NetIQ® eDirectory™
インストールガイド

2019年10月

保証と著作権

保証と著作権、商標、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。

本書およびライブラリについて

この『*インストールガイド*』には、eDirectory 9.2のインストール方法が記載されています。本書の対象読者はネットワーク管理者です。

『*NetIQ eDirectory インストールガイド*』の最新版については、NetIQ eDirectory online documentationのWebサイトを参照してください。

本書の読者

このガイドはネットワーク管理者を対象としています。

ライブラリに含まれているその他の情報

ライブラリには次の情報リソースが含まれています。

管理ガイド

eDirectoryの管理および設定方法について説明します。

Linuxプラットフォーム用チューニングガイド

Linuxプラットフォーム上のeDirectoryを分析し、すべての展開において優れたパフォーマンスが実現されるように調整する方法について説明します。

これらのガイドは、NetIQ eDirectory 9.2 documentationのWebサイトで入手できます。

eDirectory管理ユーティリティの詳細については、『*NetIQ iManager管理ガイド*』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。改善のためのご提案は、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［**コメントを追加**］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Qmunity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Qmunityは、頼みにしているIT投資が持つ可能性を余すことなく実現するために必要な知識の習得に役立ちます。詳細については、http://community.netiq.comを参照してください。

1 インストールとアップグレードの機能

この章では、NetIQ eDirectory 9.2のインストールとアップグレードの機能について説明します。

次の表に、新機能とその新機能がサポートされるプラットフォームについて示します。

機能	Linux	Windows
eDirectory 9.2インストール用の複数のパッケージ形式	✓	✗
任意の場所へのアプリケーションファイルのインストール	✓	✓
任意の場所へのデータファイルのインストール	✓	✓
任意の場所への環境設定ファイルのインストール	✓	✗
非ルートユーザによるインストール	✓	✗
高可用性クラスタへのインストールに対する強化されたサポート	✓	✓
FHSの準拠	✓	✗
LSBの準拠	✓	✗
サーバのヘルスチェック	✓	✓
SecretStoreの統合	✓	✓
eDirectory Instrumentationインストール	✓	✓

このセクションでは、次の情報について説明します。

eDirectory 9.2インストール用の複数のパッケージ形式

Linuxでは、eDirectory 9.2をホストでインストールする時にさまざまなファイル形式を選択するオプションが用意されています。選択できるファイル形式を次の表に示します。

ユーザのタイプとインストール場所	Linux
ルートユーザ	
デフォルトの場所	RPM
任意の場所	tarball
非ルートユーザ	
任意の場所	tarball

tarballを使用したインストールの詳細については、30 ページの 「tarballデプロイメントのeDirectory 9.2をアップグレードする」を参照してください。

任意の場所にeDirectory 9.2をインストールする

eDirectory 9.2では、アプリケーション、データ、および環境設定ファイルをインストールする場所を自由に選択できます。

eDirectory 9.2を任意の場所にインストールするシナリオの1つは、ホストに以前のバージョンのeDirectoryがインストールされており、それをアップグレードする前にeDirectory 9.2をテストする場合です。このようにすると、既存のeDirectory設定を変更せずに、この新しいバージョンをテストすることもできます。その後で、既存のバージョンを保持するか、eDirectory 9.2にアップグレードするかを決定できます。

注: SLPとSNMPサブエージェントはデフォルトの場所にインストールされます。

このセクションでは、任意の場所にさまざまなファイルをインストールする方法について説明します。

- 12 ページの 「アプリケーションファイルに任意の場所を指定する」
- 13 ページの 「データファイルに任意の場所を指定する」
- 13 ページの 「環境設定ファイルに任意の場所を指定する」

アプリケーションファイルに任意の場所を指定する

eDirectoryのインストール中に、選択した場所にアプリケーションファイルをインストールできます。

Linux

eDirectory 9.2を任意の場所にインストールする場合、tarballインストールファイルを使用して、eDirectory 9.2を選択した場所に展開することができます。

Windows

eDirectory 9.2より前でも、インストールウィザードの実行中にアプリケーションファイルに任意の場所を指定することができました。

データファイルに任意の場所を指定する

eDirectoryの設定中に、選択した場所にデータファイルを保存できます。データファイルには、data、dib、およびlogディレクトリが含まれます。

Linux

任意の場所でデータファイルを設定する場合、ndsconfigユーティリティの-dまたは-Dオプションのいずれかを使用できます。

オプション	説明
-d *任意の場所*	指定したパスにDIB(eDirectoryデータベース)ディレクトリを作成します。 **注:** このオプションは、eDirectory 9.2より前にも存在しました。
-D *任意の場所*	data(pidやソケットIDなどのデータを含む)、dib、およびlogディレクトリを、指定したパスに作成します。

Windows

Windowsでは、インストール中にDIBパスを入力するように指示されます。選択するパスを入力してください。

環境設定ファイルに任意の場所を指定する

eDirectoryの設定中には、環境設定ファイルの保存先にするパスを選択できます。

Linux

nds.conf環境設定ファイルを異なる場所に設定するには、ndsconfigユーティリティの--config-fileオプションを使用します。

その他の環境設定ファイル(modules.conf、ndsimon.conf、およびice.confなど)を異なる場所にインストールするには、次の操作を実行します。

1. すべての環境設定ファイルを新しい場所にコピーします。
2. 次のように入力して新しい場所を設定します。

   ndsconfig set n4u.nds.configdir *任意の場所*

Windows

Windowsでは、環境設定ファイルに任意の場所を指定することはできません。

非ルートユーザによるインストール

eDirectory 9.2以上では、非ルートユーザによるeDirectoryサーバのインストールと設定がサポートされています。eDirectoryの以前のバージョンでは、ホストで実行されるeDirectoryの単一のインスタンスのみを、ルートユーザだけがインストールおよび設定できました。

eDirectory 9.2以上では、非ルートユーザがtarballビルドを使ってeDirectoryをインストールできます。同一または異なるユーザによるeDirectoryのバイナリインストールの複数インスタンスが存在できます。ただし、ルート以外のユーザのインストールに対しても、Novell International Cryptographic Infrastructure (NICI)、SNMP、およびSLPなどのシステムレベルのサービスはルート権限によってのみインストールが可能です。eDirectoryの機能のために、NICIは必須のコンポーネントで、SNMPとSLPはオプションのコンポーネントです。また、パッケージのインストールについては、シングルインスタンスのみがルートユーザによってインストール可能です。

