NetIQ® Identity Manager
セットアップガイド (Windows 用)

2019 年 10 月

保証と著作権

NetIQ の保証と著作権、免責事項、保証、輸出およびその他の使用制限、米国政府の規制による権利、特許ポリシー、および FIPS コンプライアンスの詳細については、https://www.netiq.com/company/legal/ を参照してください。

Copyright (C) 2019 NetIQ Corporation. **All rights reserved.**

目次

本書およびライブラリについて **11**
NetIQ 社について **13**

ページのパート I Identity Manager 環境の概要 **17**

1 Identity Manager コンポーネントの簡単な紹介 **19**

Identity Manager サーバのコンポーネント . . . 20
Identity Manager サーバ . . . 21
リモートローダ . . . 22
ファンアウトエージェント . . . 22
iManager . . . 22
Identity アプリケーションのコンポーネント . . . 23
ユーザアプリケーション . . . 23
認証サービス . . . 24
Self-Service Password Reset . . . 24
Web アプリケーションサーバ . . . 24
Identity Applications データベース . . . 25
Identity Applications 用のドライバ . . . 25
Identity Reporting のコンポーネント . . . 26
Identity Reporting . . . 26
認証サービス . . . 26
Self-Service Password Reset . . . 27
Identity Reporting データベース . . . 27
Web アプリケーションサーバ . . . 27
Identity Reporting 用のドライバ . . . 28
Sentinel Log Management for Identity Governance and Administration . . . 28
Identity Manager ツール . . . 29
Designer for Identity Manager . . . 29
Identity Manager 用の Analyzer . . . 29
機能アーキテクチャ . . . 30
Identity Manager の展開オプション . . . 31
Identity Manager 展開のサンプル . . . 32
Advanced Edition 展開のサンプル . . . 34
Standard Edition 展開のサンプル . . . 36

ページのパート II Identity Manager のインストールの計画 **39**

2 インストールの計画 **41**

ハードウェア要件の決定 . . . 41
展開計画ワークシート . . . 42
サイズ決定ワークシート . . . 42
アーキテクチャワークシート . . . 43
システム要件ワークシート . . . 44
Identity Manager コンポーネントが使用するポートの確認 . . . 44

ページのパート III Identity Manager コンポーネントのインストールと設定 47

3 インストールおよび設定プロセスの概要 49

インストールの順序 . . . 49
Identity Manager サーバ、Identity Applications、および Identity Reporting コンポーネントのインストールおよび設定プロセスの理解 . . . 49
インストール方法のタイプ . . . 50
インストールオプション . . . 50
設定モードのタイプ . . . 51
設定時における直感的でないパスワードの使用 . . . 51
Designer および Analyzer のインストールプロセスの理解 . . . 51
インストール手順 . . . 51
Identity Manager サーバ、Identity Applications、および Identity Reporting のインストール手順 . . . 52
リモートローダのインストール . . . 53
Java リモートローダのインストール . . . 54
SSPR のインストール . . . 56
環境設定の理解 . . . 57
Identity Manager エンジンの環境設定ワークシート . . . 57
Identity Applications の環境設定ワークシート . . . 59
Identity Reporting の環境設定ワークシート . . . 61
Self-Service Password Reset の環境設定ワークシート . . . 64
インストール後の手順 . . . 65
preferIPv4Stack プロパティを JVM に渡す . . . 65
サーバのヘルスの確認 . . . 65
ヘルスの統計の監視 . . . 66
複合インデックスの作成 . . . 66
クライアントが開始した SSL 再ネゴーシエーションを拒否するように Identity Applications を設定する . . . 68

4 インストールを完了するための最終ステップ 69

Identity Vault の設定 . . . 69
アイデンティティボールトへの Identity Applications および Identity Reporting 証明書の手動インポート . . . 69
リモートローダとドライバの設定 . . . 70
パスワードを忘れた場合の管理の設定 . . . 70
Self Service Password Reset によるパスワードを忘れた場合の管理 . . . 70
外部システムによるパスワードを忘れた場合の管理 . . . 73
分散環境またはクラスタ化環境におけるダッシュボードの SSPR リンクの更新 . . . 74
識別情報アプリケーションのデータベースの設定 . . . 75
Oracle データベースの設定 . . . 75
SQL Server データベースの設定 . . . 77
識別情報アプリケーションの設定 . . . 78
識別情報アプリケーションの設定の管理 . . . 78
識別情報アプリケーション用の REST API の展開 . . . 102
Oracle サービス名を使用した Oracle データベースへのアクセス . . . 102
手動によるデータベーススキーマの作成 . . . 103
識別情報アプリケーションのシングルサインオン設定の管理 . . . 105
識別情報アプリケーションの起動 . . . 105
識別情報アプリケーションの設定と使用方法の検討事項 . . . 105
データ収集用のランタイム環境の設定 . . . 106

識別情報アプリケーションからのデータ収集に関するデータ収集サービスドライバの設定 106
データ収集サービスドライバの移行 . . . 107
カスタム属性とカスタムオブジェクトのサポートの追加 . . . 109
複数のドライバセットのサポートの追加 . . . 112
SSL を使用したリモートモードでのドライバ実行設定 . . . 114
Identity Reporting の設定 . . . 115
［Identity Data Collection Services (アイデンティティデータ収集サービス)］ページへのデータソースの手動追加 . . . 116
Oracle データベースでのレポートの実行 . . . 116
データベーススキーマの手動生成 . . . 116
Identity Reporting 用の REST API の展開 . . . 119
リモート PostgreSQL データベースへの接続 . . . 119
Identity Manager のアクティベート . . . 120
Identity Manager コンポーネントが使用するポートの確認 . . . 121

ページのパート IV Designer のインストール 125

5 Designer のインストールの計画 127

Designer のインストールチェックリスト . . . 127

6 Designer のインストール 129

Windows の実行可能ファイルの実行 . . . 129
サイレントインストールプロセスの使用 . . . 129
スペース文字が含まれるインストールパスの変更 . . . 130

ページのパート V Analyzer のインストール 131

7 Analyzer のインストールの計画 133

Analyzer のインストールチェックリスト . . . 133

8 Analyzer のインストール 135

Windows の実行可能ファイルの実行 . . . 135
サイレントインストールプロセスの使用 . . . 135

9 インストール後のタスク 137

接続システムの設定 . . . 137
ドライバセットの作成と設定 . . . 137
ドライバセットの作成 . . . 138
デフォルトのパスワードポリシーのドライバセットへの割り当て . . . 138
アイデンティティボールトでのパスワードポリシーオブジェクトの作成 . . . 139
カスタムパスワードポリシーの作成 . . . 139
アイデンティティボールトでのデフォルト通知コレクションオブジェクトの作成 . . . 140
ドライバの作成 . . . 140
ポリシーの定義 . . . 141
ドライバアクティビティの管理 . . . 141
Identity Manager のアクティベート . . . 141

ページのパート VI Identity Manager のアップグレード 143

10 Identity Manager のアップグレードの準備 145

Identity Manager のアップグレードのチェックリスト . . . 145
アップグレードとマイグレーションの理解 . . . 147
アップグレードの順序 . . . 149
サポートされているアップグレードパス . . . 149
Identity Manager 4.7.x バージョンからのアップグレード . . . 149
Identity Manager 4.6.x バージョンからのアップグレード . . . 151
現在の設定のバックアップ . . . 153
Designer のプロジェクトのエクスポート . . . 154
ドライバの環境設定のエクスポート . . . 155

11 Identity Manager コンポーネントのアップグレード 157

Designer のアップグレード . . . 157
Identity Manager エンジンコンポーネントのアップグレード . . . 158
アイデンティティボールトのアップグレード . . . 158
Identity Manager エンジンのアップグレード . . . 160
リモートローダのアップグレード . . . 162
Java リモートローダのアップグレード . . . 163
iManager のアップグレード . . . 163
Identity Applications のアップグレード . . . 166
アップグレードプログラムについて . . . 167
アップグレードの前提条件 . . . 167
システム要件 . . . 167
PostgreSQL データベースのアップグレード . . . 167
Identity Applications のドライバパッケージのアップグレード . . . 170
Identity Applications のアップグレード . . . 170
アップグレード後のタスク . . . 171
Identity Reporting のアップグレード . . . 175
アップグレードの前提条件 . . . 175
Identity Reporting のアップグレード . . . 175
Reporting のアップグレード後の手順 . . . 176
データベースにおける reportRunner への参照の変更 . . . 176
Identity Reporting のアップグレードの検証 . . . 177
Analyzer のアップグレード . . . 177
Identity Manager ドライバの停止と起動 . . . 178
ドライバの停止 . . . 178
ドライバの起動 . . . 179
Identity Manager ドライバのアップグレード . . . 180
新しいドライバの作成 . . . 180
既存のコンテンツをパッケージのコンテンツと交換 . . . 181
現在のコンテンツを維持しつつパッケージを使用する新しいコンテンツを追加 . . . 181
新しいサーバをドライバセットに追加する . . . 182
新しいサーバをドライバセットに追加する . . . 182
ドライバセットから古いサーバを削除する . . . 183
ドライバへのカスタムポリシーとルールの復元 . . . 184
Designer を使用したドライバへのカスタムポリシーとルールの復元 . . . 184
iManager を使用したドライバへのカスタムポリシーおよびルールの復元 . . . 185

12 Advanced Edition から Standard Edition への切り替え 187

ページのパート VII Identity Manager のデータの新しいインストールへのマイグレート 189

13 Identity Manager をマイグレートする準備 191

マイグレーションを実行するためのチェックリスト . . . 191

14 Identity Manager の新しいサーバへのマイグレート 193

Identity Manager のマイグレーションのチェックリスト . . . 193
Designer プロジェクトのマイグレーションの準備 . . . 194
ドライバセットのサーバ固有情報のコピー . . . 195
Designer でサーバ固有の情報をコピーする . . . 195
iManager でサーバ固有の情報を変更する . . . 196
ユーザアプリケーションのサーバ固有の情報を変更する . . . 197
Identity Manager エンジンの新しいサーバへのマイグレート . . . 197
ユーザアプリケーションドライバのマイグレート . . . 197
新しいベースパッケージのインポート . . . 197
既存のベースパッケージのアップグレード . . . 198
マイグレートしたドライバの展開 . . . 198
識別情報アプリケーションのアップグレード . . . 199
Identity Applications の移行 . . . 199
データベースの新しいサーバへの移行 . . . 200
新しいサーバへの Identity Applications のインストール . . . 201
識別情報アプリケーションのマイグレーションの完了 . . . 201
SQL ファイルを実行する Oracle データベースの準備 . . . 201
ブラウザのキャッシュのフラッシュ . . . 202
SharedPagePortlet の最大タイムアウト設定の更新 . . . 203
グループの自動クエリ設定の無効化 . . . 203

ページのパート VIII Microsoft Azure での Identity Manager の展開 205

15 Microsoft Azure での Identity Manager の計画と実装 207

前提条件 . . . 207
展開手順 . . . 207
リソースグループの作成 . . . 209
仮想ネットワークとサブネットの作成 . . . 209
アプリケーションゲートウェイの作成 . . . 210
仮想マシンインスタンスの作成 . . . 212
VM のホストエントリの更新 . . . 214
Designer の設定 . . . 215
アプリケーションゲートウェイの設定 . . . 215

16 ハイブリッド Identity Manager のシナリオの例 219

マルチサーバドライバセット接続の使用 . . . 219
eDirectory ドライバ接続の使用 . . . 220

17 Identity Manager のコンポーネントのアンインストール 223

識別ボールトのアンインストール . . . 223
識別ボールトからのオブジェクトの削除 . . . 224
Identity Manager エンジンのアンインストール . . . 224
リモートローダのアンインストール . . . 225
Identity Applications のアンインストール . . . 225
Roles Based Provisioning Module のドライバの削除 . . . 225
Identity Applications のアンインストール . . . 226
Identity Reporting のコンポーネントのアンインストール . . . 226
レポーティングドライバの削除 . . . 227
Identity Reporting のアンインストール . . . 227
Analyzer のアンインストール . . . 228
iManager のアンインストール . . . 228
Windows での iManager のアンインストール . . . 228
iManager ワークステーションのアンインストール . . . 229
Designer のアンインストール . . . 229

18 トラブルシューティング 231

Identity Manager エンジンのトラブルシューティング . . . 231
Identity Applications および RBPM インストールのトラブルシューティング . . . 232
インストールとアンインストールのトラブルシューティング . . . 235
ログインのトラブルシューティング . . . 240
SSPR のページ要求エラーのトラブルシューティング . . . 243
Windows 2016 で .NET リモートローダが起動しない問題のトラブルシューティング . . . 243
Azure 展開でフォームをロードするときの 502 不正なゲートウェイのトラブルシューティング . 243

ページのパート IX 高可用性のための Identity Manager の展開 245

19 クラスタ環境における Identity Manager のインストールの準備 247

前提条件 . . . 247
識別ボールト . . . 247
識別情報アプリケーション . . . 248
Identity Applications のデータベース . . . 248
識別情報アプリケーションで使用するクラスタの準備 . . . 249
Tomcat 環境のクラスタグループの理解 . . . 249
ワークフローエンジン ID のシステムプロパティの設定 . . . 249
クラスタ内の各ユーザアプリケーションでの同じマスタキーの使用 . . . 250

20 Identity Manager のクラスタ展開ソリューションのサンプル 251

前提条件 . . . 251
eDirectory クラスタでの NetIQ Identity Manager の設定 . . . 251
リモートローダのクラス化 . . . 252

21 Identity Applications のクラスタ展開ソリューションのサンプル 253

前提条件 . . . 254
インストール手順 . . . 255

クラスタリングのパーミッションインデックスの有効化 261

本書およびライブラリについて

このセットアップガイドには、NetIQ Identity Manager (Identity Manager) 製品のインストール手順が記載されています。このガイドでは、分散環境に個々のアプリケーションをインストールするプロセスについて説明します。

本書の読者

本書は、組織の識別情報管理ソリューションの構築に必要なコンポーネントのインストールを行う識別情報アーキテクトおよび識別情報管理者向けの情報を提供します。

ライブラリに含まれているその他の情報

Identity Manager のライブラリの詳細については、Identity Manager マニュアルの Web サイトを参照してください。

NetIQ 社について

当社はグローバルなエンタープライズソフトウェア企業であり、お客様の環境において絶えず挑戦となる変化、複雑さ、リスクという 3 つの要素に焦点を当て、それらをお客様が制御するためにどのようにサポートできるかを常に検討しています。

当社の観点

変化に適応すること、複雑さとリスクを管理することは普遍の課題

実際、直面するあらゆる課題の中で、これらは、物理環境、仮想環境、およびクラウドコンピューティング環境の安全な評価、監視、および管理を行うために必要な制御を脅かす最大の要因かもしれません。

重要なビジネスサービスの改善と高速化を可能にする

当社は、IT 組織に可能な限りの制御能力を付与することが、よりタイムリーでコスト効率の高いサービス提供を実現する唯一の方法だと信じています。組織が継続的な変化を遂げ、組織を管理するために必要なテクノロジが実質的に複雑さを増していくにつれ、変化と複雑さという圧力はこれからも増え続けていくことでしょう。

当社の理念

単なるソフトウェアではなく、インテリジェントなソリューションを販売する

確かな制御手段を提供するために、まずお客様の IT 組織が日々従事している現実のシナリオを把握することに努めます。そのようにしてのみ、実証済みで測定可能な結果を成功裏に生み出す、現実的でインテリジェントな IT ソリューションを開発することができます。これは単にソフトウェアを販売するよりもはるかにやりがいのあることです。

当社の情熱はお客様の成功を推し進めること

お客様が成功するためにわたしたちには何ができるかということが、わたしたちのビジネスの核心にあります。製品の着想から展開まで、当社は次のことを念頭に置いています。お客様は既存資産とシームレスに連動して動作する IT ソリューションを必要としており、展開後も継続的なサポートとトレーニングを必要とし、変化を遂げるときにも共に働きやすいパートナーを必要としています。究極的に、お客様の成功こそがわたしたちの成功なのです。

当社のソリューション

- ID およびアクセスのガバナンス
- アクセス管理

- セキュリティ管理
- システムおよびアプリケーション管理
- ワークロード管理
- サービス管理

セールスサポートへのお問い合わせ

製品、価格、および機能についてのご質問は、各地域のパートナーへお問い合わせください。パートナーに連絡できない場合は、弊社のセールスサポートチームへお問い合わせください。

各国共通 :	www.netiq.com/about_netiq/officelocations.asp
米国およびカナダ :	1-888-323-6768
電子メール :	info@netiq.com
Web サイト :	www.netiq.com

テクニカルサポートへのお問い合わせ

特定の製品に関する問題については、弊社のテクニカルサポートチームへお問い合わせください。

各国共通 :	www.netiq.com/support/contactinfo.asp
北米および南米 :	1-713-418-5555
ヨーロッパ、中東、アフリカ :	+353 (0) 91-782 677
電子メール :	support@netiq.com
Web サイト :	www.netiq.com/support

マニュアルサポートへのお問い合わせ

弊社の目標は、お客様のニーズを満たすマニュアルの提供です。本製品のマニュアルは、NetIQ Web サイトから HTML 形式および PDF 形式で入手することができます。ログインしなくてもマニュアルページにアクセスできます。マニュアルを改善するためのご提案がございましたら、**www.netiq.com/documentation** に掲載されている本マニュアルの HTML 版で、各ページの下にある［comment on this topic］をクリックしてください。Documentation-Feedback@netiq.com 宛てに電子メールを送信することもできます。貴重なご意見をぜひお寄せください。

オンラインユーザコミュニティへのお問い合わせ

NetIQ のオンラインコミュニティである NetIQ Communities は、他のユーザや NetIQ のエキスパートとやり取りできるコラボレーションネットワークです。NetIQ Communities では、より迅速な情報、役立つリソースへの便利なリンク、および NetIQ エキスパートとのやり取りの場を提供しています。事業成功の鍵である IT への投資効果を最大にするために必要な知識が確実に身につけられるよう手助けしています。詳細については、https://www.netiq.com/communities/ を参照してください。

Identity Manager 環境の概要

このガイドでは、Identity Manager をインストールおよび設定するために完了する必要のあるタスクに焦点を当てています。インストールを開始する前に

NetIQ Identity Manager を初めて使用する場合は、以下のセクションの情報を使用して、ソリューションとそれを構成するコンポーネントを理解してください。ダウンロードしてインストールできるコンポーネントは、Identity Manager Edition によって決まります。

- Identity Manager コンポーネントの簡単な紹介
- 機能アーキテクチャ

1 Identity Manager コンポーネントの簡単な紹介

お客様のさまざまなニーズに対応するために、Identity Manager は Advanced Edition と Standard Edition で利用可能です。各エディションは特定の機能セットで構成され、各機能は複数のコンポーネントによって処理されます。したがって、Identity Manager の実装には、要件に応じて次のコンポーネントの 1 つまたはすべてを含めることができます。

- Identity Manager サーバ
- 識別情報アプリケーション
- Identity Reporting
- Identity Manager ツール

図 1-1 には、Identity Manager Advanced Edition 環境に展開されるコンポーネントが示されています。

図 1-1 *Identity Manager Advanced Edition のコンポーネント*

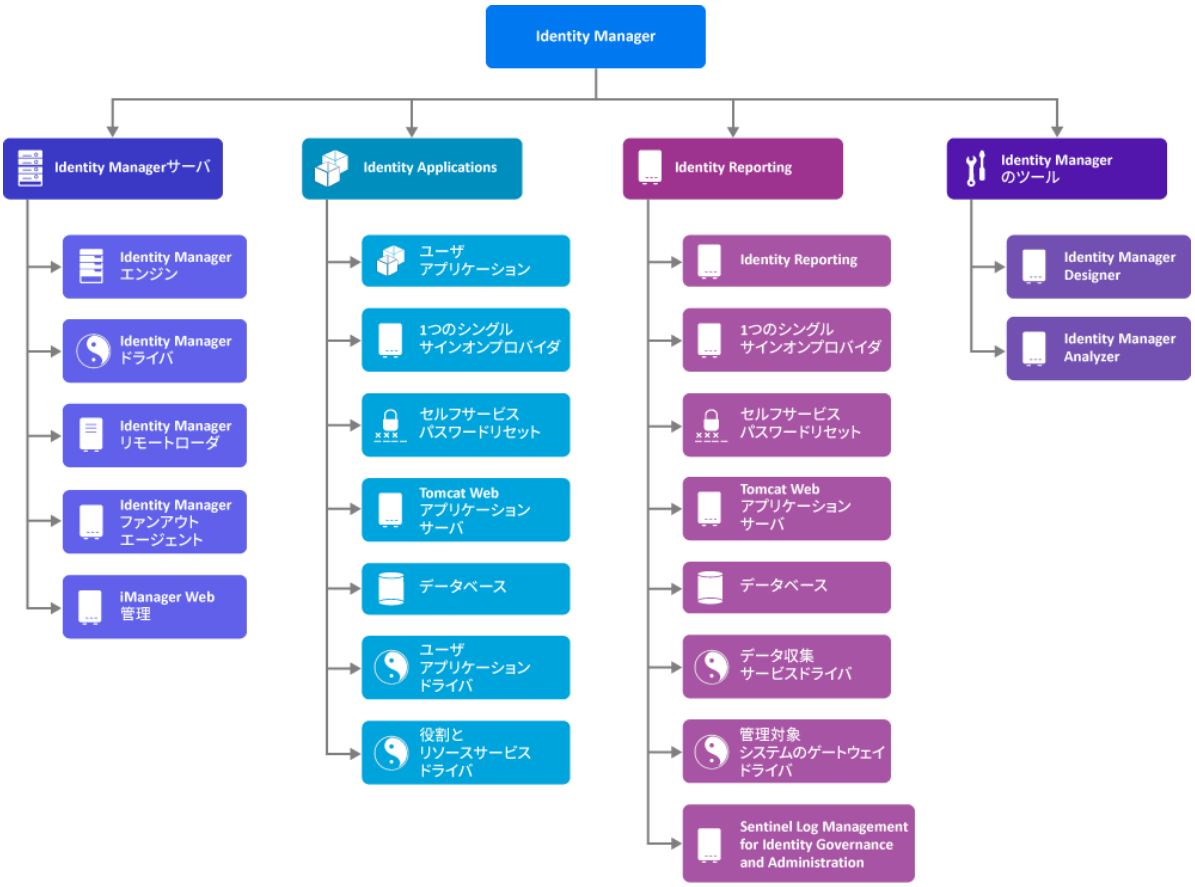
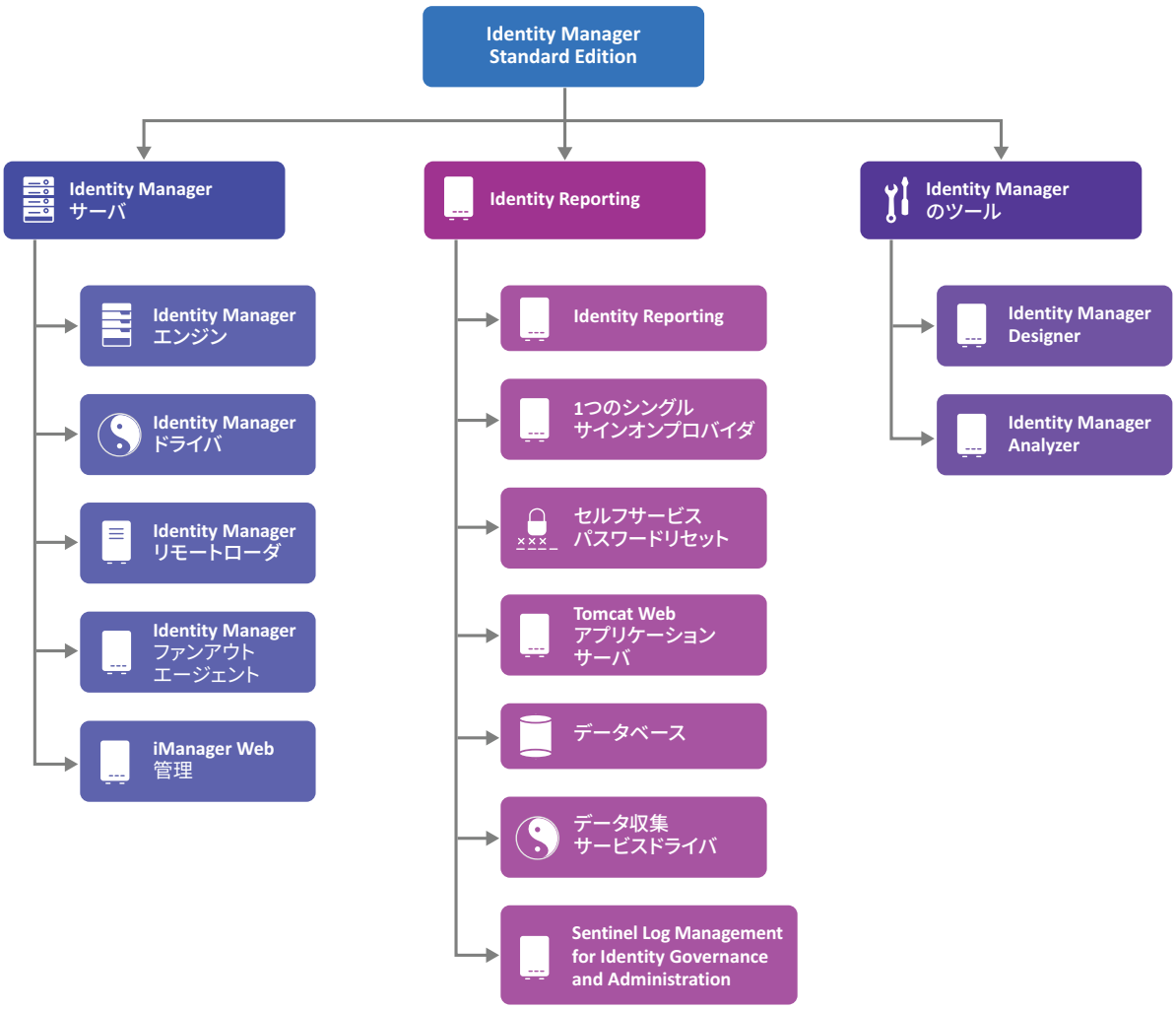


図 1-2 には、Identity Manager Standard Edition 環境に展開されるコンポーネントが示されています。

図 1-2 *Identity Manager Standard Edition のコンポーネント*



コンポーネント同士の相互作用に基づいて、一部のコンポーネントはコンポーネントのグループとして論理的にインストールされます。一部のコンポーネントは、インストール操作を簡単にするためにスタンドアロンコンポーネントとしてインストールされます。コンポーネントが互いにどのように相互作用するかについては、『NetIQ Identity Manager Overview and Planning Guide』を参照してください。

後続のセクションの情報を確認し、コンポーネントをグループ化する方法および各コンポーネントまたはコンポーネントのグループをインストールする方法を理解してください。

Identity Manager サーバのコンポーネント

すべてのインストールに必要

Identity Manager Server インストールは、以下のコンポーネントで構成されています。

Identity Manager サーバ

Identity Manager Server は Identity Manager 内でタスクを実行します。Identity Vault、Identity Manager エンジン、および Identity Manager ドライバで構成されます。

Identity Manager Server の操作をサポートするために、インストールプログラムによって、サポートされているバージョンの Oracle Java Runtime Environment (JRE) がインストールされます。Identity Manager Server コンポーネントをインストールするには、インストールプログラムの **[Identity Manager エンジン]** インストールオプションを使用します。

識別ボールト

Identity Manager エンジンをインストールすると、インストールプロセスによって Identity Vault への接続が作成および設定されます。Identity Manager は、すべての識別情報データのデフォルトリポジトリとして Identity Vault を使用します。識別情報データには、ユーザアカウントと組織データを含む、管理された識別情報の現在の状態が含まれます。

Identity Manager エンジン

Identity Manager エンジンは、識別ボールトまたは接続アプリケーションで発生するすべてのデータ変更を処理します。Identity Manager エンジンが実行されているサーバを Identity Manager サーバと呼びます。

Identity Manager ドライバ

Identity Manager Server はユーザのプロビジョニングを処理し、ドライバを介して接続されたシステムアカウントとグループを管理します。ドライバは、接続されたシステムへのソフトウェアインタフェースです。

Identity Manager ドライバは、Identity Manager Server アーキテクチャの一部として実行されます。ドライバは、ネイティブエンドポイントタイプシステムテクノロジへのゲートウェイとして機能します。たとえば、Active Directory Services を実行しているコンピュータを管理できるのは、Active Directory ドライバが、Identity Manager サーバまたは Identity Manager サーバが通信できるターゲットアプリケーションサーバにインストールされている場合のみです。ドライバは、接続されたシステムに存在するオブジェクトを管理します。管理対象オブジェクトには、アカウント、グループ、およびオプションでエンドポイントタイプ固有のオブジェクトが含まれます。

ドライバは、Identity Manager エンジンのアクションを、「Microsoft Exchange 接続システムでの新しい電子メールアカウントの作成」などの接続システムでの変更に変換します。Identity Manager で設定されているすべてのドライバにはイベントキャッシュファイル (TAO ファイル) が関連付けられています。イベントは、ドライバによって処理される前に、キャッシュファイルにキャッシュされます。デフォルトでは、キャッシュファイルは Identity Vault の DIB (Data Information Base) ディレクトリに配置されます。

Identity Manager には、さまざまなタイプの接続システムとの接続を管理するためにいくつかのドライバ (Java、ネイティブ、.NET) が組み込まれています。また、Identity Manager には、カスタムドライバを開発する機能も用意されています。これにより、自家製のアプリケーションや、テクノロジインタフェースがなくすぐに使用できるドライバを利用できないリポジトリなど、さまざまな他のシステムとのデータ同期が可能になります。

リモートローダ

ドライバは、Identity Manager Server にローカルでインストールするか、リモートローダを使用してインストールできます。リモートローダはドライバをロードし、リモートサーバにインストールされているドライバの代わりに Identity Manager エンジンと通信します。アプリケーションを Identity Manager エンジンと同じサーバで実行する場合、そのサーバにドライバをインストールできます。一方、アプリケーションを Identity Manager エンジンと同じサーバで実行しない場合は、ドライバをアプリケーションサーバにインストールする必要があります。ご使用の環境のワークロードを軽減したり、設定を容易にしたりする場合、リモートローダを Tomcat および Identity Manager サーバとは別のサーバにインストールできます。リモートローダの詳細については、『NetIQ Identity Manager Driver Administration Guide』の「リモートローダを使用するタイミングの決定」を参照してください。

[Identity Manager リモートローダサーバ] インストールオプションを使用して、リモートローダサービスとドライバインスタンスをリモートローダにインストールします。

ファンアウトエージェント

Identity Manager ファンアウトエージェントは、Java Database Connectivity (JDBC) ファンアウトドライバが複数の JDBC ファンアウトドライバインスタンスを作成するために使用するインストールコンポーネントです。ファンアウトドライバは、最小限の手間で複数のデータベースにユーザ、グループ、およびパスワードをプロビジョニングします。これにより、Identity Manager 管理者が同じポリシーを使用して複数の JDBC ドライバを設定し、同じタイプの複数のデータベースをプロビジョニングする必要がなくなります。ユーザアカウントを一元管理し、必要に応じて自動的に作成、設定、保守、および削除することができます。詳細については、『*NetIQ Identity Manager Driver for JDBC Fanout Implementation Guide*』を参照してください。

ファンアウトエージェントをインストールするには、インストールプログラムの **[Identity Manager ファンアウトエージェント]** インストールオプションを使用します。

iManager

Novell iManager はブラウザベースのツールで、Identity Manager など、数多くの Novell および NetIQ 製品を単一点で管理できます。iManager を使用して、Identity Manager Identity Applications では管理できない、Identity Manager Server のオプションやドライバ属性の管理などの管理タスクを実行できます。iManager の詳細については、『*NetIQ iManager 管理ガイ*

ド』を参照してください。iManager 用の Identity Manager プラグインをインストールした後は、Identity Manager を管理できるだけでなく、Identity Manager システムに関するリアルタイムのヘルスおよびステータス情報を受信できます。

iManager では Designer と同様のタスクを実行できるほか、システムのヘルスも監視できます。NetIQ では、管理タスクに iManager を使用することをお勧めします。Designer はパッケージへの変更、モデリング、および展開前のテストを必要とする設定タスクに使用してください。

Identity Manager では、iManager を使用した Identity Manager プラグインのインストールが必要です。Identity Manager は、iManager クライアントと Identity Manager プラグインをインストールする単一のインストーラを提供します。iManager は Identity Manager サーバまたは別のコンピュータにインストールできます。

iManager をインストールするには、インストールプログラムの iManager Web 管理インストールオプションを使用します。

ヒント : コンポーネントについて学習した後、運用環境で使用するためにコンポーネントがどのようにインストールおよび設定されているかを十分に理解する必要があります。

Identity アプリケーションのコンポーネント

Advanced Edition のインストールに必要

Identity アプリケーションは、ブラウザベースの複数の Web アプリケーションが相互接続されたセットです。これにより、組織では、ユーザが利用できるさまざまな役割とリソースに関連付けられたユーザアカウントおよび許可を管理することができます。役割の要求やパスワードの変更など、ユーザに対してセルフサービスサポートを提供するように Identity アプリケーションを設定することができます。役割とリソースの管理および割り当ての効率が向上するようにワークフローを設定することも可能です。Identity アプリケーションは、管理コンソール (管理タスク用)、ユーザコンソール (ダッシュボード)、およびこれらのタスクの実行に役立つ REST サービスで構成されています。

注 : Identity アプリケーションをインストールする前に、Identity Manager エンジンをインストールしておく必要があります。

Identity アプリケーションコンポーネントをインストールするには、インストールプログラムの **[Identity アプリケーション]** インストールオプションを使用します。

Identity アプリケーションインストールは、以下のコンポーネントで構成されています。

ユーザアプリケーション

ユーザアプリケーションはブラウザベースの Web アプリケーションで、さまざまな識別情報セルフサービスタスクと役割プロビジョニングタスクを実行できます。製品の以前のバージョンでユーザアプリケーションインタフェースを使用して実行されたタスクの一部は、管理コンソールとユーザコンソールを含む新しいユーザインタフェースに移動されま

した。ユーザアプリケーションは、新しいユーザインタフェースにはまだ存在しない機能の一部を引き続き提供します。詳細については、『NetIQ Identity Manager - Identity アプリケーションに対する管理者ガイド』を参照してください。

認証サービス

認証サービスは、Identity アプリケーション機能へのアクセスを提供します。Identity Manager でのシングルサインオンアクセスの使用の詳細については、『NetIQ Identity Manager - Administrator's Guide to the Identity Applications』を参照してください。

認証サービスは、NetIQ One Single Sign-On Provider (OSP) コンポーネントによって提供されます。Identity アプリケーションでは、OSP のローカルインストールが必要です。OSP は、Identity アプリケーションとともに自動的にインストールされます。

Self-Service Password Reset

セルフサービスパスワード管理サービスは、セルフサービスパスワード管理へのアクセスを提供します。Identity アプリケーションの NetIQ SSPR (Self Service Password Reset) は、識別情報アプリケーションにアクセスできるユーザが、管理者の助けを借りずに自分でパスワードをリセットできる機能です。

Identity アプリケーションインストールプロセスによって SSPR がデフォルトで有効になります。ただし、展開で SSPR が必要な場合、または Standard Edition をインストールする場合は、SSPR を別のコンピュータにインストールすることを選択できます。SSPR を Advanced Edition で別のコンピュータにインストールする場合、両方のコンポーネントのインストールを手動または ConfigUpdate ユーティリティを使用して完了した後、Identity アプリケーション環境設定ファイル (ism-configuration.properties) でパスワード管理設定を定義する必要があります。

Web アプリケーションサーバ

アプリケーションサーバは、Identity アプリケーションコンポーネントが実行されるランタイムフレームワークを提供します。Identity アプリケーションは、WAR (Web Application Resource または Web application ARchive) ファイルとしてパッケージ化されています。インストールプロセスにより、WAR ファイルをアプリケーションサーバに展開することができます。アプリケーションサーバは Java™ 仮想マシンを実行し、アプリケーションコードのランタイム環境を提供します。次の WAR ファイルが、Identity アプリケーションのコンポーネントの URL に適用されます。

- **IDMProv** (ユーザアプリケーションインタフェース用)
- **idmdash** (ダッシュボード用)
- **idmadmin** (Identity アプリケーション管理インタフェース用)

ユーザが idmdash または idmadmin アプリケーションを操作するとき、これらのアプリケーションは基礎となる IDMProv.war ファイルに対してクエリを実行し、ユーザの情報を取得します。IDMProv.war は REST API および SOAP API を公開します。これらの API では、idmdash および idmadmin にユーザインタフェースを提供する情報が含まれています。

Identity アプリケーションは、インストールキットに含まれている Apache Tomcat アプリケーションサーバで実行されます。Tomcat アプリケーションサーバをサポートするために、インストールプログラムはサポートされているバージョンの JRE と Apache ActiveMQ をインストールします。

Identity Applications データベース

Identity アプリケーションデータベースは、ローカライズされたラベル、エンタイトルメント値、電子メールサーバ設定など、Identity アプリケーションの環境設定データを維持します。また、ワークフローエンジンに必要なワークフロー状態データも格納します。Identity アプリケーションでサポートされているデータベースは、PostgreSQL、Oracle、および Microsoft SQL Server です。

Identity アプリケーションインストールプログラムは、Identity アプリケーションのデフォルトデータベースとして機能する、サポートされているバージョンの PostgreSQL データベースを自動的にインストールします。PostgreSQL をデータベースとして使用しない場合は、Identity アプリケーションを使用してサポートされているバージョンの Oracle または MS SQL データベースを設定できます。Identity アプリケーションには、データベースと通信するために Java Database Connectivity ドライバ (JDBC タイプ 4 ドライバ) が必要です。インストールプログラムは、データベースの JDBC ドライバの場所と名前の入力を求めます。したがって、Identity アプリケーションのインストールを開始する前に、データベースインストールディレクトリからこの JDBC ドライバを取得する必要があります。

- PostgreSQL データベースの場合、ドライバは Identity Manager インストールプログラムにバンドルされています。
- Oracle データベースの場合、Oracle Web サイトからドライバをダウンロードできます。
- Microsoft SQL Server データベースの場合、Microsoft Web サイトからドライバをダウンロードします。

データベースは、Identity アプリケーションサーバまたはリモートコンピュータにローカルに配置できます。リモートデータベースを使用する場合は、データベースへの接続を設定する必要があります。

Identity Applications 用のドライバ

Identity アプリケーションコンポーネントには、次のドライバが必要です。

ユーザアプリケーションドライバ

設定情報を格納し、識別ボールトで変更が行われた場合に Identity アプリケーションに通知します。識別ボールト内のイベントでワークフローをトリガできるようドライバを設定できます。このドライバから、ワークフローのプロビジョニングアクティビティの成否をユーザアプリケーションに通知することもできます。これにより、ユーザは要求の最終的なステータスを参照することができます。

役割とリソースのサービスドライバ

すべての役割の割り当てを管理し、承認を必要とする役割の割り当て要求のワークフローを開始し、グループまたはコンテナメンバシップに従って間接的な役割の割り当てを維持します。このドライバは、役割のメンバーシップに基づいてユーザのエンタイトルメントを付与および取り消しして、完了した要求のクリーンアップ手順を実行します。このドライバは、役割要求に加えてリソース要求も維持します。

インストールプログラムの [Identity アプリケーション] インストールオプションは、ユーザアプリケーションドライバおよび役割とリソースのサービスドライバを Identity Vault に展開します。

Identity Reporting のコンポーネント

(オプション) このコンポーネントはレポーティング機能を実装する予定がある場合にのみ、インストールしてください

Identity Reporting では、お客様のユーザのエンタイトルメントに関する完全なビューが提供され、組織内で識別情報に対して付与された権限や許可の過去および現在の状況を確認するのに必要な知識が得られます。Identity Manager は、Identity Vault および接続システムから収集された情報を含む、Identity Manager 環境のステータスを監視するために使用できる事前定義されたレポートを提供します。Identity Manager に用意されているレポートを使用するには、Identity Manager に含まれている Identity Reporting をインストールします。Identity Reporting には、カスタムレポートの作成プロセスを容易にするレポートパッケージツールも含まれています。Identity Reporting のユーザインタフェースを使用すると、パフォーマンスを最適化するために、レポートを混雑していない時間帯に実行するようスケジュールするのが楽になります。Identity Reporting の詳細については、『Administrator Guide to NetIQ Identity Reporting』を参照してください。

注 : Identity Reporting を Advanced Edition にインストールする前に、Identity アプリケーションをインストールする必要があります。

Identity Reporting インストールは、以下のコンポーネントで構成されています。

Identity Reporting

レポーティングサービスを呼び出してレポートを生成するブラウザベースのアプリケーション。レポーティングサービスは、すべてのレポート管理情報 (レポート定義やスケジュールなど)、データベースビュー、およびレポーティングに必要な設定情報を格納する、Identity Reporting リポジトリ (識別情報ウェアハウス) からレポートを生成するために必要なデータを取得します。

認証サービス

認証サービスは OSP コンポーネントによって提供されます。詳細については、24 ページの「認証サービス」を参照してください。

注 : OSP は、Identity Reporting とともに自動的にインストールされます。ただし、Advanced Edition のインストールでは、Identity Reporting は Identity Applications でインストールされるのと同じ認証サービスを使用できます。同じ認証サービスを使用する場合は、Identity Reporting 設定時に認証設定を指定する必要があります。

Self-Service Password Reset

セルフサービスパスワード管理サービスは、セルフサービスパスワード管理へのアクセスを提供します。詳細については、24 ページの 「Self-Service Password Reset」 を参照してください。

Identity Reporting データベース

Identity Reporting データベース (識別情報ウェアハウス) は、Identity Vault および組織内の接続システムの実際の状態と望ましい状態に関する情報を保存します。この情報からレポートを生成して、ユーザや役割などのオブジェクト間の関係を表示することができます。データベースは、Identity Reporting サーバまたはリモートコンピュータにローカルに配置できます。Identity Manager は、データソースを使用してデータベースに接続します。Identity Reporting には、データベースと通信するために Java Database Connectivity ドライバ (JDBC タイプ 4 ドライバ) が必要です。JDBC ドライバにより、Identity Reporting サーバはデータソースと通信できます。Identity Reporting でサポートされているデータベースは、PostgreSQL、Oracle、および Microsoft SQL です。

- PostgreSQL データベースの場合、このドライバは Identity Manager インストールプログラムにバンドルされています。
- Oracle データベースの場合、Oracle Web サイトからドライバをダウンロードできます。
- Microsoft SQL Server データベースの場合、Microsoft Web サイトからドライバをダウンロードします。

注 : Identity Reporting コンポーネントをインストールする前に、Identity Manager Server をインストールする必要があります。

Web アプリケーションサーバ

アプリケーションサーバは、Identity Reporting コンポーネントが実行されるランタイムフレームワークを提供します。次の WAR ファイルが、Identity Reporting のコンポーネントの URL に適用されます。

- **IDMRPT** (Identity Reporting アプリケーション / インタフェース用)
- **idmdcs** (Identity Manager データ収集サービス用)

ユーザが IDMRPT または idmdcs アプリケーションを操作するとき、これらのアプリケーションはレポーティングサービスに対してクエリを実行し、ユーザの情報を取得します。レポーティングサービスは、IDMRPT および idmdcs にユーザインタフェースを提供する情報が含まれる REST API を公開します。

Web アプリケーションサーバの詳細については、24 ページの 「Web アプリケーションサーバ」を参照してください。

Identity Reporting 用のドライバ

Identity Reporting コンポーネントには、次のドライバが必要です。

Managed System Gateway Driver

識別ボールトに問い合わせて管理対象システムから次のタイプの情報を収集します。

- すべての管理対象システムのリスト
- 管理対象システムのすべてのアカウントのリスト
- エンタイトルメントの種類、値、割り当て、および管理対象システムのユーザアカウントプロファイル

データ収集サービスドライバ

データ収集サービスは、データ収集サービスドライバを使用して、識別ボールトに保存されているオブジェクト (アカウント、役割、リソース、グループ、チームメンバーシップなど) の変更をキャプチャします。このドライバは、自身をサービスに登録し、変更イベント (データの同期、追加、変更、および削除イベント) をサービスにプッシュします。

このサービスには、次の 3 つのサブサービスが含まれます。

- **レポートデータコレクタ** : プルデザインモデルを使用して、1 つ以上の識別ボールトデータソースからデータを取得します。収集は、一連の環境設定パラメータによって決定され、定期的に実行されます。データを収集するために、コレクタが Managed System Gateway Driver を呼び出します。
- **イベントドリブンデータコレクタ** : プッシュデザインモデルを使用して、データ収集サービスドライバが取得したイベントデータを収集します。
- **非管理対象アプリケーションデータコレクタ**: それぞれのアプリケーション専用に記述された REST エンドポイントを呼び出すことによって、1 つ以上の非管理対象アプリケーションからデータを取得します。非管理対象アプリケーションとは、識別ボールトに接続されていない企業内のアプリケーションのことです。

インストールプロセスの **[Identity Reporting]** インストールオプションは、Managed System Gateway ドライバとデータ収集サービスドライバを Identity Vault に展開します。

Sentinel Log Management for Identity Governance and Administration

Sentinel Log Management for Identity Governance and Administration (IGA) は、脅威、リスク、およびポリシー関連の決定を行うための情報をエンタープライズ内の多くのソースから受信し、標準化し、優先順位を決定して表示する、セキュリティ情報およびイベント管理 (SIEM) ソリューションです。Sentinel Log Management for (IGA) は、Identity Reporting、

Identity アプリケーション、および Identity Vault を含むいくつかの NetIQ 製品で実行されたアクションに関連するログイベントをキャプチャします。これらのイベントは、Identity Reporting リポジトリ (識別情報ウェアハウス) 内のパブリックスキーマに格納されます。

Identity Manager は、Sentinel Log Management for IGA 用に別個のインストールプログラム (SentinelLogManagementForIGA8.2.2.0.tar.gz) を提供します。

Identity Manager ツール

すべてのインストールに必要

Identity Manager には、ソリューションの実装、カスタマイズ、および保守を容易にする管理ツールのセットが含まれています。これらのツールの一部は Identity Manager とともにインストールされ、一部は個別にインストールする必要があります。

Designer for Identity Manager

Designer for Identity Manager (Designer) は、ネットワーク環境またはテスト環境における Identity Manager ソリューションの設計、テスト、ドキュメント化、および展開を支援します。Identity Manager プロジェクトをオフライン環境で設定してからライブシステムに展開できます。設計上の観点から、Designer は次のことに役立ちます。

- Identity Manager ソリューションを構成するすべてのコンポーネントをグラフィカルに表示し、それらがどのように相互作用しているかを確認する。
- テストソリューションの一部または全体を運用環境に展開する前に、Identity Manager 環境を変更およびテストして、想定どおりに動作しているかを確認します。

Designer は、設計情報とレイアウト情報を維持します。ボタンをクリックするだけで、好みのフォーマットで情報を印刷できます。さらに、エンタープライズレベルのプロジェクト作業を複数のチームで共有することもできます。

Identity Manager は、Designer 用に別個のインストールプログラムを提供します。

Identity Manager 用の Analyzer

Analyzer for Identity Manager (Analyzer) は、内部データ品質ポリシーへの準拠を支援するデータ分析、クレンジング、調整、およびレポーティングの各機能を提供します。Analyzer を使用すると、企業内に保存されているすべてのデータを分析、拡張、および制御できます。Analyzer には、次の機能があります。

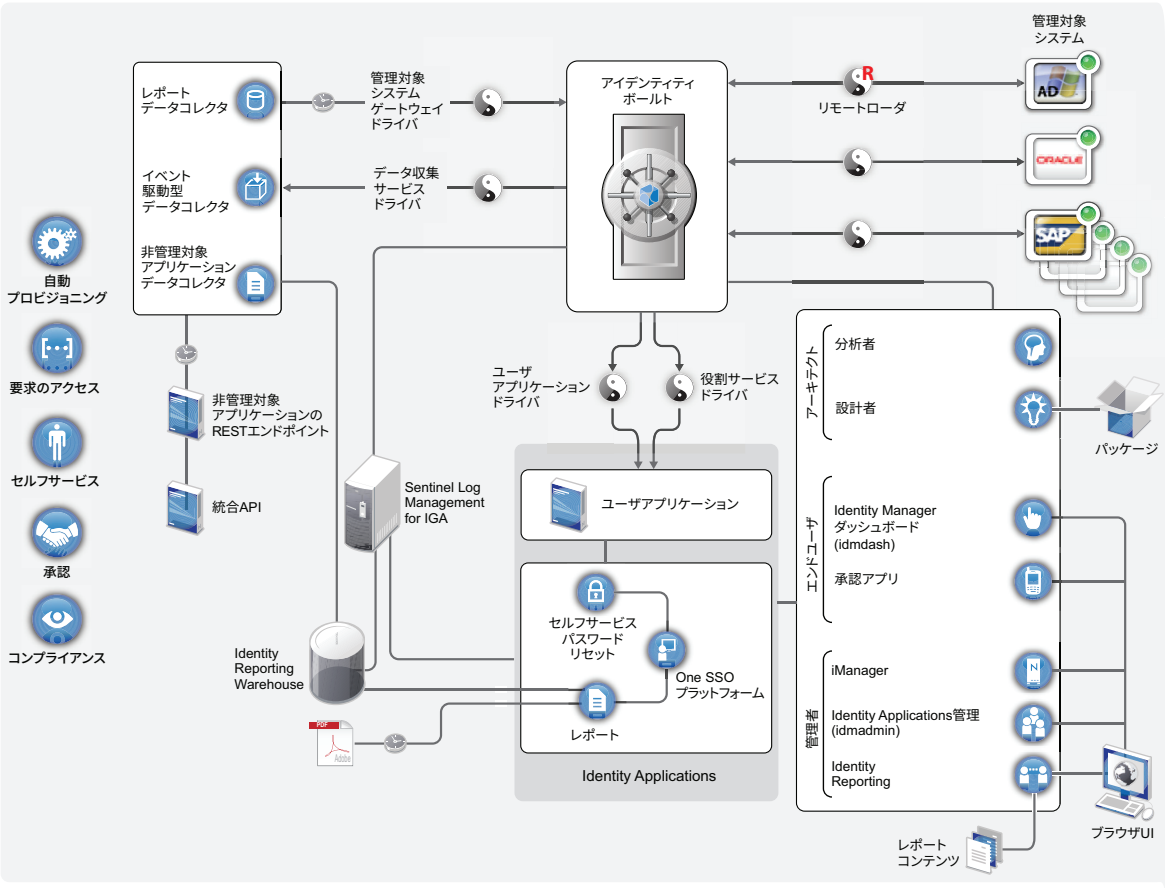
- Analyzer のスキーママップにより、アプリケーションのスキーマ属性を、Analyzer の基本スキーマの対応するスキーマ属性に関連付けます。これにより、データ分析およびクリーニング操作によって異種システム間の類似する値を適切に関連付けることができます。このために、Analyzer は Designer のスキーママッピング機能を利用します。

- Analysis Profile エディタを使用すると、1 つ以上のデータセットインスタンスを分析するためのプロファイルを設定できます。各分析プロファイルには 1 つ以上のメトリクスが含まれており、これらを基準にして属性値を評価することで、データが定義済みのデータフォーマット標準にどの程度準拠しているかを確認できます。
- Matching Profile エディタを使用して、1 つ以上のデータセットの値を比較できます。指定したデータセット内に重複する値がないかどうか、または 2 つのデータセット間で一致する値がないかどうかを確認できます。

Identity Manager は、Analyzer 用に別個のインストールプログラムを提供します。

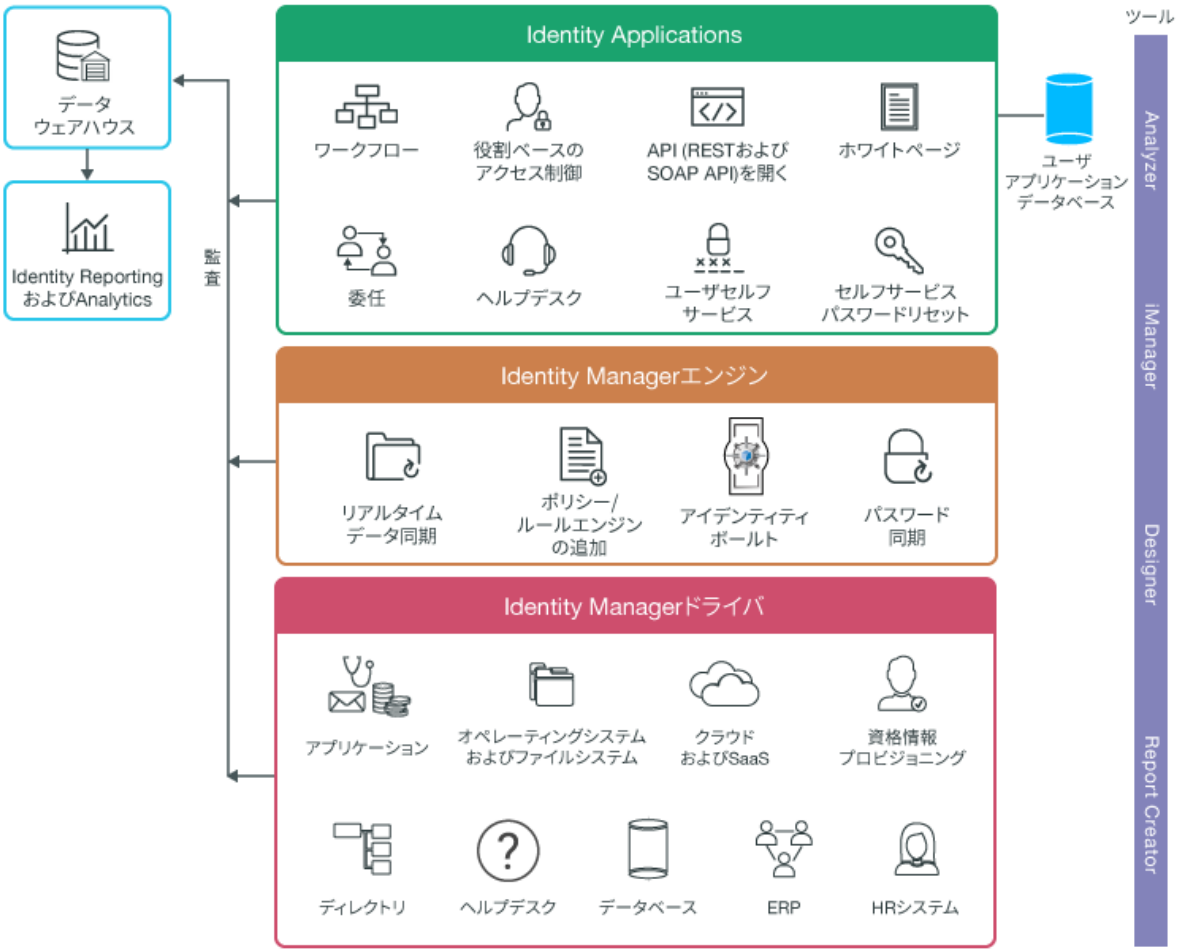
さまざまな Identity Manager コンポーネントの目的とインストール方法を理解したら、図 1-3 を参照して、コンポーネントが互いにどのように相互作用するかを理解してください。

図 1-3 *Identity Manager のコンポーネントの相互作用*



機能アーキテクチャ

次の図は、Identity Manager コンポーネントの基本的な機能アーキテクチャを示しています。この図は、考えられるすべての統合を網羅しているわけではありません。



可能な展開シナリオの詳細については、Identity Manager の展開オプションを参照してください。

Identity Manager の展開オプション

Identity Management ソリューションの物理環境を計画する場合は、次の表を参照してください。これらの展開ユースケースでは、Identity Management の物理アーキテクチャと、コンポーネント製品がどのように接続され、相互および他の製品と通信するかについての概要を提供します。Identity Management の機能アーキテクチャとコンポーネントの概要については、30 ページの 「機能アーキテクチャ」を参照してください。

