戶端」(第 171 頁)。
<input type="checkbox"/>	6. 若要啟用 Analyzer，請參閱第 24.4.2 節「啟用 Analyzer」(第 215 頁)。
<input type="checkbox"/>	7. (選擇性) 若要升級 Analyzer，請參閱第 26.7 節「升級 Analyzer」(第 245 頁)。

## 14.2 安裝 Analyzer 的先決條件

本節提供安裝 Analyzer 的先決條件和注意事項。

- ◆ 在執行 SLES 12 SP3 作業系統的電腦上安裝 Analyzer 之前，請確定已安裝以下程式庫：
  - ◆ libswt3-gtk2-3.3.0-0.20.8.9mdv2008.0.i586.rpm
  - ◆ libxcomposite1-0.4.1-1mdv2010.1.i586.rpm

- ◆ libgdk\_pixbuf2.0\_0-2.20.1-1mdv2010.1.i586.rpm
- ◆ libgtk+-x11-2.0\_0-2.12.1-2.1mdv2008.0.i586.rpm
- ◆ 在執行 RHEL 7.3 或更新版本平台的電腦上安裝 Analyzer 之前，必須先安裝 gtk2.i686.rpm。例如，可以從作業系統廠商網站下載套件。

## 14.3 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	2 GB
視訊解析度	1024*768 (建議 1280*1025)
作業系統 (已認證)	<p>下列作業系統之一：</p> <ul style="list-style-type: none"> <li>◆ SLES 12 SP3</li> <li>◆ SLES 12 SP2</li> <li>◆ RHEL 7.4</li> <li>◆ RHEL 7.3</li> <li>◆ openSUSE Leap 42.1</li> </ul> <p><b>附註：</b> <i>已認證</i>指作業系統已進行全面測試且受支援。</p>
作業系統 (受支援)	<p>已認證作業系統的最新版 <b>Service Pack</b></p> <p><b>附註：</b> <i>受支援</i>指作業系統尚未進行測試，但預期可正常運作</p>
虛擬化系統	<ul style="list-style-type: none"> <li>◆ Hyper-V Server 2012 R2</li> <li>◆ VMWare ESX 5.0 及更新版本</li> </ul> <p>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。</p>
其他軟體	<ul style="list-style-type: none"> <li>◆ Gettext 公用程式</li> </ul>



# 15 安裝 Analyzer

本章將引導您完成安裝 Analyzer 及設定其環境的程序。

- 第 15.1 節「使用精靈安裝 Analyzer」(第 169 頁)
- 第 15.2 節「以靜默模式安裝 Analyzer」(第 170 頁)
- 第 15.3 節「將 XULrunner 新增至 Analyzer.ini 中」(第 170 頁)
- 第 15.4 節「安裝 Analyzer 的稽核用戶端」(第 171 頁)

## 15.1 使用精靈安裝 Analyzer

以下程序描述如何透過圖形使用者介面或主控台使用安裝精靈在 Linux 或 Windows 平台上安裝 Analyzer。若要執行靜默模式的無人管理安裝，請參閱第 15.2 節「以靜默模式安裝 Analyzer」(第 170 頁)。

若要進行安裝準備工作，請檢閱第 14.1 節「Analyzer 的安裝核對清單」(第 167 頁)中列出的先決條件和系統要求。

- 1 以 root 或管理員身分登入您要安裝 Analyzer 的電腦。
- 2 (視情況而定) 如果您已取得 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 (預設位於 /Analyzer/packages 目錄中)。
- 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 .tgz 或 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 執行安裝程式：

```
./install
```
- 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 (視情況而定) 完成第 15.3 節「將 XULrunner 新增至 Analyzer.ini 中」(第 170 頁)中的步驟。
- 9 (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。
- 10 若要啟用 Analyzer，請參閱「啟用 Analyzer」(第 215 頁)。

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

依預設，安裝程式會在 **Program Files (x86)\NetIQ\Analyzer** 目錄中安裝 **Analyzer**。

- 1 以 root 或管理員身分登入您要安裝 **Analyzer** 的電腦。
- 2 (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 **Analyzer** 安裝檔案的目錄 (預設位於 **products/Analyzer/** 目錄中)。
- 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 .tgz 或 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 **analyzerInstaller.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，請發出下列其中一個指令：
  - ◆ **Linux** : `install -i silent -f analyzerInstaller.properties`
  - ◆ **Windows** : `install.exe -i silent -f analyzerInstaller.properties`
- 6 (視情況而定) 在 Linux 電腦上，完成第 15.3 節「將 **XULrunner** 新增至 **Analyzer.ini** 中」(第 170 頁) 中的步驟。
- 7 若要啟用 **Analyzer**，請參閱「啟用 **Analyzer**」(第 215 頁)。

## 15.3 將 XULrunner 新增至 Analyzer.ini 中

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

---

**附註：**在 SLED 11 上建議使用 **XULrunner 1.9.0.19**，在 openSUSE 11.4 上建議使用 **XULrunner 1.9.0.2**。這些版本會隨相應的作業系統一起提供。

---

- 1 導覽至預設位於以下位置的 **Analyzer** 安裝目錄：

```
home/admin/analyzer
```
- 2 在 **gedit** 編輯器中開啟 **Analyzer.ini** 檔案。
- 3 在參數清單的末尾新增下面的行：

```
-Dorg.eclipse.swt.browser.XULRunnerPath=/usr/lib/xulrunner-1.9/
```

例如，**Analyzer.ini** 檔案的內容應如下所示：

```
-vmargs  
-Xms256m  
-Xmx1024m  
-XX:MaxPermSize=128m  
-XX:+UseParallelGC  
-XX:ParallelGCThreads=20  
-XX:+UseParallelOldGC  
-Dorg.eclipse.swt.browser.XULRunnerPath=/usr/lib/xulrunner-1.9/
```

4 儲存 Analyzer.ini 檔案。

5 啟動 Analyzer。

## 15.4 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 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 使用 rpm 指令啟動 XDAS 用戶端的安裝程式。

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。



# VII

## 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。



# 16 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
<input type="checkbox"/>	1. 安裝 Identity Applications。如需詳細資訊，請參閱第 9 章「安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting」(第 83 頁)。
<input type="checkbox"/>	2. (選擇性) 安裝 Identity Reporting。如需詳細資訊，請參閱第 9 章「安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting」(第 83 頁)。
<input type="checkbox"/>	3. 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 17 章「在 Identity Manager 中使用 One SSO Provider 進行單一登入存取」(第 177 頁)。
<input type="checkbox"/>	4. 安裝您要用於 Identity Manager 的驗證系統。例如 Access Manager 或 Kerberos。
<input type="checkbox"/>	5. (視情況而定) 設定 Access Manager 和 OSP。如需詳細資訊，請參閱第 18 章「對 NetIQ Access Manager 使用 SAML 驗證進行單一登入」(第 179 頁)。
<input type="checkbox"/>	6. 驗證單一登入設定。如需詳細資訊，請參閱第 19 章「驗證是否可對 Identity Applications 進行單一登入存取」(第 185 頁)。





# 17 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。

## 17.1 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。

## 17.2 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 11.6.1 節「執行 Identity Applications 組態公用程式」(第 126 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。
    - ◆ 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。

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。
- ◆ 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。

## 17.3 將 Self Service Password Reset 設定為信任 OSP

為了使單一登入正常運作，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。

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)。

# 18 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)。

## 18.1 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。

## 18.2 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 18.2.1 節「為 Access Manager 建立 SSL 證書」(第 180 頁)
- 第 18.2.2 節「在 Identity Manager 可信證書儲存區中安裝 Access Manager 證書」(第 180 頁)
- 第 18.2.3 節「在 Access Manager 可信證書儲存區中安裝 SSL 伺服器證書」(第 181 頁)

## 18.2.1 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 18.2.2 節「在 Identity Manager 可信證書儲存區中安裝 Access Manager 證書」(第 180 頁)。

## 18.2.2 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，`/opt/netiq/common/jre/bin/keytool -importcert -trustcacerts -alias <NAM-cert> -keystore /opt/netiq/common/jre/lib/security -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 18.2.3 節「在 Access Manager 可信證書儲存區中安裝 SSL 伺服器證書」(第 181 頁)。

## 18.2.3 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 18.4.2 節「[建立 SAML 的屬性集](#)」(第 182 頁)。

## 18.3 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 11.6.1 節「[執行 Identity Applications 組態公用程式](#)」(第 126 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。

## 18.4 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 18.4.1 節「複製 Identity Manager 的中繼資料」(第 182 頁)
- ◆ 第 18.4.2 節「建立 SAML 的屬性集」(第 182 頁)
- ◆ 第 18.4.3 節「將 Identity Manager 新增為可信的服務提供者」(第 183 頁)

### 18.4.1 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「將 Identity Manager 新增為可信的服務提供者」(第 183 頁) 中您可以存取的文件中。

### 18.4.2 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。



### 18.4.3 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 182 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 182 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。

## 18.5 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 /opt/novell/idm/apps 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**。



# 19 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 11.6 章「完成 Identity Applications 的設定」(第 126 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。



# 20 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。

您必須擁有證書才能將 Tomcat 伺服器設定為使用 SSL 進行通訊。可透過兩種方法來獲取證書：

- ◆ 外部可信的證書管理中心 (CA) 核發的證書
- ◆ 自行簽署的證書

安裝程式會使用 Identity Vault 核發的證書，自動為 Identity Applications 與 Identity Reporting 元件設定安全連接 (HTTPS)。對於生產環境，建議您使用外部證書管理中心核發的證書。

## 20.1 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
<input type="checkbox"/>	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 20.2 節「 <a href="#">建立金鑰儲存區和證書簽署要求</a> 」(第 188 頁)。
<input type="checkbox"/>	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 20.4 節「 <a href="#">使用自行簽署的證書啟用 SSL</a> 」(第 190 頁)。對於生產環境，則建議使用外部 CA 核發的證書。
<input type="checkbox"/>	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 20.3 節「 <a href="#">使用外部 CA 簽署的證書啟用 SSL</a> 」(第 189 頁)。
<input type="checkbox"/>	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 20.6 節「 <a href="#">更新應用程式伺服器的 SSL 設定</a> 」(第 195 頁)與第 20.7 節「 <a href="#">在組態公用程式中更新 SSL 設定</a> 」(第 196 頁)。

## 20.2 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。

依預設，安裝程式會在 /opt/netiq/idm/apps/tomcat/conf 中建立名為 tomcat.ks 的金鑰儲存區，然後使用此金鑰儲存區來設定 https 連接。如果您建立了同名的金鑰儲存區檔案，請取代此目錄中的此金鑰儲存區檔案。

- 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，/opt/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 /opt/netiq/idm/apps/tomcat/conf
export PATH=/opt/netiq/common/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，`/opt/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 20.3 節「使用外部 CA 簽署的證書啟用 SSL」(第 189 頁)。
- 對於自行簽署的證書，請參閱第 20.4 節「使用自行簽署的證書啟用 SSL」(第 190 頁)。

## 20.3 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 20.2 節「建立金鑰儲存區和證書簽署要求」(第 188 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，`/opt/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，`/opt/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 IDMTREE.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輸入到 **idm.jks**。這是一個集中式金鑰儲存區，用於儲存供 **Identity Applications** 和 **Identity Reporting** 使用的所有證書。例如：

```
keytool -import -trustcacerts -alias root -keystore /opt/netiq/idm/apps/tomcat/conf/idm.jks -file IDMTTESTREE.der
```

- 5** 更新應用程式伺服器的 **SSL** 設定，請參閱第 20.6 節「更新應用程式伺服器的 **SSL** 設定」(第 195 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 20.7 節「在組態公用程式中更新 **SSL** 設定」(第 196 頁)。
- 7** 更新 **Self Service Password Reset** 的 **SSL** 設定。如需詳細資訊，請參閱第 20.8 節「更新 **Self Service Password Reset** 的 **SSL** 設定」(第 197 頁)。
- 8** 重新啟動 **Tomcat**。

## 20.4 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 20.4.1 節「輸出證書管理中心」(第 190 頁)
- ◆ 第 20.4.2 節「產生自行簽署的證書」(第 191 頁)

### 20.4.1 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 **IDMTTESTTREE 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 **IDMTESTTREE 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，**/opt/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 /opt/netiq/common/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.keystore
```

例如，

```
keytool -list -v -alias root -keystore IDMkey.keystore
```

伺服器會列出證書。

## 20.4.2 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 20.2 節「建立金鑰儲存區和證書簽署要求」(第 188 頁)

- 1 登入 iManager。
- 2 導覽至證書伺服器 > 發放證書。
- 3 瀏覽至第 20.2 節「建立金鑰儲存區和證書簽署要求」(第 188 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，`/opt/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  
/opt/netiq/common/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 20.6 節「更新應用程式伺服器的 `SSL` 設定」(第 195 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 20.7 節「在組態公用程式中更新 `SSL` 設定」(第 196 頁)。
- 11 更新 `Self Service Password Reset` 的 `SSL` 設定。如需詳細資訊，請參閱第 20.8 節「更新 `Self Service Password Reset` 的 `SSL` 設定」(第 197 頁)。
- 12 重新啟動 `Tomcat`。

## 20.5 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 20.5.1 節「在 `Sentinel` 與 `Identity Manager` 引擎 / 遠端載入器之間啟用 `SSL`」(第 193 頁)
- ◆ 第 20.5.2 節「在 `Sentinel` 與使用者應用程式之間啟用 `SSL`」(第 194 頁)



## 20.5.1 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 重新啟動 Identity Manager 服務。

## 20.5.2 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 瀏覽至 `\products\RBPM\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。

## 20.6 更新應用程式伺服器的 SSL 設定

安裝程式會自動設定代管 Identity Applications 和 Identity Reporting 的應用程式伺服器，以支援 SSL 通訊。它預設會在位於 /opt/netiq/idm/apps/tomcat/conf/ 目錄下的 server.xml 檔案中建立連接器。

```
<Connector port="https_port" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="150"
SSLEnabled="true" scheme="https" secure="true" clientAuth="false" sslProtocol="TLSv1.2"
keystoreFile="path_to_keystore_file" keystorePass="keystore_password" sslEnabledProtocols="TLSv1.2"
/>
```

位於：

### keystoreFile

指定金鑰儲存區檔案（例如，idmapps.keystore 檔案）的路徑。將該檔案放在 /opt/netiq/idm/apps/tomcat/conf/ 目錄中。

### keystorePass

指定 tomcat.ks 檔案的密碼。

您必須驗證 `server.xml` 檔案中的金鑰儲存區密碼和金鑰儲存區檔案路徑是否正確。

若要修改安裝提供的值，請執行以下動作：

- 1 如果 Tomcat 正在執行，請將其停止。
- 2 導覽至 Tomcat 的 `conf` 目錄 (預設為 `/opt/netiq/idm/apps/tomcat/conf/`)。
- 3 確定 `conf` 目錄中包含金鑰儲存區檔案。例如，`tomcat.ks`。

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 20.2 節「建立金鑰儲存區和證書簽署要求」(第 188 頁)。

- 4 在文字編輯器中開啟 `conf` 目錄中的 `server.xml` 檔案。
- 5 設定 Tomcat 伺服器的 SSL 連接埠。

例如，SSL 的連接器連接埠為 8543。

另外，請將 `redirectPort` 屬性更新為 8543，然後儲存 `server.xml`。

例如：

