NetIQ® Identity Manager
統合インストールガイド

2017 年 2 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) 2017 NetIQ Corporation. **All rights reserved.**

目次

本書およびライブラリについて

『*統合インストールガイド*』では、統合インストールプログラムを使用して NetIQ Identity Manager (Identity Manager) 製品をインストールする方法について説明します。本ガイドでは多くの箇所で、スタンドアロンインストールプログラムを使用して Identity Manager をインストールする方法を詳しく説明した『NetIQ Identity Manager セットアップガイド』を参照しています。

本書の読者

本書には、自社組織向けの識別情報管理ソリューションを評価する目的で Identity Manager をインストールする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が記載されています。

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、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。より迅速な情報、有益なリソースへの役立つリンク、NetIQ エキスパートとのやり取りを提供する NetIQ Communities は、信頼のおける IT 投資が持つ可能性を完全に実現するために必要な知識を習得するために役立ちます。詳細については、community.netiq.com を参照してください。

1 はじめに

NetIQ は、ご使用の環境に Identity Manager をインストールして設定する方法を 2 つ用意しています。1 つは統合インストールソリューションで、もう 1 つは各コンポーネントまたはコンポーネント群のインストールプログラムです。「統合インストール」プログラムでは、多くの設定にデフォルト値を使用してすべてのコンポーネントをインストールおよび設定できます。これらの設定は、通常のインストールに役立ちます。NetIQ では、インストール用のこれらの設定を保持しておくことをお勧めします。

統合インストールプログラムを使用して、1 つの Linux または Windows コンピュータ上にすべてのコンポーネントをインストールすることができます。ただし、Linux コンピュータ上にのみインストールできる NetIQ Sentinel Log Management for Identity Governance and Administration コンポーネントは除きます。「スタンドアロンインストール」プログラムでは、1 つ以上の Identity Manager コンポーネントを個別にインストールしたり、大半の設定をカスタマイズしたりできます。

次の作業に進む前に、さまざまな Identity Manager コンポーネントについて確実に理解してください。詳細については、『*NetIQ Identity Manager セットアップガイド*』の「Identity Manager のコンポーネントの概要」を参照してください。

1.1 統合インストールプログラムとスタンドアロンインストールプログラムの違いの理解

統合インストールプログラムを使用するか、それともスタンドアロンインストールプログラムの 1 つを使用するかを判断するには、次の情報を使用します。

統合インストールプログラム

Identity Manager を評価する場合や、テスト環境を構築する場合は、このプログラムを使用することをお勧めします。このプログラムでは、必要なすべてのコンポーネントのインストールが 1 つのインストールプロセスにまとめられています。統合インストールプログラムの機能は次のとおりです。

- Red Hat Enterprise Linux (RHEL) 7.3 以降、SUSE Linux Enterprise Server (SLES) 12 SP1 以降、または Windows 2012 R2 プラットフォーム上で実行できます。
- 大部分の設定にデフォルト値を適用する
- すべてのコンポーネントを単一のサーバ環境にインストールする
- サポートされているすべてのオペレーティングシステムに対して PostgreSQL 9.6.x を使用する
- サポートされているすべてのオペレーティングシステムに対して Apache Tomcat を使用する

重要 : 統合インストールプログラムを使用する際には、以下の制限事項が適用されます。

- RHEL 6.x および SLES 11 以降のプラットフォーム上で Identity Manager をインストールするために使用することはできません。

代わりに、個別のコンポーネントインストーラを使用して、これらのプラットフォームにサポートされている Identity Manager コンポーネントをインストールします。どのプラットフォームでどのコンポーネントがサポートされているかについては、『*NetIQ Identity Manager セットアップガイド*』を参照してください。

- コンソールモードでは実行できない
- Identity Manager Standard Edition のインストールに使用できない
- クラスタ環境では使用できない
- 運用環境では使用できない

スタンドアロンインストールプログラム

このオプションは、識別情報管理ソリューションのステージング環境または運用環境で使用することをお勧めします。スタンドアロンインストールプログラムでは、より柔軟に使用環境を設定できます。このプロセスの機能は次のとおりです。

- コンポーネントの設定をカスタマイズできる
- 分散環境にインストールできる
- 複数のデータベースプラットフォームをサポートする
- 複数のアプリケーションサーバをサポートする
- サポートされる運用環境を構築する

スタンドアロンインストールプロセスの使用の詳細については、『NetIQ Identity Manager セットアップガイド』を参照してください。

1.2 統合インストールプロセスの理解

統合インストールプロセスでは、さまざまな Identity Manager コンポーネントのインストールプログラムが内部で実行されます。インストーラは、単一サーバ環境における最も一般的な設定に対してデフォルト値を提供します。これらの設定は通常のインストールで使用されます。NetIQ では、インストール用のこれらの設定を保持しておくことをお勧めします。分散された環境に Identity Manager コンポーネントをインストールする場合、各コンピュータ上で統合インストールプログラムを実行し、どれをインストールするかを指定します。

インストールプロセスの開始時にパスワードを指定することで、インストールするコンポーネントのすべてのパスワードパラメータにそのパスワードを適用できます。インストールされたコンポーネントの設定にはデフォルト設定が適用されます。インストールプロセスの一部としてデフォルト設定を変更することも、後で設定を変更することもできます。たとえば、プロセスを開始する際に、すべてのパスワード値に適用するパスワードを指定できます。

注 : 統合インストールプロセスを使用して、既存のインストール環境をアップグレードすることはできません。

以降のセクションでは、このプロセスでインストールできるコンポーネントとそれらのデフォルト設定について説明します。

1.2.1 Identity Manager サーバ

このオプションは次の Identity Manager コンポーネントをインストールします。

- 識別ボールト
- Identity Manager エンジン
- iManager プラグイン
- Identity Manager ドライバ
- リモートローダ
- ファンアウトエージェント

注 : JDBC Fan-Out ドライバにのみ適用されます。このオプションが選択されている場合、インストールプログラムにより、JDBC Fan-Out ドライバ用のファンアウトエージェントがインストールされます。JDBC Fan-Out ドライバはファンアウトエージェントを使用して、複数の JDBC Fan-Out ドライバのインスタンスを作成します。ファンアウトエージェントは、Fan-Out ドライバの接続オブジェクトの設定に基づいて JDBC ドライバインスタンスをロードします。詳細については、『*NetIQ Identity Manager Driver for JDBC Fan-Out Implementation Guide*』を参照してください。

デフォルトでは、識別ボールトの管理アカウントは admin です。コンポーネントの設定時にこの値を変更できます。インストールプロセス中に識別ボールト用のツリー構造が自動的に作成されます。詳細については、14 ページのセクション 1.3「識別ボールトのデフォルトの構造の理解」を参照してください。

1.2.2 識別情報アプリケーション

このオプションは、次の Identity Manager コンポーネントとサポートソフトウェアをインストールします。

- Catalog Administrator
- Home and Provisioning Dashboard
- Roles Based Provisioning Module (RBPM)
- 役割およびリソースサービスドライバ
- ユーザアプリケーション
- ユーザアプリケーションドライバ
- One SSO Provider
- PostgreSQL
- Self Service Password Reset
- Tomcat

注 : GUI またはサイレントモードでの RBPM のインストールを選択した場合、Identity Reporting および Sentinel Log Management for IGA のオプションも選択されていることを確認してください。

このインストールプロセスでは、Oracle JRE、オープンソースバージョンの Apache Tomcat Web サーバ、Apache ActiveMQ、および PostgreSQL データベースサーバが Identity Manager の基盤として提供されています。このインストーラを使用することで、これらのコンポーネントを別途ダウンロードすることなくインストールできます。ただし、NetIQ は、これらのコンポーネントに対するエンタープライズサポートを提供していません。

NetIQ では、ステージングおよび運用環境ではエンタープライズアプリケーションサーバを使用し、この簡易インストーラは開発環境の構築に使用することをお勧めします。NetIQ は、これらのコンポーネントのアップデートやサポート、管理、設定、またはチューニングを提供しません。サポートが必要な場合は、それぞれのコンポーネントのサードパーティプロバイダに問い合わせてください。

インストールプロセスによって作成されるアカウントとデータベースは次のとおりです。

デフォルトの項目	説明
idmuserappdb	識別情報アプリケーション用データベース
idmadmin	idmuserappdb データベースの管理者ユーザアカウント
uaadmin	ユーザアプリケーションの管理者ユーザアカウント

さらに、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も作成および設定されます。他のドライバを設定するには、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。

識別情報アプリケーションの詳細については、『NetIQ Identity Manager セットアップガイド』の「Understanding the Components for Managing User Provisioning」および「Installing the Identity Applications」を参照してください。

1.2.3 Identity Reporting

このオプションは次の Identity Manager コンポーネントをインストールします。

- Identity Reporting Module
- Managed System Gateway driver (MSGW)
- データ収集サービス用ドライバ (DCS)

複数の種類のイベント監査システムがインストールされている場合でも、Identity Reporting が通信できるイベント監査サービスは 1 つだけです。イベントを記録するために、Identity Reporting は、Sentinel とともにインストールされる SIEM データベースを必要とします。

Identity Reporting の詳細については、『NetIQ Identity Manager セットアップガイド』の「Identity Reporting」および「Identity Reporting のインストール」を参照してください。

1.2.4 Sentinel Log Management for Identity Governance and Administration

このオプションは新しい PostgreSQL データベースに Log Management for IGA (Sentinel) をインストールします。

重要 : Linux で、統合インストールプログラムを使用してインストールする場合、NetIQ は、Sentinel Log Management for IGA と Identity Reporting を同じコンピュータ上にインストールするように制限しています。個別のコンポーネントインストーラを使用してこれらのコンポーネントをインストールする場合、同じコンピュータ上または分散された環境にインストールすることができます。

Sentinel Log Management for IGA では、イベントを表示して、これらのイベントを処理することができます。実行できるアクションの一部は次のとおりです。

- syslog、audit などのイベントソース用データ収集の設定
- イベントのリアルタイム表示
- イベントデータの関連付け
- Event Forwarding

Sentinel Log Management for IGA の詳細については、『*NetIQ Identity Manager Setup Guide*』の「Sentinel Log Management for Identity Governance and Administration のインストールと管理」を参照してください。

1.2.5 iManager

このオプションは iManager とそのワークステーションクライアントをインストールします。設定プロセス中に、iManager が通信に使用するデフォルトのポートを変更できます。iManager の詳細については、『NetIQ Identity Manager セットアップガイド』の iManager および iManager のインストールを参照してください。

1.2.6 Designer

このオプションはローカルコンピュータに Designer をインストールします。Designer にはユーザがプログラム可能なパラメータはありません。Designer の詳細については、『NetIQ Identity Manager セットアップガイド』の Designer for Identity Manager および Designer のインストールの計画を参照してください。