展開オプション	概要
1 台のコンピュータ上の単一サーバ構成	最も基本的な展開構成では、1 台のコンピュータ上に Identity Manager サーバとその他の必要なアプリケーションが含まれます。ワークロードを満たすために、コンピュータに必要なメモリ、速度、および使用可能なディスク容量があることを確認する必要があります。これは、基本的な展開のユースケースであり、Proof-of-Concept (POC) およびデモ目的にのみ適しています。運用環境には適さない場合があります。

展開オプション	概要
分散サーバ構成	この展開では、1 台のコンピュータ上に Identity Manager サーバがあり、1 台以上の追加のコンピュータに他のすべての必要なアプリケーションがあります。たとえば、Identity アプリケーション、iManager、OSP、SSPR などのコンポーネントを、別のコンピュータで実行することができます。レポーティングサービスのコンポーネントをホストする追加のコンピュータを組み込んで、Sentinel Log Management for IGA コンポーネントを実行するためのシステム要件を満たすことができます。
高可用性の展開	高可用性とは、プライマリサーバで障害が発生した場合、または保守のために一時的にシャットダウンされた場合に、スタンバイサーバに自動的に切り替わる冗長動作です。Identity Manager は、以下のコンポーネントの高可用性環境へのインストールをサポートしています。 ◆ 識別ボールト ◆ Identity Manager エンジン ◆ リモートローダ ◆ Identity Reporting を除く、識別情報アプリケーション 一般的なクラスタ構成には、負荷分散と耐障害性のために Identity アプリケーションをホストする Tomcat Application Server ノードが含まれます。すべての通信はロードバランサを介してルーティングされています。すべてのノードは、Identity Vault および Identity アプリケーションデータベースの同じインスタンスと通信します。この構成はスケーラブルです。負荷を処理するノードの数を簡単に増やすことができます。

Identity Manager 展開のサンプル

Identity Manager を使用すると、ユーザの識別情報と、接続システム上のアプリケーションおよびアカウントへのアクセスを制御できます。必要な機能に基づいて、インストールする Identity Manager Edition を選択し、次にインストールするコンポーネントを決定します。次の表に、Identity Manager Advanced Edition および Identity Manager Standard Edition が提供する機能を示します。

機能	Advanced Edition	Standard Edition	インストールするコンポーネント
ルールベースの自動化されたユーザプロビジョニング	✓	✓	Identity Manager エンジンと Designer
リアルタイム Identity 同期	✓	✓	Identity Manager エンジンと Designer
パスワード管理とパスワードセルフサービス	✓	✓	Identity Manager エンジンと SSPR

機能	Advanced Edition	Standard Edition	インストールするコンポーネント
ユニフォーム Identity 情報ツール (Analyzer)	✓	✓	Analyzer
REST API およびシングルサインオンのサポート	✓	✓ (限定サポートのみ)	Identity Manager エンジン、OSP、および Identity Reporting
現在の状態のレポーティング	✓	✓	Identity Manager エンジンおよび Identity Reporting
役割ベースのエンタープライズレベルのプロビジョニング	✓	✗	Identity Manager エンジンおよび Identity アプリケーション
ビジネスポリシー適用に対する自動化された承認ワークフロー	✓	✗	Identity Manager エンジン、Designer、および Identity アプリケーション
Identity アプリケーションの高度なセルフサービス	✓	✗	Identity Manager エンジンおよび Identity アプリケーション
簡単なリソースプロビジョニングのためのリソースモデルとカタログ	✓	✗	Identity Manager エンジンおよび Identity アプリケーション
履歴状態のレポーティング	✓	✗	Identity Manager エンジンおよび Identity Reporting
接続されたシステムのレポーティング	✓	✗	Identity Manager エンジンおよび Identity Reporting
役割およびリソースの管理	✓	✗	Identity Manager エンジンおよび Identity アプリケーション

注 : すべての Identity Manager インストールにおいて、Identity Manager Server が中心的なコンポーネントとなります。Identity Manager のエディションに応じて、Identity Reporting のみ、または Identity Reporting と Identity アプリケーションの両方が Tomcat アプリケーションサーバにインストールされます。Identity Manager コンポーネント固有のインストーラを

使用して、必要に応じて他のコンポーネントをインストールします。たとえば、Designer、Analyzer、または Sentinel Log Management for Identity Governance and Administration をインストールします。

さらに、Identity Manager をインストールする前に、実装の目標を確認し、高可用性やスケーラビリティなどの物理トポロジオプションに注意を払ってください。これにより、組織の要件に一致する構成を特定することができます。

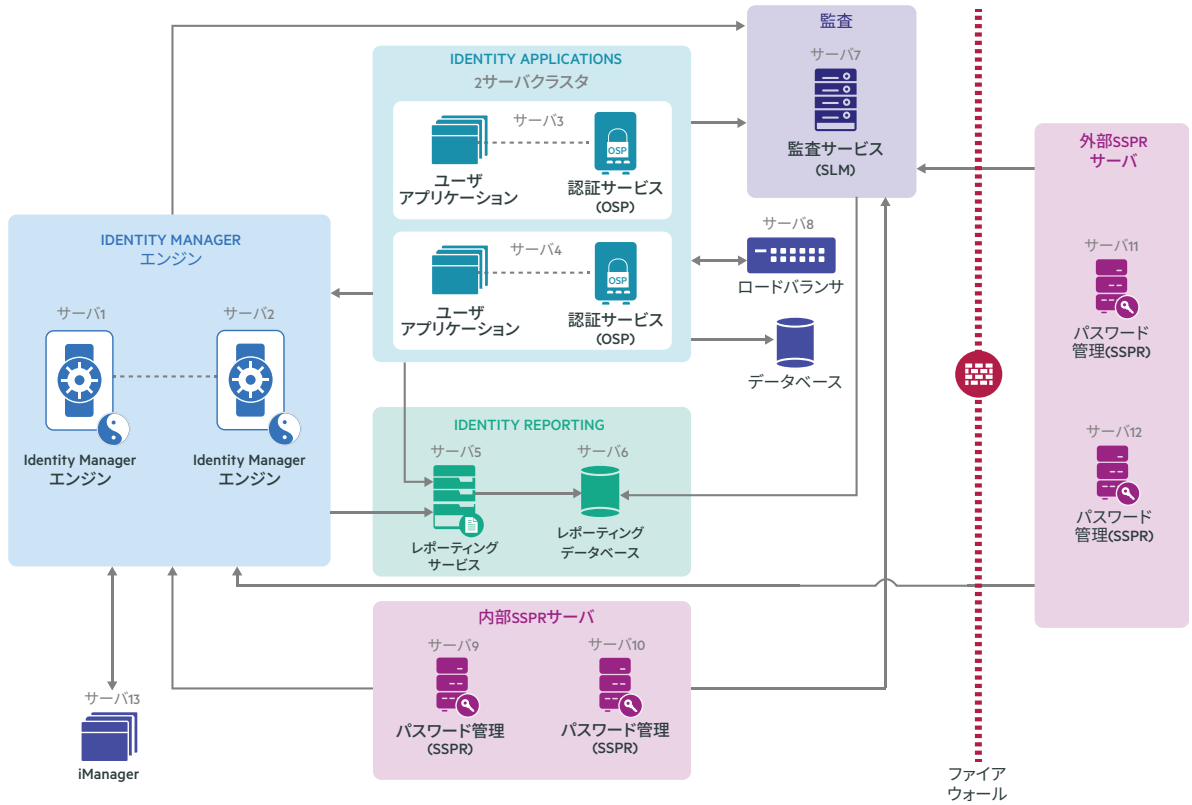
高可用性により、データ、アプリケーション、サービスなどの重要なネットワークリソースを効率的に管理できます。単一障害点を減らし、冗長コンポーネントを使用することにより、高可用性を実装することができます。同様に、識別情報管理コンポーネントの複数のインスタンスをロードバランサで接続すると、可用性の高い環境を実現できます。

このセクションでは、Advanced Edition および Standard Edition の実装を大まかに示す 2 つの例を説明します。これらを参考にして、実装の展開ダイアグラムを策定することができます。

Advanced Edition 展開のサンプル

図 1-4 は、Identity Manager Advanced Edition インストールの大まかな展開トポロジを示しています。

図 1-4 Advanced Edition 展開のサンプル



- Identity Manager Server コンポーネントとその基礎となるリポジトリ (Identity Vault) および Web 対応コンポーネント (Identity アプリケーションおよび Identity Reporting) は、イントラネットゾーンにインストールされます。この場合、ロードバランサにより、トラフィックが Identity アプリケーションコンポーネントにルーティングされます。この展開では、これらのコンポーネントがファイアウォールによってインターネットトラフィックから切り離されているので、セキュリティが強化されます。
- Identity Manager Serverコンポーネントは、2サーバ(プライマリ/セカンダリ)構成を使用するように設定されています。仮想論理 IP アドレスはプライマリサーバでアクティブになります。プライマリサーバは、プライマリ (アクティブ) ノードとして機能し、もう一方のサーバがセカンダリノードとして機能します。プライマリサーバに障害が発生すると、論理 IP アドレスはセカンダリサーバに移動します。この場合、すべてのプロセスはセカンダリサーバで開始されます。論理 IP アドレスが移動し、他のすべてのプロセスが開始されると、セカンダリサーバにアクセスするアプリケーションプロセスで、一時的にサービスが失われる場合があります。すべてのコンポーネントは、常に同じ Identity Vault サーバを使用します。
- SSPR サービスはファイアウォールの内外で利用でき、組織のローカルユーザおよびモバイルユーザのパスワード管理のニーズに対処します。ファイアウォール内にインストールされたサービスは、ローカルパスワード管理のニーズに対処します。パスワー

ドを忘れた場合、モバイルワーカーは VPN にアクセスできません。このため、内部に配置された SSPR サービスにアクセスできなくなります。ファイアウォールの外側に配置されている SSPR サービスに直接アクセスして、パスワードを管理することができます。

- ユーザアプリケーションおよび認証サービス (OSP) は、負荷を処理し Identity アプリケーションのフェールオーバープロセスをサポートするために、クラスタに展開されます。クラスタノードは、別のコンピュータにインストールされている同じ Identity アプリケーションデータベースにアタッチされます。この展開では、クラスタにノードを追加できるので、スケーラビリティが向上します。クラスタ設定は、新たに追加されたノードにすぐに送信されます。ロードバランサは通常クラスタの一部で、クラスタ設定とともにフェールオーバーポリシーを理解しています。この設定では、すべてのクラスターノードはいつでもアクティブです。ロードバランサは複数のノードに負荷を分散し、各ノードのワークロードがほぼ同じになるようにします。ノードに障害が発生すると、そのノードに対して行われた要求がクラスタ内の存続しているノードに転送されます。このインストールはサイト内の高可用性ソリューションであるので、2 ノードのハードウェアベースのクラスタを使用して Identity アプリケーションコンポーネントの高可用性を実現し、ローカルのハードウェアおよびソフトウェアの障害からの保護を提供します。

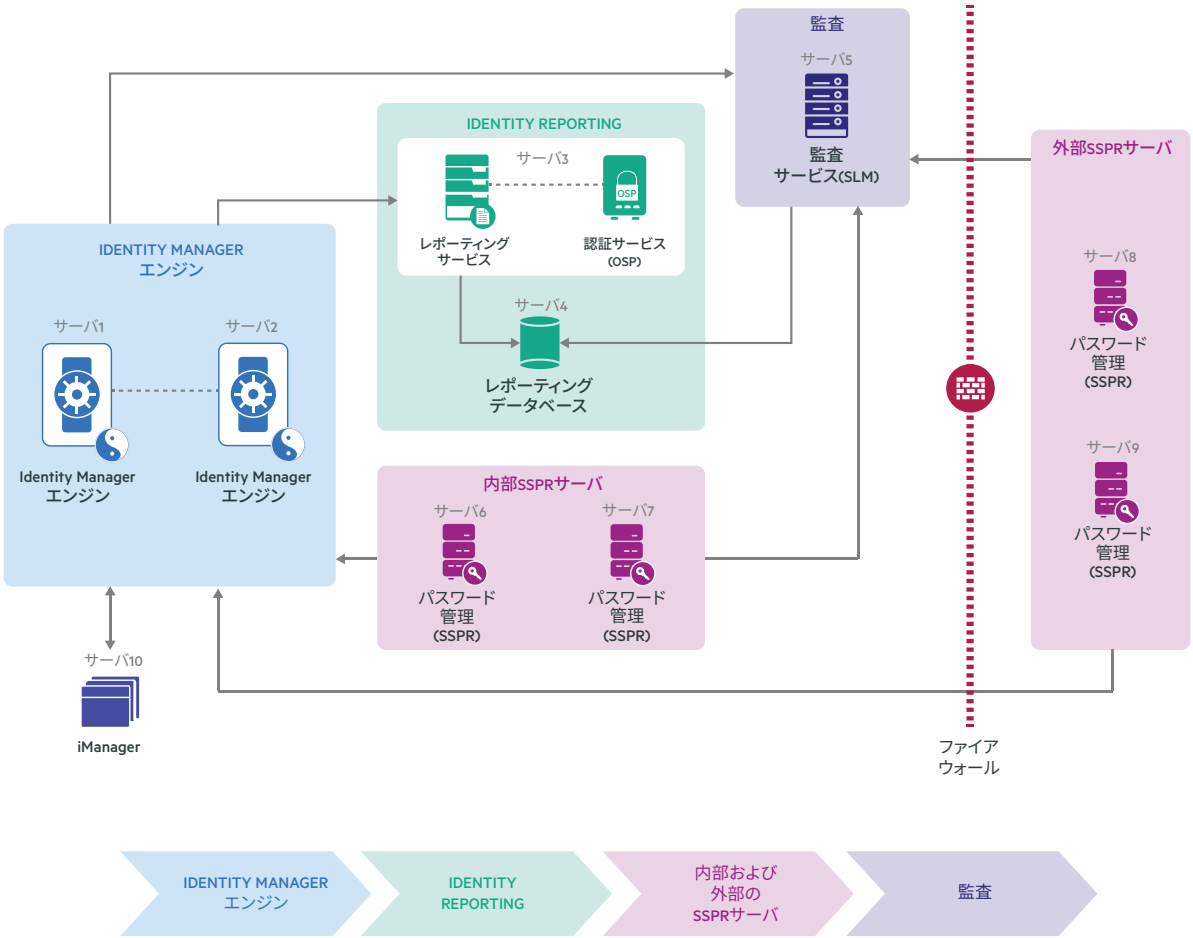
NetIQ ではこの設定をテスト済みであり、推奨しています。

注 : Identity Manager は、Identity Reporting コンポーネントのクラスタリングをサポートしていません。

Standard Edition 展開のサンプル

運用展開では、セキュリティポリシーにより、環境の高度な認証と保護を提供する認証サービスをパブリックネットワークに公開しないように指定することができます。図 1-5 は、Identity Manager Standard Edition インストールの大まかな展開トポロジを示しています。

図 1-5 Standard Edition 展開のサンプル



- Identity Manager Server コンポーネントとその基礎となるリポジトリ (Identity Vault) および Identity Reporting コンポーネントは、イントラネットゾーンにインストールされます。インターネット Web トラフィックは、保護を強化するためにファイアウォールの背後にインストールされている Web サーバを介して Identity Reporting コンポーネントにルーティングされます。この展開では、これらのコンポーネントがファイアウォールによってインターネットトラフィックから切り離されているので、セキュリティが強化されます。
- Identity Manager Server コンポーネントは、2 サーバ (プライマリ / セカンダリ) 構成を使用するように設定されています。仮想論理 IP アドレスはプライマリサーバでアクティブになります。プライマリサーバは、アクティブノードとして機能し、もう一方のサーバがセカンダリノードとして機能します。プライマリサーバに障害が発生すると、論理 IP アドレスはセカンダリサーバに移動します。この場合、すべてのプロセスはセカンダリサーバで開始されます。論理 IP アドレスが移動し、他のすべてのプロセスが開始されると、セカンダリサーバにアクセスするアプリケーションプロセスで、一時的にサービスが失われる場合があります。すべてのコンポーネントは、常に同じ Identity Vault サーバを使用します。
- SSPR サービスはファイアウォールの内外で利用でき、組織のローカルユーザおよびモバイルユーザのパスワード管理のニーズに対処します。ファイアウォール内にインストールされたサービスは、ローカルパスワード管理のニーズに対処します。パスワー

ドを忘れた場合、モバイルワーカーは VPN にアクセスできません。このため、内部に配置された SSPR サービスにアクセスできなくなります。ファイアウォールの外側に配置されている SSPR サービスに直接アクセスして、パスワードを管理することができます。

NetIQ ではこの設定をテスト済みであり、推奨しています。

注 : Identity Manager は、Identity Reporting コンポーネントのクラスタリングをサポートしていません。

II Identity Manager のインストールの計画

Identity Manager 実装の計画は、Identity Manager がユーザを管理する方法と、ビジネス目標を達成するために必要な機能に依存します。以下の点を考慮して、決定を行ってください。

- 識別情報をどのように管理するか。
- 自動プロビジョニングが必要か。
- ワークフローを使用して実装する必要があるのはどのビジネス要件か。

決定の結果により、要件に合わせて Identity Manager を実装する最適な方法が決まります。

大企業には Identity Manager を展開する前に計画を必要とする追加のタスクがあります。詳細については、『NetIQ Identity Manager Overview and Planning Guid』の「計画」セクションを参照してください。

2 インストールの計画

次の表に、実装する機能をサポートするためにインストールするコンポーネントを示します。これらのコンポーネントのインストール手順については、インストールセクションを参照してください。

機能	インストールするコンポーネント
社内ディレクトリのユーザの識別情報を管理する	Identity Manager サーバ
接続システムのアカウントをプロビジョニングする	Identity Manager サーバ 識別情報アプリケーション ユーザアプリケーションドライバ 役割とリソースのサービスドライバ Designer **注 :** Identity Manager ドライバのインストール手順については、Identity Manager ドライバのマニュアル Web サイトで、インストールするドライバのタイプに対応したドライバ実装ガイドを参照してください。
認証	Identity Manager サーバ 1 つの Single Sign-on プロバイダ
パスワード管理	Identity Manager サーバ Self Service Password Management
Identity Manager アクティビティに関するレポートを生成する	Identity Manager サーバ Identity Reporting 1 つの Single Sign-on プロバイダ

ハードウェア要件の決定

Identity Manager のインストールに必要なハードウェアは、次の 2 つの要因に左右されます。

- 実装する機能
- 展開のサイズ

以下の展開タイプは、展開のサイズを見積もるのに役立ちます。

展開のタイプ	ハードウェア要件
概念実証 (デモ)	開発環境でのデモまたは基本テストで使用する単一サーバ展開。
Basic	小規模から中規模の実装に適したマルチサーバ実装。 このタイプの実装では、Identity Manager Server およびそのコンポーネントを実行するために 1 台のサーバと、Identity Applications および Identity Reporting のコンポーネントを実行するために 2 台の追加サーバが必要です。
中間	中規模の実装に適した高可用性実装。
大企業	フェールオーバー機能を提供する Identity Manager エンジンクラスタと、シングルサインオンアクセス (Windows 上の OSP) および負荷分散と耐障害性をサポートする別の Identity Applications クラスタと認証サービスを含む、高可用性実装。

展開計画ワークシート

このトピックの情報を使用して、Identity Manager の新しい実装の詳細を理解してください。

***表 2-1** 計画ワークシート*

計画アクティビティ	ワークシート
ユースケースに基づいて実装タイプを決定し、展開のサイズを設定します	サイズ決定ワークシート
展開アーキテクチャを設計します。環境をサポートするために必要な物理コンピュータ / サーバおよびその他のシステムの数をリストします	アーキテクチャワークシート
ご使用のシステムがシステム要件を満たしていることを確認します	システム要件ワークシート
ネットワークポートを確認して、デフォルトのポートが使用中のポートと競合するかどうかを判断します	Identity Manager コンポーネントが使用するポートの確認

サイズ決定ワークシート

従う手順と設計要素は展開のサイズによって異なるため、展開のサイズを正しく見積もることが重要です。各コンポーネントのサイズとスケーラビリティに関する考慮事項を確認して、容量要件を理解してください。

表 2-2 サイズ決定ワークシート

特性	値
物理コンピュータ / サーバの数	
プライマリ Identity Manager サーバで実行されているドライバの数	
セカンダリ Identity Manager サーバで実行されているドライバの数	
クラスタ内の Identity Applications ノードの数	
Identity Applications データベースの数	
ファイアウォール内の Self-Service Password Reset インスタンスの数	
さらに続く …	

アーキテクチャワークシート

展開のサイズを決定したら、適切な展開を選択し、展開をサポートするために必要な物理コンピュータ / サーバの数を記録します。

表 2-3 アーキテクチャワークシート

展開のユースケース
すべてのドライバを使用した Identity Manager Server フェールオーバー展開
実行中のドライバの数
Identity Applications 高可用性展開

システム要件ワークシート

推奨されるハードウェア、サポートされるオペレーティングシステム、およびサポートされる仮想環境については、Identity Manager 4.8 のシステム要件を参照してください。

特定のリリースのシステム要件については、Identity Manager マニュアルの Web サイトにあるリリースに付属のリリースノートを参照してください。Identity Manager の実装は IT 環境のニーズに応じて異なる可能性があるため、現在の環境の Identity Manager アーキテクチャを完成させる前に、NetIQ コンサルティングサービスまたは NetIQ Identity Manager パートナーに連絡する必要があります。

Identity Manager コンポーネントが使用するポートの確認

Identity Manager コンポーネントは、Identity Manager コンポーネント間の適切な通信のために異なるポートを使用します。

注 : デフォルトポートがすでに使用されている場合は、Identity Manager コンポーネント用に別のポートを指定してください。

ポート番号	コンポーネント	ポートの使用
389	識別ボールト	Identity Manager コンポーネントとの平文での LDAP 通信に使用されます。
465	Identity Reporting	SMTP メールサーバとの通信に使用されます。
524	識別ボールト	NetWare Core Protocol (NCP) 通信に使用されます。
636	識別ボールト	Identity Manager コンポーネントとの TLS/SSL による LDAP 通信に使用されます。
5432	識別情報アプリケーション	識別情報アプリケーションデータベースとの通信に使用されます。
7707	Identity Reporting	Managed System Gateway ドライバによって、識別ボールトとの通信に使用されます。
8000	リモートローダ	TCP/IP 通信のためにドライバインスタンスによって使用されます。 **注 :** リモートローダの各インスタンスには一意のポートが割り当てられる必要があります。
8005	識別情報アプリケーション	Tomcat によって、シャットダウンコマンドのリスンに使用されます。
8009	識別情報アプリケーション	Tomcat によって、HTTP ではなく AJP プロトコルを使用した Web コネクタとの通信に使用されます。
8028	識別ボールト	NCP 通信との平文での HTTP 通信に使用されます。
8030	識別ボールト	NCP 通信との HTTPS 通信に使用されます。

ポート番号	コンポーネント	ポートの使用
8080	識別情報アプリケーション iManager	Tomcat によって平文での HTTP 通信に使用されます。
8090	リモートローダ	リモートローダによって、リモートインタフェースシムからの TCP/IP 接続のリスンに使用されます。 **注 :** リモートローダの各インスタンスには一意のポートが割り当てられる必要があります。
8109	識別情報アプリケーション	統合インストールプロセスの使用時にのみ適用されます。 Tomcat によって、HTTP ではなく AJP プロトコルを使用した Web コネクタとの通信に使用されます。
8180	識別情報アプリケーション	Identity Applications が実行されている Tomcat アプリケーションサーバによって、HTTP 通信に使用されます。
8443	識別情報アプリケーション iManager	Tomcat によって、HTTPS (SSL) 通信、または SSL 通信に対する要求のリダイレクトに使用されます。
8543	識別情報アプリケーション	デフォルトではリスンしません。 TLS/SSL プロトコルを使用していないときに、Tomcat によって、SSL 転送を求める要求のリダイレクトに使用されます。
9009	iManager	Tomcat によって MOD_JK に使用されます。
5432	Identity Reporting	PostgreSQL データベース Sentinel で使用されます。
45654	ユーザアプリケーション	Tomcat がクラスタグループとともに実行されている場合、識別情報アプリケーションのデータベースがインストールされているサーバによって、通信のリスンに使用されます。

III Identity Manager コンポーネントのインストールと設定

このセクションでは、Identity Manager コンポーネントのインストールと設定のプロセスを順を追って説明します。詳細については、51 ページの 「インストール手順」を参照してください。

Identity Manager コンポーネントがインストールされ、基本設定が完了したら、コンポーネントを完全に機能させるために追加の設定手順をいくつか実行する必要があります。詳細については、69 ページの第 4 章「インストールを完了するための最終ステップ」を参照してください。

3 インストールおよび設定プロセスの概要

このセクションでは、Identity Manager コンポーネントのインストールと設定のプロセスについて説明します。設定プロセスを開始する前に、各コンポーネントの設定オプションを確認する必要があります。詳細については、環境設定の理解を参照してください。

Designer や Analyzer など、一部のコンポーネントでは設定は必要ない場合があります。

インストールの順序

一部のコンポーネントのインストールプログラムでは、以前にインストールしたコンポーネントに関する情報が必要になるため、コンポーネントは以下の順序でインストールする必要があります。

- Sentinel Log Management for Identity Governance and Administration (IGA) (Linux コンピュータでのみサポートされるインストール)
- Identity Manager サーバのコンポーネント
- Identity Applications のコンポーネント (Advanced Edition の場合のみ)
- Identity Reporting のコンポーネント
- Designer for Identity Manager
- Identity Manager 用の Analyzer

コンポーネントをインストールする前に、各コンポーネントのインストールの前提条件と考慮事項を確認する必要があります。

Identity Manager サーバ、Identity Applications、および Identity Reporting コンポーネントのインストールおよび設定プロセスの理解

Identity Manager は、以下の Identity Manager コンポーネントをインストールおよび設定するためのウィザードベースのインストール方法を提供します。

- Identity Manager サーバ
- 識別情報アプリケーション
- Identity Reporting

インストーラを使用すると、これらのコンポーネントを対話形式またはサイレントでインストールおよび設定することができます。インストールプロセスでは、インストールされたコンポーネントの値を指定できます。

またインストールプロセスにより、ファイルシステムに JRE、Apache Tomcat、PostgreSQL、ActiveMQ、および OpenSSL などの依存コンポーネントのリポジトリも作成されます。同じコンピュータに複数の Identity Manager コンポーネントをインストールする場合、インストールプロセスでは、依存コンポーネントを必要とする Identity Manager コンポーネントごとに依存コンポーネントのコピーを複数作成する代わりに、このリポジトリを参照します。たとえば、Identity Applications と Identity Reporting は、同じコンピュータにインストールされている場合、同じ Tomcat を使用します。

インストール方法のタイプ

Identity Manager では、対話的なインストール方法およびサイレントなインストール方法をサポートしています。サイレント (非対話型) インストールでは、ユーザインタフェースは表示されず、ユーザに対する質問も行われません。

対話的な方法

インストールするコンポーネントを選択する必要があります。選択に基づいて、コンポーネントがインストールされます。

サイレントな方法

プロパティファイルにインストールするコンポーネントの値を指定する必要があります。インストールプログラムが呼び出されると、プロパティファイルからこれらの値を読み取ります。環境内の異なるコンピュータで同じプロパティファイルを使用して、サイレントインストールを実行することができます。

インストールオプション

次の表は、インストールプログラムに用意されているインストールオプションを使用してインストールされるコンポーネントについて説明しています。

***表 3-1** インストールオプション*

インストールオプション	インストールされるコンポーネント
Identity Manager エンジン	Identity Vault、Identity Manage エンジン、リモートローダサービス、iManager Web Administrator と Identity プラグイン、ファンアウトエージェント、およびドライバをインストールします。
識別情報アプリケーション	Identity Applications、One SSO Provider (OSP)、ユーザアプリケーションドライバ、役割とリソースサービスドライバ (RRSD)、PostgreSQL、およびセルフサービスパスワードリセット (SSPR) をインストールします。 **注 :** Identity Applications とは異なるサーバに SSPR をインストールする場合は、<iso mounted location>\common\sspr\ ディレクトリにある install.exe を使用します。
Identity Reporting	Identity Reporting、OSP、PostgreSQL、Data Collection Service ドライバ (DCS)、および Managed System Gateway (MSG) ドライバをインストールします。

設定モードのタイプ

次の方法で Identity Manager コンポーネントを設定することができます。

- 標準
- カスタム

標準設定は、ほとんどの設定オプションでデフォルト設定が選択されます。カスタム設定では、要件に応じてカスタム値を指定できます。このオプションを使用して、ほとんどの設定を設定できます。

設定時における直感的でないパスワードの使用

ほとんどの Identity Manager コンポーネントでは、設定段階でパスワードを指定する必要があります。設定時間を短縮するために、すべての環境設定パラメータに同じパスワードを適用するようプロセスに指示できます。

パスワードは 6 文字以上にする必要があります。辞書にある単語を使用しないでください。辞書の単語は、辞書リストによく付属している自由に利用できるパスワード解読ツールに対して脆弱です。辞書の単語を使用する必要がある場合は、数字と句読点を組み合わせてみてください。

Designer および Analyzer のインストールプロセスの理解

Identity Manager は、Designer と Analyzer に個別の Windows インストールプログラムを提供しています。Designer および Analyzer のインストールプログラムは、製品のダウンロードサイトで入手できます。

Designer

Designer は、Identity_Manager_4.8_Windows_Designer.tar.gz ファイルを使用してインストールできます。サイレントインストールの場合、designerInstaller.properties ファイルでインストールの値を指定します。それ以外の場合、インストーラはインストールのデフォルトのパラメータ値を採用します。

Designer は設定を必要としません。

Analyzer

Analyzer は、Identity_Manager_4.8_Windows_Analyzer.tar.gz ファイルを使用してインストールできます。サイレントインストールの場合、designerInstaller.properties ファイルでインストールの値を指定します。それ以外の場合、インストーラはインストールのデフォルトのパラメータ値を採用します。

Analyzer は設定を必要としません。

インストール手順

このトピックでは、Identity Manager コンポーネントのインストール方法を理解します。

Identity Manager サーバ、Identity Applications、および Identity Reporting のインストール手順

このセクションでは、対話的な方法またはサイレントな方法で Identity Manager Server、Identity Applications、および Identity Reporting コンポーネントをインストールするプロセスについて説明します。インストールプログラムの [Identity Manager Server] オプションでは、32 ビット、64 ビット、および .NET リモートローダをインストールできます。

注 : Identity Manager エンジンをインストールする前に、Windows サーバが最新の Windows のパッチで更新されていることを確認し、Windows サーバを再起動します。

インタラクティブインストール

1 ダウンロードサイトから Identity_Manager_4.8_Windows.iso をダウンロードします。

2 ダウンロード済みの iso をマウントします。

3 インストールするコンポーネントに基づいて、以下の場所で入手可能な install.exe を実行します。

- **Identity Manager サーバ :** <iso mounted location>\IdentityManagerServer
- **識別情報アプリケーション :** <iso mounted location>\IdentityApplications
- **Identity Reporting:** <iso mounted location>\IdentityReporting

4 インストールで使用する言語を選択し、[OK] をクリックします。

[はじめに] 画面に、インストール可能なコンポーネントが表示されます。

5 [次へ] をクリックします。

6 使用許諾契約書の条項を確認し、同意します。

7 インストールするコンポーネントを選択し、[次へ] をクリックします。

8 インストールフォルダを指定して、[次へ] をクリックします。

注 : カスタムインストールフォルダには、. や _ などの特殊文字を含めないでください。

---

9 インストールの種類を選択します。

- 標準インストール
- カスタムインストール

10 選択したインストールのモードに基づいて、インストールパラメータは異なります。必要な詳細を指定します。設定パラメータの詳細については、以下の表を参照してください。

- Identity Manager エンジンの設定
- Identity Applications の設定
- Identity Reporting の設定

11 インストール前の概要ページで詳細を確認し、[インストール] をクリックします。

サイレントインストール

Identity Manager コンポーネントのサイレントインストールを実行するには、各コンポーネントの .iso に用意されているプロパティファイルを使用します。Identity Manager メディアの <iso_downloaded_location>\<*Identity Manager Component*>\response-files の場所にサンプルプロパティファイルが含まれています。

サイレントインストールを使用してコンポーネントをインストールするには、以下のアクションを実行します。

1. NetIQ ダウンロード Web サイトから Identity_Manager_4.8_Windows.iso をダウンロードします。
2. ダウンロード済みの .iso をマウントします。
3. コンポーネントのインストールに使用するインストールのモードに基づいて、以下の場所に用意されている typical_install.properties または custom_install.properties ファイルを使用します。
   - **Identity Manager サーバ :** <iso mounted location>\IdentityManagerServer\response-files
   - **識別情報アプリケーション :** <iso mounted location>\IdentityApplications\response-files
   - **Identity Reporting:** <iso mounted location>\IdentityReporting\response-files
4. 要件に応じてインストールパラメータを変更します。設定パラメータの詳細については、以下の表を参照してください。
   - Identity Manager エンジンの設定
   - Identity Applications の設定
   - Identity Reporting の設定
5. サイレントインストールを実行するには、インストールするコンポーネントのディレクトリから次のコマンドを実行します。

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

   次に例を示します。

   .\install.exe -i silent -f *C:\Users\Administrator\Desktop typical_install_idmengine.properties*
6. (オプション) デフォルトのインストール場所については、インストールログを参照します。たとえば、次のファイルを確認できます。

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

リモートローダのインストール

Identity Manager には、スタンドアロンサーバにリモートローダをインストールするオプションが用意されています。Identity Manager エンジンとリモートローダを別々のコンピュータにインストールする場合、このオプションを使用します。

注 : このオプションを使用して、64 ビットリモートローダおよび .NET リモートローダをインストールできます。32 ビットリモートローダをインストールするには、Identity Manager サーバ、Identity Applications、および Identity Reporting のインストール手順を参照してください。

インタラクティブインストール

1. NetIQ ダウンロード Web サイトから Identity_Manager_4.8_RL_Windows.iso をダウンロードします。
2. ダウンロード済みの .iso をマウントします。
3. マウントされた場所から、install.exe ファイルを実行します。
4. インストールで使用する言語を選択し、**[OK]** をクリックします。
5. **[次へ]** をクリックします。
6. 使用許諾契約書の条項を確認し、同意します。
7. **[次へ]** をクリックします。
8. インストールフォルダを指定して、**[次へ]** をクリックします。
9. **[インストール]** をクリックします。

サイレントインストール

1. NetIQ ダウンロード Web サイトから Identity_Manager_4.8_RL_Windows.iso をダウンロードします。
2. ダウンロード済みの .iso をマウントします。
3. <ISO mounted location>\response-files に移動します。
4. サイレントインストールを実行するには、プロパティファイルのディレクトリから次のコマンドを実行します。

   install.exe -i silent -f install.properties

Java リモートローダのインストール

Identity Manager は、Java リモートローダを使用して、1 つのサーバで実行されている Identity Manager エンジンと、rdxml が動作しない別の場所で実行されている Identity Manager ドライバとの間でデータを交換します。Java リモートローダ、dirxml_jremote は、互換性のある JRE と Java Sockets がインストールされた、サポート対象の任意の Windows プラットフォームにインストールできます。

1. Identity Manager エンジンをホストするサーバで、アプリケーションシムの ..so ファイルまたは .jar ファイルをコピーします。これらのファイルは、デフォルトでは C:\NetIQ\idm\NDS\lib ディレクトリにあります。
2. Java リモートローダをインストールするコンピュータ (ターゲットコンピュータ) にログインします。
3. ターゲットコンピュータに、サポートされているバージョンの JRE がインストールされていることを確認します。
4. NetIQ ダウンロード Web サイトから Identity_Manager_4.8_Windows.iso をダウンロードします。
5. ダウンロード済みの .iso をマウントします。

6 <iso mounted location>\IdentityManagerServer\products\IDM\java_remoteloader ディレクトリに移動します。

7 dirxml_jremote_dev.tar.gz ファイルをターゲットコンピュータ上の目的の場所にコピーします。たとえば、ファイルを C:\NetIQ\idm にコピーします。

8 次のいずれかのファイルをターゲットコンピュータ上の目的の場所にコピーします。

- dirxml_jremote.tar.gz
- dirxml_jremote_mvs.tar

  mvs の詳細については、dirxml_jremote_mvs.tar ファイルを untar し、ドキュメント usage.html を参照してください。

9 ターゲットコンピュータで、.tar.gz ファイルを圧縮解除して展開します。

たとえば、7-Zip またはサポートされているソフトウェアを使用して、.tar.gz ファイルを圧縮解除します。

10 CLASSPATH 環境変数を、lib フォルダに存在するすべての jar に設定します。ドライバに固有の依存 jar がある場合、これらの jar ファイルを lib フォルダにコピーし、CLASSPATH 環境変数をこれらの jar にも設定します。

たとえば、次のように設定します。

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

11 PATH 環境変数を、Java.exe 用に JDK または JRE の bin フォルダに設定します。

12 展開されていない dirxml_jremote.tar.gz ディレクトリの lib サブディレクトリから dirxml_jremote スクリプトに jar ファイルの場所を指定する必要があります。たとえば、\lib*.jar です。

13 サンプル環境設定ファイル config8000.txt をアプリケーションシム用に設定します。

dirxml_jremote.tar.gz jar ファイルに、このファイルが含まれています。詳細については、『*NetIQ Identity Manager Driver Administration Guide*』の「Configuring the Remote Loader and Drivers」を参照してください。

14 次のコマンドを使用してリモートローダを起動します。

14a リモートローダのパスワードを指定するには :

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

次に例を示します。

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

14b リモートローダを開始するには :

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

次に例を示します。

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

14c リモートローダを停止するには :

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

次に例を示します。

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

SSPR のインストール

インストーラには、SSPR を個別にインストールするオプションが用意されています。Identity Applications と SSPR を別々のコンピュータにインストールする場合、このオプションを使用します。これは、Standard Edition で SSPR をインストールする唯一のオプションです。SSPR は Standard Edition では自動的にインストールされません。

SSPR の対話型インストールまたはサイレントインストールを実行できます。

インタラクティブインストール

1. NetIQ ダウンロード Web サイトから Identity_Manager_4.8_Windows.iso をダウンロードします。
2. ダウンロード済みの .iso をマウントします。
3. <ISO mounted location>\common\sspr ディレクトリに移動します。
4. install.exe ファイルを実行します。
5. インストールで使用する言語を選択し、[OK] をクリックします。
6. [次へ] をクリックします。
7. 使用許諾契約書の条項を確認し、同意します。
8. [次へ] をクリックします。
9. インストールフォルダを指定して、[次へ] をクリックします。
10. SSPR の環境設定を指定します。詳細については、64 ページの 「Self-Service Password Reset の環境設定ワークシート」を参照してください。
11. [次へ] をクリックします。
12. [インストール] をクリックします。

サイレントインストール

1. NetIQ ダウンロード Web サイトから Identity_Manager_4.8_Windows.iso をダウンロードします。
2. ダウンロード済みの .iso をマウントします。
3. <ISO mounted location>\common\sspr ディレクトリに移動します。
4. サイレントインストールを実行するには、プロパティファイルのディレクトリから次のコマンドを実行します。

   install.exe -i silent -f sspr_silentinstall.properties

環境設定の理解

以下のワークシートを使用して、Identity Manager コンポーネントを設定するときに指定する必要がある情報を収集できます。

Identity Manager エンジンの環境設定ワークシート

以下のワークシートを使用して、Identity Manager エンジンを設定するときに指定する必要がある情報を収集できます。

表 3-2 *Identity Manager エンジンの設定*

パラメータ	説明
Identity Vault DIB の場所	Identity Vault DIB の場所を指定します。
新しいツリーの作成	新しい Identity Vault ツリーを作成する場合は、このオプションを選択します。
ツリー名	**[新しいツリーの作成]** オプションを選択した場合にのみ適用されます。 アイデンティティボールトツリー名を指定します。
既存のツリーに追加	リモートサーバに存在する Identity Vault ツリーに接続する場合は、このオプションを選択します。IP アドレスのみを指定する必要があります。ホスト名または FQDN はサポートされていません。
ホスト	**[既存のツリーに追加]** オプションを選択した場合にのみ適用されます。 Identity Vault に IP アドレスを指定します。

パラメータ	説明
セキュア LDAP ポート	[既存のツリーに追加] オプションを選択した場合にのみ適用されます。 識別ボールトが SSL (Secure Sockets Layer) プロトコルを使用した LDAP 要求をリスンするポートを指定します。デフォルトは 636 です。eDirectory がインストールされる前にサーバにロードされているサービスがデフォルトのポートを使用している場合は、別のポートを指定する必要があります。
管理者 DN	Identity Manager エンジンの管理者名を指定します。デフォルト値は、cn=admin,ou=sa,o=system です。
管理者パスワード	管理者オブジェクトのパスワードを指定します。たとえば、password です。
Identity Vault サーバコンテキスト (LDAP 形式)	サーバコンテナの DN を指定します。デフォルト値は ou=servers, o=system です。
Identity Vault ドライバセット (LDAP 形式)	ドライバセットのコンテキスト DN を指定します。デフォルト値は cn=DriverSet, o=system です。
平文 LDAP ポート	識別ボールトが平文の LDAP 要求をリスンするポートを指定します。デフォルトの設定は 389 です。
セキュア LDAP ポート	識別ボールトが SSL (Secure Sockets Layer) プロトコルを使用した LDAP 要求をリスンするポートを指定します。デフォルトの設定は 636 です。eDirectory がインストールされる前にサーバにロードされているサービスがデフォルトのポートを使用している場合は、別のポートを指定する必要があります。
平文 HTTP ポート	HTTP スタックが動作するポートを平文で指定します。デフォルト値は 8028 です。
Secure HTTP port (セキュア HTTP ポート)	HTTP スタックが TLS/SSL プロトコルを使用して動作するポートを指定します。デフォルトの設定は 8030 です。
RSA Key Size	[新しいツリーの作成] オプションを選択した場合にのみ適用されます。 RSA 証明書のキーサイズを指定します。使用可能な値は 2048、4096、および 8192 ビットです。デフォルトの設定は 4096 です。
EC Curve	[新しいツリーの作成] オプションを選択した場合にのみ適用されます。 EC 証明書の楕円曲線 (EC) 制限を指定します。使用可能な値は P256、P384、および P521 です。デフォルト値は P384 です。

パラメータ	説明
証明書の有効期間	[新しいツリーの作成] オプションを選択した場合にのみ適用されます。 証明書の有効期間を年単位で指定します。
iManager HTTP ポート	Tomcat アプリケーションサーバの HTTP ポートを指定します。デフォルトの設定は 8080 です。
iManager SSL ポート	Tomcat アプリケーションサーバの HTTPS ポートを指定します。デフォルトの設定は 8443 です。

Identity Applications の環境設定ワークシート

以下のワークシートを使用して、Identity Applications を設定するときに指定する必要がある情報を収集できます。

表 3-3 *Identity Applications の設定*

パラメータ	説明
Install Self-Service Password Reset (Self-Service Password Reset のインストール)	SSPR コンポーネントをインストールするかどうかを指定します。
ホスト	アイデンティティボールトがインストールされているサーバの IP アドレスを指定します。
セキュア LDAP ポート	識別ボールトが SSL (Secure Sockets Layer) プロトコルを使用した LDAP 要求をリスンするポートを指定します。デフォルトの設定は 636 です。eDirectory がインストールされる前にサーバにロードされているサービスがデフォルトのポートを使用している場合は、別のポートを指定する必要があります。
管理者 DN	Identity Manager エンジンの管理者名を指定します。デフォルト値は、cn=admin,ou=sa,o=system です。
管理者パスワード	新しい認証サーバをインストールする場合にのみ適用されます。LDAP 認証サーバの管理者アカウントのパスワードを指定します。
ルートコンテナ DN	ルートコンテナを指定します。デフォルト値は o=data です。
ユーザコンテナ DN	新しい認証サーバをインストールする場合にのみ適用されます。 Access Review にログイン可能なユーザアカウントを保存する LDAP 認証サーバ内のコンテナを指定します。たとえば、o=data です。

パラメータ	説明
管理者コンテナ DN	新しい認証サーバをインストールする場合にのみ適用されます。 管理者アカウントを保存する LDAP 認証サーバ内のコンテナを指定します。
ドライバセット DN	ドライバセット DN を指定します。
Deploy Identity Applications Drivers (Identity Applications ドライバの展開)	ユーザアプリケーションドライバと役割およびリソースサービスドライバを展開する場合は、このオプションを選択します。
Select the Database Platform for Identity Applications (Identity Applications のデータベースプラットフォームを選択)	Identity Applications で使用するデータベースを選択します。オプションは、PostgreSQL、Oracle、および Microsoft SQL Server です。
新しい PostgreSQL サーバ	PostgreSQL データベースの新しいインスタンスをインストールする場合は、このオプションを選択します。
既存の PostgreSQL サーバ	既存の PostgreSQL データベースサーバに接続する場合は、このオプションを選択します。
データベースホスト	サーバの名または IP アドレスを指定します。
データベースポート	サーバがユーザアプリケーションとの通信に使用するポートを指定します。デフォルトでは値は 5432 に設定されています。
Identity アプリケーションデータベース名	Identity Applications のデータベース名を指定します。
ワークフローエンジンデータベース名	ワークフローエンジンのデータベース名を指定します。
データベースユーザ	ユーザアプリケーションによるデータベースデータのアクセスと変更を許可するアカウント名を指定します。
データベースユーザのパスワード	データベースのユーザのパスワードを指定します。
データベースドライバ Jar	データベースプラットフォームの JAR ファイルを指定します。ドライバ JAR ファイルは、データベースベンダーにより提供され、データベースサーバのシンクライアント JAR を表します。たとえば、PostgreSQL の場合、postgresql-9.4-1212.jdbc42.jar(デフォルトでは C:\NetIQ\idm\apps\Postgres フォルダにあります) を指定できます。NetIQ では、サードパーティベンダのドライバ JAR ファイルをサポートしていません。
When would you like the schema to be created (スキーマをいつ作成するか)	データベーススキーマをパートプロセスとしていつ作成するかを指定します。使用可能なオプションは、**[Now (今すぐ)]**、**[At Application Startup (アプリケーションの開始時)]**、および **[Write SQL to a File (SQL のファイルへの書き込み時)]** です。
アプリケーションサーバホスト	Tomcat がインストールされる IP アドレスを指定します。

パラメータ	説明
アプリケーションサーバ HTTPS ポート	Tomcat がインストールされるポートを指定します。デフォルトでは値は 8543 に設定されています。
ログイン画面名	ユーザログイン画面に表示するカスタム名を指定します。デフォルト値は Identity Access (Identity Access) です。 Identity Applications をアップグレードする際には、ログイン画面名が自動的に NetIQ Access に変更されます。
Identity Applications Administrator (識別情報アプリケーション管理者)	LDAP 認証サーバの管理者アカウントの DN を指定します。たとえば、cn=uaadmin,ou=sa,o=data
管理者パスワード	Identity Applications 管理者パスワードを指定します。
Set this password as a common password for other settings (このパスワードを他の設定の共通パスワードとして設定)	共通のパスワードを設定する場合は、このオプションを選択します。 **注 :** Tomcat キーストアのデフォルトパスワードは changeit です。
OAuth Keystore Password (OAuth キーストアのパスワード)	**[Set this password as a common password for other settings (このパスワードを他の設定の共通パスワードとして設定)]** チェックボックスを選択している場合にのみ適用されます。 OAuth キーストアパスワードを指定します。
SS0 クライアントパスワード	**[Set this password as a common password for other settings (このパスワードを他の設定の共通パスワードとして設定)]** チェックボックスを選択している場合にのみ適用されます。 SSO クライアントパスワードを指定します。
SSPR 設定パスワード	**[Set this password as a common password for other settings (このパスワードを他の設定の共通パスワードとして設定)]** チェックボックスを選択している場合にのみ適用されます。 SSPR 設定パスワードを指定します。
フォームレンダラ HTTPS ポート	フォームレンダラ HTTPS ポートを指定します。デフォルトでは値は 8600 に設定されています。
ワークフローエンジン ID	ワークフローエンジン ID の一意の値を指定します。

Identity Reporting の環境設定ワークシート

以下のワークシートを使用して、Identity Reporting を設定するときに指定する必要がある情報を収集できます。

表 3-4 Identity Reporting の設定

パラメータ	説明
ホスト	アイデンティティボールトがインストールされているサーバの IP アドレスを指定します。
セキュア LDAP ポート	識別ボールトが SSL (Secure Sockets Layer) プロトコルを使用した LDAP 要求をリスンするポートを指定します。デフォルトの設定は 636 です。eDirectory がインストールされる前にサーバにロードされているサービスがデフォルトのポートを使用している場合は、別のポートを指定する必要があります。
管理者 DN	Identity Manager エンジンの管理者名を指定します。デフォルト値は、cn=admin,ou=sa,o=system です。
管理者パスワード	LDAP 認証サーバの管理者アカウントのパスワードを指定します。
ユーザコンテナ DN	新しい認証サーバをインストールする場合にのみ適用されます。 Access Review にログイン可能なユーザアカウントを保存する LDAP 認証サーバ内のコンテナを指定します。たとえば、o=data です。
管理者コンテナ DN	新しい認証サーバをインストールする場合にのみ適用されます。 管理者アカウントを保存する LDAP 認証サーバ内のコンテナを指定します。
ドライバセット DN	ドライバセット DN を指定します。
Deploy Identity Reporting Drivers (Identity Reporting ドライバの展開)	データ収集サービスドライバと Managed System Gateway サービスドライバを展開する場合は、このオプションを選択します。
Select the Database Platform for Identity Reporting (Identity Reporting のデータベースプラットフォームを選択)	Identity Reporting で使用するデータベースを選択します。オプションは、PostgreSQL、Oracle、および Microsoft SQL Server です。
新しい PostgreSQL サーバ	PostgreSQL データベースの新しいインスタンスをインストールする場合は、このオプションを選択します。
既存の PostgreSQL サーバ	既存の PostgreSQL データベースサーバに接続する場合は、このオプションを選択します。
データベースホスト	サーバの名または IP アドレスを指定します。
データベースポート	サーバが Identity Reporting との通信に使用するポートを指定します。デフォルトでは値は 5432 に設定されています。
データベース名	Identity Reporting のデータベース名を指定します。

パラメータ	説明
データベースユーザのパスワード	データベースのユーザのパスワードを指定します。
データベースアカウントパスワード	Identity Reporting のデータベースアカウントパスワードを指定します。
アプリケーションサーバホスト	Tomcat がインストールされる IP アドレスを指定します。
アプリケーションサーバ HTTPS ポート	Tomcat がインストールされるポートを指定します。デフォルトでは値は 8543 に設定されています。
外部 OSP サーバ	外部の OSP サーバに接続する場合は、このオプションを選択します。たとえば、Identity Applications が使用するリモート OPS に接続する場合は、このオプションを使用します。
OSP サーバホスト	**[外部 OSP サーバ]** オプションを選択した場合にのみ適用されます。 OSP がインストールされているサーバの IP アドレスを指定します。
OSP サーバポート	**[外部 OSP サーバ]** オプションを選択した場合にのみ適用されます。 OSP サーバポートを指定します。
OSP キーストア	**[外部 OSP サーバ]** オプションを選択した場合にのみ適用されます。 OSP キーストアファイルの場所を指定します。
OSP キーストアパスワード	**[外部 OSP サーバ]** オプションを選択した場合にのみ適用されます。 OSP キーストアパスワードを指定します。
OSP クライアントパスワード	**[外部 OSP サーバ]** オプションを選択した場合にのみ適用されます。 OSP クライアントパスワードを指定します。
Identity Reporting 管理者	Identity Reporting の管理者名を指定します。デフォルト値は、cn=uaadmin,ou=sa,o=data です。
Identity Reporting 管理者パスワード	Identity Reporting の管理者パスワードを指定します。
Set this password as a common password for other settings (このパスワードを他の設定の共通パスワードとして設定)	共通のパスワードを設定する場合は、このオプションを選択します。

Self-Service Password Reset の環境設定ワークシート

以下のワークシートを使用して、Self-Service Password Reset (SSPR) を設定するときに指定する必要がある情報を収集できます。

このセクションは、Identity Applications と SSPR を別々のコンピュータにインストールする場合にのみ適用されます。

表 3-5 SSPR 設定

パラメータ	説明
ホスト	アイデンティティボールトがインストールされているサーバの IP アドレスを指定します。
セキュア LDAP ポート	識別ボールトが SSL (Secure Sockets Layer) プロトコルを使用した LDAP 要求をリスンするポートを指定します。デフォルトの設定は 636 です。eDirectory がインストールされる前にサーバにロードされているサービスがデフォルトのポートを使用している場合は、別のポートを指定する必要があります。
管理者 DN	Identity Manager エンジンの管理者名を指定します。デフォルト値は、cn=admin,ou=sa,o=system です。
管理者パスワード	LDAP 認証サーバの管理者アカウントのパスワードを指定します。
ユーザコンテナ DN	新しい認証サーバをインストールする場合にのみ適用されます。 Access Review にログイン可能なユーザアカウントを保存する LDAP 認証サーバ内のコンテナを指定します。たとえば、o=data です。
管理者コンテナ DN	新しい認証サーバをインストールする場合にのみ適用されます。 管理者アカウントを保存する LDAP 認証サーバ内のコンテナを指定します。
アプリケーションサーバホスト	Tomcat がインストールされる IP アドレスを指定します。
アプリケーションサーバ HTTPS ポート	Tomcat がインストールされるポートを指定します。デフォルトでは値は 8543 に設定されています。
Identity Applications Administrator (識別情報アプリケーション管理者)	LDAP 認証サーバの管理者アカウントの DN を指定します。たとえば、cn=uaadmin,ou=sa,o=data
管理者パスワード	Identity Applications 管理者パスワードを指定します。
アプリケーションサーバホスト	OSP がインストールされているサーバの IP アドレスを指定します。
アプリケーションサーバ HTTPS ポート	OSP サーバ HTTPS ポートを指定します。

パラメータ	説明
認証サーバクライアントパスワード	OSP クライアントパスワードを指定します。

インストール後の手順

このセクションでは、識別情報アプリケーションのインストール後に Tomcat 環境を更新する方法について説明します。

- 65 ページの 「preferIPv4Stack プロパティを JVM に渡す」
- 65 ページの 「サーバのヘルスの確認」
- 66 ページの 「ヘルスの統計の監視」
- 66 ページの 「複合インデックスの作成」
- 68 ページの 「クライアントが開始した SSL 再ネゴーシエーションを拒否するように Identity Applications を設定する」

preferIPv4Stack プロパティを JVM に渡す

識別情報アプリケーションは、JGroups を使用してキャッシュを実装します。環境設定によっては、mcast_addr のバインディングが確実に成功するように、preferIPv4Stack プロパティを true に設定するように JGroups が要求します。

このオプションが設定されていない場合、次のエラーが発生する可能性があります。

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

次のエラーも発生する可能性があります。

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

パラメータ java.net.preferIPv4Stack=true は、たとえば extend.local.config.dir のようなその他のシステムプロパティと同じ方法で設定できるシステムプロパティです。

サーバのヘルスの確認

ほとんどのロードバランサは、HTTP サーバが稼働しおよびリスンしているかどうかを判断するためのヘルスチェック機能を提供します。ユーザアプリケーションには、ロードバランサに HTTP ヘルスチェックを設定するために使用できる URL が含まれます。URL は次のとおりです。

http://<NodeIP>:port/IDMProv/jsps/healthcheck.jsp

ヘルスの統計の監視

REST API により、ユーザアプリケーションのヘルスに関する情報を取得できます。API は、現在実行中のスレッド、メモリ消費、キャッシュ、およびクラスタ情報についてシステムにアクセスし、GET 操作を使用して情報を返します。