```
<Connector port="8543" protocol="HTTP/1.1" maxThreads="150" SSLEnabled="true" scheme="https"
secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile="/opt/netiq/idm/apps/tomcat/
conf/idmaps.keystore" keystorePass="encrypted_password"/>
```

- 6 啟動 Tomcat。

例如，`systemctl start netiq-tomcat.service`

## 20.7 在組態公用程式中更新 SSL 設定

安裝程式會自動進行 SSL 設定。若要修改安裝提供的值，請執行以下動作：

- 1 如果 Tomcat 正在執行，請使用 `services.msc` 檔案將其停止。  
例如，`systemctl status netiq-tomcat.service`。
- 2 導覽至預設位於 Identity Applications 安裝目錄中的 RBPM 組態公用程式。
- 3 在指令提示符處，執行組態公用程式 (`configupdate.sh`)：

---

**附註：**您可能需要花幾分鐘時間等待公用程式啟動。

---

- 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 啟動 Tomcat。

## 20.8 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：

`/opt/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`



## 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：





# 21 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](#)。

## 21.1 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 21.1.1 節「建立驅動程式集」](#) (第 201 頁)
- [第 21.1.2 節「將預設密碼規則指定給驅動程式集」](#) (第 201 頁)
- [第 21.1.3 節「在 Identity Vault 中建立密碼規則物件」](#) (第 202 頁)
- [第 21.1.4 節「建立自訂密碼規則」](#) (第 203 頁)
- [第 21.1.5 節「在 Identity Vault 中建立預設通知集合物件」](#) (第 203 頁)

### 21.1.1 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)。

### 21.1.2 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 21.1.3 節「在 Identity Vault 中建立密碼規則物件」](#) (第 202 頁) 與[第 21.1.4 節「建立自訂密碼規則」](#) (第 203 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。

## 21.1.3 在 Identity Vault 中建立密碼規則物件

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

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

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

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

---

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

---

2 若要在 Identity Vault 中新增 DirXML-PasswordPolicy 物件，請執行以下動作以從檔案輸入屬性：

從包含 **ldapmodify** 公用程式的目錄中，輸入以下指令：

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

例如：

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

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

## 21.1.4 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 21.1.3 節「在 **Identity Vault** 中建立密碼規則物件」(第 202 頁)。

---

## 21.1.5 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**。

## 21.2 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。

## 21.3 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。

# 22 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。

- 第 22.1 節「使用 Self Service Password Reset 進行忘記密碼管理」(第 205 頁)
- 第 22.2 節「使用外部系統進行忘記密碼管理」(第 207 頁)
- 第 22.3 節「針對分散式環境或叢集環境更新儀表板中的 SSPR 連結」(第 208 頁)

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

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

- 第 22.1.1 節「將 Identity Manager 設定為使用 Self Service Password Reset」(第 205 頁)
- 第 22.1.2 節「為 Identity Manager 設定 Self Service Password Reset」(第 206 頁)
- 第 22.1.3 節「鎖定 SSPR 組態」(第 206 頁)

### 22.1.1 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 11.6.1 節「執行 Identity Applications 組態公用程式」(第 126 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。

## 22.1.2 為 Identity Manager 設定 Self Service Password Reset

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

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

---

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

---

- 1 使用您在安裝期間指定的組態密碼登入 SSPR。
- 2 在「設定」頁面中，修改密碼規則和處理安全回應問題的設定。如需設定 SSPR 設定預設值的詳細資訊，請參閱《[NetIQ Self Service Password Reset Administration Guide](#)》(NetIQ Self Service Password Reset 管理指南) 中的「[Configuring Self Service Password Reset](#)」(設定 Self Service Password Reset)。
- 3 鎖定 SSPR 組態檔案 (SSPRConfiguration.xml)。如需鎖定組態檔案的詳細資訊，請參閱「[鎖定 SSPR 組態](#)」(第 206 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。

## 22.1.3 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。

## 22.2 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：

- 第 22.2.1 節「指定外部忘記密碼管理 WAR 檔案」(第 207 頁)
- 第 22.2.2 節「測試外部忘記密碼組態」(第 208 頁)
- 第 22.2.3 節「設定應用程式伺服器之間的 SSL 通訊」(第 208 頁)

### 22.2.1 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 11.6.1 節「執行 Identity Applications 組態公用程式」(第 126 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，請指定外部傳遞密碼 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 208 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。

## 22.2.2 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。

## 22.2.3 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。

## 22.3 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。



# 23 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。

## 23.1 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 23.1.1 節「停止驅動程式」](#) (第 209 頁)
- [第 23.1.2 節「啟動驅動程式」](#) (第 210 頁)

### 23.1.1 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 209 頁)
- 「使用 [iManager](#) 來停止驅動程式」 (第 209 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 連接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。

## 23.1.2 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 210 頁)
- ◆ 「使用 iManager 來啟動驅動程式」(第 210 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「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。



# 24 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 24.1 節「安裝產品啟用身分證明」(第 213 頁)
- 第 24.2 節「檢閱 Identity Manager 和驅動程式的產品啟用」(第 214 頁)
- 第 24.3 節「啟用 Identity Manager 驅動程式」(第 214 頁)
- 第 24.4 節「啟用特定的 Identity Manager 元件」(第 214 頁)

## 24.1 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：**對於要啟用的每個驅動程式，啟用包含驅動程式的整合模組。

---

- 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」。

## 24.2 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。

## 24.3 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 24.1 節「安裝產品啟用身分證明」(第 213 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。

## 24.4 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。

- 第 24.4.1 節「啟用 Designer」(第 215 頁)
- 第 24.4.2 節「啟用 Analyzer」(第 215 頁)
- 第 24.4.3 節「啟用 Sentinel Log Management for IGA」(第 215 頁)

## 24.4.1 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 和 Catalog Administrator。

## 24.4.2 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，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 在 **Micro Focus Customer Center** 頁面中按一下**造訪 NetIQ 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。

## 24.4.3 啟用 Sentinel Log Management for IGA

您可在安裝 Sentinel 時新增授權。本節提供有關在安裝 Sentinel 後新增授權金鑰的資訊。

如果您使用的是預設安裝的試用版授權金鑰，則必須在試用版金鑰過期前啟用 Sentinel，以免 Sentinel 功能中斷。如需如何採購授權的資訊，請造訪 [Identity Manager 產品網站](#)。

您可以使用 Sentinel 主要介面或透過指令行來新增授權金鑰。

- ◆ 「使用 [Sentinel 主要介面新增授權金鑰](#)」(第 215 頁)
- ◆ 「[透過指令行新增授權金鑰](#)」(第 216 頁)

### 使用 Sentinel 主要介面新增授權金鑰

- 1 以管理員身分登入 Sentinel 主要介面。
- 2 按一下**關於 > 授權**。
- 3 按一下「授權」區段中的「**新增授權**」。

4 在「金鑰」欄位中指定授權金鑰。

在指定授權後，以下資訊會出現在「預覽」區段中：

- ◆ **特性**：授權提供的功能。
- ◆ **主機名稱**：此欄位僅供 NetIQ 內部使用。
- ◆ **序號**：此欄位僅供 NetIQ 內部使用。
- ◆ **EPS**：授權金鑰內建的事件率。超過此速率時，Sentinel 會產生警告，但會繼續收集資料。
- ◆ **過期**：授權的過期日。您必須在過期日之前指定有效的授權金鑰，以避免功能中斷。

5 按一下「儲存」。

## 透過指令行新增授權金鑰

如果您使用的是 Sentinel 傳統安裝，則可以使用 `softwarekey.sh` 程序檔透過指令行來新增授權。

- 1 以 root 身分登入 Sentinel 伺服器。
- 2 移至 `/opt/novell/sentinel/bin` 目錄。
- 3 輸入下列指令以變更為 novell 使用者：  
`su novell`
- 4 指定下列指令以執行 `softwarekey.sh` 程序檔。  
`./softwarekey.sh`
- 5 輸入 1 以插入授權金鑰。
- 6 指定授權金鑰，然後按 **Enter**。



# 升級 Identity Manager

此部分提供升級 Identity Manager 各元件的資訊。



# 25

## 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 25.1 節「Identity Manager 的升級核對清單」(第 219 頁)
- 第 25.2 節「瞭解升級程序」(第 220 頁)
- 第 25.3 節「支援的升級路徑」(第 221 頁)
- 第 25.4 節「備份目前組態」(第 224 頁)

### 25.1 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
<input type="checkbox"/>	1. 瞭解升級程序。如需詳細資訊，請參閱第 25.2 節「瞭解升級程序」(第 220 頁)。
<input type="checkbox"/>	2. 查看將 Identity Manager 升級至 4.7 的受支援路徑。如需受支援升級路徑的資訊，請參閱第 25.3 節「支援的升級路徑」(第 221 頁)。
<input type="checkbox"/>	3. 確定您已取得用於升級 Identity Manager 的安裝套件。
<input type="checkbox"/>	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 15 頁)。
<input type="checkbox"/>	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 5.9 章「準備安裝」(第 42 頁)和您要升級至的版本的《版本說明》。
<input type="checkbox"/>	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 25.4 節「備份目前組態」(第 224 頁)。
<input type="checkbox"/>	7. 將 Designer 升級至最新版本。如需詳細資訊，請參閱第 26.2 節「升級 Designer」(第 227 頁)。
<input type="checkbox"/>	8. 將 Sentinel Log Management for IGA 升級至最新版本。如需詳細資訊，請參閱第 26.6.3 節「升級 Sentinel Log Management for IGA」(第 243 頁)。
<input type="checkbox"/>	9. 在執行 Identity Manager 的伺服器上，將 Identity Vault (eDirectory) 升級至 9.1。這是 Identity Manager 引擎升級程序的第一步。如需詳細資訊，請參閱第 26.3.1 節「升級 Identity Vault」(第 228 頁)。  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)。
<input type="checkbox"/>	10. 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 23.1.1 節「停止驅動程式」(第 209 頁)。

	核對清單項目
<input type="checkbox"/>	<p>11. 升級 Identity Manager 引擎。如需詳細資訊，請參閱第 26.3 節「升級 Identity Manager 引擎」(第 228 頁)。</p> <p><b>附註：</b>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 29.4 節「將 Identity Manager 引擎移轉至新伺服器」(第 258 頁)。</p>
<input type="checkbox"/>	<p>12. (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 26.3.3 節「升級遠端載入器」(第 229 頁)。</p>
<input type="checkbox"/>	<p>13. 將 iManager 升級至 3.1。如需詳細資訊，請參閱第 26.3.4 節「升級 iManager」(第 230 頁)。</p>
<input type="checkbox"/>	<p>14. 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「在升級或重新安裝後更新 iManager 外掛程式」(第 231 頁)。</p>
<input type="checkbox"/>	<p>15. (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 26.4 節「升級 Identity Manager 驅動程式」(第 232 頁)。</p> <p>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。</p>
<input type="checkbox"/>	<p>16. 升級 Identity Applications。如需詳細資訊，請參閱第 26.5 節「升級 Identity Applications」(第 233 頁)。</p>
<input type="checkbox"/>	<p>17. 升級 Identity Reporting。如需詳細資訊，請參閱第 26.6 節「升級 Identity Reporting」(第 242 頁)。</p>
<input type="checkbox"/>	<p>18. 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 23.1.2 節「啟動驅動程式」(第 210 頁)。</p>
<input type="checkbox"/>	<p>19. (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 26.8 節「將新伺服器新增至驅動程式集」(第 246 頁)。</p>
<input type="checkbox"/>	<p>20. (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 26.9 節「將自訂規則還原至驅動程式」(第 247 頁)。</p>
<input type="checkbox"/>	<p>21. 升級 Analyzer。如需詳細資訊，請參閱第 26.7 節「升級 Analyzer」(第 245 頁)。</p>
<input type="checkbox"/>	<p>22. 啟用升級後的 Identity Manager 解決方案。如需詳細資訊，請參閱第 24 節「啟用 Identity Manager」(第 213 頁)。</p>

## 25.2 瞭解升級程序

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 249 頁)。

## 25.3 支援的升級路徑

Identity Manager 4.7 支援從 4.6.x 和 4.5.6 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 25.3.1 節「從 Identity Manager 4.6.x 版本升級」](#) (第 221 頁)
- ◆ [第 25.3.2 節「從 Identity Manager 4.5.x 版本升級」](#) (第 222 頁)

### 25.3.1 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	<ol style="list-style-type: none"><li>1. 將作業系統升級至支援的版本。</li><li>2. 將 Identity Vault 升級至 9.1。</li><li>3. 將 Identity Manager 引擎升級至 4.7。</li></ol>
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	<ol style="list-style-type: none"><li>1. 安裝 Designer 4.7。</li><li>2. 將工作空間從 NCP 轉換為 LDAP。</li></ol> <p>Designer 4.7 基於 LDAP 執行。使用此版本之前，請參閱《<a href="#">NetIQ Identity Manager LDAP Designer 版本說明</a>》。</p>

元件	基礎版本	升級後的版本
Identity Applications	4.6.x	<p>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。</p> <ol style="list-style-type: none"> <li>1. 將作業系統升級至支援的版本。</li> <li>2. 將資料庫升級至支援的版本。有關受支援的資料庫版本，請參閱第 8.5.3 節「Identity Applications 的系統要求」(第 75 頁)。</li> <li>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。</li> <li>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。</li> <li>5. 將 Identity Applications 升級至 4.7。</li> <li>6. 停止 Tomcat。</li> </ol>
Identity Reporting	4.6.x	<ol style="list-style-type: none"> <li>1. 將作業系統升級至支援的版本。</li> <li>2. 將資料庫升級至支援的版本。如需受支援資料庫版本的詳細資訊，請參閱第 8.6.4 節「Identity Reporting 的系統要求」(第 80 頁)。</li> <li>3. 將 SLM for IGA 升級至支援的版本。</li> <li>4. 更新資料收集服務和受管理服務閘道驅動程式套件。</li> <li>5. 升級 Identity Reporting 4.7。</li> <li>6. (視情況而定) 從 Identity Manager 的「資料收集服務」頁面建立資料同步規則。</li> </ol>

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](#)

## 25.3.2 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	<ol style="list-style-type: none"> <li>1. 將作業系統升級至支援的版本。</li> <li>2. 將 Identity Vault 升級至 9.1。</li> <li>3. 將 Identity Manager 引擎升級至 4.7。</li> </ol>
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	<ol style="list-style-type: none"> <li>1. 安裝 Designer 4.7。</li> <li>2. 將工作空間從 NCP 轉換為 LDAP。</li> </ol> <p>Designer 4.7 基於 LDAP 執行。使用此版本之前，請參閱 <a href="#">《NetIQ Identity Manager LDAP Designer 版本說明》</a>。</p>
Identity Applications	4.5.x (其中 x 為 0 至 5)	<ul style="list-style-type: none"> <li>◆ 如果您使用的是 JBoss 或 Websphere，請移轉至 Tomcat 應用程式伺服器。</li> <li>◆ 套用 4.5.6 修補程式。</li> </ul>	<p>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。</p> <ol style="list-style-type: none"> <li>1. 將作業系統升級至支援的版本。</li> <li>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。</li> <li>3. 將資料庫升級至支援的版本。有關受支援的資料庫版本，請參閱第 8.5.3 節「Identity Applications 的系統要求」(第 75 頁)。</li> <li>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。</li> <li>5. 將 Identity Applications 升級至 4.7。</li> <li>6. 停止 Tomcat。</li> </ol>

元件	基礎版本	中間步驟	升級後的版本
Identity Reporting	4.5.x (其中 x 為 0 至 5)	<ul style="list-style-type: none"> <li>如果您使用的是 JBoss 或 Websphere，請移轉至 Tomcat 應用程式伺服器。</li> <li>套用 4.5.6 修補程式。</li> </ul>	<ol style="list-style-type: none"> <li>將作業系統升級至支援的版本。</li> <li>將資料庫升級至支援的版本。如需受支援資料庫版本的詳細資訊，請參閱第 8.6.4 節「Identity Reporting 的系統要求」(第 80 頁)。</li> <li>將事件稽核服務資料移轉至受支援版本的 PostgreSQL 或 Oracle 資料庫。</li> <li>安裝 SLM for IGA。</li> <li>更新資料收集服務和受管理服務閘道驅動程式套件。</li> <li>將 Identity Reporting 移轉至 4.7。如需詳細資訊，請參閱第 29.8 節「移轉 Identity Reporting」(第 262 頁)。</li> <li>(視情況而定)從 Identity Manager 的「資料收集服務」頁面建立資料同步規則。</li> </ol>

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](#)》

## 25.4 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 25.4.1 節「輸出 Designer 專案」(第 225 頁)
- 第 25.4.2 節「輸出驅動程式的組態」(第 226 頁)



## 25.4.1 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 225 頁)
- ◆ 「從 Identity Vault 建立新專案」(第 225 頁)

### 輸出目前的專案

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

- 1 在 Designer 中開啟您的專案。
- 2 在模型產生器中，請在 Identity Vault 上按一下滑鼠右鍵，然後選取「即時」>「比較」。
- 3 評估專案並調整差異，然後按一下「確定」。

如需詳細資訊，請參閱《[NetIQ Designer for Identity Manager Administration Guide](#)》(NetIQ Designer for Identity Manager 管理指南) 中的「[Using the Compare Feature When Deploying](#)」(在部署時使用比較功能)。

- 4 在工具列上選取「專案」>「輸出」。
- 5 按一下「全選」，以全選所有資源來加以輸出。
- 6 選取專案的儲存位置及儲存格式，然後按一下「完成」。

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

### 從 Identity Vault 建立新專案

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

- 1 安裝 Designer。
- 2 啟動 Designer，然後為工作空間指定位置。
- 3 選取是否要檢查線上更新，然後按一下「確定」。
- 4 在「歡迎」頁上，按一下「執行 Designer」。
- 5 在工具列上，選取「專案」>「輸入專案」>「Identity Vault」。
- 6 指定專案名稱，然後針對專案使用預設位置或選取不同位置。
- 7 按「下一步」。
- 8 指定以下用於連接 Identity Vault 的值：
  - ◆ **主機名稱**：表示 Identity Vault 伺服器的 IP 位址或 DNS 名稱
  - ◆ **使用者名稱**：表示用於向 Identity Vault 驗證的使用者 DN
  - ◆ **密碼**：表示驗證使用者的密碼
- 9 按「下一步」。
- 10 讓 Identity Vault 綱要和「預設通知集合」維持選取狀態。
- 11 展開「預設通知集合」，然後取消選取不需要的語言。

「預設通知集合」會翻譯成多種語言。您可以輸入所有語言或只選取您使用的語言。

- 12 按一下「**瀏覽**」，然後瀏覽至要輸入的驅動程式集並加以選取。
- 13 針對此 Identity Vault 內的每個驅動程式集重複**步驟 12**，然後按一下「**完成**」。
- 14 專案輸入後按一下「**確定**」。
- 15 若您只有一個 Identity Vault，則所有作業已完成。如果您有多個 Identity Vault，請繼續進行**步驟 16**。
- 16 按一下工具列上的「**即時**」>「**輸入**」。
- 17 對其他各個 Identity Vault 重複**步驟 8**到**步驟 14**。

## 25.4.2 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 226 頁)
- ◆ 「使用 iManager 來建立驅動程式的輸出」(第 226 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**。

# 26 升級 Identity Manager 的元件

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

- ◆ 第 26.1 節「升級順序」(第 227 頁)
- ◆ 第 26.2 節「升級 Designer」(第 227 頁)
- ◆ 第 26.3 節「升級 Identity Manager 引擎」(第 228 頁)
- ◆ 第 26.4 節「升級 Identity Manager 驅動程式」(第 232 頁)
- ◆ 第 26.5 節「升級 Identity Applications」(第 233 頁)
- ◆ 第 26.6 節「升級 Identity Reporting」(第 242 頁)
- ◆ 第 26.7 節「升級 Analyzer」(第 245 頁)
- ◆ 第 26.8 節「將新伺服器新增至驅動程式集」(第 246 頁)
- ◆ 第 26.9 節「將自訂規則還原至驅動程式」(第 247 頁)

## 26.1 升級順序

必須依照以下順序來升級 Identity Manager 的各元件：

1. Designer
2. Sentinel Log Management for IGA
3. Identity Vault
4. Identity Manager 引擎
5. 遠端載入器
6. 擴送代理程式
7. iManager
8. Identity Applications (適用於 Advanced Edition)
9. Identity Reporting
10. Analyzer

---

附註：一次只能升級一個元件。

---

## 26.2 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 啟動 Designer 安裝程式。如需詳細資訊，請參閱第 13 章「安裝 Designer」(第 163 頁)。

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)。

## 26.3 升級 Identity Manager 引擎

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

### 26.3.1 升級 Identity Vault

- 1 如第 5.11 節「下載安裝檔案」(第 48 頁) 中所述下載 Identity\_Manager\_4.7\_Linux.iso。
- 2 掛接下載的 .iso。
- 3 從 .iso 檔案的根目錄中，導覽至 IDVault/setup 目錄。
- 4 執行以下指令：  
`./nds-install`
- 5 接受授權合約並繼續安裝。
- 6 指定 **adminDN**。例如，`cn=admin.ou=sa.o=system`。
- 7 當系統提示停止 eDirectory 例項並升級 NICI 時，指定 `y`。
- 8 指定是否要設定增強型背景驗證。

---

**附註：**如果升級 DIB 失敗，並且 `nds-install` 提示執行 `ndsconfig` 升級，請在執行 `nds-install` 後執行該升級指令。如果升級後 eDirectory 服務未啟動，請執行 `ndsconfig` 升級指令。如需詳細資訊，請參閱《[NetIQ eDirectory Installation Guide](#)》(NetIQ eDirectory 安裝指南)。

---

### 26.3.2 升級 Identity Manager 引擎

驗證是否已停止驅動程式。如需詳細資訊，請參閱第 23.1.1 節「停止驅動程式」(第 209 頁)。

在開始升級程序前，請確定快取檔案中沒有事件。當您將 Identity Manager 引擎升級至 4.7 版本時，引擎安裝程式會清理現有 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

執行以下步驟來升級 Identity Manager 引擎：

- 1 從 NetIQ 下載網站下載 Identity\_Manager\_4.7\_Linux.iso。
- 2 掛接下載的 .iso。
- 3 執行以下指令：  
./install.sh
- 4 通讀授權合約。
- 5 輸入 y 以接受授權合約。
- 6 指定是否要升級 Identity Manager 元件。可用選項有 y 和 n。
- 7 選取 Identity Manager 引擎。
- 8 指定以下詳細資料：  
**Identity Vault 管理員**：指定 Identity Vault 管理員名稱。  
**Identity Vault 管理員密碼**：指定 Identity Vault 管理員密碼。

### 26.3.3 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。

- 1 建立遠端載入器組態檔案的備份。
- 2 驗證是否已停止驅動程式。如需指示，請參閱第 23.1.1 節「停止驅動程式」(第 209 頁)。
- 3 停止每一個驅動程式的遠端載入器服務或精靈。
  - ◆ **遠端載入器**：rdxml -config *path\_to\_configfile* -u
  - ◆ **Java 遠端載入器**：dirxml\_jremote -config *path\_to\_configfile* -u
- 4 從 NetIQ 下載網站下載 Identity\_Manager\_4.7\_Linux.iso。
- 5 掛接下載的 .iso。
- 6 執行以下指令：  
./install.sh
- 7 通讀授權合約。
- 8 輸入 y 以接受授權合約。
- 9 指定是否要升級 Identity Manager 元件。可用選項有 y 和 n。
- 10 選取遠端載入器。
- 11 完成安裝後，驗證組態檔案是否包含您的環境資訊。
- 12 (視情況而定) 如果組態檔案有問題，請複製您在步驟 1 中建立的備份檔案。否則，請繼續下一步。
- 13 啟動每一個驅動程式的遠端載入器服務或精靈。
  - ◆ **遠端載入器**：rdxml -config *path\_to\_config\_file*
  - ◆ **Java 遠端載入器**：dirxml\_jremote -config *組態檔案的路徑*

## 26.3.4 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。

在將 iManager 升級至 3.1 之前，請確定您的 eDirectory 版本已升級至 9.1。

升級程序包括以下活動：

- ◆ 「升級 iManager」(第 230 頁)
- ◆ 「更新職能服務」(第 230 頁)
- ◆ 「重新安裝或移轉 Plug-in Studio 的外掛程式」(第 231 頁)
- ◆ 「在升級或重新安裝後更新 iManager 外掛程式」(第 231 頁)

## 升級 iManager

在升級 iManager 之前，請確保電腦符合先決條件和系統要求。

---

**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。

---

- 1 如第 5.11 節「下載安裝檔案」(第 48 頁)中所述下載 `Identity_Manager_4.7_Linux.iso`。
- 2 掛接下載的 `.iso`。
- 3 執行以下指令：  
`./install.sh`
- 4 通讀授權合約。
- 5 輸入 `y` 以接受授權合約。
- 6 指定 iManager 以繼續升級。

## 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。
  - ◆ 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**。

## 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。

## 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。

- 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。



## 26.4 升級 Identity Manager 驅動程式

NetIQ 透過**套件**提供新驅動程式內容。您可以在 Designer 中管理、維護和建立套件。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)。

您可透過以下方式將驅動程式升級至套件：

- 第 26.4.1 節「建立新驅動程式」(第 232 頁)
- 第 26.4.2 節「以套件中的內容取代現有內容」(第 232 頁)
- 第 26.4.3 節「保留目前內容並透過套件新增新內容」(第 233 頁)

### 26.4.1 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。

### 26.4.2 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 25.4.2 節「輸出驅動程式的組態」(第 226 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 26.9 節「將自訂規則還原至驅動程式」(第 247 頁)。



## 26.4.3 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 25.4.2 節「輸出驅動程式的組態」(第 226 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。

## 26.5 升級 Identity Applications

本節提供有關升級 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
- ◆ PostgreSQL 資料庫

升級後，元件會升級至以下版本：

- ◆ Tomcat – 8.5.27
- ◆ ActiveMQ – 5.15.2
- ◆ Java – 1.8.0\_162
- ◆ One SSO Provider – 6.2.1
- ◆ Self-Service Password Reset – 4.2.0.4

本節提供關於以下主題的資訊：

- ◆ [第 26.5.1 節「瞭解升級程式」](#) (第 234 頁)
- ◆ [第 26.5.2 節「升級的先決條件和注意事項」](#) (第 234 頁)
- ◆ [第 26.5.3 節「系統要求」](#) (第 235 頁)
- ◆ [第 26.5.4 節「升級 PostgreSQL 資料庫」](#) (第 235 頁)
- ◆ [第 26.5.5 節「升級 Identity Applications 的驅動程式套件」](#) (第 238 頁)
- ◆ [第 26.5.6 節「升級 Identity Applications」](#) (第 238 頁)
- ◆ [第 26.5.7 節「升級後任務」](#) (第 239 頁)

## 26.5.1 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` 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。

## 26.5.2 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 4.7 的詳細資訊，請參閱[第 25.3 節「支援的升級路徑」](#) (第 221 頁)。

- ◆ **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。確認伺服器具有足夠儲存備份的空間，另外還有可供升級的可用空間。

如果您已將 Identity Applications 安裝在非根分割區的其他分割區中，請確定該分割區具有足夠的空間用來儲存備份組態。另外，請確定 `/tmp` 目錄具有足夠的空間用來儲存記錄和暫存檔案。如果此目錄不能提供所需的空間，請將 `IATEMPDIR` 環境變數設定為分割區上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 `IATEMPDIR` 設定為某個目錄：

1. 開啟終端機並輸入以下指令：