1.2.7 Analyzer

このオプションはローカルコンピュータに Analyzer をインストールします。Analyzer にはユーザがプログラム可能なパラメータはありません。Analyzer の詳細については、『NetIQ Identity Manager セットアップガイド』の Analyzer for Identity Manager および Analyzer のインストールを参照してください。

1.3 識別ボールトのデフォルトの構造の理解

統合インストールプロセスにより、Identity Manager のほとんどの展開環境に適した識別ボールトのデフォルトの構造が作成されます。

図 1-1 識別ボールトのデフォルトの構造

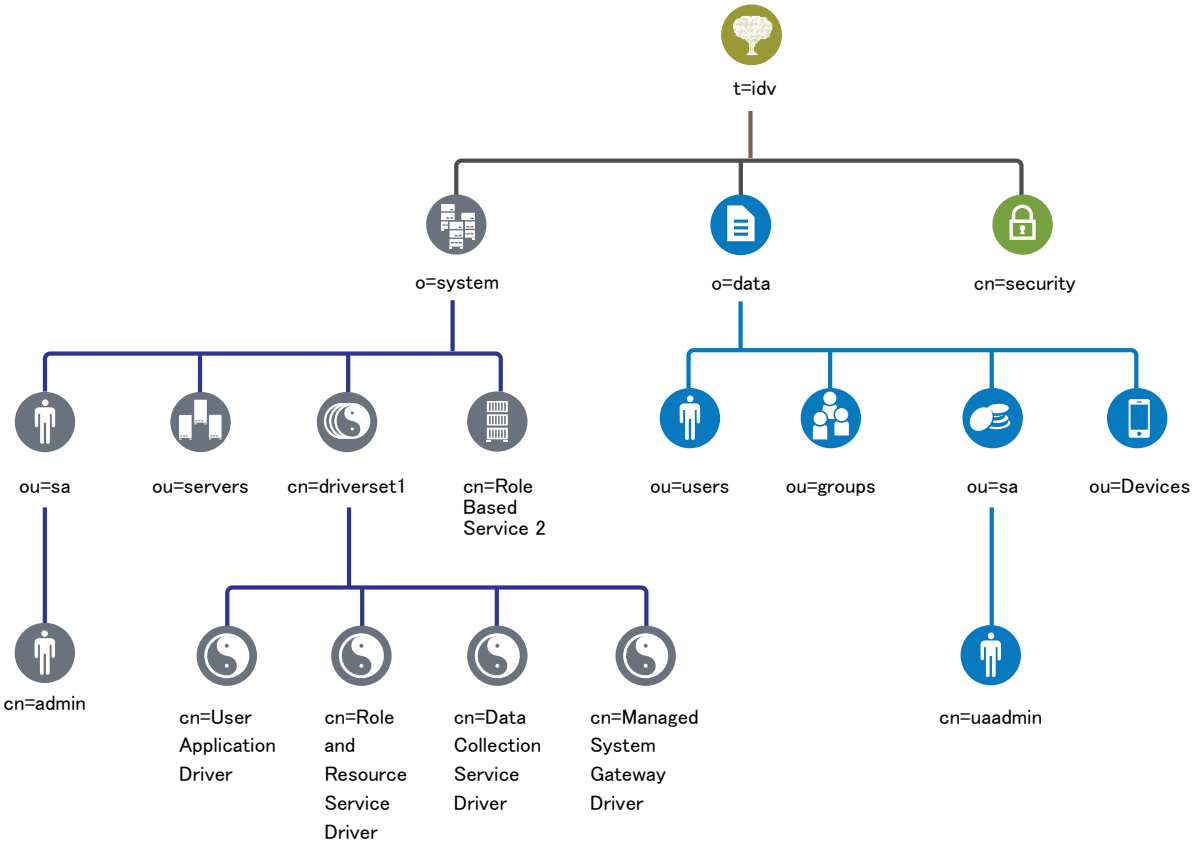

表 1-1 識別ボールトのオブジェクトの説明

オブジェクト	説明
t=idv	eDirectory ツリーの名前です。たとえば、idv です。
o=system	Identity Manager のシステムオブジェクトはすべて system という組織にあります。このコンテナおよびすべてのサブコンテナにアクセスできるユーザは管理者だけにしてください。詳細については、16 ページのセクション 1.3.1「システムコンテナ」を参照してください。
ou=sa.o=system	ou=sa.o=system コンテナは、すべてのシステムユーザを保持します。システムユーザとは、管理者、ドライバ管理者、およびその他の管理者です。
cn=admin.ou=sa.o=system	これはツリーの管理者アカウントです。
ou=servers.o=system	このコンテナは、サーバオブジェクト、およびサーバに関連付けられたすべてのオブジェクトを保持します。これにより、サーバオブジェクトを他のシステムオブジェクトから分離できます。

オブジェクト	説明
cn=driverset1.o=system	ドライバセットオブジェクトは、すべてのドライバオブジェクトを保持します。ドライバセットオブジェクトはシステムコンテナの直下に配置されます。
cn=User Application Driver.cn=driverset1.o=system	ユーザアプリケーションドライバは、ユーザアプリケーションに関連付けられたすべてのタスクを管理します。
cn=Role and Resource Service Driver.cn=driverset1.o=system	役割およびリソースサービスドライバは、Roles Based Provisioning Module に関連付けられたすべてのタスクを管理します。
cn=Data Collection Service Driver.cn=driverset1.o=system	データ収集サービスドライバは、Identity Reporting Module に関連付けられたタスクを管理します。
cn=Managed System Gateway Driver.cn=driverset1.o=system	Managed System Gateway Driver は、Identity Reporting Module に関連付けられたタスクを管理します。
cn=Role Based Service 2.o=system	このコンテナには、iManager が Identity Manager で動作できるようにするオブジェクトを保持します。
o=data	Identity Manager のデータオブジェクトはすべて data という組織にあります。管理者は、すべてのユーザがこのコンテナおよびすべてのサブコンテナにアクセスできるようにする必要があります。詳細については、16 ページのセクション 1.3.2「データコンテナ」を参照してください。
ou=users.o=data	識別ボールト内にあるすべてのユーザオブジェクトのデフォルトコンテナ。
ou=groups.o=data	識別ボールト内にあるすべてのグループオブジェクトのデフォルトコンテナ。
ou=sa.o=data	ユーザアプリケーション、Roles Based Provisioning Module、および Identity Reporting Module の役割管理者、スーパーユーザ、およびサービスアカウントのデフォルトコンテナ。
cn=uaadmin.ou=sa.o=data	ユーザアプリケーション管理者オブジェクト。
ou=Devices.o=data	デバイスのデフォルトコンテナ。
cn=security	セキュリティコンテナには、ツリーおよび Identity Manager のすべてのセキュリティオブジェクトを保持します。このコンテナおよびすべてのサブコンテナにアクセスできるユーザは管理者だけにしてください。詳細については、16 ページのセクション 1.3.3「セキュリティコンテナ」を参照してください。

このデフォルトの構造は主に、単一環境でのインストール向けに便利です。たとえば、これは小中規模の Identity Manager の展開に適した構造です。マルチテナント環境では、構造がわずかに異なる可能性があります。また、この方法では、大規模なツリーや分散型のツリーを整理できません。

Identity Manager 4.0 以降では、主に組織コンテナを使用するので、ユーザ、グループ、およびサービスの管理者は同じコンテナ内に配置されます。可能な限り組織 (o=) を使用し、状況に適うのであれば組織単位 (ou=) を使用してください。Identity Manager の構造は、システムコンテナ、データコンテナ、およびセキュリティコンテナという 3 つの主要コンポーネントを使用することでスケーラビリティを持つように設定されています。

1.3.1 システムコンテナ

システムコンテナは、1 つの組織です。デフォルトでは、o=system として指定されます。このコンテナは、識別ボールトおよび Identity Manager システム用の技術情報および環境設定情報のすべてを保持しています。システムコンテナは、主に次のサブコンテナを保持しています。

ou=sa

サービス管理者コンテナは、識別ボールトとドライバの管理オブジェクトを保持します。管理者ユーザのみがシステムのサブツリーにアクセスできます。識別ボールトのデフォルト管理者は admin.sa.system です。このコンテナ内のオブジェクトを sa (サービス管理者ユーザ / スーパーユーザ / サービスアカウント) と呼ぶことがあります。

サーバ

サーバオブジェクトには、関連するさまざまなオブジェクトが存在し、それらのオブジェクトはサーバオブジェクトと同じコンテナ内に存在する必要があります。ツリーに追加されるサーバの数が増えると、それらのオブジェクトをすべてスクロールするのが非常に煩雑になる場合があります。

サーバオブジェクトはすべて servers.system コンテナの下に含める必要があります。ただし管理者は、環境内で展開されたサーバごとに個別のサーバコンテナを作成することができます。コンテナの名前は、サーバオブジェクトの名前になります。

このような構造になっているのは、スケーラビリティを確保するためです。サーバに関連付けられているすべてのオブジェクト (ボリューム、ライセンス、証明書) が同じ場所に収まり、必要なオブジェクトを容易に検索できます。

ドライバセット

ドライバセットは、Identity Manager エンジンの環境設定中に別のパーティションとして作成されます。識別ボールトは、ドライバセットオブジェクトをシステムコンテナに保持します。この構造は、システムコンテナにさらにドライバセットを追加してスケールアップすることを可能にします。iManager の役割ベースのサービスもシステムコンテナに格納されています。

1.3.2 データコンテナ

データコンテナは、グループ、ユーザ、役割管理者、デバイス、およびその他のオブジェクトを保持します。このデータによってシステムが構成されます。グループ、ユーザ、およびサービス管理者 (sa) コンテナは組織単位です。お客様の組織上の慣習に応じて、追加の組織単位を使用してデータを構造化できます。たとえば、サービス管理者 (ou=sa) コンテナは、ユーザアプリケーション管理者のオブジェクトとサービス管理者アカウントをすべて保持しています。

1.3.3 セキュリティコンテナ

セキュリティコンテナとは、識別ボールトのインストール時に作成される特殊なコンテナです。これは、dc, o, または ou の代わりに cn=security と指定されます。このコンテナは、識別ボールトのすべてのセキュリティオブジェクトを保持します。たとえば、認証局やパスワードのポリシーが含まれています。

2 Identity Manager のインストールの計画

このセクションでは、各 Identity Manager コンポーネントの前提条件とシステム要件など、Identity Manager 環境の計画時に役立つ情報について説明します。すべてのコンポーネントを同じコンピュータにインストールする必要はありません。ただし、統合インストールプログラムはクラスタ環境への Identity Manager インストールはサポートしていません。