- **メモリの情報 (JVM およびシステムメモリ):** システムメモリ、JVM によって消費されるメモリなどのメモリ関連の情報を読み込みます。

  次に例を示します。

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

- **スレッドの情報 :** CPU 集約型スレッドに関する情報を読み込み、CPU の高負荷の原因となるトップスレッドのリストを返します。

  次に例を示します。

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

  JVM のスレッドのスタックトレースにアクセスするには、スタックパラメータを **[True]** に設定します。

  次に例を示します。

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

  JVM のスレッド数を指定するには、**[thread-count]** パラメータの値を指定します。

  次に例を示します。

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

- **キャッシュの情報 :** ユーザアプリケーションのキャッシュ情報を読み込みます。

  次に例を示します。

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

- **クラスタの情報 :** クラスタ関連の情報を読み込みます。

  次に例を示します。

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

注 : REST API を使用して、ユーザアプリケーションヘルス統計を表示するには、セキュリティ管理者である必要があります。

複合インデックスの作成

アイデンティティアプリケーションをインストールまたはアップグレードした後で、Identity Manager ダッシュボードでユーザをソートするために使用する各属性の複合インデックスを手動で作成します。eDirectory インストールパスにある ndsindex ユーティリティ

を使用して複合インデックスを作成できます。複合インデックスに $ 記号を使用して区切られる複数の属性を指定できます。複合インデックスに必要な基本属性を以下に示します。

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

次のコマンドは、ndsindex ユーティリティを使用して複合インデックスを作成できます。

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

たとえば、[Title (役職)] に基づいてユーザをソートするには、次のコマンドを実行します。

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

変換エクスポートユーティリティを使用して複合インデックスを作成することもできます。

インデックスを作成するには、LDIF ファイルを使用する必要があります。LDIF ファイルがインポートされた後で、リンバをトリガすることでインデックス作成アクティビティを起動します。そうでない場合は、リンバが自動的にトリガされるときにインデックスが作成されます。

[タイトル] 属性でユーザをソートするための複合インデックスを作成する LDIF ファイルの例 :

```
dn: cn=osg-nw5-7, o=Novell

changetype: modify

add: indexDefinition

indexDefinition: 0$sntitleindex$0$0$0$1$Title$surname
```

詳細については、『*NetIQ eDirectory 管理ガイド*』の「LDIF ファイル」を参照してください。

クライアントが開始した SSL 再ネゴーシエーションを拒否するように Identity Applications を設定する

デフォルトでは、Identity Applications インストーラは非セキュア接続 (http) を設定します。特定の条件下では、非セキュア接続を使用すると、クライアントが開始した Identity Applications サーバとの SSL 再ネゴーシエーションが原因で、Identity Manager がサービス拒否攻撃にさらされる可能性が高まります。この問題を回避するため、<tomcat-install-directory>\bin\setenv.bat ファイルの CATALINA_OPTS エントリに次のフラグを追加します。

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

4 インストールを完了するための最終ステップ

Identity Manager コンポーネントのインストールと設定が完了したら、ご使用の環境でソリューションが適切に機能するように特定のタスクを実行する必要があります。たとえば、ビジネスプロセスで定義されたポリシーと要件を満たすようにインストールしたドライバを設定し、監査イベントを収集するように Sentinel Log Management for IGA を設定します。

インストール後のタスクには、通常次の項目が含まれます。

- 69 ページの 「Identity Vault の設定」
- 70 ページの 「リモートローダとドライバの設定」
- 70 ページの 「パスワードを忘れた場合の管理の設定」
- 75 ページの 「識別情報アプリケーションのデータベースの設定」
- 78 ページの 「識別情報アプリケーションの設定」
- 106 ページの 「データ収集用のランタイム環境の設定」
- 115 ページの 「Identity Reporting の設定」
- 120 ページの 「Identity Manager のアクティベート」
- 121 ページの 「Identity Manager コンポーネントが使用するポートの確認」

Identity Vault の設定

- アイデンティティボールトへの Identity Applications および Identity Reporting 証明書の手動インポート

アイデンティティボールトへの Identity Applications および Identity Reporting 証明書の手動インポート

- Identity Applications および Identity Reporting コンポーネントのカスタム証明書がある場合は、これらの証明書をアイデンティティボールトの cacerts (C:\NetIQ\eDirectory\jre\lib\security\cacerts) にインポートします。

  たとえば、次の keytool コマンドを使用して、証明書をアイデンティティボールトにインポートすることができます。

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

- SSPR をユーザアプリケーションサーバとは異なるサーバにインストールする場合、SSPR アプリケーション証明書をユーザアプリケーションの idm.jks (C:\NetIQ\idm\apps\tomcat\conf\idm.jks) にインポートします。

  たとえば、次の keytool コマンドを使用して、証明書をユーザアプリケーションにインポートすることができます。

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

リモートローダとドライバの設定

リモートローダにより、Identity Manager ドライバは、接続されたアプリケーションと同じサーバにアイデンティティボールトおよび Identity Manager エンジンをインストールすることなく、接続されたアプリケーションにアクセスできます。リモートローダを使用するには、Identity Manager エンジンと安全に接続できるようにアプリケーションシムを設定する必要があります。さらに、リモートローダと Identity Manager ドライバ両方の設定も必要です。この情報は、『*NetIQ Identity Manager Driver Administration Guide*』の「Configuring the Remote Loader and Drivers」に詳細に説明されています。

パスワードを忘れた場合の管理の設定

Identity Manager インストールには、忘れたパスワードをリセットするプロセスの管理に役立つセルフサービスパスワードリセットが含まれています。それとは別に、外部パスワード管理システムを使用する方法があります。

- 70 ページの 「Self Service Password Reset によるパスワードを忘れた場合の管理」
- 73 ページの 「外部システムによるパスワードを忘れた場合の管理」
- 74 ページの「分散環境またはクラスタ化環境におけるダッシュボードの SSPR リンクの更新」

Self Service Password Reset によるパスワードを忘れた場合の管理

SSPR と識別情報アプリケーションをインストールすると、通常はパスワードを忘れた場合の管理を有効にできます。ただし、パスワードを変更した後に SSPR がユーザを転送する識別情報アプリケーションのランディングページの URL を指定していない場合があります。また、パスワードを忘れた場合の管理を有効にする必要がある場合もあります。この節では、次のトピックについて説明します。

- 71 ページの「セルフサービスパスワードリセットを使用するための Identity Manager の設定」
- 71 ページの「Identity Manager で使用するためのセルフサービスパスワードリセットの設定」
- 72 ページの 「SSPR 設定のロック」

セルフサービスパスワードリセットを使用するための Identity Manager の設定

このセクションでは、SSPR を使用するために Identity Manager を設定する方法について説明します。

1 識別情報アプリケーションをインストールしたサーバにログインします。

2 設定更新ユーティリティを実行します。詳細については、49 ページのセクション 3「インストールおよび設定プロセスの概要」を参照してください。

3 ユーティリティで **[認証] > [パスワードの管理]** の順に移動します。

4 **[パスワード管理プロバイダ]** では、**[Self-Service Password Reset (SSPR)]** を指定します。

5 (オプション) ユーザ名またはパスワードをリセットするためのリンク、または Identity Applications ログインページで新しいユーザアカウントをアクティブにするためのリンクを提供するには、**[ユーザインタフェース]** ドロップダウンリストから **[Other links (その他のリンク)]** を選択してから、必要なチェックボックスを選択します。または、**[ユーザインタフェース]** ドロップダウンリストから、**[Can't sign in? (サインインできませんか ?)]** を選択して、共通リンクを提供することもできます。Identity Applications ログインページに次のリンクが表示されます。**[Click here if you've forgotten your username or password, or if you need to register. (ユーザ名またはパスワードを忘れた場合、または登録が必要な場合は、ここをクリックしてください。)]**

6 **[IDM SSO Clients (IDM SSO クライアント)] > [Self Service Password Reset]** の順に移動します。

7 **[OAuth クライアント ID]** では、認証サーバに認識させる SSPR のシングルサインオンクライアントの名前を指定します。デフォルト値は sspr です。

8 **[OAuth クライアントシークレット]** では、SSPR のシングルサインオンクライアントのパスワードを指定します。

9 **[OAuth redirect URL (OAuth リダイレクト URL)]** では、認証完了時に認証サーバがブラウザクライアントをリダイレクトする絶対 URL を指定します。

   次の形式を使用を使用します : protocol://server:port/path。たとえば、http://10.10.10.48:8180/sspr/public/oauth です。

10 変更を保存して、ユーティリティを閉じます。

Identity Manager で使用するためのセルフサービスパスワードリセットの設定

このセクションでは、Identity Manager と一緒に使用するために SSPR を設定する方法について説明します。たとえば、パスワードポリシーや秘密の質問の答えの質問を変更できます。

Identity Manager と一緒に SSPR をインストールしたときに、管理者がこのアプリケーションを設定するために使用できるパスワードを指定しました。SSPR 設定を変更してから、管理者アカウントまたは管理者グループが SSPR を設定できるように指定することをお勧めします。

注 : ユーザアプリケーションサーバとは異なるサーバに SSPR をインストールする場合は、SSPR アプリケーション証明書がユーザアプリケーション cacerts に追加されていることを確認します。

1 インストール時に指定した設定パスワードを使用して、SSPR にログインします。

2 ［設定］ページで、パスワードポリシーと秘密の質問の答えの質問の設定を変更します。SSPR 設定のデフォルト値を設定する方法の詳細については、『*NetIQ Self Service Password Reset Administration Guide*』の「Configuring Self Service Password Reset」を参照してください。

3 SSPR 設定ファイル (SSPRConfiguartion.xml) をロックします。設定ファイルのロックの詳細については、72 ページの 「SSPR 設定のロック」を参照してください。

4 (オプション) 設定をロックした後で SSPR 設定を変更するには、SSPRConfiguartion.xml ファイルで configIsEditable 設定を true に設定する必要があります。

5 SSPR からログアウトします。

6 変更を有効にするには、Tomcat を再起動します。

SSPR 設定のロック

1 **[http://<IP/DNS name>:<port>/sspr]** にアクセスします。SSPR ポータルに移動します。

2 Identity Manager に管理者アカウントでログインするか、または既存のログイン資格情報でログインします。

3 ページ上部の **[Configuration Manager (環境設定マネージャ)]** をクリックし、インストール時に指定した設定パスワードを指定します。

4 **[Configuration Editor (環境設定エディタ)]** をクリックし、**[設定］ > ［LDAP Settings (LDAP 設定)]** の順に移動します。

5 SSPR 設定ファイル (SSPRConfiguartion.xml) をロックします。

5a ［Administrator Permission (管理者許可)］セクションで、識別ボールト内の SSPR に対する管理者権限を持つユーザまたはグループを表すフィルタを LDAP フォーマットで定義します。デフォルトでは、このフィルタは groupMembership=cn=Admins,ou=Groups,o=example と設定されています。

たとえば、ユーザアプリケーション管理者の場合は「uaadmin (cn=uaadmin)」と設定します。

これにより、設定を変更するためのすべての権限を持つ SSPR 管理者ユーザを除いて、ユーザは SSPR で設定を変更できなくなります。

5b LDAP クエリが結果を返していることを確認するために、**[View Matches (一致の表示)]** をクリックします。

設定にエラーがある場合は、次の設定オプションに進めません。SSPR は問題のトラブルシューティングに役立つエラー詳細を表示します。

5c **[保存]** をクリックします。

5d ポップアップされる確認ウィンドウで [OK] をクリックします。

SSPR がロックされている間は、管理者ユーザが表示する管理インタフェースには、［Dashboard (ダッシュボード)］、［User Activity (ユーザアクティビティ)］、［Data Analysis (データ分析)］など、SSPR がロックされる前は表示されていなかった追加オプションが表示されます。

6 (オプション) 設定をロックした後で SSPR 設定を変更するには、SSPRConfiguartion.xml ファイルで configIsEditable 設定を true に設定する必要があります。

7 SSPR からログアウトします。

8 ステップ 3 で定義されている管理者ユーザとして SSPR に再ログインします。

9 [Close Configuration (設定を閉じる)] をクリックし、[OK] をクリックして変更を確認します。

10 変更を有効にするには、Tomcat を再起動します。

外部システムによるパスワードを忘れた場合の管理

外部システムを使用するには、パスワードを忘れた場合機能を含む WAR ファイルの場所を指定する必要があります。このプロセスには次の作業が含まれます。

- 73 ページの 「外部からパスワードを忘れた場合を管理する WAR ファイルの指定」
- 74 ページの 「外部パスワードを忘れた場合の環境設定のテスト」
- 74 ページの 「アプリケーションサーバ間の SSL 通信の設定」

外部からパスワードを忘れた場合を管理する WAR ファイルの指定

インストール時にこれらの値を指定せずに、後で設定を変更する場合、RBPM 設定ユーティリティを使用するか、ユーザアプリケーションで管理者として変更します。

1 (状況によって実行) RBPM 設定ユーティリティで設定を変更するには、次の手順を実行します。

1a 識別情報アプリケーションをインストールしたサーバにログインします。

1b RBPM 設定ユーティリティを実行します。詳細については、49 ページのセクション 3「インストールおよび設定プロセスの概要」を参照してください。

1c ユーティリティで [認証］ > ［パスワードの管理] の順に移動します。

1d [パスワード管理プロバイダ] では [ユーザアプリケーション (レガシ)] を指定します。

2 (状況によって実行) ユーザアプリケーションで設定を変更するには、次の手順を実行します。

2a ユーザアプリケーションの管理者としてログインします。

2b [管理］ > ［アプリケーション環境設定］ > ［パスワードモジュールのセットアップ］ > ［ログイン] の順に移動します。

3 ［**パスワードを忘れた場合**］では、[外部] を指定します。

4 [パスワードを忘れた場合リンク] では、ログインページでユーザが［**パスワードを忘れた場合**］をクリックしたときに表示するリンクを指定します。ユーザがこのリンクをクリックすると、アプリケーションはユーザを外部パスワード管理システムに転送します。次に例を示します。

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

5 [パスワードを忘れた場合の返信リンク] では、ユーザがパスワードを忘れた場合の手順の実行完了後に表示するリンクを指定します。このリンクをクリックすると、指定したリンクにリダイレクトされます。次に例を示します。

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

6 [パスワードを忘れた場合の Web サービス URL] では、パスワードを忘れた場合の外部 WAR が識別情報アプリケーションを呼び戻すために使用する Web サービスの URL を指定します。次の形式を使用してください。

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

識別情報アプリケーションに対してセキュアな Web サービス通信を保証するために、返信リンクでは SSL を使用する必要があります。詳細については、74 ページの 「アプリケーションサーバ間の SSL 通信の設定」を参照してください。

7 ExternalPwd.war を、外部パスワード WAR 機能を実行するリモートアプリケーションサーバ展開ディレクトリに手動でコピーします。

外部パスワードを忘れた場合の環境設定のテスト

外部パスワード WAR ファイルがあり、これにアクセスして［パスワードを忘れた場合］機能をテストする場合は、次の場所でアクセスできます。

- ブラウザ内で直接アクセスします。外部パスワード WAR ファイルで［パスワードを忘れた場合］ページに移動します。たとえば、http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp に移動します。
- ユーザアプリケーションログインページで、[パスワードを忘れた場合] のリンクをクリックします。

アプリケーションサーバ間の SSL 通信の設定

外部パスワード管理システムを使用する場合、アイデンティティアプリケーションおよびパスワードを忘れた場合の外部管理 WAR ファイルを展開している Tomcat インスタンス間に SSL 通信を設定する必要があります。詳細については、Tomcat マニュアルを参照してください。

分散環境またはクラスタ化環境におけるダッシュボードの SSPR リンクの更新

インストールプロセスは、識別情報アプリケーションおよび Identity Reporting と同じアプリケーションサーバ上に SSPR が展開されていると想定しています。デフォルトでは、ダッシュボードの [アプリケーション] ページにある組み込みリンクは、ローカルシステム

上の SSPR を参照する相対 URL フォーマットを使用します。たとえば、\sspr\private\changepassword です。分散環境またはクラスタ化環境にアプリケーションをインストールする場合、SSPR リンクの URL を更新する必要があります。

詳細については、*アイデンティティアプリケーションのヘルプ*を参照してください。

1. ダッシュボードに管理者としてログインします。たとえば、uaadmin としてログインします。
2. **[編集]** をクリックします。
3. ［Edit Home Items (ホームアイテムの編集)］ページで、更新するアイテムの上にマウスを移動し、編集アイコンをクリックします。たとえば、**[マイパスワードの変更]** を選択します。
4. **[リンク]** では絶対 URL を指定します。たとえば、「http://10.10.10.48:8180/sspr/changepassword」と指定します。
5. **[保存]** をクリックします。
6. 更新する SSPR リンクごとにこの手順を繰り返します。
7. 終了したら、**[I'm done (完了)]** をクリックします。
8. ログアウトしてから一般ユーザとしてログインし、変更されているかどうかをテストします。

識別情報アプリケーションのデータベースの設定

識別情報アプリケーションのデータベースは、設定データの保存やワークフローアクティビティのデータの保存などのタスクをサポートします。アプリケーションをインストールする前に、データベースがインストールされ、設定されている必要があります。サポートされているデータベースの詳細については、NetIQ Identity Manager システム要件ページを参照してください。

注 : 新しいバージョンの RBPM と識別情報アプリケーションに移行する場合、前のインストールで使用していたデータベースと同じデータベースを使用する必要があります。前のインストールとは、移行元のインストールのことです。

- 75 ページの 「Oracle データベースの設定」
- 77 ページの 「SQL Server データベースの設定」

Oracle データベースの設定

このセクションでは、ユーザアプリケーションで Oracle データベースを使用する場合の設定オプションについて説明します。サポートされている Oracle のバージョンについては、NetIQ Identity Manager 技術情報 Web サイトを参照してください。

データベースの互換性レベルの確認

Oracle の異なるリリースからのデータベースは、これらが同じ機能をサポートし、これらの機能が同様に実行される場合には互換性があります。互換性がない場合は、特定の機能または操作が想定されるように動作しない場合があります。たとえば、識別情報アプリケーションを展開できないスキーマの作成は失敗します。

データベースの互換性レベルを確認するには、次の手順を実行します。

1. データベースエンジンに接続します。
2. SQL Server データベースエンジンの適切なインスタンスに接続した後で、**[オブジェクトエクスプローラ]** で、サーバ名をクリックします。
3. **[データベース]** を展開します。さらに、データベースに応じて、ユーザデータベースを選択するか、**[システムデータベース]** を展開してシステムデータベースを選択します。
4. データベースを右クリックし、**[プロパティ]** をクリックします。

   [データベースのプロパティ] ダイアログボックスが開きます。
5. **[ページの選択]** ペインで、**[オプション]** をクリックします。

   現在の互換性レベルが **[互換性レベル]** リストボックスに表示されます。
6. **[互換性レベル]** を確認するには、クエリウィンドウで以下を入力し、**[実行]** をクリックします。

   SQL> SELECT name, value FROM v$parameter

   WHERE name = 'compatible';

予期される結果は 12.2.0.1 です

文字セットの設定

ユーザアプリケーションデータベースは、Unicode エンコーディング文字セットを使用する必要があります。データベースを作成する際に AL32UTF8 を使用してこの文字セットを指定します。

Oracle 12c データベースに UTF-8 が設定されていることを確認するには、次のコマンドを実行します。

```
select * from nls_database_parameters;
```

データベースに UTF-8 が設定されていない場合、次の情報が表示されます。

```
NLS_CHARACTERSET
WE8MSWIN1252
```

設定されている場合、データベースに UTF-8 が設定されていることを示す次の情報が表示されます。

```
NLS_CHARACTERSET
AL32UTF8
```

注 : JDBC JAR バージョン ojdbc6.jar を使用することをお勧めします。

文字セットの設定の詳細については、「Choosing an Oracle Database Character Set」を参照してください。

管理者ユーザアカウントの設定

ユーザアプリケーションを使用するには、Oracle データベースユーザアカウントが特定の特権を持つ必要があります。SQL Plus ユーティリティで、次のコマンドを入力します。

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

ここで、*idmuser* はユーザアカウントを表します。

SQL Server データベースの設定

このセクションでは、ユーザアプリケーションで SQL Server データベースを使用する場合の設定オプションについて説明します。サポートされている SQL Server のバージョンについては、NetIQ Identity Manager 技術情報 Web サイトを参照してください。

文字セットの設定

SQL Server では、ユーザはデータベースの文字セットを指定できません。ユーザアプリケーションは SQL Server の文字データを NCHAR カラムタイプ (UTF-8 をサポート) で保存します。

注 : SQL でサポートされている照合は、SQL_Latin1_General_CP1_CI_AS だけです。

管理者ユーザアカウントの設定

Microsoft SQL Server のサポートされているバージョンをインストールした後、SQL Server Management Studio などのアプリケーションを使用してデータベースとデータベースユーザを作成します。データベースユーザアカウントは、次の特権を持つ必要があります。

- CREATE TABLE
- DELETE
- INSERT
- SELECT
- UPDATE

注 : Microsoft SQL Server 2014 では JDBC JAR バージョン sqljdbc4.jar を、Microsoft SQL Server 2016 では sqljdbc42.jar を使用することをお勧めします。

識別情報アプリケーションの設定

- 78 ページの 「識別情報アプリケーションの設定の管理」
- 102 ページの 「識別情報アプリケーション用の REST API の展開」
- 102 ページの 「Oracle サービス名を使用した Oracle データベースへのアクセス」
- 103 ページの 「手動によるデータベーススキーマの作成」
- 105 ページの 「識別情報アプリケーションのシングルサインオン設定の管理」
- 105 ページの 「識別情報アプリケーションの起動」
- 105 ページの 「識別情報アプリケーションの設定と使用方法の検討事項」

識別情報アプリケーションの設定の管理

識別情報アプリケーション設定ユーティリティを使用して、ユーザアプリケーションドライバと識別情報アプリケーションの設定を管理できます。識別情報アプリケーションのインストールプログラムは、アプリケーションの設定にかかる時間を短縮するために、このユーティリティを呼び出します。これらの設定のほとんどは、インストール後にも変更できます。

設定ユーティリティ (configupdate.bat) を実行するファイルは、デフォルトでは、Identity Applications (C:\NetIQ\idm\apps\UserApplication) のインストールサブディレクトリにあります。

注 : クラスタでは、そのすべてのメンバーの環境設定は同一です。

このセクションでは、設定ユーティリティの設定について説明します。これらの設定は複数のタブとして編成されています。Identity Reporting をインストールする場合、インストールプロセスはユーティリティに Identity Reporting 用のパラメータを追加します。

- 78 ページの 「識別情報アプリケーション設定ユーティリティの実行」
- 79 ページの 「User Application Parameters (ユーザアプリケーションのパラメータ)」
- 90 ページの 「Reporting Parameters (Reporting パラメータ)」
- 92 ページの 「認証パラメータ」
- 97 ページの 「SSO Clients Parameters (SSO クライアントパラメータ)」
- 101 ページの 「CEF 監査パラメータ」

識別情報アプリケーション設定ユーティリティの実行

1 テキストエディタで configupdate.properties ファイルを開き、次のオプションが設定されていることを確認します。

```
edit_admin="true"

use_console="false"
```

2 コマンドプロンプトで、設定ユーティリティ (configupdate.bat) を実行します。

注 : ユーティリティが起動するまで数分待つ必要がある場合があります。

User Application Parameters (ユーザアプリケーションのパラメータ)

識別情報アプリケーションを設定する際、このタブでは、識別情報アプリケーションが識別ボールトと通信する場合に使用する値を定義します。いくつかの設定は、インストールプロセスを完了するために必須です。

デフォルトでは、このタブには基本オプションが表示されます。すべての設定を表示するには、**[詳細オプションの表示]** をクリックします。このタブには、次の設定グループがあります。

- 79 ページの 「識別ボールト設定」
- 80 ページの 「識別ボールト DN」
- 83 ページの 「識別ボールトユーザ ID」
- 84 ページの 「識別ボールトユーザグループ」
- 85 ページの 「識別ボールト証明書」
- 85 ページの 「電子メールサーバ設定」
- 88 ページの 「トラステッドキーストア」
- 88 ページの 「NetIQ Sentinel デジタル署名証明書 & キー」
- 88 ページの 「その他」
- 90 ページの 「コンテナオブジェクト」

識別ボールト設定

このセクションでは、識別情報アプリケーションが識別ボールト内のユーザの識別情報と役割にアクセスできるようにする設定を定義します。いくつかの設定は、インストールプロセスを完了するために必須です。

識別ボールトサーバ

必須

LDAP サーバのホスト名または IP アドレスを指定します。たとえば、「myLDAPhost」と指定します。

LDAP ポート

識別ボールトが平文の LDAP 要求をリスンするポートを指定します。デフォルトは 389 です。

LDAP セキュアポート

識別ボールトが SSL (Secure Sockets Layer) プロトコルを使用した LDAP 要求をリスンするポートを指定します。デフォルトは 636 です。

eDirectory がインストールされる前にサーバにロードされているサービスがデフォルトのポートを使用している場合は、別のポートを指定する必要があります。

識別ボールト管理者

必須

LDAP 管理者の資格情報を指定します。たとえば、「cn=admin」というようになります。このユーザは識別ボールトにすでに存在している必要があります。

識別情報アプリケーションはこのアカウントを使用して、識別ボールトへの管理接続を行います。この値は、マスタキーに基づいて暗号化されます。

識別ボールト管理者パスワード

必須

LDAP 管理者のパスワードを指定します。このパスワードは、マスタキーに基づいて暗号化されます。

パブリック匿名アカウントの使用

ログインしていないユーザが LDAP パブリック匿名アカウントにアクセスできるかどうかを指定します。

セキュア管理者接続

RBPM が管理者アカウント関連のすべての通信で SSL プロトコルを使用するかどうかを指定します。この設定を行っても、SSL を必要としない他の処理は SSL を使用せずに処理を実行できます。

注 : このオプションを選択すると、パフォーマンスが低下する可能性があります。

セキュアなユーザ接続

RBPM がログインユーザアカウント関連のすべての通信で TLS/SSL プロトコルを使用するかどうかを指定します。この設定を行っても、TLS/SSL を必要としない他の処理は TLS/SSL を使用せずに動作できます。

注 : このオプションを選択すると、パフォーマンスが低下する可能性があります。

識別ボールト DN

このセクションでは、識別情報アプリケーションと Identity Manager の他のコンポーネントの間で通信できるようにするコンテナとユーザアカウントの識別名を定義します。いくつかの設定は、インストールプロセスを完了するために必須です。

ルートコンテナ DN

必須

ルートコンテナの LDAP 識別名を指定します。これは、ディレクトリ抽象化層で検索ルートが指定されない場合に、デフォルトのエンティティ定義検索ルートとして使用されます。たとえば、「o=mycompany」と指定します。

ユーザコンテナ DN

必須

詳細オプションを表示すると、このパラメータは［識別ボールトユーザ識別情報］に表示されます。

ユーザコンテナの LDAP 識別名 (DN) または完全修飾 LDAP 名を指定します。この設定には次の考慮事項が適用されます。

- このコンテナ (とその下位) のユーザは、識別情報アプリケーションへのログインを許可されます。
- Identity Applications をホストする Tomcat を起動したことがある場合、configupdate.bat ファイルを使用してこの設定を変更することはできません。
- このコンテナには、ユーザがユーザアプリケーションドライバを設定したときに指定したユーザアプリケーション管理者が含まれている必要があります。含まれていない場合、指定したアカウントはワークフローを実行できません。

グループコンテナ DN

必須

詳細オプションを表示すると、このパラメータは［識別ボールトユーザグループ］に表示されます。

グループコンテナの LDAP 識別名 (DN) または完全修飾 LDAP 名を指定します。この設定には次の考慮事項が適用されます。

- ディレクトリ抽象化レイヤ内のエンティティ定義では、この DN を使用します。
- Identity Applications をホストする Tomcat を起動したことがある場合、configupdate.bat ファイルを使用してこの設定を変更することはできません。

ユーザアプリケーションドライバ

必須

ユーザアプリケーションドライバの識別名を指定します。

たとえば、ドライバが UserApplicationDriver、ドライバセットの名前が myDriverSet、ドライバセットのコンテキストが o=myCompany である場合、「cn=UserApplicationDriver,cn=myDriverSet,o=myCompany」と指定します。

ユーザアプリケーション管理者

必須

ユーザアプリケーションの指定したユーザコンテナの管理タスクを実行する権限を持つ識別ボールト内の既存のユーザアカウントを指定します。この設定には次の考慮事項が適用されます。

- ユーザアプリケーションをホストする Tomcat を起動したことがある場合、configupdate.bat ファイルを使用してこの設定を変更することはできません。
- ユーザアプリケーションの展開後にこの割り当てを変更するには、ユーザアプリケーションの **[管理］ > ［セキュリティ]** ページを使用します。

- このユーザアカウントは、ユーザアプリケーションの [管理] タブを使用してポータルを管理する権利を持ちます。
- ユーザアプリケーション管理者が、iManager、Designer、またはユーザアプリケーション ([要求と承認] タブ) に公開されているワークフロー管理タスクに参加する場合は、この管理者に、ユーザアプリケーションドライバに含まれるオブジェクトインスタンスに対する適切なトラスティ権限を与える必要があります。詳細については、『*User Application Administration Guide*』を参照してください。

プロビジョニング管理者

ユーザアプリケーション全体で使用可能なプロビジョニングワークフロー機能を管理する識別ボールト内の既存のユーザアカウントを指定します。

ユーザアプリケーションを展開した後でこの割り当てを変更するには、ユーザアプリケーションの [管理］ >［管理者の割り当て] ページを使用します。

整合性管理者

[コンプライアンス] タブのすべての機能を実行することをメンバーに許可するシステム役割を実行する識別ボールト内の既存のアカウントを指定します。この設定には次の考慮事項が適用されます。

- 識別情報アプリケーションを展開した後にこの割り当てを変更するには、ユーザアプリケーションの [管理］ >［管理者の割り当て] ページを使用します。
- 設定を更新する際、この値に対する変更が有効になるのは、有効なコンプライアンス管理者が割り当てられていない場合のみです。有効なコンプライアンス管理者が存在する場合は、変更は保存されません。

役割管理者

任意の役割の作成、削除、または変更および任意のユーザ、グループ、またはコンテナへの役割割り当ての付与または取消をメンバーに許可する役割を指定します。さらに役割のメンバーは、任意のユーザに対してレポートを実行できます。この設定には次の考慮事項が適用されます。

- デフォルトでは、この役割にはユーザアプリケーション管理者が割り当てられています。
- 識別情報アプリケーションを展開した後にこの割り当てを変更するには、ユーザアプリケーションの [管理］ >［管理者の割り当て] ページを使用します。
- 設定を更新する際、この値に対する変更が有効になるのは、有効な役割管理者が割り当てられていない場合のみです。有効な役割管理者が存在する場合は、変更は保存されません。

セキュリティ管理者

セキュリティドメイン内のすべての機能をメンバーに付与する役割を指定します。この設定には次の考慮事項が適用されます。

- セキュリティ管理者は、セキュリティドメイン内のすべてのオブジェクトで可能なアクションをすべて実行できます。セキュリティドメインを使用すると、セキュリティ管理者は RBPM 内のすべてのドメインのすべてのオブジェクトのアク

セス許可を設定できます。セキュリティ管理者はチームを構成でき、またドメイン管理者、委任管理者、およびその他のセキュリティ管理者も割り当てることができます。

- 識別情報アプリケーションを展開した後にこの割り当てを変更するには、ユーザアプリケーションの [管理] > [管理者の割り当て] ページを使用します。

リソース管理者

リソースドメイン内のすべての機能をメンバーに付与する役割を指定します。この設定には次の考慮事項が適用されます。

- リソース管理者はリソースドメイン内のすべてのオブジェクトで可能なアクションをすべて実行できます。
- 識別情報アプリケーションを展開した後にこの割り当てを変更するには、ユーザアプリケーションの [管理] > [管理者の割り当て] ページを使用します。

RBPM 設定管理者

構成ドメイン内のすべての機能をメンバーに付与する役割を指定します。この設定には次の考慮事項が適用されます。

- RBPM 設定管理者は、構成ドメイン内のすべてのオブジェクトで可能なアクションをすべて実行できます。RBPM 設定管理者は、RBPM 内のナビゲーション項目へのアクセスを制御します。また、RBPM 設定管理者は委任と代理サービス、ユーザインタフェースのプロビジョニング、およびワークフローエンジンを設定します。
- 識別情報アプリケーションを展開した後にこの割り当てを変更するには、ユーザアプリケーションの [管理] > [管理者の割り当て] ページを使用します。

RBPM レポーティング管理者

レポーティング管理者を指定します。デフォルトでは、インストールプログラムが他のセキュリティフィールドと同じユーザをこの値に表示します。

識別ボールトユーザ ID

このセクションでは、識別情報アプリケーションが識別ボールト内のユーザコンテナと通信できるようにする値を定義します。いくつかの設定は、インストールプロセスを完了するために必須です。

このセクションの設定は、[詳細オプションの表示] を選択した場合のみ表示されます。

ユーザコンテナ DN

必須

詳細オプションを表示していない場合、このパラメータは［識別ボールト DN］に表示されます。

ユーザコンテナの LDAP 識別名 (DN) または完全修飾 LDAP 名を指定します。この設定には次の考慮事項が適用されます。

- このコンテナ (とその下位) のユーザは、識別情報アプリケーションへのログインを許可されます。

- Identity Applications をホストする Tomcat を起動したことがある場合、configupdate.bat ファイルを使用してこの設定を変更することはできません。
- このコンテナには、ユーザがユーザアプリケーションドライバを設定したときに指定したユーザアプリケーション管理者が含まれている必要があります。含まれていない場合、指定したアカウントはワークフローを実行できません。

ユーザ検索スコープ

識別ボールトユーザがコンテナを検索できるスコープの深さを指定します。

ユーザオブジェクトクラス

LDAP ユーザのオブジェクトクラスを指定します。通常は inetOrgPerson です。

ログイン属性

ユーザのログイン名を表す LDAP 属性を指定します。たとえば、「cn」と指定します。

名前付け属性

ユーザまたはグループをルックアップする際に識別子として使用する LDAP 属性を指定します。これはログイン属性とは異なります。ログイン属性はログイン時にのみ使用されます。たとえば、「cn」と指定します。

ユーザメンバーシップ属性

(オプション) ユーザのグループメンバーシップを表す LDAP 属性を指定します。この名前を指定する際、スペースを使用しないでください。

識別ボールトユーザグループ

このセクションでは、識別情報アプリケーションが識別ボールト内のグループコンテナと通信できるようにする値を定義します。いくつかの設定は、インストールプロセスを完了するために必須です。

このセクションの設定は、**[詳細オプションの表示]** を選択した場合のみ表示されます。

グループコンテナ DN

必須

詳細オプションを表示していない場合、このパラメータは［識別ボールト DN］に表示されます。

グループコンテナの LDAP 識別名 (DN) または完全修飾 LDAP 名を指定します。この設定には次の考慮事項が適用されます。

- ディレクトリ抽象化レイヤ内のエンティティ定義では、この DN を使用します。
- Identity Applications をホストする Tomcat を起動したことがある場合、configupdate.bat ファイルを使用してこの設定を変更することはできません。

グループコンテナのスコープ

識別ボールトユーザがグループコンテナを検索できるスコープの深さを指定します。

グループオブジェクトクラス

LDAP グループのオブジェクトクラスを指定します。通常は groupofNames です。

グループメンバーシップ属性

(オプション) ユーザのグループメンバーシップを指定します。この名前にはスペースを使用しないでください。

ダイナミックグループの使用

ダイナミックグループを使用するかどうかを指定します。

[ダイナミックグループオブジェクトクラス] の値も指定する必要があります。

ダイナミックグループオブジェクトクラス

[ダイナミックグループの使用] を選択している場合のみ適用されます。

LDAP ダイナミックグループのオブジェクトクラスを指定します。通常は dynamicGroup です。

識別ボールト証明書

このセクションでは、JRE キーストアのパスとパスワードを定義します。いくつかの設定は、インストールプロセスを完了するために必須です。

キーストアパス

必須

Tomcat が動作するために使用している JRE のキーストア (cacerts) ファイルへのフルパスを指定します。手動でパスを入力するか、または cacerts ファイルを参照して指定できます。この設定には次の考慮事項が適用されます。

- 現在の環境における RBPM のインストールディレクトリを指定する必要があります。デフォルト値は正しい場所に設定されます。
- 識別情報アプリケーションのインストールプログラムは、キーストアファイルを変更します。

キーストアパスワード

必須

キーストアファイルのパスワードを指定します。デフォルトは、「changeit」です。

電子メールサーバ設定

このセクションでは、電子メールベースの承認に使用できる、電子メール通知を有効にする値を定義します。詳細については、『*NetIQ Identity Manager - Identity アプリケーションに対する管理者ガイド*』を参照してください。

通知テンプレートホスト

アイデンティティアプリケーションをホストする Tomcat の名前または IP アドレスを指定します。たとえば、「myapplication serverServer」と指定します。

この値は、電子メールテンプレートの $HOST$ トークンと置き換えられます。インストールプログラムはこの情報を使用して、プロビジョニング要求タスクと承認通知を参照する URL を作成します。

通知テンプレート PORT

アイデンティティアプリケーションをホストする Tomcat のポート番号を指定します。

プロビジョニング要求タスクと承認通知で使用する電子メールテンプレートの $PORT$ トークンがこの値で置き換えられます。

通知テンプレートセキュアポート

アイデンティティアプリケーションをホストする Tomcat のセキュアポート番号を指定します。

プロビジョニング要求タスクと承認通知で使用する電子メールテンプレートの $SECURE_PORT$ トークンがこの値で置き換えられます。

通知テンプレートプロトコル

ユーザの電子メールを送信する際に URL に使用する非セキュアプロトコルを指定します。たとえば、「http」と指定します。

プロビジョニング要求タスクと承認通知で使用する電子メールテンプレートの $PROTOCOL$ トークンがこの値で置き換えられます。

通知テンプレートセキュアプロトコル

ユーザの電子メールを送信する際に URL に使用するセキュアプロトコルを指定します。たとえば、「https」と指定します。

プロビジョニング要求タスクと承認通知で使用する電子メールテンプレートの $SECURE_PROTOCOL$ トークンがこの値で置き換えられます。

通知 SMTP 電子メール送信者

識別情報アプリケーションが電子メール通知を送信するために使用する電子メールアカウントを指定します。

SMTP サーバ名

識別情報アプリケーションがプロビジョニング電子メールに使用する SMTP 電子メールホストの IP アドレスまたは DNS 名を指定します。localhost は使用しないでください。

サーバには認証が必要です

サーバに認証が必要かどうかを指定します。

電子メールサーバに対する資格情報も指定する必要があります。

ユーザ名

[サーバには認証が必要です] を有効にした場合にのみ適用されます。

電子メールサーバのログインアカウントの名前を指定します。

[Password (パスワード)]

[サーバには認証が必要です] を有効にした場合にのみ適用されます。

メールサーバのログインアカウントのパスワードを指定します。

SMTP TLS の使用

メールサーバ間の転送中に電子メールメッセージのコンテンツをセキュリティ保護するかどうかを指定します。

電子メール通知イメージの場所

電子メール通知に添付するイメージへのパスを指定します。

Identity Applications サーバと電子メールサーバの両方がセキュアな接続を使用するように設定されている場合は、次の条件が満たされていることを確認します。

- Identity Applications サーバと電子メールサーバ間のセキュアな接続を確立するために使用される証明書は、信頼できる CA 証明書です。
- イメージパスに https を使用します。たとえば、https://localhost:8543/IDMProv/images です。

Identity Applications がプレーンテキスト通信に http を使用するサーバ上で動作している場合は、イメージパスの https を http に置き換えます。イメージパスの例 : http://localhost:8080/IDMProv/images

Sign email (電子メールの署名)

送信メッセージにデジタル署名を追加するかどうかを指定します。

このオプションを有効にする場合は、キーストアと署名キーの設定も指定する必要があります。

キーストアパス

[Sign email (電子メールの署名)] を有効にした場合にのみ適用されます。

電子メールをデジタルで署名するために使用するキーストア (cacerts) ファイルへのフルパスを指定します。手動でパスを入力するか、または cacerts ファイルを参照して指定できます。

たとえば、C:\NetIQ\idm\apps\jre\lib\security\cacerts です。

キーストアパスワード

[Sign email (電子メールの署名)] を有効にした場合にのみ適用されます。

キーストアファイルのパスワードを指定します。たとえば、changeit です。

Alias of signature key (署名キーのエイリアス)

[Sign email (電子メールの署名)] を有効にした場合にのみ適用されます。

キーストアの署名キーの別名を指定します。たとえば、idmapptest です。

Signature key password (署名キーのパスワード)

[Sign email (電子メールの署名)] を有効にした場合にのみ適用されます。

署名キーを含むファイルを保護するパスワードを指定します。たとえば、changeit です。

トラステッドキーストア

このセクションでは、識別情報アプリケーションのトラステッドキーストアの値を定義します。このセクションの設定は、[詳細オプションの表示] を選択した場合のみ表示されます。

トラステッドストアパス

信頼される署名者のすべての証明書が含まれるトラステッドキーストアへのパスを指定します。入力しない場合は、識別情報アプリケーションはシステムプロパティ javax.net.ssl.trustStore からパスを取得します。このシステムプロパティからパスを取得できない場合、インストールプログラムはデフォルトで jre\lib\security\cacerts に設定します。

トラステッドストアパスワード

トラステッドキーストアのパスワードを指定します。入力しない場合は、識別情報アプリケーションはシステムプロパティ javax.net.ssl.trustStorePassword からパスワードを取得します。このシステムプロパティからパスを取得できない場合、インストールプログラムはデフォルトで changeit に設定します。

このパスワードは、マスタキーに基づいて暗号化されます。

トラステッドストアタイプ

トラステッドストアパスがデジタル署名に Java キーストア (JKS) または PKCS12 のどちらを使用するかを指定します。

NetIQ Sentinel デジタル署名証明書 & キー

このセクションでは、Identity Manager がイベント監査のために Sentinel と通信できるようにする値を定義します。このセクションの設定は、[詳細オプションの表示] を選択した場合のみ表示されます。

Sentinel デジタル署名証明書

Sentinel に送信される監査メッセージを OAuth サーバが認証するために使用するカスタム公開鍵証明書が表示されます。

Sentinel デジタル署名秘密鍵

Sentinel に送信される監査メッセージを OAuth サーバが認証するために使用するカスタム秘密鍵ファイルへのパスを指定します。

その他

このセクションの設定は、[詳細オプションの表示] を選択した場合のみ表示されます。

OCSP URI

クライアントインストールがオンライン証明書状態プロトコル (OCSP) を使用する際に使用する Uniform Resource Identifier(URI) を指定します。たとえば、「http://host:port/ocspLocal」と指定します。

OCSP URI によって、トラステッド証明書オンラインの状態は更新されます。

許可設定パス

許可環境設定ファイルの完全修飾名を指定します。

識別ボールトインデックス

インストール時にインストールプログラムで manager、ismanager、および srvprvUUID の各属性にインデックスを作成するかどうかを指定します。インストール後にそれらのインデックスの新しい場所を参照するように設定を変更できます。この設定には次の考慮事項が適用されます。

- これらの属性にインデックスがない場合、Identity Applications ユーザは、Identity Applications のパフォーマンスの低下を感じる可能性があります。
- 識別情報アプリケーションをインストールした後、iManager を使用して、手動でこれらのインデックスを作成できます。
- パフォーマンスを最大化するには、インストール時にインデックスを作成する必要があります。
- 識別情報アプリケーションをユーザが使用できるようにする前に、これらのインデックスをオンラインモードにする必要があります。
- インデックスを作成または削除するには、**[サーバDN]**にも値を指定する必要があります。

サーバ DN

識別ボールトインデックスを作成または削除する必要がある場合にのみ適用されます。

インデックスを作成または削除する eDirectory サーバを指定します。

指定できるサーバは一度に 1 つだけです。複数の eDirectory サーバでインデックスを設定するには、RBPM 設定ユーティリティを複数回実行する必要があります。

Reinitialize RBPM Security (RBPM セキュリティの再初期化)

インストールプロセスの終了時に RBPM セキュリティをリセットするかどうかを指定します。識別情報アプリケーションを再展開する必要もあります。

IDMReport URL

Identity Manager Reporting モジュールの URL を指定します。たとえば、「http://hostname:port/IDMRPT」と指定します。

カスタムテーマのコンテキスト名

ブラウザで Identity Applications を表示する際に使用するカスタマイズしたテーマの名前を指定します。

ログメッセージの識別子プレフィックス

idmuserapp_logging.xml ファイルの CONSOLE アペンダと FILE アペンダのレイアウトパターンで使用する値を指定します。デフォルト値は RBPM です。

RBPM コンテキスト名の変更

RBPM のコンテキスト名を変更するかどうかを指定します。

役割とリソースドライバの新しい名前と DN も指定する必要があります。

RBPM コンテキスト名

[RBPM コンテキスト名の変更] を選択している場合にのみ適用されます。

RBPM の新しいコンテキスト名を指定します。

役割ドライバの DN

[RBPM コンテキスト名の変更] を選択している場合にのみ適用されます。

役割とリソースドライバの DN を指定します。

コンテナオブジェクト

このセクションのパラメータはインストール時にのみ適用されます。

このセクションでは、コンテナオブジェクトの値を定義したり、新しいコンテナオブジェクトを作成したりできます。

Selected(選択済み)

使用するコンテナオブジェクトタイプを指定します。

コンテナオブジェクトタイプ

コンテナの地域、国、部門、組織、またはドメインを指定します。

iManager 内で自分のコンテナを定義でき、これを [新規コンテナオブジェクトの追加] の下に追加できます。

コンテナ属性名

指定したコンテナオブジェクトタイプに関連付けられている属性タイプの名前を指定します。

新規コンテナオブジェクトの追加 : コンテナオブジェクトタイプ

新しいコンテナとして使用可能な識別ボールトのオブジェクトクラスの LDAP 名を指定します。

新規コンテナオブジェクトの追加 : コンテナ属性名

新しいコンテナオブジェクトタイプに関連付けられている属性タイプの名前を指定します。

Reporting Parameters (Reporting パラメータ)

識別情報アプリケーションを設定する際、このタブでは、Identity Reporting を管理するための値を定義します。Identity Reporting をインストールすると、このタブが追加されます。

デフォルトでは、このタブには基本オプションが表示されます。すべての設定を表示するには、[詳細オプションの表示] をクリックします。このタブには、次の設定グループがあります。

- 91 ページの 「電子メール配信設定」
- 91 ページの 「レポート保持の値」
- 92 ページの 「ロケールの変更」

- 92 ページの 「役割の設定」
- 92 ページの 「送信プロキシ」

電子メール配信設定

このセクションでは、通知を送信するための値を定義します。

SMTP サーバホスト名

Identity Reporting が通知を送信する際に使用する電子メールサーバの DNS 名または IP アドレスを指定します。localhost は使用しないでください。

SMTP サーバポート

SMTP サーバのポート番号を指定します。

SMTP は SSL を使用

電子メールサーバとの通信に TLS/SSL プロトコルを使用するかどうかを指定します。

サーバは認証が必要

電子メールサーバとの通信に認証を使用するかどうかを指定します。

SMTP ユーザ名

認証に使用する電子メールアドレスを指定します。

値を指定する必要があります。サーバで認証が不要の場合は、無効なアドレスを指定できます。

SMTP ユーザパスワード

サーバは認証が必要と指定している場合にのみ適用されます。

SMTP ユーザアカウントのパスワードを指定します。

デフォルト電子メールアドレス

電子メールサーバとの通信に認証を使用するかどうかを指定します。

レポート保持の値

このセクションでは、完了したレポートを保持するための値を定義します。

レポートの単位 , レポート有効期間

Identity Reporting が完了したレポートを保持する期間を指定します。この期間が経過すると、完了したレポートは削除されます。たとえば、6 カ月を指定するには、[レポート有効期間] フィールドに「6」と入力し、[レポートの単位] フィールドで [月] を選択します。

レポートの場所

レポート定義を保存する場所のパスを指定します。たとえば、C:\NetIQ\idm\apps\IdentityReporting です。

ロケールの変更

このセクションでは、Identity Reporting の使用言語に関する値を定義します。Identity Reporting は特定のロケールを使用して検索します。詳細については、『Administrator Guide to NetIQ Identity Reporting』を参照してください。

役割の設定

このセクションでは、Identity Reporting がレポートを生成する際に使用する認証ソースに関する値を定義します。

認証ソースの追加

レポーティングのために追加する認証ソースのタイプを指定します。次の認証ソースを指定できます。

- **デフォルト**
- **LDAP ディレクトリ**
- **File (ファイル)**

送信プロキシ

「Identity Manager 4.8.1 以降のバージョンを使用する場合にのみ適用されます。」

このセクションでは、Identity Reporting がレポートのダウンロードに使用するリバースプロキシサーバを使用するための値を定義します。

Use Proxy

レポーティングでリバースプロキシサーバを使用するオプションを指定します。

- **ホスト名または IP アドレス**
- **ポート**
- **Use TLS (TLS の使用)**

  ネットワークプロトコルとして TCP を使用する場合にのみ適用されます。

認証パラメータ

アイデンティティアプリケーションを設定する際、このタブでは、Tomcat がユーザをアイデンティティアプリケーションおよびパスワード管理のページに転送するために使用する値を定義します。

デフォルトでは、このタブには基本オプションが表示されます。すべての設定を表示するには、**[詳細オプションの表示]** をクリックします。このタブには、次の設定グループがあります。

- 93 ページの 「[Authentication Server(認証サーバ)]」
- 93 ページの 「認証の設定」
- 94 ページの 「認証方式」

- 95 ページの 「パスワード管理」
- 96 ページの 「Sentinel デジタル署名証明書とキー」

[Authentication Server(認証サーバ)]

このセクションでは、識別情報アプリケーションが認証サーバに接続するための設定を定義します。

OAuth サーバのホスト識別子

必須

トークンを OSP に発行する認証サーバの相対 URL を指定します。たとえば、「192.168.0.1」と指定します。

OAuth サーバの TCP ポート

認証サーバのポートを指定します。

Access Manager is the OAuth provider (Access Manager は OAuth プロバイダです)

OAuth の OSP から NAM への変換は、設定更新ユーティリティの認証タブからはサポートされていません。このオプションを非表示にするには、configupdate.sh.properties ファイルで、no_nam_oauth の値を “true” に設定します。

OAuth サーバは TLS/SSL を使用しています

認証サーバが通信に TLS/SSL を使用するかどうかを指定します。

オプションの TLS/SSL トラストストアファイル

[OAuth サーバは TLS/SSL を使用しています] *を選択し、詳細オプションを表示している場合にのみ適用されます。*

オプションの TLS/SSL トラストストアパスワード

[OAuth サーバは TLS/SSL を使用しています] *を選択し、詳細オプションを表示している場合にのみ適用されます。*

TLS/SSL 認証サーバのキーストアファイルをロードする際に使用するパスワードを指定します。

注 : キーストアパスおよびパスワードを指定せず、認証サーバの信頼証明書が JRE トラストストア (cacerts) に存在しない場合、Identity Applications は TLS/SSL プロトコルを使用する認証サービスに接続できません。

認証の設定

このセクションでは、認証サーバの設定を定義します。

管理コンテナの LDAP DN

必須

OSP が認証する必要がある管理者ユーザオブジェクトが含まれる識別ボールト内のコンテナの識別名を指定します。たとえば、「ou=sa,o=data」と指定します。

重複解決名前付け属性

同じ cn 値を持つ複数の eDirectory ユーザオブジェクトを区別するために使用する LDAP 属性の名前を指定します。デフォルト値は mail です。

コンテキストへの認証ソースの制限

識別ボールト内のユーザコンテナおよび管理者コンテナにおける検索を、そのコンテナ内のユーザオブジェクトのみに限定するのか、それともサブコンテナも検索対象にするのかを指定します。

セッションタイムアウト (分)

ユーザが何も操作せずに一定時間が経過するとサーバはそのユーザセッションをタイムアウトさせますが、その時間を分単位で指定します。デフォルト値は 20 分です。

アクセストークンのライフタイム (秒)

OSP アクセストークンの有効期間の秒数を指定します。デフォルト値は 60 秒です。

リフレッシュトークンのライフタイム (時間)

OSP リフレッシュトークンの有効期間の秒数を指定します。リフレッシュトークンは OSP が内部的に使用します。既定値は 48 時間です。

認証方式

このセクションでは、Identity Manager のブラウザベースのコンポーネントにログインするユーザを OSP が認証できるようにする値を定義します。

メソッド

ユーザがログオンする際に Identity Manager が使用する認証タイプを指定します。

- ［**名前とパスワード**］: OSP は識別ボールトを使用して認証を検証します。
- ［**Kerberos**］: OSP は Kerberos チケットサーバと識別ボールトの両方から認証を受け入れます。**[マッピング属性名]** の値も指定する必要があります。
- ［**SAML 2.0**］: OSP は SAML アイデンティティプロバイダとアイデンティティボールトの両方から認証を受け入れます。**[マッピング属性名]** と **[メタデータ URL]** の値も指定する必要があります。

マッピング属性名

[Kerberos] *または* **[SAML]** *を指定している場合にのみ適用されます。*

Kerberos チケットサーバまたは識別情報プロバイダの SAML 表現にマッピングする属性の名前を指定します。

メタデータ URL

[SAML] *を指定している場合にのみ適用されます。*

OSP が認証要求を SAML にリダイレクトする際に使用する URL を指定します。

パスワード管理

このセクションでは、ユーザがパスワードの変更をセルフサービス操作として実行できるようにする値を定義します。

パスワード管理プロバイダ

使用するパスワード管理システムのタイプを指定します。

［**ユーザアプリケーション (レガシ)**］ : Identity Manager が従来使用していたパスワード管理プログラムを使用します。このオプションを使用すると、外部パスワード管理プログラムを使用することもできます。

［**Self Service Password Reset (SSPR)**］ : ユーザが管理者の助けを借りずに自分でパスワードをリセットできる Identity Applications に含まれている NetIQ Self Service Password Reset サービスを使用します。Identity Applications ダッシュボードログインページに表示されるリンクを選択して、ユーザが要件に基づいてログインアクセスをリセットするための適切なアクションを選択できるようにします。詳細については、96 ページの「ユーザインタフェース」を参照してください。

SSPR は、**[パスワード管理プロバイダ]** フィールドのデフォルトの選択です。

パスワードを忘れた場合

*このメニューリストは、**[ユーザアプリケーション (レガシ)]** を選択している場合にのみ適用されます。*

ユーザアプリケーションまたは外部システムのどちらに統合されているパスワード管理システムを使用するかを指定します。

- ［**内部**］ : デフォルトの内部パスワード管理機能を使用します。/jsps/pwdmgt/ForgotPassword.jsp(最初は http(s) プロトコルなし)。これは、ユーザを、外部 WAR ではなく、ユーザアプリケーションに組み込まれた［パスワードを忘れた場合］機能にリダイレクトします。
- ［外部］ : パスワードを忘れた場合の外部 WAR を使用して、Web サービス経由でユーザアプリケーションを呼び戻します。外部システムの設定も指定する必要があります。

［パスワードを忘れた場合］リンク

外部パスワード管理システムを使用する場合にのみ適用されます。

パスワードを忘れた場合の機能ページを参照する URL を指定します。外部または内部のパスワード管理 WAR にある ForgotPassword.jsp ファイルを指定します。

パスワードを忘れた場合の返信リンク

外部パスワード管理システムを使用する場合にのみ適用されます。

ユーザがパスワードを忘れた場合の操作を実行した後でクリックできるように、**[パスワードを忘れた場合の返信リンク]** の URL を指定します。

パスワードを忘れた場合の Web サービス URL

外部パスワード管理システムを使用する場合にのみ適用されます。

パスワードを忘れた場合の外部 WAR がユーザアプリケーションを呼び戻してパスワードを忘れた場合のコア機能を実行するために使用する URL を指定します。次の形式を使用してください。