```
export IATEMPDIR=/opt/custom_tmp
```

其中，`/opt/custom_tmp` 是具有足夠可用磁碟空間的目錄路徑。

---

**附註：**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。

如果用於執行 Identity Applications 的應用程式伺服器不是 Tomcat，請在執行升級前將該應用程式伺服器移轉至 Tomcat。如需詳細資訊，請參閱「[從 Websphere 或 JBoss 移轉至 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[第 26.5.4 節「升級 PostgreSQL 資料庫」](#) (第 235 頁)。

- ◆ **Role and Resource Service 驅動程式套件已升級：** 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)。

- ◆ **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，

```
export CATALINA_OPTS="-Dsspr.applicationPath=/home/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. 在頁面右上角的下拉式功能表中按一下**組態管理器**。
3. 按一下 **LocalDB**。
4. 按一下**下載 LocalDB**。

## 26.5.3 系統要求

升級程序會為所安裝元件的目前組態建立備份。確認伺服器具有足夠儲存備份的空間，另外還有可供升級的可用空間。

## 26.5.4 升級 PostgreSQL 資料庫

需要執行以下升級前步驟以升級 PostgreSQL 資料庫。

- 1 停止 PostgreSQL 服務。

```
su -s /bin/sh - postgres -c "/opt/netiq/idm/apps/postgres/bin/pg_ctl stop -w -D /opt/netiq/idm/apps/postgres/data"
```

- 2 停用 PostgreSQL 服務的現有單位檔案。

```
systemctl disable postgresql-9.6.service
```

- 3 清理 PostgreSQL 服務的現有單位檔案。

```
rm /usr/lib/systemd/system/postgresql-9.6.service
```

```
systemctl daemon-reload
```

```
systemctl reset-failed
```

- 4 建立備份目錄並備份現有 PostgreSQL 目錄。

例如：

```
mkdir -p /home/backup
```

```
cp -rvf /opt/netiq/idm/apps/postgres/ /home/backup/
```

- 5 導覽至掛接 Identity\_Manager\_4.7\_Linux.iso 的位置。

- 6 導覽至 /common/packages/postgres/ 目錄。

- 7 安裝新版 PostgreSQL。

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

---

**附註：** PostgreSQL 主目錄會從先前安裝的自訂位置變更為 /opt/netiq/idm/postgres/。

---

- 8** 在 PostgreSQL 安裝位置中建立 data 目錄。

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

例如：

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

- 9** 變更新安裝 PostgreSQL 目錄的許可權。

```
chown -R postgres:postgres <postgres directory path>
```

例如：

```
chown -R postgres:postgres /opt/netiq/idm/postgres
```

- 10** 建立 postgres 使用者主目錄。

例如，`mkdir -p /home/users/postgres`

- 11** 變更新建立 PostgreSQL 使用者主目錄的許可權。

```
chown -R postgres:postgres <postgres home directory path>
```

例如：

```
chown -R postgres:postgres /home/users/postgres
```

- 12** 輸出 PostgreSQL home 目錄

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

例如：

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

- 13** 輸出 PostgreSQL 密碼：

```
export PGPASSWORD=<輸入資料庫密碼>
```

- 14** 啟始化資料庫。

```
su -s /bin/sh - postgres -c "LANG=en_US.UTF-8 <POSTGRES_HOME>/bin/initdb -D  
<POSTGRES_HOME>/data"
```

例如：

```
su -s /bin/sh - postgres -c "LANG=en_US.UTF-8 /opt/netiq/idm/postgres/bin/initdb -D /opt/netiq/idm/  
postgres/data"
```

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

**15a** 導覽至 /etc/ 目錄。

**15b** 編輯 passwd 檔案。

```
vi /etc/passwd
```

**15c** 將 postgres 使用者的主目錄變更為 /opt/netiq/idm/postgres/。

- 16** 導覽至 /opt/netiq/idm/postgres/ 目錄。

- 17** 以 postgres 使用者身分登入。

例如：

```
su postgres
```

- 18** 移轉現有資料。

例如：

```
/opt/netiq/idm/postgres/bin/pg_upgrade --old-datadir /opt/netiq/idm/apps/postgres/data/ --new-datadir /opt/netiq/idm/postgres/data/ --old-bindir /opt/netiq/idm/apps/postgres/bin --new-bindir /opt/netiq/idm/postgres/bin/
```

- 19 以 postgres 使用者身分登出。
- 20 更新 pg\_hba.conf 檔案以信任伺服器網路：
  - 20a 導覽至 /opt/netiq/idm/postgres/data/ 目錄。
  - 20b 編輯 pg\_hba.conf 檔案：

```
vi pg_hba.conf
```
  - 20c 在 pg\_hba.conf 檔案中新增下行：

```
host all all 0.0.0.0/0 trust
```
- 21 為了確保 PostgreSQL 例項會監聽 localhost 以外的其他網路例項，請更新組態檔案：
  - 21a 導覽至 /opt/netiq/idm/postgres/data/ 目錄。
  - 21b 編輯 postgresql.conf 檔案：

```
vi postgresql.conf
```
  - 21c 在 postgresql.conf 檔案中新增下行：

```
listen_addresses = '**
```

---

**附註：**若要監聽受限的網路介面，請指定以逗號分隔的 IP 位址清單。

---

- 22 在 <postgres home directory path>/data 下建立 pg\_log 目錄。  
例如：

```
mkdir -p /opt/netiq/idm/postgres/data/pg_log
```
- 23 變更 pg\_log 目錄的許可權。  

```
chown -R postgres:postgres <postgres directory path>/data/pg_log
```

  
例如：

```
chown -R postgres:postgres /opt/netiq/idm/postgres/data/pg_log
```
- 24 啟動 PostgreSQL 服務。  

```
systemctl start netiq-postgresql
```

  
此指令將啟動新的 PostgreSQL 服務。
- 25 (選擇性) 從圖形使用者介面啟動新 pgAdmin：
  - 25a 將 scripts 目錄從舊的 postgres 主目錄複製到新的 postgres 主目錄。  
例如：

```
cp -rvf /opt/netiq/idm/apps/postgres/scripts /opt/netiq/idm/postgres
```
  - 25b 導覽至 /opt/netiq/idm/postgres/scripts 目錄。
  - 25c 編輯 launchpgadmin.sh，以新的 PostgreSQL 路徑取代舊路徑。  
以 /opt/netiq/idm/postgres 取代 /opt/netiq/idm/apps/postgres/。
  - 25d 導覽至 /usr/share/application 目錄，然後編輯 .desktop 應用程式以提供 launchpgadmin.sh 的新路徑。  
**SLES：**編輯 pg-pgadmin-9\_6.desktop 應用程式，以新的 launchpgadmin.sh 路徑取代 EXEC 值  
例如：

將 "Exec=/opt/netiq/idm/apps/postgres/scripts/launchpgadmin.sh" 的值變更為 : "Exec=/opt/netiq/idm/postgres/scripts/launchpgadmin.sh"

**RHEL**：導覽至 /usr/share/application，然後建立包含以下詳細資料的 pg-pgadmin-9\_6.desktop 檔案：

例如：

```
[Desktop Entry]
Version=1.0
Encoding=UTF-8
Name=pgAdmin 4
Exec=/opt/netiq/idm/postgres/scripts/launchpgadmin.sh
Icon=pg-pgadmin-9_6.png
Terminal=false
Type=Application
```

**25e** 從系統中移除舊的 postgres 主目錄。

```
rm -rf /opt/netiq/idm/apps/postgres/
```

**25f** 為使變更生效，請重新啟動您的系統。

## 26.5.5 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 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。

---

## 26.5.6 升級 Identity Applications

---

**附註：**如果 Identity Applications 和 SSPR 安裝在不同的伺服器上，您需要手動升級 SSPR。如需詳細資訊，請參閱「[升級 SSPR](#)」(第 239 頁)。

---

- ◆ 「[升級 Identity Applications](#)」(第 239 頁)
- ◆ 「[升級 SSPR](#)」(第 239 頁)

## 升級 Identity Applications

下面的程序介紹如何升級 Identity Applications。

- 1 從 NetIQ 下載網站下載 Identity\_Manager\_4.7\_Linux.iso。
- 2 掛接下載的 .iso。
- 3 執行以下指令：  
./install.sh
- 4 通讀授權合約。
- 5 輸入 y 以接受授權合約。
- 6 指定是否要升級 Identity Manager 元件。可用選項有 y 和 n。
- 7 選取 Identity Applications 以繼續升級。
- 8 指定以下詳細資料：  
**SSPR 安裝資料夾**：指定 SSPR 安裝資料夾。  
**使用者應用程式資料夾**：指定使用者應用程式資料夾。  
**Identity Applications One SSO 服務密碼**：指定 One SSO 密碼。  
**Identity Applications 資料庫 JDBC jar 檔案**：指定資料庫 JAR 檔案。現有資料庫 jar 檔案的預設位置為 /opt/netiq/idm/apps/postgres/postgresql-9.4.1212.jar。  
**建立 Identity Applications 的綱要**：指定要在何時建立資料庫綱要。可用選項有現在、啟動和檔案。