インストール後に、非ルートユーザは個々のtarballインストールやバイナリインストールを用いて、eDirectoryサーバインスタンスの設定ができます。つまり、1つのホストでeDirectoryサーバの複数のインスタンスが実行できます。なぜなら、ルートユーザもルート以外のユーザも、パッケージやtarballインストールを用いることで、異なるeDirectoryサーバインスタンスを1つのホスト上で設定できるからです。複数インスタンスの機能の詳細については、31 ページの 「複数インスタンスをアップグレードする」を参照してください。

非ルートユーザによるインストールと設定は、Linuxプラットフォームでのみ適用可能です。非ルートユーザによるインストールや設定に関する詳細については、36 ページの 「非ルートユーザによるeDirectory 9.2のインストール」を参照してください。

標準の準拠

eDirectory 9.2は次の標準に準拠しています。

- 14 ページの 「FHSの準拠」
- 15 ページの 「LSBの準拠」

FHSの準拠

他製品のアプリケーションファイルとの間でファイルの衝突を回避するため、eDirectory 9.2はFHS (File system Hierarchy Standard)に従っています。この機能は、Linuxのみで使用できます。

eDirectoryがこのディレクトリ構造に従うのは、デフォルトの場所にインストールすることを選択した場合のみです。任意の場所を選択した場合、ディレクトリ構造は、*任意の場所* *デフォルトの場所*になります。

たとえば、eDir88ディレクトリにインストールすることを選択した場合、eDir88ディレクトリ内は同じディレクトリ構造になり、マニュアルページは、/eDir88/opt/novell/manディレクトリにインストールされます。

次の表に、ディレクトリ構造の変更を示します。

ディレクトリに保存されるファイルのタイプ	ディレクトリの名前とパス
実行ファイルのバイナリとスタティックシェルスクリプト	/opt/novell/eDirectory/bin

ディレクトリに保存されるファイルのタイプ	ディレクトリの名前とパス
ルートが使用する実行ファイルのバイナリ	/opt/novell/eDirectory/sbin
スタティックライブラリまたはダイナミックライブラリのバイナリ	/opt/novell/eDirectory/lib
環境設定ファイル	/etc/opt/novell/eDirectory/conf
読み書きを行う実行時のダイナミックデータ(DIBなど)	/var/opt/novell/eDirectory/data
ログファイル	/var/opt/novell/eDirectory /log
Linuxマニュアルページ	/opt/novell/man

環境変数のエクスポート

eDirectory 9.2でFHS実装を使用する場合は、パスの環境変数を更新してエクスポートする必要があります。これによって次の問題が生じます。

- エクスポートするすべてのパスを覚えておく必要があります。シェルを開くときには常に、これらのパスをエクスポートしてからユーティリティの使用を開始する必要があります。
- バイナリのセットを複数使用する場合は、複数のシェルを開くか、または設定を解除して異なるバイナリのセットへのパスを頻繁に設定する必要があります。

この問題を解決するため、/opt/novell/eDirectory/bin/ndspathスクリプトを次のように使用することができます。

- 次のとおり、ndspathスクリプトをユーティリティの前に指定して、ユーティリティを実行します。

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

- 次のとおり、現在のシェル内のパスをエクスポートします。

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

- このコマンドの入力後、通常どおりにユーティリティを実行します。プロファイル内のスクリプト(bashrc、または同様のスクリプト)を呼び出します。こうすることで、ログインするか新しいシェルを開けば、直接ユーティリティを使い始めることができます。

LSBの準拠

eDirectory 9.2はLSB (Linux Standard Base)に準拠するようになりました。LSBでは、FHSに準拠することも推奨されています。LinuxのeDirectoryパッケージにはすべて、*novell*というプリフィックスが付けられています。たとえば、NDSservの名前はnovell-NDSservになっています。

サーバのヘルスチェック

NetIQ eDirectoryには、アップグレード前にサーバが安全な状態であるかどうかを判断するのに役立つ、サーバのヘルスチェックが組み込まれています。

サーバのヘルスチェックは、どのアップグレードでもデフォルトで実行され、パッケージが実際にアップグレードされる前に行われます。ただし、診断ツールのndscheckを実行してヘルスチェックを行うこともできます。

定期的なヘルスチェックの手順の詳細については、『NetIQ eDirectory管理ガイド』の「*NetIQ eDirectoryのメンテナンス*」を参照してください。

ヘルスチェックの必要性

eDirectoryの以前のリリースでは、アップグレードを進める前にサーバの状態はチェックされませんでした。状態が不安定であると、アップグレード処理が失敗し、eDirectoryは不整合な状態になってしまいます。場合によっては、アップグレード前の設定に戻すことができない場合もあります。

新しいヘルスチェックツールによってこの問題が解決され、サーバをアップグレードする準備を確実に整えることができます。

サーバが正常であることの確認基準

サーバヘルスチェックのユーティリティは、ツリーが正常に機能していることを確認するため、所定のヘルスチェックを実行します。これらのヘルスチェックがすべて正しく完了すると、ツリーは正常に機能していると見なされます。

ヘルスチェックを実行する

サーバのヘルスチェックは次の2種類の方法で実行できます。

- 16 ページの 「アップグレードと同時に実行」
- 17 ページの 「スタンドアロンユーティリティとして実行」

注: ヘルスチェックユーティリティを実行するには、管理者の権利を持っている必要があります。ユーティリティを実行するために設定できる最小限の権利はパブリックの権利です。ただし、パブリックの権利では、NetWareコアプロトコル(NCP)オブジェクトの一部とパーティション情報が利用できません。

アップグレードと同時に実行

eDirectoryをアップグレードするときは常に、デフォルトでヘルスチェックが実行されます。

Linux

アップグレード時には常にデフォルトで、実際のアップグレード処理が開始される前にヘルスチェックが実行されます。

デフォルトのヘルスチェックを省略するため、nds-installユーティリティで「-j」オプションを使用することができます。

Windows

サーバのヘルスチェックは、インストールウィザードの一部として行われます。ヘルスチェックは、プロンプトが表示されたときに有効または無効にすることができます。

スタンドアロンユーティリティとして実行

サーバのヘルスチェックは、いつでもスタンドアロンユーティリティとして実行できます。次の表では、ヘルスチェックユーティリティについて説明します。

表 1-1 *ヘルスチェックユーティリティ*

プラットフォーム	ユーティリティ名
Linux	ndscheck 構文: `ndscheck -h hostname:port -a admin_FDN -F logfile_path --config-file configuration_file_name_and_path` **注:** -hまたは--config-fileを指定できますが、両方のオプションを同時に指定することはできません。
Windows	ndscheck