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

ユーザインタフェース

このメニューリストは、**[Self Service Password Reset (SSPR)]** を選択した場合にのみ適用されます。

Identity Applications ダッシュボードのログインページに表示するリンクを指定します。デフォルトの選択の **[Can't sign in? (サインインできませんか ?)]** には、ユーザ名またはパスワードをリセットしたり、ログインページでアクセス許可を登録したりするための共通リンクが表示されます。**[なし]** を選択すると、ユーザは自分でパスワードをリセットすることはできません。

「**[Other links (その他のリンク)]**」を選択する場合は、選択に次のオプションが利用できます。

- ［パスワードを忘れた場合］ : 既存のユーザがパスワードを忘れた場合に、パスワードをリセットするためにクリックできるリンクを提供します。
- ［Forgot Username (ユーザ名を忘れた場合)］ : 既存のユーザがユーザ名とパスワードを忘れた場合に、これらをリセットするためにクリックできるリンクを提供します。
- ［Activate account (アカウントの有効化)］ : Identity Applications にアクセスするための新しいユーザアカウントを作成するためにユーザがクリックできるリンクを提供します。

Sentinel デジタル署名証明書とキー

このセクションでは、Identity Manager がイベント監査のために Sentinel と通信できるようにする値を定義します。

Sentinel デジタル署名証明書

監査システムに送信される監査メッセージを OSP サーバが認証するために使用するカスタム公開鍵証明書を指定します。

Novell Audit で使用するために証明書を設定する方法の詳細については、『*Novell Audit Administration Guide*』の「Managing Certificates」を参照してください。

Sentinel デジタル署名秘密鍵

監査システムに送信される監査メッセージを OSP サーバが認証するために使用するカスタム秘密鍵ファイルへのパスを指定します。

SSO Clients Parameters (SSO クライアントパラメータ)

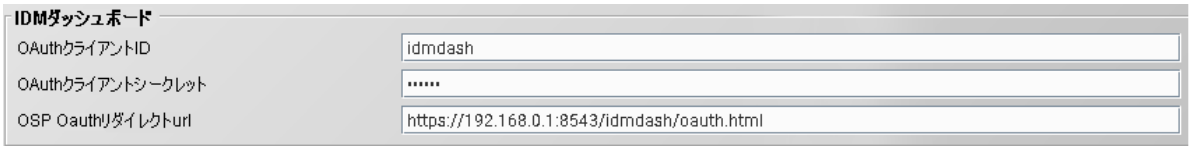
識別情報アプリケーションを設定する際、このタブでは、識別情報アプリケーションへのシングルサインオンアクセスを管理する値を定義します。

デフォルトでは、このタブには基本オプションが表示されます。すべての設定を表示するには、[**詳細オプションの表示**] をクリックします。このタブには、次の設定グループがあります。

- 97 ページの 「IDM ダッシュボード」
- 98 ページの 「IDM 管理者」
- 98 ページの 「RBPM」
- 99 ページの 「レポーティング」
- 100 ページの 「IDM データ収集サービス」
- 100 ページの 「DCS Driver (DCS ドライバ)」
- 101 ページの 「セルフサービスパスワードリセット」

IDM ダッシュボード

このセクションでは、ユーザが識別情報アプリケーションのプライマリログインの場所である、Identity Manager ダッシュボードにアクセスするために使用する必要がある URL の値を定義します。



OAuth クライアント ID

必須

ダッシュボードのシングルサインオンクライアントを認証サーバに認識させるために使用する名前を指定します。デフォルト値は idmdash です。

OAuth クライアントシークレット

必須

ダッシュボードのシングルサインオンクライアントのパスワードを指定します。

OSP OAuth リダイレクト URL

必須

認証完了時に認証サーバがブラウザクライアントをリダイレクトする絶対 URL を指定します。

使用するフォーマットは、protocol://server:port/path です。たとえば、https://192.168.0.1:8543/idmdash/oauth.html です。

IDM 管理者

このセクションでは、ユーザが［Identity Manager 管理者］ページにアクセスするために必要な URL の値を定義します。

OAuth クライアント ID

必須

Identity Manager 管理者のシングルサインオンクライアントを認証サーバに認識させるために使用する名前を指定します。デフォルト値は idmadmin です。

OAuth クライアントシークレット

必須

［Identity Manager 管理者］のシングルサインオンクライアントのパスワードを指定します。

OSP OAuth リダイレクト URL

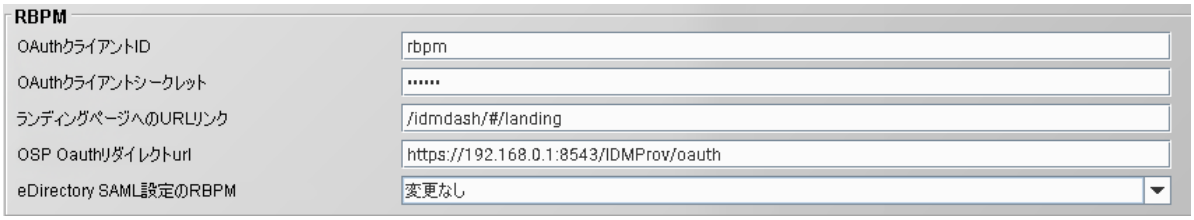
必須

認証完了時に認証サーバがブラウザクライアントをリダイレクトする絶対 URL を指定します。

使用するフォーマットは、protocol://server:port/path です。たとえば、https://192.168.0.1:8543/idmadmin/oauth.html です。

RBPM

このセクションでは、ユーザがユーザアプリケーションにアクセスするために必要な URL の値を定義します。



OAuth クライアント ID

必須

ユーザアプリケーションのシングルサインオンクライアントを認証サーバに認識させるために使用する名前を指定します。デフォルト値は rbpm です。

OAuth クライアントシークレット

必須

ユーザアプリケーションのシングルサインオンクライアントのパスワードを指定します。

ランディングページへの URL リンク

必須

ユーザアプリケーションから［ダッシュボード］にアクセスするために使用する相対 URL を指定します。デフォルト値は /landing です。

OSP OAuth リダイレクト URL

必須

認証完了時に認証サーバがブラウザクライアントをリダイレクトする絶対 URL を指定します。

使用するフォーマットは、protocol://server:port/path です。たとえば、https://192.168.0.1:8543/IDMProv/oauth です。

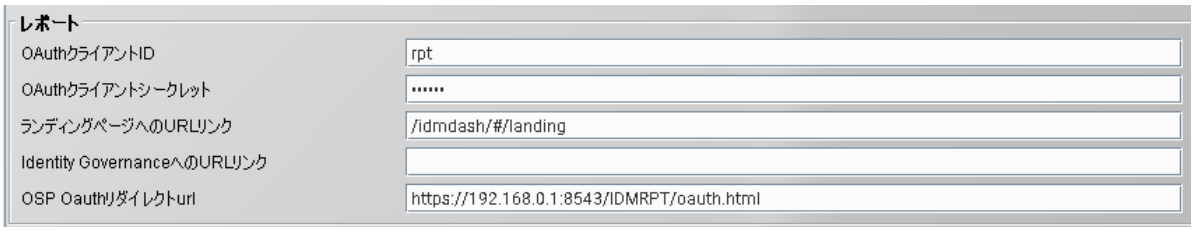
RBPM から eDirectory SAML への設定

必須

SSO 認証に必要な、RBPM から eDirectory SAML への設定を指定します。

レポーティング

このセクションでは、ユーザが Identity Reporting にアクセスするために必要な URL の値を定義します。このセクションの値は、Identity Manager ソリューションに Identity Reporting を追加している場合にのみ表示されます。



OAuth クライアント ID

必須

Identity Reporting のシングルサインオンクライアントを認証サーバに認識させるために使用する名前を指定します。デフォルト値は rpt です。

OAuth クライアントシークレット

必須

Identity Reporting のシングルサインオンクライアントのパスワードを指定します。

ランディングページへの URL リンク

必須

Identity Reporting から［ダッシュボード］にアクセスするために使用する相対 URL を指定します。デフォルト値は /idmdash/#/landing です。

Identity Reporting と識別情報アプリケーションを異なるサーバにインストールしている場合は、絶対 URL を指定します。使用するフォーマットは、protocol://server:port/path です。たとえば、https://192.168.0.1:8543/IDMRPT/oauth です。

OSP OAuth リダイレクト URL

必須

認証完了時に認証サーバがブラウザクライアントをリダイレクトする絶対 URL を指定します。

使用するフォーマットは、protocol://server:port/path です。たとえば、https://192.168.0.1:8543/IDMRPT/oauth です。

IDM データ収集サービス

このセクションでは、ユーザが Identity Manager データ収集サービスにアクセスするために必要な URL の値を定義します。

OAuth クライアント ID

必須

Identity Manager データ収集サービスのシングルサインオンクライアントを認証サーバに認識させるために使用する名前を指定します。デフォルト値は idmdcs です。

OAuth クライアントシークレット

必須

Identity Manager データ収集サービスのシングルサインオンクライアントのパスワードを指定します。

OSP OAuth リダイレクト URL

必須

認証完了時に認証サーバがブラウザクライアントをリダイレクトする絶対 URL を指定します。

使用するフォーマットは、protocol://server:port/path です。たとえば、https://192.168.0.1:8543/idmdcs/oauth.html です。

DCS Driver (DCS ドライバ)

このセクションでは、データ収集サービスドライバを管理するための値を定義します。

図 4-1

OAuth クライアント ID

データ収集サービスドライバのシングルサインオンクライアントを認証サーバに認識させるために使用する名前を指定します。このパラメータのデフォルト値は dcsdrv です。

OAuth クライアントシークレット

データ収集サービスドライバのシングルサインオンクライアントのパスワードを指定します。

セルフサービスパスワードリセット

このセクションでは、ユーザが SSPR にアクセスするために必要な URL の値を定義します。

OAuth クライアント ID

必須

SSPR のシングルサインオンクライアントを認証サーバに認識させるために使用する名前を指定します。デフォルト値は sspr です。

OAuth クライアントシークレット

必須

SSPR のシングルサインオンクライアントのパスワードを指定します。

OAuth redirect URL (OAuth リダイレクト URL)

必須

認証完了時に認証サーバがブラウザクライアントをリダイレクトする絶対 URL を指定します。

使用するフォーマットは、protocol://server:port/path です。たとえば、https://192.168.0.1:8543/sspr/public/oauth.html です。

CEF 監査パラメータ

このセクションでは、CEF 監査パラメータを管理するための値を定義します。

Send audit events (監査イベントの送信)

CEF を Identity Applications の監査イベントに使用するかどうかを指定します。

[接続先のホスト]

監査サーバの DNS 名または IP アドレスを指定します。

送信先ポート

監査サーバのポートを指定します。

Network Protocol (ネットワークプロトコル)

CEF イベントを受信するために監査サーバによって使用されるネットワークプロトコルを指定します。

Use TLS (TLS の使用)

ネットワークプロトコルとして TCP を使用する場合にのみ適用されます。

監査サーバが TCP と TLS を併用するように設定されているかどうかを指定します。

Intermediate event store directory (中間イベントストアディレクトリ)

CEF イベントが監査サーバに送信される前のキャッシュディレクトリの場所を指定します。

注 : novlua 許可が中間イベントストアディレクトリに設定されていることを確認します。設定されていない場合、IDMDash および IDMProv アプリケーションにアクセスできません。また、OSP イベントのどれも中間イベントストアディレクトリに記録されません。たとえば、chown novlua:novlua <directorypath> コマンドを使用して、ディレクトリの許可と所有権を変更できます。ここで、<directorypath> は中間イベントストアディレクトリです。

識別情報アプリケーション用の REST API の展開

識別情報アプリケーションコンポーネントには、識別情報アプリケーション内のさまざまな機能を有効にする複数の REST API が組み込まれています。REST サービスは、OAUTH2 プロトコルを使用して認証を提供します。ブラウザまたはスクリプトで curl コマンドを使用してこれらの API を呼び出して、管理タスクを自動化することができます。REST API および対応するドキュメントは、idmappsdoc.war ファイルで入手できます。war は、Identity Applications がインストールされるときに自動的に展開されます。詳細については、REST API のマニュアルを参照してください。

Identity Applications がインストールされているサーバで REST API ドキュメントにアクセスするには、ブラウザのアドレスバーで https://<identity applications servername>:<Port>/idmappsdoc を指定します。たとえば、https://192.168.0.1:8543/idmappsdoc です。

Oracle サービス名を使用した Oracle データベースへのアクセス

Oracle System ID (SID) または Oracle サービス名を使用して、Oracle データベースに接続することができます。Identity Applications インストーラは SID のみを受け入れます。サービス名を使用してデータベースにアクセスする場合は、SID を介して接続して、1 つのデータベースインスタンスへの Identity Applications インストールを完了します。インストールが完了したら、以下のアクションを実行します。

1 次のコマンドを実行して、Oracle データベースにサービス名を作成します。

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

ここで、SERVICE 1 は Oracle サービスの名前です。

注 : サービス名は大文字でも小文字でも指定できます。大文字と小文字は区別されません。

2 Tomcat の server.xml ファイルで、ファイル内の Oracle データソースの詳細を変更して、サービス名を定義します。

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

3 Tomcat を再起動します。

4 サービス名が catalina.out ログファイルに含まれていることを確認します。

5 Identity Applications がデータベースに適切に接続されていることを確認します。

手動によるデータベーススキーマの作成

識別情報アプリケーションをインストールする際、データベースへの接続またはデータベーステーブルの作成を後回しにできます。データベースに対する許可を持たないユーザは、このオプションを選択する必要がある場合があります。インストールプログラムは、ユーザがデータベーススキーマを作成するために使用できる SQL ファイルを作成します。インストール後に、再インストールを行わずに、データベーステーブルを再作成することもできます。それには、識別情報アプリケーションのデータベースを削除して、それと同じ名前で新しいデータベースを作成します。

SQL ファイルによるデータベーススキーマの生成

このセクションでは、ユーザがデータベーススキーマを生成するために使用できる SQL ファイルをインストールプログラムが作成していると想定しています。この SQL ファイルが存在しない場合は、104 ページの 「データベーススキーマを生成する SQL ファイルの手動による作成」を参照してください。

注 : この SQL ファイルを SQL*Plus で実行しないでください。このファイルの行長は 4000 文字を超えています。

---

1. アプリケーションサーバを停止します。
2. データベースサーバにログインします。
3. 識別情報アプリケーションが使用するデータベースを削除します。
4. ステップ 3 で削除したデータベースと同じ名前で新しいデータベースを作成します。
5. インストールプロセスで作成された SQL スクリプトのある場所に移動します。デフォルトでは、*/installation_path*/userapp/sql ディレクトリにあります。
6. (状況によって実行) Oracle データベースの場合、関数 CONCAT_BLOB の定義の後にバックスラッシュ (/) を挿入します。次に例を示します。

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

7. データベース管理者に、ユーザアプリケーションデータベースを作成および設定する SQL スクリプトを実行させます。
8. Tomcat を再起動します。

データベーススキーマを生成する SQL ファイルの手動による作成

インストール後に、SQL ファイルがなくても、再インストールを行わずに、データベーステーブルを再作成できます。このセクションでは、SQL ファイルを持たない場合にデータベーススキーマを作成する方法について説明します。

1. Tomcat を停止します。
2. 識別情報アプリケーションデータベースをホストするサーバにログインします。
3. 既存のデータベースを削除します。
4. ステップ 3 で削除したデータベースと同じ名前で新しいデータベースを作成します。
5. テキストエディタで NetIQ-Custom-Install.log ファイルを開きます。このファイルは、デフォルトでは、識別情報アプリケーションのインストールディレクトリのルートにあります。次に例を示します。

   C:\NetIQ\idm\apps\UserApplication
6. NetIQ-Custom-Install.log ファイルで次のコマンドを検索し、コピーします。

   C:\NetIQ\idm\jre\bin\java -Xms256m -Xmx256m -Dwar.context.name=IDMProv -Ddriver.dn="cn=User Application Driver,cn=driverset1,o=system" - Duser.container="o=data" -jar C:\NetIQ\idm\jre\liquibase.jar -- databaseClass=liquibase.database.core.PostgresDatabase -- driver=org.postgresql.Driver -- classpath=C:\NetIQ\idm\apps\postgresql\postgresql-9.4.1212jdbc42.jar C:\NetIQ\idm\apps\UserApplication\IDMProv.war -- changeLogFile=DatabaseChangeLog.xml -- url="jdbc:postgresql://localhost:5432/ idmuserappdb" --contexts="prov,newdb" --logLevel=info -- logFile=C:\NetIQ\idm\apps\UserApplication\db.out --username=******** -- password******** update
7. 識別情報アプリケーションで使用するデータベースをインストールしたサーバにログインします。
8. 端末でコピーしたコマンド文字列を貼り付けます。

   注 : 正しいコマンドは updateSQL です。update だった場合は updateSQL に変更してください。

   ---
9. コマンドでデータベースユーザ名とパスワードを表すアスタリスク (*) を、認証に必要な実際の値で置き換えます。また、SQL ファイルの名前が一意であることを確認します。
10. コマンドを実行します。
11. (状況によって実行) インストールプロセスでデータベースにデータを設定せずに SQL ファイルを生成した場合、データベース管理者にそのファイルを渡してデータベースサーバにインポートします。詳細については、103 ページの 「SQL ファイルによるデータベーススキーマの生成」を参照してください。
12. データベース管理者が SQL ファイルをインポートした後、Tomcat を起動します。

識別情報アプリケーションのシングルサインオン設定の管理

インストールプロセスにより、Identity Manager のシングルサインオンアクセス用の認証サービス (OSP) がインストールされます。ただし、OSP 認証サーバを設定して、Kerberos チケットサーバまたは SAML から認証を受け入れることもできます。インストール後に識別情報アプリケーションのシングルサインオン設定を行うには、『*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*』の「Configuring Single Sign-on Access in Identity Manager」を参照してください。

識別情報アプリケーションの起動

Identity Applications を設定した後は、Tomcat サービスと ActiveMQ サービスを再開してください。

systemctl restart netiq-tomcat

systemctl restart netiq-activemq

識別情報アプリケーションの設定と使用方法の検討事項

識別情報アプリケーションを設定および初めて使用する際、次の検討事項が適用されます。

- インストールプロセス中、インストールプログラムによりログファイルがインストールディレクトリに書き込まれます。これらのファイルには、設定に関する情報が含まれています。現在の識別情報アプリケーション環境を設定した後で、これらのログファイルを削除するか、安全な場所に保存することを検討する必要があります。インストールプロセス中、データベーススキーマをファイルに書き込むことも選択できます。このファイルにはデータベースについての説明的な情報が含まれているので、インストールプロセスが完了した後で、安全な場所に移動する必要があります。
- (状況によって実行) アイデンティティアプリケーションを監査するには、現在の環境に Identity Reporting と監査サービスがインストールされ、イベントをキャプチャするように設定されている必要があります。また、識別情報アプリケーションを監査用に設定する必要があります。
- ユーザが識別情報アプリケーションにアクセスできるようにするには、次のアクティビティを完了する必要があります。
  - 必要なすべての Identity Manager ドライバがインストールされていることを確認します。
  - すべてのブラウザで cookie を有効にします。cookie が無効な場合、アプリケーションは機能しません。
- 異なるサーバ上に Identity Applications および SSPR がインストールされている場合は、Identity Applications サーバの cacerts に Identity Applications として CN による SSPR トラステッド証明書をインポートする必要があります。

データ収集用のランタイム環境の設定

このセクションでは、ランタイム環境が正常に動作していることを確認するために実行する必要がある追加の設定手順について説明します。さらに、トラブルシューティングの手法に加え、注意を要するデータベーステーブルに関する情報についても説明します。

このプロセスには次の作業が含まれます。

- 106 ページの 「識別情報アプリケーションからのデータ収集に関するデータ収集サービスドライバの設定」
- 107 ページの 「データ収集サービスドライバの移行」
- 109 ページの 「カスタム属性とカスタムオブジェクトのサポートの追加」
- 112 ページの 「複数のドライバセットのサポートの追加」
- 114 ページの 「SSL を使用したリモートモードでのドライバ実行設定」

理解が困難な問題が 1 つ以上のドライバで発生する場合は、『*NetIQ Identity Reporting Module Guide*』の「Troubleshooting the Drivers」を参照してください。

識別情報アプリケーションからのデータ収集に関するデータ収集サービスドライバの設定

識別情報アプリケーションを Identity Reporting と適切に連携させるには、OAuth プロトコルをサポートするように DCS ドライバを設定する必要があります。

注

- 現在の環境で Identity Reporting を使用している場合は、DCS ドライバをインストールして設定するだけで済みます。
- 現在の環境で DCS ドライバが複数設定されている場合は、各ドライバに対して次の手順を実行する必要があります。

---

1. Designer にログインします。
2. Designer でプロジェクトを開きます。
3. (状況によって実行) DCS ドライバをサポートされているパッチバージョンにまだアップグレードしていない場合は、次の手順を実行します。
   - **3a** 最新の DCS ドライバパッチファイルをダウンロードします。
   - **3b** パッチファイルをサーバ上の場所に展開します。
   - **3c** ターミナルで、ご使用の環境用のパッチ RPM を展開した場所へ移動し、次のコマンドを実行します。

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

   - **3d** アイデンティティボールトを再起動します。

3e Designer で、サポートされているバージョンのデータ収集サービスベースパッケージがインストールされていることを確認します。必要に応じて、続行する前に最新バージョンをインストールします。

3f Designer で DCS ドライバを再展開して再起動します。

4 ［**アウトライン**］ビューで、DCS ドライバを右クリックし、[プロパティ] を選択します。

5 [ドライバ環境設定] をクリックします。

6 [ドライバパラメータ] タブをクリックします。

7 [Show connection parameters (接続パラメータの表示)] をクリックし、[show (表示)] を選択します。

8 [SSO Service Support (SSO サービスのサポート)] をクリックし、[はい] を選択します。

9 Identity Reporting の IP アドレスとポートを指定します。

10 SSO サービスクライアントのパスワードを指定します。デフォルトのパスワードは driver です。

11 [適用] をクリックし、[OK] をクリックします。

12 [アウトライン] ビューで、DCS ドライバを右クリックし、[プロパティ ］ > ［展開] の順に選択します。

13 [展開] をクリックします。

14 DCS ドライバの再起動を求めるプロンプトが表示される場合は、[はい] をクリックします。

15 [OK] をクリックします。

データ収集サービスドライバの移行

オブジェクトを識別情報ウェアハウスに同期するには、データ収集サービスドライバを移行する必要があります。

1 iManager にログインします。

2 データ収集サービスドライバの [概要] パネルで、[Migrate From Identity Vault (識別ボールトからの移行)] を選択します。

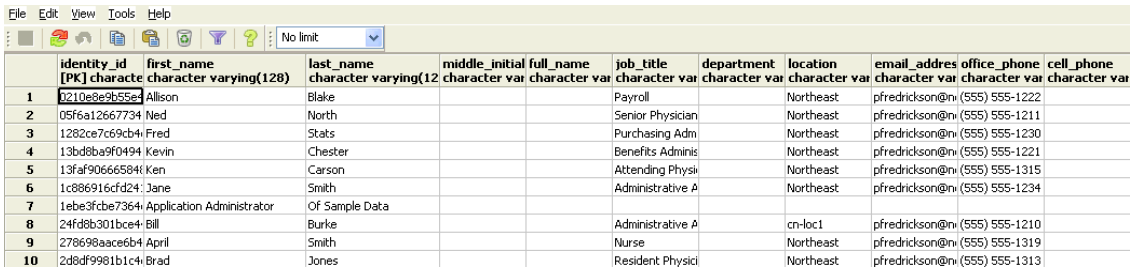
3 関連データが含まれる組織を選択して、[開始] をクリックします。

注 : 保存されているデータの量によっては、マイグレーションプロセスに数分かかる場合があります。次に進む前にマイグレーションプロセスが完了するまで待ってください。

---

4 マイグレーションプロセスが終わるまでしばらく待ちます。

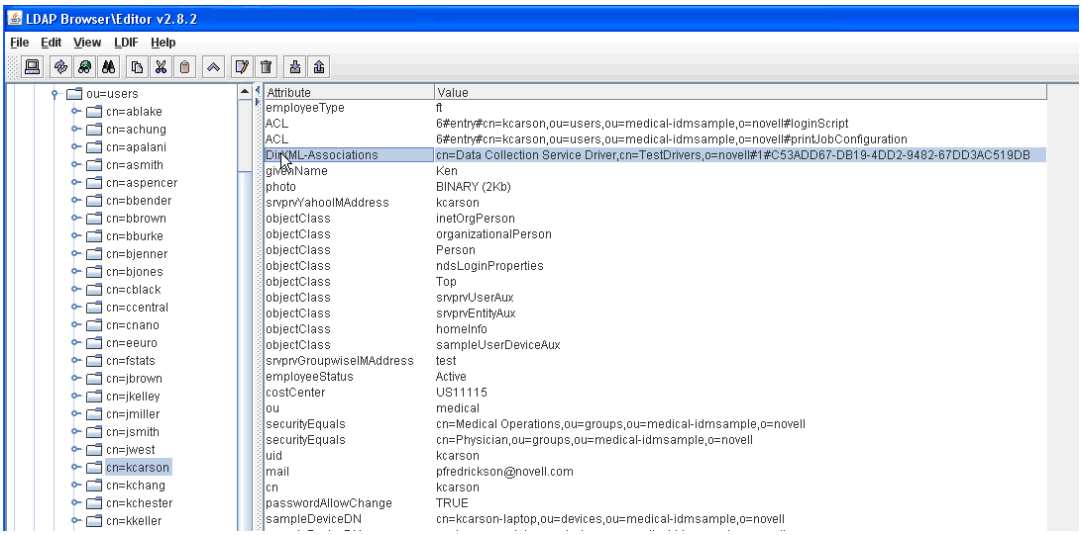
5 識別ボールト内にある識別情報とアカウントの情報を提供する [idmrpt_identity] テーブルおよび [idmrpt_acct] テーブルに、次のタイプの情報が含まれていることを確認します。



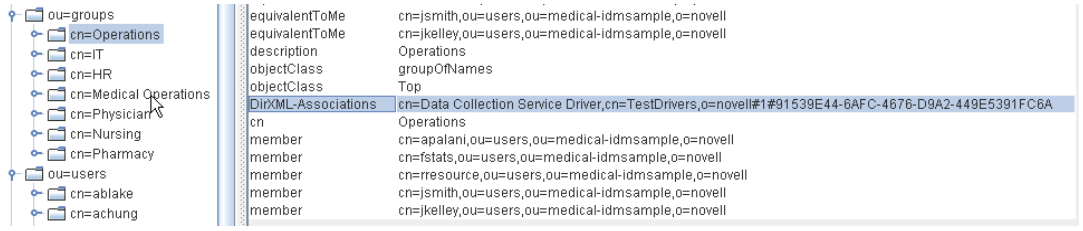
	identity_id [PK] characte	first_name character varying(128)	last_name character varying(12	middle_initial character var	full_name character var	job_title character var	department character var	location character var	email_addres character var	office_phone character var	cell_phone character var
1	0210e8e9b55e4	Allison	Blake			Payroll		Northeast	pfredrickson@n	(555) 555-1222	
2	05f6a12667734	Ned	North			Senior Physician		Northeast	pfredrickson@n	(555) 555-1211	
3	1282ce7c69cb4	Fred	Stats			Purchasing Adm		Northeast	pfredrickson@n	(555) 555-1230	
4	13bd8ba9f0494	Kevin	Chester			Benefits Adminis		Northeast	pfredrickson@n	(555) 555-1221	
5	13faf90666584	Ken	Carson			Attending Physi		Northeast	pfredrickson@n	(555) 555-1315	
6	1c886916cfd24	Jane	Smith			Administrative A		Northeast	pfredrickson@n	(555) 555-1234	
7	1ebe3fcbe7364	Application Administrator	Of Sample Data								
8	24fd8b301bce4	Bill	Burke			Administrative A		cn-loc1	pfredrickson@n	(555) 555-1210	
9	278698aace6b4	April	Smith			Nurse		Northeast	pfredrickson@n	(555) 555-1319	
10	2d8df9981b1c4	Brad	Jones			Resident Physici		Northeast	pfredrickson@n	(555) 555-1313	

6 LDAP ブラウザで、マイグレーションプロセスによって［DirXML-Associations (DirXML 関連付け)］に次の参照が追加されていることを確認します。

- 各ユーザについて次のタイプの情報を確認します。



- 各グループについて次のタイプの情報を確認します。



7 [idmrpt_group] テーブルのデータが次の情報のように表示されることを確認します。

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

このテーブルには、各グループの名前のほかに、そのグループが動的であるか、それともネストされているかを示すフラグが表示されます。さらに、グループが移行済みかどうかも表示されます。オブジェクトがユーザアプリケーションで変更されているものの、まだ移行されていない場合、同期ステータス (idmrpt_syn_state) が 0 に設定されている可能性があります。たとえば、ユーザをグループに追加し、ドライバがまだ移行されていない場合、この値が 0 に設定されている可能性があります。

8 (オプション) 次のテーブルのデータを確認します。

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

9 (オプション) 管理対象システムのゲートウェイドライバのデータ収集状態に関する情報が表示される [idmrpt_ms_collect_state] テーブルに新しい行が含まれていることを確認します。

このテーブルには、管理対象システムのどの REST エンドポイントが実行されたかに関するデータが記録されます。この時点では、まだこのドライバのデータ収集プロセスを開始していないため、テーブルに行はありません。

カスタム属性とカスタムオブジェクトのサポートの追加

デフォルトのデータ収集スキームに含まれないカスタム属性とカスタムオブジェクトのデータを収集して永続化するよう、データ収集サービスドライバを設定できます。このためには、データ収集サービスドライバフィルタを変更する必要があります。フィルタを変更しても、オブジェクトの同期はすぐにはトリガされません。その代わりに、新しく追加した属性とオブジェクトは、識別ボールトで追加、変更、または削除イベントが発生したときにデータ収集サービスに送信されます。

カスタム属性とカスタムオブジェクトのサポートを追加する場合、レポートを変更して拡張属性と拡張オブジェクトの情報を組み込む必要があります。拡張オブジェクトと拡張属性に関する最新データと履歴データは、次のビューで提供されます。

- idm_rpt_cfg.idmrpt_ext_idv_item_v
- idm_rpt_cfg.idmrpt_ext_item_attr_v

このプロセスには次の作業が含まれます。

- 110 ページの 「拡張オブジェクトを使用するためのドライバの設定」
- 110 ページの 「データベースへの名前と説明の組み込み」
- 111 ページの 「既知のオブジェクトタイプへの拡張属性の追加」

拡張オブジェクトを使用するためのドライバの設定

任意のオブジェクトまたは属性をデータ収集サービスフィルタポリシーに追加できます。新しいオブジェクトまたは属性を追加する場合、GUID (購読者同期を使用) およびオブジェクトクラス (購読者通知を使用) をマップする必要があります。次に例を示します。

```
<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>
```

データベースへの名前と説明の組み込み

データベースにオブジェクトの名前と設定を指定する場合、_dcsName および _dcsDescription に対するスキーママッピングポリシーを追加する必要があります。このスキーママッピングポリシーは、オブジェクトインスタンスの属性値をそれぞれ列 idmrpt_ext_idv_item.item_name および idmrpt_ext_idv_item.item_desc にマップします。スキーママッピングポリシーを追加しない場合、属性は子テーブル idmrpt_ext_item_attr で設定されます。

次に例を示します。

```
<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>
```

次の SQL の例では、データベース内にあるこれらのオブジェクトと属性の値を表示できます。

```
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
```

既知のオブジェクトタイプへの拡張属性の追加

属性をデータ収集サービスドライバのフィルタポリシーに追加し、XML 参照ファイル (IdmrptIdentity.xml) でレポーティングデータベースに明示的にマップしていない場合、値には idmrpt_ext_attr テーブルの属性参照が取り込まれ、idmrpt_ext_item_attr テーブルで管理されます。

次の SQL の例は、これらの拡張属性を示しています。

```
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'
```

ユーザオブジェクトのほかに、次のオブジェクトのフィルタポリシーにも拡張属性を追加し、データベースにそれらの属性を入力できます。

- nrfRole
- nrfResource
- コンテナ

注 : インストールした製品は organizationUnit、Organization、および Domain をサポートしています。コンテナタイプは idmrpt_container_types テーブルで管理されます。

- グループ
- nrfSod

拡張属性と親テーブルまたはオブジェクトの関連付けは、idmrpt_cat_item_types.idmrpt_table_name 列を参照することで確認できます。この列には、idm_rpt_data.idmrpt_ext_item_attr.cat_item_id 列を親テーブルのプライマリキーに結合する方法が記述されています。

複数のドライバセットのサポートの追加

Data Collection Service Scoping パッケージ (NOVLDCSSCPNG) は、複数のドライバセットと、データ収集サービスドライバおよび管理対象システムのゲートウェイドライバのペアを複数使用するエンタープライズ環境において、静的および動的なスコープ設定機能を実現します。

インストール中またはインストール後に、このパッケージをインストールするデータ収集サービスドライバの役割を決定する必要があります。次のいずれかの役割を選択する必要があります。

- **プライマリ** このドライバは、他のドライバセットのサブツリーを除くすべてを同期します。プライマリデータ収集サービスドライバは、識別ボールト全体にサービスを提供したり、1 つ以上のセカンダリドライバと連携して動作したりする可能性があります。
- **セカンダリ** このドライバは専用のドライバセットのみを同期し、それ以外は何も同期しません。通常、セカンダリデータ収集サービスドライバには、別のドライバセットで実行されているプライマリドライバが必要です。そうでない場合、ローカルドライバセットの外部にあるデータはデータ収集サービスに送信されません。
- **Custom** 管理者はカスタムスコープ設定ルールを定義できます。暗黙のスコープはローカルドライバセットのみで、それ以外は、カスタムスコープのリストに明示的に追加されていない限り、すべてスコープの範囲外とみなされます。カスタムスコープは、同期するサブオーディネートまたはサブツリーが含まれる識別ボールト内にあるコンテナのスラッシュ形式の識別名です。

このスコープ設定パッケージが必要になるのは、次に挙げるような特定の設定シナリオのみです。

- **1 つのサーバと、1 つのドライバセットの識別ボールト。:** このシナリオでは、スコープを設定する必要がないため、スコープ設定パッケージをインストールする必要はありません。
- **複数のサーバと、1 つのドライバセットの識別ボールト。:** このシナリオでは、次のガイドラインに従う必要があります。
  - Identity Manager サーバがデータ収集元の全パーティションのレプリカを保持する必要があります。
  - このシナリオでは、スコープ設定は必要ないため、スコープ設定パッケージはインストールしません。

- **複数のサーバと、複数のドライバセットの識別ボールト。**: このシナリオでは、次の 2 つの基本設定があります。
  - すべてのサーバがデータ収集元の全パーティションのレプリカを保持する設定。

    この設定では、次のガイドラインに従う必要があります。
    - 複数の DCS ドライバによって同じ変更が処理されるのを避けるため、スコープ設定が必要です。
    - すべてのDCSドライバにスコープ設定パッケージをインストールする必要があります。
    - 1 つの DCS ドライバをプライマリドライバとして選択する必要があります。
    - 他のDCSドライバはすべてセカンダリドライバになるように設定する必要があります。
  - すべてのサーバがデータ収集元の全パーティションのレプリカを「保持しない」設定。

    この設定では、次の 2 つの状況が考えられます。
    - データ収集元の全パーティションは「1 つの」 Identity Manager サーバによってのみ保持されます。

      この場合、次のガイドラインに従う必要があります。
      - 複数の DCS ドライバによって同じ変更が処理されるのを避けるため、スコープ設定が必要です。
      - すべてのDCSドライバにスコープ設定パッケージをインストールする必要があります。
      - すべてのDCSドライバをプライマリドライバになるように設定する必要があります。
    - データの収集元の全パーティションは「1 つの Identity Manager サーバのみによって保持されません」(一部のパーティションは複数の Identity Manager サーバで保持されます)。

      この場合、次のガイドラインに従う必要があります。
      - 複数の DCS ドライバによって同じ変更が処理されるのを避けるため、スコープ設定が必要です。
      - すべてのDCSドライバにスコープ設定パッケージをインストールする必要があります。
      - すべてのDCSドライバをプライマリドライバになるように設定する必要があります。

        各ドライバに対してカスタムスコープ設定ルールを定義し、作成したスコープが重複していないことを確認する必要があります。

SSL を使用したリモートモードでのドライバ実行設定

リモートモードで実行する場合、データ収集サービスドライバおよび管理対象のシステムゲートウェイドライバを、SSL を使用するように設定できます。このセクションでは、SSL を使用してリモートモードで実行されるようにドライバを設定する手順について説明します。

管理対象システムのゲートウェイドライバに対してキーストアを使用して SSL を設定する

1 iManager でサーバ証明書を作成します。

   1a [Roles and Tasks (役割とタスク)] ビューで、[NetIQ Certificate Server] > [Create Server Certificate (サーバ証明書の作成)] の順にクリックします。

   1b 管理対象システムのゲートウェイドライバがインストールされているサーバオブジェクトを参照して選択します。

   1c 証明書のニックネームを指定します。

   1d 作成方法として [Standard (標準)] を選択し、[次へ] をクリックします。

   1e [終了] をクリックし、[閉じる] をクリックします。

2 iManager を使用してサーバ証明書をエクスポートします。

   2a [Roles and Tasks (役割とタスク)] ビューで、[NetIQ Certificate Access (NetIQ 証明書アクセス)] > [Server Certificates (サーバ証明書)] の順にクリックします。

   2b ステップ 1 で作成した証明書を選択して、[エクスポート] をクリックします。

   2c [証明書] メニューで、証明書の名前を選択します。

   2d [Export private key (秘密鍵のエクスポート)] がオンになっていることを確認します。

   2e パスワードを入力し、[次へ] をクリックします。

   2f [Save the exported certificate (エクスポートされた証明書の保存)] をクリックし、エクスポートされた pfx 証明書を保存します。

3 ステップ 2 でエクスポートした pfx 証明書を Java キーストアにインポートします。

   3a Java に付属するキーツールを使用します。JDK 6 以上を使用する必要があります。

   3b コマンドプロンプトで次のコマンドを入力します。

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

   次に例を示します。

```
keytool -importkeystore -srckeystore cert.pfx -srcstoretype PKCS12
-destkeystore msgw.jks
```

   3c 要求されたときにはパスワードを入力してください。

4 iManager を使用して、このキーストアを使用するように管理対象システムのゲートウェイドライバの設定を変更します。

4a [Identity Manager Overview (Identity Manager の概要)] から、管理対象システムのゲートウェイドライバが含まれるドライバセットをクリックします。

4b ［driver state (ドライバ状態)］アイコンをクリックし、[Edit properties (プロパティの編集)］ > ［Driver configuration (ドライバ環境設定)] の順に選択します。

4c [Show Connection Parameters (接続パラメータの表示)] を［true］に設定し、[Driver configuration mode (ドライバ環境設定モード)] を［remote (リモート)］に設定します。

4d キーストアファイルの完全なパスとパスワードを入力します。

4e 保存してドライバを再起動します。

5 iManager を使用して、このキーストアを使用するようにデータ収集サービスドライバの設定を変更します。

5a [Identity Manager Overview (Identity Manager の概要)] から、管理対象システムのゲートウェイドライバが含まれるドライバセットをクリックします。

5b ［driver state (ドライバ状態)］アイコンをクリックし、[Edit properties (プロパティの編集)］ > ［Driver configuration (ドライバ環境設定)] の順に選択します。

5c [Managed System Gateway Registration (管理対象システムのゲートウェイの登録)] という見出しの下にある [Managed System Gateway Driver Configuration Mode (管理対象システムのゲートウェイドライバの環境設定モード)] を［remote (リモート)］に設定します。

5d キーストアの完全なパス、パスワード、およびステップ 1c で入力した別名を入力します。

5e 保存してドライバを再起動します。

Identity Reporting の設定

Identity Reporting のインストール後でも、さまざまなインストールプロパティを変更できます。変更するには、設定更新ユーティリティ (configupdate.sh) ファイルを実行します。

環境設定ツールで Identity Reporting の設定を変更した場合、変更を反映するには Tomcat を再起動する必要があります。ただし、Identity Reporting の Web ユーザインタフェースで変更を加えた場合は、サーバの再起動は必要ありません。

- 116 ページの 「［Identity Data Collection Services (アイデンティティデータ収集サービス)］ページへのデータソースの手動追加」
- 116 ページの 「Oracle データベースでのレポートの実行」
- 116 ページの 「データベーススキーマの手動生成」
- 119 ページの 「Identity Reporting 用の REST API の展開」
- 119 ページの 「リモート PostgreSQL データベースへの接続」

[Identity Data Collection Services (アイデンティティデータ収集サービス)] ページへのデータソースの手動追加

1. Identity Reporting アプリケーションにログインします。
2. [データソース] をクリックします。
3. [[追加]] をクリックします。
4. [データソースの追加] ダイアログボックスで、[事前定義リストから選択します] ラジオボタンをクリックします。
5. [IDMDCSDataSource] を選択します。
6. [保存] をクリックします。

Oracle データベースでのレポートの実行

Identity Reporting は、リモートの Oracle データベースに対してレポートを実行できます。Oracle データベースを実行しているサーバに ojbc8.jar ファイルが存在することを確認します。

データベーススキーマの手動生成

インストール後にデータベーススキーマを手動で生成するには、データベースについて次のいずれかの手順を実行します。

- 116 ページの 「PostgreSQL データベースに対する Create_rpt_roles_and_schemas.sql スキーマの設定」
- 117 ページの 「Oracle データベースに対する Create_rpt_roles_and_schemas.sql スキーマの設定」
- 118 ページの「MS SQL データベースに対する Create_rpt_roles_and_schemas.sql スキーマの設定」
- 118 ページの 「データベースチェックサムのクリア」

PostgreSQL データベースに対する Create_rpt_roles_and_schemas.sql スキーマの設定

1. C:\NetIQ\idm\apps\IdentityReporting\sql にある SQL、create_dcs_roles_and_schemas.sql および create_rpt_roles_and_schemas.sql を使用して、データベースに必要な役割を追加します。
2. postgres ユーザとして PGAdmin にログインします。
3. クエリツールを実行します。
4. Create_rpt_roles_and_schemas および Create_dcs_roles_and_schemas プロシージャを作成するには、これらの SQL からクエリツールにコンテンツをコピーして、接続されているデータベースに対して実行します。
5. IDM_RPT_DATA、IDM_RPT_CFG、および IDMRPTUSER 役割を作成するには、次のコマンドを指定された順序で実行します。

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

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

たとえば、IDM_RPT_DATA、IDMRPTUSER、および IDM_RPT_CFG のパスワードが、それぞれ *password*、*password1*、および *password2* の場合、以下のコマンドを実行する必要があります。

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

Select CREATE_RPT_ROLES_AND_SCHEMAS('password2');
```

6 get_formatted_user_dn.sql のコンテンツを C:\NetIQ\idm\apps\IdentityReporting\sql からクエリツールにコピーし、接続されたデータベースに対して実行します。

注 : データベーススキーマ作成オプションとして **[File]** を選択した場合、get_formatted_user_dn.sql 関数を手動で追加する必要があります。データベーススキーマ作成オプションとして **[Now]** または **[Startup]** を選択した場合、インストーラはこの関数をデータベースに追加します。

Oracle データベースに対する Create_rpt_roles_and_schemas.sql スキーマの設定

1 C:\NetIQ\idm\apps\IdentityReporting\sql から create_dcs_roles_and_schemas-orcale.sql および create_rpt_roles_and_schemas-orcale.sql を使用して、データベースに必要な役割を追加します。

2 データベース管理者ユーザとして SQL Developer にログインします。

3 Create_rpt_roles_and_schemas および Create_dcs_roles_and_schemas プロシージャを作成するには、これらの SQL から SQL Developer にコンテンツをコピーして、接続されているデータベースに対して実行します。

4 IDM_RPT_DATA、IDM_RPT_CFG、および IDMRPTUSER 役割を作成するには、次のコマンドを指定された順序で実行します。

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

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

たとえば、IDM_RPT_DATA、IDMRPTUSER、および IDM_RPT_CFG のパスワードが、それぞれ *password*、*password1*、および *password2* の場合、以下のコマンドを実行する必要があります。

```
begin
CREATE_DCS_ROLES_AND_SCHEMAS('password', 'password1');
end;

begin
CREATE_RPT_ROLES_AND_SCHEMAS('password2');
end;
```

5 get_formatted_user_dn-oracle.sql のコンテンツを C:\NetIQ\idm\apps\IdentityReporting\sql から SQL Developer にコピーし、接続されたデータベースに対して実行します。

注 : データベーススキーマ作成オプションとして File を選択した場合、**[get_formatted_user_dn-oracle.sql]** 関数を手動でデータベースに追加する必要があります。データベーススキーマ作成オプションとして **[Now]** または **[Startup]** を選択した場合、インストーラはこの関数をデータベースに追加します。

MS SQL データベースに対する Create_rpt_roles_and_schemas.sql スキーマの設定

1 delete_create_dcs_roles_and_schemas-mssql.sql および delete_get_formatted_user_dn-mssql.sql を実行します。

2 C:\NetIQ\idm\apps\IdentityReporting\sql から create_dcs_roles_and_schemas.mssql および create_rpt_roles_and_schemas.mssql を使用して、データベースに必要な役割を追加します。

3 データベース管理者ユーザとして SQL Developer にログインします。

4 Create_rpt_roles_and_schemas および Create_dcs_roles_and_schemas プロシージャを作成するには、コンテンツを create_dcs_roles_and_schemas.mssql および create_rpt_roles_and_schemas.mssql から SQL Developer にコピーし、接続されたデータベースに対して実行します。

5 IDM_RPT_DATA、IDM_RPT_CFG、および IDMRPTUSER 役割を作成するには、次のコマンドを指定された順序で実行します。

execute CREATE_DCS_ROLES_AND_SCHEMAS '<Set pwd for IDM_RPT_DATA>', '<Set pwd for IDMRPTUSER>'

execute CREATE_DCS_ROLES_AND_SCHEMAS '<Set pwd for IDM_RPT_DATA>', '<Set pwd for IDMRPTUSER>'

6 get_formatted_user_dn.sql のコンテンツを C:\NetIQ\idm\apps\IdentityReporting\sql から SQL Developer にコピーし、接続されたデータベースに対して実行します。

データベースチェックサムのクリア

1 C:\NetIQ\idm\apps\IdentityReporting\sql で次の .sql ファイルを見つけます。

- 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 データベースチェックサムをクリアします。

2a 各 .sql で clearchsum コマンドを実行するには、各ファイルの初めに次の行を追加します。

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

変更されたコンテンツは次のようになるはずです。

```
--
*********************************************************************
**
-- 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 対応するユーザで各 .sql を実行します。

3 データベースに変更をコミットします。

Identity Reporting 用の REST API の展開

Identity Reporting には、レポーティング機能内でさまざまな機能を可能にする複数の REST API が組み込まれています。これらの REST API は認証に OAuth2 プロトコルを使用します。

Tomcat では、Identity Reporting がインストールされるときに、rptdoc war および dcsdoc war が自動的に展開されます。

リモート PostgreSQL データベースへの接続

PostgreSQL データベースが別のサーバにインストールされている場合は、リモートデータベースの postgresql.conf および pg_hba.conf ファイルのデフォルト設定を変更する必要があります。

1 postgresql.conf ファイルのリスニングアドレスを変更します。

デフォルトでは、PostgreSQL は localhost 接続をリスンできます。リモート TCP/IP 接続は許可されません。リモート TCP/IP 接続を許可するには、C:\NetIQ\idm\apps\postgres\data\postgresql.conf ファイルに次のエントリを追加します。

```
listen_addresses = '*'
```

サーバ上に複数のインタフェースがある場合は、リスンされる特定のインタフェースを指定できます。

2 pg_hba.conf ファイルにクライアント認証エントリを追加します。

デフォルトで、PostgreSQL は localhost からの接続のみを受諾します。リモート接続は拒否します。これは、有効なパスワード (md5 キーワード) を入力したユーザには IP アドレスからのログインを許可する、アクセス制御ルールを適用することによって制御されます。リモート接続を受け入れるには、C:\NetIQ\idm\apps\postgres\data\pg_hba.conff ファイルに次のエントリを追加します。

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

たとえば、192.168.104.24/26 trust です。

これは IPv4 アドレスに対してのみ機能します。IPv6 アドレスの場合、次のエントリを追加します。

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

特定のネットワーク上にある複数のクライアントコンピュータからの接続を許可する場合は、このエントリに CIDR アドレス形式でネットワークアドレスを指定します。

pg_hba.conf ファイルは、次のクライアント認証形式をサポートしています。

- ローカルデータベースユーザ認証方法 [認証オプション]
- ホストデータベースユーザ CIDR アドレス認証方法 [認証オプション]
- hostssl データベースユーザ CIDR アドレス認証方法 [認証オプション]
- hostnossl データベースユーザ CIDR アドレス認証方法 [認証オプション]

CIDR アドレス形式の代わりに、次の形式を使用して別のフィールドに IP アドレスとネットワークマスクを指定できます。

- ホストデータベースユーザ IP アドレス IP マスク認証方法 [認証オプション]
- hostssl データベースユーザ IP アドレス IP マスク認証方法 [認証オプション]
- hostnossl データベースユーザ IP アドレス IP マスク認証方法 [認証オプション]

3 リモート接続をテストします。

3a リモート PostgreSQL サーバを再起動します。

3b ユーザ名とパスワードを使用してリモートでサーバにログインします。

Identity Manager のアクティベート

Identity Manager をインストールする場合や、Identity Manager を初めて実行する場合、アクティベーションコードは必要ありません。ただし、アクティベーションコードがない場合、インストールから 90 日を経過すると Identity Manager は機能しなくなります。この 90 日の期間中またはその後いつでも Identity Manager をアクティベートできます。詳細については、『*NetIQ Identity Manager Overview and Planning Guide*』の「Activating Identity Manager」を参照してください。

Identity Manager コンポーネントが使用するポートの確認

Identity Manager コンポーネントは、互いに通信するためにさまざまなポートを使用します。デフォルトではファイアウォールでポートが開かれます。Identity Manager コンポーネントで使用されるポートを確認するには、『*NetIQ Identity Manager Security Guide*』の「Understanding Identity Manager Communication」を参照してください。

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

```
  requests:
      cpu: "1"
      memory: 1Gi
volumeMounts:
  - name: data
    mountPath: /config
env:
- name: UPGRADE_IDM
  value:
- name: IS_ADVANCED_EDITION
  value:
- name: INSTALL_ENGINE
  value:
- name: INSTALL_IDVAULT
  value:
- name: IS_COMMON_PASSWORD
  value:
- name: COMMON_PASSWORD
  value:
- name: TREE_CONFIG
  value:
- name: ID_VAULT_PASSWORD
  value:
- name: ID_VAULT_EXISTING_SERVER
  value:
- name: ID_VAULT_EXISTING_NCP_PORT
  value:
- name: ID_VAULT_EXISTING_LDAPS_PORT
  value:
- name: ID_VAULT_EXISTING_CONTEXTDN
  value:
- name: ID_VAULT_TREENAME
  value:
- name: ID_VAULT_ADMIN_LDAP
  value:
- name: ID_VAULT_ADMIN
  value:
- name: ID_VAULT_PASSWORD
  value:
- name: ID_VAULT_VARDIR
  value:
- name: ID_VAULT_DIB
  value: '
- name: ID_VAULT_NCP_PORT
  value:
- name: ID_VAULT_LDAP_PORT
  value:
- name: ID_VAULT_LDAPS_PORT
  value:
- name: ID_VAULT_HTTP_PORT
  value:
```

```
    - name: ID_VAULT_HTTPS_PORT
      value:
    - name: ID_VAULT_CONF
      value:
    - name: ID_VAULT_DRIVER_SET
      value:
    - name: ID_VAULT_DEPLOY_CTX
      value:
    - name: ID_VAULT_SERVER_CONTEXT
      value:
volumes:
  - name: data
    persistentVolumeClaim:
      claimName: task-pv-claim1
```

IV Designer のインストール

このセクションでは、Designer for Identity Manager のインストールプロセスを順を追って説明します。デフォルトでは、インストールプログラムは C:\NetIQ にコンポーネントをインストールします。

重要 : Designer インストールプログラムを含むディレクトリ名にスペースが含まれていないことを確認します。たとえば、Designer Install という名前を付けないでください。代わりに、DesignerInstall にしてください。

インストールを開始する前にインストールプロセスを確認することをお勧めします。詳細については、127 ページの第 5 章「Designer のインストールの計画」を参照してください。

5 Designer のインストールの計画

このセクションでは、Designer のインストールに必要な前提条件、考慮事項、およびシステムセットアップについて説明します。まず、次のチェックリストを参照してインストールプロセスを理解します。

- 127 ページの 「Designer のインストールチェックリスト」

Designer のインストールチェックリスト

インストールを開始する前に、次の手順を確認することをお勧めします。

	チェックリストの項目
❑	1. 計画情報を確認します。詳細については、39 ページのパート II「Identity Manager のインストールの計画」を参照してください。
❑	2. Designer のインストールに関する考慮事項を検討し、コンピュータが前提条件を満たしていることを確認します。
❑	3. Designer をインストールするため、次のいずれかのセクションを参照します。 ◆ 129 ページの 「Windows の実行可能ファイルの実行」 ◆ 129 ページの 「サイレントインストールプロセスの使用」
❑	4. 残りの Identity Manager コンポーネントをインストールします。
❑	5. (オプション) Identity Manager ソリューション用のプロジェクトを開始するため、『*NetIQ Designer for Identity Manager Administration Guide*』を参照します。

6 Designer のインストール

Identity Manager Designer は、ターゲットコンピュータに応じて、実行可能ファイル、バイナリファイル、またはテキストモードを使用してインストールできます。サイレントインストールも実行可能です。

Identity Manager の複数のコンポーネントでは Designer のパッケージが必要です。Designer をインストールする際に、インストールプログラムは自動的に複数のパッケージを新しいプロジェクトに追加します。

- 129 ページの 「Windows の実行可能ファイルの実行」
- 129 ページの 「サイレントインストールプロセスの使用」
- 130 ページの 「スペース文字が含まれるインストールパスの変更」

Windows の実行可能ファイルの実行

1. Designer をインストールするコンピュータに管理者アカウントでログインします。
2. NetIQ ダウンロード Web サイトから Identity_Manager_4.8_Designer_Windows.zip をダウンロードします。
3. Identity_Manager_4.8_Designer_Windows.zip ファイルを展開します。
4. designer_install フォルダに移動します。
5. install.exe ファイルを実行します。
6. インストールプロセスが完了するまで、ウィザードの手順に従います。

サイレントインストールプロセスの使用

スクリプトを使用することで、Designer をサイレントインストールできます。ユーザによる操作は必要ありません。designerInstaller.properties ファイルを編集していない限り、-i silent オプションはインストールにデフォルトのパラメータ値を使用します。

1. Designer をインストールするコンピュータに管理者アカウントでログインします。
2. インストールプログラムが含まれるディレクトリに移動します。
3. (オプション) Designer のインストールディレクトリと言語を設定するため、次の手順を実行します。

   3a designerInstaller.properties ファイルを開きます。このファイルは、デフォルトでは *Path_to_unzipped_Designer_file*\designer_install ディレクトリにあります。

   3b このプロパティファイルで、次のパラメータの値を変更します。

   USER_INSTALL_DIR

   Designer をインストールする場所のパスを指定します。次に例を示します。

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

末尾が designer ディレクトリでないパスを指定した場合、Designer のインストールプログラムによって自動的に designer ディレクトリが付加されます。

SELECTED_DESIGNER_LOCALE

インストール後に Designer を起動する言語を次の中から 1 つ指定します。

- zh_CN - 中国語 (簡体字)
- zh_TW - 中国語 (繁体字)
- nl - オランダ語
- en - 英語
- fr - フランス語
- de - ドイツ語
- it - イタリア語
- ja - 日本語
- pt_BR - ポルトガル語 (ブラジル)
- es - スペイン語