## 升級 SSPR

---

**附註：**如果 SSPR 安裝在與 Identity Applications 和 OSP 伺服器不同的伺服器上，則必須單獨升級 SSPR。

---

- 1 如第 5.11 節「下載安裝檔案」(第 48 頁)中所述下載 Identity\_Manager\_4.7\_Linux.iso。
- 2 掛接下載的 .iso。
- 3 從 .iso 檔案的根目錄中，導覽至 SSPR 目錄。
- 4 執行以下指令：  
./install.sh
- 5 通讀授權合約。
- 6 輸入 y 以接受授權合約。

### 26.5.7 升級後任務

- ◆ 驗證 configupdate 公用程式中的 **RBPM 至 eDirectory SAML** 組態參數是否設定為自動。
  1. 啟動 configupdate 公用程式。
  2. 導覽至 **SSO 用戶端 > RBPM**，並將 **RBPM 至 eDirectory SAML** 組態設定為自動。
  3. 儲存變更。
  4. 啟動 Tomcat。

- ◆ 變更 OSP 目錄的許可權和擁有權：  
`chmod +x novlua:novlua /opt/netiq/idm/apps/osp`
- ◆ 手動刪除先前版本的 Tomcat 和 ActiveMQ 服務。  
`/etc/init.d/idmapps_tomcat_init`  
`/etc/init.d/idmapps_activemq_init`

您還必須手動還原 Tomcat、SSPR、OSP 或 Identity Applications 的自訂設定。

- ◆ 「Java」(第 240 頁)
- ◆ 「Tomcat」(第 240 頁)
- ◆ 「Identity Applications」(第 241 頁)
- ◆ 「One SSO Provider」(第 242 頁)
- ◆ 「Kerberos」(第 242 頁)

## Java

驗證升級後的 JRE 位置 (`jre/lib/security/cacerts`) 是否包含較舊 JRE 位置中的所有證書。如果某個證書遺失，請手動將該證書輸入到升級後的 JRE 的 `cacerts` 中。

- 1 使用 `keytool` 指令輸入 `java cacerts`：

```
keytool -import -trustcacerts -file Certificate_Path -alias ALIAS_NAME -keystore cacerts
```

---

**附註：**升級後，JRE 儲存在 Identity Applications 安裝位置。例如：`/opt/netiq/idm/apps/jre`。

---

- 2 驗證 JRE 主目錄位置。

```
tomcat/bin/setenv.sh
```

- 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：

- ◆ 還源自訂的 `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](#)。

驗證新的 `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 `/opt/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** (位於 `/opt/novell/eDirectory/lib64/nds-modules/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 <keyalias> -srckeystore <backup cacert> -srcstorepass
changeit -destkeystore /opt/novell/eDirectory/lib64/nds-modules/jre/lib/security/cacerts
-deststorepass changeit
```

- 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。

如果您在執行升級程式前已將自訂網路位置資料夾重新命名為 **IDMProv**，則應使用 `configupdate` 公用程式將該網路位置資料夾名稱變更為原來的網路位置名稱。例如，原來的自訂網路位置名稱為 **IDMDev**，現在它被重新命名為 **IDMProv**。

請完成以下步驟將網路位置名稱改回為原來的網路位置名稱：

- 1 導覽至使用者應用程式目錄 (位於 `/opt/netiq/idm/apps/UserApplication` 中)。
- 2 (選擇性) 若要以圖形使用者介面模式啟動 `configupdate` 公用程式，請確定 `configupdate.sh.properties` 檔案中的 `use_console` 選項設定為 `false`。  
需要執行此步驟的原因是，升級公用程式會將此選項的值變更為 `true`。  
或者，在 **Linux** 上啟動 `configupdate` 公用程式，並傳遞額外的指令行引數。

```
./configupdate.sh use_console=false
```

- 3 啟動 `configupdate` 公用程式。  
`configupdate.sh`
- 4 在使用者應用程式索引標籤中按一下 **進階選項**，然後執行以下步驟：
  - 4a 核取變更 **RBPM** 網路位置名稱核取方塊。
  - 4b 將 **RBPM** 網路位置名稱變更為原來的網路位置名稱。
  - 4c 瀏覽並選取相應的角色驅動程式 **DN**，然後按一下 **確定**。
  - 4d 使用以下指令變更 **WAR** 檔案的許可權和擁有權。

```
chmod 755 <Original_Context_Name>.war; chown -R novlua:novlua <Original_Context_Name>.war
```

例如，如果原來的自訂網路位置名稱為 IDMDev：

```
chmod 755 IDMDev.war; chown -R novlua:novlua IDMDev.war
```

5 (視情況而定) 如果您已完成所有升級後任務，則請啟動 Identity Applications 的 Tomcat 服務。

## One SSO Provider

如果 OSP 和使用者應用程式部署在不同的伺服器上，請使用組態更新公用程式更新 SSO 用戶端參數。如需詳細資訊，請參閱第 11.6.5 節「SSO 用戶端參數」(第 141 頁)中的「IDM 儀表板」(第 141 頁)。

位於 /etc/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。

## 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。

## 26.6 升級 Identity Reporting

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

---

附註：確定資料庫已升級至支援的版本。

---

1. 將資料庫升級至支援的版本。如需升級 PostgreSQL 資料庫的資訊，請參閱第 26.5.4 節「升級 PostgreSQL 資料庫」(第 235 頁)。
2. 升級驅動程式套件。如需詳細資訊，請參閱第 26.6.2 節「升級 Identity Reporting 的驅動程式套件」(第 243 頁)。
3. 升級 / 移轉至 Sentinel Log Management for IGA。

如果您要從 Identity Reporting 4.6.x 升級，請將 Sentinel Log Management for IGA 升級至 4.7 版本。如需詳細資訊，請參閱第 26.6.3 節「升級 Sentinel Log Management for IGA」(第 243 頁)。

如果您要從 Identity Reporting 4.5.x 移轉，請從 EAS 移轉至 Sentinel Log Management for IGA。如需詳細資訊，請參閱第 29.8.1 節「從事件稽核服務移轉至 Sentinel Log Management for IGA」(第 262 頁)。

4. 升級 Identity Reporting。如需詳細資訊，請參閱第 26.6.5 節「升級 Identity Reporting」(第 244 頁)。

## 26.6.1 升級的先決條件和注意事項

執行升級前，請注意以下事項：

- ◆ 在升級期間，請務必指定 `postgresql-9.4.1212.jar` 檔案的正確位置。預設位置為 `/opt/netiq/idm/postgres/`。在下列情況下，資料庫連接將失敗：
  - ◆ 如果提供的路徑不正確
  - ◆ 如果提供的 `jar` 檔案不正確
  - ◆ 如果啟用了防火牆
  - ◆ 如果資料庫不接受來自遠端機器的連接
- ◆ 如果您的資料庫設定在 **SSL** 上，請從 `server.xml` 檔案的 `PATH` 中移除 `ssl=true`，該檔案位於以下位置：

```
/opt/netiq/idm/apps/tomcat/conf/
```

例如，將

```
jdbc:postgresql://<postgres db>:5432/idmuserappdb?ssl=true
```

變更為

```
jdbc:postgresql://<postgres db>:5432/idmuserappdb
```

## 26.6.2 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。
- 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 重複相同程序，以升級資料收集服務驅動程式的套件。

---

**附註：**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**。

---

## 26.6.3 升級 Sentinel Log Management for IGA

- 1 從 NetIQ 下載網站下載 `SentinelLogManagementForIGA8.1.1.0.tar.gz`。
  - 2 導覽至要擷取檔案的目錄。
  - 3 執行以下指令來擷取檔案
- ```
tar -zxvf SentinelLogManagementForIGA8.1.1.0.tar.gz
```

- 4 導覽至 SentinelLogManagementforIGA 目錄。
- 5 若要安裝 SLM for IGA，請執行以下指令：  
`./install.sh`
- 6 指定要用於安裝的語言，然後按 Enter。
- 7 輸入 y 以接受授權合約。

---

**附註：**升級 SLM for IGA 後，您需要手動輸入最新的收集器。

1. 導覽至 NetIQ 下載網站。
  2. 下載 SentinelLogManagementForIGA8.1.1.0.tar.gz 檔案。
  3. 擷取檔案並導覽至 /content/ 目錄。
  4. 輸入 Identity Manager 收集器。
- 

## 26.6.4 升級作業系統

將作業系統從 SLES 11 升級至 SLES 12 時，作業系統的升級程序會刪除一些 SLM for IGA RPM。

以下指令可確保 SLM for IGA 在您升級作業系統後能正常運作。

---

**附註：**升級作業系統前，必須先升級 SLM for IGA。

---

請使用下列步驟升級作業系統：

- 1 導覽至擷取 Sentinel 安裝檔案的目錄。
- 2 停止 Sentinel 服務：  
`rcsentinel stop`
- 3 執行以下指令：  
`./install.sh --preosupgrade`
- 4 升級作業系統。
- 5 執行以下指令：  
`./install.sh --postosupgrade`
- 6 重新啟動 Sentinel 服務：  
`rcsentinel restart`

## 26.6.5 升級 Identity Reporting

- 1 從 NetIQ 下載網站下載 Identity\_Manager\_4.7\_Linux.iso。
- 2 掛接下載的 .iso。
- 3 執行以下指令：  
`./install.sh`
- 4 通讀授權合約。
- 5 輸入 y 以接受授權合約。

- 6 指定是否要升級 Identity Manager 元件。可用選項有 **y** 和 **n**。
- 7 選取 Identity Reporting 以繼續升級。
- 8 指定以下詳細資料：
  - 已安裝 OSP**：指定是否已安裝 OSP。
  - 用於備份的 Reporting 安裝資料夾**：指定 Reporting 安裝資料夾。
  - 建立 Identity Reporting 的綱要**：指定要在何時建立資料庫綱要。
  - Identity Reporting 資料庫 JDBC jar 檔案**：指定 Identity Reporting 的資料庫 JAR 檔案。現有資料庫 jar 檔案的預設位置為 /opt/netiq/idm/apps/postgres/postgresql-9.4.1212.jar。
  - Identity Reporting 資料庫使用者**：指定 Reporting 資料庫使用者的名稱。
  - Identity Reporting 資料庫帳戶密碼**：指定 Reporting 資料庫密碼。

## 26.6.6 Reporting 的升級後步驟

---

**附註：**執行升級後，Identity Manager 4.6.1 將報告不能正常運作。您只能使用 Identity Manager 4.7 報告。

---

如果在升級期間為資料庫綱要建立選取了啟動或檔案，請務必執行以下操作：

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

## 26.6.7 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。

## 26.7 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 Identity\_Manager\_4.7\_Linux\_Analyzer.tar.gz。
- 2 將該 .zip 檔案擷取到包含 Analyzer 安裝檔案 (例如外掛程式、解除安裝程序檔和其他 Analyzer 檔案) 的目錄。
- 3 重新啟動 Analyzer。

4 若要驗證您是否已成功套用新的修補程式，請完成以下步驟：

4a 啟動 Analyzer。

4b 按一下說明 > 關於 Analyzer。


4c 檢查程式顯示的是否為新版本。

## 26.8 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。

### 26.8.1 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 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」。

### 26.8.2 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 246 頁)
- 「使用 iManager 從驅動程式集移除舊的伺服器」(第 247 頁)
- 「解除舊伺服器」(第 247 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。


## 26.9 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 26.9.1 節「使用 Designer 將自訂規則還原至驅動程式」](#) (第 247 頁)
- [第 26.9.2 節「使用 iManager 將自訂規則還原至驅動程式」](#) (第 248 頁)

### 26.9.1 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 23.1.2 節「啟動驅動程式」(第 210 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。

## 26.9.2 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 23.1.2 節「啟動驅動程式」(第 210 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。



# 27 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 Identity Vault dib 目錄。  
`/var/opt/novell/eDirectory/data/dib`
  - 2b 建立一個新檔案，將其命名為 `.idme`，並在其中新增 2(數值)。
  - 2c 重新啟動 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 `/opt/netiq/idm/apps/tomcat/webapps` 目錄中移除以下 WAR 檔案和 Webapps 資料夾：
  - ◆ IDMPProv\*
  - ◆ 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.sh`，然後指定以下參數的值：

「報告」索引標籤：指定以下區段中的設定：

  - ◆ ID Vault
  - ◆ Identity Vault 使用者身分
  - ◆ 報告管理員
    - ◆ 報告管理員角色容器 DN。例如，`ou=sa,o=data`
    - ◆ 報告管理員。例如，`cn=uaadmin,ou=sa,o=data`

「驗證」索引標籤：指定以下區段中的設定：

- ◆ 驗證伺服器
  - ◆ **OAuth** 伺服器主機識別碼。例如，驗證伺服器的 IP 位址或 DNS 名稱 ( 如 192.168.0.1 )
  - ◆ **OAuth** 伺服器 TCP 連接埠
  - ◆ **OAuth** 伺服器正在使用 TLS/SSL
- ◆ 驗證組態
  - ◆ **OAuth** 金鑰儲存區檔案。例如， /opt/netiq/idm/apps/osp/osp.jks
  - ◆ **OAuth** 使用之金鑰的金鑰別名
  - ◆ **OAuth** 所用金鑰的金鑰密碼
  - ◆ 工作階段逾時 ( 分鐘 )。例如， 60 分鐘。

「SSO 用戶端」索引標籤：指定以下區段中的設定：

- ◆ 報告
  - ◆ 抵達頁面的 **URL** 連結。例如， http://192.168.0.1:8180/IDMRPT
- ◆ Self Service Password Reset
  - ◆ **OAuth** 用戶端 ID。例如， *sspr*
  - ◆ **OAuth** 用戶端機密。例如， <*sspr* 用戶端機密 >
  - ◆ **OSP OAuth** 重新導向 **URL**。例如， http://192.168.0.1:8180/sspr/public/oauth

如需組態公用程式的詳細資訊，請參閱「執行 **Identity Applications** 組態公用程式」 ( 第 126 頁 )。

10 儲存變更並結束組態公用程式。

11 啟動 Tomcat。



# 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 217 頁)。如需升級與移轉之間差異的詳細資訊，請參閱第 25.2 節「瞭解升級程序」(第 220 頁)。



# 28

## 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。

### 28.1 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                                                                                                         |
|--------------------------|----------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | 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 25.2 節「瞭解升級程序」(第 220 頁)。                                                       |
| <input type="checkbox"/> | 2. 確保您已取得用於移轉 Identity Manager 資料的最新安裝套件。                                                                      |
| <input type="checkbox"/> | 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 15 頁)。                                                  |
| <input type="checkbox"/> | 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 5.9 節「準備安裝」(第 42 頁)和您要升級至的版本的《版本說明》。                   |
| <input type="checkbox"/> | 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 26.3.1 節「升級 Identity Vault」(第 228 頁)。                  |
| <input type="checkbox"/> | 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 29.4 節「將 Identity Manager 引擎移轉至新伺服器」(第 258 頁)。 |
| <input type="checkbox"/> | 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 31 頁)。                                        |
| <input type="checkbox"/> | 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 26.3.3 節「升級遠端載入器」(第 229 頁)。                |
| <input type="checkbox"/> | 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 29.1 節「Identity Manager 的移轉核對清單」(第 255 頁)。             |
| <input type="checkbox"/> | 10. 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 29.3.1 節「在 Designer 中複製伺服器特定資訊」(第 257 頁)。                                     |
| <input type="checkbox"/> | 11. (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 29.3 節「複製驅動程式集的伺服器特定資訊」(第 256 頁)。            |
| <input type="checkbox"/> | 12. 將驅動程式更新為套件格式。如需詳細資訊，請參閱第 26.4 節「升級 Identity Manager 驅動程式」(第 232 頁)。                                        |
| <input type="checkbox"/> | 13. (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 26.9 節「將自訂規則還原至驅動程式」(第 247 頁)。                                    |

|                          | 核對清單項目                                                                                 |
|--------------------------|----------------------------------------------------------------------------------------|
| <input type="checkbox"/> | 14. 安裝 Identity Reporting 和關聯的驅動程式。如需詳細資訊，請參閱第 29.8 節「移轉 Identity Reporting」(第 262 頁)。 |
| <input type="checkbox"/> | 15. 從驅動程式集移除舊的伺服器。如需詳細資訊，請參閱第 26.8.2 節「從驅動程式集移除舊的伺服器」(第 246 頁)。                        |
| <input type="checkbox"/> | 16. 啟用升級後的 Identity Manager 解決方案。如需詳細資訊，請參閱第 24 節「啟用 Identity Manager」(第 213 頁)。       |

## 28.2 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 23.1.1 節「停止驅動程式」(第 209 頁)
- ◆ 第 23.1.2 節「啟動驅動程式」(第 210 頁)

# 29

## 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 29.1 節「Identity Manager 的移轉核對清單」(第 255 頁)
- 第 29.2 節「準備用於移轉的 Designer 專案」(第 256 頁)
- 第 29.3 節「複製驅動程式集的伺服器特定資訊」(第 256 頁)
- 第 29.4 節「將 Identity Manager 引擎移轉至新伺服器」(第 258 頁)
- 第 29.5 節「移轉使用者應用程式驅動程式」(第 258 頁)
- 第 29.6 節「升級 Identity Applications」(第 259 頁)
- 第 29.7 節「完成 Identity Applications 的移轉」(第 260 頁)
- 第 29.8 節「移轉 Identity Reporting」(第 262 頁)

### 29.1 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                                                                                                                                                                                                                                                                     |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | 1. 備份 Identity Manager 解決方案的目錄和資料庫。                                                                                                                                                                                                                                        |
| <input type="checkbox"/> | 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 5.7.4 節「建議的伺服器設定」(第 39 頁)和元件的最新《版本說明》。<br><br><b>附註：</b> 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 <b>現有資料庫</b> 。如需詳細資訊，請參閱第 9 章「安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting」(第 83 頁)。 |
| <input type="checkbox"/> | 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。                                                                                                                                                                                                             |
| <input type="checkbox"/> | 4. 將現有的使用者應用程式驅動程式輸入到 Designer 中。                                                                                                                                                                                                                                          |
| <input type="checkbox"/> | 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 29.2 節「準備用於移轉的 Designer 專案」(第 256 頁)。                                                                                                                                                                                         |
| <input type="checkbox"/> | 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 29.4 節「將 Identity Manager 引擎移轉至新伺服器」(第 258 頁)。                                                                                                                                          |
| <input type="checkbox"/> | 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。                                                                                                                                                                                                               |
| <input type="checkbox"/> | 8. 移轉使用者應用程式驅動程式。如需詳細資訊，請參閱第 29.5 節「移轉使用者應用程式驅動程式」(第 258 頁)。                                                                                                                                                                                                               |

|                          | 核對清單項目                                                                                                              |
|--------------------------|---------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | 9. 升級 Identity Applications。如需詳細資訊，請參閱第 26.5 節「升級 Identity Applications」(第 233 頁)。                                  |
| <input type="checkbox"/> | 10. (視情況而定) 若要使用安裝程序建立的 SQL 檔案來升級 Oracle 資料庫，請準備好 Oracle 環境。如需詳細資訊，請參閱第 29.7.1 節「準備 Oracle 資料庫以執行 SQL 檔案」(第 260 頁)。 |
| <input type="checkbox"/> | 11. 確保您的瀏覽器不包含先前版本 Identity Manager 的內容。如需詳細資訊，請參閱第 29.7.2 節「衝洗瀏覽器快取」(第 261 頁)。                                     |
| <input type="checkbox"/> | 12. (視情況而定) 恢復 SharedPagePortlet 的自訂設定。如需詳細資訊，請參閱第 29.7.3 節「更新 SharedPagePortlet 的最大逾時設定」(第 261 頁)。                 |
| <input type="checkbox"/> | 13. 確保在使用者未提供過濾參數時，搜尋群組選項不會顯示任何資訊。如需詳細資訊，請參閱第 29.7.4 節「停用群組的自動查詢設定」(第 261 頁)。                                       |

## 29.2 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。

## 29.3 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 29.3.1 節「在 Designer 中複製伺服器特定資訊」](#) (第 257 頁)
- ◆ [第 29.3.2 節「在 iManager 中變更伺服器特定資訊」](#) (第 257 頁)
- ◆ [第 29.3.3 節「變更使用者應用程式的伺服器特定資訊」](#) (第 258 頁)

## 29.3.1 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 23.1.2 節「啟動驅動程式」](#) (第 210 頁)。

## 29.3.2 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。

### 29.3.3 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.sh`。

- 1 導覽至預設位於使用者應用程式安裝子目錄中的組態更新公用程式。
- 2 在指令提示符處，啟動組態更新公用程式：  
`configupdate.sh`
- 3 依照第 11.6 章「完成 Identity Applications 的設定」（第 126 頁）所述指定值。

## 29.4 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 9 章「安裝 Identity Manager 引擎、Identity Applications 和 Identity Reporting」（第 83 頁）。

## 29.5 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。

### 29.5.1 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」。

## 29.5.2 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。

## 29.5.3 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。

## 29.6 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。

- ◆ (視情況而定) 如果現有資料庫在 **Oracle** 上執行，並且您要指示安裝程式撰寫一個 **SQL** 檔案來更新綱要，則必須執行額外的步驟。如需詳細資訊，請參閱第 29.7.1 節「準備 **Oracle** 資料庫以執行 **SQL** 檔案」(第 260 頁)。
- ◆ 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。

如需升級 **Identity Applications** 的詳細資訊，請參閱第 26.5 節「升級 **Identity Applications**」(第 233 頁)。

## 29.7 完成 **Identity Applications** 的移轉

在升級或移轉 **Identity Applications** 後，請完成移轉程序。

### 29.7.1 準備 **Oracle** 資料庫以執行 **SQL** 檔案

在安裝期間，您可能選擇了撰寫一個 **SQL** 檔案來更新 **Identity Applications** 資料庫。如果資料庫在 **Oracle** 平台上執行，則您必須先執行一些步驟才能執行該 **SQL** 檔案。

- 1 在資料庫中執行以下 **SQL** 陳述式：