ヘルスチェックのタイプ

アップグレード時やndscheckユーティリティを実行する場合、次のタイプのヘルスチェックが行われます。

- 基本的なサーバの状態
- パーティションとレプリカの状態

ndscheckユーティリティを実行すると、ヘルスチェックの結果は画面に表示され、ndscheck.logに記録されます。ログファイルの詳細については、「19ページの 「ログファイル」」を参照してください。

アップグレードの一部としてヘルプチェックを実行した場合、ヘルスチェックの後にエラーの深刻度に基づいて、アップグレードを続行するかどうかの確認が求められるか、または処理が中断されます。エラーの詳細については、「18 ページの 「状態のカテゴリ」」に記載されています。

基本的なサーバの状態

これは、ヘルスチェックの最初の段階です。ヘルスチェックユーティリティは次の内容をチェックします。

1. eDirectoryサービスが動作している。DIBが開いていて、ツリー名などの基本的なツリー情報を読むことができる。
2. サーバがそれぞれのポート番号を監視している。

LDAPに関しては、TCPポート番号とSSLポート番号を取得して、サーバがこれらのポートを監視しているかどうかをチェックします。

同様に、HTTPセキュアポート番号とHTTPSセキュアポート番号を取得して、サーバがこれらのポートを監視しているかどうかをチェックします。

パーティションとレプリカの状態

基本的なサーバの状態のチェック後は、次のとおり、パーティションとレプリカの状態をチェックします。

1. ローカルに保持されているパーティションのレプリカの状態をチェックします。
2. サーバによって保持されているすべてのパーティションのレプリカリングを読み込み、レプリカリング内のすべてのサーバが動作していて、すべてのレプリカが使用可能な状態であることをチェックします。
3. レプリカリング内のすべてのサーバについて、時刻同期を確認します。これによって、サーバ間の時刻の差が表示されます。

状態のカテゴリ

サーバの状態は、チェック中に検出されるエラーに基づいて、次の3つカテゴリに分類されます。ヘルスチェックのステータスは、ログファイルに記録されます。詳細については、「19 ページの「ログファイル」」を参照してください。

ヘルスチェックのステータスは、正常、警告、および重大の3つに分類されます。

正常

ヘルスチェックが成功した場合、サーバの状態は正常です。

アップグレードは中断されずに続行されます。

警告

ヘルスチェック中に小さなエラーが見つかった場合、サーバの状態は警告に分類されます。

アップグレードの一部としてヘルスチェックが実行されている場合、中止するか続行するかの確認を求められます。

警告は通常、次の状況で発生します。

1. サーバがLDAPポートとHTTPポート(通常、セキュリティ保護、または両方)を監視していない。
2. レプリカリング内のいずれの非マスタサーバにも接続できない。
3. レプリカリング内のサーバが同期していない。

重大

ヘルスチェック中に致命的なエラーが見つかった場合、サーバの状態は重大に分類されます。

ヘルスチェックがアップグレードの一部として実行されている場合、アップグレード操作は破棄されます。

重大な状態は通常、次の状況で発生します。

1. DIBを開くことができないか読み込むことができない。DIBはロックされているか破損している可能性があります。
2. レプリカリング内のすべてのサーバに接続できない。
3. ローカルに保持されているパーティションが使用中である。
4. レプリカが使用可能な状態ではない。

ログファイル

サーバヘルスチェック操作は、アップグレードで実行される場合も、スタンドアロンユーティリティとして実行される場合も、状態をログファイルに保存します。

ログファイルの内容は、チェック実行時に画面に表示されるメッセージと同様です。

ヘルスチェックのログファイルには、次のものが含まれています。

- ヘルスチェックのステータス(正常、警告、または重大)。
- NetIQのサポートサイトのURL。

次の表に、さまざまなプラットフォームでのログファイルの場所を示します。

***表 1-2** ヘルスチェックのログファイルの場所*

プラットフォーム	[ログファイル名]	[ログファイルの場所]
Linux	ndscheck.log	ndscheck -Fユーティリティで指定した場所に依存します。 -Fオプションを使用しない場合は、次に示すように、コマンドラインで指定した別のオプションによって、ndscheck.logファイルの場所が決定されます。 1. -hオプションを使用した場合、ndscheck.logファイルはユーザのホームディレクトリに保存されます。 2. --config-fileオプションを使用した場合、ndscheck.logファイルはサーバインスタンスのログディレクトリに保存されます。または、インスタンスの一覧からインスタンスを選択することもできます。
Windows	ndscheck.log	*インストールディレクトリ*

SecretStoreとeDirectoryとの統合

eDirectory 9.2には、eDirectoryの設定中にNovell SecretStore 3.4を設定するオプションが用意されています。eDirectory 9.0以前は、SecretStoreを手動でインストールする必要がありました。

SecretStoreは、簡単で安全なパスワード管理ソリューションです。SecretStoreでは、eDirectoryに対する1つの認証を使用して、Linux、Windows、Web、およびメインフレームアプリケーションのほとんどにアクセスすることができます。

eDirectoryによる認証が完了すると、SecretStoreに対応するアプリケーションは、適切なログインアカウント情報の格納と取得を行います。SecretStoreを使用すると、パスワード保護されているアプリケーション、Webサイト、およびメインフレームへのアクセスに必要なパスワードをすべて記憶しておいたり、同期したりする必要がなくなります。

eDirectoryとともにSecretStore 3.4を設定するには、次の操作を実行できます。

- **Linux:**

  ndsconfig add -m ssパラメータを使用します。ここでssは、SecretStoreを表すオプションのパラメータです。モジュール名を指定しない場合は、すべてのモジュールがインストールされます。SecretStoreを設定しない場合は、-m no_ssを指定することで、このオプションにno_ss値を渡します。
- **Windows:**

  eDirectoryをインストールする際に、SecretStoreモジュールの設定をするかどうかを指定するオプションがあります。デフォルトでは、このオプションは選択されています。