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。

2.1 インストールのチェックリスト

次のチェックリストには、テスト環境または評価環境への Identity Manager のインストールを計画する場合における高度な手順が記載されています。

	チェックリストの項目
❑	1. Identity Manager コンポーネント間の相互作用を理解します。詳細については、9 ページの第 1 章「はじめに」を参照してください。
❑	2. コンポーネント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と要件を満たしていることを確認します。 ◆ 統合インストールプロセスに固有の前提条件 : 18 ページのセクション 2.2「統合インストールプログラムの使用上の考慮事項」 ◆ 各コンポーネントの要件 : 19 ページのセクション 2.3「前提条件とシステム要件」 **重要 :** イベント監査のために、Identity アプリケーションと Identity Reporting の機能を Sentinel Log Management for IGA にインストールする必要があります。Sentinel は、Linux コンピュータ上にのみインストールできます。Windows コンピュータを使用している場合は、Sentinel のインストール用に Linux コンピュータが 1 台以上必要になります。
❑	3. 統合インストールプロセスによってサーバに追加されるコンポーネント、ソフトウェア、およびデフォルト設定を確認します。詳細については、35 ページの第 5 章「環境設定パラメータの理解」を参照してください。
❑	4. 識別ボールトのデフォルトのセットアップを確認します。詳細については、14 ページのセクション 1.3「識別ボールトのデフォルトの構造の理解」を参照してください。
❑	5. (状況によって実行) Red Hat Enterprise Linux 7.*x* 環境にコンポーネントをインストールする場合、コンピュータに正しいライブラリがインストールされていることを確認します。詳細については、『NetIQ Identity Manager セットアップガイド』の Installing Identity Manager on an RHEL 7.x Server を参照してください。

チェックリストの項目
❑ 6. 統合インストールプロセスを実行します。 ◆ ガイド付きインストールについては、26 ページのセクション 3.3「インストールウィザードの使用」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、27 ページのセクション 3.4「サイレントインストールの実行」を参照してください。
❑ 7. インストールされたコンポーネントを設定します。 ◆ ガイド付きプロセスについては、30 ページのセクション 4.2「環境設定ウィザードの使用」を参照してください。 ◆ サイレント設定については、33 ページのセクション 4.4「サイレント設定の実行」を参照してください。
❑ 8. インストールを完了します。詳細については、45 ページの第 6 章「統合インストールプロセスの最終手順」を参照してください。
❑ 9. Identity Manager をアクティベートします。詳細については、47 ページの第 7 章「Identity Manager 製品のアクティベート」を参照してください。

2.2 統合インストールプログラムの使用上の考慮事項

このセクションでは、統合インストールプログラムを使用してすべての Identity Manager コンポーネントをインストールする場合の考慮事項について説明します。ここに特に明記されていない限り、サーバおよびワークステーションは 19 ページのセクション 2.3「前提条件とシステム要件」に示す前提条件と要件も満たす必要があります。

- ❒ 統合インストールプロセスを使用して、既存のインストール環境をアップグレードすることはできません。
- ❒ Identity アプリケーションまたは Identity Reporting などのコンポーネントでは、Apache Tomcat アプリケーションサーバの使用が必要になります。インストールに 1 つまたは両方が指定されている場合、統合インストールプログラムによって自動的にサポート対象バージョンの Tomcat がインストールされます。
- ❒ Identity アプリケーションをインストールする際、統合インストールプログラムでは Identity Reporting のインストールも要求されます。
- ❒ すべてのコンポーネントを 1 台のコンピュータにインストールする場合、Linux コンピュータにインストールする必要があります。Windows コンピュータを使用している場合は、Sentinel Log Management for IGA のインストール用に Linux コンピュータが 1 台以上必要になります Identity アプリケーションおよび Identity Reporting では、監査のために Sentinel Log Management for IGA のインストールが要求されます。
- ❒ 統合インストールプログラムは、Hotfix 2 適用済みの eDirectory 9.0.2 をインストールします。このバージョンの eDirectory と互換性のある iManager 3.0.2 Patch 1 もインストールします。eDirectory 8.8.8 Patch 9 Hotfix 2 および iManager 2.7.7 Patch 9 を使用するには、コンポーネントインストーラを使用してインストールします。詳細については、『*NetIQ Identity Manager Setup Guide*』を参照してください。

2.3 前提条件とシステム要件

評価のためにすべてのコンポーネントを 1 台のコンピュータにインストールすることも、統合インストーラを使用してさまざまなコンポーネントを複数のシステムとプラットフォームにインストールすることもできます。このためには、統合インストールプログラムを複数回実行して、適切なコンポーネントを選択する必要があります。

2.3.1 前提条件

統合インストールプログラムを起動する前に、次の前提条件を完了していることを確認してください。

すべてのプラットフォーム

重要 : Sentinel Log Management for Identity Governance and Administration (IGA) は、Linux 環境にのみインストールできます。Identity Manager で Identity アプリケーションおよび Identity Reporting の機能を評価する場合、Windows コンピュータで統合インストーラを使用する前に、Linux コンピュータに Sentinel Log Management for IGA をインストールする必要があります。

- ❒ eDirectory をインストールする前に、ツリー名をサーバ参照に解決する方法を用意する必要があります。NetIQ では、SLP (サービスロケーションプロトコル) サービスを使用することをお勧めします。NetIQ eDirectory のバージョン 8.8 より前のリリースでは SLP もインストールされていました。ただし、バージョン 8.8 以上では、SLP は別途インストールする必要があります。詳細については、『NetIQ Identity Manager セットアップガイド』の *Using OpenSLP or hosts.nds for Resolving Tree Names* を参照してください。
- ❒ 効率的なパフォーマンスが得られるよう、eDirectory インフラストラクチャ用のサーバには静的 IP アドレスを設定する必要があります。サーバで DHCP アドレスを使用すると、eDirectory で予測不可能な結果が発生する可能性があります。コンピュータの DNS 名が解決可能であることを確認します。解決できない場合は、このコンピュータのエントリを /etc/hosts ファイルに追加し、DNS 名を解決可能にします。
- ❒ すべてのネットワークサーバ間で時刻を同期します。NetIQ では、NTP (ネットワークタイムプロトコル) オプションを使用することをお勧めします。

Linux

- ❒ (状況によって実行) Red Hat Enterprise Linux 7.x 環境にコンポーネントをインストールする場合、コンピュータに正しいライブラリがインストールされていることを確認します。詳細については、『NetIQ Identity Manager セットアップガイド』の Installing Identity Manager on an RHEL 7.x Server を参照してください。
- ❒ (状況によって実行) ガイドに従って SUSE Linux Enterprise Server 12 SP1 以降のプラットフォームにインストールする場合、コンピュータに以下のライブラリがインストールされていることを確認してください。
  - libXtst6-32bit-1.2.1-4.4.1.x86_64
  - libXrender-32bit
  - libXi6-32bit

一般的に、.rpm ファイルは http://rpmfind.net/linux などの Web サイトからダウンロードできます。たとえば、この Web ページから libXtst6-32bit-1.2.1-4.4.1.x86_64.rpm をダウンロードすることができます。

- ❒ 使用する Linux プラットフォームに unzip RPM がインストールされていることを確認します。
- ❒ /etc/hosts ファイルに記述できるループバックアドレスは 1 つだけです。複数のループバックアドレスが記述されている場合は、エディタを使用してそれらを削除し、設定を修正します。次に例を示します。

```
127.0.0.1 localhost.localdomain localhost #loopback
#127.0.0.2 server1
192.0.2.1 server1
```

Windows

- ❒ 統合インストーラで Identity Manager をインストールするには、Windows コンピュータに対する管理権が必要です。
- ❒ インストールプロセスを開始する前に、Windows オペレーティングシステムで最新のサービスパックが実行されている必要があります。

2.3.2 システム要件

次の要件は、すべてのコンポーネントまたはほとんどのコンポーネントを同じコンピュータにインストールする場合に適用されます。特定のコンポーネントの要件を理解する必要がある場合は、『*NetIQ Identity Manager セットアップガイド*』の Considerations and Prerequisites for Installation を参照してください。

次の情報を使用して、Identity Manager システムを正常にインストールして設定できるようにします。

カテゴリ	要件
プロセッサ	2GHz のプロセッサを搭載したマルチ CPU コンピュータ
メモリ	6GB 以上
ディスク容量	40GB 以上 **注 :** データを設定および入力するには追加のディスク容量が必要になります。この容量は、接続システムおよび識別ボールト内のオブジェクトの数に応じて異なる可能性があります。
オペレーティングシステム	次のうちの 1 つ以上 : ◆ SLES 12 SP1 以降 (64 ビット) ◆ RHEL 7.3 以降 (64 ビット) ◆ Windows Server 2012 R2 (64 ビット)

カテゴリ	要件
仮想システム	次のいずれか : ◆ Windows Server 2012 R2 の Hyper-V ◆ VMware ESXi 5.5 **重要 :** NetIQ では、NetIQ 製品が動作するオペレーティングシステムを正式にサポートするエンタープライズクラスの仮想システムで Identity Manager をサポートします。仮想システムのベンダーが該当のオペレーティングシステムを正式にサポートしていれば、NetIQ はそのオペレーティングシステム上の Identity Manager スタック全体をサポートします。
オペレーティングシステムのホットフィックス	NetIQ では、Identity Manager をインストールする前に、製造元の自動更新機能に従ってオペレーティングシステムの最新パッチを適用することをお勧めします。
Web ブラウザ	**デスクトップコンピュータ :** (次のバージョン以上) ◆ Apple Safari 9 ◆ Google Chrome 51 以降 ◆ Microsoft Internet Explorer 11 以降、Edge ◆ Mozilla FireFox 46 以降 **iPad:** (次のバージョン以上) ◆ Safari 9 以降 (iOS 9、10 上) **注 :** 識別情報アプリケーションにアクセスするには、ブラウザで Cookie が有効になっている必要があります。Cookie が無効な場合、この製品は動作しません。

2.3.3 インストールできるコンポーネント

デフォルトでは、統合インストールプログラムによって以下の Identity Manager コンポーネントがインストールされます。

***表 2-1** 統合インストールプログラムによってインストールされる Identity Manager のコンポーネントおよびそれらのバージョン*

Identity Manager のコンポーネント	バージョン
識別ボールト (eDirectory)	9.0.2 Hotfix 2
Identity Manager エンジン	4.6
リモートローダ	4.6
One SSO Provider	6.1.3
Self-Service Password Reset	4.1.0
Oracle Java Development Kit	1.8.0_112
Apache Tomcat	8.5.9