```
ALTER TABLE DATABASECHANGELOG ADD ORDEREXECUTED INT;
UPDATE DATABASECHANGELOG SET ORDEREXECUTED = -1;
ALTER TABLE DATABASECHANGELOG MODIFY ORDEREXECUTED INT NOT NULL;
ALTER TABLE DATABASECHANGELOG ADD EXECTYPE VARCHAR(10);
UPDATE DATABASECHANGELOG SET EXECTYPE = 'EXECUTED';
ALTER TABLE DATABASECHANGELOG MODIFY EXECTYPE VARCHAR(10) NOT NULL;
```

- 2 執行以下 **updateSQL** 指令：

```
/opt/novell/idm/jre/bin/java -Xms256m -Xmx256m -Dwar.context.name=IDMProv
-jar /opt/novell/idm/liquibase.jar
--databaseClass=com.novell.soa.persist.liquibase.OracleUnicodeDatabase
--driver=oracle.jdbc.driver.OracleDriver
--classpath=/root/ojdbc8.jar:/opt/novell/idm/tomcat/server/IDMProv/deploy/IDMProv.war
--changeLogFile=DatabaseChangeLog.xml
--url="jdbcURL" --logLevel=debug
--logFile=/opt/novell/idm/db.out --contexts="prov,updatedb" --username=xxxx
--password=xxxx updateSQL > /opt/novell/idm/db.sql
```

- 3 在文字編輯器中，開啟預設位於 / 安裝路徑 / userapp / sql 目錄中的 **SQL** 檔案。
- 4 在函數 **CONCAT\_BLOB** 的定義後面插入一個反斜線 (/)。例如

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

/
```

5 執行 SQL 檔案。

---

**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。

---

## 29.7.2 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。

## 29.7.3 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」。

## 29.7.4 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：



## 29.8 移轉 Identity Reporting

移轉先前版本的 Identity Manager 涉及到移轉 Identity Reporting。請務必注意以下事項：

- ◆ 手動將事件稽核服務資料移轉至 PostgreSQL 資料庫。
- ◆ 清理現有 Reporting 安裝。
- ◆ 在新伺服器上執行 Identity Reporting 4.7 的全新安裝。
- ◆ 為新安裝的 Identity Reporting 指定現有驗證服務和 Identity Vault 的安裝位置。

### 29.8.1 從事件稽核服務移轉至 Sentinel Log Management for IGA

本節提供有關將 EAS 資料庫中的 SIEM 資料移轉至受支援 PostgreSQL 資料庫的資訊。

您必須建立必要的角色和表空間，以確保移轉期間不會出現故障。

#### 準備新 PostgreSQL 資料庫

- 1 停止 EAS 以確保不會有任何事件傳送到 EAS 伺服器。
- 2 使用 iManager 停止 DCS 驅動程式：
  - 2a 登入 iManager。
  - 2b 停止 DCS 驅動程式。