3c プロパティファイルを保存して閉じます。

4 プロパティファイルのディレクトリから次のコマンドを実行します。

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

スペース文字が含まれるインストールパスの変更

ディレクトリ名にスペースが含まれる場所に Designer をインストールできます。ただし、Designer のインストール後、Designer が適切に機能するよう、StartDesigner.bat ファイルと Designer.ini ファイルを変更する必要があります。スペースを手動でエスケープ文字 (「\」) に置き換えます。次に例を示します。

変更前 :

```
C:\designer installation
```

変更後 :

```
C:\designer\ installation
```

V Analyzer のインストール

このセクションでは、Analyzer for Identity Manager のインストールプロセスを順を追って説明します。Analyzer は、ワークステーションにインストールするシッククライアントコンポーネントです。Analyzer を使用して、Identity Manager ソリューションに追加する接続システムのデータを調査し、クリーンアップできます。計画段階で Analyzer を使用すると、必要な変更、およびそれらの変更を行うための最善の方法を判断できます。

デフォルトでは、インストールプログラムは C:\NetIQ\Analyzer にコンポーネントをインストールします。

インストールを開始する前にインストールプロセスを確認することをお勧めします。詳細については、133 ページの 「Analyzer のインストールチェックリスト」を参照してください。

7 Analyzer のインストールの計画

このセクションには、Analyzer for Identity Manager のインストールを準備するためのガイドが記載されています。インストールを開始する前にインストールプロセスを確認することをお勧めします。

- 133 ページの 「Analyzer のインストールチェックリスト」

Analyzer のインストールチェックリスト

インストールプロセスを開始する前に、次の手順を確認することをお勧めします。

	チェックリストの項目
❑	1. 計画情報を確認します。詳細については、39 ページのパート II「Identity Manager のインストールの計画」を参照してください。
❑	2. Analyzer のインストールに関する考慮事項を検討し、コンピュータが前提条件を満たしていることを確認します。
❑	3. Analyzer をインストールするため、次の各セクションを参照します。 ◆ インストールウィザードを使用するには、135 ページの 「Windows の実行可能ファイルの実行」を参照してください。 ◆ サイレントインストールについては、135 ページの 「サイレントインストールプロセスの使用」を参照してください。
❑	4. Analyzer を有効にするには、『*NetIQ Identity Manager Overview and Planning Guide*』の「Activating Analyzer」を参照してください。

8 Analyzer のインストール

このセクションでは、Analyzer のインストールプロセス、および使用環境を Analyzer 用に設定するプロセスを順を追って説明します。

- 135 ページの 「Windows の実行可能ファイルの実行」
- 135 ページの 「サイレントインストールプロセスの使用」

Windows の実行可能ファイルの実行

1. Analyzer をインストールするコンピュータに管理者アカウントでログインします。
2. NetIQ ダウンロード Web サイトから Identity_Manager_4.8_Analyzer_Windows.zip をダウンロードします。
3. Identity_Manager_4.8_Analyzer_Windows.zip ファイルを展開します。
4. analyzer_install フォルダに移動します。
5. install.exe ファイルを実行します。
6. インストールプロセスが完了するまで、ウィザードの手順に従います。

サイレントインストールプロセスの使用

スクリプトを使用することで、Analyzer をサイレントインストールできます。ユーザによる操作は必要ありません。analyzerInstaller.properties ファイルを編集していない限り、-i silent オプションはインストールにデフォルトのパラメータ値を使用します。

1. Analyzer をインストールするコンピュータに管理者アカウントでログインします。
2. インストールプログラムが含まれるディレクトリに移動します。
3. (オプション) Analyzer のインストールディレクトリと言語を設定するため、次の手順を実行します。

   3a analyzerInstaller.properties ファイルを開きます。このファイルは、デフォルトでは *Path_to_unzipped_Analyzer_file*\analyzerInstall ディレクトリにあります。

   3b このプロパティファイルで、次のパラメータの値を変更します。

   USER_INSTALL_DIR

   Analyzer をインストールする場所のパスを指定します。次に例を示します。

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

   末尾が analyzer ディレクトリでないパスを指定した場合、Analyzer のインストールプログラムによって自動的に analyzer ディレクトリが付加されます。

SELECTED_ANALYZER_LOCALE

インストール後に Analyzer を起動する言語を次の中から 1 つ指定します。

- zh_CN - 中国語 (簡体字)
- zh_TW - 中国語 (繁体字)
- nl - オランダ語
- en - 英語
- fr - フランス語
- de - ドイツ語
- it - イタリア語
- ja - 日本語
- pt_BR - ポルトガル語 (ブラジル)
- es - スペイン語

3c プロパティファイルを保存して閉じます。

4 プロパティファイルのディレクトリから次のコマンドを実行します。

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

9 インストール後のタスク

Identity Manager がインストールされた後、ビジネスプロセスにより定義されたポリシーと要件を満たすように、インストールしたドライバを設定する必要があります。監査イベントを収集するように Sentinel Log Management for IGA を設定する必要もあります。インストール後のタスクには、通常次の項目が含まれます。

- 137 ページの 「接続システムの設定」
- 137 ページの 「ドライバセットの作成と設定」
- 140 ページの 「ドライバの作成」
- 141 ページの 「ポリシーの定義」
- 141 ページの 「ドライバアクティビティの管理」
- 141 ページの 「Identity Manager のアクティベート」

接続システムの設定

Identity Manager により、アプリケーション、ディレクトリ、およびデータベースで情報を共有できます。ドライバ固有の設定手順については、Identity Manager ドライバのマニュアルを参照してください。

ドライバセットの作成と設定

ドライバセットは、複数の Identity Manager ドライバを格納するコンテナです。任意のサーバで一度に関連付けできるドライバセットは 1 つだけです。ドライバセットを作成するには Designer ツールを使用できます。サーバがすでにドライバセットに関連付けられている場合に、サーバを新しいドライバセットに割り当てると、サーバは元のドライバセットから削除されます。

アイデンティティボールトとのパスワード同期をサポートするためには、Identity Manager でドライバセットにパスワードポリシーが設定されている必要があります。Identity Manager でデフォルトのユニバーサルパスワードポリシーパッケージを使用するか、既存の組織の要件に基づいてパスワードポリシーを作成できます。ただし、パスワードポリシーには DirMXL-PasswordPolicy オブジェクトが含まれている必要があります。ポリシーオブジェクトにアイデンティティボールトが存在しない場合は、オブジェクトを作成できます。

- 138 ページの 「ドライバセットの作成」
- 138 ページの 「デフォルトのパスワードポリシーのドライバセットへの割り当て」
- 139 ページの 「アイデンティティボールトでのパスワードポリシーオブジェクトの作成」

- 139 ページの 「カスタムパスワードポリシーの作成」
- 140 ページの 「アイデンティティボールトでのデフォルト通知コレクションオブジェクトの作成」

ドライバセットの作成

Designer for Identity Manager では、ドライバセットを作成および設定するための多数の設定を用意しています。これらの設定により、グローバル環境設定値、ドライバセットパッケージ、ドライバセット名前付きパスワード、ログレベル、トレースレベル、および Java 環境パラメータを指定できます。詳細については、『*NetIQ Designer for Identity Manager Administration Guide*』の「Configuring Driver Sets」を参照してください。

デフォルトのパスワードポリシーのドライバセットへの割り当て

アイデンティティボールトの各ドライバセットに DirMXL-PasswordPolicy オブジェクトを割り当てる必要があります。Identity Manager のデフォルトのユニバーサルパスワードポリシーパッケージには、このポリシーオブジェクトが含まれています。デフォルトのポリシーによりユニバーサルパスワードポリシーがインストールされて割り当てられ、Identity Manager エンジンがドライバ用にランダムパスワードを自動的に生成する方法を制御します。

または、カスタムパスワードポリシーを使用する場合は、パスワードポリシーオブジェクトとポリシーを作成する必要があります。詳細については、139 ページの 「アイデンティティボールトでのパスワードポリシーオブジェクトの作成」および 139 ページの 「カスタムパスワードポリシーの作成」を参照してください。

1. Designer でプロジェクトを開きます。
2. ［アウトライン］ペインで、プロジェクトを展開します。
3. **[パッケージカタログ ］ > ［共通]** を展開し、デフォルトのユニバーサルパスワードポリシーパッケージが存在するかどうかを確認します。
4. (状況によって実行) パスワードポリシーパッケージが Designer に一覧表示されていない場合は、次の手順を実行します。
   - **4a** **[パッケージカタログ]** を右クリックします。
   - **4b** **[パッケージのインポート]** を選択します。
   - **4c** **[Identity Manager Default Universal Password Policy (Identity Manager のデフォルトのユニバーサルパスワードポリシー)]** を選択し、**[OK]** をクリックします。

     表にすべての使用可能なパッケージが表示されるようにするには、**[Show Base Packages Only (基本パッケージのみ表示)]** の選択を解除する必要があります。
5. 各ドライバセットを選択し、パスワードポリシーを割り当てます。

アイデンティティボールトでのパスワードポリシーオブジェクトの作成

DirMXL-PasswordPolicy オブジェクトがアイデンティティボールトに存在しない場合は、Designer または ldapmodify ユーティリティを使用してこのオブジェクトを作成できます。Designer でこれを実行する方法の詳細については、『*NetIQ Designer for Identity Manager Administration Guide*』の「Configuring Driver Sets」を参照してください。ldapmodify ユーティリティを使用するには、次の手順を使用します。

1 テキストエディタで、次の属性を持つ LDAP Data Interchange Format (LDIF) ファイルを作成します。

```
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>
```

注 : コンテンツをそのままコピーすると、ファイルにいくつかの非表示の特殊文字が挿入される場合があります。これらの属性をアイデンティティボールトに追加する際に ldif_record() = 17 のエラーメッセージが表示される場合は、2 つの DN 間にスペースを挿入してください。

2 識別ボールトに DirMXL-PasswordPolicy オブジェクトを追加するには、Identity Manager インストールキットの install/utilities ディレクトリから ldapmodify.exe を実行して、ファイルから属性をインポートします。

カスタムパスワードポリシーの作成

Identity Manager でデフォルトのパスワードポリシーを使用するのではなく、組織の要件に基づいて新しいポリシーを作成できます。パスワードポリシーは、ツリー構造全体、パーティションルートコンテナ、コンテナ、または特定のユーザに割り当てることができます。管理を簡易化するには、ツリー内のできるだけ高い位置にパスワードポリシーを割り当てることをお勧めします。詳細については、『*Password Management 3.3.2 Administration Guide*』の「Creating Password Policies」を参照してください。

注 : ドライバセットに DirXML-PasswordPolicy オブジェクトを割り当てる必要もあります。詳細については、139 ページの 「アイデンティティボールトでのパスワードポリシーオブジェクトの作成」を参照してください。

アイデンティティボールトでのデフォルト通知コレクションオブジェクトの作成

デフォルトの通知コレクションは、電子メール通知テンプレートのセットとテンプレートから生成された電子メールを送信する際に使用される SMTP サーバを含むアイデンティティボールトオブジェクトです。デフォルトの通知コレクションオブジェクトがアイデンティティボールトに存在しない場合は、Designer を使用して作成できます。

1 Designer でプロジェクトを開きます。
2 ［アウトライン］ペインで、プロジェクトを展開します。
3 アイデンティティボールトを右クリックし、アイデンティティボールトの **[プロパティ]** をクリックします。
4 **[パッケージ]** をクリックし、**[Add Packages (パッケージの追加)]** アイコンをクリックします。
5 すべての通知テンプレートパッケージを選択し、**[OK]** をクリックします。
6 **[インストール]** 操作でパッケージをインストールするには、**[適用]** をクリックします。
7 通知テンプレートをアイデンティティボールトに展開します。

ドライバの作成

ドライバを作成するには、Designer で提供されているパッケージ管理機能を使用します。使用する各 Identity Manager ドライバに対して、ドライバオブジェクトを作成し、ドライバ設定をインポートします。ドライバオブジェクトには、設定パラメータとそのドライバのポリシーが含まれます。ドライバオブジェクトを作成する一貫として、ドライバパッケージをインストールしてから、環境に合わせてドライバ設定を変更します。

ドライバパッケージには、デフォルトのポリシーセットが含まれています。これらのポリシーは、データ共有モデルを簡単に実装できるようにすることを目的としています。ほとんどの場合は、出荷時のデフォルト設定を使用してドライバを設定してから、環境の要件に応じてドライバの設定を変更します。ドライバを作成して設定した後で、それをアイデンティティボールトに展開して起動します。一般的に、ドライバの作成プロセスには次のアクションが含まれます。

1. ドライバパッケージのインポート
2. ドライバパッケージのインストール
3. ドライバオブジェクトの設定
4. ドライバオブジェクトの展開
5. ドライバオブジェクトの起動

追加情報およびドライバ固有の情報については、Identity Manager ドライバの Web サイトから関連するドライバ実装ガイドを参照してください。

ポリシーの定義

ポリシーにより、識別 \'83\'7bールトに対する情報フローを特定の環境に合わせてカスタ\'83\'7d イズできます。たとえば、ある会社ではメインのユーザクラスとして inetorgperson を使用していて、別の会社では User を使用しているとします。これを処理するために、各システムで呼び出すユーザを Identity Manager エンジンに指示するポリシーが作成されています。接続システム間でユーザに影響する操作をやり取りする場合、Identity Manager は、この変更を行うポリシーを適用します。

また、ポリシーは、新しいオブジェクトの作成、属性値の更新、スキーマ変換の実行、一致条件の定義、Identity Manager の関連付けの維持など、多くのタスクを実行します。

NetIQ では、Designer を使用して、ビジネスニーズを満たすようにドライバのポリシーを定義することをお勧めします。ポリシーの詳細ガイドについては、『*NetIQ Identity Manager - Using Designer to Create Policies* guide』および『*NetIQ Identity Manager Understanding Policies Guide*』を参照してください。Identity Manager が使用する文書型定義 (DTD) については、Identity Manager DTD Reference を参照してください。リソースには次のものが含まれます。

- 使用可 \'94\'5c な各ポリシーの詳細な説明
- 各条件、アクション、名詞、および動詞のサンプルと \'8d\'5c 文を含む、Policy Builder の詳細なユーザガイドとリファレンス
- XSLT スタイルシートを使用したポリシー作成の説明

ドライバアクティビティの管理

Identity Manager ドライバの管理および設定機能を使用するには、Designer または iManager を使用してください。これらの機能は、『*NetIQ Identity Manager Driver Administration Guide*』に詳細に記載されています。

Identity Manager のアクティベート

Identity Manager をインストールする場合や、Identity Manager を初めて実行する場合、アクティベーションコードは必要ありません。ただし、アクティベーションコードがない場合、インストールから 90 日を経過すると Identity Manager は機能しなくなります。この 90 日の期間中またはその後いつでも Identity Manager をアクティベートできます。詳細については、『*NetIQ Identity Manager Overview and Planning Guide*』の「Understanding Licensing and Activation」を参照してください。

VI Identity Manager のアップグレード

このセクションでは、Identity Manager のコンポーネントのアップグレードについて説明します。既存データを新しいサーバにマイグレートするには、189 ページのパート VII「Identity Manager のデータの新しいインストールへのマイグレート」を参照してください。アップグレードとマイグレーションの違いの詳細については、147 ページの 「アップグレードとマイグレーションの理解」を参照してください。

10 Identity Manager のアップグレードの準備

このセクションでは、Identity Manager ソリューションを最新バージョンにアップグレードする準備について説明します。Identity Manager の大部分のコンポーネントは、ターゲットコンピュータに応じて、実行可能ファイルまたはバイナリファイルを使用して、またはテキストモードで、アップグレードできます。アップグレードを実行するには、Identity Manager インストールキットをダウンロードして、圧縮解除する必要があります。

警告 : Identity Manager 4.8 とともにインストールされるコンポーネントを更新するには、常に Identity Manager パッチチャネルを利用する必要があります。そうしないと、通常の Identity Manager パッチの更新中に重大な競合が発生する可能性があります。

- 145 ページの 「Identity Manager のアップグレードのチェックリスト」
- 147 ページの 「アップグレードとマイグレーションの理解」
- 149 ページの 「アップグレードの順序」
- 149 ページの 「サポートされているアップグレードパス」
- 153 ページの 「現在の設定のバックアップ」

Identity Manager のアップグレードのチェックリスト

アップグレードを実行するには、次のチェックリストの手順を実行することをお勧めします。

	チェックリストの項目
❑	1. アップグレードとマイグレーションの違いをレビューします。詳細については、147 ページの 「アップグレードとマイグレーションの理解」を参照してください。
❑	2. Identity Manager 4.6.4 にアップグレードします。4.6.4 より古いバージョンからバージョン 4.8 にアップグレードまたはマイグレートすることはできません。詳細については、『NetIQ Identity Manager 4.5 Setup Guide』を参照してください。
❑	3. Identity Manager をアップグレードする最新のインストールキットを用意していることを確認します。詳細については、『*NetIQ Identity Manager Overview and Planning Guide*』の「Identity Manager の入手場所」を参照してください。
❑	4. Identity Manager の最新バージョンのハードウェアとソフトウェアの前提条件をコンピュータが満たしていることを確認します。

	チェックリストの項目
❑	5. 現在のプロジェクト、ドライバ環境設定、およびデータベースをバックアップします。詳細については、153 ページの 「現在の設定のバックアップ」を参照してください。
❑	6. Designer を最新バージョンにアップグレードします。詳細については、157 ページの 「Designer のアップグレード」を参照してください。
❑	7. iManager をインストールするか、Identity Manager の最新バージョンにアップグレードします。詳細については、次のいずれかのセクションを参照してください。 • **の確認** : 51 ページの 「インストール手順」 • **アップグレード** : 163 ページの 「iManager のアップグレード」
❑	8. Identity Manager を実行しているサーバ上で、eDirectory を最新のバージョンにアップグレードしてパッチを適用します。
❑	9. iManager のプラグインを iManager のバージョンと一致するようにアップデートします。詳細については、166 ページの 「iManager プラグインのアップグレードまたは再インストール後のアップデート」を参照してください。
❑	10. Identity Manager エンジンのインストール先であるサーバに関連付けられているドライバを停止します。詳細については、178 ページの 「Identity Manager ドライバの停止と起動」を参照してください。
❑	11. Identity Manager エンジンをアップグレードします。詳細については、160 ページの「Identity Manager エンジンのアップグレード」を参照してください。 **注 :** Identity Manager エンジンを新しいサーバにマイグレートしている場合、現在の Identity Manager サーバ上のものと同じ eDirectory レプリカを使用できます。詳細については、197 ページの 「Identity Manager エンジンの新しいサーバへのマイグレート」を参照してください。
❑	12. (状況によって実行) Identity Manager エンジンのドライバセットのいずれかのドライバがリモートローダドライバである場合、ドライバごとにリモートローダサーバをアップグレードします。詳細については、162 ページの 「リモートローダのアップグレード」を参照してください。
❑	13. (状況によって実行) パッケージを使用する場合、既存のドライバのパッケージをアップグレードして、新しいポリシーを取得します。詳細については、180 ページの 「Identity Manager ドライバのアップグレード」を参照してください。 この手順は、パッケージのより新しいバージョンが入手可能で、ドライバのポリシーに既存のドライバに追加する新しい機能が含まれている場合にのみ必要です。
❑	14. (状況によって実行) SSPR がインストールされていない場合は、これをインストールします。詳細については、56 ページの 「SSPR のインストール」を参照してください。
❑	15. 識別情報アプリケーションをアップグレードします。詳細については、166 ページの 「Identity Applications のアップグレード」を参照してください。
❑	16. Identity Reporting をアップグレードします . 詳細については、175 ページの「Identity Reporting のアップグレード」を参照してください。

	チェックリストの項目
❑	17. 識別情報アプリケーションと Identity Manager エンジンの関連ドライバを起動します。詳細については、178 ページの 「Identity Manager ドライバの停止と起動」を参照してください。
❑	18. (状況によって実行) Identity Manager エンジンまたは識別情報アプリケーションを新しいサーバにマイグレートした場合、この新しいサーバをドライバセットに追加します。詳細については、182 ページの 「新しいサーバをドライバセットに追加する」を参照してください。
❑	19. (状況によって実行) カスタムポリシーとルールがある場合は、カスタマイズされている設定を復元します。詳細については、184 ページの 「ドライバへのカスタムポリシーとルールの復元」を参照してください。
❑	20. アップグレードした Identity Manager ソリューションをアクティベートします。詳細については、141 ページの 「Identity Manager のアクティベート」を参照してください。

アップグレードとマイグレーションの理解

既存の Identity Manager インストールの最新バージョンをインストールする場合、通常は**アップグレード**を実行します。ただし、新しいバージョンの Identity Manager が既存のバージョンからのアップグレードパスを提供していない場合は、4.8 へのアップグレードが可能なバージョンにアップグレードする必要があります。または、新しいマシンへのマイグレーションを実行することもできます。**マイグレーション**は、新しいサーバに Identity Managers をインストールして、既存のデータをこの新しいサーバにマイグレートすることとして定義されています。

製品評価期間中または Advanced Edition のアクティベーション後に、ご使用の環境で Advanced Edition 機能が必要ないときは、Standard Edition に「切り替え」たい場合があります。Identity Manager では、簡単な手順に従って、Advanced Edition から Standard Edition に切り替えることができます。

アップグレード

Identity Manager 4.7 Standard Edition および Advanced Edition は、通常はアップグレード可能です。

- **Identity Manager 4.7 Standard Edition:** Identity Manager 4.7 Standard Edition を現在インストールしている場合は、それを Identity Manager 4.8 Standard Edition に直接アップグレードできます。詳細については、『*NetIQ Identity Manager 4.8 Standard Edition をインストールおよびアップグレードするためのクイックスタートガイド*』を参照してください。

Identity Manager 4.7 Standard Edition を Identity Manager 4.8 Advanced Edition にアップグレードするには、次のいずれかのアプローチを選択して、アップグレードを完了してください。

- Identity Manager 4.7 Standard EditionをIdentity Manager 4.8 Standard Editionにアップグレードし、それを Identity Manager 4.8 Advanced Edition にアップグレードします。
- Identity Manager 4.7 Standard Edition を Identity Manager 4.7 Advanced Edition にアップグレードし、それを Identity Manager 4.8 Advanced Edition にアップグレードします。

- **Identity Manager 4.7 Advanced Edition:** 現在 Identity Manager 4.7 Advanced Edition をインストールしている場合は、それを Identity Manager 4.8 Advanced Edition に直接アップグレードできます。詳細については、145 ページの 「Identity Manager のアップグレードのチェックリスト」を参照してください。

NICI の最新バージョンを含む Identity Manager 4.7.4 を 4.8 にアップグレードすると、NICI の最新バージョンがすでにインストールされているので、Upgrade.log に終了コード 1603 が表示されます。このコードは無視して構いません。

マイグレーション

直接アップグレードを実行できない場合もあります。このようなシナリオでは、マイグレーションが推奨されます。たとえば、今後サポートされないオペレーティングシステムを実行しているサーバ上に Identity Manager をインストールしていた場合、アップグレードではなく、マイグレーションを実行する必要があります。

1 つのドライバセットに複数のサーバを関連付けている場合、一度に 1 台のサーバに対してアップグレードまたはマイグレーションを実行することができます。時間が足りずに一度ですべてのサーバをアップグレードしない場合、各サーバのアップグレードが完了するまでは、ドライバは複数のバージョンの Identity Manager と連携して動作します。

重要 : Identity Manager 4.8 以降でのみサポートされているドライバの機能を有効にした場合、バージョンが混在しているサーバでは、ドライバは動作を停止します。古いエンジンは新しい機能を扱うことができません。そのため、すべてのサーバを Identity Manager 4.8 以降にアップグレードするまでは、ドライバは動作しません。

Advanced Edition から Standard Edition への切り替え

Identity Manager では、製品評価期間または Advanced Edition のアクティベーション後に、Advanced Edition から Standard Edition に切り替えることができます。

重要 : Advanced Edition のアクティベーションをすでに適用している場合は、すべての Standard Edition 機能が Advanced Edition で使用可能であるため、Standard Edition に移行する必要はありません。ご使用の環境で Advanced Edition 機能が必要なく、Identity Manager の展開をスケールダウンする場合にのみ Standard Edition に切り替える必要があります。詳細については、「187 ページの第 12 章「Advanced Edition から Standard Edition への切り替え」」を参照してください。

アップグレードの順序

Identity Manager のコンポーネントは、次の順序でアップグレードする必要があります。

1. Designer
2. iManager
3. Sentinel Log Management for IGA (Linux コンピュータ上にのみインストールできます)
4. 識別ボールト
5. Identity Manager エンジン
6. リモートローダ
7. iManager プラグイン
8. Identity Applications (Advanced Edition 用)
9. Identity Reporting
10. Analyzer
11. セルフサービスパスワードリセット

サポートされているアップグレードパス

Identity Manager 4.8 は、4.7.x および 4.6.x バージョンからのアップグレードをサポートします。アップグレードを開始する前に、現在のバージョンに対応するリリースノートの情報を確認することをお勧めします。

注 : Identity Manager を 4.8 バージョンにアップグレードするには、Identity Manager 4.8 アップグレード有効化パッチを適用する必要があります。このパッチを適用する条件は、Identity Manager の現在のバージョンによって異なります。詳細については、『NetIQ Identity Manager 4.8 Upgrade Enablement Patch Release Notes』を参照してください。

- 149 ページの 「Identity Manager 4.7.x バージョンからのアップグレード」
- 151 ページの 「Identity Manager 4.6.x バージョンからのアップグレード」

Identity Manager 4.7.x バージョンからのアップグレード

次の表に、Identity Manager 4.7.x バージョンのコンポーネントごとのアップグレードパスを一覧表示します。

コンポーネント	ベースバージョン	アップグレード済みのバージョン
Identity Manager エンジン	4.7.x	1. オペレーティングシステムを、サポートされるバージョンにアップグレードします。 2. アイデンティティボールトを 9.2 にアップグレードします。 3. Identity Manager エンジンを 4.8 にアップグレードします。
リモートローダ / 展開エージェント	4.7.x	4.8 リモートローダ / 展開エージェントをインストールします。
Designer	4.7.x	Designer 4.8 のインストール
識別情報アプリケーション	4.7.x	Identity Applications をアップグレードする前に、アイデンティティボールトおよび Identity Manager エンジンがそれぞれ 9.2 および 4.8 にアップグレードされていることを確認します。 1. オペレーティングシステムを、サポートされるバージョンにアップグレードします。 2. データベースを、サポートされるバージョンにアップグレードします。サポートされているデータベースのバージョンについては、NetIQ Identity Manager 技術情報 Web サイト (https://www.netiq.com/products/identity-manager/advanced/technical-information/) を参照してください。 3. (状況によって実行) SSPR が別のサーバにインストールされている場合は、コンポーネントを 4.8 バージョンにアップグレードします。 4. ユーザアプリケーションドライバ、役割およびリソースドライバのパッケージを更新します。 5. Identity Applications を 4.8 にアップグレードします。 6. Tomcat を停止します。

コンポーネント	ベースバージョン	アップグレード済みのバージョン
Identity Reporting	4.7.x	1. オペレーティングシステムを、サポートされるバージョンにアップグレードします。 2. データベースを、サポートされるバージョンにアップグレードします。サポートされているデータベースのバージョンの詳細については、NetIQ Identity Manager 技術情報 Web サイトを参照してください。 3. SLM for IGA をサポートされているバージョンにアップグレードします (インストールは Linux コンピュータでのみサポートされます)。 4. データ収集サービスドライバと管理対象サービスゲートウェイドライバのパッケージを更新します。 5. Identity Reporting 4.8 をアップグレードします。 6. (状況によって実行)［Identity Manager データ収集サービス］ページからデータ同期ポリシーを作成します。

アップグレードを開始する前に、Identity Manager ドキュメントページで現在のバージョンに対応するリリースノートの情報を確認することをお勧めします。

Identity Manager 4.6.x バージョンからのアップグレード

次の表に、Identity Manager 4.6.x バージョンのコンポーネントごとのアップグレードパスを一覧表示します。

コンポーネント	ベースバージョン	中間手順	アップグレード済みのバージョン
Identity Manager エンジン	4.6.x(ここで x は 0 ～ 3 です)	4.6.4 パッチを適用します。	1. オペレーティングシステムを、サポートされるバージョンにアップグレードします。 2. アイデンティティボールトを 9.2 にアップグレードします。 3. Identity Manager エンジンを 4.8 にアップグレードします。
リモートローダ / 展開エージェント	4.6.x。ここで x は 0 ～ 3 です。	4.6.4 パッチを適用します。	4.8 リモートローダ / 展開エージェントをインストールします。

コンポーネント	ベースバージョン	中間手順	アップグレード済みのバージョン
Designer	4.6.x。ここで x は 0 ～ 3 です。		Designer 4.8 のインストール
識別情報アプリケーション	4.6.x。ここで x は 0 ～ 3 です。	4.6.4 パッチを適用します。	Identity アプリケーションをアップグレードする前に、識別ボールトと Identity Manager エンジンがそれぞれバージョン 9.2 と 4.8 にアップグレードされていることを確認します。 1. オペレーティングシステムを、サポートされるバージョンにアップグレードします。 2. ユーザアプリケーションドライバ、役割およびリソースドライバのパッケージを更新します。 3. データベースを、サポートされるバージョンにアップグレードします。サポートされているデータベースのバージョンについては、NetIQ Identity Manager 技術情報 Web サイトを参照してください。 4. (状況によって実行) SSPR が別のサーバにインストールされている場合は、コンポーネントを 4.8 バージョンにアップグレードします。 5. Identity Applications を 4.8 にアップグレードします。 6. Tomcat を停止します。

コンポーネント	ベースバージョン	中間手順	アップグレード済みのバージョン
Identity Reporting	4.6.x。ここで x は 0 ～ 3 です。	4.6.4 パッチを適用します。	1. オペレーティングシステムを、サポートされるバージョンにアップグレードします。 2. データベースを、サポートされるバージョンにアップグレードします。サポートされているデータベースのバージョンの詳細については、NetIQ Identity Manager 技術情報 Web サイトを参照してください。 3. SLM for IGA をサポートされているバージョンにアップグレードします (インストールは Linux コンピュータでのみサポートされます)。 4. データ収集サービスドライバと管理対象サービスゲートウェイドライバのパッケージを更新します。 5. Identity Reporting を 4.8 に移行します。 6. (状況によって実行) [Identity Manager データ収集サービス] ページからデータ同期ポリシーを作成します。

アップグレードを開始する前に、Identity Manager ドキュメントページで現在のバージョンに対応するリリースノートの情報を確認することをお勧めします。

現在の設定のバックアップ

アップグレードを実行する前に、Identity Manager ソリューションの現在の設定をバックアップすることをお勧めします。ユーザアプリケーションをバックアップする必要はありません。すべてのユーザアプリケーションの環境設定は、ユーザアプリケーションドライバに保存されます。バックアップは次の方法で作成できます。

- 154 ページの 「Designer のプロジェクトのエクスポート」
- 155 ページの 「ドライバの環境設定のエクスポート」

Designer のプロジェクトのエクスポート

Designer のプロジェクトには、スキーマおよびすべてのドライバ構成情報が含まれています。Identity Manager ソリューションのプロジェクトを作成すると、すべてのドライバを 1 ステップでエクスポートでき、ドライバごとに個別のエクスポートファイルを作成する必要はありません。

- 154 ページの 「現在のプロジェクトのエクスポート」
- 154 ページの 「識別ボールトからプロジェクトを新規作成する」

現在のプロジェクトのエクスポート

すでに Designer プロジェクトがある場合には、以下の方法で、プロジェクト内の情報が識別ボールトの内容と同期されているかどうか確認してください。

1. Designer で、プロジェクトを開きます。
2. モデラーで、［識別ボールト］アイコンを右クリックして、[ライブ］ > ［比較] の順に選択します。
3. プロジェクトを評価し、相違点があれば一致させて、[OK] をクリックします。

   詳細については、『*NetIQ Designer for Identity Manager Administration Guide*』の「展開時の比較機能の使用」を参照してください。
4. ツールバーで、[プロジェクト］ > ［エクスポート] を選択します。
5. [すべて選択] をクリックして、すべてのリソースをエクスポートするように選択します。
6. プロジェクトを保存する場所と、そのフォーマットを選択し、[完了] をクリックします。

   プロジェクトは、現在のワークスペースの場所を除き、任意の場所に保存できます。Designer にアップグレードする場合には、ワークスペースロケーションを新規作成する必要があります。詳細については、『*NetIQ Designer for Identity Manager Administration Guide*』の「プロジェクトのエクスポート」を参照してください。

識別ボールトからプロジェクトを新規作成する

現在の Identity Manager ソリューションの Designer プロジェクトがない場合は、現在のソリューションをバックアップするためにプロジェクトを作成する必要があります。

1. Designer をインストールします。
2. Designer を起動して、ワークスペースの場所を指定します。
3. オンラインのアップデートをチェックするかどうかを指定して、[OK] をクリックします。
4. ［ようこそ］ページで、[Designer の実行] をクリックします。
5. ツールバーで、[プロジェクト］ > ［プロジェクトのインポート］ > ［識別ボールト] を選択します。

6 プロジェクトの名前を指定します。それから、プロジェクトのデフォルトの場所を使用するか、または別の場所を選択します。

7 [次へ] をクリックします。

8 識別ボールトに接続するために次の値を指定します。

- ［**ホスト名**］ : 識別ボールトサーバの IP アドレスまたは DNS 名
- ［**ユーザ名**］ : 識別ボールトで認証するために使用するユーザの DN
- ［**パスワード**］ : 認証ユーザのパスワード

9 [次へ] をクリックします。

10 ［識別ボールトのスキーマ］と［デフォルトの通知コレクション］は選択したままにします。

11 ［デフォルト通知コレクション］を展開し、必要のない言語を選択解除します。

デフォルトの通知コレクションは、多くの言語に翻訳されています。すべての言語をインポートすることもできますし、使用する言語だけを選択することもできます。

12 [参照] をクリックして、インポートするドライバセットを参照し、選択します。

13 この識別ボールトのドライバセットごとにステップ 12 を繰り返し、[完了] をクリックします。

14 プロジェクトがインポートされたら、[OK] をクリックします。

15 識別ボールトが 1 つだけの場合には、これで完了です。複数の識別ボールトがある場合には、ステップ 16 に進みます。

16 ツールバーの [ライブ］ > ［インポート] をクリックします。

17 追加の識別ボールトごとに、ステップ 8 からステップ 14 を繰り返します。

ドライバの環境設定のエクスポート

ドライバのエクスポートを作成することは、現在の環境設定のバックアップを作成することです。ただし、Designer は現在のところ、役割ベースのエンタイトルメントドライバとポリシーのバックアップは作成しません。iManager を使用して、役割ベースのエンタイトルメントドライバをエクスポートしてあるかどうかを確認してください。

- 155 ページの 「Designer によるドライバ環境設定のエクスポート」
- 156 ページの 「iManager を使用したドライバのエクスポートの作成」

Designer によるドライバ環境設定のエクスポート

1 Designer のプロジェクトで最新バージョンのドライバが使用されていることを確認します。詳細については、『*NetIQ Designer for Identity Manager Administration Guide*』の「Importing a Library, a Driver Set, or a Driver from the Identity Vault」を参照してください。

2 ［モデラー］で、アップグレードするドライバの行を右クリックします。

3 [環境設定ファイルのエクスポート] を選択します。

4 環境設定ファイルを保存する場所を参照して、[保存] をクリックします。

5 ［結果］ページで [OK] をクリックします。

6 各ドライバに対して、ステップ 1 ～ステップ 5 を繰り返します。

iManager を使用したドライバのエクスポートの作成

1 iManager で、[Identity Manager］ > ［Identity Manager の概要] の順に選択します。

2 ツリーでその場所を参照して選択し、ドライバセットオブジェクトを検索してから、［検索］アイコン をクリックします。

3 アップグレードするドライバを格納するドライバセットオブジェクトをクリックします。

4 アップグレードするドライバをクリックして、[エクスポート] をクリックします。

5 [次へ] をクリックして、[環境設定にリンクされているかどうかにかかわらず、含まれるすべてのポリシーをエクスポート] を選択します。

6 [次へ] をクリックし、[名前を付けて保存] をクリックします。

7 [ディスクに保存] を選択し、[OK] をクリックします。

8 [完了] をクリックします。

9 各ドライバに対して、ステップ 1 ～ステップ 8 を繰り返します。

11 Identity Manager コンポーネントのアップグレード

このセクションでは、Identity Manager の個々のコンポーネントをアップグレードする方法の詳細について説明します。たとえば、Designer は最新バージョンにアップグレードして、iManager はアップグレードしないということができます。アップグレード後に実行する必要がある可能性がある手順についても説明します。

- 157 ページの 「Designer のアップグレード」
- 158 ページの 「Identity Manager エンジンコンポーネントのアップグレード」
- 166 ページの 「Identity Applications のアップグレード」
- 175 ページの 「Identity Reporting のアップグレード」
- 177 ページの 「Analyzer のアップグレード」
- 178 ページの 「Identity Manager ドライバの停止と起動」
- 180 ページの 「Identity Manager ドライバのアップグレード」
- 182 ページの 「新しいサーバをドライバセットに追加する」
- 184 ページの 「ドライバへのカスタムポリシーとルールの復元」

Designer のアップグレード

1. Designer がインストールされているサーバに管理者としてログインします。
2. プロジェクトのバックアップコピーを作成するために、プロジェクトをエクスポートします。

   エクスポートの詳細については、『*NetIQ Designer for Identity Manager Administration Guide*』の「プロジェクトのエクスポート」を参照してください。
3. Identity_Manager_4.8_Designer_Windows.zip ファイルから Designer インストールプログラムを起動します。(<Designer zip extracted location>\designer_install\install.exe)
4. Designer をインストールする言語を選択し、使用許諾契約書の条項を確認し、同意します。
5. Designer がインストールされているディレクトリを指定し、すでに Designer がインストールされていることを示すメッセージの中で [はい] をクリックします。
6. ショートカットをデスクトップ上に配置するか、デスクトップメニュー内に配置するかを選択します。
7. 概要を確認して、[インストール] をクリックします。
8. リリースノートをレビューし、[次へ] をクリックします。
9. Designer の起動を選択し、[Done (完了)] をクリックします。

10 Designer のワークスペースの場所を指定し、[OK] をクリックします。

11 プロジェクトを閉じて変換する必要があることを示す警告メッセージで [OK] をクリックします。

12 [プロジェクト] ビューで、プロジェクトを展開し、[Project needs conversion (プロジェクトには変換が必要)] をダブルクリックします。

13 プロジェクトコンバータウィザードが実行する手順を確認し、[次へ] をクリックします。

14 プロジェクトのバックアップ用に名前を指定し、[次へ] をクリックします。

15 変換時に行われる内容の概要を確認し、[Convert (変換)] をクリックします。

16 変換終了後に概要を確認し、[開く] をクリックします。

Designer の最新バージョンにアップグレードした後、古いバージョンで作成した Designer プロジェクトをすべてインポートする必要があります。インポートプロセスを開始すると、Designer はプロジェクトコンバータウィザードを実行します。このウィザードは、古いバージョンで作成したプロジェクトを最新バージョンに変換します。ウィザードで [プロジェクトをワークスペースにコピーする] を選択します。プロジェクトコンバータの詳細については、『*NetIQ Designer for Identity Manager Administration Guide*』を参照してください。

Identity Manager エンジンコンポーネントのアップグレード

Identity Manager エンジンをアップグレードする前に、アイデンティティボールトをアップグレードしてください。Identity Manager エンジンアップグレードプロセスは、ホストコンピュータのファイルシステムに保存されているドライバシムファイルをアップデートします。

アイデンティティボールトのアップグレード

1 『*NetIQ Identity Manager Overview and Planning Guide*』の「Identity Manager の入手場所」の指示に従って、Identity_Manager_4.8_Windows.iso をダウンロードします。

2 ダウンロード済みの .iso をマウントします。

3 <iso mounted location>\IdentityManagerServer\products\eDirectory\x64 ディレクトリに移動します。

4 eDirectory_920_Windows_x86_x64.exe ファイルを実行します。

5 [Basic (基本)] タブで、次の詳細を指定します。

- [新しいツリー] を選択する場合は、次の詳細を指定します。
  - **Tree Name:** 識別ボールトのツリー名を指定します。
  - **Server FDN (サーバ FDN):** サーバ FDN を指定します。

注 : 識別ボールトでは、NCP サーバオブジェクトの FDN を最大 256 文字まで設定できますが、このオブジェクトの長さに基づいて他のより長いオブジェクトが作成されるため、この変数をずっと小さい値に制限することをお勧めします。

- **Tree Admin (ツリー管理者):** 識別ボールトの管理者名を指定します。
- **Admin Password:** 管理者パスワードを指定します。

- **[Existing Tree (既存のツリー)]** を選択する場合は、次の詳細を指定します。
  - **IP アドレス :** 識別ボールトの既存ツリーの IP アドレスを指定します。
  - **ポート番号 :** 既存のツリーのポート番号を指定します。デフォルトは 524 です。
  - **Server FDN (サーバ FDN):** サーバ FDN を指定します。
  - **Tree Admin (ツリー管理者):** 識別ボールトの既存の管理者名を指定します。
  - **Admin Password:** 管理者パスワードを指定します。

6 (状況によって実行) **[詳細]** タブで、次の詳細を指定します。

- 識別ボールトサーバでIPv6アドレスを使用するには、**[Enable IPv6 (IPv6を有効にする)]** を選択します。

注 : NetIQ では、このオプションを有効にすることをお勧めします。インストール後に IPv6 アドレス指定を有効にするには、セットアッププログラムを再度実行する必要があります。

- 拡張バックグラウンド認証 (EBA) を有効にする場合は、**[EBA を有効にする]** を選択します。
- HTTP 平文およびセキュアポートを指定します。デフォルト値はそれぞれ 8028 と 8030 です。
- LDAP 平文およびセキュアポートを指定します。デフォルト値はそれぞれ 389 と 636 です。

7 **[インストール場所]** フィールドで、識別ボールトがインストールされる場所を指定します。

8 **[DIB Location (DIB の場所)]** フィールドで、DIB ファイルが配置される場所を指定します。

9 **[アップグレード]** をクリックして、アップグレードプロセスを続行します。

Identity Manager エンジンのアップグレード

ドライバを停止していることを確認します。詳細については、178 ページの 「ドライバの停止」を参照してください。

Identity Manager エンジンをアップグレードするには、次の手順を実行します。

1. NetIQ ダウンロード Web サイトから Identity_Manager_4.8_Windows.iso をダウンロードします。
2. ダウンロード済みの .iso をマウントします。
3. <ISO installed location>\IdentityManagerServer フォルダに移動して、install.exe を実行します。
4. インストールで使用する言語を選択し、**[OK]** をクリックします。
5. イントロダクションページで、**[次へ]** をクリックします。
6. 使用許諾契約書の条項を確認して同意し、**[次へ]** をクリックします。

   インストールされたコンポーネントとそのバージョンが表示されます。
7. **[Identity Manager エンジン]** を選択して、**[次へ]** をクリックします。
8. Identity Manager エンジンの環境設定を指定します。詳細については、57 ページの「Identity Manager エンジンの環境設定ワークシート」を参照してください。
9. アップグレード前の概要ページで設定を確認し、**[アップグレード]** をクリックします。

MapDB 3.0.5 の使用

Identity Manager エンジンに加えて、MapDB は以下の Identity Manager ドライバによって使用されます。

- データ収集サービス
- JDBC
- LDAP
- Managed System Gateway
- Office 365 および Azure Active Directory
- Salesforce

これらのドライバのいずれかを使用している場合は、ドライバをアップグレードする前に次のセクションを確認する必要があります。

- 161 ページの「ドライババージョンに関する Identity Manager 4.8 エンジンサポートの理解」
- 161 ページの 「MapDB キャッシュファイルの手動削除」

ドライババージョンに関する Identity Manager 4.8 エンジンサポートの理解

MapDB を使用する Identity Manager ドライバをアップグレードする前に、以下の考慮事項を確認してください。

- Identity Manager 4.8 に付属のドライバは、Identity Manager 4.8 エンジンまたはリモートローダと互換性があります。特定のドライバ実装ガイドのドライバアップグレード手順に従う必要があります。
- Identity Manager 4.8 より前に出荷されたドライバは、Identity Manager 4.8 エンジンまたはリモートローダと互換性がありません。
- Identity Manager 4.8 に付属のドライバは、Identity Manager 4.7.x エンジンまたはリモートローダと後方互換性がありません。
- Identity Manager 4.8 に付属のドライバは、Identity Manager 4.6.x エンジンまたはリモートローダと後方互換性がありません。

MapDB キャッシュファイルの手動削除

Identity Manager エンジンのアップグレードプロセスでは、既存の MapDB キャッシュファイル (dx*) の一部が Identity Vault の DIB ディレクトリに残ります。ドライバのアップグレード後に、ドライバのこれらのファイルを手動で削除する必要があります。このアクションにより、ドライバが Identity Manager 4.8 エンジンで正しく動作することが保証されます。

次の表に、削除する必要がある MapDB キャッシュファイルを示します。

Identity Manager ドライバ	削除する MapDB 状態キャッシュファイル
データ収集サービス	DCSDriver_<driver instance guid>-*
	<driver instance guid>-*
JDBC	jdbc_<driver instance guid>_*
LDAP	ldap_<driver instance guid>*
Managed System Gateway	MSGW-<driver-instance-guid>.*
Office 365 および Azure Active Directory	<Azure driver name>_obj.db.*
Salesforce	<Salesforce driver name>.*
	<Salesforce driver name>

ここで、「*」は MapDB 状態キャッシュファイルの名前を表します。Salesforce ドライバの場合、MapDB 状態キャッシュファイルもドライバ名で表されます。これらのファイルの例を以下に示します。

- DCSDriver_<driver instance guid>-0.t, <driver instance guid>-1.p
- jdbc_<driver instance guid>_0.t, jdbc_<driver instance guid>_1
- ldap_<driver instance guid>b, ldap_<driver instance guid>b.p
- MSGW-<driver instance guid>.p, MSGW-<driver instance guid>.t

- <Azure driver name>_obj.db.t, <Azure driver name>_obj.db.p
- <Salesforce driver name>.p, <Salesforce driver name>.t,Salesforce driver1

リモートローダのアップグレード

リモートローダを実行している場合は、リモートローダファイルをアップグレードする必要があります。

注 : .NET リモートローダをアップグレードする前に、ご使用のシステムにすべての Windows Update が正常にインストールされていることを確認してください。

---

1. リモートローダ環境設定ファイルのバックアップを作成します。ファイルのデフォルトの場所は、C:\...\RemoteLoader*remoteloadername*-config.txt です。
2. ドライバを停止していることを確認します。手順については、『*NetIQ Identity Manager Driver Administration Guide*』の「Stopping, Starting, or Restarting a Driver in Designer」を参照してください。
3. 各ドライバのリモートローダサービスまたはデーモンを停止します。

   リモートローダコンソールで、リモートローダインスタンスを選択してから、**[停止]** をクリックします。
4. Windows タスクマネージャを使用して lcache プロセスを停止します。
5. NetIQ ダウンロード Web サイトから Identity_Manager_4.8_Windows.iso をダウンロードします。
6. ダウンロード済みの .iso をマウントします。
7. <ISO installed location>\IdentityManagerServer フォルダに移動して、install.exe を実行します。
8. インストールで使用する言語を選択し、**[OK]** をクリックします。
9. イントロダクションページで、**[次へ]** をクリックします。
10. 使用許諾契約書の条項を確認して同意し、**[次へ]** をクリックします。

    インストールされたコンポーネントとそのバージョンが表示されます。
11. **[リモートローダサービス]** を選択して、**[次へ]** をクリックします。
12. アップグレード前の概要ページで、**[アップグレード]** をクリックします。
13. アップグレードが完了したら、環境設定ファイルに現在の環境の情報が含まれていることを確認します。
14. (状況によって実行) 環境設定ファイルに問題がある場合は、手順 1 で作成したバックアップファイルをコピーします。問題がない場合は、次の手順に進んでください。
15. 各ドライバのリモートローダサービスまたはデーモンを起動します。

重要 : ドライバが MapDB を使用する場合、ドライバをアップグレードした後、ドライバの既存の MapDB 状態キャッシュファイルを手動で削除します。Identity Manager エンジンのアップグレードプロセスでは、これらのファイルのすべてが Identity Vault の DIB ディレクトリから削除されないため、この操作が必要になります。詳細については、160 ページの「MapDB 3.0.5 の使用」を参照してください。

Java リモートローダのアップグレード

1 リモートローダ環境設定ファイルのバックアップを作成します。ファイルのデフォルトの場所は、C:\...\RemoteLoader*remoteloadername*-config.txt です。

2 ドライバを停止していることを確認します。手順については、『*NetIQ Identity Manager Driver Administration Guide*』の「Stopping, Starting, or Restarting a Driver in Designer」を参照してください。

3 各ドライバのリモートローダサービスまたはデーモンを停止します。

リモートローダコンソールで、リモートローダインスタンスを選択してから、**[停止]** をクリックします。

4 Windows タスクマネージャを使用して lcache プロセスを停止します。

5 NetIQ ダウンロード Web サイトから Identity_Manager_4.8_Windows.iso をダウンロードします。

6 ダウンロード済みの .iso をマウントします。

7 <ISO installed location>\IdentityManagerServer\products\IDM\java_remoteloader フォルダに移動します。

8 既存の Java リモートローダインストール済みディレクトリにある dirxml_jremote_dev.tar.gz ファイルをコピーして置き換えます。

9 既存のセットアップに存在するファイルに基づいて、既存の Java リモートローダインストール済みディレクトリにある次のファイルのいずれかをコピーして置き換えます。

- dirxml_jremote.tar.gz
- dirxml_jremote_mvs.tar

10 手順 8 および手順 9 でコピーしたファイルを展開します。

7-zip またはサポートされているソフトウェアを使用して、.tar.gz ファイルを圧縮解除します。

11 (状況によって実行) 環境設定ファイルに問題がある場合は、手順 1 で作成したバックアップファイルをコピーします。問題がない場合は、次の手順に進んでください。

注 : version.txt ファイルを使用して、最新バージョンの Java リモートローダがあることを確認してください。

---

12 各ドライバのリモートローダサービスまたはデーモンを起動します。

iManager のアップグレード

iManager のアップグレードプロセスは、ポート値や認定されたユーザなど、configiman.properties ファイルに既存の環境設定値を使用します。iManager を 3.2 バージョンにアップグレードする前に、以下を実行することをお勧めします。

- eDirectory を 9.2 バージョンにアップグレードする。
- server.xml および context.xml の環境設定ファイルをバックアップする。

アップグレードプロセスでは、次のアクティビティを実行します。

- 164 ページの 「iManager のアップグレード」
- 164 ページの 「役割ベースサービスの更新」
- 165 ページの 「Plug-in Studio でのプラグインの再インストールまたはマイグレート」
- 166 ページの 「iManager プラグインのアップグレードまたは再インストール後のアップデート」

iManager のアップグレード

iManager をアップグレードする前に、コンピュータが前提条件とシステム要件を満たすことを確認します。

注 : アップグレードプロセスは、iManager の古いバージョンで設定されていた HTTP ポートと SSL ポートの値を使用します。

---

1. NetIQ ダウンロード Web サイトから Identity_Manager_4.8_Windows.iso をダウンロードします。
2. ダウンロード済みの .iso をマウントします。
3. <ISO installed location>\IdentityManagerServer フォルダに移動して、install.exe を実行します。
4. インストールで使用する言語を選択し、**[OK]** をクリックします。
5. イントロダクションページで、**[次へ]** をクリックします。
6. 使用許諾契約書の条項を確認して同意し、**[次へ]** をクリックします。

   インストールされたコンポーネントとそのバージョンが表示されます。
7. **[iManager Web 管理]** を選択して、**[次へ]** をクリックします。
8. iManager の設定を指定します。詳細については、57 ページの 「Identity Manager エンジンの環境設定ワークシート」を参照してください。
9. アップグレード前の概要ページで設定を確認し、**[アップグレード]** をクリックします。

役割ベースサービスの更新

iManager で使用可能な機能をすべて表示および使用できるように、RBS モジュールを最新バージョンにアップデートすることをお勧めします。

注

- iManager をアップデートまたは再インストールする場合、インストールプログラムは既存のプラグインをアップデートしません。プラグインを手動でアップデートするには、iManager を起動し、[Configure (設定)] > [Plug-in Installation (プラグインのインストール)] > [Available Novell Plug-in Modules (利用できる Novell プラグインモジュール)] の順に移動します。
- iManager の複数のインストールで、それぞれ異なる数のプラグインがローカルにインストールされている可能性があります。その結果、[Role Based Services (役割ベースサービス)] > [RBS Configuration (RBS 設定)] ページから生成する特定のコレクションのモジュールレポートに不一致が表示される可能性があります。iManager の複数のインストールの間でプラグインの数を同じにするには、ツリーの各 iManager インスタンスに同じプラグインのサブセットをインストールする必要があります。

古い RBS オブジェクトをチェックしてアップデートするには :

1 iManager にログインします。

2 ［設定］ビューで [役割ベースサービス］ > ［RBS の設定] の順に選択します。

［2.*x* Collections (2.x コレクション)］タブページの表で古いモジュールをレビューします。

3 モジュールをアップデートするには、次の手順を実行します。

3a アップデートするコレクションの [Out-Of-Date ()] 列の数値をクリックします。

古いモジュールのリストが表示されます。

3b アップデートするモジュールを選択します。

3c 表の上部にある [Update (アップデート)] をクリックします。

Plug-in Studio でのプラグインの再インストールまたはマイグレート

［Plug-in Studio (Plug-in Studio)］でプラグインを別の iManager インスタンスまたは iManager の新しいバージョンまたはアップデートされたバージョンにマイグレートまたは複製できます。

1 iManager にログインします。

2 iManager の［Configure (設定)］ビューで、[Role Based Services (役割ベースサービス)]>［Plug-in Studio (Plug-in Studio)］の順に選択します。

コンテンツフレームには、プラグインが属する RBS コレクションの場所を含む、インストールされたカスタムプラグインのリストが表示されます。

3 再インストールまたはマイグレートするプラグインを選択し、[Edit (編集)] をクリックします。

注 : 編集できるプラグインは一度に 1 つだけです。

4 [インストール] をクリックします。

5 再インストールまたはマイグレートする必要があるプラグインごとに、これらの手順を繰り返します。

iManager プラグインのアップグレードまたは再インストール後のアップデート

iManager をアップグレードするか、または再インストールする際に、インストールプロセスは既存のプラグインをアップデートしません。プラグインが正しい iManager バージョンに一致していることを確認します。

注 : これは、Open Enterprise Server 2018 で iManager から Identity Manager プラグインを更新する唯一の方法です。

---

1. iManager を開きます。
2. **[Configure (設定)]** > **[Plug-in Installation (プラグインのインストール)]** > **[Available Novell Plug-in Modules (利用できる Novell プラグインモジュール)]** の順に移動します。
3. プラグインをアップデートします。

Identity Applications のアップグレード

このセクションでは、次のコンポーネントの更新を含む、Identity Applications およびサポートするソフトウェアのアップグレードについて説明します。

- Identity Manager ユーザアプリケーション
- OSP (One SSO Provider)
- Self-Service Password Reset (SSPR)
- Tomcat、JDK、および ActiveMQ

アップグレード後は、コンポーネントが次のバージョンにアップグレードされます。

- Tomcat – 8.5.40
- ActiveMQ – 5.15.9
- Java 8 Update 222
- One SSO Provider – 6.3.4
- セルフサービスパスワードリセット – 4.4.0.3
- Identity Applications – 4.8
- Identity Reporting – 6.5

このセクションでは、次のトピックについて説明します。

- 167 ページの 「アップグレードプログラムについて」
- 167 ページの 「アップグレードの前提条件」
- 167 ページの 「システム要件」
- 167 ページの 「PostgreSQL データベースのアップグレード」
- 170 ページの 「Identity Applications のドライバパッケージのアップグレード」