Identity Manager のコンポーネント	バージョン
PostgreSQL	9.6.10
Apache ActiveMQ	5.14
iManager およびプラグイン	3.0.2 Patch1
識別情報アプリケーション	4.6
Sentinel Log Management for IGA	8.0.0.1
Identity Reporting Module	5.5
Designer	4.6
Analyzer	4.6

2.3.4 デフォルトのインストール先

統合インストールプログラムは、表 2-2 に示す場所に Identity Manager コンポーネントをインストールします。Windows コンピュータでは、インストールするコンポーネントの場所を指定できます。Linux コンピュータでは、コンポーネントは事前定義済みの場所に配置されます。

***表 2-2** 統合インストールプログラムによって設定されているデフォルトのインストール先*

Identity Manager のコンポーネント	デフォルトのインストールパス
Linux	
識別ボールト (eDirectory)	/opt/novell/eDirectory
Identity Manager エンジン	/opt/novell/eDirectory
リモートローダ	/opt/novell/dirxml
ファンアウトエージェント	/opt/novell/dirxml/fanoutagent
Sentinel Log Management for IGA	/opt/novell/sentinel (Linux のみ)
JRE	/opt/netiq/idm/jre
Tomcat	/opt/netiq/idm/apps/tomcat
PostgreSQL	/opt/netiq/idm/apps/postgres
ActiveMQ	/opt/netiq/idm/apps/activemq
OSP	/opt/netiq/idm/apps/osp
SSPR	/opt/netiq/idm/apps/sspr
ユーザアプリケーション	/opt/netiq/idm/apps/UserApplication
識別情報アプリケーション	/opt/netiq/idm/apps
Identity Reporting	/opt/netiq/idm/apps/IDMReporting
iManager およびプラグイン	/var/opt/novell/iManager

Identity Manager のコンポーネント	デフォルトのインストールパス
Analyzer	/opt/netiq/idm/tools/Analyzer
Designer	/opt/netiq/idm/tools/Designer
Windows	
識別ボールト (eDirectory)	C:\NetIQ\IdentityManager\NDS
Identity Manager エンジン	C:\NetIQ\IdentityManager\NDS
リモートローダ	C:\NetIQ\IdentityManager\RemoteLoader
ファンアウトエージェント	C:\NetIQ\IdentityManager\FanoutAgent
JRE	C:\NetIQ\IdentityManager\jre
Tomcat	C:\NetIQ\IdentityManager\apps\tomcat
PostgreSQL	C:\NetIQ\IdentityManager\apps\posgres
OSP	C:\NetIQ\IdentityManager\apps\osp
SSPR	C:\NetIQ\IdentityManager\apps\sspr
ActiveMQ	C:\NetIQ\IdentityManager\apps\activemq
ユーザアプリケーション	C:\NetIQ\IdentityManager\apps\UserApplication
Identity Reporting	C:\NetIQ\IdentityManager\apps\IDMReporting
iManager	C:\NetIQ\IdentityManager\iManager
Analyzer	C:\NetIQ\IdentityManager\tools\Analyzer
Designer	C:\NetIQ\IdentityManager\tools\Designer

3 Identity Manager のインストール

統合インストーラは、すべての Identity Manager コンポーネントのバイナリファイルをインストールし、コンポーネントを設定します。コンポーネントのインストールと設定を同時に行うことも、それぞれを別の手順で行うこともできます。

3.1 ISO ファイルのダウンロード

NetIQ のダウンロードサイトからインストールファイルをダウンロードする必要があります。

.iso ファイルをダウンロードする

1. NetIQ ダウンロード Web サイトにアクセスします。
2. ［**Product or Technology**］メニューで、［**Identity Manager**］を選択します。
3. ［**Select Version**］フィールドで［**Identity Manager 4.6**］を選択し、［**送信**］をクリックします。
4. ［**Identity Manager 4.6**］のリンクをクリックし、［**proceed to download**］をクリックします。
5. NetIQ カスタマーセンター ID でログインします。
6. ご使用のプラットフォームに適した .iso ファイルを選択し、画面の指示に従ってファイルをダウンロードします。

統合インストールファイル (install.exe または install.bin) は、Identity Manager .iso ファイルの最上位にあります。.iso ファイルをマウントするか、.iso ファイルから作成した DVD にアクセスして、Identity Manager のインストールファイルにアクセスします。

3.2 統合インストールのすべての環境設定パラメータでの同一パスワードの使用

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、統合インストールの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。

Linux

インストールプログラムまたは設定プログラムを起動する前に、次のコマンドを入力します。

```
export USER_SUPPLIED_PASSWORD=password
```

次に例を示します。

```
export USER_SUPPLIED_PASSWORD=test123
```

Windows

次のいずれかの操作を実行します。

- **[System Properties (システムのプロパティ)] > [Environment Variables (環境変数)]** の順に選択し、USER_SUPPLIED_PASSWORD を追加して変数の値を指定します。
- インストールプログラムまたは設定プログラムを起動する前に、次のコマンドを入力します。

  ```
  set USER_SUPPLIED_PASSWORD=password
  ```

  次に例を示します。

  ```
  set USER_SUPPLIED_PASSWORD=test123
  ```

3.3 インストールウィザードの使用

次の手順では、インストールウィザードを使用して Linux または Windows プラットフォームに Identity Manager をインストールする方法について説明します。無人のサイレントインストールを実行するには、27 ページのセクション 3.4「サイレントインストールの実行」を参照してください。

インストールの準備をするために、17 ページのセクション 2.1「インストールのチェックリスト」に記載されている前提条件とシステム要件を確認します。関連するインストール情報については、最新のリリースノートも参照してください。

利便性のため、Identity Manager で指定する必要があるほとんどのパスワードに対してインストールプロセス中に適用するパスワードを指定できます。

ウィザードを使用して Identity Manager をインストールする

1. コンポーネントをインストールするコンピュータに root または管理者ユーザとしてログインします。
2. .iso ファイルをマウントするか、.iso ファイルから DVD を作成します。詳細については、25 ページのセクション 3.1「ISO ファイルのダウンロード」を参照してください。
3. (オプション) 統合インストールの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インストールプロセスに指示します。詳細については、25 ページのセクション 3.2「統合インストールのすべての環境設定パラメータでの同一パスワードの使用」を参照してください。
4. .iso ファイルのルートディレクトリからインストールファイルにアクセスし、次のいずれかの操作を実行します。
   - **Linux**: 「./install.bin」と入力します。
   - **Windows**: install.exe を実行します。
5. タイトルページで、ドロップダウンリストから適切な言語を選択し、[OK] をクリックします。
6. [イントロダクション] ページで、インストール可能なさまざまな Identity Manager コンポーネントを参照して、[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て同意し、[次へ] をクリックします。

   注 : 使用許諾契約に同意するには、使用許諾契約全体を読んで文末までスクロールする必要があります。

8. ローカルサーバにインストールするコンポーネントを指定し、[次へ] をクリックします。

コンポーネントのオプションの詳細については、10 ページのセクション 1.2「統合インストールプロセスの理解」を参照してください。

9 (状況によって実行) Windows サーバでインストールフォルダを指定し、［次へ］をクリックします。

10 インストール前の概要を確認して、［インストール］をクリックします。

注 : 選択したコンポーネントによっては、インストールプロセスが完了するまでに多少時間がかかる場合があります。

---

11 インストールが完了したら、次のいずれかの操作を実行して、インストールされたコンポーネントを設定します。

- **すぐに設定する場合** : ［Continue Now (直ちに続行)］を選択します。
- 「後で設定する場合」: Continue Now (直ちに続行) チェックボックスをクリアします。

注 : 後で設定する場合は、Identity Manager コンポーネントを設定するまで、マシンを再起動したり、サービスを開始したり停止したりしないでください。

環境設定パラメータはいつでも変更できます。ただし、さまざまなパラメータを指定しない限り、Identity Manager を実行することはできません。詳細については、29 ページの第 4 章「Identity Manager コンポーネントの設定」を参照してください。

注 : Designer や Analyzer など、一部のコンポーネントでは設定は必要ありません。

---

12 ［完了］をクリックします。

3.4 サイレントインストールの実行

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。代わりに、システムはプロパティファイルの情報を使用します。ガイド付きインストールを実行するには、26 ページのセクション 3.3「インストールウィザードの使用」を参照してください。インストールの準備をするために、17 ページのセクション 2.1「インストールのチェックリスト」に記載されている前提条件とシステム要件を確認します。関連するインストール情報については、最新のリリースノートも参照してください。

利便性のため、Identity Manager で指定する必要があるシングルサインオンパスワードに対してインストールプロセス中に適用するパスワードを指定できます。詳細については、29 ページのセクション 4.1「コンポーネントの設定に関する考慮事項」を参照してください。

サイレントインストールを実行する

1 コンポーネントをインストールするコンピュータに root または管理者としてログインします。

2 .iso ファイルをマウントしてから、インストールファイルが保存されているディレクトリに移動します。デフォルトの場所は *<extracted_iso_path>/install/propfiles/install.properties* ディレクトリです。

3 サイレントインストール用の install.properties ファイルを編集します。これは、デフォルトでは次のディレクトリにあります。

- **Linux**: install/propfiles
- **Windows**: install\propfiles

4 インストールファイルが保存されているディレクトリに移動します。デフォルトの場所は install ディレクトリです。

5 サイレントインストール用の install.properties ファイルを編集します。これは、デフォルトでは次のディレクトリにあります。

- **Linux**: install/propfiles
- **Windows**: install\propfiles

6 (オプション) 統合インストールの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インストールプロセスに指示します。詳細については、25 ページのセクション 3.2「統合インストールのすべての環境設定パラメータでの同一パスワードの使用」を参照してください。

7 サイレントインストールを実行するため、次のいずれかのコマンドを発行します。

- **Linux**: install.bin -i silent -f <*extracted_iso_path*>/install/propfiles/install.properties
- **Windows**: install.exe -i silent -f <*extracted_iso_path*>/install/propfiles/install.properties

8 (状況によって実行) 設定を続行するには、install.properties ファイルに以下の値を入力します。

- CONTINUE_CONFIGURE=true を指定します。
- CONFIGURE_PROPERTY_FILE プロパティで設定ファイルのパスを指定します。たとえば、新しいツリーを設定する場合、configure_new_tree.properties を指定します。既存のツリーに対して configure_existing_tree.properties を指定します。詳細については、29 ページの第 4 章「Identity Manager コンポーネントの設定」を参照してください。

9 (状況によって実行) 後でコンポーネントを設定するため、次のいずれかのコマンドを発行します。

- **Linux**: configure.bin -i silent -f <*extracted_iso_path*>/install/propfiles/configure_<*new/existing*>_tree.properties
- **Windows**: configure.exe -i silent -f <*extracted_iso_path*>/install/propfiles/configure_<*new/existing*>_tree.properties