SecretStoreの使用法に関する詳細については、『*Novell SecretStore 3.4 Administration Guide (Novell SecretStore 3.4管理ガイド)* (https://www.netiq.com/documentation/secretstore34/)』を参照してください。

eDirectory Instrumentationインストール

以前のeDirectory Instrumentationは、Novell Auditに組み込まれていました。eDirectory Instrumentationは、別途インストールする必要があります。

eDirectory Instrumentationのインストール、設定、およびアンインストールの詳細については、『NetIQ eDirectory管理ガイド』の「*eDirectoryイベントの監査*」を参照してください。

その他の情報

この章で説明する機能の詳細については、次のマニュアルを参照してください。

- *NetIQ eDirectory管理ガイド*
- Linuxについて: nds-install、ndsconfig、およびndscheckのマニュアルページ

2 NetIQ eDirectoryのLinuxへのインストールまたはアップグレード

LinuxサーバでNetIQ eDirectory 9.2をインストールまたはアップグレードする場合は、次の情報を参照してください。

システム要件

eDirectoryは、最小要件として以下のいずれかの64ビットのプラットフォームにインストールする必要があります。

- メモリ
  - eDirectoryサーバをインストールするための300MBの空きディスク容量
  - 50,000ユーザごとに150MBの空きディスク容量
- 仮想化システム
  - VMware ESXi
- 次のいずれかのオペレーティングシステムが必要です。

  次の表は、アイデンティティボールトが動作可能な、認定済みサーバオペレーティングシステムおよびサポートされているサーバオペレーティングシステムのリストを示しています。

  重要: 認定済みとは、完全にテストされてサポートされているオペレーティングシステムを意味します。ただし、サポートされているオペレーティングシステムとして一覧表示されている場合は、まだテストされていないが、機能することが想定されていることを意味します。

認定済みサーバオペレーティングシステムのバージョン	サポートされているオペレーティングシステム	備考
SUSE Linux Enterprise Server 12 (SLES) SP3およびSP4	新しいバージョンのサポートパックでサポート	システム要件に関する最新情報については、『リリースノート』を参照してください。

認定済みサーバオペレーティングシステムのバージョン	サポートされているオペレーティングシステム	備考
SUSE Linux Enterprise Server 15およびSLES 15 SP1	新しいバージョンのサポートパックでサポート	システム要件に関する最新情報については、『リリースノート』を参照してください。 **注:** SLES 15 でndstraceおよびldif2dibユーティリティを使用するには、SLES 15リポジトリからncursesのバージョン5をインストールします。
Red Hat Enterprise Linux (RHEL) 7.6、7.7	新しいバージョンのサポートパックでサポート	システム要件に関する最新情報については、『リリースノート』を参照してください。 **注:** eDirectory 9.0 SP4以降では、RHEL 7.xでの非ルートインストールがサポートされています。
RHEL 8.0	新しいバージョンのサポートパックでサポート	システム要件に関する最新情報については、『リリースノート』を参照してください。 **注** ◆ RHEL 8でndstraceおよびldif2dibユーティリティを使用するには、RHEL 8リポジトリからncursesのバージョン5をインストールします。 ◆ RHEL 8では、SELinuxをpermissiveモードに設定する必要があります。

実行しているSUSE Linuxのバージョンを調べるには、/etc/os-releaseファイルを確認します。

Red Hatシステムに、Red Hat Errataから配布されている最新のglibc (http://rhn.redhat.com/errata)パッチ(32ビットと64ビットの両方)が適用されていることを確認してください。glibcライブラリのバージョンは2.4以上である必要があります。

注: Bツリーファイルシステム(BTRFS)はeDirectoryでサポートされていません。

eDirectoryのバージョンの確認

eDirectoryのバージョンを確認するには、次のいずれかの手順を実行します。

- ndsstatを実行する。

  ndsstatユーティリティにより、eDirectoryツリー名、完全に識別されたサーバ名、およびeDirectoryバージョンなど、eDirectoryサーバに関連する情報が表示されます。次の例のeDirectory 9.2は製品バージョン(マーケティング文字列)を示し、40201.12はバイナリバージョン(内部ビルド番号)を示します。

```
osg-dt-srv17:/>ndsstat
Tree Name: SNMP-HPUX-RASH
Server Name: .CN=osg-dt-srv17.O=novell.T=SNMP-HPUX-RASH.
Binary Version: 40201.12
Root Most Entry Depth: 0
Product Version: eDirectory for Linux x86_64 v9.2 [DS]
```

ndsstatの実行方法の詳細については、『「NetIQ eDirectory管理ガイド」』の「NetIQ eDirectory用のLinuxコマンドとそれらの使用法」またはndsstatのマニュアルページ(ndsstat.1m)を参照してください。

- ndsd --versionを実行する。

  ndsdの実行方法の詳細については、『「NetIQ eDirectory管理ガイド」』の「NetIQ eDirectory用のLinuxコマンドとそれらの使用法」またはndsdのマニュアルページ(ndsd.1m)を参照してください。

- iMonitorを実行する。

  エージェントの概要ページで［認識サーバ］をクリックします。次に、［データベースで認識されているサーバ］の下にある［認識サーバ］をクリックします。［エージェントリビジョン］カラムに各サーバの内部ビルド番号が表示されます。たとえば、NetIQ eDirectory 9.2のエージェントリビジョン番号は40002.79などです。

  iMonitorの実行の詳細については、『「NetIQ eDirectory管理ガイド」』の「*iMonitorへのアクセス*」を参照してください。

- rpm -qi NDSservを実行する。

  このコマンドを入力すると、ndsd --versionに似た情報が表示されます。

前提条件

重要: 既存のeDirectory環境をアップグレードする前に、現在インストールされているNetIQアプリケーションとサードパーティ製アプリケーションがeDirectory 9.2に対応しているかどうかを確認してください。他のNetIQ製品の前提条件は、NetIQ Documentationサイト (http://www.netiq.com/documentation/)で確認できます。eDirectoryインスタンスをアップグレードする前に、そのインスタンスをバックアップすることをお勧めします。

- ❒ オペレーティングシステムに基づいて、次のRPMをインストールするようにしてください。
  - **RHEL 7.x:** yum-utilsおよびcreaterepo
  - **RHEL 8.x:** dnf-utilsおよびcreaterepo
  - **SLES:** Zypper
- ❒ (状況によって実行) Novell International Cryptographic Infrastructure (NICI) 3.2およびeDirectory 9.2でサポートされているキーサイズは、最大8192ビットです。8KBのキーサイズを使用するには、すべてのサーバがeDirectory 9.2にアップグレードされている必要があります。また、iManagerなどの管理ユーティリティを使用しているすべてのワークステーションにNICI 3.2がインストールされている必要があります。