- 170 ページの 「Identity Applications のアップグレード」
- 171 ページの 「アップグレード後のタスク」

アップグレードプログラムについて

アップグレードプロセスは、既存のコンポーネントから設定値を読み込みます。この情報には、ism-configuration.properties、server.xml、SSPRConfiguration.xml、および他の設定ファイルが含まれます。これらの設定ファイルを使用して、アップグレードプロセスにより、コンポーネントのアップグレードプログラムが内部的に起動します。また、このプログラムは現在のインストールのバックアップも作成します。

アップグレードの前提条件

データベースが SSL 経由で設定されている場合は、C:\NetIQ\idm\apps\tomcat\conf にあるパスから取得される server.xml ファイルで ssl=true を sslmode=require に置き換えます。

たとえば、次のように変更します。

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

変更先 :

```
jdbc:postgresql://<postgres db>:5432/idmuserappdb?sslmode=require
```

システム要件

アップグレードプロセスにより、インストールされたコンポーネントの現在の設定のバックアップが作成されます。ご使用のサーバにバックアップを格納するための十分な容量と、アップグレードに使用可能な追加の空き容量があることを確認します。

PostgreSQL データベースのアップグレード

重要 : アップグレードプロセスは、データベースのサイズによって時間がかかる場合があります。したがって、それに応じてアップグレードを計画してください。

1. サーバ上で実行されている PostgreSQL サービスを停止します。
2. C:\Netiq\idm\apps の postgres ディレクトリの名前を変更します。

   たとえば、postgres の名前を postgresql_old に変更します。
3. 次のコマンドを実行して、古いサービスを削除します。

   sc delete <postgres service name>
4. ご使用のオペレーティングシステムでサポートされている PortgreSQL バージョンをインストールします。

PostgreSQL の現在のインストール場所以外を選択する必要があります。

4a Identity_Manager_4.8_Windows.iso イメージファイルをマウントし、\common\postgres_tomcat ディレクトリに移動します。

4b TomcatPostgreSQL.exe ファイルを実行します。

インストール中に **[PostgreSQL]** オプションのみを選択します。

注

- **[PostgreSQL の詳細]** ページにデータベース詳細を入力しないでください。**[データベースログインアカウントの作成]** および **[空のデータベースの作成]** の選択が解除されていることを確認します。
- 古いおよび新しいPostgreSQLインストールディレクトリの管理者権限があることを確認します。

---

5 新たにインストールされた PostgreSQL サービスを停止します。**[サービス]** に移動し、*<PostgreSQL version number>* サービスを検索して、サービスを停止します。

注 : 適切な権限を持つユーザは、有効な認証情報を入力した後で、停止操作を実行できます。

---

6 次のアクションを実行して、新たにインストールされた PostgreSQL ディレクトリの許可を変更します。

postgres ユーザを作成します。

1. **[コントロールパネル］ > ［ユーザアカウント］ > ［ユーザアカウント］ > ［アカウントの管理]** の順に移動します。
2. **[ユーザアカウントの追加]** をクリックします。
3. ［ユーザの追加］ページで、ユーザ名として postgres を指定し、そのユーザのパスワードを入力します。

postgres ユーザに、既存の PostgreSQL ディレクトリおよび新たにインストールされた PostgreSQL ディレクトリへの許可を付与します。

1. PostgreSQL ディレクトリを右クリックして、**[プロパティ］ > ［セキュリティ］ > ［編集]** の順に移動します。
2. ユーザに完全な許可を付与するには、**[フルコントロール]** を選択します。
3. **[適用]** をクリックします。

7 postgres ユーザとして PostgreSQL ディレクトリにアクセスします。

1. サーバに postgres ユーザとしてログインします。

   ログインする前に、このユーザに対してリモート接続が許可されているかどうかを確認することで、postgres が Windows サーバに接続できることを確認します。
2. 新しい postgres インストールの場所からデータディレクトリを削除します。たとえば、C:\NetIQ\idm\apps\postgres\data
3. コマンドプロンプトを開き、次のコマンドを使用して、PGPASSWORD を設定します。

```
set PGPASSWORD=<your pg password>
```

4. 新たにインストールされた PostgreSQL ディレクトリに移動します。
5. initdb を postgres データベースユーザとして実行します。

   initdb.exe -D <new_data_directory> -E UTF8 -U postgres

   次に例を示します。

   initdb.exe -D C:\NetIQ\idm\apps\postgres\data -E UTF8 -U postgres

8 新しい PostgreSQL bin ディレクトリから PostgreSQL をアップグレードします。次のコマンドを実行して、**[Enter]** をクリックします。

注 : **[Method]** タイプを C:\NetIQ\idm\apps\postgres\data\ ディレクトリにある pg_hba.conf で、md5 から trust に設定していることを確認します。

```
pg_upgrade.exe --old-datadir "C:\NetIQ\idm\apps1\postgres\data" --new-
datadir "C:\NetIQ\idm\apps1\postgresql962\data" --old-bindir
"C:\NetIQ\idm\apps1\postgres\bin" --new-bindir
"C:\NetIQ\idm\apps1\postgresql962\bin"
```

9 アップグレード後に、新しい postgres データディレクトリ (C:\NetIQ\idm\apps\postgres\data) にある pg_hba.conf と postgresql.conf ファイルを古い postgres ディレクトリからのファイルと置き換えます。

10 アップグレードされた PostgreSQL データベースサービスを開始します。

[サービス] に移動し、*<PostgreSQL version number>* サービスを検索して、サービスを開始します。

注 : 適切な権限を持つユーザは、有効な認証情報を入力した後で、開始操作を実行できます。

---

11 古い PostgreSQL サービスを無効にして、そのサービスが自動的に開始されないようにします。

12 (オプション) 新たにインストールされた PostgreSQL サービスの bin ディレクトリから古いデータファイルを削除します。

1. postgres ユーザとしてログインします。
2. bin ディレクトリに移動し、analyze_new_cluster.bat および delete_old_cluster.bat ファイルを実行します。

   たとえば、C:\NetIQ\idm\apps\postgresql\bin です。

注 : この手順は、古いデータファイルを削除する場合にのみ実行する必要があります。

Identity Applications のドライバパッケージのアップグレード

Tomcat を停止し、ユーザアプリケーションドライバ、役割およびリソースサービスドライバのパッケージを最新バージョンに更新する必要があります。パッケージを最新バージョンにアップグレードする方法については、『*NetIQ Designer for Identity Manager Administration Guide*』の「Upgrading Installed Packages」を参照してください。

ユーザアプリケーションドライバパッケージをアップグレードした後、ワークフローテンプレートパッケージを手動で追加する必要があります。

1 Designer で、[ユーザアプリケーションドライバ] > [プロパティ] に移動します。
2 ［パッケージ］をクリックして、➕をクリックします。
3 [ワークフローテンプレートの作成] を選択します。
4 [OK] をクリックしてから、[完了] をクリックしてインストールを完了します。
5 ユーザアプリケーションドライバを展開します。

重要 : ユーザアプリケーションドライバのアップグレードの一環として、電子メール通知テンプレートがインストールまたはアップグレードされる場合は、[デフォルトの通知コレクション] オブジェクトを展開する必要があります。

Identity Applications のアップグレード

以下の手順では、次のコンポーネントをアップグレードする方法について説明します。

- 識別情報アプリケーション
- OSP
- Tomcat
- PostgreSQL
- SSPR (Identity Applications と同じコンピュータにインストールされている場合)
- ActiveMQ

Identity Applications をアップグレードするには次の手順を実行します。

1 NetIQ ダウンロード Web サイトから Identity_Manager_4.8_Windows.iso をダウンロードします。
2 ダウンロード済みの .iso をマウントします。
3 <ISO installed location>\IdentityApplications フォルダに移動して、install.exe を実行します。
4 インストールで使用する言語を選択し、[OK] をクリックします。
5 イントロダクションページで、[次へ] をクリックします。
6 使用許諾契約書の条項を確認して同意し、[次へ] をクリックします。
インストールされたコンポーネントとそのバージョンが表示されます。
7 [Identity Applications] を選択して、[次へ] をクリックします。

8 Identity Applications の環境設定を指定します。詳細については、59 ページの 「Identity Applications の環境設定ワークシート」を参照してください。

注

- NetIQ では、Identity Applications と同じサーバ上に PostgreSQL データベースをインストールしている場合は、Identity Manager インストーラを使用してワークフローデータベースを作成することをお勧めします。
- アップグレード時に、データベース JDBC JAR ファイルを手動で指定する必要があります。たとえば、PostgreSQL データベースを使用している場合は、tomcat\lib フォルダ外にあるデータベース JAR ファイルの場所を指定する必要があります。

9 アップグレード前の概要ページで設定を確認し、[アップグレード] をクリックします。

コンポーネントをインストールした場所に応じて、プロセスによりその場所にバックアップディレクトリが作成され、バックアップしたディレクトリに (バックアップの時間を示す) タイムスタンプが付加されます。

次に例を示します。

- Tomcat – C:\NetIQ\idm\apps\tomcat_backup_02262018_033634
- OSP および SSPR - C:\NetIQ\idm\apps\osp_sspr_backup_02262018_033634
- ActiveMQ - C:\NetIQ\idm\apps\activemq_backup_02262018_033634
- ユーザアプリケーション - C:\NetIQ\idm\apps\UserApplication_backup_02262018_033634
- Identity Reporting - C:\NetIQ\idm\apps\IdentityReporting_backup_02262018_033634

アップグレード後のタスク

異なるサーバ上に Identity Applications と SSPR をインストールしている場合は、Identity Applications サーバの cacerts に Identity Applications として CN による SSPR トラステッド証明書をインポートする必要があります。

Tomcat、SSPR、OSP、または Identity Applications のカスタマイズされた設定を手動で復元する必要もあります。

必要なコンポーネントについてアップグレード後の手順を実行します。

- 172 ページの 「Java」
- 172 ページの 「Tomcat」
- 173 ページの 「識別情報アプリケーション」
- 174 ページの 「One SSO Provider」
- 174 ページの 「Self-Service Password Reset」
- 175 ページの 「Kerberos」

Java

新しい JRE のアップグレード場所にある証明書 (jre\lib\security\cacerts) を古い JRE の場所を使用して確認します。証明書がない場合は、cacerts に手動でインポートします。

1 keytool コマンドを使用して、java cacerts をインポートします。

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

注 : アップグレード後、JRE はアイデンティティアプリケーションのインストール場所に保存されます。たとえば、C:\NetIQ\idm\apps\jre です。

---

2 アイデンティティボールトを再起動します。

3 JRE ホームの場所が tomcat\bin\setenv.bat であることを確認します。

4 **[設定更新]** ユーティリティを起動し、cacerts のパスを確認します。

Tomcat

1 (状況によって実行) アップグレードプロセスによって前に作成されたバックアップからカスタマイズされたファイルを復元するには、次のタスクを実行します。

- カスタマイズされた HTTPS 証明書を復元します。これらの証明書を復元するには、バックアップした server.xml から \tomcat\conf ディレクトリの新しい server.xml ファイルに Java Secure Socket Extension (JSSE) のコンテンツをコピーします。
- バックアップした Tomcat ディレクトリから新しい Tomcat ディレクトリに設定ファイルをコピーしないでください。新しいバージョンのデフォルトの設定から開始し、必要に応じて変更します。詳細については、Apache の Web サイトを参照してください。

  新しい server.xml ファイルに、次のエントリがあることを確認します。

```
<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"/>
 -->
```

  または

```
<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"/>
 -->
```

注 : クラスタ環境で、server.xml の Cluster タグを手動でコメント解除して、C:\netiq\idm\apps\osp_backup_<date> にある最初のノードからすべてのノードに osp.jks をコピーします。

- カスタマイズしたキーストアファイルがある場合は、新しい server.xml ファイルに正しいパスを含めてください。
- Identity Applications の証明書を、C:\NetIQ\eDirectory\jre\lib\security\cacerts にあるアイデンティティボールトにインポートします。

  たとえば、次の keytool コマンドを使用して、証明書をアイデンティティボールトにインポートすることができます。

  ```
  keytool -importkeystore -alias <User Application certificate alias>
  -srckeystore <backup cacert> -srcstorepass changeit -destkeystore
  C:\NetIQ\eDirectory\jre\lib\security\cacerts
  ```

2 (状況によって実行) ユーザアプリケーションに移動し、バックアップした設定を読み取ることにより、カスタマイズされた設定を手動で復元します。

識別情報アプリケーション

Identity Applications を 4.6 SP4 から 4.8 にアップグレードしているときに、Dcom.novell.afw.wf.engine-id=IDMProv パラーメータが tomcat/bin フォルダ内の setenv ファイルに存在していることを確認する必要があります。Identity Applications のアップグレード後にこのパラメータがなくなる場合は、setenv ファイルにパラメータを手動で追加して、Tomcat サーバを再起動します。

One SSO Provider

デフォルトでは、logevent.conf ファイルにある LogHost エントリは、localhost に設定されています。

LogHost エントリを変更するには、アップグレードプロセス時に作成したバックアップからカスタマイズされた OSP 設定を手動で復元します。

Self-Service Password Reset

SSPR をアップグレードした後で、設定更新ユーティリティを使用して SSO クライアントパラメータを更新します。詳細については、97 ページの 「SSO Clients Parameters (SSO クライアントパラメータ)」を参照してください。

SSPR 設定の詳細を更新するには、次の手順を実行します。

1 SSPR ポータルに管理者としてログインします。

2 監査サーバの詳細を更新するには、次の手順を実行します。

2a **[YourID] > [Configuration Editor (環境設定エディタ)]** の順に移動して、設定パスワードを指定します。

2b **[設定] > [Auditing] > [Audit Forwarding] > [Syslog Audit Server Certificates]** の順に選択します。

2c サーバからこれらの証明書をインポートして、**[保存]** をクリックします。

3 SSPR に **[LocalDB]** をインポートします。

3a ドロップダウンメニューから **[YourID] > [Configuration Manager (環境設定マネージャ)]** の順に移動します。

3b **[LocalDB]** をクリックします。

3c **[Import (Upload) LocalDB Archive File (LocalDB アーカイブファイルのインポート (アップロード))]** をクリックします。

4 (状況によって実行) SSPR の設定を制限するには :

4a リストから **[YourID] > [Configuration Manager (環境設定マネージャ)]** の順に移動します。

4b **[Restrict Configuration (設定の制限)]** をクリックします。

5 SSPR の管理者許可を設定します。65 ページの 「インストール後の手順」を参照してください。

アップグレードが正常に完了したことを確認するには、アップグレードしたコンポーネントを起動します。

たとえば、Identity Manager ダッシュボードを起動し、**[バージョン情報]** をクリックします。アプリケーションが **[4.8.0]** などの新しいバージョンを示しているかどうかを確認します。

Kerberos

アップグレードユーティリティにより、コンピュータ上に新しい Tomcat フォルダが作成されます。keytab や Kerberos_login.config などの Kerberos ファイルが古い Tomcat フォルダ上にある場合は、バックアップしたフォルダから新しい Tomcat フォルダにこれらのファイルをコピーします。

Identity Reporting のアップグレード

Identity Reporting には 2 つのドライバが含まれます。また、NetIQ Event Auditing Service から Sentinel Log Management for IGA にコンテンツを移行する必要がある場合があります。アップグレードは次の順序で実行します。

1. Sentinel Log Management for IGA をアップグレードします。詳細については、『NetIQ Identity Manager Setup Guide for Linux』の「Upgrading Sentinel Log Management for IGA」を参照してください。
2. Identity Reporting をアップグレードします。

アップグレードの前提条件

データベースが SSL 経由で設定されている場合は、C:\NetIQ\idm\apps\tomcat\conf にあるパスから取得される server.xml ファイルで ssl=true を sslmode=require に置き換えます。

たとえば、次のように変更します。

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

変更先 :

```
jdbc:postgresql://<postgres db>:5432/idmrptdb?sslmode=require
```

Identity Reporting のアップグレード

Identity Reporting をアップグレードする前に、Identity Applications と SLM for IGA をアップグレードする必要があります。Identity Reporting をアップグレードするには、古いバージョンの上に新しいバージョンをインストールします。

Identity Reporting をアップグレードするには次の手順を実行します。

1. NetIQ ダウンロード Web サイトから Identity_Manager_4.8_Windows.iso をダウンロードします。
2. ダウンロード済みの .iso をマウントします。
3. <ISO installed location>\IdentityReporting フォルダに移動して、install.exe を実行します。
4. インストールで使用する言語を選択し、[OK] をクリックします。
5. イントロダクションページで、[次へ] をクリックします。
6. 使用許諾契約書の条項を確認して同意し、[次へ] をクリックします。

   インストールされたコンポーネントとそのバージョンが表示されます。

7 [Identity Reporting] を選択して、[次へ] をクリックします。

8 Identity Reporting の環境設定を指定します。詳細については、61 ページの 「Identity Reporting の環境設定ワークシート」 を参照してください。

9 アップグレード前の概要ページで設定を確認し、[アップグレード] をクリックします。

注 : ism-configuration.properties ファイルの com.netiq.rpt.ssl-keystore.type プロパティはアップグレード前に設定された値 (JKS/PKCS12) を保持します。

Reporting のアップグレード後の手順

Identity Reporting を 4.8 にアップグレードした後で、/opt/netiq/idm/apps/tomcat/conf/ ディレクトリにある ism-configuration.properties ファイルに移動し、次のアクションを実行します。

- com.netiq.rpt.landing.url プロパティの値を次のように変更します。

  com.netiq.rpt.landing.url = ${com.netiq.idm.osp.url.host}/idmdash/#/landing

- com.netiq.idmdcs.landing.url プロパティの値を次のように変更します。

  com.netiq.idmdcs.landing.url = ${com.netiq.idm.osp.url.host}/idmdash/#/landing

- 次の形式で com.netiq.rpt.redirect.url プロパティの値を指定します。https:<hostname>:<port>/path

  例 : com.netiq.rpt.redirect.url = https://192.168.0.1:8543/IDMRPT/oauth.html

データベースにおける reportRunner への参照の変更

Identity Reporting をアップグレードした後、および Tomcat を初めて起動する前に、データベースの reportRunner への参照を更新していることを確認してください。

1 Tomcat を停止します。

2 Identity Reporting インストールディレクトリに移動し、reportContent フォルダを ORG-reportContent に名前を変更します。

  例 : C:\NetIQ\idm\apps\IdentityReporting

3 Tomcat フォルダの下にある一時および作業ディレクトリを削除します。

4 PostgreSQL データベースにログインします。

  4a 次のテーブルにある reportRunner 参照を検索します。

  - idm_rpt_cfg.idmrpt_rpt_params
  - idm_rpt_cfg.idmrpt_definition

  4b 次の delete ステートメントを発行します。

```
DELETE FROM idm_rpt_cfg.idmrpt_rpt_params WHERE
rpt_def_id='com.novell.content.reportRunner';

DELETE FROM idm_rpt_cfg.idmrpt_definition WHERE
def_id='com.novell.content.reportRunner';
```

5 Tomcat を起動します。

ログをチェックして、レポートが正しい reportRunner で再生成されているかどうか確認します。

6 Identity Reporting にログインしてレポートを実行します。

Identity Reporting のアップグレードの検証

1 Identity Reporting を起動します。

2 ツールで古いレポートと新しいレポートが表示されることを検証します。

3 **[カレンダ]** を参照し、スケジュールされたレポートが表示されるかどうかを確認します。

4 **[設定]** ページに管理対象アプリケーションと管理対象外アプリケーションの設定が表示されることを確認します。

5 他の設定がすべて正しく見えることを検証します。

6 完了したレポートがリストに表示されるかどうかを検証します。

Analyzer のアップグレード

Analyzer をアップグレードするために、NetIQ はパッチファイルを .zip 形式で提供しています。Analyzer をアップグレードする前に、コンピュータが前提条件とシステム要件を満たすことを確認します。詳細については、アップデートのリリースノートを参照してください。

1 NetIQ ダウンロード Web サイトから Identity_Manager_4.8_Analyzer_Windows などのパッチファイルをダウンロードします。

2 この .zip ファイルを Analyzer インストールファイル (プラグイン、アンインストールスクリプト、および他の Analyzer ファイルなど) が置かれているディレクトリに展開します。

3 Analyzer を再起動します。

4 新しいパッチの適用に成功したことを検証するために、次の手順を実行します。

4a Analyzer を起動します。

4b **[ヘルプ］ >［About Analyzer (バージョン情報)]** の順にクリックします。

4c 新しいバージョン (たとえば **[4.6 Update 1]**) とビルド ID(たとえば **[20121128]**) が表示されるかどうかをチェックします。

Identity Manager ドライバの停止と起動

アップグレードプロセスやインストールプロセスで正しいファイルを変更または置換できるようにするには、Identity Manager ドライバを起動または停止しなければならない場合があります。このセクションでは、次の操作について説明します。

- 178 ページの 「ドライバの停止」
- 179 ページの 「ドライバの起動」

ドライバの停止

ドライバのファイルを変更する場合、あらかじめドライバを停止しておくことが重要です。

- 178 ページの 「Designer を使用したドライバの停止」
- 178 ページの 「iManager を使用したドライバの停止」

Designer を使用したドライバの停止

1 Designer で、識別ボールトのオブジェクトを [アウトライン] タブで選択します。

2 モデラーツールバーで、[すべてのドライバを停止] アイコンをクリックします。

これにより、プロジェクトの一部であるすべてのドライバが停止します。

3 ドライバを手動開始に設定すると、アップグレードプロセスを完了しない限りドライバは開始されません。

3a [アウトライン] タブの［ドライバ］アイコンをダブルクリックします。

3b [ドライバ環境設定］ >［起動時のオプション] の順に選択します。

3c [手動] を選択し、[OK] をクリックします。

3d 各ドライバに対して、ステップ 3a ～ステップ 3c を繰り返します。

iManager を使用したドライバの停止

1 iManager で、[Identity Manager］ >［Identity Manager の概要] の順に選択します。

2 ツリーでその場所を参照して選択し、ドライバセットオブジェクトを検索してから、［検索］アイコンをクリックします。

3 ドライバセットオブジェクトをクリックします。

4 [ドライバ］ >［すべてのドライバを停止] の順にクリックします。

5 各ドライバセットオブジェクトに対して、ステップ 2 ～ステップ 4 を繰り返します。

6 ドライバを手動開始に設定すると、アップグレードプロセスを完了しない限りドライバは開始されません。

6a iManager で、[Identity Manager］ >［Identity Manager の概要] の順に選択します。

6b ツリーでその場所を参照して選択し、ドライバセットオブジェクトを検索してから、［検索］アイコンをクリックします。

6c ドライバセットオブジェクトをクリックします。

6d ドライバアイコンの右上隅をクリックし、[プロパティの編集] をクリックします。

6e［ドライバ環境設定］ページの [起動時のオプション] で [手動] を選択し、[OK] をクリックします。

6f ツリーの各ドライバに対して、ステップ 6a ～ステップ 6e を繰り返します。

ドライバの起動

Identity Manager コンポーネントがすべてアップデートされたら、ドライバを再起動します。ドライバが実行状態になったら、ドライバをテストして、すべてのポリシーが依然と同様に機能していることを確認することをお勧めします。

- 179 ページの 「Designer を使用したドライバの起動」
- 179 ページの 「iManager を使用したドライバの起動」

Designer を使用したドライバの起動

1 Designer で、識別ボールトのオブジェクトを [アウトライン] タブで選択します。

2 モデラーツールバーの [すべてのドライバを起動] アイコン をクリックします。これにより、プロジェクト内のすべてのドライバが起動されます。

3 ドライバ起動オプションを設定します。

3a [アウトライン] タブの［ドライバ］アイコン をダブルクリックします。

3b [ドライバ環境設定］ >［起動時のオプション] を選択します。

3c [自動開始] を選択するか、ドライバの起動方法を選択し、[OK] をクリックします。

3d 各ドライバに対して、ステップ 3a ～ステップ 3c を繰り返します。

4 ドライバをテストして、ポリシーが設計どおりに機能していることを確認します。ポリシーのテスト方法の詳細については、『*NetIQ Identity Manager - Using Designer to Create Policies*』の「ポリシーシミュレータを使用したポリシーのテスト」を参照してください。

iManager を使用したドライバの起動

1 iManager で、[Identity Manager］ >［Identity Manager の概要] の順に選択します。

2 ツリーでその場所を参照して選択し、ドライバセットオブジェクトを検索してから、［検索］アイコン をクリックします。

3 ドライバセットオブジェクトをクリックします。

4 [ドライバ］ >［すべてのドライバを起動] の順にクリックして、すべてのドライバを同時に起動します。

または

［ドライバ］アイコンの右上部分で、[ドライバの起動] をクリックして、各ドライバを別々に起動します。

5 ドライバが複数ある場合、ステップ 2 ～ステップ 4 の手順を繰り返します。

6 ドライバ起動オプションを設定します。

6a iManager で、[Identity Manager] > [Identity Manager の概要] の順に選択します。

6b ツリーでその場所を参照して選択し、ドライバセットオブジェクトを検索してから、[検索] アイコン をクリックします。

6c ドライバセットオブジェクトをクリックします。

6d ドライバアイコンの右上隅をクリックし、[プロパティの編集] をクリックします。

6e [ドライバ設定] ページの [起動オプション] で、[自動開始] またはドライバの起動方法を選択し、[OK] をクリックします。

6f 各ドライバに対して、ステップ 6b ～ステップ 6e を繰り返します。

7 ドライバをテストして、ポリシーが設計どおりに機能していることを確認します。

iManager にはポリシーシミュレータはありません。ポリシーをテストするには、ポリシーを実行するイベントを発生させます。たとえば、ユーザの作成、ユーザの変更、またはユーザの削除などです。

Identity Manager ドライバのアップグレード

新しいドライバの内容は、ドライバ環境設定ファイルではなく、「パッケージ」を使用して提供されます。パッケージの管理、保守、および作成には、Designer を使用します。iManager はパッケージに対応していますが、Designer はユーザが iManager で変更したドライバの内容を保持しません。パッケージ管理の詳細については、『*NetIQ Designer for Identity Manager Administration Guide*』の「Understanding Packages」を参照してください。

ドライバをパッケージにアップグレードするには、次の手順を実行します。

- 180 ページの 「新しいドライバの作成」
- 181 ページの 「既存のコンテンツをパッケージのコンテンツと交換」
- 181 ページの 「現在のコンテンツを維持しつつパッケージを使用する新しいコンテンツを追加」

重要 : ドライバが MapDB を使用する場合、ドライバをアップグレードした後、ドライバの既存の MapDB 状態キャッシュファイルを手動で削除します。Identity Manager エンジンのアップグレードプロセスではこれらのファイルのすべてが消去されないため、この操作が必要になります。詳細については、160 ページの 「MapDB 3.0.5 の使用」 を参照してください。

新しいドライバの作成

ドライバをパッケージにアップグレードする最も簡単な方法は、既存のドライバを削除し、パッケージを使用して新しいドライバを作成する方法です。新しいドライバに必要なすべての機能を追加します。手順はドライバごとに異なります。手順については、Identity

Manager ドライバマニュアルの Web サイトで個別のドライバガイドを参照してください。ドライバは以前と同様に機能しますが、ドライバの環境設定ファイルのコンテンツの代わりにパッケージのコンテンツを使用するようになります。

既存のコンテンツをパッケージのコンテンツと交換

ドライバによって作成された関連付けを維持する必要がある場合、ドライバを削除して再作成する必要はありません。関連付けを維持したまま、ドライバのコンテンツをパッケージで置き換えることができます。

パッケージからのコンテンツで既存のコンテンツを置き換えるには

1. ドライバおよびドライバに含まれるカスタマイズされたすべてのコンテンツのバックアップを作成します。

   方法については、155 ページの 「ドライバの環境設定のエクスポート」を参照してください。

2. Designer で、ドライバ内に保存されているすべてのオブジェクトを削除します。ドライバ内部に保存されているポリシー、フィルタ、エンタイトルメント、および他のすべての項目を削除します。

   注 : Designer には、最新のパッケージをインポートする自動インポート機能があります。ドライバパッケージをパッケージカタログに手動でインポートする必要はありません。

   詳細については、『*NetIQ Designer for Identity Manager Administration Guide*』の「パッケージカタログへのカタログのインポート」を参照してください。

   ---

3. 最新のパッケージをドライバにインストールします。

   これらの手順は各ドライバに固有です。手順については、Identity Manager ドライバマニュアルの Web サイトで個別のドライバガイドを参照してください。

4. カスタムポリシーとルールがある場合はドライバに復元します。方法については、184 ページの 「ドライバへのカスタムポリシーとルールの復元」を参照してください。

現在のコンテンツを維持しつつパッケージを使用する新しいコンテンツを追加

パッケージに含まれる機能が、ドライバの現在の機能と重複しない限り、現在の状態のままドライバを維持しつつ、パッケージを使用して新しい機能を追加できます。

パッケージをインストールする前に、ドライバ環境設定ファイルのバックアップを作成します。パッケージをインストールすると、パッケージが既存のポリシーを上書きし、ドライバが動作を停止する可能性があります。ポリシーが上書きされた場合、バックアップのドライバ環境設定ファイルをインポートして、ポリシーを再作成できます。

開始前に、カスタマイズされたポリシーに、デフォルトのポリシーと異なるポリシー名が付いていることを確認します。ドライバ環境設定が新しいドライバファイルでオーバーレイされると、既存のポリシーは常に上書きされます。一意の名前が付けられていないカスタムポリシーは失われます。

パッケージを使用してドライバに新しいコンテンツを追加するには

1 ドライバおよびドライバに含まれるカスタマイズされたすべてのコンテンツのバックアップを作成します。

方法については、155 ページの 「ドライバの環境設定のエクスポート」を参照してください。

注 : Designer には、最新のパッケージをインポートする自動インポート機能があります。ドライバパッケージをパッケージカタログに手動でインポートする必要はありません。

詳細については、『*NetIQ Designer for Identity Manager Administration Guide*』の「パッケージカタログへのカタログのインポート」を参照してください。

---

2 ドライバにパッケージをインストールします。

手順については、Identity Manager ドライバマニュアルの Web サイトで個別のドライバガイドを参照してください。

3 ドライバに必要なパッケージを追加します。これらの手順は各ドライバに固有です。

詳細については、Identity Manager ドライバマニュアルの Web サイトを参照してください。

ドライバには、パッケージによって追加された新しい機能が含まれます。

新しいサーバをドライバセットに追加する

Identity Manager を新しいサーバにアップグレードまたはマイグレートする場合、ドライバセット情報をアップデートする必要があります。このセクションでは、このプロセスについて説明します。Designer または iManager を使用してドライバセットをアップデートできます。

新しいサーバをドライバセットに追加する

iManager を使用している場合には、新しいサーバをドライバセットに追加する必要があります。Designer には、この手順を実行するサーバ用のマイグレーションウィザードが含まれています。Designer を使用している場合には、195 ページの 「Designer でサーバ固有の情報をコピーする」にスキップしてください。iManager を使用している場合には、以下の手順を実行します。

1 iManager で、 をクリックして、［Identity Manager の管理］ページを表示します。

2 **[Identity Manager の概要]** をクリックします。

3 ドライバセットを含んでいるコンテナをブラウズして、選択します。

4 ドライバセット名をクリックして、［ドライバセットの概要］ページにアクセスします。

5 **[サーバ］ > ［サーバの追加]** をクリックします。

6 新しい Identity Manager サーバを参照して選択し、**[OK]** をクリックします。

ドライバセットから古いサーバを削除する

新しいサーバがすべてのドライバを実行した後、ドライバセットから古いサーバを削除できます。

- 183 ページの 「Designer を使用してドライバセットから古いサーバを削除する」
- 183 ページの 「iManager を使用してドライバセットから古いサーバを削除する」
- 183 ページの 「古いサーバの退役」

Designer を使用してドライバセットから古いサーバを削除する

1. Designer で、プロジェクトを開きます。
2. Modeler で、ドライバセットを右クリックし、[プロパティ] を選択します。
3. [サーバリスト] を選択します。
4. [Selected Servers (選択したサーバ)] リストで古い Identity Manager サーバを選択し、[<] をクリックして、[Selected Servers (選択したサーバ)] リストからサーバを削除します。
5. [OK] をクリックし、変更を保存します。
6. 識別ボールトに変更を展開します。

   詳細については、『*NetIQ Designer for Identity Manager Administration Guide*』の「識別ボールトへのドライバセットの展開」を参照してください。

iManager を使用してドライバセットから古いサーバを削除する

1. iManager で、 をクリックして、［Identity Manager の管理］ページを表示します。
2. [Identity Manager の概要] をクリックします。
3. ドライバセットを含んでいるコンテナをブラウズして、選択します。
4. ドライバセット名をクリックして、［ドライバセットの概要］ページにアクセスします。
5. [サーバ］ > ［サーバの削除] をクリックします。
6. 古い Identity Manager サーバを選択して、[OK] をクリックします。

古いサーバの退役

この時点で、古いサーバがホストしているドライバはありません。このサーバが必要でなくなった場合は、追加の手順を実行し、サーバを廃止する必要があります。

1. このサーバから eDirectory のレプリカを削除します。

   詳細については、『*NetIQ eDirectory Administration Guide*』の「レプリカの削除」を参照してください。
2. このサーバから eDirectory を削除します。

   詳細については、TID 10056593, “Removing a Server From an NDS Tree Permanently” を参照してください。

ドライバへのカスタムポリシーとルールの復元

ドライバの新しいパッケージをインストールまたはアップグレードした後、新しいドライバ環境設定ファイルをオーバーレイした後にカスタムポリシーとルールを復元する必要があります。これらのポリシーに別の名前が付いている場合、ポリシーはドライバ内にそのまま保存されていますが、リンクが壊れているので、再設定する必要があります。

- 184 ページの 「Designer を使用したドライバへのカスタムポリシーとルールの復元」
- 185 ページの 「iManager を使用したドライバへのカスタムポリシーおよびルールの復元」

Designer を使用したドライバへのカスタムポリシーとルールの復元

ポリシーセットにポリシーを追加できます。この手順は、アップグレードしたドライバを運用環境に移動する前に、テスト環境で実行する必要があります。

1. [アウトライン] ビューで、アップグレードしたドライバを選択してから、[ポリシーフローの表示] アイコン をクリックします。
2. カスタマイズしたポリシーをドライバに復元する必要があるポリシーセットを右クリックして、[ポリシーの追加] > [既存の項目をコピー] の順に選択します。
3. カスタマイズしたポリシーを参照して選択し、[OK] をクリックします。
4. カスタマイズしたポリシーの名前を指定し、[OK] をクリックします。
5. ファイルの競合を示すメッセージが表示されたら、[はい] をクリックしてプロジェクトを保存します。
6. ポリシービルダでポリシーが開いたら、コピーしたポリシーの情報が正しいことを確認します。
7. ドライバに復元する必要があるカスタマイズした各ポリシーに対して、ステップ 2 ～ ステップ 6 を繰り返します。
8. ドライバを起動してテストします。

   ドライバの起動の詳細については、『*NetIQ Identity Manager Driver Administration Guide*』の「Stopping, Starting, or Restarting a Driver in Designer」を参照してください。ドライバのテストの詳細については、『*NetIQ Identity Manager - Using Designer to Create Policies*』の「ポリシーシミュレータを使用したポリシーのテスト」を参照してください。
9. ポリシーが動作することを確認したら、ドライバを運用環境に移します。

iManager を使用したドライバへのカスタムポリシーおよびルールの復元

アップグレードしたドライバを運用環境に移す前に、テスト環境でこれらの手順を実行します。

1. iManager で、[Identity Manager] > [Identity Manager の概要] の順に選択します。
2. ツリーでその場所を参照して選択し、ドライバセットオブジェクトを検索してから、[検索] アイコン をクリックします。
3. アップグレードしたドライバを含むドライバセットオブジェクトをクリックします。
4. ドライバアイコンをクリックしてから、カスタマイズしたポリシーを復元する必要があるポリシーセットを選択します。
5. [挿入] をクリックします。
6. [既存のポリシーを使用する] を選択し、カスタムポリシーを参照して選択します。
7. [OK] をクリックし、[閉じる] をクリックします。
8. ドライバに復元する必要がある各カスタムポリシーに対して、ステップ 3 ～ステップ 7 を繰り返します。
9. ドライバを起動してテストします。

   ドライバの起動については、『*NetIQ Identity Manager Driver Administration Guide*』の「Stopping, Starting, or Restarting a Driver in Designer」を参照してください。iManager にはポリシーシミュレータはありません。ポリシーをテストするには、ポリシーを実行するイベントを発生させます。たとえば、ユーザの作成、ユーザの変更、またはユーザの削除などです。
10. ポリシーが動作することを確認したら、ドライバを運用環境に移します。

12 Advanced Edition から Standard Edition への切り替え

ご使用の環境で Advanced Edition 機能が必要なく、Identity Manager の展開をスケールダウンする場合にのみ Standard Edition に切り替える必要があります。

1 (状況によって実行) すでに Advanced Edition のアクティベーションを適用している場合は、それを削除します。

2 (状況によって実行) Standard Edition 評価モードに切り替える場合は、次のアクションを実行します。

   2a C:\Novell\NDS\DIBFiles の識別ボールト dib ディレクトリに移動します。

   2b 新しいファイルを作成し、それに .idme という名前を付け、そのファイルに 2 (数字) を追加します。

   2c eDirectory を再起動します。

   2d 手順 4 に進みます

3 (状況によって実行) すでに Standard Edition のアクティベーションを購入している場合は、アクティベーションを適用します。

4 Tomcat を停止します。

5 C:\NetIQ\idm\apps\tomcat\webapps ディレクトリから次の WAR ファイルと Webapps フォルダを削除します。

   - IDMProv*
   - IDMRPT*
   - dash*
   - idmdash*
   - landing*
   - rra*
   - rptdoc*

6 次の既存のフォルダをバックアップディレクトリに移動します。

   - IDMReporting
   - UserApplication

7 ism-configuration.properties ファイルを C:\NetIQ\IDM\apps\tomcat\conf ディレクトリからバックアップディレクトリにコピーします。

8 Identity Manager 4.8 iso ファイルから Identity Reporting をインストールします。

9 *<reporting install folder>*/bin ディレクトリから configupdate.bat を起動し、次のパラメータの値を指定します。

［**レポーティング**］**タブ**：次のセクションの設定を指定します。

- アイデンティティボールト
- 識別ボールトユーザ ID
- レポート管理者
  - **[レポーティング管理者の役割コンテナの DN]**. たとえば、ou=sa,o=data
  - **[レポート管理者]**。たとえば、cn=uaadmin,ou=sa,o=data

［**認証**］**タブ**：次のセクションの設定を指定します。

- Authentication Server(認証サーバ)
  - **[OAuth サーバのホスト識別子]**. たとえば、192.99.17.22 のような認証サーバの IP アドレスまたは DNS 名
  - **[OAuth サーバの TCP ポート]**
  - **[OAuth サーバは TLS/SSL を使用しています]**
- 認証の設定
  - **[OAuth キーストアファイル]**. たとえば、C:\NetIQ\idm\apps\osp\osp.jks です。
  - **[OAuth で使用するためのキー別名]**
  - **[Key password of key for use by OAuth (OAuth で使用するキーのキーパスワード)]**
  - **[セッションタイムアウト (分)]**. たとえば、60 分です。

［**SSO クライアント**］**タブ**：次のセクションの設定を指定します。

- レポーティング
  - **[ランディングページへの URL リンク]**. たとえば、http://192.168.0.1:8180/IDMRPT です。
- セルフサービスパスワードリセット
  - **[OAuth クライアント ID]**. たとえば、*sspr* です。
  - OAuth クライアントシークレット。たとえば、*<sspr client secret>* です。
  - **[OSP OAuth リダイレクト URL]**. たとえば、http://192.168.0.2:8180/sspr/public/oauth です。

設定ユーティリティの詳細については、78 ページの 「識別情報アプリケーション設定ユーティリティの実行」を参照してください。

10 設定ユーティリティで変更を保存して終了します。

11 Tomcat を起動します。

VII Identity Manager のデータの新しいインストールへのマイグレート

このセクションでは、Identity Manager のコンポーネントの既存データを新しいインストールにマイグレートするための情報を提供します。ほとんどのマイグレーションタスクは、識別情報アプリケーションに適用されます。Identity Manager のコンポーネントをアップグレードするには、143 ページのパート VI「Identity Manager のアップグレード」を参照してください。アップグレードとマイグレーションの違いの詳細については、147 ページの「アップグレードとマイグレーションの理解」を参照してください。

13 Identity Manager をマイグレートする準備

このセクションでは、Identity Manager ソリューションを新しいインストールにマイグレートする準備について説明します。

マイグレーションを実行するためのチェックリスト

マイグレーションを実行するために、次のチェックリストの手順を実行することをお勧めします。

	チェックリストの項目
❑	1. Identity Manager のデータをマイグレートするために最新のインストールキットを用意していることを確認します。
❑	2. Identity Manager の最新バージョンのハードウェアとソフトウェアの前提条件をコンピュータが満たしていることを確認します。
❑	3. Identity Vault をサポートされている最新バージョンにアップグレードします。
❑	4. 現在の Identity Manager サーバにあるのと同じ eDirectory のレプリカを、新しいサーバに追加します。詳細については、193 ページのセクション 14「Identity Manager の新しいサーバへのマイグレート」を参照してください。
❑	5. 新しいサーバで Identity Manager をインストールします。詳細については、39 ページの 「Identity Manager のインストールの計画」を参照してください。
❑	6. (状況によって実行) ドライバセットのいずれかのドライバがリモートローダドライバである場合、各ドライバのリモートローダサーバをアップグレードします。詳細については、162 ページの 「リモートローダのアップグレード」を参照してください。
❑	7. (状況によって実行) 古いサーバでユーザアプリケーションを実行している場合、そのコンポーネントとドライバをアップデートします。詳細については、193 ページの 「Identity Manager のマイグレーションのチェックリスト」を参照してください。
❑	8. 新しいサーバをドライバセットに追加します。詳細については、182 ページの 「新しいサーバをドライバセットに追加する」を参照してください。
❑	9. ドライバごとに、サーバ固有の情報を変更します。詳細については、195 ページの「Designer でサーバ固有の情報をコピーする」を参照してください。

	チェックリストの項目
❑	10. (状況によって実行) RBPM を使用できる場合、ユーザアプリケーションのサーバ固有情報を古いサーバのものから新しいサーバのものに更新します。詳細については、195 ページの 「ドライバセットのサーバ固有情報のコピー」を参照してください。
❑	11. ドライバをアップデートしてパッケージフォーマットにします。詳細については、180 ページの 「Identity Manager ドライバのアップグレード」を参照してください。
❑	12. (状況によって実行) カスタムポリシーとルールがある場合、カスタマイズされている設定を復元します。詳細については、184 ページの 「ドライバへのカスタムポリシーとルールの復元」を参照してください。
❑	13. ドライバセットから古いサーバを削除します。詳細については、183 ページの 「ドライバセットから古いサーバを削除する」を参照してください。
❑	14. アップグレードした Identity Manager ソリューションをアクティベートします。詳細については、141 ページの 「Identity Manager のアクティベート」を参照してください。

14 Identity Manager の新しいサーバへのマイグレート

このセクションでは、ユーザアプリケーションから新しいサーバ上の識別情報アプリケーションにマイグレートする方法について説明します。既存のインストールをアップグレードできない場合もマイグレーションが必要になる可能性があります。このセクションでは、次のアクティビティについて説明します。

- 193 ページの 「Identity Manager のマイグレーションのチェックリスト」
- 194 ページの 「Designer プロジェクトのマイグレーションの準備」
- 195 ページの 「ドライバセットのサーバ固有情報のコピー」
- 197 ページの 「Identity Manager エンジンの新しいサーバへのマイグレート」
- 197 ページの 「ユーザアプリケーションドライバのマイグレート」
- 199 ページの 「識別情報アプリケーションのアップグレード」
- 199 ページの 「Identity Applications の移行」
- 201 ページの 「識別情報アプリケーションのマイグレーションの完了」

Identity Manager のマイグレーションのチェックリスト

次のチェックリストの手順を完了することをお勧めします。

	チェックリストの項目
❑	1. Identity Manager ソリューションのディレクトリとデータベースのバックアップ
❑	2. 識別情報アプリケーションを除いて、Identity Manager のコンポーネントの最新バージョンがインストールされていることを確認します。 **注 :** 現在のユーザアプリケーションデータベースを引き続き使用するには、インストールプログラムで [**既存のデータベース**] を指定します。
❑	3. 識別ボールトのヘルスチェックを実行し、スキーマが適切に拡張されていることを確認します。TID 3564075 を使用してヘルスチェックを完了します。
❑	4. 既存のユーザアプリケーションドライバを Designer にインポートします。
❑	5. Designer プロジェクトをアーカイブします。これはドライバのマイグレーション前の状態を表します。詳細については、194 ページの 「Designer プロジェクトのマイグレーションの準備」を参照してください。

	チェックリストの項目
❑	6. (状況によって実行) Identity Manager エンジンを新しいサーバにマイグレートするには、eDirectory のレプリカを新しいサーバにコピーします。詳細については、197 ページの 「Identity Manager エンジンの新しいサーバへのマイグレート」を参照してください。
❑	7. Designer の最新バージョンで新しい Designer プロジェクトを作成し、ユーザアプリケーションドライバをインポートしてマイグレーションを準備します。
❑	8. ユーザアプリケーションドライバをマイグレートします。詳細については、197 ページの 「ユーザアプリケーションドライバのマイグレート」を参照してください。
❑	9. 2 つのドライバを識別ボールトに展開します。
❑	10. 識別情報アプリケーションをアップグレードします。詳細については、166 ページの 「Identity Applications のアップグレード」を参照してください。
❑	11. 古いバージョンの Identity Manager のコンテンツがブラウザに含まれていないことを確認します。詳細については、202 ページの 「ブラウザのキャッシュのフラッシュ」を参照してください。
❑	12. (状況によって実行) SharedPagePortlet のカスタム設定を回復します。詳細については、203 ページの 「SharedPagePortlet の最大タイムアウト設定の更新」を参照してください。
❑	13. ユーザがフィルタのパラメータを入力するまで、グループの検索オプションに情報が表示されないことを確認します。詳細については、203 ページの 「グループの自動クエリ設定の無効化」を参照してください。

Designer プロジェクトのマイグレーションの準備

ドライバをマイグレートする前に、Designer プロジェクトのマイグレーションを準備するためにいくつかの手順を実行する必要があります。

注 : マイグレートする Designer プロジェクトが存在しない場合、[ファイル] > [インポート] > [プロジェクト (識別ボールトから)] を使用して新しいプロジェクトを作成します。

1. Designer を起動します。
2. (状況によって実行) マイグレートするユーザアプリケーションを含む Designer プロジェクトが既存の場合、そのプロジェクトをバックアップします。
   - **2a** プロジェクトビューでプロジェクト名を右クリックして、[プロジェクトのコピー] を選択します。
   - **2b** プロジェクトの名前を指定して、[OK] をクリックします。
3. 既存のプロジェクトのスキーマをアップデートするには、次の手順を実行します。
   - **3a** [モデラー] ビューで [識別ボールト] を選択します。
   - **3b** [ライブ] > [スキーマ] > [インポート] の順に選択します。

4 (オプション) プロジェクトの Identity Manager のバージョン番号が適切であることを検証するには、次の手順を実行します。

4a ［モデラー］ビューで、［識別ボールト］を選択し、[プロパティ] をクリックします。

4b 左のナビゲーションメニューで [サーバリスト] を選択します。

4c サーバを選択し、[編集] をクリックします。

[Identity Manager バージョン] に最新バージョンが表示されるはずです。

ドライバセットのサーバ固有情報のコピー

各ドライバおよびドライバセットに保存されているサーバ固有のすべての情報を、新しいサーバの情報にコピーする必要があります。その中には、新しいサーバに存在せず、コピーする必要がある、ドライバセットの GCV と他のデータも含まれます。サーバ固有の情報は、次のものに含まれています :

- グローバル構成値
- エンジン制御値
- 名前付きパスワード
- ドライバの認証情報
- ドライバの起動オプション
- ドライバパラメータ
- ドライバセットデータ

これは、Designer または iManager で実行できます。Designer を使用する場合には、自動的なプロセスです。iManager を使用する場合には、手動のプロセスです。バージョン 3.5 より古い Identity Manager サーバを 3.5 以降の Identity Manager サーバにマイグレートする場合、iManager を使用する必要があります。サポートされている他のすべてのマイグレーションパスの場合は、Designer を使用できます。

- 195 ページの 「Designer でサーバ固有の情報をコピーする」
- 196 ページの 「iManager でサーバ固有の情報を変更する」
- 197 ページの 「ユーザアプリケーションのサーバ固有の情報を変更する」

Designer でサーバ固有の情報をコピーする

この手順は、ドライバセットに保存されているすべてのドライバに影響します。

1 Designer で、プロジェクトを開きます。

2 [アウトライン] タブで、サーバを右クリックして、[移行] を選択します。

3 概要を読んで新しいサーバにマイグレートされる項目を確認し、[次へ] をクリックします。

4 選択可能なサーバのリストからターゲットサーバを選択して、[次へ] をクリックします。

リストに表示されているサーバだけが、現在ドライバセットに関連付けられておらず、ソースサーバの Identity Manager のバージョンと等しいか新しいサーバです。

5 次のいずれかのオプションを選択します。

- **ターゲットサーバをアクティブにする**：ソースサーバの設定をターゲットサーバにコピーして、ソースサーバのドライバを無効にします。このオプションを使用することをお勧めします。
- **ソースサーバをアクティブのままにする**：設定をコピーせずに、ターゲットサーバのすべてのドライバを無効にします。
- **ターゲットソースサーバの両方をアクティブにする**：ソースサーバの設定をターゲットサーバにコピーし、ソースサーバまたはターゲットサーバのドライバは無効にしません。このオプションはお勧めできません。両方のドライバを起動すると、同じ情報が 2 つの異なるキューに書き込まれます。これは障害を起こす可能性があります。

6 [移行] をクリックします。

7 変更されたドライバを識別ボールトに展開します。

詳細については、『*NetIQ Designer for Identity Manager Administration Guide*』の「識別ボールトへのドライバセットの展開」を参照してください。

8 ドライバを起動します。

詳細については、『*NetIQ Identity Manager Driver Administration Guide*』の「Stopping, Starting, or Restarting a Driver in Designer」を参照してください。

iManager でサーバ固有の情報を変更する

1 iManager で、 をクリックして、[Identity Manager の管理] ページを表示します。

2 [Identity Manager の概要] をクリックします。

3 ドライバセットを含んでいるコンテナをブラウズして、選択します。

4 ドライバセット名をクリックして、[ドライバセットの概要] ページにアクセスします。

5 ドライバの右上隅をクリックし、[ドライバの停止] をクリックします。

6 ドライバの右上隅をクリックし、[プロパティの編集] をクリックします。

7 古いサーバの情報を含むすべてのサーバ固有のドライバパラメータ、グローバル環境設定値、エンジン制御値、名前付きパスワード、ドライバ認証データ、およびドライバの起動オプションを、新しいサーバの情報にコピーまたはマイグレートします。最大ヒープサイズ、Java の設定などのグローバル環境設定値やドライバセットのその他のパラメータは、古いサーバの値と同一の値を持つ必要があります。

8 [OK] をクリックして、すべての変更を保存します。

9 ドライバの右上隅をクリックして、ドライバを起動します。

10 ドライバセットのドライバごとに、ステップ 5 ～ステップ 9 を繰り返します。

ユーザアプリケーションのサーバ固有の情報を変更する

新しいサーバを認識するようにユーザアプリケーションを再設定する必要があります。configupdate.bat を実行します。

1. デフォルトでユーザアプリケーションのインストールサブディレクトリにある設定更新ユーティリティに移動します。
2. コマンドプロンプトで、設定更新ユーティリティ (configupdate.bat) を起動します。
3. 78 ページの 「識別情報アプリケーションの設定の管理」の説明に従って、値を指定します。

Identity Manager エンジンの新しいサーバへのマイグレート

Identity Manager エンジンを新しいサーバにマイグレートする場合、古いサーバで現在使用している eDirectory のレプリカを維持できます。

1. 新しいサーバで、サポートされているバージョンの eDirectory をインストールします。
2. 現在の Identity Manager サーバにあるのと同じ eDirectory のレプリカを、新しいサーバにコピーします。

   詳細については、『*NetIQ eDirectory 管理ガイド*』の「Administering Replicas」を参照してください。
3. 新しいサーバで Identity Manager エンジンをインストールします。

ユーザアプリケーションドライバのマイグレート

新しいバージョンの Identity Manager にアップグレードする場合または別のサーバにマイグレートする場合、ユーザアプリケーションドライバの新しいベースパッケージをインポートするか、または既存のパッケージをアップグレードする必要がある可能性があります。たとえば、**[User Application Base Version 2.2.0.20120516011608]** をインポートします。

Identity Manager プロジェクトの作業を開始すると、プロジェクトに新しいパッケージをインポートするように、Designer からのメッセージが自動的に表示されます。その時点で手動でパッケージをインポートすることもできます。

新しいベースパッケージのインポート

1. Designer でプロジェクトを開きます。
2. **[パッケージカタログ]** を右クリックして［パッケージのインポート］をクリックし、適切なパッケージを選択します。

3 (状況によって実行)［パッケージのインポート］ダイアログのリストにユーザアプリケーションベースパッケージが表示されない場合、次の手順を実行します。

3a ［Browse］ボタンをクリックします。

3b *designer_root*/packages/eclipse/plugins/NOVLUABASE_*version_of_latest_package*.jar のある場所に移動します。

3c **[OK]** をクリックします。

4 **[OK]** をクリックします。

既存のベースパッケージのアップグレード

1 Designer でプロジェクトを開きます。

2 ユーザアプリケーションドライバを右クリックします。

3 **[ドライバ］ > ［プロパティ］ > ［パッケージ]** の順にクリックします。

ベースパッケージをアップグレードできる場合、**[アップグレード]** 列にチェックマークが表示されます。

4 アップグレード可能なパッケージの **[操作の選択]** をクリックします。

5 ドロップダウンリストで **[アップグレード]** をクリックします。

6 アップグレード後のバージョンを選択します。**[OK]** をクリックします。

7 **[Apply (適用)]** をクリックします。

8 パッケージをアップグレードするための適切な情報をフィールドに入力します。次に、**[次へ]** をクリックします。

9 インストールの概要を読みます。続いて、**[終了]** をクリックします。

10 ［パッケージ管理］ページを閉じます。

11 **[適切なパッケージバージョンのみを表示]** の選択を解除します。

マイグレートしたドライバの展開

ドライバのマイグレーションは、ユーザアプリケーションドライバを識別ボールトに展開するまで完了しません。移行後のプロジェクトは、移行した環境設定全体のみを展開できる状態になります。マイグレートした設定に定義をインポートすることはできません。マイグレートした設定全体を展開した後は、この制約は解除され、個々のオブジェクトを展開したり、定義をインポートしたりできるようになります。

1 Designer でプロジェクトを開いて、マイグレートされたオブジェクトに対してプロジェクトチェッカを実行します。

詳細については、『*NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications*』の「Validating Provisioning Objects」を参照してください。設定に検証エラーがある場合はそのことが表示されます。これらのエラーを修正するまでは、ドライバを展開できません。

2 **[アウトライン]** ビューで、ユーザアプリケーションドライバを右クリックします。

3 [展開] を選択します。

4 ドライバセットのユーザアプリケーションドライバごとにこのプロセスを繰り返します。

識別情報アプリケーションのアップグレード

識別情報アプリケーションのアップグレードプログラムを実行する場合、次の検討事項を確実に反映します。

- 前のユーザアプリケーションで使用していたデータベースと同じデータベースを使用します。前のインストールとは、移行元のインストールのことです。インストールプログラムで、データベースタイプとして [既存のデータベース] を指定します。
- ユーザアプリケーションコンテキストに別の名前を指定できます。
- 前のインストールとは異なるインストール先を指定します。
- Tomcat のサポートされているバージョンを参照します。
- 大文字と小文字を区別する照合をデータベースに対して使用しないでください。大文字と小文字を区別する照合はサポートされていません。大文字と小文字を区別しない照合により、移行中に重複キーエラーが発生する場合があります。重複キーエラーが発生した場合は、照合を確認して修正してから、識別情報アプリケーションを再インストールします。サポートされる照合は SQL_Latin1_General_CP1_CI_AS のみです。