4 Identity Manager コンポーネントの設定

インストールした Identity Manager コンポーネントの設定は、統合インストールプロセスに従って進めることも、サイレントで行うこともできます。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。環境設定パラメータの詳細については、35 ページの第 5 章「環境設定パラメータの理解」を参照してください。

注

- ユーザが識別情報アプリケーションにログインできるようにするため、admin.sa.system、uaadmin.sa.data、および users.data には設定プロセス中にサンプルパスワードポリシーが割り当てられます。この処理の一部として、［Password Retrieval (パスワードの取得)］オプションの［**Allow admin to retrieve passwords (管理者にパスワードの取得を許可する)**］設定も有効になります。
- 統合インストールプログラムは、単一サーバ環境における最も一般的な設定に対してデフォルト値を提供します。これらの設定は通常のインストールで使用されます。NetIQ では、インストール用のこれらの設定を保持しておくことをお勧めします。

4.1 コンポーネントの設定に関する考慮事項

統合インストールプロセスを使用してインストール済みコンポーネントを設定する前に、次の考慮事項を確認します。

- 設定できるのは、ローカルコンピュータにインストールされたコンポーネントだけです。
- インストールまたは設定の前に、統合インストールの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。詳細については、25 ページのセクション 3.2「統合インストールのすべての環境設定パラメータでの同一パスワードの使用」を参照してください。
- /etc/hosts ファイルにループバックアドレス 127.0.0.1 と実際の IP アドレスのエントリが記述されていることを確認します。詳細については、19 ページのセクション 2.3「前提条件とシステム要件」を参照してください。
- 識別情報アプリケーションおよび Identity Reporting コンポーネントを設定する場合、［**Advanced Settings (詳細設定)**］を選択して、localhost が設定されているフィールドを有効な IP アドレスまたは DNS 名に変更します。localhost から値を変更しないと、設定は失敗します。
- Identity Manager サーバのみを設定する場合は、logevent.conf ファイル (Linux) または logevent.cfg ファイル (Windows) にログサーバの詳細を手動で追加します。識別情報アプリケーションまたは Identity Reporting を設定する場合にのみ、統合インストールプロセスはこのログサーバの詳細を使用してファイルを更新します。
- デフォルトでは、Sentinel Log Management for IGA は 8643 ポートを使用します。ただし、インストール後に異なるポートを使用するように Sentinel Log Management for IGA を設定できます。詳細については、『NetIQ Sentinel インストールと設定ガイド』の「インストール後の環境設定の変更」を参照してください。

- 既存のツリーにセカンダリサーバを追加する前に、ヘルスチェックを実行する必要があります。統合インストールプロセス中にヘルスチェックは実行されません。
- 統合インストールプロセスを使用してセカンダリサーバをツリーに追加した場合、サーバは、そのルートと専用のドライバセットパーティションのコピーのみを受け取ります。
  - さらに、このセカンダリサーバでデータ収集サービスドライバをプライマリとして使用した場合、ドライバは、レポートする必要があるオブジェクトの変更を認識できません。このサーバでデータ収集サービスドライバを設定するには、『NetIQ Identity Manager セットアップガイド』のデータ収集サービス用ドライバの設定を参照してください。
  - データ収集サービスドライバをこのセクションサーバに配置する場合、サーバが機能するには、サーバにツリーパーティションのコピーが保持されている必要があります。

設定値の詳細については、35 ページの第 5 章「環境設定パラメータの理解」を参照してください。

4.2 環境設定ウィザードの使用

環境設定ウィザードを使用すると、インストールの実行時に選択したすべての Identity Manager コンポーネントを順を追って設定できます。

Identity Manager コンポーネントを設定するには

1 (状況によって実行) 既存のツリーにセカンダリサーバを追加するため、次の手順を実行します。

1a ndscheck ユーティリティを探します。このユーティリティは、デフォルトでは次のディレクトリにあります。

- **Linux**: /opt/novell/eDirectory/bin/ndscheck
- **Windows**: *install_location*\NDS

1b 必須パラメータを指定して、次のコマンドを実行します。

ndscheck [-h *hostname port*] [-a *admin_FDN*] [-w *password*]

2 (状況によって実行) インストール手順の 27 ページのステップ 12 から続行した場合、30 ページのステップ 6 にスキップします。

3 (オプション) 統合インストールの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設定プロセスに指示します。詳細については、25 ページのセクション 3.2「統合インストールのすべての環境設定パラメータでの同一パスワードの使用」を参照してください。

4 (状況によって実行) 設定を手動で開始するため、次のいずれかの操作を実行します。

- **Linux (GUI)**: 「./configure.bin」と入力します。
- **Windows**: configure.exe を実行します。

5 タイトルページで、ドロップダウンリストから適切な言語を選択し、[**OK**] をクリックします。

6 システムにインストールされているコンポーネントを確認して、[**次へ**] をクリックします。

7 ローカルサーバで設定するコンポーネントを選択し、[**次へ**] をクリックします。

8 次の情報を使用して各コンポーネントを設定します。

- **識別ボールト :** 識別ボールト内に新しいツリーを作成するか、それとも既存のツリーを変更するかを指定し、環境に合わせてツリーを設定します。詳細については、35 ページのセクション 5.1「識別ボールト」を参照してください。

- **Sentinel Log Management for IGA:** Sentinel Log Management for IGA に関する設定情報を指定します。詳細については、39 ページのセクション 5.3「Sentinel Log Management for IGA」を参照してください。

  重要 : Sentinel Log Management for IGA は、Linux コンピュータ上にのみインストールできます。ただし、Identity Reporting Module を設定するには、有効な Sentinel が必要です。

- **識別情報アプリケーション :** 識別情報アプリケーションの設定情報を指定します。監査サーバの IP アドレスまたは DNS 名前を指定する必要があります。いずれかを指定しないと、設定は失敗します。詳細については、40 ページのセクション 5.4「識別情報アプリケーション」を参照してください。

  重要 : [**Advanced Settings (詳細設定)**] を選択して、localhost が設定されているフィールドを有効な IP アドレスまたは DNS 名に変更する必要があります。デフォルトのパラメータを localhost から変更しないと、設定は失敗します。

- **(状況によって実行) Identity Manager サーバ :** 既存の eDirectory ツリーにインストールする場合は、既存の Identity Manager サーバの情報を指定します。詳細については、39 ページのセクション 5.2「Identity Manager サーバ」を参照してください。
- **Identity Reporting Module:** Identity Reporting Module を使用するには、Sentinel がインストールおよび設定済みである必要があります。Sentinel は Linux コンピュータ上にのみインストールできます。Windows コンピュータを使用している場合、Windows コンピュータ上の Identity Reporting Module を設定するには、Linux コンピュータに Sentinel をインストールする必要があります。

  Identity Reporting Module の設定情報を指定します。詳細については、42 ページのセクション 5.5「Identity Reporting Module」を参照してください。
- **ツール :** Linux のみ。[**Advanced Settings (詳細設定)**] を選択して、デフォルトの HTTP ポートを変更します。詳細については、44 ページのセクション 5.6「ツール」を参照してください。

9 [**次へ**] をクリックして、各コンポーネントの設定を実行します。

10 設定情報の概要を確認して、[**設定**] をクリックします。

11 設定の概要を確認して、[**完了**] をクリックします。

注 : 設定中にエラーが発生した場合、統合インストーラにインストールログの場所が表示されます。インストールログを確認して、設定が失敗した原因を特定してください。

4.3 サイレント設定用のプロパティファイルの編集

各コンポーネントの設定を完了するのに必要なパラメータが記述されたプロパティファイルを作成または変更することによって、Identity Manager コンポーネントのサイレント設定を実行できます。Identity Manager のメディアには、すべてのコンポーネントを 1 台のサーバにインストールした場合に使用できるサンプルファイルが 2 つ付属しています。

プロパティファイルを編集する

1 (状況によって実行) すべてのコンポーネントを同じサーバにインストールした場合、サンプルプロパティファイルの 1 つを編集します。サンプルプロパティファイルは、デフォルトでは次のディレクトリにあります。

- **Linux**: install/propfiles
- **Windows**: install\propfiles

たとえば、新しいツリーを作成するには、configure_new_tree.properties ファイルを使用します。

2 (状況によって実行) すべてのコンポーネントを同じサーバにインストールしなかった場合は、次の手順を実行して、インストールしたコンポーネントのプロパティファイルを生成します。

2a 次のコマンドを実行します。

```
./install.bin -i silent -DSELECTED_PRODUCTS=components_to_be_configured -f
filename.properties
```

ここで、*filename*.properties は、サンプルプロパティファイルの 1 つを表します。

プログラムにより、指定したコンポーネントがインストールされていることが確認され、コンポーネントの必須パラメータのリストが生成されます。

2b ステップ 2a で実行したコマンドの出力を使用して、新しいプロパティファイルを作成します。

2c SELECTED_PRODUCTS 変数をファイルに追加し、設定するコンポーネントを指定します。

3 このプロパティファイルで、インストールしたコンポーネントの設定を指定します。詳細については、35 ページの第 5 章「環境設定パラメータの理解」を参照してください。

4 プロパティファイルに次のパスワード変数を追加します。

パスワード変数	適用対象のユーザアカウントまたはサービス
IA_IDVAULT_ADMIN_PASSWORD	識別ボールト管理者
IA_RBPM_POSTGRESQL_DB_PASSWORD	識別情報アプリケーションデータベース管理者 (idmadmin)
IA_RBPM_USERAPPADMIN_PASSWORD	ユーザアプリケーション管理者 (uaadmin)
IA_REPORTING_NOVL_DB_USER_PASSWORD	Identity Reporting データベース管理者
IA_REPORTING_IDM_SERVER_PASSWORD	Identity Reporting サーバユーザ (idmrptsrv)
IA_REPORTING_IDM_USER_PASSWORD	Identity Reporting ユーザ (idmrptuser)
-DUSER_SUPPLIED_PASSWORD	シングルサインオンサービス

サイレントインストールの開始時に duser_supplied_password 変数を記述した場合、その値はすでにシングルサインオンパスワードに適用されています。

5 ファイルを保存して閉じます。

4.4 サイレント設定の実行

各コンポーネントの設定を完了するのに必要なパラメータが記述されたプロパティファイルを作成することによって、Identity Manager コンポーネントのサイレント設定を実行できます。Identity Manager のメディアには、すべてのコンポーネントを 1 台のサーバにインストールした場合に使用できるサンプルファイルが 2 つ付属しています。