  認証局(CA)サーバをeDirectory 9.2にアップグレードするとき、キーサイズは変更されず、2Kのままになります。8Kのキーサイズを作成するには、eDirectory 9.2サーバでCAを再作成する必要があります。また、CAを作成する際に、デフォルトのキーサイズを2Kから8Kに変更する必要があります。

eDirectoryをインストールすると、 nds-installユーティリティが自動的にNICIをインストールします。eDirectoryのインストールの詳細については、「33 ページの 「nds-installユーティリティを使用してeDirectoryコンポーネントをインストールする」」を参照してください。ただし、管理ユーティリティがインストールされているワークステーションに、eDirectoryそのものではなくNICIだけをインストールする必要がある場合は、NICIを手動でインストールする必要があります。NICIの手動インストールの詳細については、「37 ページの 「NICI のインストール」」を参照してください。

- ❒ (状況によって実行)サービスロケーションプロトコル(SLP)は、DNSが使用できないときにSLPを使用してツリー名を解決する計画の場合に限り、インストールおよび設定する必要があります。

  eDirectory 9.2では、SLPはeDirectoryインストールの一部としてインストールされません。

  ルートユーザだけがSLPをインストールできます。

  SLPのインストールの詳細については、「32 ページの 「eDirectoryでのSLPの使用」」を参照してください。

注: SLPサービスは、eDirectory 9.1以上では動作しません。

- ❒ マルチキャストルーティングを使用するためのLinuxホストの有効化

  マルチキャストルーティングを使用するためにホストが有効になっていることを確認するには、次のコマンドを入力します。

  ```
  /bin/netstat -nr
  ```

  ルーティングテーブルに、次のエントリがあればマルチキャストルーティングが有効になっています。

  ```
  224.0.0.0 0.0.0.0
  ```

  このエントリがない場合は、rootとしてログインし、次のコマンドを入力してマルチキャストルーティングを有効にします。

  ```
  route add -net 224.0.0.0 netmask 240.0.0.0 dev interface
  ```

  *interface*は、取り付けられ、使用されているNICに応じて、eth0、hme0、hme1、またはhme2などの値になります。

  マルチキャストおよびブロードキャストルータの詳細については、OpenSLP Webサイト (http://www.openslp.org/doc/html/UsersGuide/Installation.html)を参照してください。

- ❒ ネットワークサーバ時刻が同期されている

  すべてのネットワークサーバの時刻を同期するには、NTP (ネットワーク時刻プロトコル)のntpを使用します。

- ❒ (状況によって実行)セカンダリサーバをインストールする場合は、製品をインストールするパーティション内のレプリカがすべて、オンの状態になっている必要があります。

- ❒ (状況によって実行)管理者以外のユーザとしてセカンダリサーバを既存のツリーにインストールしている場合、コンテナを作成し、そのコンテナをパーティションで分割します。次の権限を持っていることを確認します。

  - 対象のパーティションに対するスーパバイザ権。
  - すべての属性権: W0.KAP.Securityオブジェクトに対する読み込み権、比較権、および書き込み権。
  - エントリ権: Securityコンテナオブジェクトに対するブラウズ権。

- すべての属性権: Securityコンテナオブジェクトに対する読み込み権、比較権。
- (状況によって実行)W1.KAP.Securityオブジェクトが存在する場合は、すべての属性権: このオブジェクトに対する読み込み権、比較権、および書き込み権。W1.KAP.Securityオブジェクトの詳細については、『NICI Administration Guide (NICI管理ガイド)』の「*Creating an AES 256-Bit Tree Key (AES 256 ビットツリーキーを作成する)*」を参照してください。

❒ (状況によって実行)管理者以外のユーザとしてセカンダリサーバを既存のツリーにインストールしている場合、ツリー内の少なくとも1台のサーバのeDirectoryバージョンが、コンテナ管理者として追加しているセカンダリのeDirectoryバージョンと同じかそれ以上である必要があります。追加しているセカンダリの方が新しいバージョンである場合、ツリーの管理者がスキーマを拡張してから、コンテナ管理者でセカンダリを追加する必要があります。

❒ セカンダリサーバを追加できるように、eDirectoryの設定中に、SLPサービスとファイアウォールのNetWare Core Protocol (NCP)ポート(デフォルトは524)を必ず有効にしてください。必要に応じて、さらに以下のサービスポートも有効にできます。

- LDAP (クリアテキスト) - 389
- LDAP (セキュリティ保護) - 636
- HTTP (クリアテキスト) - 8028
- HTTP (セキュリティ保護) - 8030

ユーザ定義ポートを有効にしてある場合は、eDirectoryの設定時にそのポートを指定する必要があります。

注: このステップはシステムにサービスロケーションプロトコル(SLP)が設定されている場合にのみ必要です。

❒ eDirectory 8.8 SP8以降のバージョンを9.2にアップグレードする際に、ユーザ定義ポートを8008および8010に設定しないでください。ポートを8008または8010に設定すると、ndsconfigの実行時に、サーバがeDirectory 8.8.*x*より前のサーバであると想定され、ポートが自動的に8028および8030にリセットされます。

❒ 以前のバージョンでSecretStoreがまだ設定されていなかった場合、またはSecretStoreを設定しない場合は、eDirectoryアップグレードの際に、-m no_ssオプションを指定してnds-installユーティリティを使用してください。

❒ eDirectory 9.2へのアップグレード中に最新のプラットフォームエージェント(PA)がインストールされていない場合は、場所<eDirectory build extracted folder>/eDirectory/setup/からnovell-AUDTplatformagent-2.0.2-80.x86_64.rpmファイルを実行してインストールしてください。

❒ NetIQ eDirectory管理ツールボックス(eMBox)を使用すると、サーバ上でもリモートでもeDirectoryのバックエンドユーティリティすべてにアクセスできます。コマンドラインクライアントは、Javaアプリケーションです。これを実行するには、Oracle Javaの最新バージョン(1.8以上)をインストールする必要があります。また、古いバージョンのJavaすべてで、使用可能なパッチアップグレードをインストールしてアップグレードしてください。最新バージョンのJavaをインストールしたら、次の環境変数をエクスポートします。

- EDIR_JAVA_HOME
- JAVA_HOME
- JRE_HOME

注:

- 前述の環境変数が何も検出されないと、コマンドラインクライアントはデフォルトPATH環境変数でJavaバイナリを検索します。
- eDirectory 9.0 SP4より前のバージョンを使用している場合、コマンドラインクライアントを実行するには、eDirectoryと一緒にインストールされたJavaランタイム環境(Oracle Java 1.8)にアクセスできなければなりません。

スタティックIPアドレスを設定する

eDirectoryを効率的に実行するには、サーバでスタティックIPアドレスが設定されている必要があります。DHCPアドレスのサーバにeDirectoryを設定すると、予期しない結果が発生することがあります。

ハードウェア要件

ハードウェア要件は、eDirectoryの実装条件によって異なります。キャッシュメモリの量とプロセッサの速さという、2つの要因によってパフォーマンスが向上します。最適な結果を得るためには、ハードウェアで可能な限り多くのDIB (Directory Information Base)セットをキャッシュに入れるようにします。

eDirectoryはシングルプロセッサ上で良好に動作します。しかし、NetIQ eDirectory 9.2なら、マルチプロセッサの利点を活用できます。プロセッサを追加すると、ログインなど、一部の領域のパフォーマンスが向上します。また、複数のプロセッサ上で複数のスレッドをアクティブにすることでもパフォーマンスは上がります。eDirectory自体は、プロセッサ集約型ではなく、入出力集約型です。

次の表に、eDirectory for Linuxの一般的なシステム要件を示します。

オブジェクト	メモリ	ハードディスク
100,000	2GB以上	300MB
100万	4GB	1.5GB
1,000万	4GB以上	15GB

バックリンク処理の強制実行

NetIQ eDirectoryにアップグレードすると内部eDirectory識別子が変わるため、オブジェクトの整合性を保つために、バックリンクされたオブジェクトを更新するバックリンク処理を行う必要があります。

バックリンクでは、他のサーバ上のオブジェクトへの外部参照が追跡されます。バックリンク処理は、サーバ上の各外部参照について、実オブジェクトが正しい位置に存在することを確認するほか、マスタレプリカのすべてのバックリンク属性を確認します。バックリンク処理はデータベースがオープンされた2時間後に実行され、その後780分(13時間)ごとに実行されます。実行間隔には、2分から10,080分(7日)までの任意の値を設定できます。

eDirectoryにマイグレーションした後、ndstrace -l>log&コマンドを発行して、DSTrace処理を開始します。この処理はバックグラウンドで実行されます。これにより、バックリンクプロセス結果を適切に分析できます。分析には4～10分かかります。DSTrace OSのコマンドプロンプトからndstrace -c 'set ndstrace=*B'コマンドを発行して、バックリンク処理を強制実行することができます。最初の手順で作成されたログファイルの結果を確認します。次に、ndstrace -uコマンドを発行してDSTrace処理をアンロードします。バックリンク処理の実行は、レプリカが存在しないサーバ上では特に重要です。

eDirectoryをアップグレードする

eDirectoryのアップグレードでは、eDirectory 8.8.8.x 64ビットからeDirectory 9.2 64ビットへのアップグレードが可能です。

注: 32ビットバージョンのeDirectoryを64ビットバージョンのeDirectoryにアップグレードするには、まず32ビットバージョンをeDirectory 8.8.x 64ビットバージョンにアップグレードし、次にそれをeDirectory 9.2にアップグレードします。64ビットのeDirectoryをeDirectory 9.2にアップグレードする場合と同じ手順に従います。

次のセクションでは、インストール済みの既存のeDirectoryを現在のバージョンにアップグレードするのに役立つ情報を提供します。

- 27 ページの 「サーバのヘルスチェック」
- 28 ページの 「OES以外のLinuxサーバでのアップグレード」
- 28 ページの 「Linux上でのeDirectoryの無人アップグレード」
- 30 ページの 「tarballデプロイメントのeDirectory 9.2をアップグレードする」
- 31 ページの 「複数インスタンスをアップグレードする」

注: ndsconfig upgradeコマンドは、HTTP、LDAP、SNMP、SAS、およびNMAS (NetIQ Modular Authentication Service)などの個別のコンポーネントで必要な環境設定をアップグレードするために使用します。

サーバのヘルスチェック

eDirectory 9.2の場合、eDirectoryのアップグレードの際に、デフォルトでサーバヘルスチェックが実行され、サーバをアップグレードしても安全かどうかが確認されます。

- 161 ページの 「パーティションとレプリカの状態」

ヘルスチェックの結果に基づいて、次のようにアップグレードが継続または中止されます。

- すべてのヘルスチェックに成功すると、アップグレードは継続されます。
- あまり重大でないエラーの場合、アップグレードを継続するか中止するかを問うメッセージが表示されます。
- 重大なエラーの場合、アップグレードは中止されます。

あまり重大でないエラーと重大なエラーの一覧については「159 ページの付録 B「eDirectoryヘルスチェック」」を参照してください。

サーバのヘルスチェックのスキップ

サーバのヘルスチェックをスキップするには、インストールフォルダからnds-install -jまたはndsconfig upgrade -jを実行します。

詳細については、「159 ページの付録 B「eDirectoryヘルスチェック」」を参照してください。

OES以外のLinuxサーバでのアップグレード

eDirectoryのアップグレードはeDirectory 8.8 以降でサポートされます。

アップグレードするには、nds-installユーティリティを使用します。このユーティリティは、Linuxプラットフォーム用にダウンロードしたファイルのSetupディレクトリにあります。Setupディレクトリから次のコマンドを入力します。

```
./nds-install
```

eDirectory 9.2にアップグレードすると、環境設定ファイル、データファイル、およびログファイルのデフォルトの保存先は、それぞれ/etc/opt/novell/eDirectory/conf、/var/opt/novell/eDirectory/data、/var/opt/novell/eDirectory/logに変わります。

新しい/var/opt/novell/eDirectory/dataディレクトリは、/var/ndsディレクトリへのシンボリックリンクを使用します。

古い環境設定ファイル/etc/nds.confは、/etc/opt/novell/eDirectory/confディレクトリに移行されます。古い環境設定ファイル/etc/nds.conf、および/var/ndsにある古いログファイルは参照できるように保持されます。

注: DIBのアップグレードが失敗し、nds-installから指示があった場合は、nds-install実行後にndsconfig upgradeを実行してください。RHEL 6.8から7.1へのOSのアップグレード後にeDirectoryサービスが開始しない場合、ndsconfig upgradeコマンドを実行してください。