識別情報アプリケーションのアップグレードの詳細については、166 ページの 「Identity Applications のアップグレード」を参照してください。

Identity Applications の移行

大文字と小文字を区別する照合をデータベースに対して使用しないでください。大文字と小文字を区別する照合はサポートされていません。大文字と小文字を区別する照合により、移行中に重複キーエラーが発生する場合があります。重複キーエラーが発生した場合は、照合を確認して修正してから、識別情報アプリケーションを再インストールします。サポートされる照合は SQL_Latin1_General_CP1_CI_AS のみです。

Identity Applications を移行する前に、/opt/netiq/common/openssl/lib64/ ディレクトリから、libssl.so.1.0.0 および libcrypto.so.1.0.0 ライブラリをインストールする必要があります。

Identity Applications の移行には以下が含まれます。

- 200 ページの 「データベースの新しいサーバへの移行」
- 201 ページの 「新しいサーバへの Identity Applications のインストール」

データベースの新しいサーバへの移行

ユーザアプリケーションデータベースが [PostgreSQL] 上にある場合、以下の手順を実行します。

1 [PostgreSQL] がインストールされているサーバにログインします。

2 コマンドプロンプトを開き、postgres bin ディレクトリに移動して、データを .sql ファイルにエクスポートします。

例 : pg_dumpall -U postgres > dump.sql

3 [PostgreSQL] をインストールする新しいサーバにログインします。

4 次に示すように、[PostgreSQL] をインストールします。

4a Software License and Download (ソフトウェアライセンスおよびダウンロード) (https://sldlogin.microfocus.com/) ポータルから、Identity_Manager_4.8.x_Windows.iso をダウンロードしてマウントします。

4b Identity_Manager_4.8.x_Windows.iso をマウントした場所に移動します。

4c <Mount location>\common\packages\postgres\ ディレクトリに移動します。

4d PostgreSQL インストーラを実行します。

5 C:\NetIQ\IDM\postgres に移動して、データディレクトリを削除します。

6 [PostgreSQL] がインストールされている場所にデータディレクトリを作成し、postgres ユーザがディレクトリへのアクセス権を持っていることを確認します。

7 コマンドプロンプトを開いて、postgres bin ディレクトリに移動し、次に示すようにデータベースを初期化します。

例 : initdb.exe -D C:\NetIQ\IDM\postgres\data -E WIN1252 -U postgres

8 次のエントリが C:\NetIQ\IDM\postgres\data の下にある pg_hba.conf ファイルに存在することを確認します。

IPv6 ローカル接続 :

host all all ::1/128 trust

host all all 0.0.0.0/0 trust

9 postgresql.conf ファイルで次のコメントが解除されていることを確認します。

listen_addresses = '*'

port=5432

10 run から実行中の services.msc から postgres サービスを再起動します。

11 コマンドプロンプトを開き、postgres bin ディレクトリに移動して、新しい [PostgreSQL] データベースにデータをインポートしてから、手順 2 で説明したように収集されたダンプを使用します。

例 : psql -U postgres < dump.sql

新しいサーバへの Identity Applications のインストール

次の手順では、新しいサーバへの Identity Applications のインストールについて説明します。

1. NetIQ ダウンロード Web サイト (https://dl.netiq.com/) から Identity_Manager_4.8.x_Windows.iso をダウンロードします。
2. ファイル .iso をマウントします。
3. Identity apps ディレクトリに移動して、**[Identity Applications]** をインストールし、ユーザアプリケーションと役割およびリソースサービスドライバの展開をスキップします。
   - **3a** カスタムインストールモードを選択します。
   - **3b** アイデンティティボールトの詳細を入力します。
   - **3c** **[Deploy Identity Applications Driver (Identity Applications ドライバの展開)]** の選択を解除します。
4. **[既存の PostgreSQL]** サーバを選択して、必要な詳細を入力し、インストールを続行します。

識別情報アプリケーションのマイグレーションの完了

識別情報アプリケーションのアップグレードまたはマイグレードの後で、マイグレーションプロセスを完了します。

SQL ファイルを実行する Oracle データベースの準備

インストールプロセス中、識別情報アプリケーションのデータベースを更新する SQL ファイルを書き込むことを選択できます。Oracle プラットフォームでデータベースを実行している場合、SQL ファイルを実行するには、次の手順を実行する必要があります。

1. データベースで次の SQL ステートメントを実行します。

```
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. 次の updateSQL コマンドを実行します。:

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

3 生成される SQL ファイルをテキストエディタで開きます。このファイルは、デフォルトでは *installation_path*\userapp\sql ディレクトリにあります。

4 関数 CONCAT_BLOB の定義の後にバックスラッシュ (/) を挿入します。例

```
  -- 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 SQL ファイルを実行します。

SQL ファイルを実行する方法の詳細については、103 ページの 「手動によるデータベーススキーマの作成」を参照してください。

注 : この SQL ファイルを SQL*Plus で実行しないでください。このファイルの行長は 4000 文字を超えています。

ブラウザのキャッシュのフラッシュ

識別情報アプリケーションにログインする前に、ブラウザのキャッシュをフラッシュする必要があります。キャッシュをフラッシュしない場合、ランタイムエラーが発生する可能性があります。

SharedPagePortlet の最大タイムアウト設定の更新

SharedPagePortlet のデフォルト設定または初期設定をカスタマイズしている場合、この設定はデータベースに保存されており、上書きされることはありません。したがって、［セルフサービス］タブに移動したときに、常に適切な共有ページが強調表示されるわけではありません。この問題が発生しないことを保証するには、次の手順を実行します。

1 ユーザアプリケーションの管理者としてログインします。

2 **[Administration (管理)]** > **［Portlet Administration (ポートレット管理)]** の順に移動します。

3 **[共有ページナビゲーション]** を展開します。

4 左のポートレットツリーで **[共有ページナビゲーション]** をクリックします。

5 ページの右側で **[設定]** をクリックします。

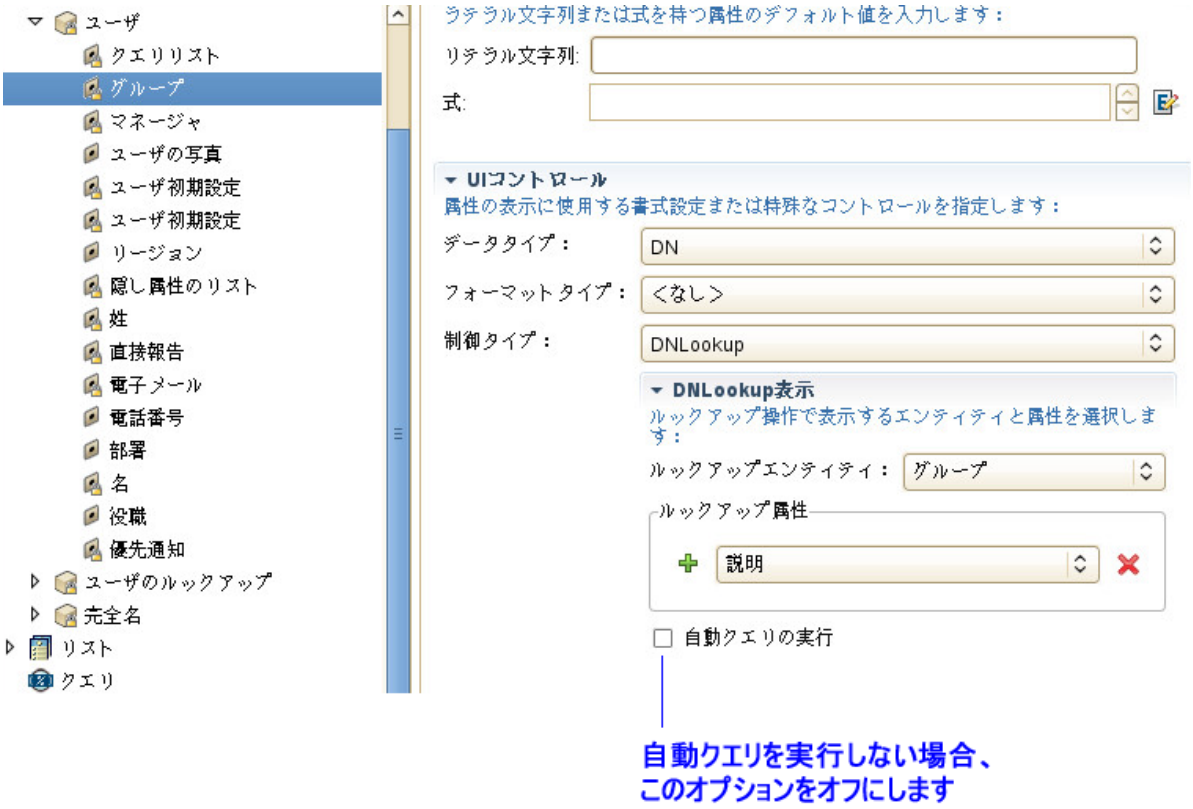
6 **[最大タイムアウト]** が 0 に設定されていることを確認します。

7 **[Save Settings]** をクリックします。

グループの自動クエリ設定の無効化

デフォルトでは、ディレクトリ抽象化レイヤの［グループ］エンティティの［DNLookup 表示］は有効です。このことは、グループを割り当てるためにオブジェクトセレクタを開くと、検索しなくてもデフォルトですべてのグループが表示されることを意味します。グループ検索ウィンドウには、ユーザが検索条件を入力するまで何も結果が表示されないようにする必要があるので、この設定を変更する必要があります。

この設定は、次に示すように、Designer で **[自動クエリの実行]** の選択を解除することで変更できます。


ユーザ
クエリリスト
グループ
マネージャ
ユーザの写真
ユーザ初期設定
ユーザ初期設定
リージョン
隠し属性のリスト
姓
直接報告
電子メール
電話番号
部署
名
役職
優先通知
ユーザのルックアップ
完全名
リスト
クエリ
リテラル文字列または式を持つ属性のデフォルト値を入力します：
リテラル文字列:
式:
UIコントロール
属性の表示に使用する書式設定または特殊なコントロールを指定します：
データタイプ：
DN
フォーマットタイプ：
<なし>
制御タイプ：
DNLookup
DNLookup表示
ルックアップ操作で表示するエンティティと属性を選択します：
ルックアップエンティティ：
グループ
ルックアップ属性
説明
自動クエリの実行
自動クエリを実行しない場合、
このオプションをオフにします

VIII Microsoft AzureでのIdentity Managerの展開

このセクションでは、Microsoft Azure クラウドでの Identity Manager の計画と実装について説明します。

- 207 ページの第 15 章「Microsoft Azure での Identity Manager の計画と実装」
- 219 ページの第 16 章「ハイブリッド Identity Manager のシナリオの例」

15 Microsoft AzureでのIdentity Managerの計画と実装

Identity Manager では、Microsoft Azure で以下の Identity Manager コンポーネントを展開するためのサポートが追加されています。

- Identity Manager エンジン
- Identity Manager ドライバとリモートローダ
- iManager
- Designer
- 識別情報アプリケーション
- Identity Reporting

注 : Sentinel Log Management の展開は Microsoft Azure ではサポートされていません。

前提条件

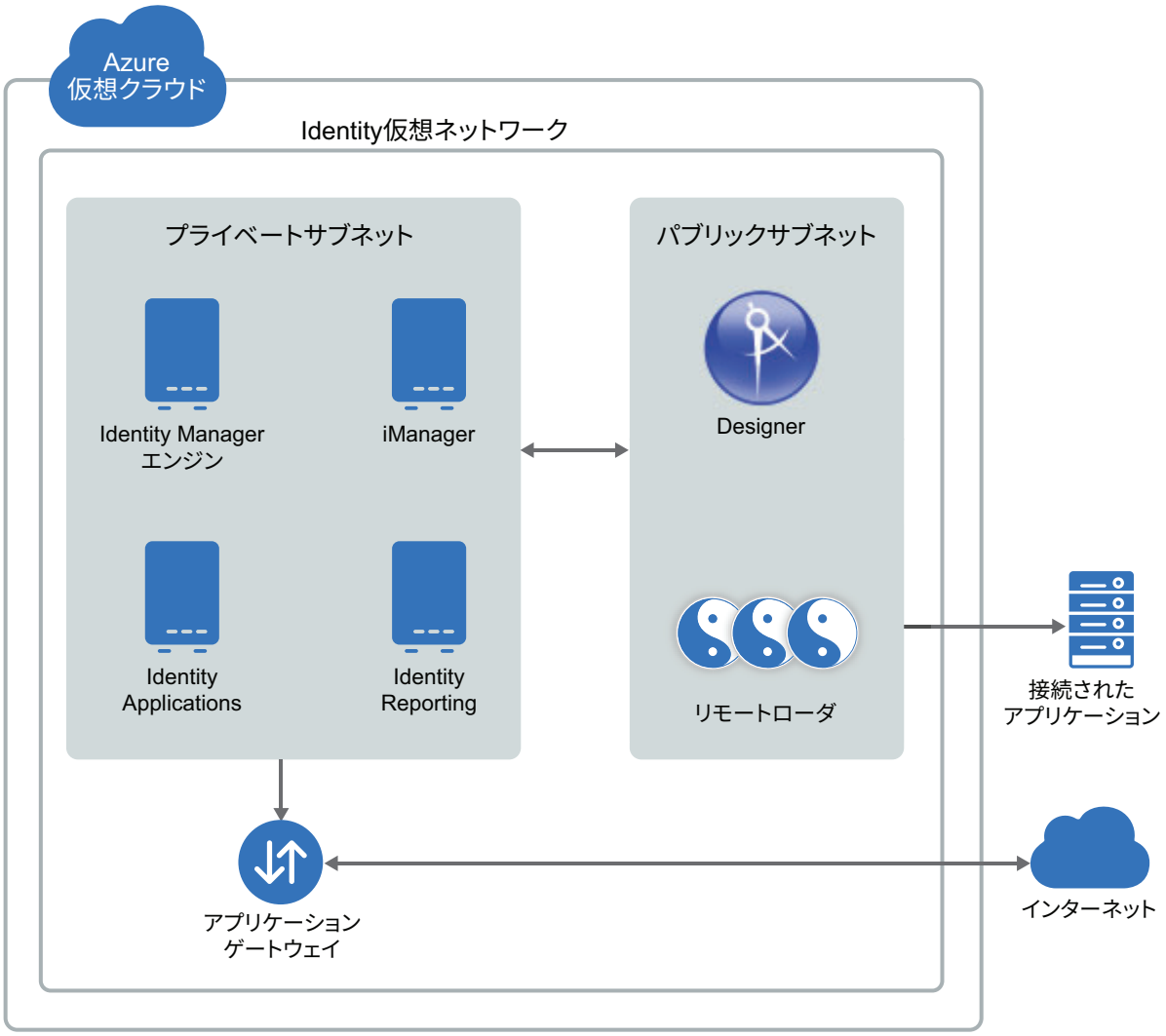
Identity Manager コンポーネントのシステム要件に加えて、以下の前提条件を満たしていることを確認してください。

- Microsoft Azure の管理アカウント。
- Identity_Manager_4.8_Windows.iso と Designer がダウンロードされ、抽出され、Identity Manager コンポーネントのインスタンスで利用可能になっている。
- ローカルクライアントマシンから Azure VM インスタンスに接続するためのリモートデスクトップ。

展開手順

Identity Manager コンポーネントは、要件に基づいてプライベートネットワークまたはパブリックネットワークに展開できます。図 15-1 は、以降のセクションで使用されるサンプル展開を示しています。

図 15-1 Microsoft Azure での Identity Manager の展開



Identity Manager コンポーネントは、複数のコンポーネントが異なるサーバにどのように分散されるかに応じて、さまざまな組み合わせで Microsoft Azure 上に展開することができます。ただし、展開手順はすべてのシナリオで同じです。

展開手順は、次の手順で構成されます。

- 209 ページの 「リソースグループの作成」
- 209 ページの 「仮想ネットワークとサブネットの作成」
- 210 ページの 「アプリケーションゲートウェイの作成」
- 212 ページの 「仮想マシンインスタンスの作成」
- 214 ページの 「VM のホストエントリの更新」
- 215 ページの 「Designer の設定」
- 215 ページの 「アプリケーションゲートウェイの設定」

リソースグループの作成

リソースグループを作成し、このグループに Identity Manager で使用するために必要なリソースを追加することをお勧めします。新しいリソースグループを作成するには、次の手順を実行します。

1 Azure ポータルにログインします。

2 [リソースグループ] をクリックします。

3 [作成] をクリックします。

4 [基本] タブで、次の手順を実行します。

4a ドロップダウンリストから [サブスクリプション] を選択します。

4b 新しいリソースグループ名を入力します。

4c [地域] ドロップダウンリストから場所を選択します。例 : インド中部

4d [Next : Tags (次の手順 : タグ) >] をクリックします。

5 [タグ] タブで、[Next : Review + Create (次の手順 : レビューと作成) >] をクリックします。

6 [Review + create (レビューと作成)] タブで、[作成] をクリックします。

仮想ネットワークとサブネットの作成

1 Azure ポータルにログインします。

2 検索に「仮想ネットワーク」と入力します。

3 ［サービス］で、[仮想ネットワーク] を選択します。

4 [作成] をクリックします。

5 [基本] タブで、次の詳細を指定します。

フィールド	説明
[サブスクリプション]	ドロップダウンリストからサブスクリプションを選択します。
[Resource Group]	ドロップダウンから既存のリソースグループを選択します。
[名前]	仮想ネットワークの名前を指定します。
[地域]	ドロップダウンリストから場所を選択します。例 : インド中部

5a [Next : IP Addresses (次の手順 : IP アドレス) >] をクリックします。

6 ［IP アドレス］タブで、[サブネットの追加] をクリックします。

6a [サブネットの追加] をクリックします。

6a1 サブネット名を指定します。たとえば、デフォルトと指定します。

6a2 サブネットアドレス範囲を指定します。たとえば、10.1.0.0/24 と指定します。

6a3 [追加] をクリックします。

6b [Next : Security (次の手順 : セキュリティ) >] をクリックします。

7 [セキュリティ] タブで、すべてのフィールドでデフォルト値のままにし、[Next : Tags (次の手順 : タグ) >] をクリックします。

8 [タグ] タブで、[Next : Review + Create (次の手順 : レビューと作成) >] をクリックします。

9 [Review + create (レビューと作成)] タブで、設定を確認して、[作成] をクリックします。

アプリケーションゲートウェイの作成

1 Azure ポータルにログインします。

2 [Create a Resource (リソースの作成)] をクリックします。

3 [カテゴリ] > [ネットワーク] > [Application Gateway] の順に移動します。

4 [基本] タブで、次の詳細を指定します。

フィールド	説明
[サブスクリプション]	ドロップダウンリストからサブスクリプションを選択します。
[Resource Group]	ドロップダウンから既存のリソースグループを選択します。
[Application gateway name (アプリケーションゲートウェイ名)]	アプリケーションゲートウェイ名を指定します。
[地域]	ドロップダウンリストから場所を選択します。例 : インド中部
[ティア]	必要なティアを選択します。例 : [Standard V2]
[最小インスタンス数]	値 **0** を指定します。
[最大インスタンス数]	値 **10** を指定します。
[仮想ネットワーク]	作成済みの仮想ネットワークと対応するサブネットを選択します。209 ページの 「仮想ネットワークとサブネットの作成」を参照してください。

4a 残りのフィールドのデフォルト値をそのままにして、[Next : Frontends (次の手順 : フロントエンド) >] をクリックします。

5 [フロントエンド] タブで、次の手順を実行します。

5a [パブリック] を選択します。

5b [パブリック IP アドレス] で、[新規追加] をクリックします。

5b1 パブリック IP アドレス名を指定します。例 : idmgateway.centralindia.cloudapp.azure.com

5b2 [OK] をクリックします。

5c [Next : Backends (次の手順 : バックエンド) >] をクリックします

6 [バックエンド] タブで、次の手順を実行します。

6a [Add a backend pool (バックエンドプールの追加)] をクリックします。

6a1 バックエンドプール名を指定します。

6a2 ターゲットなしのバックエンドプールを追加するには、[はい] を選択します。

6a3 [追加] をクリックします。

6b [Next : Configuration (次の手順 : 構成) >] をクリックします。

7 [構成] タブで、次の手順を実行します。

7a [ルーティング規則] で、[Add a routing rule (ルーティング規則の追加)] をクリックします。

7b 規則名を指定します。

7c [リスナー] タブで、次の詳細を指定します。

フィールド	説明
[リスナー名]	リスナー名を指定します。
[フロントエンド IP]	ドロップダウンから［パブリック］を選択します。
[プロトコル]	[HTTP] を選択します。
[Port](ポート)	値 **80** を指定します。

7d 残りのフィールドのデフォルト値をそのままにします。

7e [Backend targets (バックエンドターゲット)] タブで、次の詳細を指定します。

フィールド	説明
[Backend targets (バックエンドターゲット)]	ドロップダウンからバックエンドターゲットを選択します。
[HTTP 設定]	[新規追加] をクリックして、HTTP 設定名を指定します。すべてのフィールドでデフォルト値のままにし、[追加] をクリックします。

7e1 [追加] をクリックします。

7f [Next : Tags (次の手順 : タグ) >] をクリックします。

8 [タグ] タブで、[Next : Review + Create (次の手順 : レビューと作成) >] をクリックします。

9 [Review + create (レビューと作成) >] タブで、設定を確認して、[作成] をクリックします。

注 : アプリケーションゲートウェイの設定に関連する詳細については、215 ページの 「アプリケーションゲートウェイの設定」を参照してください。

仮想マシンインスタンスの作成

Identity Manager コンポーネントをホストする別の仮想マシンを作成します。

1 Azure ポータルにログインします。

2 検索に「仮想マシン」と入力します。

3 ［サービス］で、[仮想マシン] を選択します。

4 [作成] をクリックし、[仮想マシン] を選択します。

5 [基本] タブで、次の手順を実行します。

5a ドロップダウンリストから [サブスクリプション] を選択します。

5b ドロップダウンリストから既存のリソースグループを選択します (209 ページの「リソースグループの作成」を参照してください)。

5c [仮想マシン名] を指定します。

5d [地域] ドロップダウンリストから場所を選択します。例 : インド中部

5e [イメージ] ドロップダウンリストから、必要な [Windows Server] を選択します。例 : Windows Server 2019

5f [サイズ] ドロップダウンリストから仮想マシンのサイズを選択します。

5g [ユーザ名]、[パスワード]、および [パスワードの確認] を指定します。

5h［ライセンス］で、[Windows Server License (Windows Server ライセンス)] を選択し、対象となる [Windows Server License with Software Assurance (ソフトウェアアシュアランス付き Windows Server ライセンス)] を選択して確認します。

5i 残りのフィールドのデフォルト値をそのままにします。

5j [Next : Disks (次の手順 : ディスク) >] をクリックします。

6 [ディスク] タブで、次の手順を実行します。

6a [OS disk type (OS ディスクの種類)] ドロップダウンリストからディスクの種類を選択します。例 : Premium SSD

6b ドロップダウンリストから、必要な暗号化タイプを選択します。

6c [Next : Networking (次の手順 : ネットワーク) >] をクリックします。

7 [ネットワーク] タブで、次の手順を実行します。

7a 作成済みの仮想ネットワークと対応するサブネットを選択します。209 ページの「仮想ネットワークとサブネットの作成」を参照してください。

7b［ネットワークセキュリティグループ］で、[詳細設定] を選択します。

7c ドロップダウンリストから既存のネットワークセキュリティグループを選択します。

7c1 (状況によって実行) ネットワークセキュリティグループが利用できない場合は、[新規作成] をクリックします。

7c2 ネットワークセキュリティグループ名を指定します。

7c3 [Add an inbound role (受信役割の追加)] をクリックし、必要な詳細を指定します。

7c4 [Add an outbound role (送信役割の追加)] をクリックし、必要な詳細を指定します。

7c5 [OK] をクリックします。

7d 残りのフィールドのデフォルト値をそのままにします。

7e [Next : Management (次の手順 : 管理) >] をクリックします。

8 [管理] タブで、すべてのフィールドでデフォルト値のままにし、[Next : Advanced (次の手順 : 詳細設定) >] をクリックします。

9 [詳細設定] タブで、すべてのフィールドでデフォルト値のままにし、[Next : Tags (次の手順 : タグ) >] をクリックします。

10 [タグ] タブで、すべてのフィールドでデフォルト値のままにし、[Next : Review + create (次の手順 : レビューと作成) >] をクリックします。

11 [Review + create (レビューと作成)] タブで、設定を確認して、[作成] をクリックします。

VM のホストエントリの更新

アプリケーションゲートウェイのパブリック DNS 名またはエイリアス DNS レコードセットを使用して、Identity Manager コンポーネントにアクセスすることができます。Identity Manager コンポーネントが相互に通信できるようにするには、各 VM の hosts ファイルを編集し、そのホスト名を解決するエントリを追加します。

***表 15-1** ホストエントリの更新*

コンポーネント	説明
Identity Engine	Identity Engine VM の **hosts** ファイルに移動します。次に例を示します。 C:\Windows\System32\drivers\etc\hosts **次のエントリで hosts ファイルを変更します。** <IP address of Identity engine VM> <Private DNS Name of Identity engine VM> 例 : 10.0.1.1 identityengine.example.com <IP address of Identity applications VM> <Public DNS Name of application gateway> 例 : 10.0.1.2 idmgateway.centralindia.cloudapp.azure.com

コンポーネント	説明
識別情報アプリケーション	Identity Engine VM の **hosts** ファイルに移動します。次に例を示します。 C:\Windows\System32\drivers\etc\hosts **次のエントリで hosts ファイルを変更します。** <IP address of Identity engine VM> <Private DNS Name of Identity engine VM> 例 : 10.0.1.1 identityengine.example.com <IP address of Identity applications VM> <Public DNS Name of application gateway> 例 : 10.0.1.2 idmgateway.centralindia.cloudapp.azure.com

Identity Reporting および iManager のホストエントリを更新するには、214 ページの 表 15-1 の「**Identity Applications**」を参照してください。

注 : Identity Manager コンポーネントのインストールについては、51 ページの 「インストール手順」を参照してください。

Designer の設定

1 パブリックサブネットで、仮想マシンインスタンスを起動します。212 ページの 「仮想マシンインスタンスの作成」を参照してください。

Windows セキュリティグループの場合、rdesktop ポートのみを使用します。たとえば、3389 と指定します。.

2 Designer をインストールします。125 ページのパート IV「Designer のインストール」を参照してください。

アプリケーションゲートウェイの設定

仮想マシンでホストされている Identity Manager コンポーネントを外部ネットワークが使用できるように、アプリケーションゲートウェイを設定します。

1 iManager、Identity Applications、フォーム、Identity Reporting などの Identity Manager コンポーネント用に、個別のバックエンドプールを設定します。

1a **[バックエンドプール]** で、**[追加]** をクリックします。

1b 次の詳細を指定します。

フィールド	説明
[名前]	Identity Manager コンポーネントを識別するバックエンドプールの名前を指定します。
[タイプ]	タイプを指定するには、次のいずれかの手順に従ってください。 ◆ **IP アドレスまたは FQDN:** 必要な Identity Manager コンポーネントの IP アドレスまたは FQDN を指定します。 ◆ **仮想マシン :** 必要な Identity Manager コンポーネントをホストしている仮想マシンを選択します。

1c [OK] をクリックします。

この手順を繰り返して、追加のバックエンドプールを設定します。

2 iManager、Identity Applications、フォーム、Identity Reporting などの Identity Manager コンポーネント用に、個別の HTTP 設定を設定します。

注 : 必要な Identity Manager コンポーネントのパブリック証明書をエクスポートしたことを確認してください。

2a [HTTP 設定] で、[追加] をクリックします。

2b 次の詳細を指定します。

フィールド	説明
[名前]	Identity Manager コンポーネントを識別する HTTP 設定の名前を指定します。
[プロトコル]	HTTPS を選択します。
[ポート]	Identity Manager コンポーネントのポートを指定します。 次に例を示します。 ◆ **iManager:** 8443 ◆ **識別情報アプリケーション :** 8543 ◆ **フォーム :** 8600 ◆ **Identity Reporting:** 8643
[バックエンド認証証明書]	1. ［新規作成］を選択します。 2. 証明書の名前を指定します。 3. 対応する Identity Manager コンポーネントのエクスポートされたパブリック証明書を参照してアップロードします。 4. ［証明書の追加］をクリックします。

2c [OK] をクリックします。

この手順を繰り返して、追加の HTTP 設定を行います。

3 iManager、Identity Applications、フォーム、Identity Reporting などの各 Identity Manager コンポーネント用に、個別のリスナーを設定します。

注 : アイデンティティボールトから .PFX 証明書をエクスポートしたことを確認します。

3a [リスナー] で、[基本] をクリックします。

3b 次の詳細を指定します。

フィールド	説明
[名前]	Identity Manager コンポーネントを識別するリスナーの名前を指定します。
[フロントエンド IP 構成]	1. 仮想ネットワークおよび以前に作成されたサブネットを選択します。209 ページの 「仮想ネットワークとサブネットの作成」を参照してください。 2. アプリケーションの名前とポート番号を指定します。次に例を示します。 **iManager:** 8443 **識別情報アプリケーション :** 8543 **フォーム :** 8600 **Identity Reporting:** 8643
[プロトコル]	[HTTPS] を選択します。
[証明書]	1. PFX 証明書を参照してアップロードします。 2. 証明書の名前とパスワードを指定します。

3c [OK] をクリックします。

この手順を繰り返して、追加のリスナーを設定します。

4 iManager、Identity Applications、フォーム、Identity Reporting などの Identity Manager コンポーネントの基本ルールを作成し、このルールをそれぞれのバックエンドプール、リスナー、および HTTP 設定に関連付けます。

4a [ルール] で、[追加] をクリックします。

4b 次の詳細を指定します。

フィールド	説明
[名前]	Identity Manager コンポーネントの識別に役立つルールの名前を指定します。
[リスナー]	ステップ 3 で作成されたそれぞれのリスナーを選択します。
[バックエンドプール]	ステップ 1 で作成されたそれぞれのバックエンドプールを選択します。
[HTTP 設定]	ステップ 2 で作成されたそれぞれの HTTP 設定を選択します。

4c [OK] をクリックします。

この手順を繰り返して、追加のルールを設定します。

16 ハイブリッド Identity Manager のシナリオの例

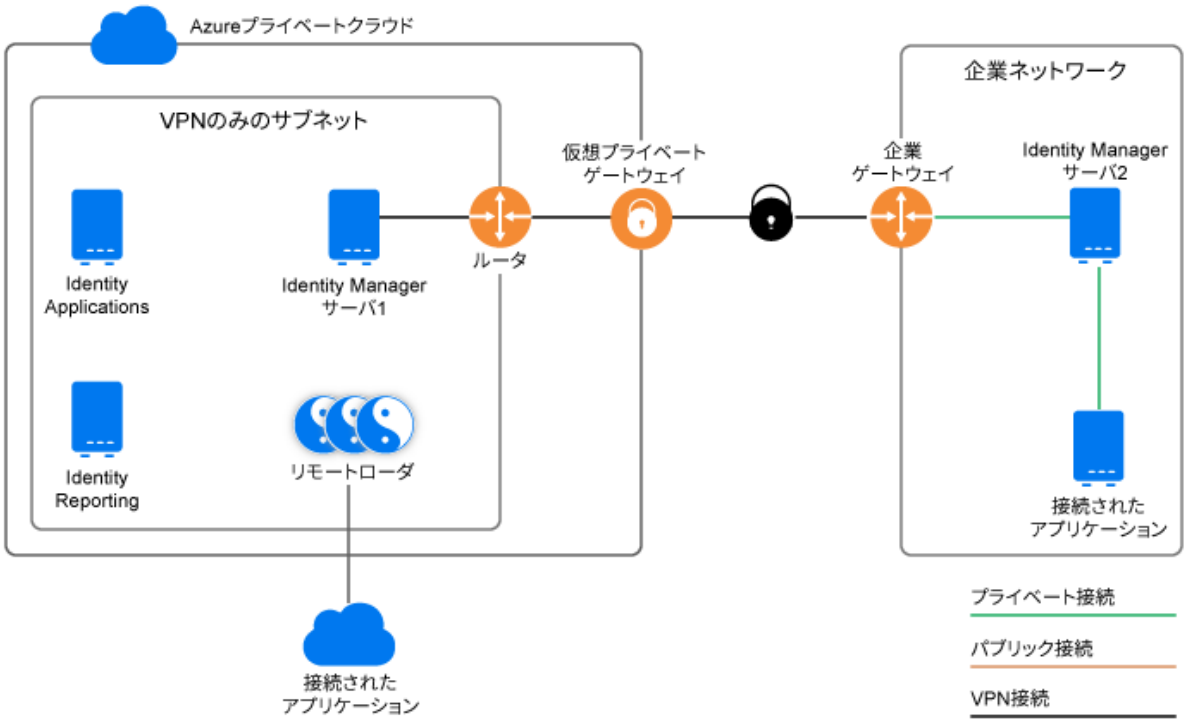
エンタープライズプレミスと MS Azure クラウド間で識別情報がシームレスに同期される Identity Manager コンポーネントを設定できます。このタイプのハイブリッドシナリオを実装するには、Azure サブネットとエンタープライズネットワークの間に VPN 接続を設定する必要があります。このセクションでは、以下のハイブリッドシナリオについて説明します。

- 219 ページの 「マルチサーバドライバセット接続の使用」
- 220 ページの 「eDirectory ドライバ接続の使用」

マルチサーバドライバセット接続の使用

このシナリオでは、1 つのサーバが Azure クラウドにインストールされ、もう 1 つのサーバがエンタープライズプレミスにインストールされている、少なくとも 2 つの Identity Manager サーバが、同じ eDirectory ツリーとドライバセットを使用します。これには、VPN 接続を介して識別情報を同期するために Identity Vault レプリケーションチャネルを使用する完全なレプリカサーバが含まれます。エンタープライズネットワークまたは Azure クラウドで実行されている Identity Manager サーバは、それぞれの接続アプリケーション間で識別情報を同期します。

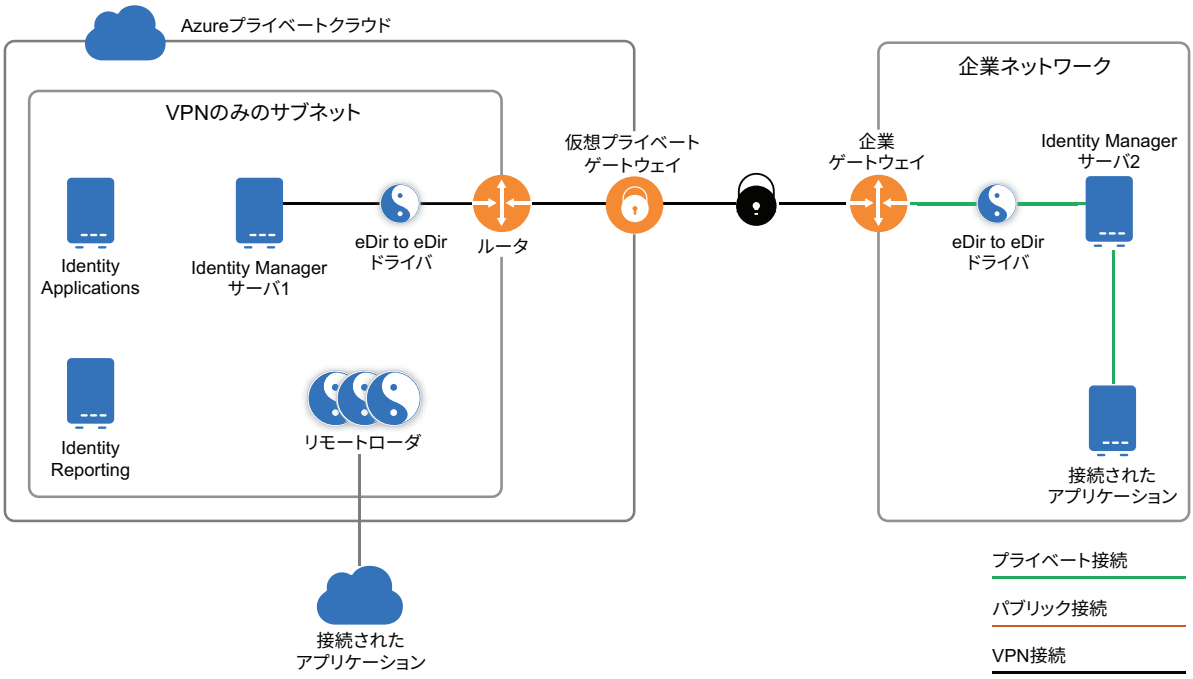
図 16-1 マルチサーバドライバセット接続を使用したハイブリッドシナリオ



eDirectory ドライバ接続の使用

このシナリオは、1 つのツリーが Azure クラウドに属し、他のツリーがエンタープライズネットワークに属する 2 つの別個の eDirectory ツリーに Identity Manager サーバがインストールされている場合に適しています。この設定では、eDirectory ドライバを使用して、VPN 接続を介して Azure クラウドとエンタープライズネットワーク間の識別情報を同期します。エンタープライズネットワークまたは Azure クラウドで実行されている Identity Manager サーバは、それぞれの接続アプリケーション間で識別情報を同期します。

図 16-2 eDirectory ドライバ接続を使用したハイブリッドシナリオ



Azure クラウドとエンタープライズネットワーク間の通信は制限されています。デルタ変更のみを同期します。ドライバフィルタを設定することにより、同期する属性を制御できます。ポリシーエンジンを利用して、属性を同期するための追加のコントロールを定義することもできます。たとえば、パスワード属性の同期を制限し、複数のユーザが異なるパスワードを使用して Azure クラウドとエンタープライズネットワークから Identity Manager サーバにアクセスできるようにします。

17 Identity Manager のコンポーネントのアンインストール

このセクションでは、Identity Manager のコンポーネントをアンインストールするプロセスについて説明します。コンポーネントによっては、アンインストールするための前提条件があります。アンインストールプロセスを始める前に、必ずコンポーネントごとのセクション全体をレビューしてください。

注 : Identity Manager コンポーネントをアンインストールする前に、Tomcat、PostgreSQL、ActiveMQ などのすべてのサービスを停止する必要があります。

識別ボールトのアンインストール

識別ボールトをアンインストールする前に、eDirectory のツリー構造とレプリカの配置を理解する必要があります。たとえば、ツリーに複数のサーバが存在するかどうかを知る必要があります。

1 (状況によって実行) eDirectory ツリーに複数のサーバが存在する場合、次の手順を実行します。

   1a (状況によって実行) eDirectory をインストールしたサーバにマスタレプリカが保持されている場合、eDirectory を削除する前に、レプリカリング内の別のサーバをマスタになるようにプロモートする必要があります。

   詳細については、『*NetIQ eDirectory 管理ガイド*』の「パーティションおよびレプリカの管理」を参照してください。

   1b (状況によって実行) eDirectory をインストールしたサーバのツリーにパーティションの唯一のコピーが保持されている場合、このパーティションを親パーティションにマージするか、または別のサーバにこのパーティションのレプリカを追加してマスタレプリカを保持させます。

   詳細については、『*NetIQ eDirectory 管理ガイド*』の「パーティションおよびレプリカの管理」を参照してください。

   1c eDirectory データベースでヘルスチェックを実行します。発生したエラーを修正してから次に進みます。

   詳細については、『*NetIQ eDirectory 管理ガイド*』の「eDirectory の正常な動作の維持」を参照してください。

2 識別ボールトのアンインストール :

   [コントロール パネル] のプログラムを追加および削除するユーティリティを使用します。たとえば、Windows Server 2012 R2 では、**[プログラムと機能]** をクリックします。**[NetIQ eDirectory]** を右クリックして、**[アンインストール]** をクリックします。

3 (状況によって実行) eDirectory ツリーに複数のサーバが存在する場合、次の手順を実行します。

3a サーバ固有のオブジェクトがツリーに残っている場合、それらを削除します。

3b ヘルスチェックを再実行して、サーバが正しくツリーから削除されていることを確認します。

詳細については、『*NetIQ eDirectory 管理ガイド*』の「eDirectory の正常な動作の維持」を参照してください。

識別ボールトからのオブジェクトの削除

Identity Manager をアンインストールする最初のステップでは、すべての Identity Manager オブジェクトを識別ボールトから削除します。ドライバセットの作成時に、ウィザードにより、ドライバセットを 1 つのパーティションにするようメッセージが表示されます。いずれかのドライバセットオブジェクトが eDirectory のパーティションルートオブジェクトでもある場合、ドライバセットオブジェクトを削除するには、パーティションを親パーティションにマージする必要があります。

識別ボールトからオブジェクトを削除するには :

1 eDirectory データベースでヘルスチェックを実行し、発生したエラーを修正してから次に進みます。

詳細については、『*NetIQ eDirectory 管理ガイド*』の「eDirectory の正常な動作の維持」を参照してください。

2 eDirectory ツリーに対するすべての権限を持つ管理者として iManager にログインします。

3 [パーティションとレプリカ] > [パーティションのマージ] の順に選択します。

4 パーティションのルートオブジェクトであるドライバセットオブジェクトを参照して選択し、[OK] をクリックします。

5 マージプロセスが完了するまで待ってから、[OK] をクリックします。

6 ドライバセットオブジェクトを削除します。

ドライバセットオブジェクトを削除する際、そのドライバセットに関連付けられているすべてのドライバオブジェクトが削除されます。

7 eDirectory データベースにある各ドライバセットオブジェクトに対して、すべて削除されるまで、ステップ 3 ～ステップ 6 を繰り返します。

8 ステップ 1 を繰り返して、すべてのマージが完了し、オブジェクトがすべて削除されたことを確認します。

Identity Manager エンジンのアンインストール

Identity Manager エンジンをインストールする際、インストールプロセスは Identity Manager サーバにアンインストールスクリプトを配置します。このスクリプトを使用して、インストール時に作成されたすべてのサービス、パッケージ、およびディレクトリを削除できます。

注 : Identity Manager エンジンをアンインストールする前に、識別ボールトを準備します。詳細については、224 ページの 「識別ボールトからのオブジェクトの削除」を参照してください。

Windows サーバで Identity Manager エンジンをアンインストールするには、[コントロールパネル] のプログラムを追加および削除するユーティリティを使用します。たとえば、Windows 2012 R2 では、**[プログラムと機能]** をクリックします。**[Identity Manager]** を右クリックして、**[アンインストール]** をクリックします。

リモートローダのアンインストール

リモートローダをインストールすると、インストールプロセスはサーバ上にアンインストールスクリプトを配置します。このスクリプトを使用して、インストール時に作成されたすべてのサービス、パッケージ、およびディレクトリを削除できます。

Windows サーバでリモートローダをアンインストールするには、[コントロール パネル] のプログラムを追加および削除するユーティリティを使用します。

Identity Applications のアンインストール

Roles Based Provisioning Module (RBPM) のコンポーネントは、ドライバやデータベースなど、1 つずつアンインストールする必要があります。

RBPM に関連するランタイムコンポーネントをアンインストールする必要がある場合、Windows 上でサイレントモードでアンインストールプログラムを実行している場合を除いて、アンインストールプログラムは自動的にサーバを再起動します。Windows サーバを手動で再起動する必要があります。

注 : RBPM をアンインストールする前に、Identity Manager エンジンをアンインストールします。詳細については、224 ページの 「Identity Manager エンジンのアンインストール」を参照してください。

Roles Based Provisioning Module のドライバの削除

Designer または iManager を使用して、ユーザアプリケーションドライバおよび役割とリソースサービスドライバを削除できます。

1 ユーザアプリケーションドライバおよび役割ドライバとリソースドライバを停止します。使用するコンポーネントに応じて、次のどちらかのアクションを実行します。
   - **Designer:** ドライバ行を右クリックし、**[Live (ライブ)]** > **[Stop Driver (ドライバの停止)]** をクリックします。
   - **iManager:** [Driver Set Overview (ドライバセットの概要)] ページで、ドライバ画像の右上隅をクリックして、**[Stop Driver (ドライバの停止)]** をクリックします。

2 ユーザアプリケーションドライバおよび役割ドライバとリソースドライバを削除します。使用するコンポーネントに応じて、次のどちらかのアクションを実行します。

- **Designer:** ドライバ行を右クリックし、[削除] をクリックします。
- **iManager:** ［Driver Set Overview (ドライバセットの概要)］ページで、[Drivers (ドライバ)］ > ［Delete drivers (ドライバの削除)] の順にクリックし、削除するドライバをクリックします。

Identity Applications のアンインストール

Tomcat からユーザアプリケーションとそのデータベースをアンインストールする必要があります。ここでは、Tomcat と PostgreSQL からユーザアプリケーションとそのデータベースを削除する方法について説明します。他のアプリケーションサーバとデータベースを使用している場合の手順については、その製品のマニュアルを参照してください。

重要 : ユーザアプリケーションを削除する場合、ユーザアプリケーションのスクリプトとサポートファイルがインストールされているフォルダからすべてのフォルダとファイルが削除されるので、注意が必要です。ファイルを削除する際、無意識に Tomcat または PostgreSQL をアンインストールする可能性があります。たとえば、インストールフォルダは通常、C:\NetIQ\idm\apps\UserApplication です。このフォルダには、Tomcat と PostgreSQL のフォルダも置かれています。

---

1 ユーザアプリケーションをインストールしたサーバにログインします。

2 ［コントロール パネル］のプログラムを追加および削除するユーティリティを開きます。たとえば、Windows Server 2012 R2 では、[プログラムと機能] をクリックします。

3 [Identity Manager User Application (Identity Manager ユーザアプリケーション)] を右クリックして、[アンインストール] をクリックします。

Identity Reporting のコンポーネントのアンインストール

Identity Reporting のコンポーネントをアンインストールする場合、次の順序で実行する必要があります。

1. ドライバを削除します。詳細については、227 ページの 「レポーティングドライバの削除」を参照してください。
2. Identity Reporting を削除します。詳細については、227 ページの 「Identity Reporting のアンインストール」を参照してください。
3. Sentinel を削除します。詳細については、『NetIQ Identity Manager セットアップガイド (Linux 用)』の「Sentinel Log Management for IGA のアンインストール」を参照してください。

注 : ディスク容量を節約するために、Identity Reporting のインストールプログラムは Java 仮想マシン (JVM) をインストールしません。したがって、1 つまたは複数のコンポーネントをアンインストールするには、使用可能な JVM が存在し、その JVM が PATH で指定

されていることを確認します。アンインストールの際にエラーが発生した場合、JVM の場所をローカルの PATH 環境変数に追加してからアンインストールプログラムを再実行します。

レポーティングドライバの削除

Designer または iManager を使用して、データ収集および Managed System Gateway ドライバを削除できます。

1 ドライバを停止します。使用するコンポーネントに応じて、次のどちらかのアクションを実行します。
   - **Designer:** ドライバごとに、ドライバ行を右クリックして、**[ライブ] > [ドライバの停止]** の順にクリックします。
   - **iManager:** [Driver Set Overview (ドライバセットの概要)] ページで、各ドライバ画像の右上隅をクリックして、**[Stop Driver (ドライバの停止)]** をクリックします。
2 ドライバを削除します。使用するコンポーネントに応じて、次のどちらかのアクションを実行します。
   - **Designer:** ドライバごとに、ドライバ行を右クリックして、**[削除]** をクリックします。
   - **iManager:** [Driver Set Overview (ドライバセットの概要)] ページで、**[Drivers (ドライバ)] > [Delete drivers (ドライバの削除)]** の順にクリックし、削除するドライバをクリックします。

Identity Reporting のアンインストール

Identity Reporting を削除する前に、データ収集および Managed System Gateway ドライバを削除済みであることを確認します。詳細については、227 ページの 「レポーティングドライバの削除」を参照してください。

重要 : Identity Reporting アンインストールプログラムは Reporting インストールディレクトリからすべてのファイルとフォルダを削除するので、アンインストールプログラムを実行する前に、これまでに生成したレポートを Reporting インストールディレクトリから使用しているコンピュータの別の場所にコピー済みであることを確認します。たとえば、Reporting インストールフォルダは、C:\NetIQ\idm\apps\IDMReporting です。

Identity Reporting をアンインストールするには、[コントロールパネル] のプログラムを追加および削除するユーティリティを使用します。たとえば、Windows Server 2012 R2 では、**[プログラムと機能]** をクリックします。**[Identity Reporting]** を右クリックして、**[アンインストール]** をクリックします。

Analyzer のアンインストール

1 Analyzer を閉じます。

2 Analyzer をアンインストールします。

［コントロール パネル］のプログラムを追加および削除するユーティリティを使用します。たとえば、Windows Server 2008 では、**[プログラムと機能]** をクリックします。**[Analyzer for Identity Manager]** を右クリックして、**[アンインストール]** をクリックします。

iManager のアンインストール

このセクションでは、iManager と iManager ワークステーションをアンインストールする方法について説明します。iManager または関連するサードパーティコンポーネントをアンインストールする場合、特定の順序で実行する必要はありません。これらのコンポーネントのアンインストールに関する検討事項をレビューすることをお勧めします。

- Web サーバまたはサーブレットコンテナをアンインストールすると、iManager を実行できなくなります。
- すべてのプラットフォームで、アンインストールによって削除されるのは、最初にインストールされたファイルのみです。アプリケーションが実行中に作成したファイルは、アンインストールプロセスによって削除されません。たとえば、Tomcat が実行中に作成したログファイルと自動生成設定ファイルです。
- 当初インストールの際に追加されたディレクトリ構造内で作成または変更されたファイルは、アンインストールプロセスによって削除されません。これにより、アンインストールプロセスが誤ってデータを削除しないことが保証されます。
- iManager のアンインストールは、ツリー内で設定した RBS の設定には影響しません。ログファイルまたはカスタムコンテンツは、アンインストールプロセスによって削除されません。

重要 : iManager をアンインストールする前に、残しておくすべてのカスタムコンテンツや他の特別な iManager ファイルをバックアップします。たとえば、カスタマイズしたプラグインです。

Windows での iManager のアンインストール

iManager のコンポーネントをアンインストールするには、［コントロール パネル］のプログラムを追加および削除するユーティリティを使用します。アンインストールプロセスには、次の条件が適用されます。

- ［コントロール パネル］のユーティリティには、iManager とは別に、Tomcat と NICI が表示されます。これらのプログラムを今後使用しない場合はアンインストールします。

- iManager がインストールされているサーバに eDirectory もインストールされている場合、NICI をアンインストールしないでください。eDirectory を実行するには、NICI が必要です。
- iManager をアンインストールする際、すべての iManager ファイルを削除するかどうかを確認するプロンプトが表示されます。**[はい]** を選択すると、それらのファイルが削除されますが、その中にはすべてのカスタムコンテンツが含まれます。ただし、2.7 RBS オブジェクトは eDirectory ツリーから削除されず、スキーマは同じ状態のまま残ります。

iManager ワークステーションのアンインストール

iManager ワークステーションをアンインストールするには、ファイルを展開したディレクトリを削除します。

Designer のアンインストール

1. Designer を閉じます。
2. オペレーティングシステムに応じた手順で、Designer をアンインストールします。

   ［コントロール パネル］のプログラムを追加および削除するユーティリティを使用します。たとえば、Windows Server 2008 では、**[プログラムと機能]** をクリックします。**[Designer for Identity Manager]** を右クリックして、**[アンインストール]** をクリックします。

18 トラブルシューティング

このセクションでは、Identity Manager のインストールに関する問題のトラブルシューティングに役立つ情報について説明します。Identity Manager のトラブルシューティングの詳細については、特定のコンポーネントのガイドを参照してください。

Identity Manager エンジンのトラブルシューティング

次の表に、発生する可能性のある問題とそれを解決するための推奨されるアクションを示します。問題が続く場合は、NetIQ の担当者にお問い合わせください。

項目	推奨されるアクション
eDirectory 初期化プロセスが進行中の場合、Identity Manager エンジンは起動できません。この問題は、ほとんどの場合、eDirectory DIB が非常に大きい場合に発生します。	この問題を回避するには、次の手順を実行します。 1. [SLEEP_BEFORE_ENGINE_STARTUP] というシステム環境変数を作成し、変数の値を 0 ～ 600 に設定します。値は秒単位で示されます。 **注 :** 無効な値、または 600 より大きい値を指定すると、値はデフォルトの 600 になります。 2. eDirectory を再起動します。 3. (状況によって実行) dhost.log をチェックして、メッセージとログを確認します。
マルチサーバ環境では、認識されない拡張例外が表示されます。	プライマリサーバに、セカンダリサーバ用の読み取り / 書き込みパーティションを確保します。 1. iManager にログインします。 2. [役割およびタスク] > [パーティションとレプリカ] > [レプリカビュー] の順にクリックします。 3. セカンダリサーバを選択します。 4. 選択したサーバに読み取り / 書き込み許可を割り当てます。 **注 :** ドライバセットにセカンダリサーバが追加されていることを確認してください。

Identity Applications および RBPM インストールのトラブルシューティング

次の表に、発生する可能性のある問題とそれを解決するための推奨されるアクションを示します。問題が続く場合は、NetIQ の担当者にお問い合わせください。

項目	推奨されるアクション
ダッシュボードページの [役割] ウィジェットと [セルフタスク] ウィジェットには、データは表示されません。ブラウザのコンソールでチェックする場合、404 エラーが表示されます。この問題は、デフォルトの IDMProv 展開コンテキストがカスタムコンテキストに変更された場合に発生します。	この問題を解決するには、影響を受けるウィジェットの REST API URL を変更する必要があります。次の手順を実行します。 1. Identity Manager ダッシュボードに管理者としてログインします。 2. ダッシュボードページに移動して、[ダッシュボードの管理] をクリックします。 3. [役割] ウィジェットのウィジェット設定を編集するには、次の手順を実行します。 a. ⚙をクリックします。 b. [URL] フィールドで、デフォルトの IDMProv コンテキストを次のようにカスタムコンテキストに変更します : /<custom-context>/rest/access/assignments/advanced?nextIndex=1&sortBy=name&sortOrder=ASC&forceRefresh=true&searchScope=role&size=20 ここで、<custom-context> は Identity Manager 展開で使用しているコンテキストです。 c. [適用] をクリックします。 4. [セルフタスク] ウィジェットのウィジェット設定を編集するには、次の手順を実行します。 a. ⚙をクリックします。 b. [URL] フィールドで、デフォルトの IDMProv コンテキストを次のようにカスタムコンテキストに変更します : /<custom-context>/rest/access/tasks/list?fromIndex=1&size=10&q=*&sortOrder=asc&sortBy=createTime&assignedTo=assignedTo&recipient=recipientAsMe&expireUnit=weeks&expireWithin=&proxyUser=&assignStatus=&delegatedTasks=false&status= c. [適用] をクリックします。 5. [編集完了] をクリックします。

項目	推奨されるアクション
クラスタにインストールされている Identity Applications がアップグレードされて Tomcat が再起動される場合に、クラスタリングが予期するように機能しない。	クラスタのすべてのノードで次のアクションを実行します。 1. C:\NetIQ\IDM\apps\tomcat\conf フォルダにある server.xml ファイルに移動します。 2. server.xml の次の行のコメントを解除します。 <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/> 3. バックアップされている Tomcat ディレクトリからすべてのカスタム設定をリストアします。 4. Tomcat を再起動します。
アップグレードプロセスは、デフォルトの Identity Applications 管理アカウントを cn=uaadmin.ou=sa.o=data として設定しません。次のエラーが catalina.out ファイルに記録されます。 `AuthorizationManagerService [RBPM] Error occured calculating effective rights for attribute: nrfAccessMgrRevokeRole on object: cn=complianceAdmin,cn=System,cn=Level20,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=UserApplication,cn=Driver Set,o=system for trustee: cn=uaadmin,ou=sa,o=data.com.novell.srvprv.spi.security.IDMAuthorizationException: Error occured calculating effective rights for attribute: nrfAccessMgrRevokeRole on object: cn=complianceAdmin,cn=System,cn=Level20,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=UserApplication,cn=Driver Set,o=system for trustee: cn=uaadmin,ou=sa,o=data.at com.novell.idm.security.authorization.ldap.LdapRightsUtil.getPropertyRights(LdapRightsUtil.java:152)` `Unable to fetch roles from edirectory in the predefined time set.`	1. setenv.bat ファイルに移動し、CATALINA_OPTS エントリで、-Dncpclient_req_timeout プロパティの値を「1150」に変更します。 2. Tomcat を再起動します。