設定できるパラメータの詳細については、35 ページの第 5 章「環境設定パラメータの理解」を参照してください。

サイレント設定を実行する

1 (状況によって実行) 既存のツリーにセカンダリサーバを追加するため、次の手順を実行します。

1a ndscheck ユーティリティを探します。このユーティリティは、デフォルトでは次のディレクトリにあります。

- **Linux**: /opt/novell/eDirectory/bin/ndscheck
- **Windows**: *install_location*\NDS

1b 必須パラメータを指定して、次のコマンドを実行します。

ndscheck [-h *hostname port*] [-a *admin_FDN*] [-w *password*]

2 (オプション) 統合インストールの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設定プロセスに指示します。詳細については、25 ページのセクション 3.2「統合インストールのすべての環境設定パラメータでの同一パスワードの使用」を参照してください。

3 サイレント設定を実行するため、次のいずれかのコマンドを発行します。

- **Linux**: configure.bin -i silent -f <*extracted_iso_path*>*/install/propfiles/configure_new_tree.properties*
- **Windows**: configure.exe -i silent -f <*extracted_iso_path*>*/install/propfiles/configure_new_tree.properties*

5 環境設定パラメータの理解

このセクションでは、インストールした Identity Manager を適切に設定するために指定する必要があるパラメータを定義します。インストールプログラムを使用して、コンポーネントのインストール後すぐにコンポーネントを設定できます。

注 : 多くのコンポーネントではパスワードが必要なため、そのパスワードを指定する必要があります。すべてのパラメータで同じパスワードを使用できます。そのためには、インストールプロセスの開始時にパスワードを指定します。詳細については、インストール方法を参照してください。

5.1 識別ボールト

このセクションでは、識別ボールト用の eDirectory ツリーの設定を定義します。一部のパラメータは、新しいツリーの設定にも既存のツリーの設定にも適用されます。プログラムによって表示されるのは基本パラメータです。すべてのパラメータを表示するには、[**Advanced Settings (詳細設定)**] をクリックします。

5.1.1 新しいツリーの作成

まだ eDirectory ツリーが存在しない場合は、次のパラメータを使用します。このセクションで説明するすべてのパラメータは、新しいツリーの作成時に役立ちます。

新しいツリーの作成

識別ボールト用の新しい eDirectory ツリーを作成するには、このオプションを選択します。

ツリー名

作成するツリーの名前を指定します。ツリー名は次の要件を満たしている必要があります。

- ネットワーク内では、重複するツリー名を使用することはできません。
- ツリー名の長さは 2 ～ 32 文字にする必要があります。
- ツリー名で使用できる文字は、文字 (a ～ z、A ～ Z)、数字 (0 ～ 9)、ハイフン (-)、およびアンダースコア (_) のみです。

別のツリーがある場合は、ツリー名に関する社内基準を作成しておくと、今後ツリーをマージする場合に作業が容易になります。

管理者のパスワード

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、netiq123 です。インストールプログラムによって作成される管理者オブジェクトには、インストールプログラムによってこのパスワードが設定されます。

詳細設定

残りの設定はすべて［**Advanced Settings (詳細設定)**］にあります。［**Advanced Settings (詳細設定)**］を変更しなかった場合は、表示されているデフォルト設定が使用されます。

識別ボールト管理者

少なくともサーバの追加先のコンテキストに対してフル権限を持つ、ツリー内の管理者オブジェクトの相対識別名 (RDN) を指定します。デフォルトの名前は admin です。

インストールプログラムは、ツリー内でのすべての操作にこの名前を使用します。

NCP ポート

Linux サーバにのみ適用されます。

識別ボールトが Identity Manager コンポーネントとの通信に使用する NCP (NetWare Core Protocol) ポートを指定します。デフォルトは 524 です。

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 の使用の詳細については、『NetIQ Identity Manager セットアップガイド』の Using LDAP to Communicate with the Identity Vault を参照してください。

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。LDAP の使用の詳細については、『NetIQ Identity Manager セットアップガイド』の Using LDAP to Communicate with the Identity Vault を参照してください。

HTTP ポート

HTTP スタックが平文で動作するポートを指定します。デフォルトは 8028 です。

iManager で使用する HTTP スタックポートとは異なる HTTP スタックポートを指定する必要があります。詳細については、『*NetIQ iManager Administration Guide*』を参照してください。

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。デフォルトは 8030 です。

iManager で使用する HTTP スタックポートとは異なる HTTP スタックポートを指定する必要があります。詳細については、『*NetIQ iManager Administration Guide*』を参照してください。

eDirectory Instance path (eDirectory インスタンスパス)

Linux サーバにのみ適用されます。

このサーバ上のこの eDirectory インスタンスのパスを指定します。デフォルトのパスは /var/opt/novell/eDirectory です。1 つのサーバ上で eDirectory の複数のインスタンスを実行できます。

DIB パス

ディレクトリ情報ベース (DIB) ファイルをインストールするローカルシステムのパスを指定します。デフォルトでは、これらのファイルは次の場所に配置されます。

- **Linux**: /var/opt/novell/eDirectory/data/dib
- **Windows**: C:\NetIQ\IdentityManager\NDS\DIBFiles\

DIB データファイルは eDirectory のデータベースファイルです。ご使用の環境用の DIB データファイルに必要な空き領域がデフォルトの場所の空き領域よりも大きい場合は、異なるパスを指定できます。

重要 : Windows では、DIB ファイルは \NDS ディレクトリに存在する必要があります。Windows で DIB ファイルのデフォルトの場所を変更すると、Identity Manager エンジンの設定は失敗します。

パスワードとの単純バインドに TLS を必要とする

(オプション) 平文の LDAP 要求を受信する際に、識別ボールトが TLS (Transport Layer Security) プロトコルを必要とするかどうかを選択します。このオプションはデフォルトで有効になっています。

Enable SecretStore (SecretStore の有効化)

Windows サーバにのみ適用されます。

(オプション) eDirectory の設定時に SecretStore を有効にするかどうかを選択します。詳細については、『*NetIQ eDirectory Installation Guide*』の SecretStore Integration with eDirectory を参照してください。

5.1.2 既存のツリーへの追加

すでに eDirectory ツリーが存在している場合は、次のパラメータを使用して、この新しいサーバを既存のツリーに追加します。

重要 : 新しいサーバを既存のツリーに追加するとどのような影響があるかを理解していることを確認してください。詳細については、29 ページのセクション 4.1「コンポーネントの設定に関する考慮事項」を参照してください。

既存のツリーに追加

識別ボールト用に変更するツリーがすでに存在する場合、このオプションを選択します。

既存のツリー名

既存の eDirectory ツリーの名前を指定します。

既存のサーバのアドレス

ルートパーティションのマスタレプリカを保持するサーバの IP アドレスを指定します。

Existing port number (既存のポート番号)

上で指定したサーバの NCP ポートを指定します。NCP のデフォルトポートは 524 です。

既存のサーバのコンテキスト DN

既存のツリー内でこのサーバを配置するコンテキストの LDAP DN を指定します。デフォルト値は、統合インストーラによって作成される識別ボールト構造の ou=servers,o=system です。詳細については、14 ページのセクション 1.3「識別ボールトのデフォルトの構造の理解」を参照してください。

既存のサーバの管理者名

eDirectory 管理者の名前を指定します。デフォルトの名前は admin です。詳細については、14 ページのセクション 1.3「識別ボールトのデフォルトの構造の理解」を参照してください。

既存のサーバの管理者のコンテキスト DN

既存のツリー内で eDirectory 管理者が存在するコンテキストの LDAP DN を指定します。デフォルト値は、統合インストーラによって作成される識別ボールト構造の ou=sa,o=system です。詳細については、14 ページのセクション 1.3「識別ボールトのデフォルトの構造の理解」を参照してください。

既存のサーバ管理者のパスワード

eDirectory 管理者のパスワードを指定します。

詳細設定

残りの設定はすべて［**Advanced Settings (詳細設定)**］にあります。［**Advanced Settings (詳細設定)**］を変更しなかった場合は、表示されているデフォルト設定が使用されます。

LDAP ポート

既存の eDirectory ツリーが平文の 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 の使用の詳細については、『NetIQ Identity Manager セットアップガイド』の Using LDAP to Communicate with the Identity Vault を参照してください。

セキュア LDAP ポート

既存の eDirectory ツリーが 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。

LDAP の使用方法の詳細については、『NetIQ Identity Manager セットアップガイド』の「識別ボールトと通信するための LDAP の使用」を参照してください。

HTTP ポート

HTTP スタックが平文で動作するポートを指定します。デフォルトは 8028 です。

iManager で使用する HTTP スタックポートとは異なる HTTP スタックポートを指定する必要があります。詳細については、『*NetIQ Manager Administration Guide*』を参照してください。

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。デフォルトは 8030 です。

iManager で使用する HTTP スタックポートとは異なる HTTP スタックポートを指定する必要があります。詳細については、『*NetIQ iManager Administration Guide*』を参照してください。

DIB パス

ディレクトリ情報ベース (DIB) ファイルをインストールするローカルシステムのパスを指定します。デフォルトでは、これらのファイルは次の場所に配置されます。

- **Linux**: /var/opt/novell/eDirectory/data/dib
- **Windows**: C:\NetIQ\IdentityManager\NDS\DIBFiles\

DIB データファイルは eDirectory のデータベースファイルです。ご使用の環境用の DIB データファイルに必要な空き領域がデフォルトの場所の空き領域よりも大きい場合は、異なるパスを指定できます。

重要 : Windows では、DIB ファイルは \NDS ディレクトリに存在する必要があります。Windows で DIB ファイルのデフォルトの場所を変更すると、Identity Manager エンジンの設定は失敗します。

パスワードとの単純バインドに TLS を必要とする

(オプション) 平文の LDAP 要求を受信する際に、識別ボールトが TLS (Transport Layer Security) プロトコルを必要とするかどうかを選択します。このオプションはデフォルトで有効になっています。

Enable SecretStore (SecretStore の有効化)

Windows サーバにのみ適用されます。

(オプション) eDirectory の設定時に SecretStore を有効にするかどうかを選択します。詳細については、『*NetIQ eDirectory Installation Guide*』の SecretStore Integration with eDirectory を参照してください。

5.2 Identity Manager サーバ

統合インストールプログラムに［**Identity Manager Server (Identity Manager サーバ)**］の各フィールドが表示されるのは、サーバを既存の eDirectory ツリーに追加するよう選択した場合のみです。

重要 : 統合インストーラではアップグレードはサポートされていません。Identity Manager がすでに展開されている場合、Identity Manager ソリューションをアップグレードするには、通常のインストーラを使用する必要があります。詳細については、『NetIQ Identity Manager セットアップガイド』の Upgrading Identity Manager を参照してください。