**2c** 編輯驅動程式內容，以將啟動選項設定為手動。

此步驟可確保驅動程式不會自動啟動。

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

此步驟可確保移轉期間不會出現故障。

**3a** 執行以下指令以建立必要角色：

```
CREATE ROLE esec_app
    NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE esec_user
    NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

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

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

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

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

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

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

**3b** 執行以下指令以建立表空間：

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

例如，

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

**3c** 執行以下指令以建立 **SIEM** 資料庫：

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



## 輸出 EAS 中的資料

- 1 停止 EAS 以確保不會有任何事件傳送到 EAS 伺服器。
- 2 使用 iManager 停止 DCS 驅動程式：
  - 2a 登入 iManager。
  - 2b 停止 DCS 驅動程式。
  - 2c 編輯驅動程式內容，以將啟動選項設定為**手動**。  
此步驟可確保驅動程式不會自動啟動。
- 3 將 EAS 資料庫中的資料輸出到檔案：
  - 3a 登入 EAS 使用者帳戶：  
`# su - novleas`
  - 3b 指定 EAS 使用者具有完全存取權的位置，例如 `/home/novleas`。
  - 3c 導覽至 PostgreSQL 安裝目錄並執行以下指令：  
例如，  
`export PATH=/opt/novell/sentinel_eas/3rdparty/postgresql/bin/:$PATH`  
`export LD_LIBRARY_PATH=/opt/novell/sentinel_eas/3rdparty/postgresql/lib/:$LD_LIBRARY_PATH`
  - 3d 使用以下指令將資料輸出到 .sql 檔案：  
`./pg_dump -p < 連接埠號碼 > -U < 使用者名稱 > -d < 資料庫名稱 > -f < 輸出位置 >`  
例如，  
`./pg_dump -p 15432 -U dbauser SIEM -f /home/novleas/SIEM.sql`

## 將資料輸入到新 PostgreSQL 資料庫中

- 1 停止 EAS 以確保不會有任何事件傳送到 EAS 伺服器。
- 2 使用 iManager 停止 DCS 驅動程式：
  - 2a 登入 iManager。
  - 2b 停止 DCS 驅動程式。
  - 2c 編輯驅動程式內容，以將啟動選項設定為**手動**。  
此步驟可確保驅動程式不會自動啟動。
- 3 將資料輸入到新的 PostgreSQL 資料庫：
  - 3a (視情況而定) 建立一個 postgres 使用者。  
此步驟僅針對 Windows。Linux 上會自動建立使用者。
  - 3b 將**步驟 3d** 中輸出的檔案複製到該 postgres 使用者具有完全存取權的位置。例如，`/opt/netiq/idm/postgres`
  - 3c 執行以下指令以將資料輸入到 PostgreSQL 資料庫。  
`psql -d < 資料庫名稱 > -U < 使用者名稱 > -f < 輸出檔案所在位置的完整路徑 >`  
例如，  
`psql -d SIEM -U postgres -f /opt/netiq/idm/apps/postgres/SIEM.sql`
- 4 檢查有無任何移轉記錄錯誤，如有則予以解決。



---

附註：Identity Manager 4.7 報告將不使用從 EAS 移轉至 SLM for IGA 的稽核資料，而是使用直接從 SLM for IGA 同步的稽核資料。

---

## 29.8.2 設定新 Reporting 伺服器

將 EAS 資料輸入到新 PostgreSQL 資料庫後，在另一部伺服器上安裝新 Reporting 應用程式，並讓它指向 Identity Vault 和現有驗證服務。

- 1 停止執行現有 Reporting 應用程式的現有 Tomcat 服務。
- 2 在 Tomcat 安裝路徑外部，為 /opt/netiq/idm/apps/ 下 tomcat/webapps 目錄和 Reporting 主目錄中的現有 Identity Reporting WAR 檔案建立備份
- 3 從現有 server.xml 檔案中移除 EAS 項目。
- 4 在移轉 EAS 資料的同一個 PostgreSQL 資料庫中建立新資料庫。
- 5 在新伺服器上安裝和設定 Identity Reporting，並讓它指向現有的單一登入服務和 Identity Vault。如需詳細資訊，請參閱第 10 章「設定安裝的元件」(第 91 頁)。
- 6 若要讓現有單一登入服務指向新安裝的 Identity Reporting，請使用組態更新公用程式修改 Identity Reporting 組態項目。
- 7 重新啟動執行現有單一登入服務的 Tomcat 伺服器。

## 29.8.3 建立資料同步規則

設定 Reporting 伺服器之後，需要建立資料同步規則，以將事件從 SLM for IGA 轉遞到 Reporting 資料庫。升級至 Identity Reporting 4.7 時，需要注意以下事項。

---

附註：

- ◆ 如果您要從 Identity Reporting 4.5.6 升級至 Identity Reporting 4.7，則需要在 Identity Manager 的「資料收集服務」頁面中建立新規則。如需詳細資訊，請參閱《[Administrator Guide to NetIQ Identity Reporting](#)》(NetIQ Identity Reporting 管理員指南) 中的「[About the Data Sync Policies tab](#)」(關於「資料同步規則」索引標籤)。
  - ◆ 如果您要從 Identity Reporting 4.6.x 升級至 Identity Reporting 4.7，請依照《[NetIQ Identity Manager 4.7 版本說明](#)》的「[Identity Manager 升級問題](#)」中的步驟操作。
-



# 30 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。

---

## 30.1 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。

## 30.2 解除安裝 Identity Manager 引擎

安裝程式提供了 Identity Manager 的解除安裝程序檔。使用此程序檔可以移除安裝期間建立的所有服務、套件和目錄。

---

**附註：**在解除安裝 Identity Manager 引擎之前，請準備 Identity Vault。如需詳細資訊，請參閱第 30.1 節「從 Identity Vault 中移除物件」(第 267 頁)。

---

若要解除安裝 Identity Manager 引擎：

- 1 導覽至安裝時掛接 iso 的位置。
- 2 從 .iso 檔案的根目錄中，執行以下指令：

`./uninstall.sh`

- 3 指定要解除安裝的元件。

例如，指定 **1** 會解除安裝 Identity Manager 引擎。您還可以同時解除安裝多個元件。例如，指定 **1,2,3** 會解除安裝 Identity Manager 引擎、遠端載入器和擴送代理程式。

## 30.3 解除安裝 Identity Applications

- 1 導覽至安裝時掛接 .iso 的位置。
- 2 從 .iso 檔案的根目錄中，執行以下指令：

`./uninstall.sh`

- 3 指定要解除安裝的元件。

例如，指定 **1** 會解除安裝 Identity Applications。

## 30.4 解除安裝 Identity Reporting 元件

您必須依照以下順序解除安裝 Identity Reporting 的元件：

1. 刪除驅動程式。如需詳細資訊，請參閱第 30.4.1 節「刪除報告驅動程式」(第 268 頁)。
2. 刪除 Identity Reporting。如需詳細資訊，請參閱第 30.4.2 節「解除安裝 Identity Reporting」(第 269 頁)。
3. 刪除 Sentinel。如需詳細資訊，請參閱第 30.4.3 節「解除安裝 Sentinel」(第 269 頁)。

---

**附註：**為了節省磁碟空間，Identity Reporting 的安裝程式不會安裝 Java 虛擬機器 (JVM)。因此，若要解除安裝一或多個元件，請確保您有可用的 JVM，並且該 JVM 位於 PATH 中。如果在解除安裝期間遇到錯誤，請將 JVM 的位置新增至本地 PATH 環境變數，然後再次執行解除安裝程式。

---

### 30.4.1 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。

## 30.4.2 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 30.4.1 節「刪除報告驅動程式」(第 268 頁)。

- 1 導覽至安裝時掛接 .iso 的位置。
- 2 從 .iso 檔案的根目錄中，執行以下指令：  
`./uninstall.sh`
- 3 指定要解除安裝的元件。  
例如，指定 1 會解除安裝 Identity Reporting。

## 30.4.3 解除安裝 Sentinel

- 1 登入 Sentinel 伺服器。
- 2 導覽至包含解除安裝程序檔的目錄：  
`/opt/novell/sentinel/setup/`
- 3 執行下列指令：  
`./uninstall.sh`
- 4 當系統提示您重新確認要繼續解除安裝時，請按 y。  
程序檔會先停止服務，然後再將服務完全移除。

## 30.5 解除安裝 Designer

- 1 關閉 Designer。
- 2 解除安裝 Designer  
導覽至包含解除安裝程序檔的目錄 (預設為 <安裝目錄>/designer/UninstallDesigner/Uninstall Designer for Identity Manager)。  
若要執行該程序檔，請輸入 `./uninstall`

## 30.6 解除安裝 Analyzer

- 1 關閉 Analyzer。
- 2 根據作業系統解除安裝 Analyzer：  
導覽至預設位於 <安裝目錄>/analyzer/UninstallAnalyzer 目錄中的 Uninstall Analyzer for Identity Manager 程序檔。  
若要執行該程序檔，請輸入 `./解除安裝`



# 31 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。

## 31.1 使用者應用程式和 RBPM 安裝疑難排解

下表列出了您可能遇到的問題，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                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 從 configupdate 公用程式 (configupdate.sh) 中對 OSP 啟用 CEF 稽核時，嘗試登入 IDMRPT 會失敗。                                                                                                                             | 請執行以下步驟來解決此問題： <ol style="list-style-type: none"><li>1. 導覽至 /opt/netiq/idm/apps/tomcat/conf 目錄中的 ism-configuration.properties 和 idmrptcore_logging.xml 檔案。</li><li>2. 分別編輯 ism-configuration.properties 和 idmrptcore_logging.xml 檔案。</li><li>3. 在 ism-configuration.properties 和 idmrptcore_logging.xml 檔案中，分別將 <b>com.netiq.ism.audit.cef.protocol</b> 和 <b>&lt;protocol&gt;</b> 的值從 <b>tcp</b> 變更為 <b>TCP</b>。</li><li>4. 重新啟動 Tomcat。</li></ol> |
| 如果 Identity Applications 和 Identity Reporting 安裝在同一部伺服器上，並且您為資料庫建立選項選取了啟動，將會在記錄中看到一些例外。                                                                                                              | 若要清除這些例外，請手動重新啟動 Tomcat。                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 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： <ul style="list-style-type: none"><li>◆ Identity Vault 連接和證書</li><li>◆ 電子郵件設定</li><li>◆ Identity Manager 引擎使用者身分和使用者群組</li><li>◆ Access Manager 或 iChain 設定</li></ul> | 不依賴安裝程式來執行組態公用程式。<br><b>Linux</b> ：從安裝目錄 (預設為 /opt/netiq/idm/apps/configupdate/) 中執行以下指令：<br><br>./configupdate.sh                                                                                                                                                                                                                                                                                                                                 |
| 啟動 Tomcat 會導致以下例外：<br><br>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。 | <p>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。</p> <p>使用 <b>keytool</b> 指令，來輸入證書檔案：</p> <pre>keytool -import -trustcacerts -alias <i>aliasName</i> -file <i>certFile</i> -keystore ../lib/security/cacerts -storepass changeit</pre> <ul style="list-style-type: none"> <li>以您為此證書選擇的唯一名稱來取代 <i>aliasName</i>。</li> <li>以證書檔案的完整路徑和名稱來取代 <i>certFile</i>。</li> <li>預設金鑰儲存區密碼為 <b>changeit</b> (如果您有不同的密碼，請指定它)。</li> </ul> |
| 電子郵件通知無法傳送。          | <p>執行 <b>configupdate</b> 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：<b>Email From</b> 和 <b>Email Host</b>。</p> <p><b>Linux</b>：從安裝目錄 (預設為 <code>/opt/netiq/idm/apps/UserApplication/</code>) 執行以下指令：</p> <pre>./configupdate.sh</pre>                                                                                                                                                                                    |

## 31.2 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。                                                                                                                                                                                                                                                                                               |
| 當您從 Identity Applications 頁面登出時，SSPR 顯示錯誤 5053 ERROR_APP_UNAVAILABLE。 | 忽略此錯誤，它不會導致功能受損。                                                                                                                                                                                                                                                                                                                                                            |
| 在第一次登入 Identity Applications 時不提示處理安全回應                               | <ol style="list-style-type: none"> <li>確定 SSPR 服務器具有使用 FQDN 建立的證書。</li> <li>登入使用者應用程式伺服器，並啟動 ConfigUpdate (<code>/opt/netiq/idm/apps/configupdate/</code>) 公用程式。</li> <li>導覽至 <b>SSO 用戶端 &gt; Self Service Password Reset</b>，並確定設定正確。</li> </ol> <p>如果 SSPR 安裝在其他伺服器上，請確定 SSPR 證書已輸入到使用者應用程式伺服器上 <code>/opt/netiq/idm/apps/tomcat/conf</code> 中的 <code>idm.jks</code>。</p> |



| 問題                     | 建議的動作                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 存取 SSPR URL 時瀏覽器顯示空白頁面 | <p>未使用 OSP 正確設定 SSPR 時，會出現這種情況。SSPR 記錄會顯示以下資訊：</p> <pre>2018-01-24T22:24:02Z, ERROR, oauth.OAuthConsumerServlet, 5071 ERROR_OAUTH_ERROR (unexpected error communicating with oauth server: password.pwm.error.PwmUnrecoverableException: 5071 ERROR_OAUTH_ERROR (io error during oauth code resolver http request to oauth server: Certificate for &lt;IP&gt; doesn't match any of the subject alternative names: [IP]))</pre> <ol style="list-style-type: none"> <li>1. 驗證執行 OSP 的 Tomcat 伺服器是否具有使用 FQDN 建立的有效證書。登入使用者應用程式伺服器，並啟動 <b>ConfigUpdate</b> 公用程式。導覽至 <b>SSO 用戶端 &gt; Self Service Password Reset</b>，並確定設定正確。</li> <li>2. 透過覆寫 OSP 登入方法登入 SSPR (例如，<code>https://&lt;sspr sserver ip&gt;:&lt;port&gt;/sspr/private/Login?sso=false</code>)。</li> <li>3. 導覽至頁面右上角的組態編輯器。</li> <li>4. 指定設定密碼，然後按一下登入。</li> <li>5. 導覽至 <b>LDAP &gt; LDAP 目錄 &gt; 預設 &gt; 連接</b>。</li> <li>6. 如果 LDAP 證書不正確，請按一下清除。</li> <li>7. 若要重新輸入證書，請按一下從伺服器輸入。</li> <li>8. 導覽至設定 &gt; 單一登入 (SSO) 用戶端 &gt; <b>OAuth</b>，並在 <b>OAuth Web 服務伺服器證書</b> 下驗證證書是否正確。</li> <li>9. 如果證書不正確，請按一下清除。</li> <li>10. 若要重新輸入證書，請按一下從伺服器輸入。</li> </ol> <p>從不同的目錄啟動 <b>ConfigUpdate</b> 公用程式時發生錯誤</p> <p><b>ConfigUpdate</b> 公用程式會報告錯誤。它將不儲存任何變更。例如，如果您使用 <code>/opt/netiq/idm/apps/configupdate/configupdate.sh</code> 指令啟動 <b>configupdate</b> 公用程式，它不會啟動。</p> <p>您應導覽至 <code>/opt/netiq/idm/apps/configupdate/</code> 目錄，然後執行 <code>./configupdate.sh</code> 指令。</p> |

## 31.3 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 <b>netiq</b> 目錄。如果您已從電腦中移除所有 <b>NetIQ</b> 軟體，則可以自己來刪除該目錄。 |



# A

## 使用 Identity Vault 的多個例項

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 A.1 節「瞭解 eDirectory 中的 Identity Manager 物件」(第 275 頁)
- ◆ 第 A.2 節「在伺服器上複製 Identity Manager 需要的物件」(第 275 頁)
- ◆ 第 A.3 節「使用範圍過濾來管理不同伺服器上的使用者」(第 277 頁)
- ◆ 第 A.4 節「瞭解 Identity Vault 安裝套件中的 Linux 套件」(第 278 頁)

### A.1 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。

### A.2 在伺服器上複製 Identity Manager 需要的物件

如果 Identity Manager 環境呼叫多個伺服器，以執行多個 Identity Manager 驅動程式，則應在計劃中確保將特定的 eDirectory 物件複製到要執行這些 Identity Manager 驅動程式的伺服器上。