注: 時刻同期が原因でヘルスチェックに失敗することがあります。この問題を解決するには、インスタンス間で時刻同期を実行してください。アップグレード中のこの警告メッセージは無視してもかまいません。

Linux上でのeDirectoryの無人アップグレード

Linux用のeDirectoryには、無人アップグレードを円滑に行うためのスイッチ、オプション、インストールスクリプト、および環境設定ユーティリティが用意されています。以降のセクションで、LinuxでeDirectoryを無人アップグレードするためのさまざまな手順について説明します。

1. eDirectoryのヘルスチェックを実行します。

   アップグレードが計画されているすべてのルートインスタンスのヘルスチェックは、ndscheckユーティリティを使って、手動で実行します。

   1a LD_LIBRARY_PATHを次の場所にエクスポートします:*<eDirectoryをuntarした場所>*/eDirectory/setup/utils

   1b 次のいずれかのコマンドを使って、ndscheckを実行します。

   ```
   <untarred location of eDirectory>/eDirectory/setup/utils/ndscheck -a <user name> -w passwd --config-file <nds.conf with absolute path>
   ```

環境変数からパスワードを渡す場合: *<88SP8をuntarした場所>*/eDirectory/setup/utils/ndscheck -a <*ユーザ名*> -w env:<*環境変数*> --config-file <*絶対パスで指定したnds.conf*>

ファイルからパスワードを渡す場合: *<88SP8をuntarした場所>*/eDirectory/setup/utils/ndscheck -a <*ユーザ名*> -w file:<*ファイル名*> --config-file <*絶対パスで指定したnds.conf*>

いずれも、ヘルスチェックの自動化スクリプトで使用できます。次に例を示します。

```
/Builds/eDirectory/utils/ndscheck -a admin.novell -w n
/Builds/eDirectory/utils/ndscheck -a admin.novell -w env:ADM_PASWD
/Builds/eDirectory/utils/ndscheck -a admin.novell -w file:adm_paswd
```

2 eDirectory 9.2パッケージをアップグレードします。

2a 以下のようにnds-installスクリプトを実行して、パッケージをアップグレードします。

```
nds-install -u -i -j
```

3 次の環境変数を更新します。

```
PATH=/opt/novell/eDirectory/bin:/opt/novell/eDirectory/sbin:$PATH
LD_LIBRARY_PATH=/opt/novell/eDirectory/lib:/opt/novell/eDirectory/lib/nds-
modules:/opt/novell/lib:$LD_LIBRARY_PATH
MANPATH=/opt/novell/man:/opt/novell/eDirectory/man:$MANPATH
TEXTDOMAINDIR=/opt/novell/eDirectory/share/locale
```

4 ndsconfigユーティリティで、すべてのルートインスタンスに対して以下のコマンドを実行してeDirectoryをアップグレードします。

```
ndsconfig upgrade -a <user name> -w passwd -c --config-file <nds.conf with absolute
path> --configure-eba-now <yes/no>
```

注: 拡張バックグラウンド認証を有効にするには、ndsconfig upgradeコマンドの--configure-eba-nowスイッチで*yes*を指定します。有効にしない場合は、*no*を指定して後から設定します。

環境変数からパスワードを渡す場合: ndsconfig upgrade -a <*ユーザ名*> -w env:<*環境変数*> -c --config-file <*絶対パスで指定したnds.conf*> --configure-eba-now <yes/no>

ファイルからパスワードを渡す場合: ndsconfig upgrade -a <*ユーザ名*> -w file:<*絶対/相対パスで指定したファイル名*> -c --config-file <*絶対パスで指定したnds.conf*> --configure-eba-now <yes/no>

上記のいずれの方法も、eDirectoryアップグレードの自動化スクリプトで使用できます。次に例を示します。

```
ndsconfig upgrade -a admin.novell -w n -c -–config-file /etc/opt/novell/
eDirectory/conf/nds.conf --configure-eba-now <yes/no>

ndsconfig upgrade -a admin.novell -w env:ADM_PASWD -c --config-file /etc/opt/
novell/eDirectory/conf/nds.conf --configure-eba-now <yes/no>

ndsconfig upgrade -a admin.novell -w <password file path>/adm_paswd -c --
config-file /etc/opt/novell/eDirectory/conf/nds.conf --configure-eba-now <yes/
no>
```

tarballデプロイメントのeDirectory 9.2をアップグレードする

tarballデプロイメントをeDirectory 8.8からeDirectory 9.2にアップグレードする場合、次の手順を実行してください。

1. tarballビルドをダウンロードします。
2. 次の環境設定ファイルのバックアップを作成します。
   - $NDSHOME/eDirectory/etc/opt/novell/eDirectory/conf/ndsimon.conf
   - $NDSHOME/eDirectory/etc/opt/novell/eDirectory/conf/ice.conf
   - $NDSHOME/eDirectory/etc/opt/novell/eDirectory/conf/ndsimonhealth.conf
   - $NDSHOME/eDirectory/etc/opt/novell/eDirectory/conf/ndssnmp/ndssnmp.cfg
   - $NDSHOMEは、eDirectoryがインストールされている場所です。
3. eDirectory 8.8 SP1未満のバージョンをアップグレードする場合は、次の手順を実行します。
   - ndscheck -D --config-file conf_file_pathを使って、ディスクの空き容量をチェックします。
   - 各サーバインスタンスのDIBロケーションの下に、upgradeDIBという空のファイルを作成します。

     インスタンスのリストは、ndsmanageユーティリティを使って取得できます。
4. ndscheckを使って、すべてのインスタンスに対してアップグレード前のヘルスチェックを実行し、アップグレードを進める前に、エラーがないかndscheck.logファイルを確認します。
5. ndsmanageを使って、すべてのインスタンスを停止します。
6. eDirectoryのインストール先と同じ場所($NDSHOME)でtarballをuntarします。tarballを同じ場所にuntarすることで、バイナリファイルとライブラリが上書きされます。
7. 必要に応じて、以下のパッケージをアップグレードします。

プラットフォーム　コマンド	パッケージ
Linux	◆ novell-NOVLsubag-9.2.0-0.x86_64.rpm ◆ nici64-3.2.0-0.00.x86_64.rpm **注:** 64ビットのNICIのインストールの詳細については、「37 ページの 「NICI のインストール」」を参照してください。