ドライバセット名

新しい Identity Manager ドライバセットオブジェクトの名前を指定します。Identity Manager を動作させるには、このオブジェクトを作成する必要があります。新しいツリーを作成する場合、このオブジェクトは統合インストーラによって作成されます。

ドライバセットのコンテキスト DN

ドライバセットオブジェクトを作成するコンテナの LDAP DN を指定します。デフォルトの場所は、統合インストーラによって作成される識別ボールト構造の o=system です。詳細については、14 ページのセクション 1.3「識別ボールトのデフォルトの構造の理解」を参照してください。

5.3 Sentinel Log Management for IGA

Sentinel Log Management for IGA を使用すると、Identity Manager コンポーネントを監査することができます。このコンポーネントは、Identity アプリケーションおよび Identity Reporting コンポーネントを設定する前にインストールして実行する必要があります。そうしない場合、これらのコンポーネントの設定は失敗します。

Sentinel パスワード

Sentinel 管理者のパスワードを指定します。このアカウントはインストールプロセスで作成されます。

注 : SLES サーバの場合、パスワードはシステムパスワードポリシーを満たす必要があります。

dbauser パスワード

識別情報ウェアハウスを変更できる admin アカウントのパスワードを指定します。このアカウントはインストールプロセスで作成されます。

注 : SLES サーバの場合、パスワードはシステムパスワードポリシーを満たす必要があります。

詳細設定

残りの設定はすべて［**Advanced Settings (詳細設定)**］にあります。［**Advanced Settings (詳細設定)**］を変更しなかった場合は、表示されているデフォルト設定が使用されます。

5.4 識別情報アプリケーション

このセクションでは、ユーザアプリケーションなどの識別情報アプリケーションの設定を定義します。プログラムによって表示されるのは基本パラメータです。すべてのパラメータを表示するには、［**Advanced Settings (詳細設定)**］をクリックします。

重要 :［**Advanced Settings (詳細設定)**］を選択して、localhost が設定されているフィールドを有効な IP アドレスまたは DNS 名に変更する必要があります。デフォルトのパラメータを localhost から変更しないと、設定は失敗します。

OSP server host (OSP サーバホスト)

OSP をインストールする計画で、LDAP 認証サーバにするサーバの 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。

OSP の詳細については、『NetIQ Identity Manager セットアップガイド』の Using Single Sign-on Access in Identity Manager を参照してください。

OSP keystore password (OSP キーストアパスワード)

OAuth サーバで新しいキーストアをロードするために作成するパスワードを指定します。

パスワードは 6 文字以上にする必要があります。

SSPR config password (SSPR 環境設定パスワード)

SSPR (Self-Service Password Reset) を設定するために作成するパスワードを指定します。

デフォルトでは、SSPR に環境設定パスワードは設定されていません。パスワードを設定しないと、SSPR にログイン可能なユーザであれば誰でも設定を変更できます。

Service password (サービスのパスワード)

SSPR、識別情報アプリケーション、および Identity Reporting で使用される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。

パスワードは 6 文字以上にする必要があります。

Identity Applications admin password (識別情報アプリケーション管理者のパスワード)

ユーザアプリケーションの管理者のパスワードを指定します。このアカウントは、インストールプロセス中に識別ボールト内に作成され、ユーザアプリケーションに対して指定したユーザコンテナの管理者タスクを実行する権利が付与されます。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、アカウント名は uaadmin です。
- ユーザアプリケーションをホストするアプリケーションサーバを起動したことがある場合、configupdate.sh ファイルまたは 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。
- 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］>［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、『*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。

idmadmin DB user password (idmadmin DB ユーザのパスワード)

識別情報アプリケーションのデータベースの管理者のパスワードを指定します。

デフォルトでは、アカウントは idmadmin です。

Tomcat shutdown port (Tomcat シャットダウンポート)

すべての Web アプリケーションと Tomcat を正常にシャットダウンするために使用するポートを指定します。デフォルトは 8105 です。

Tomcat HTTP port (Tomcat HTTP ポート)

Tomcat サーバがクライアントコンピュータとの通信に使用するポートを指定します。デフォルトは 8080 です。SSL を使用する場合、デフォルトは 8443 です。詳細については、『NetIQ Identity Manager セットアップガイド』の「署名入り証明書による SSL の有効化」を参照してください。

Tomcat redirect port (Tomcat リダイレクトポート)

(状況によって実行) TLS/SSL プロトコルを使用しない場合、SSL トランスポートを必要とする要求をアプリケーションサーバがリダイレクトする先のポートを指定します。デフォルトは 8543 です。

Tomcat AJP port (Tomcat AJP ポート)

(オプション) アプリケーションサーバが HTTP はなく AJP プロトコルを使用する Web コネクタと通信する場合に使うポートを指定します。デフォルトは 8109 です。

このパラメータは、アプリケーションサーバで Web アプリケーションに含まれる静的なコンテンツを管理する場合、またはアプリケーションサーバの SSL 処理を利用する場合に使用します。

Audit server host (監査サーバホスト)

Sentinel および Identity Reporting が使用する SIEM データベース (識別情報ウェアハウス) をホストするサーバの 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。

重要 : 識別情報アプリケーションを設定する前に、監査サーバをインストールして実行する必要があります。統合インストールプログラムが監査サーバと通信できない場合、設定は失敗します。

詳細設定

残りの設定はすべて［**Advanced Settings (詳細設定)**］にあります。［**Identity Application host (識別情報アプリケーションのホスト)**］フィールドを localhost から IP アドレスまたは DNS 名に変更する必要があります。［**Advanced Settings (詳細設定)**］を変更しなかった場合は、表示されているデフォルト設定が使用され、設定は失敗します。

Identity Applications Administrator (識別情報アプリケーション管理者)

識別情報アプリケーションの管理者アカウントの名前を指定します。デフォルト値は uaadmin です。

Identity Applications host (識別情報アプリケーションホスト)

アプリケーションサーバ上のユーザアプリケーションクライアントに接続する URL 設定を指定します。localhost は使用しないでください。

5.5 Identity Reporting Module

このセクションでは、Identity Reporting Module の設定を定義します。プログラムによって表示されるのは基本パラメータです。すべてのパラメータを表示するには、［**Advanced Settings (詳細設定)**］をクリックします。

重要 : Identity Reporting Module には Sentinel が必要です。Sentinel は Linux コンピュータ上でのみ実行されます。Windows コンピュータにインストールする場合、Windows 上の Identity Reporting Module の設定を続行するには、まず Linux コンピュータに Sentinel をインストールする必要があります。

Managed System Gateway port (Managed System Gateway のポート)

MSGW ドライバが識別ボールトとの通信に使用するポートを指定します。

デフォルトは 7707 です。

Data Collection Service host (データ収集サービスホスト)

データ収集サービスをホストするサーバの 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。

詳細設定

残りの設定はすべて［**Advanced Settings (詳細設定)**］にあります。［**Advanced Settings (詳細設定)**］を変更しなかった場合は、表示されているデフォルト設定が使用されます。

サブコンテナ検索の有効化

Identity Reporting Module でサブコンテナの検索をサポートするかどうかを選択します。デフォルトでは、このオプションは有効です。

Use secure LDAP connections (セキュア LDAP 接続を使用)

サーバがセキュア LDAP 接続を使用して通信するかどうかを選択します。

［**LDAP ポート**］も指定する必要があります。

LDAP ポート

識別ボールトをホストするサーバと通信するためのポートを指定します。35 ページのセクション 5.1「識別ボールト」で［**LDAP secure port (LDAP セキュアポート)**］に指定した値と同じ値を指定します。

非セキュア通信の場合は平文ポートを指定することもできます。その場合、［**Use secure LDAP connections (セキュア LDAP 接続を使用)**］は選択しないでください。

トークンの有効期限の値 (分)

認証用トークンの保持期間を指定します。デフォルト値は 60 分です。

Retain completed reports: Duration and Units (完了したレポートの保持 : 期間と単位)

Identity Reporting Module が完了したレポートを削除するまでの保持期間を選択します。たとえば、6 カ月を指定するには、期間に［**月**］を選択してから、単位に「6」を指定します。

サブコンテナのログイン属性

レポート用データの収集時に Identity Manager が指定したユーザコンテナのサブツリーを検索するために使用するログイン属性を指定します。デフォルト値は cn です。

注 : 特殊文字が使用されている DN を指定する場合、それらの文字をエスケープしなければならないことがあります。詳細については、RFC 2253/4514 のセクション 2 を参照してください。

SMTP server host (SMTP サーバホスト)

Identity Reporting Module 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。デフォルト値は localhost です。これを有効な IP アドレスまたは DNS 名に変更します。

SMTP サーバーポート

電子メールサーバのポート番号を指定します。デフォルトは 435 です。

SMTP userID (SMTP ユーザ ID)

(状況によって実行) 電子メールサーバとの通信に認証を使用する場合、認証に使用する電子メールアドレスを指定します。

［**Requires server authentication for SMTP (SMTP のサーバ認証が必要)**］も選択する必要があります。

SMTP ユーザのパスワード

認証に使用する電子メールアドレスに関連付けられたパスワードを指定します。

デフォルトの電子メールアドレス

Identity Reporting が電子メール通知の発信元として使用する電子メールアドレスを指定します。

SMTP に SSL を使用

電子メールサーバとの通信に SSL を使用するかどうかを指定します。デフォルトの設定では、このオプションは無効になっています。

Require server authentication for SMTP (SMTP のサーバ認証が必要)

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 userid (SMTP ユーザ ID)**］および［**SMTP ユーザのパスワード**］の値も指定する必要があります。デフォルトの設定では、このオプションは無効になっています。

5.6 ツール

このセクションでは、Identity Manager の各種ツール (iManager、Analyzer、および Designer) の設定を定義します。現在のところ、プログラム可能なパラメータを備えているのは iManager のみです。これらのパラメータは Linux コンピュータで設定中にのみ表示されます。すべてのパラメータを表示するには、［**Advanced Settings (詳細設定)**］をクリックします。

注 : 識別ボールトで使用する HTTP スタックポートとは異なる HTTP スタックポートを指定する必要があります。詳細については、『*NetIQ iManager Administration Guide*』を参照してください。

HTTP ポート

iManager が平文で通信する場合に使用するスタックポート番号を指定します。デフォルトは 8080 です。

Secure HTTP port (セキュア HTTP ポート)

iManager が TLS/SSL プロトコルを使用して通信する場合に使用するスタックポート番号を指定します。デフォルトは 8443 です。

6 統合インストールプロセスの最終手順

統合インストーラが完了したら、Identity Manager コンポーネントがインストールされ、基本設定が完了しています。ただし、さまざまなコンポーネントを完全に機能させるには、ドライバを作成して追加の設定手順を実行する必要があります。