只要過濾後的複製本中包含驅動程式需要讀取或同步化的所有物件和屬性，便可以使用過濾後的複製本。

請記住您必須針對「Identity Manager 驅動程式」物件提供其所要同步化之任何物件的足夠 eDirectory 權限，可以藉由明確授予權限，或者讓「驅動程式」物件安全性等值於具有所需權限的物件來提供。

執行 Identity Manager 驅動程式的 eDirectory 伺服器 (或驅動程式參照的 eDirectory 伺服器，如果您使用的是遠端載入器) 必須保存下列的主檔案系統物件或讀 / 寫複製本：

- ◆ 該伺服器的「驅動程式集」物件。

每個執行 **Identity Manager** 的伺服器都應該具有一個「驅動程式集」物件。除非您有特定需要，否則請勿將多個伺服器與相同的「驅動程式集」物件相關聯。

---

**附註：**建立驅動程式集物件時，預設設定是建立個別的分割區。**NetIQ** 建議在「驅動程式集」物件上建立獨立的分割區。若要讓 **Identity Manager** 得以運作，伺服器必須保有「驅動程式集」物件的完整複製本。如果伺服器具有「驅動程式集」物件安裝位置的完整複製本，則不需要分割區。

---

- ◆ 該伺服器的「伺服器」物件。

「伺服器」物件是必要的，因為它可讓驅動程式產生物件的金鑰配對。它對於遠端載入器認證資訊也很重要。

- ◆ 您想要與此驅動程式例項同步化的物件。

除非物件的複製本與驅動程式在同一個伺服器上，否則驅動程式無法同步化那些物件。事實上，**Identity Manager** 驅動程式會同步化在伺服器上所複製之所有容器中的物件，除非您建立範圍過濾規則來另外指定。

例如，如果您想要驅動程式同步化所有使用者物件，最簡單的方法就是在保存您的所有使用者之主檔案系統物件或讀 / 寫複製本的伺服器上使用一個驅動程式例項。

不過，許多環境並沒有包含所有使用者複製本的單一伺服器，而是全部使用者會分散在多個伺服器上。在這種情況下，您有兩種選擇：

- ◆ **將使用者聚集至單一伺服器上。**您可以將複製本新增至現有的伺服器上，來建立保留所有使用者的單一伺服器。如果需要，可以使用過濾後的複製本來減少 **eDirectory** 資料庫的大小，只要過濾後複製本中包含必要的使用者物件和屬性。
- ◆ **使用範圍過濾，在多個伺服器上使用多個驅動程式例項。**如果您不想將使用者聚集至單一伺服器，則需要判定保留所有使用者的伺服器組，並在其中每個伺服器上設定一個 **Identity Manager** 驅動程式例項。

若要防止驅動程式的各個例項嘗試同步化相同的使用者，您需要使用「範圍過濾」，以定義每個驅動程式例項應該同步化的使用者。範圍過濾是指，將規則新增至每個驅動程式，以將驅動程式的管理範圍限制在特定的容器。請參閱「[使用範圍過濾來管理不同伺服器上的使用者](#)」(第 277 頁)。

- ◆ **在多個伺服器上使用多個驅動程式例項，不使用範圍過濾。**如果您想讓驅動程式的多個例項在不同的伺服器上執行，但不使用過濾後的複製本，則需要在不同驅動程式例項上定義規則，讓驅動程式可以在同一 **Identity Vault** 中處理不同的物件組。
- ◆ 您想要驅動程式在建立使用者時使用的「範本」物件 (如果您選擇使用範本)。

**Identity Manager** 驅動程式不需要您指定 **eDirectory** 「範本」物件來建立使用者。但是，如果您指定驅動程式在 **eDirectory** 中建立使用者時應該使用範本，則必須在執行驅動程式的伺服器上複製「範本」物件。

- ◆ 您想要 **Identity Manager** 驅動程式用於管理使用者的任何容器。

例如，如果您已建立名為「未啟用使用者」的容器來保留已停用的使用者帳戶，則必須在執行驅動程式的伺服器上擁有該容器的主複製本或讀 / 寫複製本 (最好是主要複製本)。

- ◆ 驅動程式需要參考的任何其他物件 (例如，驅動程式的工作順序物件)。

如果驅動程式只是讀取，而不變更其他物件，則那些物件在伺服器上的複製本可以是唯讀複製本。

## A.3 使用範圍過濾來管理不同伺服器上的使用者

範圍過濾是指，將規則新增至每個驅動程式規則，以將驅動程式的動作範圍限制在特定的容器。下面是您需要使用範圍過濾的兩種情況：

- 您想要驅動程式僅同步化特定容器中的使用者。

**Identity Manager** 驅動程式預設會對所執行之伺服器上複製之所有容器中的物件，進行同步化。若要縮小該範圍，則您必須建立範圍過濾規則。

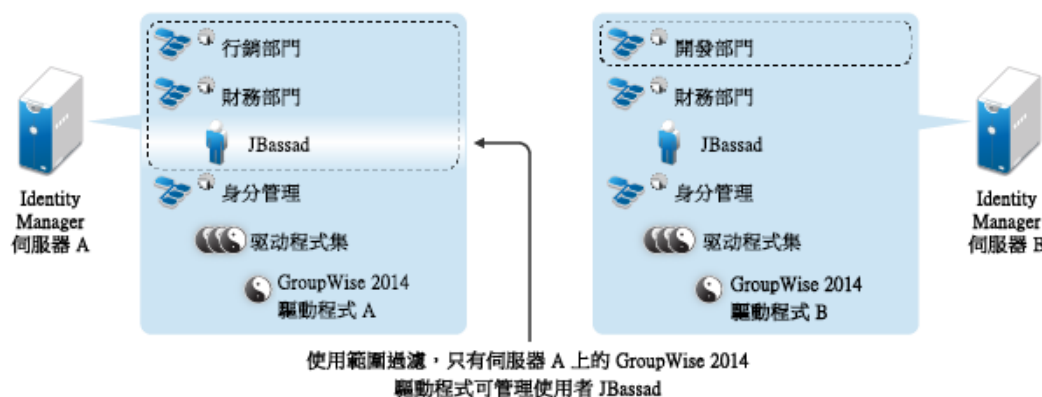
- 您想要 **Identity Manager** 驅動程式同步化所有使用者，但不想將所有使用者複製到相同的伺服器上。

若要同步化所有使用者，但不將他們複製到單一伺服器上，您需要判斷何者為保留所有使用者的伺服器組，然後在其中每個伺服器上建立 **Identity Manager** 驅動程式例項。若要防止驅動程式的兩個例項嘗試同步化相同的使用者，您需要使用「範圍過濾」，以定義每個驅動程式例項應該同步化的使用者。

**附註：**即使您的伺服器複製本目前沒有重疊，你也應該使用範圍過濾。以後，可以將複製本新增至伺服器，並可以無意地建立重疊。如果您將範圍過濾放置在適當位置，則 **Identity Manager** 驅動程式不會嘗試同步化相同的使用者，即使以後會將複製本新增至伺服器。

圖 A-1(第 277 頁)顯示了一個範例 **Identity Vault**，其中有三個存放使用者的容器：「行銷部門」、「財務部門」和「開發部門」。它也會顯示保存驅動程式集的「身分識別管理」容器。其中每個容器中都是一個個別分割區。在此範例中，**Identity Manager** 管理員有兩個 **Identity Vault** 伺服器：伺服器 A 和伺服器 B。這兩個伺服器都不包含所有使用者的副本。每個伺服器包含三個分割區中的兩個，因此伺服器所保留內容的範圍重疊。

圖 A-1 範圍過濾定義同步化各個容器的驅動程式



管理員希望透過 **GroupWise 2014** 驅動程式同步網路樹中的所有使用者，但是不希望將這些使用者的複本聚合到單部伺服器上。他選擇使用兩個 **GroupWise 2014** 驅動程式例項，每部伺服器上安裝一個。他在每部 **Identity Manager** 伺服器上都安裝了 **Identity Manager**，並設定了 **GroupWise 2014** 驅動程式。

「伺服器 A」會保存「行銷部門」和「財務部門」容器的複製本。另外，該伺服器上還有一個「身分管理」容器的複本，其中存放伺服器 A 的驅動程式集以及伺服器 A 的 **GroupWise 2014** 驅動程式物件。

伺服器 B 存放「開發」容器、「財務」容器和「身分管理」容器的複本，最後一個容器存放伺服器 B 的驅動程式集和伺服器 B 的 GroupWise 2014 驅動程式物件。

因為「伺服器 A」和「伺服器 B」都會保存「財務部門」容器的複製本，所以這兩個伺服器都會保存「財務部門」容器中的使用者 JBassad。如果不使用範圍過濾，GroupWise 2014 驅動程式 A 和 GroupWise 2014 驅動程式 B 都會同步 Jbassad。範圍過濾可防止兩個驅動程式例項管理同一個使用者，因為它會定義用於同步化各個容器的驅動程式。

Identity Manager 中提供了一些預先定義的規則。有兩個規則可協助執行範圍過濾：事件轉換 - 範圍過濾 - 包括子網路樹和事件轉換 - 範圍過濾 - 排除子網路樹。如需詳細資訊，請參閱《[NetIQ Identity Manager Understanding Policies Guide](#)》(NetIQ Identity Manager 規則解讀指南)。

在此範例中，您會針對「伺服器 A」和「伺服器 B」使用「包括子網路樹」預先定義規則。您會分別定義每個驅動程式的範圍，以便它們僅同步化特定容器中的使用者。「伺服器 A」會同步化「行銷部門」和「財務部門」。「伺服器 B」會同步化「開發部門」。

## A.4 瞭解 Identity Vault 安裝套件中的 Linux 套件

NetIQ eDirectory 包含一套由一組工具組成的 Linux 套件系統，這些工具可簡化各種 eDirectory 元件的安裝和解除安裝。套件中的 `makefile` 檔案描述建立特定 eDirectory 元件需符合的要求。套件中還包含組態檔案、公用程式、程式庫、精靈和手冊頁，它們使用隨作業系統一起安裝的標準 Linux 工具。

某些套件依存於其他套件或 Identity Manager 的元件 (例如 NICI)。只有安裝了所有相依套件才能確保功能正常運作。

下表提供了關於 eDirectory 隨附之 Linux 套件的資訊。所有套件都帶有 *novell-* 字首。例如，`novell-NDSserv` 代表 `NDSserv`。

| 套件        | 描述                                                                                                                                                                                                                                                        |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NOVLice   | 包含 NetIQ Import Convert Export 公用程式。此套件依存於 NOVLmgt、NOVLxis 和 NLDAPbase 套件。                                                                                                                                                                                |
| NOVbase   | 代表目錄使用者代理程式。此套件依存於 NICI 套件。<br>此套件包含以下項目： <ul style="list-style-type: none"><li>◆ 包含 eDirectory 所需之 RSA 驗證的驗證工具箱。</li><li>◆ 獨立於平台的系統抽象程式庫、包含所有已定義目錄使用者代理程式功能的程式庫，以及綱要延伸程式庫。</li><li>◆ 組合的組態公用程式和目錄使用者代理程式測試公用程式。</li><li>◆ eDirectory 組態檔案和手冊頁。</li></ul> |
| NDScommon | 包含 eDirectory 組態檔案、安裝和解除安裝公用程式的 <code>man</code> 頁面。此套件依存於 NDSbase 套件。                                                                                                                                                                                    |
| NDSmasv   | 包含強制存取控制 (MASV) 所需的程式庫。                                                                                                                                                                                                                                   |

| 套件        | 描述                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NDSserv   | <p>包含 eDirectory 伺服器所需的所有二進位檔案和程式庫。它還包含用於管理系統上 eDirectory 伺服器的公用程式。此套件依存於 NDSbase、NDScommon、NDSmasv、NLDAPsdk、NOVLpkia 和 NOVLpkkit 套件。它還包含以下項目：</p> <ul style="list-style-type: none"> <li>◆ NDS 安裝程式庫、FLAIM 程式庫、追蹤程式庫、NDS 程式庫、LDAP 伺服器程式庫、LDAP 安裝程式庫、索引編輯器程式庫、DNS 程式庫、合併程式庫和 LDAP SDK 的 LDAP 延伸程式庫。</li> <li>◆ eDirectory 伺服器精靈。</li> <li>◆ DNS 的二進位檔案，以及用於載入和卸載 LDAP 的二進位檔案。</li> <li>◆ 用於建立 MAC 位址的公用程式、用於追蹤伺服器和變更伺服器某些全域變數的公用程式、用於備份和還原 eDirectory 的公用程式，以及用於合併 eDirectory 網路樹的公用程式。</li> <li>◆ 啟動 DNS、NDS 與 NLDAP 的程序檔。</li> <li>◆ man 頁面。</li> </ul> |
| NDSrepair | <p>包含執行時期程式庫，以及用於校正 eDirectory 資料庫中各種問題的公用程式。此套件依存於 NDSbase 套件。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| NLDAPbase | <p>包含 LDAP 程式庫、LDAP 程式庫的延伸以及下列 LDAP 工具：</p> <ul style="list-style-type: none"> <li>◆ ldapdelete</li> <li>◆ ldapmodify</li> <li>◆ ldapmodrdn</li> <li>◆ ldapsearch</li> </ul> <p>此套件依存於 NLDAPsdk 套件。</p>                                                                                                                                                                                                                                                                                                                                                   |
| NOVLnmas  | <p>包含所有 NMAS 程式庫，以及 NMAS 伺服器所需的 nmasinst 二進位檔案。此套件依存於 NICI 和 NDSmasv 套件。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| NLDAPsdk  | <p>包含 LDAP 執行時期的 NetIQ 延伸以及安全性程式庫 (用戶端 NICI)。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| NOVLsubag | <p>包含執行時期程式庫，以及適用於 eDirectory SNMP 子代理程式的公用程式。此套件依存於 NICI、NDSbase 和 NLDAPbase 套件。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| NOVLpkkit | <p>提供不需要 eDirectory 的 PKI 服務。此套件依存於 NICI 和 NLDAPsdk 套件。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| NOVLpkis  | <p>提供 PKI 伺服器服務。此套件依存於 NICI、NDSbase 和 NLDAPsdk 套件。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| NOVLsnmp  | <p>執行時期程式庫和適用於 SNMP 的公用程式。此套件依存於 NICI 套件。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| NDSdexvnt | <p>包含用於管理 NetIQ eDirectory 中針對其他資料庫產生之事件的程式庫。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| NOVLpkia  | <p>提供 PKI 服務。此套件依存於 NICI、NDSbase 和 NLDAPsdk 套件。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| NOVLembox | <p>提供 eMBox 基礎架構和 eMTools。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| NOVLimgnt | <p>包含 NetIQ 語言管理的執行時期程式庫。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| NOVLxis   | <p>包含 NetIQ XIS 的執行時期程式庫。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| NOVLsas   | <p>包含 NetIQ SAS 程式庫。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| NOVLntls  | <p>包含 NetIQ TLS 程式庫。此套件又名為 ntls。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| 套件       | 描述                                                                               |
|----------|----------------------------------------------------------------------------------|
| NOVLdif2 | 包含 NetIQ Offline Bulkload 公用程式，依存於 NDSbase、NDSserv、NOVLntls、NOVLimgnt 和 NICI 套件。 |
| NOVLncp  | 包含 NetIQ Encrypted NCP Services for Linux。此套件依存於 NDScommon 套件。                   |



# B SLES 12 SP2 上簡單的 Identity Manager 叢集部署解決方案

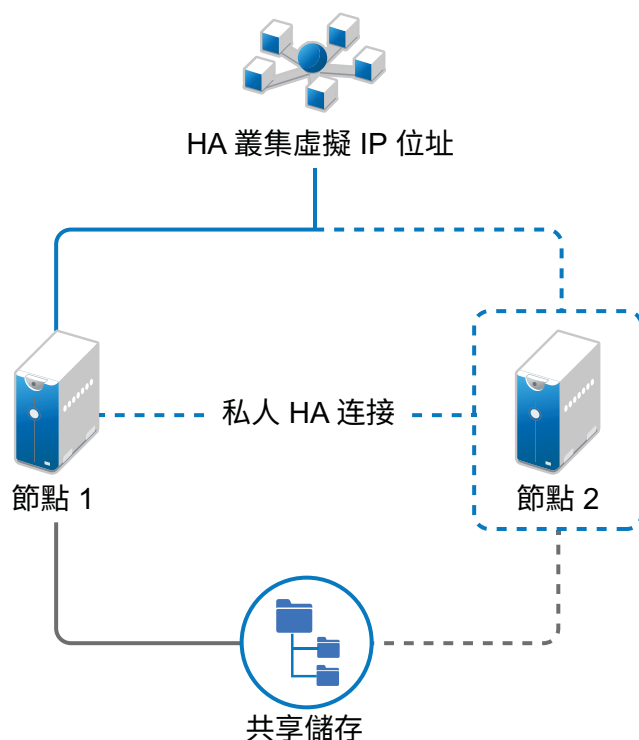
本附錄逐步說明了如何在使用共享儲存的受支援 SUSE Linux Enterprise Server (SLES) 叢集環境中設定 eDirectory 和 Identity Manager，並提供了一個 Identity Manager 叢集部署範例。

- ◆ 第 B.1 節「先決條件」(第 281 頁)
- ◆ 第 B.2 節「安裝程序」(第 282 頁)

對於使用共享儲存的線上層級 Linux 高可用性 (HA) 解決方案，建議在叢集中執行圍籬區隔機制。雖然在叢集中執行圍籬區隔機制的方法有多種，但在此範例中，我們會使用一個利用電腦分裂偵測器 (SBD) 的 STONITH 資源。

圖 B-1(第 281 頁) 顯示了一個叢集部署解決方案範例。

圖 B-1 叢集部署解決方案範例



## B.1 先決條件

- ◆ 兩部執行 SLES 12 SP2 64 位元的伺服器做為節點
- ◆ 一個執行 SLES 12 SP2 64 位元的伺服器，做為 iSCSI 伺服器

- ◆ SLES12 SP2 64 位元 HA Extension ISO 影像檔
- ◆ 六個靜態 IP：
  - ◆ 每個節點有兩個靜態 IP 位址。
  - ◆ 一個靜態 IP 位址用於叢集。此 IP 位址將會動態指定給目前執行 eDirectory 的節點。
  - ◆ 一個靜態 IP 位址用於 iSCSI 伺服器。

## B.2 安裝程序

本節介紹安裝和設定以下項目，以設定叢集環境的程序。如需設定 SLES High Availability Extension 的詳細資訊，請參閱 [SUSE Linux Enterprise High Availability Extension](#) 指南。

### B.2.1 設定 iSCSI 伺服器

iSCSI 目標是指設定為叢集中所有節點的通用儲存的裝置。它是 Linux 伺服器上建立的虛擬磁碟，可使 iSCSI 啟動器能夠透過乙太網路連接進行遠端存取。iSCSI 啟動器是指叢集中設定用於聯絡服務目標 (iSCSI) 的任一節點。iSCSI 目標應該永遠處於正常運作狀態，如此，任何充當啟動器的主機才能聯絡目標。在 iSCSI 伺服器上安裝 iSCSI 目標之前，請確保 iSCSI 目標上有足夠的空間用於通用儲存。安裝 SLES 12 SP2 後，請在其餘兩個節點上安裝 iSCSI 啟動器套件。

在安裝 SLES 12 SP2 期間：

- 1 建立一個獨立的分割區，並將分割區路徑指定為 iSCSI 共享儲存分割區。
- 2 安裝 iSCSI 目標套件。

若要設定 iSCSI 伺服器：

- 1 在目標伺服器上建立一個區塊裝置。
- 2 在終端機中輸入 `yast2 disk` 指令。
- 3 建立一個新的 Linux 分割區，並選取不格式化。
- 4 選取不掛接分割區。
- 5 指定分割區大小。
- 6 在終端機中輸入 `yast2 iscsi-server` 或 `yast2 iscsi-lio-server` 指令。
- 7 按一下服務索引標籤，然後在服務啟動選項中選取開機時。
- 8 在目標索引標籤中，按一下新增，以輸入分割區路徑 (在安裝 SLES 期間建立的路徑)。
- 9 在修改 iSCSI 目標啟始者設定頁面中，指定目標伺服器的 iSCSI 用戶端啟始者主機名稱，然後按下一步。

例如，`iqn.sles12sp2node2.com` 和 `iqn.sles12sp2node3.com`。

- 10 按一下「完成」。
- 11 在終端機中執行 `cat /proc/net/iet/volume` 指令，以驗證是否已安裝 iSCSI 目標。

## B.2.2 在所有節點上設定 iSCSI 啟動器

為了連接到 iSCSI 目標，您必須在所有叢集節點上設定 iSCSI 啟動器。

若要設定 iSCSI 啟動器：

- 1 安裝 iSCSI 啟動器套件。
- 2 在終端機中執行 `yast2 iscsi-client`。
- 3 按一下服務索引標籤，然後在服務啟動選項中選取開機時。
- 4 按一下已連接目標索引標籤，然後按一下新增，以輸入 iSCSI 目標伺服器的 IP 位址。
- 5 選取無驗證。
- 6 按下一步，然後按一下連接。
- 7 按一下切換啟動方式，將啟動選項從手動變更為自動，然後按下一步。
- 8 按一下「下一步」，然後按一下「確定」。
- 9 若要檢查目標伺服器上連接的啟動器的狀態，請在目標伺服器上執行 `cat /proc/net/iet/session` 指令。已連接到 iSCSI 伺服器的啟動器清單即會顯示。

## B.2.3 分割共享儲存

建立兩個共享儲存分割區：一個用於 SBD，另一個用於叢集檔案系統。

若要分割共享儲存：

- 1 在終端機中執行 `yast2 disk` 指令。
- 2 在進階磁碟分割程式對話方塊中選取共享磁碟區。在本範例中，請從進階磁碟分割程式對話方塊中選取 **sdb**。
- 3 按一下新增，選取主分割區選項，然後按下一步。
- 4 選取自訂大小，然後按下一步。在此範例中，自訂大小為 100 MB。
- 5 在格式化選項下，選取不格式化分割區。在此範例中，檔案系統 ID 為 0x83 Linux。
- 6 在掛接選項下，選取不掛接分割區，然後按一下完成。
- 7 按一下新增，然後選取主分割區。
- 8 按下一步，選取最大大小，然後按下一步。
- 9 在格式化選項中，選取不格式化分割區。在此範例中，我們指定 0x83 Linux 做為檔案系統 ID。
- 10 在掛接選項中，選取不掛接分割區，然後按一下完成。

## B.2.4 安裝 HA Extension

若要安裝 HA Extension：

- 1 造訪 [SUSE 下載網站](#)。

對於每個可用平台，SUSE Linux Enterprise High Availability Extension (SLE HA) 提供了兩個 ISO 影像供您下載。媒體 1 包含二進位套件，媒體 2 包含原始程式碼。

---

**附註：**根據您的系統架構選取並安裝相應的 HA Extension ISO 檔案。

---

- 2 將媒體 1 ISO 檔案下載到每部伺服器上。
- 3 開啟 **YaST 控制中心**對話方塊，然後按一下**附加產品 > 新增**。
- 4 按一下**瀏覽**並選取 DVD 或本地 ISO 影像，然後按下一步。
- 5 在**模式索引**標籤中的**主要功能**下，選取**高可用性**。  
確定已安裝高可用性下的所有元件。
- 6 按一下「接受」。

## B.2.5 設定 Softdog 監視程式

在 SLES HA Extension 中，核心中的監視程式支援預設處於啟用狀態。該產品隨附了多個不同的核心模組，用於提供硬體特定的監視程式驅動程式。系統開機時會自動載入適當的硬體監視程式驅動程式。

- 1 啟用 softdog 監視程式：  