項目	推奨されるアクション
インストール時に作成された次の Identity Applications 環境設定を 1 つまたは複数変更する必要がある。 ◆ 識別ボールトの接続および証明書 ◆ 電子メール設定 ◆ Identity Manager エンジンのユーザ識別情報とユーザグループ ◆ Access Manager または iChain の設定	インストーラとは別に、環境設定ユーティリティを実行します。 インストールディレクトリ (デフォルトでは C:\NetIQ\idm\apps\UserApplication\) から次のコマンドを実行します。 `configupdate.bat`
Tomcat を起動すると次の例外が発生する。 `port 8180 already in use`	すでに実行されている Tomcat (または他のサーバソフトウェア) のすべてのインスタンスをシャットダウンします。8180 以外のポートを使用するように Tomcat を再設定する場合は、ユーザアプリケーションドライバの config 設定を編集します。
Tomcat を起動すると、トラステッド証明書が見つからないと報告される。	Identity Applications のインストール時に指定した JDK を使用して Tomcat を起動していることを確認します。
ポータル管理ページにログインできない。	Identity Applications 管理者アカウントが存在することを確認します。このアカウントは、iManager 管理者アカウントと同じではありません。
管理者アカウントを使用しても、新しいユーザを作成できない。	Identity Applications 管理者は、最上位コンテナのトラスティである必要があり、スーパバイザ権限が必要です。Identity Applications 管理者の権利を LDAP 管理者と同等の権利に設定することを試すことができます (iManager を使用)。

項目	推奨されるアクション
アプリケーションサーバを起動すると、キーストアエラーが発生する。	アプリケーションサーバが、Identity Applications のインストール時に指定した JDK を使用していません。 次のように keytool コマンドを使用して、証明書ファイルをインポートします。 `keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit` ◆ *aliasName* は、この証明書に選択した一意の名前に置き換えます。 ◆ *certFile* は、証明書ファイルのフルパスおよび名前に置き換えます。 ◆ デフォルトのキーストアパスワードは、changeit です (別のパスワードがある場合は、それを指定します)。
電子メール通知が送信されない。	configupdate ユーティリティを実行して、次の Identity Applications 環境設定パラメータの **[電子メールの送信者]** と **[電子メールホスト]** に値を指定したかどうかを確認します。 インストールディレクトリ (デフォルトでは C:\NetIQ\idm\apps\UserApplication\) から次のコマンドを実行します。 `configupdate.bat`

インストールとアンインストールのトラブルシューティング

次の表に、発生する可能性のある問題とそれを解決するための推奨されるアクションを示します。問題が続く場合は、NetIQ の担当者にお問い合わせください。

項目	推奨されるアクション
ConfigUpdate ユーティリティを実行した後で、Identity Applications にログインできません。次のエラーメッセージが catalina.out ログファイルに表示されます。 javax.net.ssl.SSLHandshakeException: PKIX path validation failed: java.security.cert.CertPathValidatorException: Could not determine revocation status. この問題は、LDAP サーバで **[Bind Restrictions for Cipher (暗号のバインド制限)]** が Use SuiteB Cipher (128-bit) (SuiteB 暗号を使用 (128 ビット)) に設定されている場合に、Identity Manager 4.8.4 (edirectory 9.2.5) で発生します。Identity Manager はデジタル証明書を使用して、そのコンポーネントを認証して安全に通信します。証明書は、［CRL Distribution Point (CDP) (CRL 配布ポイント (CDP)］フィールドで指定されている証明書取り消しリスト (CRL) をチェックして検証されます。このフィールドでは、証明書が取り消されているかどうかを判断します。CRLDP は、ルート証明書と、キーストアファイル tomcat.ks および idm.jks に存在する中間証明書の両方で使用できます。ただし、証明書取り消しチェックは、デフォルトで無効になっています。その結果、PKIX 信頼マネージャは証明書の取り消しステータスを判断できません。	この問題を修正するには、-Dcom.sun.security.enableCRLDP プロパティを true に設定して、CRL 配布ポイントチェックを有効にします。 このプロパティを設定するには、次のアクションを実行してください。 1. Tomcat を停止します。 2. Tomcat の bin フォルダにある setenv.sh ファイルに移動します。たとえば、C:\NetIQ\idm\apps\tomcat\bin\setenv.bat です。 3. CATALINA_OPTS に次のようにプロパティ -Dcom.sun.security.enableCRLDP=true を追加します。 `export CATALINA_OPTS="-Dcom.sun.security.enableCRLDP=true"` 4. Tomcat を起動します。
Identity Manager をアップグレードした後、管理者以外のユーザは Identity Manager ダッシュボードへのログインに非常に時間がかかります。アプリケーションページとダッシュボードページのロードには、かなりの遅延があります。 この問題は、デフォルトで有効になっているネストされたグループ検索が原因で発生します。アプリケーションは、環境内にネストされたグループがあるかどうかに関係なく、ネストされたグループメンバーシップを介してログインしたユーザによって継承された許可を検索します。	(状況によって実行) 次の手順は、Identity Manager 4.8.5 以降に適用されます。 1. Identity Applications が 4.8.5 バージョンにアップグレードされたサーバにログインします。 2. C:\NetIQ\IDM\apps\tomcat\conf の場所に移動します。 3. テキストエディタで ism-configuration.properties ファイルを開きます。 4. ファイルの末尾に、次のプロパティを追加します。 DirectoryService/realms/jndi/params/USE_NESTED_GROUPS=false 5. ファイルを保存し、Tomcat を再起動します。

項目	推奨されるアクション
Identity Applications を 4.8.x バージョンにアップグレードした後で、Identity Applications ダッシュボードにログインできなくなります。この問題は、Identity Applications のアップグレード中に、アイデンティティボールトのトラストストアパスが適切なキーストア (cacerts) ファイルの場所に更新されない場合に発生します。次の例外が catalina.out ファイルに記録されます。 com.netiq.idm.auth.oauth.AuthenticationCommunicationException: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path validation failed: sun.security.validator.ValidatorException: TrustAnchor with subject "CN=***, OU=idm, O=***, L=***, ST=***, C=**" is not a CA certificate" Identity Applications は、<install_path>\Common\JRE に設定された JAVA_HOME 環境変数を使用します。トラストストアパスが JAVA_HOME で cacerts ファイルに設定されていない場合、SSL 通信は失敗し、「TrustAnchor」に関連する SSL エラーが発生します (トラストアンカーは SSL 証明書の拡張 Java セキュリティチェックとして使用されます)。	この問題を解決するには、次のアクションを実行してください。 1. Tomcat サービスを停止します。 2. Identity Applications サーバにログインし、<install_path>\idm\apps\configupdate にある configupdate ユーティリティを起動します。 3. [ユーザアプリケーション] タブで、**[Identity Vault Certificates (アイデンティティボールト証明書)]** に移動し、**[Truststore path (トラストストアパス)]** が <install_path>\Common\JRE\lib\security\cacerts に設定されていることを確認します。 4. Tomcat サービスを開始します。

項目	推奨されるアクション
分散環境の Identity Manager を 4.8.1 バージョンにアップグレードした後で、Identity Applications へのログインに失敗します。以下のようなエラーメッセージが表示されます。 Your login process did not complete successfully. Identity Applications にログインするには、Identity Applications と OSP 間のセキュアな接続を確立するためのトラストアンカー証明書が必要です。トラストアンカー証明書には、サブジェクトタイプが CA に設定された基本制約拡張が含まれている必要があります。Identity Manager は、プロパティ jdk.security.allowNonCaAnchor を使用して、証明書のトラストアンカーを検証します。デフォルトでは、このプロパティは false に設定されています。したがって、トラストアンカーが証明書で見つからない場合は、Identity Applications と OSP 間の接続を確立することができず、ログインに失敗します。また、idm-osp.log ファイルで次の例外に気づくでしょう。 sun.security.validator.ValidatorException: TrustAnchor with subject "CN=***, L=***, O=***" is not a CA certificate	この問題を解決するには、次の条件のいずれかを満たす必要があります。 ◆ Identity Applications と OSP 間のセキュアな接続を確立するために使用される証明書は、適切な基本制約拡張を含む信頼できる CA 証明書であることを確認します。 ◆ クライアントによって信頼される自己署名証明書およびカスタム証明書の場合、基本制約拡張を含まない CA 以外の証明書を許可するように、プロパティ jdk.security.allowNonCaAnchor を変更できます。次のアクションを実行して、Java セキュリティ設定を変更します。 1. C:\NetIQ\idm\apps\jre\lib\security\java.securityディレクトリに移動します。 2. プロパティ jdk.security.allowNonCaAnchor=true の値を設定します。 3. ファイルを保存します。
Identity Applications 4.8.1 バージョンにアップグレードした後で、Identity Applications ダッシュボードで許可の要求中に、フォームを開くことができません。	この問題を解決するには、次の手順を実行してください。 1. キーボードで <Windows> + <R> キーを押して、「services.msc」と入力し、**[OK]** を選択して、Windows サービスインタフェースを開きます。 2. サービス名、**[NetIQ Nginx Service]** と **[NetIQ IGA Form Renderer Service]** を検索します。サービスを右クリックして、**[Restart (再起動)]** オプションを選択します。 Identity Applications は Identity Applications ダッシュボードでフォームをレンダリングするために NGNIX サービスを使用します。
Identity Applications または Identity Reporting を 4.8 バージョンにアップグレードすると、コントロールパネルに PostgreSQL の複数のエントリが表示されます。	コントロールパネルから以前のバージョンの PostgreSQL をアンインストールします。

項目	推奨されるアクション
アンインストールプロセスが未完了と報告されるが、ログファイルには何もエラーが表示されない。	インストールファイルがデフォルトで保存される netiq ディレクトリがプロセス中に削除されていません。このディレクトリは、コンピュータから NetIQ ソフトウェアをすべて削除している場合は削除できます。
Identity Manager をアップグレードした後で、次のプロパティが ism-configuration.properties ファイルに追加されます。 com.netiq.idm.osp.ldap.admin-dn = cn=admin,ou=sa,o=system	ism-configuration.properties ファイルのプロパティをコメントアウトして、Tomcat を再起動します。機能が損なわれることはないからです。
Identity Manager をアップグレードすると、展開に SSPR がない場合でも、次の SSPR プロパティが ism-configuration.properties ファイルに追加されます。 com.netiq.sspr.redirect.url = https://___SSPR_IP___:___SSPR_TOMCAT_HTTPS_PORT___/sspr/public/oauth	ism-configuration.properties ファイルのプロパティをコメントアウトして、Tomcat を再起動します。機能が損なわれることはないからです。

項目	推奨されるアクション
Identity Manager アップグレードの後で、Tomcat を起動できません。Tomcat ログにはいくつかの例外があり、ワークフローエンジンとアイデンティティボールト間で通信障害が発生しています。	1. iManager にログインします。 2. **[Roles and Tasks (役割とタスク)]** > **[NetIQ Certificate Access (NetIQ 証明書アクセス)]** > **[Server Certificates (サーバ証明書)]** の順に移動します。 3. **[SSL CertificateDNS (SSL 証明書 DNS)]** チェックボックスをオンにして、**[エクスポート]** をクリックします。 4. **[証明書]** ドロップダウンリストで、［SSL CertificateDNS］を選択します。 5. **[Export private key (秘密鍵のエクスポート)]** チェックボックスをクリアします。**[Export format (エクスポート形式)]** が *DER* に設定されていることを確認します。 6. **[次へ]** > **[Save the exported certificate (エクスポートされた証明書の保存)]** をクリックして、システムに証明書をダウンロードします。 7. Identity Applications サーバにログインします。 8. Tomcat を停止します。 9. C:\NetIQ\Common\JRE\bin\ ディレクトリに移動して、次のコマンドを使用して、証明書を idm.jks ファイルにインポートします。 <Installed_path>\NetIQ\Common\JRE\bin\keytool -import -trustcacerts -alias <certificate_alias_name> -keystore <idm.jks> -file <certificate_file_downloaded> 10. Tomcat を再起動します。
Identity Manager を 4.7.4 から 4.8 にアップグレードした後で、Tomcat サービスが起動せず、ログファイルにエラーが報告されません。この問題は、igaworkflow データベースの afenginestate テーブルでハートビートタイマーが適切に更新されていないときに発生します。	この問題を解決するには、pgAdmin などのデータベース管理ツールにログインします。次のクエリを実行して、igaworkflow データベースの afenginestate テーブルのハートビートタイマーを手動で更新します。 update afenginestate set heartbeat=now()::timestamp;

ログインのトラブルシューティング

次の表に、発生する可能性のある問題とそれを解決するための推奨されるアクションを示します。問題が続く場合は、NetIQ の担当者にお問い合わせください。

項目	推奨されるアクション
Identity Applications と Identity Reporting が同じサーバにインストールされ、<reporting install folder>\bin ディレクトリにある設定更新ユーティリティを使用して設定変更を実行する場合は、Identity Manager ダッシュボードが起動に失敗します。次のエラーが catalina.out ログファイルで報告されます。 EboPortalBootServlet [RBPM] +++++WARNING!!!! : This portal application context, IDMProv, does not match the portal.context property set in the PortalService-conf/config.xml file.Only one portal per database is allowed.Data has been loaded using the previous portal context.To correct this you must revert back to the previous portal name of, NoCacheFilter, please consult the documentation.	設定変更については、C:\NetIQ\idm\apps\UserApplication ディレクトリにある設定更新ユーティリティを使用します。
大規模環境に (200 万オブジェクトを超える) ユーザがログインできない	eDirectory マスタとレプリカサーバの両方でルールセットを Value として指定して mail(Internet Mail Address) 属性のインデックスを追加します。
アイデンティティアプリケーションページからサインアウトする場合、SSPR に 5053 ERROR_APP_UNAVALIABLE エラーが表示される。	このエラーは無視します。機能が損なわれることはないからです。
Identity Applications への最初のログイン時に本人確認の回答が表示されない .	1. SSPR サーバに、FQDN を使用して作成された証明書があることを確認します。 2. Identity Application サーバにログインし、ConfigUpdate ユーティリティ (<installation_path>\apps\UserApplication) を起動します。 3. **[SSO クライアント] > [セルフサービスパスワードリセット]** の順に移動して、設定が正しいことを確認します。 SSPR を別のサーバにインストールした場合は、SSPR 証明書が /netiq/idm/apps/tomcat/conf の Identity Applications サーバにある idm.jks にインポートされていることを確認します。

項目	推奨されるアクション
SSPR URL にアクセスする際にブラウザに空のページが表示される .	これは、SSPR が OSP で適切に設定されていない場合に発生します。SSPR ログに次の情報が表示されます。 `2018-01-24T22:24:02Z, ERROR, oauth.OAuthConsumerServlet, 5071 ERROR_OAUTH_ERROR (unexpected error communicating with oauth server: password.pwm.error.PwmUnrecoverableException: 5071 ERROR_OAUTH_ERROR (io error during oauth code resolver http request to oauth server: Certificate for <IP> doesn't match any of the subject alternative names: [IP]))` 1. OSP が実行されている Tomcat サーバに、FQDN を使用して作成された有効な証明書があることを確認します。Identity Applications サーバにログインし、ConfigUpdate ユーティリティを起動します。**[SSO クライアント] > [セルフサービスパスワードリセット]** の順に移動して、設定が正しいことを確認します。 2. OSP ログイン方法を上書きして SSPR にログインします。(たとえば、https://<sspr sserver ip>:<port>/sspr/private/Login?sso=false) 3. ページの右上隅にある **[Configuration Editor (環境設定エディタ)]** に移動します。 4. **[Configure Password (パスワードの設定)]** を指定し、**[Sign In (サインイン)]** をクリックします。 5. **[LDAP] > [LDAP ディレクトリ] > [デフォルト] > [接続]** の順に移動します。 6. LDAP 証明書が正しくない場合は、**[クリア]** をクリックします。 7. 証明書を再インポートするには、**[Import From Server (サーバからインポート)]** をクリックします。 8. **[設定] > [Single Sign On (SSO)Client (シングルサインオン (SSO) クライアント)] > [OAuth]** の順に移動して、**[OAUTH Web サービスサーバ証明書]** の下にある証明書が正しいことを確認します。 9. 証明書が正しくない場合は、**[クリア]** をクリックします。 10. 証明書を再インポートするには、**[Import From Server (サーバからインポート)]** をクリックします。

SSPR のページ要求エラーのトラブルシューティング

次の表に、発生する可能性のある問題とそれを解決するための推奨されるアクションを示します。問題が続く場合は、NetIQ の担当者にお問い合わせください。

項目	推奨されるアクション
SSPR によって、ページの順序が異なるというページ要求エラーが報告される この問題は、SSPR ページで [戻る] ボタンをクリックするときに発生します。SSPR エラーログに、以下のような不正な順序に関するメッセージが記載されます。 `ERROR, password.pwm.servlet.TopServlet, 5035 ERROR_INCORRECT_REQUEST_SEQUENCE (expectedPageID=3, submittedPageID=4, url=<some sspr url>`	[SSPR Configuration Manager (SSPR 設定マネージャ)] > [設定] > [セキュリティ] > [Web Security (Web セキュリティ)] の順に選択してから、[戻る] ボタンの検出を無効にします。 **注 :** この設定を変更してもエンドユーザには影響しません。

Identity Applications への認証時またはログイン時に発生する一般的な問題については、『*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*』を参照してください。

Windows 2016 で .NET リモートローダが起動しない問題のトラブルシューティング

次の表に、発生する可能性のある問題とそれを解決するための推奨されるアクションを示します。問題が続く場合は、NetIQ の担当者にお問い合わせください。

項目	推奨されるアクション
これはランダムな問題です。.NET リモートローダのコマンドプロンプトのフォント設定がホストオペレーティングシステムのデフォルト設定と異なる場合に発生する可能性があります。	HKEY_CURRENT_USER\Console レジストリキーを削除してシステムのデフォルト設定に一致するようにコマンドプロンプト設定を変更し、サーバを再起動します。

Azure 展開でフォームをロードするときの 502 不正なゲートウェイのトラブルシューティング

次の表に、発生する可能性のある問題とそれを解決するための推奨されるアクションを示します。問題が続く場合は、NetIQ の担当者にお問い合わせください。

項目	推奨されるアクション
IDM 4.8 コンポーネントを Azure 環境に展開した後、次のようになります。IDM ダッシュボードで、ヘルプデスクチケットをクリックするか、タスクを承認しようとすると、次のエラーが表示される場合があります。 `502 - Web server received an invalid response while acting as a gateway or proxy server.`	この問題を解決するには、次の手順を実行します。 1. システムの Nginx\conf の場所に移動します。 例 : C:\NetIQ\Common\Nginx\conf 2. nginx.conf ファイルで、次のようにします。 a. 次の行 (error_page 502 /502.html;) の下に **error_page 404 =200 /404.html** を追加します。 b. **proxy_intercept_errors off;** を proxy_intercept_errors on; に設定します。 3. Services.msc から、NetIQ Nginx Service を再起動します。

IX 高可用性のための Identity Manager の展開

高可用性により、データ、アプリケーション、サービスなどの重要なネットワークリソースを効率的に管理できます。NetIQ では、VMWare Vmotion など、クラスタリングまたは Hypervisor クラスタリングを介した Identity Manager ソリューションの高可用性をサポートしています。高可用性環境を計画する際には、次の考慮事項が適用されます。

- 高可用性環境には次のコンポーネントをインストールできます。
  - 識別ボールト
  - Identity Manager エンジン
  - リモートローダ
  - Identity Reporting を除く、識別情報アプリケーション
- アイデンティティボールトをクラスタ環境で実行する場合は、Identity Manager エンジンもクラスタ化されます。

注 : Identity Manager は、Identity Vault と Identity Applications の間の LDAP または LDAPS 通信の負荷分散をサポートしていません。

参照する情報 ...	代わりの手段 ...
Identity Manager コンポーネントのサーバ設定の決定	『NetIQ Identity Manager Overview and Planning Guide』の「*High Availability Configuration*」を参照してください。
クラスタ内のアイデンティティボールトの実行	Identity Manager のクラスタ展開ソリューションのサンプル 『*NetIQ eDirectory Installation Guide*』の「Deploying eDirectory on High Availability Clusters」
クラスタ内の識別情報アプリケーションの実行	Identity Applications のクラスタ展開ソリューションのサンプル

お客様の Identity Manager 環境における高可用性と障害復旧の実装に関する詳しい情報は、NetIQ テクニカルサポート (https://www.netiq.com/support/) にお問い合わせください。

この次の章では、高可用性環境で Identity Manager コンポーネントをインストールおよび設定する手順を説明します。

- 247 ページの第 19 章「クラスタ環境における Identity Manager のインストールの準備」
- 251 ページの第 20 章「Identity Manager のクラスタ展開ソリューションのサンプル」
- 253 ページの第 21 章「Identity Applications のクラスタ展開ソリューションのサンプル」

19 クラスタ環境における Identity Manager のインストールの準備

- 前提条件
- 識別情報アプリケーションで使用するクラスタの準備

前提条件

- 識別ボールト
- 識別情報アプリケーション
- Identity Applications のデータベース

識別ボールト

NetIQ では、クラスタ環境に識別ボールトをインストールする前に、次の考慮事項を確認することをお勧めします。

- クラスタリングソフトウェアがインストールされている2つ以上のWindowsサーバが必要です。
- すべての識別ボールトおよび NICI データを格納するための十分なディスク容量を持つ、クラスタソフトウェアがサポートしている外部共有ストレージが必要です。
  - 識別ボールト DIB は、クラスタ共有ストレージに存在している必要があります。識別ボールトの状態データは、サービスを現在実行しているクラスタノードで使用できるように、共有ストレージに配置する必要があります。
  - 各クラスタノード上のルート識別ボールトインスタンスは、共有ストレージの DIB を使用するよう設定する必要があります。
  - さらに、共有 NICI (NetIQ International Cryptographic Infrastructure) データを共有して、サーバ固有のキーがクラスタノード間で複製されるようにすることも必要です。すべてのクラスタノードが使用する NICI のデータは、クラスタ共有ストレージに配置する必要があります。
  - NetIQ では、他のすべての eDirectory 設定およびログデータを共有ストレージに格納することをお勧めします。
- 仮想 IP アドレスが必要です。
- (状況によって実行)識別ボールトのサポート構造としてeDirectoryを使用している場合、nds-cluster-config ユーティリティでは、ルート eDirectory インスタンスの設定のみがサポートされます。クラスタ環境内での eDirectory の複数インスタンスの環境設定と、eDirectory の非ルートインストールはサポートされていません。

クラスタ環境内におけるアイデンティティボールドのインストールの詳細については、『*NetIQ eDirectory Installation Guide*』の「Deploying eDirectory on High Availability Clusters」を参照してください。

識別情報アプリケーション

Tomcat がサポートする環境に識別情報アプリケーション用のデータベースをインストールできますが、次の検討事項があります。

- クラスタには、固有のクラスタパーティション名、マルチキャストアドレス、およびマルチキャストポートが必要です。固有の識別子を使用して複数のクラスタを分離することによって、パフォーマンスの問題や異常な動作の発生を防ぎます。
  - クラスタの各メンバーで、識別情報アプリケーションのデータベースの待ち受けポートのポート番号として同一の値を指定する必要があります。
  - クラスタの各メンバーで、識別情報アプリケーションのデータベースをホストするサーバのホスト名または IP アドレスとして同一の値を指定する必要があります。
- クラスタ内のサーバの時刻を同期化する必要があります。サーバの時刻が同期していない場合、セッションタイムアウトが早期に発生し、HTTP セッションのフェールオーバーが正しく機能しない可能性があります。
- 同一ホストでは、複数のブラウザタブまたは複数のブラウザセッションで複数のログインを使用しないことをお勧めします。一部のブラウザはすべてのタブとプロセス間で cookie を共有します。そのため、複数のログインを行うと、(1 台のコンピュータを複数ユーザが共有することで認証機能に予期しない動作が発生するおそれがあるだけでなく) HTTP セッションのフェールオーバーの際に問題が発生する可能性があります。
- クラスタノードは同じサブネットに存在しています。
- フェールオーバープロキシまたは負荷分散ソリューションは、別のコンピュータにインストールされています。

Identity Applications のデータベース

データベースクラスタリングは、個々のデータベースサーバの機能です。クラスタリングは本製品の機能とは無関係なので、NetIQ はどのクラスタ化データベース設定についても公式なテストを実行していません。したがって、次の警告付きで、クラスタ化データベースサーバをサポートします。

- デフォルトで、最大接続数は 100 に設定されます。この値は、クラスタ内のワークフロー要求を処理するには小さすぎる場合があります。次の例外が表示される場合があります。

  ```
  (java.sql.SQLException: Data source rejected establishment of
  connection, message from server: "Too many connections."
  ```

  最大接続数を増やすには、my.cnf ファイルにある max_connections 変数をより高い値に設定してください。

- クラスタ化データベースサーバの一部の機能または側面を無効にする必要がある場合があります。たとえば、トランザクションレプリケーションは、重複キーを挿入しようとしたときに制約違反になるので、特定のテーブルでは無効にする必要があります。
- クラスタ化データベースサーバのインストール、設定、または最適化について、クラスタ化データベースサーバへの弊社製品のインストールも含めて、支援を提供することはありません。
- クラスタ化データベース環境で弊社製品を使用する際に問題が発生した場合は、その解決に向けて最善の努力を尽くします。複雑な環境におけるトラブルシューティング方法の多くは、問題を解決するために連携作業を必要とします。NetIQ は、自社製品の分析、プラニング、およびトラブルシューティングを実行するための専門知識を提供します。他のサードパーティ製品の分析、プラニング、およびトラブルシューティングを実行するための専門知識は、お客様から提供していただく必要があります。NetIQ 製品の問題とクラスタ設定の潜在的な問題を切り分けるために、お客様には問題の再現または非クラスタ化環境におけるコンポーネントの動作の分析をお願いします。

識別情報アプリケーションで使用するクラスタの準備

識別情報アプリケーションは HTTP のセッションレプリケーションとセッションフェールオーバーをサポートします。つまり、ノードでセッション処理中にノードにエラーが発生した場合、そのセッションは中断されることなく、同じクラスタ内の別のサーバ上で再開されます。クラスタに識別情報アプリケーションをインストールする前に、環境を準備する必要があります。

- 249 ページの 「Tomcat 環境のクラスタグループの理解」
- 249 ページの 「ワークフローエンジン ID のシステムプロパティの設定」
- 250 ページの 「クラスタ内の各ユーザアプリケーションでの同じマスタキーの使用」

Tomcat 環境のクラスタグループの理解

ユーザアプリケーションクラスタグループは UUID 名を使用して、ユーザがサーバに追加する他のクラスタグループと競合するリスクを最小限に抑えます。ユーザアプリケーション管理機能を使用して、ユーザアプリケーションクラスタグループの環境設定を変更できます。クラスタ設定の変更がサーバノードで有効になるのは、そのノードを再起動した場合のみです。

ワークフローエンジン ID のシステムプロパティの設定

クラスタ内で識別情報アプリケーションをホストする各サーバでは、ワークフローエンジンを実行できますクラスタとワークフローエンジンのパフォーマンスを保証するために、クラスタ内のすべてのサーバが同じパーティション名とパーティション UDP グループを使用する必要があります。また、クラスタ内の各サーバを起動する際に一意のワークフロー

エンジン ID を指定する必要があります。なぜなら、ワークフローエンジンのクラスタリングは、識別情報アプリケーションのキャッシュフレームワークとは独立して動作するからです。

ワークフローエンジンが適切に動作することを保証するには、Tomcat のシステムプロパティを設定する必要があります。

1 クラスタ内の識別情報アプリケーションサーバごとに、新しい JVM システムプロパティを作成します。
2 このシステムプロパティに com.novell.afw.wf.*engine-id* という名前を付けます。ここで、engine-id は一意な値です。

クラスタ内の各ユーザアプリケーションでの同じマスタキーの使用

識別情報アプリケーションは、マスタキーを使用して機密データを暗号化します。クラスタ内のすべての識別情報アプリケーションが同じマスタキーを使用する必要があります。このセクションでは、クラスタ内のすべての識別情報アプリケーションが同じマスタキーを使用することを保証する方法について説明します。

アイデンティティアプリケーションにおける機密データの暗号化の詳細については、『*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*』の「Encrypting Sensitive Identity Applications Data」を参照してください。

1 クラスタ内の 1 番目のノードにユーザアプリケーションをインストールします。
2 インストールプログラムの［セキュリティ - マスタキー］ウィンドウで、識別情報アプリケーションの新しいマスタキーが格納される master-key.txt ファイルの場所を書き留めます。デフォルトでは、このファイルはインストールディレクトリにあります。
3 クラスタ内の他のノードに識別情報アプリケーションをインストールします。
4 ［セキュリティ - マスタキー］ウィンドウで **[はい]** をクリックして、**[次へ]** をクリックします。
5 ［マスタキーのインポート］ウィンドウで、ステップ 2 で作成したテキストファイルからマスタキーをコピーします。

20 Identity Manager のクラスタ展開ソリューションのサンプル

このセクションでは、Windows 2016 プラットフォーム上のクラスタ環境に Identity Manager を設定する方法に関する段階的手順を記載します。

- 251 ページの 「前提条件」
- 251 ページの 「eDirectory クラスタでの NetIQ Identity Manager の設定」
- 252 ページの 「リモートローダのクラス化」

前提条件

Windows 2016 のクラスタ環境で実行されている Identity Vault 9.2。eDirectory クラスタの設定の詳細については、『*NetIQ eDirectory Installation Guide*』の「Clustering eDirectory Services on Windows」を参照してください。

注 : 識別ボールトは、複数のクラスタノードを使用する負荷分散をサポートしていません。eDirectory クラスタリングは、フェールオーバー機能を実現することのみを目的としています。

---

eDirectory クラスタでの NetIQ Identity Manager の設定

このセクションは、eDirectory クラスタがすでに設定されていることを前提としています。

次の手順を使用して、eDirectory クラスタ環境に Identity Manager を設定します。

1. **[クラスタマネージャ]** で、プライマリノード上の eDirectory クラスタ化役割の優先度を **[No Auto Start (自動起動しない)]** に設定します。
2. セカンダリノードを停止します。
3. Identity Manager インストールウィザードで、**[メタディレクトリサーバ]** オプションを選択して、プライマリノード上に Identity Manager エンジンをインストールします。

   重要 : ローカルストレージ上に Identity Manager エンジンをインストールしていることを確認します。

   ---
4. Identity Manager インストールウィザードは、インストール中に eDirectory クラスタ役割を停止します。この役割が停止されると、この役割のステータスが失敗と表示される場合があります。インストール後に、**[クラスタマネージャ]** から eDirectory クラスタ役割を起動します。

5 eDirectory クラスタ化役割に必要な優先度を設定し、セカンダリノードをアクティブにします。

6 DCLUSTER_INSTALL コマンドを使用して、セカンダリノード上に Identity Manager エンジンをインストールします。

例 : idm_install.exe -DCLUSTER_INSTALL="true"

リモートローダのクラス化

1 プライマリおよびセカンダリクラスタノード上にリモートローダをインストールします。

注 : 両方のプライマリおよびセカンダリノードに対して、リモートローダが同一の共有ストレージパスにインストールされていることを確認します。

---

2 (状況によって実行) リモートローダとのセキュア通信を使用している場合は、共有ストレージにすべての SSL 証明書が格納されます。

3 リモートローダクラスタ役割を作成する前に、リモートローダコンソールを開き、**[Remote Loader as a Windows Service (Windows サービスとしてリモートローダを使用)]** を選択します。

4 **[クラスタマネージャ] > [役割]** で、新しいリモートローダクラスタ役割を作成します。

役割に次の情報を指定します。

役割タイプ : 汎用サービス

サービスの選択 : Windows サービスとして登録されているリモートローダインスタンス。

名前 : クラスタ役割名

アドレス : 一意の IP アドレス

ストレージの選択 : 共有クラスタストレージ

重複するレジストリ設定 :

1. HKEY_LOCAL_MACHINE\SOFTWARE\Novell\RLConsole
2. HKEY_LOCAL_MACHINE\SOFTWARE\Novell\DirXML Remote Loader\Command port 8000

   クラスタ化するリモートローダインスタンスのレジストリパスを指定します。
3. HKEY_LOCAL_MACHINE\SOFTWARE\Novell\PassSync

注

- デフォルトで、各クラスタ役割は 1 つの Windows サービスのみを受け入れます。したがって、各リモートローダインスタンスに固有のコマンドポートおよび対応するレジストリパスを指定します。
- Active Directory ドライバのパスワードフィルタは Windows クラスタではサポートされていません。

---

21 Identity Applications のクラスタ展開ソリューションのサンプル

このセクションでは、サンプル展開で Tomcat アプリケーションサーバ上のクラスタ環境に Identity Applications を設定する方法に関する手順を記載します。

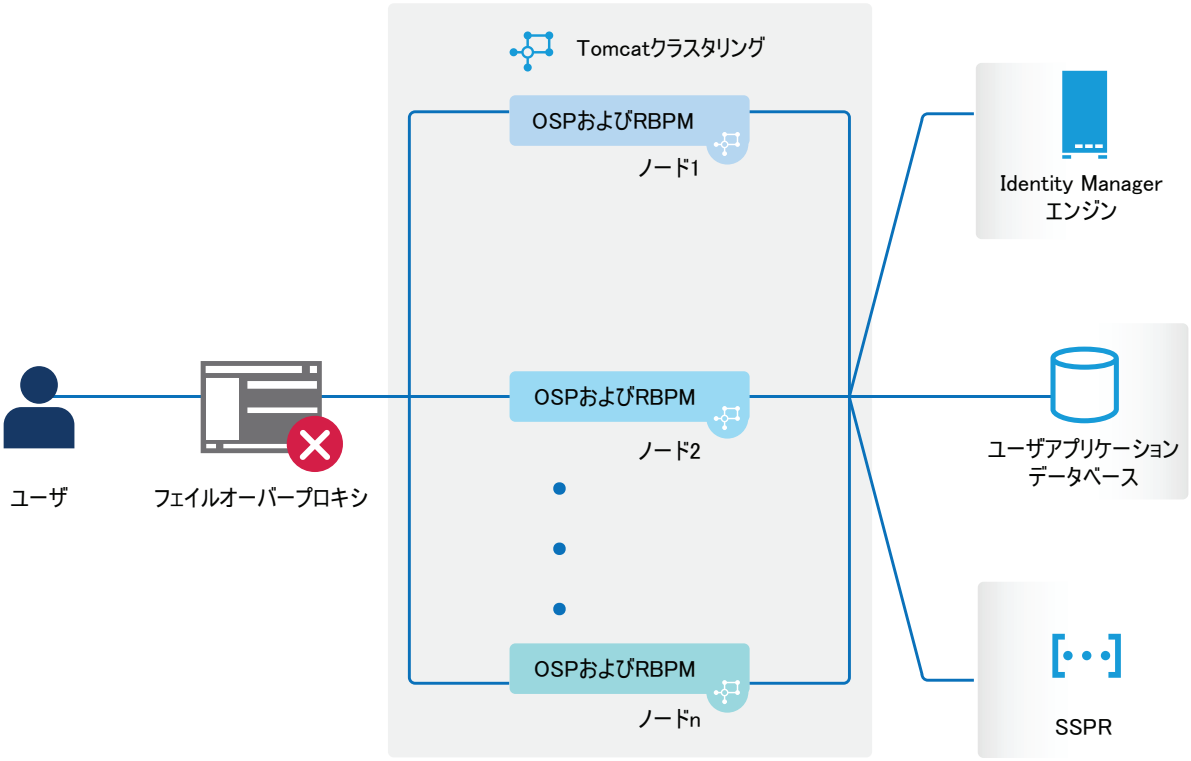
クラスタリングにより、いくつかのパラレルサーバ (クラスタノード) 上に識別情報アプリケーションを実行することができ、高可用性を実現できます。クラスタを構築するには、いくつかの Tomcat インスタンス (ノード) をグループ分けする必要があります。異なるサーバ間で負荷が分散され、サーバのいずれかで障害が発生した場合にも、識別情報アプリケーションに他のクラスタノードからアクセスできます。フェールオーバー用に、識別情報アプリケーションのクラスタを作成し、単一サーバとして機能するように設定できます。ただし、この設定には Identity Reporting は含まれません。

すべてのユーザ要求を処理し、それらをクラスタ内のサーバノードにディスパッチするロードバランサソフトウェアを使用することをお勧めします。ロードバランサは通常クラスタの一部で、クラスタ設定とともにフェールオーバーポリシーを理解しています。このため、ユーザは最適なソリューションを選択できます。

図 21-1 には、以下の前提条件を持つ 2 ノードクラスタのサンプル展開を示しています。

- すべての通信はロードバランサを介してルーティングされています。
- Identity Manager エンジンやユーザアプリケーションなどのコンポーネントは別のサーバにインストールされています。運用レベルの展開については、これが推奨されるアプローチです。
- eDirectory、Identity Manager エンジン、識別情報アプリケーション、Apache Tomcat アプリケーションサーバ、およびユーザアプリケーション用のデータベースのインストール手順に精通しています。
- OSP (One Single-Sign On Provider) およびユーザアプリケーションは同じクラスタノードにインストールされています。ただし、運用環境の異なるサーバ上に OSP をインストールできます。この場合、255 ページの 「インストール手順」で説明されるいつくかの設定の変更する必要があります。
- SSPR (Single Sign-On Password Reset) が別のコンピュータにインストールされています。運用レベルの展開については、これが推奨されるアプローチです。
- PostgreSQL はユーザアプリケーション用のデータベースとして使用されています。ただし、Oracle、SQL Server、または PostgreSQL などの、Identity Manager 4.8 でサポートされるデータベースのいずれかを使用できます。
- ユーザアプリケーションノードのすべてが eDirectory およびユーザデータベースの同じインスタンスと通信できます。要件に基づいて、ユーザアプリケーションインスタンスの数を増やすことができます。

図 21-1 クラスタ展開ソリューションのサンプル



注 : 2 ノードクラスタは、高可用を実現するために使われる最小環境設定です。ただし、このセクションのコンセプトは、ノードを追加することで、簡単にクラスタに拡張することができます。

段階的な設定を理解するのを支援するために、このサンプル展開がドキュメントの後続のセクションで参照されます。

前提条件

- Windows Server 2012、Windows Server 2012 R2、または Windows Server 2016 を実行する 2 つのサーバをノードとして使用。
- Identity Manager コンポーネントが最小バージョン 4.8 でインストールされている。Identity Manager 4.8 へのアップグレードについては、157 ページの第 11 章「Identity Manager コンポーネントのアップグレード」を参照してください。
- すべてのノードに同じアプリケーションサーバクロックがあります。これを確認にする最も簡単な方法は、NTP を使用して時間同期のために同一のネットワーク時間サーバを使用するようにノードを設定する方法です。
- クラスタノードは同じサブネットに存在します。
- フェールオーバープロキシまたは負荷分散ソリューションは、別のコンピュータにインストールされています。
- フォームのクラスタリングを実現するには、サーバ上のロードバランサの 2 つのインスタンス (一方は Identity Applications 用、他方はフォームレンダラ用) を起動します。

インストール手順

このセクションでは、Tomcat に識別情報アプリケーションの新しいインスタンスをインストールし、それをクラスタリング用に設定するための段階的な手順を説明します。

1. Identity Manager エンジンをインストールします。詳しい手順については、51 ページの「インストール手順」を参照してください。運用レベルの展開については、別のサーバ上に Identity Manager エンジンをインストールすることをお勧めします。
2. 識別情報アプリケーションの次のドライバを作成し、展開します。
   - ユーザアプリケーションドライバ
   - 役割とリソースサービスドライバ
3. Novel では、次の Identity Manager コンポーネントをインストールします。
   a. ユーザアプリケーション

      インストールプロセス中に、以下を設定します。

      i. **[Tomcat]** をアプリケーションサーバとして選択します。

      ii. **[PostgreSQL]** をデータベースプラットフォームとして選択します。

      注 : Identity Manager 4.8 がサポートするデータベースのすべてを使用できます。

      ---

      iii. 後続のページに必要なデータベースの詳細を提供します。

      iv. PostgreSQL サーバからクラスタ内のすべてのユーザアプリケーションノードにデータベースドライバ jar ファイル postgresql-9.4.1212.jar をコピーします。

      注 : Oracle や SQL Server などの他の Identity Manager 4.8 がサポートするデータベースを使用している場合は、データベースをインストールしているサーバからクラスタ内のすべてのユーザアプリケーションノードに各ドライバの jar ファイルをコピーしていることを確認します。詳細については、75 ページの「識別情報アプリケーションのデータベースの設定」を参照してください。

      ---

      v. コピーされたデータベースドライバ jar ファイルを参照して選択します。

      vi. 2 つのデータベースまたは既存のデータベース詳細ページで、**[新しいデータベース]** オプションを選択します。

      vii. ［Identity Manager Configuration (Identity Manager 設定)］ページで、**[ワークフローエンジン ID]** フィールドに固有の名前を入力します。たとえば、Engine1 for Node1 などの固有の名前を使用できます。

      viii. 新しいマスタキーを作成するには、［Security – Master Key (セキュリティ - マスタキー)］ページで、**[いいえ]** を選択します。

      識別情報アプリケーションは、マスタキーを使用して機密データを暗号化します。これはクラスタ内の識別情報アプリケーションの最初のインスタンスであるため、**[いいえ]** を選択して、新しいマスタキーを作成するようにインストールプログラムに指示する必要があります。クラスタ内で、ユーザアプリケーションのクラスタリングでは、ユーザアプリケーションのすべてのイ

ンスタンスが同じマスタキーを使用する必要があります。同じマスタキーが使用されるようにするには、これらのインスタンスの設定中に [はい] を選択して既存のキーをインポートします。

4. Node2 では、次のアクションを実行します。

   a. 便利なインストーラを使用して Tomcat をインストールします (インストールプロセス中に Tomcat のみを選択します)。

   b. OSP をインストールします。

      インストールプロセス中に、［認証の詳細］ページで Identity Manager エンジン (eDirectory) サーバの IP アドレスとポート番号を入力します。

   c. ユーザアプリケーションをインストールします。

      インストールプロセス中に、以下を設定します。

      i. [Tomcat] をアプリケーションサーバとして選択します。

      ii. [PostgreSQL] をデータベースプラットフォームとして選択します。

      注 : Identity Manager 4.8 がサポートするデータベースのすべてを使用できます。

      iii. インストール手順の後続のページで必要なデータベースの詳細を提供します。

      iv. データベースドライバ jar ファイル postgresql-9.4.1212.jar を PostgreSQL サーバから Node2 にコピーします。

      注 : Oracle や SQL Server などの他の Identity Manager 4.8 がサポートするデータベースを使用している場合は、データベースをインストールしているサーバからクラスタ内のすべてのユーザアプリケーションノードに各ドライバの jar ファイルをコピーしていることを確認します。

      v. コピーされたデータベースドライバ jar ファイルを参照して選択します。

      vi. 新しいデータベースまたは既存のデータベースの詳細ページで、[既存のデータベース] オプションを選択します。

      vii. ［Identity Manager Configuration (Identity Manager 設定)］ページで、[ワークフローエンジン ID] フィールドに固有の名前を入力します。たとえば、Engine2 for Node2 などの固有の名前を使用できます。

      viii. ［Security – Master Key (セキュリティ - マスタキー)］ページで新しいマスタキーを作成するには、[はい] を選択します。

      ユーザアプリケーションのクラスタリングでは、ユーザアプリケーションのすべてのインスタンスが同じマスタキーを使用する必要があります。同じマスタキーが使用されていることを確認するには、[はい] を選択して既存のキーをインポートします。このキーは、Node1 でユーザアプリケーションの最初のインスタンスがインストールされたときに作成されます。

      Node1 の C:\NetIQ\IDM\apps\tomcat\conf にある ism-configuration プロパティファイルからマスタキーを取得できます。マスタキーを含むパラメータは、com.novell.idm.masterkey です。

      ix. [インストール] をクリックして、インストールを完了します。

注 : 識別情報アプリケーションのインストールの詳細については、51 ページの 「インストール手順」を参照してください。

5. ロードバランササーバで、Identity Applications ポート番号を使用したロードバランサの一方のインスタンスと、すべてのクラスタノード用のフォームレンダラポート番号を使用したロードバランサの他方のインスタンスを起動します。次に例を示します。
   - ./balance 8543 apps1-au.edu.in:8543 ! apps2-au.edu.in:8543
   - .·/balance 8600 apps1-au.edu.in:8600 ! apps2-au.edu.in:8600
6. 別のコンピュータに SSPR をインストールします。

   インストールする前に、次の設定のメモを作成して、インストールプロセス中にそれを指定します。
   a. **[Tomcat]** をインストールします。インストール手順については、手順 4a を参照してください。
   b. **[SSPR]** をインストールします。

      SSPR インストール中に、次のアクションを実行します。
      i. アプリケーションサーバの接続ページで、**[Connect to external authentication server (外部認証サーバへの接続)]** を選択し、ロードバランサがインストールされているサーバの DNS 名を入力します。
      ii. ［認証の詳細］ページで、Identity Manager エンジンサーバの **[IP アドレス]** と **[ポート]** を入力します。CA 証明書のパスワードは changeit です。
   c. SSPR インストールが完了したら、SSPR (https://<IP>:<port>/sspr/private/config/ConfigEditor) を起動し、ログインします。**[Configuration Editor (環境設定エディタ)]** > **[設定]** > **[セキュリティ]**> **[Redirect Whitelist (ホワイトリストをリダイレクト)]** をクリックします。.
      i. **[Add value (値の追加)]** をクリックし、次の URL を指定します。

         https:<dns of the failover><port>/osp
      ii. 変更内容を保存します。
      iii. SSPR の設定ページで、**[設定]** > **[OAuth SSO]** をクリックし、ロードバランサソフトウェアがインストールされているサーバの DNS 名で IP アドレスを置き換えて、OSP リンクを変更します。
      iv. **[設定]** > **[アプリケーション]** をクリックし、ロードバランサソフトウェアがインストールされているサーバの DNS 名で IP アドレスを置き換えて、フォワードおよびログアウト URL を更新します。
   d. Node1 上の SSPR 情報を更新するには、C:\NetIQ\idm\apps\UserApplication\configupdate.bat にある設定ユーティリティを起動します。

      表示されるウィンドウで、**[SSO クライアント]** > **[Self Service Password Reset]** をクリックし、**[クライアント ID]**、**[パスワード]**、および **[OSP Auth redirect URL (OSP 認証リダイレクト URL)]** パラメータの値を入力します。

注 : これらのパラメータの値が Node2 で更新されていることを確認します。

7. クラスタノード上で次の設定タスクを実行します。
   a. すべてのクラスタノードの Tomcat を再起動します。
   b. ［パスワードの変更］リンクを変更するには、74 ページの 「分散環境またはクラスタ化環境におけるダッシュボードの SSPR リンクの更新」を参照してください。
   c. ［パスワードを忘れた場合］および［パスワードの変更］リンクが Node2 の SSPR IP アドレスで更新されていることを確認します。

   注 : ［パスワードの変更］および［パスワードを忘れた場合］リンクがすでに SSPR IP アドレスで更新されている場合、変更は必要ありません。

8. Node1 で、Tomcat を終了し、次のコマンドを使用して、ロードバランササーバの DNS 名を指定して、新しい osp.jks ファイルを生成します。

   C:\NetIQ\Common\JRE\bin\keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass <password> -keypass <password> -alias osp -validity 1800 -dname "cn=<loadbalancer IP/DNS>"

   例 : C:NetIQ\idm\apps\jre\bin\ -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass changeit -keypass changeit -alias osp -validity 1800 -dname "cn=mydnsname"

   注 : キーパスワードが OSP インストール中に入力したパスワードと同じであることを確認します。または、これをキーストアパスワードを含む設定更新ユーティリティを使用して変更することもできます。

9. (状況に応じて実行) osp.jks ファイルが変更で更新されているかどうかを確認するには、次のコマンドを実行します。

   C:\NetIQ\Common\JRE\bin\keytool -list -v -keystore osp.jks -storepass changeit

10. C:\NetIQ\idm\apps\osp\ にある元の osp.jks ファイルのバックアップをとり、新しい osp.jks ファイルをこの場所にコピーします。新しい osp.jks ファイルは、手順 8 で作成されています。
11. 配置されている新しい osp.jks ファイルを Node1 からクラスタの他のユーザアプリケーションノードにコピーします。
12. 各クラスタノード上で、
    a. C:\netiq\idm\apps\sites ディレクトリに移動して、ServiceRegistry.json ファイルを編集し、ロードバランサ詳細を追加します。

       ```
       {"serviceRegisteries":[{"serviceID":"IDM","restUrl":"https://<DNS of the load balancer>:8543/IDMProv"}]}
       ```

    b. C:\netiq\idm\apps\sites\ ディレクトリに移動して、config.ini ファイルを編集し、ロードバランサ DNS とポート番号を追加します。

       ```
       OSPIssuerUrl=https://<DNS of the load balancer>:8543/osp/a/idm/auth/oauth2
       OSPRedirectUrl=https://<DNS of the load balancer>:8600/forms/oauth.html
       ClientID=forms
       OSPLogoutUrl=https://<DNS of the load balancer>:8543/osp/a/idm/auth/app/logout
       ```

13. Node1 で設定ユーティリティを起動し、［ランディングページへの URL リンク］や［OAuth リダイレクト URL］などの URL 設定のすべてを［SSO クライアント］タブのロードバランサ DNS 名に変更します。

    a. 設定ユーティリティで変更を保存します。変更について ism-configuration properties ファイルを確認し、URL が Node 1 DNS およびポートを依然としてポイントしている場合は変更します。

    b. クラスタの他のすべてのノードでこの変更を反映させるには、Node1 からクラスタ内の他のユーザアプリケーションノードに、C:\NetIQ\IDM\apps\tomcat\conf にある ism-configuration properties ファイルをコピーします。

    注 : Node1 から、クラスタ内の他のノードに ism.properties ファイルをコピーしました。ユーザアプリケーションインストール中にカスタムインストールパスを指定した場合は、参照パスがクラスタノードの設定更新ユーティリティを使用して修正されていることを確認します。

    このシナリオでは、OSP とユーザアプリケーションのどちらも同じサーバにインストールされます。したがって、同じ DNS 名が URL をリダイレクトするために使用されます。

    OSP およびユーザアプリケーションが別のサーバにインストールされている場合は、OSP URL をロードバランサを参照する異なる DNS 名に変更します。OSP がインストールされるすべてのサーバに対してこれを実行します。これを行うと、すべての OSP 要求がロードバランサを介して OSP クラスタ DNS 名にディスパッチされます。これには、OSP ノードに別のクラスタがある必要があります。

    ---

14. /TOMCAT_INSTALLED_HOME/bin/ ディレクトリにある setenv.sh ファイルで次のアクションを実行します。

    a. mcast_addr バインディングが成功するためには、JGroup で preferIPv4Stack プロパティが **[true]** に設定されている必要があります。これを実行するには、すべてのノードの setenv.sh ファイルに JVM プロパティ「-Djava.net.preferIPv4Stack=true」を追加します。

    b. Node1 の setenv.sh ファイルに「-Dcom.novell.afw.wf.Engine-id=Engine1」を追加します。同様に、クラスタ内の各ノードに固有のエンジン名を追加します。たとえば、Node2 の場合、Engine2 として既存の名前を追加できます。

15. ユーザアプリケーションでクラスタリングを有効にします。

    a. Node1 で Tomcat を起動します。

    他のサーバを起動しないでください。

    b. ユーザアプリケーション管理者としてユーザアプリケーションにログインします。

    c. **[環境設定]** > **[キャッシングとクラスタ]** オプションをクリックします。

    ユーザアプリケーションに［キャッシュマネージャー］ページが表示されます。

    d. **[クラスタキャッシュ環境設定]** をクリックし、**[有効なクラスタ]** プロパティに対して **[True]** を選択します。

    e. **[保存]** をクリックします。

    f. Tomcat を再起動します。

注 : [Enable Local settings (ローカル設定を有効化)] を選択している場合は、クラスタ内の各サーバについてこの手順を繰り返します。

ユーザアプリケーションクラスタは、デフォルト UDP を使用してノード間のキャッシュ同期に JGroups を使用します。TCP を使用するようにこのプロトコルを変更する場合は、Configuring User Application to use TCP を参照してください。

16. クラスタリングのパーミッションインデックスを有効にします。詳細については、261 ページの 「クラスタリングのパーミッションインデックスの有効化」を参照してください。
17. Tomcat クラスタを有効にします。

    Tomcat server.xml ファイルを /TOMCAT_INSTALLED_HOME/conf/ から開き、すべてのクラスタノード上でこのファイルのこの行をコメント解除します。

    <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>

    高度な Tomcat クラスタリング設定の場合、Apache マニュアルの Web サイトの手順を実行します。
18. すべてのノードで Tomcat を再起動します。
19. クラスタリング用のユーザアプリケーションドラバを設定します。

    クラスタ化された環境で、ユーザアプリケーションの複数のインスタンスとともに単一のユーザアプリケーションドライバを使用できます。ドライバには、アプリケーション固有のさまざまな情報 (例 : ワークフロー環境設定情報、クラスタ情報) が保持されています。ドライバはクラスタのディスパッチャまたはロードバランサのホスト名または IP アドレスを使用するように設定する必要があります。

    a. アイデンティティボールトを管理する iManager のインスタンスにログインします。
    b. ナビゲーションフレームで、**[Identity Manager]** を選択します。
    c. **[Identity Manager の概要]** を選択します。
    d. ユーザアプリケーションドライバのドライバセットを含む Identity Manager の概要を表示するには、検索ページを使用します。
    e. ドライバアイコンの右上隅にある円形のステータスインジケータをクリックします。
    f. **[プロパティの編集]** を選択します。
    g. **[ドライバパラメータ]** で、**[ホスト]** をロードバランサのホスト名または IP アドレスに変更します。
    h. **[OK]** をクリックします。
    i. ドライバを再起動します。
20. 役割とリソースのサービスドライバの URL を変更するには、19a から 19f までの手順を繰り返し、**[ドライバ環境設定]** をクリックして、**[ユーザアプリケーションの URL]** をロードバランサ DNS 名で更新します。
21. セッションの粘着度がユーザアプリケーションノード用にロードバランサソフトウェアで作成したクラスタに対して有効になっていることを確認します。

ほとんどのロードバランサは、HTTP サーバが稼働およびリスンしているかどうかを判断するためのヘルスチェック機能を提供します。ユーザアプリケーションには、ロードバランサに HTTP ヘルスチェックを設定するために使用できる URL が含まれます。URL は次のとおりです。

http://<NodeIP>:port/IDMProv/jsps/healthcheck.jsp

クラスタリングのパーミッションインデックスの有効化

このセクションでは、クラスタリングのパーミッションインデックスの有効化手順について説明します。

1. クラスタの 1 番目のノードで iManager にログインし、**[View Objects (オブジェクトの表示)]** に移動します。
2. **[システム]** の下で、**[ユーザアプリケーションドライバ]** を含むドライバセットに移動します。
3. **[AppConfig]** > **[AppDefs]** > **[環境設定]** の順に選択します。
4. XMLData 属性を選択し、com.netiq.idm.cis.clustered プロパティを **[true]** に設定します。

   次に例を示します。

   <property>

   <key>com.netiq.idm.cis.clustered</key>

   <value>true</value>

   </property>
5. **[OK]** をクリックします。