6.1 パスワードポリシーオブジェクトのドライバセットへの割り当て

DirMXL-PasswordPolicy オブジェクトをアイデンティティボールトのツリーの各ドライバセットに割り当てる必要があります。統合インストールプロセスでは、ポリシーオブジェクトをアイデンティティボールトに追加しません。ただし、オブジェクトを作成できます。

- 45 ページのセクション 6.1.1「パスワードポリシーオブジェクトの作成」
- 46 ページのセクション 6.1.2「パスワードポリシーオブジェクトの割り当て」

6.1.1 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、以下の手順を使用して作成してください。

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 アイデンティティボールトに DirMXL-PasswordPolicy オブジェクトを追加するには、以下のアクションのいずれかを実行して、ファイルから属性をインポートします。

Linux:

ldapmodify ユーティリティを含むディレクトリから、次のコマンドを入力します。

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

次に例を示します。

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

ldapmodify ユーティリティは、デフォルトで /opt/novell/eDirectory/bin ディレクトリにあります。

Windows:

Identity Manager インストールキットの install/utilities ディレクトリから ldapmodify.exe を実行します。

6.1.2 パスワードポリシーオブジェクトの割り当て

DirMXL-PasswordPolicy オブジェクトをツリーの各ドライバセットに割り当てる必要があります。詳細については、『Password Management Administration Guide』の *Creating Password Policies* を参照してください。

6.2 Identity Manager コンポーネントの設定

インストール後に、Identity Manager コンポーネントの一部を設定する必要があります。

- **ドライバ :** ドライバごとに、そのドライバのインストールと設定の方法を説明した専用のガイドが用意されています。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。
- **識別情報アプリケーション :** ご使用の環境で動作するように、さまざまな識別情報アプリケーションを設定する必要があります。詳細については、次のガイドを参照してください。
  - NetIQ Identity Manager セットアップガイド
  - NetIQ Identity Manager - Identity アプリケーションの管理者ガイド
- **Identity Reporting:** ご使用の環境に合わせて Identity Reporting を設定する必要があります。詳細については、『*Administrator Guide to NetIQ Identity Reporting*』を参照してください。

7 Identity Manager 製品のアクティベート

このセクションの情報は、Identity Manager コンポーネントでアクティベーションが動作する仕組みについて説明します。Identity Manager コンポーネントは、インストール後 90 日以内にアクティベートする必要があります。そうしないと、90 日後にシャットダウンします。90 日以内のいつでも、またはその後でも、Identity Manager 製品をアクティベートするよう選択できます。以降のセクションの情報を使用して、Identity Manager コンポーネントをアクティベートします。

7.1 Identity Manager 製品のライセンスの購入

Identity Manager 製品ライセンスを購入し、製品をアクティベートするには、NetIQ Identity Manager 購入方法 Web ページ (https://www.netiq.com/products/identity-manager/advanced/how-to-buy/) を参照してください。

製品のライセンスをご購入になると、NetIQ よりカスタマ ID が送信されます。電子メールには、プロダクトアクティベーションキーを入手可能な NetIQ Web サイトの URL も含まれています。ご自分のカスタマ ID を思い出せない場合、またはカスタマ ID を受け取っていない場合は、担当者までお問い合わせください。

7.2 プロダクトアクティベーションキーのインストール

プロダクトアクティベーションキーは、iManager を使用してインストールする必要があります。

プロダクトアクティベーションキーをインストールする

1. ライセンスの購入後に、NetIQ からカスタマ ID が記載された電子メールが送信されます。電子メールの「注文の詳細」セクションには、キーを入手可能なサイトへのリンクが含まれています。リンクをクリックすると、サイトに移動します。
2. ライセンスのダウンロードリンクをクリックして、以下のいずれかを実行します。
   - プロダクトアクティベーションキーファイルを便利な場所に保存します。

     または
   - プロダクトアクティベーションキーファイルを開き、プロダクトアクティベーションキーの内容をクリップボードにコピーします。

     注意深く内容をコピーし、余分な線やスペースが含まれないようにします。資格情報の最初のダッシュ (-) から (----BEGIN PRODUCT ACTIVATION CREDENTIAL) 資格情報の最後のダッシュ (-) まで (END PRODUCT ACTIVATION CREDENTIAL-----) をコピーする必要があります。
3. iManager を開きます。
4. ［**Identity Manager**］>［Identity Manager の概要］の順に選択します。
5. ツリー構造でドライバセットを参照して選択します。
6. ［Identity Manager の概要］ページで、アクティブにするドライバを含むドライバセットをクリックします。

7 ［ドライバセットの概要］ページで、［**アクティベーション**］>［**インストール**］の順にクリックします。

8 Identity Manager コンポーネントをアクティブにするドライバセットを選択して、［**次へ**］をクリックします。

9 次のいずれかの操作を行います。

- Identity Manager アクティベーションキーを保存した場所を指定し、［**次へ**］をクリックします。

  または

- Identity Manager アクティベーションキーの内容をテキスト領域に貼り付け、［**次へ**］をクリックします。

10 ［**完了**］をクリックします。

注： ドライバが含まれる各ドライバセットをアクティベートする必要があります。資格情報によってツリーを有効にできます。

7.3 Identity Manager およびドライバのプロダクトアクティベーションの表示

ドライバセットごとに、Identity Manager エンジンと Identity Manager ドライバのためにインストールしたプロダクトアクティベーションキーを表示できます。

1 iManager を開きます。

2 ［**Identity Manager**］>［**Identity Manager の概要**］の順にクリックします。

3 ツリー構造でドライバセットを参照して選択してから、 をクリックして検索を実行します。

4 ［Identity Manager の概要］ページで、アクティベーション情報を表示するドライバセットをクリックします。

5 ［ドライバセットの概要］ページで、［**アクティベーション**］>［**情報**］の順にクリックします。

  アクティベーションキーのテキストを参照できます。エラーが報告された場合は、アクティベーションキーを削除できます。

注： ドライバセットの有効なプロダクトアクティベーションキーをインストールした後も、ドライバ名の横に「**アクティベーションが必要です**」と表示されることがあります。この場合、ドライバを再起動するとメッセージが消えます。

7.4 Identity Manager のドライバの有効化

購入した Identity Manager には、サービスドライバといくつかの一般的なドライバのアクティベーションが含まれています。

- **サービスドライバ：** Identity Manager エンジンを起動すると、次のサービスドライバがアクティベートされます。
  - データ収集サービス
  - エンタイトルメントサービス

- ID プロバイダ
- ループバックサービス
- Managed System Gateway
- 手動タスクサービス
- Null サービス
- 役割サービス
- ユーザアプリケーション
- WorkOrder

- **共通ドライバ：** Identity Manager エンジンを起動すると、次の一般的なドライバがアクティベートされます。
  - Active Directory
  - ADAM
  - eDirectory
  - GroupWise
  - LDAP
  - Lotus Notes

他のすべての Identity Manager ドライバのアクティベーションは別途購入する必要があります。ドライバのアクティベーションは、Identity Manager 統合モジュールとして販売されています。Identity Manager 統合モジュールには、1 つまたは複数のドライバを含めることができます。購入した Identity Manager 統合モジュールごとにプロダクトアクティベーションキーが提供されます。

Identity Manager 統合モジュールごとに 47 ページのセクション 7.2「プロダクトアクティベーションキーのインストール」の手順を実行し、ドライバを有効化する必要があります。

7.5 Analyzer のアクティベート

Analyzer を初めて起動すると、有効化するようにプロンプトが表示されます。アクティベーションを入力しないと Analyzer を使用できません。

7.6 Designer およびロールマッピング管理者の有効化

Designer およびロールマッピング管理者では、Identity Manager エンジンとドライバをアクティベートするだけで済み、追加作業は必要ありません。

8 Identity Manager のアンインストール

Identity Manager アンインストールウィザードを使用して、インストールされているすべての Identity Manager コンポーネントをアンインストールできます。各 Identity Manager コンポーネントのアンインストールの詳細については、『*NetIQ Identity Manager セットアップガイド*』の「Identity Manager のコンポーネントのアンインストール」を参照してください。

9 トラブルシューティング

統合インストールプログラムに関する問題をトラブルシューティングするには、次の情報を使用します。

9.1 ログファイルとプロパティファイルの場所

次の表には、インストールログ (ii_install.log)、環境設定ログ (ii_configure.log)、およびプロパティファイルの場所が記載されています。インストールされているコンポーネントごとにプロパティファイルがあります。

プラットフォーム	ログファイル	インストールのプロパティファイル
Windows	<*Install_Location*>\install\logs	<*Install_Location*>\install\propfiles
	デフォルトの場所 : C:\netiq\IdentityManager\install\logs	デフォルトの場所 : C:\netiq\IdentityManager\install\logs\propfiles\
Linux	/var/opt/netiq/idm/install/logs	/var/opt/netiq/idm/install/logs/propfiles/

9.2 設定の失敗のトラブルシューティング

コンポーネントの設定が失敗する場合は、次の情報を使用してトラブルシューティングします。

問題 : 識別情報アプリケーションの設定が失敗する。

推奨アクション : ログファイルにアクセスします。localhost という単語を検索します。ログでこの単語が見つかった場合は、設定時に［**Advanced Settings (詳細設定)**］のデフォルト値 localhost を有効な IP アドレスまたは DNS 名に変更していないことを意味します。もう一度設定を実行し、［**Advanced Settings (詳細設定)**］に有効な IP アドレスまたは DNS 名を入力します。

9.3 Windows でのリモートローダに関する問題のトラブルシューティング

デフォルトでは、統合インストールプログラムは、すべての Identity Manager コンポーネントを C:\NetIQ ディレクトリにインストールします。ドライバはすべて C:\Novell をデフォルトのディレクトリとして使用します。ただし、ドライバのディレクトリを手動で変更することで、ドライバを動作させることができます。

リモートローダドライバを動作させる

1. リモートローダコンソールを起動します。
2. 適切なドライバのインスタンスを追加します。
3. デフォルトのパスを C:\Novell から C:\NetIQ に変更します。
4. 通常の設定手順を続行します。

9.4 アンインストールのトラブルシューティング

アンインストールに関する問題をトラブルシューティングするには、次の情報を確認します。問題が続く場合は、NetIQ の担当者にお問い合わせください。

問題 : 完全にアンインストールされなかったことがアンインストールプロセスによって報告されるが、ログファイルにエラーが記録されていない。

推奨アクション : 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。すべての NetIQ ソフトウェアをコンピュータから削除済みの場合は、このディレクトリを手動で削除できます。