```
echo softdog > /etc/modules-load.d/watchdog.conf
```

```
systemctl restart systemd-modules-load
```
- 2 測試 softdog 模組是否已正確載入：  

```
lsmod | grep dog
```

## B.2.6 設定 HA 叢集

此範例假設您要在叢集中設定兩個節點。

設定第一個節點：

- 1 以 root 身分登入要做為叢集節點的實體或虛擬機器。
- 2 執行以下指令：  

```
ha-cluster-init
```

該指令會檢查是否存在 NTP 組態與硬體監視程式服務。這會產生 SSH 存取與 Csync2 同步所需的公用和私密 SSH 金鑰，並啟動相應的服務。
- 3 設定叢集通訊層：
  - 3a 輸入要繫結到的網路位址。
  - 3b 輸入多路廣播位址。程序檔會建議一個隨機位址，您可將其做為預設值。
  - 3c 輸入多路廣播連接埠。預設埠號碼為 5405。
- 4 將 SBD 設定為節點圍籬區隔機制：
  - 4a 按 **y** 以使用 SBD。
  - 4b 輸入要為 SBD 使用的區塊裝置分割區的永久路徑。該路徑對於叢集中的兩個節點必須一致。
- 5 設定用於叢集管理的虛擬 IP 位址：
  - 5a 按 **y** 以設定虛擬 IP 位址。
  - 5b 輸入一個未使用的 IP 位址，做為 SUSE Hawk 圖形使用者界面的管理 IP。例如，  
`192.168.1.3`。  
您可以連接至該虛擬 IP 位址，而無需登入個別叢集節點。

第一個節點啟動並執行後，使用 `ha-cluster-join` 指令新增第二個叢集節點。

#### 設定第二個節點：

- 1 以 `root` 身分登入要用於連接叢集的實體機器或虛擬機器。
- 2 執行以下指令：  
`ha-cluster-join`  
如果未設定 `NTP`，則會顯示一則訊息。該指令會檢查是否存在硬體監視程式裝置，如果不存在，將發出通知。
- 3 輸入第一個節點的 IP 位址。
- 4 輸入第一個節點的 `root` 密碼。
- 5 登入 SUSE Hawk 圖形使用者介面，然後按一下**狀態 > 節點**。例如，<https://192.168.1.3:7630/cib/live>。



## B.2.7 在叢集節點上安裝並設定 eDirectory 和 Identity Manager

- 1 在叢集節點上安裝 eDirectory：  
安裝受支援版本的 如需在高可用性叢集上設定 eDirectory 的逐步說明，請參閱《[eDirectory Installation Guide](#)》(eDirectory 安裝指南) 中的「[Deploying eDirectory on High Availability Clusters](#)」(在高可用性叢集上部署 eDirectory)。

---

**重要：**在節點 1 上安裝 eDirectory 之前，請確保節點 1 上已設定虛擬 IP。

---

- 2 使用「Metadirectory 伺服器」選項在節點 1 上安裝 Identity Manager。
- 3 使用 `DCLUSTER_INSTALL` 選項在節點 2 上安裝 Identity Manager 引擎。  
執行 `./install.bin -DCLUSTER_INSTALL="true"` 指令 (在終端機中)。  
安裝程式將在不與 eDirectory 進行任何互動的情況下安裝 Identity Manager 檔案。


## B.2.8 設定 eDirectory 資源

- 1 登入 SUSE Hawk 圖形使用者介面。
- 2 按一下**新增資源**，然後建立新群組。
  - 2a 按一下**群組**旁邊的 **+**。
  - 2b 指定群組 ID。例如，*群組 1*。

建立群組時，確定選取了以下子資源：

- ♦ *stonith-sbd*
- ♦ *admin\_addr* (叢集 IP 位址)

3 在中繼資料屬性索引標籤中，將 **target-role** 欄位設定為 *Started*，並將 **is-managed** 欄位設定為 *Yes*。

4 按一下編輯組態，然後按一下在步驟 2 中建立的群組旁邊的 。

5 在子項欄位中，新增以下子資源：

- ♦ *shared-storage*
- ♦ *eDirectory-resource*

例如，在該群組中，應該依以下順序新增資源：

- ♦ *stonith-sbd*
- ♦ *admin\_addr* (叢集 IP 位址)
- ♦ *shared-storage*
- ♦ *eDirectory-resource*

您可以視需要變更資源名稱。每個資源都有一組參數需要定義。如需 *shared-storage* 和 *eDirectory* 資源範例的資訊，請參閱 [eDirectory](#) 和 [共享儲存子資源的原始值](#)。

## B.2.9 eDirectory 和共享儲存子資源的原始值

依預設，*stonith-sbd* 和 *admin\_addr* 資源是在啟始化叢集節點時透過高可用性叢集指令設定的。

表格 B-1 *shared-storage* 的範例


| 資源 ID               | 共享儲存資源的名稱                                                                                                         |
|---------------------|-------------------------------------------------------------------------------------------------------------------|
| Class               | ocf                                                                                                               |
| Provider            | heartbeat                                                                                                         |
| Type                | Filesystem                                                                                                        |
| device              | /dev/sdc1                                                                                                         |
| directory           | /shared                                                                                                           |
| fstype              | xfs                                                                                                               |
| operations          | <ul style="list-style-type: none"><li>♦ start (60, 0)</li><li>♦ stop (60, 0)</li><li>♦ monitor (40, 20)</li></ul> |
| is-managed          | Yes                                                                                                               |
| resource-stickiness | 100                                                                                                               |
| target-role         | Started                                                                                                           |

表格 B-2 eDirectory-resource 的範例

|                     |                                                                                                                      |
|---------------------|----------------------------------------------------------------------------------------------------------------------|
| 資源 ID               | eDirectory 資源的名稱                                                                                                     |
| Class               | systemd                                                                                                              |
| Type                | ndsdtmpl-shared-conf-nds.conf@-shared-conf-env                                                                       |
| operations          | <ul style="list-style-type: none"><li>♦ start (100, 0)</li><li>♦ stop (100, 0)</li><li>♦ monitor (100, 60)</li></ul> |
| target-role         | Started                                                                                                              |
| is-managed          | Yes                                                                                                                  |
| resource-stickiness | 100                                                                                                                  |
| failure-timeout     | 125                                                                                                                  |
| migration-threshold | 0                                                                                                                    |

## B.2.10 變更位置條件約束分數

將位置條件約束分數變更為 0。

- 1 登入 SUSE Hawk 圖形使用者介面。
- 2 按一下編輯組態。
- 3 在條件約束索引標籤中，按一下叢集節點 1 旁邊的 。
- 4 在簡單索引標籤中，將分數設定為 0。
- 5 按一下「套用」。

務必將叢集中所有節點的分數設定為 0。

**附註：**當從 SUSE Hawk 圖形使用者介面中使用狀態 > 資源 > 移轉選項，將資源從一個節點移轉至另一個節點時，位置條件約束分數將變更為 *Infinity* 或 *-Infinity*。如此僅會將優先設定提供給叢集中的一個節點，並且將導致 eDirectory 操作延遲。





# C Tomcat 應用程式伺服器上的範例 Identity Applications 叢集部署解決方案

本附錄透過一個範例部署說明如何在 Apache Tomcat 應用程式伺服器上的叢集環境中設定 Identity Applications。

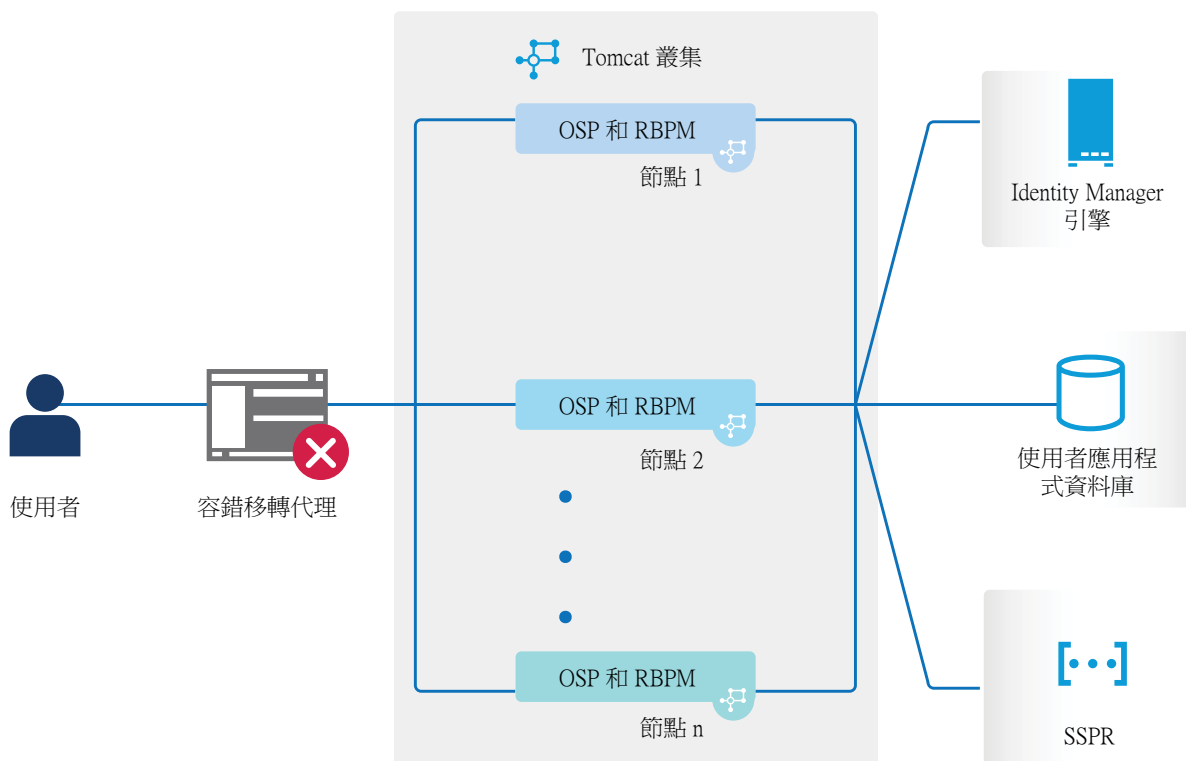
使用叢集，您可以在多部平行伺服器（叢集節點）上執行 Identity Applications，從而實現高可用性。若要建立叢集，需要將若干個 Tomcat 例項（節點）組合在一起。負載將分散在不同的伺服器之間，即使有任何伺服器發生故障，您仍可透過其他叢集節點來存取 Identity Applications。若要實現容錯移轉，您可以建立一個 Identity Applications 叢集，然後將這些 Identity Applications 設定為充當單部伺服器。不過，此組態不包括 Identity Reporting。

建議使用負載平衡器軟體，它會處理所有使用者申請並將它們發送給叢集中的伺服器節點。負載平衡器通常是叢集的一部分。它瞭解叢集組態及容錯移轉規則。您可以選取最適合您的解決方案。

圖 C-1 顯示了一個包含雙節點叢集的範例部署，並做出如下假設：

- ◆ 所有通訊都透過負載平衡器路由。
- ◆ Identity Manager 引擎和使用者應用程式等元件安裝在單獨的伺服器上。建議對生產層級部署使用此方法。
- ◆ 您熟悉 eDirectory、Identity Manager 引擎、Identity Applications、Tomcat 應用程式伺服器和使用者應用程式資料庫的安裝程序。
- ◆ SSPR (Single Sign-On Password Reset) 安裝在單獨的電腦上。建議對生產層級部署採用此方法。
- ◆ 使用 PostgreSQL 做為使用者應用程式的資料庫。不過，您可以使用支援的任何資料庫，例如 Oracle 或 MsSQL。
- ◆ 所有使用者應用程式節點均與 eDirectory 和使用者應用程式資料庫的同一個例項通訊。您可以依據自己的要求，增加使用者應用程式例項數量。

圖 C-1 叢集部署解決方案範例



附註：雙節點叢集是實現高可用性的最低組態。不過，您可以輕鬆地對包含更多節點的叢集沿用本章中的思路。

為了協助您瞭解逐步組態，本文後續小節中通篇都會參考此範例部署。

## C.1 先決條件

- 兩部執行 SUSE Linux Enterprise Server (SLES) 12 SP2 64 位元或 RedHat Enterprise Linux (RHEL) 7.3 64 位元的伺服器做為安裝了所有相依程式庫的節點。如需詳細資訊，請參閱有關 RHEL 的章節。
- 已安裝 Identity Manager 4.7 元件。
- 所有節點的應用程式伺服器時鐘都相同。確保這一點最簡單的方法就是，將節點設定為使用同一部網路時間伺服器來透過 NTP 同步時間。
- 叢集節點位於同一個子網路中。
- 容錯移轉代理或負載平衡解決方案安裝在單獨的電腦上。

## C.2 安裝程序

本節提供在 Tomcat 上安裝新 Identity Applications 例項，然後針對叢集設定該例項的逐步說明。

1. 安裝 Identity Manager 4.7 引擎。如需逐步指示，請參閱第 9.1 節「安裝 Identity Manager 引擎」（第 83 頁）。對於生產層級部署，建議將 Identity Manager 引擎安裝在單獨的伺服器上。

2. 為 Identity Applications 安裝資料庫。可以使用隨 Identity Applications 一併安裝的 PostgreSQL 資料庫。不過，建議將資料庫安裝在單獨的伺服器上。
3. 在節點 1 上，安裝並設定 Identity Applications。

在安裝期間，請確定：

- ◆ 選取新資料庫選項
- ◆ 提供唯一的工作流程引擎 ID。例如，節點 1。
- ◆ 叢集中的所有使用者應用程式節點上均有可用的資料庫 jar 檔案。對於 PostgreSQL，postgresql-9.4.1212.jar 位於 /opt/netiq/idm/postgres。

Identity Applications 使用萬能金鑰來加密敏感性資料。在 Identity Applications 組態期間，安裝程式將建立新的萬能金鑰。在叢集中，使用者應用程式叢集要求每個使用者應用程式例項都使用相同的萬能金鑰。萬能金鑰儲存在 /opt/netiq/idm/apps/tomcat/conf/ 目錄中 ism-configuration.properties 檔案內的內容 com.novell.idm.masterkey 下。

如需詳細說明，請參閱第 9.3 節「安裝 Identity Applications」(第 88 頁)。

4. 在節點 2 上，安裝並設定 Identity Applications。

在安裝期間，請確定：

- ◆ 選取現有資料庫選項
- ◆ 提供唯一的工作流程引擎 ID。例如，節點 2。
- ◆ 叢集中的所有使用者應用程式節點上均有可用的資料庫 jar 檔案。對於 PostgreSQL，postgresql-9.4.1212.jar 位於 /opt/netiq/idm/postgres。

完成節點 2 上的使用者應用程式組態後，複製節點 1 的 ism-configuration.properties 中的萬能金鑰值，並取代節點 2 的 ism-configuration.properties 中儲存的相應萬能金鑰值。萬能金鑰儲存在 ism-configuration.properties (/opt/netiq/idm/apps/tomcat/conf/) 中的內容 "com.novell.idm.masterkey" 下。

5. 在單獨的電腦上安裝 SSPR。

安裝前請記下以下設定，並在安裝過程中指定這些設定：

完成 SSPR 安裝後，依次啟動 Tomcat 和 SSPR (<http://<IP>:<連接埠>/sspr/private/config/> ConfigEditor)，然後登入其中。按一下組態編輯器 > 設定 > 安全性 > 重新導向白名單。

- a. 按一下新增值並指定以下 URL：

OSP：http://<dns of the failover>:<port>/osp

- b. 儲存變更。

- c. 在 SSPR「組態」頁面中，按一下設定 > OAuth SSO，然後修改 OSP 連結 - 以安裝負載平衡器軟體的伺服器的 DNS 名稱取代 IP 位址。

- d. 按一下設定 > 應用程式，然後更新轉遞和登出 URL - 以安裝負載平衡器軟體的伺服器的 DNS 名稱取代 IP 位址。

- e. 若要在節點 1 上更新 SSPR 資訊，請啟動位於 /opt/netiq/idm/apps/UserApplication/configupdate.sh 的組態公用程式。

- f. 按一下 SSO 用戶端 > Self Service Password Reset，輸入用戶端 ID、密碼和 OSP Auth 重新導向 URL 參數的值。如需詳細資訊，請參閱第 22.3 節「針對分散式環境或叢集環境更新儀表板中的 SSPR 連結」(第 208 頁)。

---

附註：驗證節點 2 中是否更新了這些參數的值。

---

6. 在節點 1 中，停止 Tomcat，並使用以下指令指定負載平衡器伺服器的 DNS 名稱，以產生新 osp.jks 檔案：

```
/opt/netiq/idm/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：/opt/netiq/idm/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。

---

7. (視情況而定) 若要驗證 osp.jks 檔案是否已透過這些變更更新，請執行以下指令：

```
/opt/netiq/idm/jre/bin/keytool -list -v -keystore osp.jks -storepass changeit
```

8. 備份位於 /opt/netiq/idm/apps/osp\_sspr/osp/ 中的原始 osp.jks 檔案，並將新 osp.jks 檔案複製到此位置。
9. 將節點 1 上位於 /opt/netiq/idm/apps/osp\_sspr/osp/ 中的新 osp.jks 文件複製到叢集中的其他使用者應用程式節點上。
10. 在節點 1 中啟動組態公用程式，並在「SSO 用戶端」索引標籤下將所有 URL 設定 (例如抵達頁面的 URL 連結和 OAuth 重新導向 URL) 變更為負載平衡器 DNS 名稱。
- a. 儲存在組態公用程式中所做的變更。
  - b. 若要在叢集的所有其他節點中反映此變更，請將節點 1 上位於 /TOMCAT\_INSTALLED\_HOME/conf 中的 ism-configuration properties 檔案複製到叢集中的其他使用者應用程式節點上。

---

**附註：**您之前已將節點 1 上的 ism.properties 檔案複製到叢集中的其他節點上。如果您在使用者應用程式安裝期間指定了自訂安裝路徑，請在叢集節點中使用組態更新公用程式確保參考路徑正確。

此情境中，OSP 和使用使用者應用程式安裝在同一部伺服器上；因此，為重新導向 URL 使用了相同的 DNS 名稱。

如果 OSP 和使用使用者應用程式安裝在不同的伺服器上，請將 OSP URL 變更為指向負載平衡器的不同 DNS 名稱。請對安裝了 OSP 的所有伺服器執行此操作。執行此操作可確保所有 OSP 申請均透過負載平衡器發送到 OSP 叢集 DNS 名稱。這涉及到為 OSP 節點建立一個單獨的叢集。

---

11. 在位於 /TOMCAT\_INSTALLED\_HOME/bin/ 目錄下的 setenv.sh 檔案中執行以下動作：
- a. 為確保 mcast\_addr 繫結成功，JGroups 要求將 preferIPv4Stack 內容設定為 true。為此，請在所有節點上的 setenv.sh 檔案中新增 JVM 內容「-Djava.net.preferIPv4Stack=true」。
  - b. 在節點 1 上的 setenv.sh 檔案中新增 -Dcom.novell.afw.wf.Engine-id="Engine1"。同樣，為叢集中的每個節點新增唯一的引擎名稱。例如，對於節點 2，您可以新增引擎名稱 Engine2。
12. 在使用者應用程式中啟用叢集。
- a. 在節點 1 上啟動 Tomcat。  
不要啟動任何其他伺服器。
  - b. 以使用者應用程式管理員身分登入使用者應用程式。
  - c. 按一下「管理」索引標籤。  
使用者應用程式將顯示應用程式組態入口網站。
  - d. 按一下快取。

使用者應用程式將顯示「快取管理」頁面。

- e. 為啟用叢集內容選取 **True**。
- f. 按一下**儲存**。
- g. 重新啟動 Tomcat。

---

**附註：**如果您已選取「啟用本地」設定，請針對叢集中的每個伺服器重複此程序。

使用者應用程式叢集使用 JGroups 在採用預設 UDP 的節點間進行快取同步。如果您要將此通訊協定變更為使用 TCP，請參閱《[NetIQ Analyzer for Identity Manager Administration Guide](#)》(NetIQ Analyzer for Identity Manager 管理指南) 中的「[Portal Configuration Tasks](#)」(入口網站組態任務)。

---

13. 為叢集啟用許可權索引。

- a. 在節點 1 中登入 iManager，然後導覽至檢視物件。
- b. 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。
- c. 選取 **AppConfig > AppDefs > > 組態**
- d. 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>
```

- e. 按一下**確定**。

14. 啟用 Tomcat 叢集。

在所有叢集節點上開啟 /TOMCAT\_INSTALLED\_HOME/conf/ 中的 Tomcat server.xml 檔案，並取消注釋此檔案中的下行：

```
<Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
```

對於進階 Tomcat 叢集組態，請依照 <https://tomcat.apache.org/tomcat-8.5-doc/cluster-howto.html> 中的步驟操作。

15. 在所有節點上重新啟動 Tomcat。

16. 為叢集設定使用者應用程式驅動程式。

在叢集中，必須將使用者應用程式驅動程式設定為使用叢集負載平衡器的 DNS 名稱。可使用 iManager 來設定使用者應用程式驅動程式。

- a. 登入用於管理 Identity Manager 引擎的 iManager。
- b. 在 iManager 導覽框架中，按一下 **Identity Manager** 節點。
- c. 按一下 **Identity Manager 綜覽**。
- d. 使用搜尋網頁顯示「Identity Manager 綜覽」，以尋找包含使用者應用程式驅動程式及角色與資源服務驅動程式的驅動程式集。
- e. 按一下驅動程式圖示右上角的圓形狀態指示器：  
一個功能表即會顯示，其中列出了用於啟動和停止驅動程式以及編輯驅動程式內容的指令。
- f. 選取**編輯內容**。
- g. 在「驅動程式參數」區段中，將主機變更為發送器的主機名稱或 IP 位址。

- h. 按一下**確定**。
  - i. 重新啟動驅動程式。
- 17. 若要變更角色與資源服務驅動程式的 URL，請重複步驟 18a 至 18f，然後按一下**驅動程式組態**，並以負載平衡器 DNS 名稱更新使用者應用程式 URL。
- 18. 確認針對使用者應用程式節點的負載平衡器軟體中建立的叢集啟用了工作階段綁定。
- 19. 在 Identity Manager 儀表板上設定用戶端設定。如需詳細資訊，請參閱《[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)》(NetIQ Identity Manager - Identity Applications 管理員指南) 中的「[Configuring Client Settings Mode](#)」(設定用戶端設定模式)。