8. 環境設定ファイルを復元します。
9. すべての環境変数を設定するには、$NDSHOME/eDirectory/opt/novell/eDirectory/bin/ndspathを実行します。
10. すべてのインスタンスに対してndsconfig upgrade -jを実行します。ndsconfig upgradeを実行する際は、最初にマスタレプリカ、次に読み込み/書き込みとその他という順番を守ってください。

複数インスタンスをアップグレードする

このセクションでは、次のことを説明します。

- 31 ページの 「ルートユーザが複数のインスタンスを所有している」
- 31 ページの 「非ルートユーザのインスタンス」
- 31 ページの 「アップグレードの順番」

ルートユーザが複数のインスタンスを所有している

パッケージをアップグレードした後にnds-installを実行すると、すべてのeDirectoryサーバインスタンスのDIBファイルをアップグレードするように求められます。この処理が完了するまで長時間かかることがあります。DIBアップグレードをパラレルで実行する場合は、手動で行うことができます。DIBの手動アップグレードの詳細については、『eDirectoryリリースノート』を参照してください。すべてのアクティブなインスタンスのDIBを1つずつアップグレードする場合は、インスタンスごとにndsconfig upgradeコマンドを実行します。DIBのサイズが大きい場合、[No]を選択し、個別のシェルでndsconfig upgradeをパラレルで実行することができます。これにより、各インスタンスのアップグレード時間を短縮できます。

非ルートユーザのインスタンス

非ルートユーザのインスタンスがあり、それがルートユーザのバイナリを使用している場合、パッケージをアップグレードする前に、このようなインスタンスに対してndscheck を実行し、ndscheck.logファイルを参照して、インスタンスのヘルスが適切であることを確認する必要があります。nds-installを実行すると、非ルートユーザのインスタンスを含め、すべてのインスタンスが停止します。パッケージのアップグレード後、nds-installコマンドを実行しても、非ルートユーザのインスタンスに対してndsconfig upgradeはコールされません。こうしたインスタンスを起動するには、すべての非ルートユーザのインスタンスに対してndsconfig upgradeを手動で実行する必要があります。

アップグレードの順番

ndsconfig upgradeを実行する際は、最初にマスタレプリカに対して実行し、次に読み込み/書き込みやその他のレプリカに対して実行することをお勧めします。

eDirectoryをインストールする

次のセクションでは、LinuxにおけるNetIQ eDirectoryのインストールについて説明します。

- 32 ページの 「eDirectoryでのSLPの使用」
- 33 ページの 「nds-installユーティリティを使用してeDirectoryコンポーネントをインストールする」
- 36 ページの 「非ルートユーザによるeDirectory 9.2のインストール」
- 39 ページの 「ndsconfigユーティリティを使用してeDirectoryレプリカサーバを追加または削除する」
- 45 ページの 「ndsconfigの使用によるeDirectory 9.2の複数インスタンスの設定」

- 53 ページの 「ndsconfigを使用してコンテナ名にドットを使用したツリーにLinuxサーバをインストールする」
- 53 ページの 「nmasinstユーティリティを使用してNMASを設定する」
- 54 ページの 「非ルートユーザのSNMP設定」
- 55 ページの 「ログファイルの場所」

eDirectoryでのSLPの使用

以前のeDirectoryのリリースでは、SLPはeDirectoryのインストール中にインストールされました。しかし、eDirectory 9.2では、eDirectoryをインストールする前に、個別にSLPをインストールする必要があります。

ツリー名の解決にSLPを使用する場合は、このプロトコルのインストールと設定を行う必要があります。SLPディレクトリエージェント(DA)は安定している必要があります。

1. OpenSLPがインストールされていない場合はインストールします。
2. 画面の指示に従って、SLPのインストールを完了します。
3. 次を実行してSLPを手動で起動します。

   ```
   /etc/init.d/slpd start
   ```

詳細については、「163 ページの付録 C「OpenSLP for eDirectoryの設定」」を参照してください。

同様に、SLPパッケージをアンインストールする場合は、次のようにしてSLPを手動で終了する必要があります。

```
/etc/init.d/slpd stop
```

SLPを使用する予定がない(またはできない)場合は、フラットファイルhosts.ndsを使用して、サーバ参照に対するツリー名を解決できます。SLP DAがネットワークにない場合、hosts.ndsファイルを使用してSLPマルチキャストによる遅延を回避できます。

hosts.ndsは、eDirectoryアプリケーションによって使用されるスタティックなルックアップテーブルで、eDirectoryパーティションおよびサーバを検索します。hosts.ndsファイルの各行には、各ツリーまたはサーバの以下の情報が記述されます。

- ツリー/サーバ名:ツリー名は最後はドット(.)で終了します。
- インターネットアドレス:DNS名の場合もあればIPアドレスの場合もあります。
- サーバポート:オプションです。インターネットアドレスにコロンが付加されます。

デフォルト以外のNCPポートで待ち受けしていない限り、ローカルサーバにこのファイルのエントリは必要ありません。

hosts.ndsファイルの構文は次のとおりです。

```
<[partition name.]tree name>.  <host-name/ip-addr>[:<port>] <server name>  <dns-addr/ip-addr>[:<port>]
```

次に例を示します。

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

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

詳細については、hosts.ndsのマニュアルページを参照してください。

ツリー名を解決し、eDirectoryツリーが通知されたことを確認するためにSLPを使用する場合は、eDirectoryおよびSLPのインストールが完了した後で次のように入力してください。

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

たとえば、svcname-ws属性が値SAMPLE_TREEと一致するサービスを検索するには、次のコマンドを入力します。

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

svcname-ws属性がSAMPLE_TREEとして登録されたサービスがある場合、出力は次のようになります。

```
service:ndap.novell:///SAMPLE_TREE
```

svcname-ws属性がSAMPLE_TREEとして登録されたサービスがない場合、何も出力されません。

詳細については、「163 ページの付録 C「OpenSLP for eDirectoryの設定」」を参照してください。

nds-installユーティリティを使用してeDirectoryコンポーネントをインストールする

nds-installユーティリティを使用して、eDirectoryコンポーネントをLinuxシステムにインストールします。このユーティリティは、Linuxプラットフォーム用にダウンロードしたファイルのSetupディレクトリにあります。このユーティリティでは、インストール対象として選択したコンポーネントに基づいて、必要なパッケージが追加されます。

1 setupディレクトリで、次のコマンドを入力します。

```
./nds-install
```

コマンドラインに必要なパラメータを入力していない場合、パラメータを要求するプロンプトがnds-installユーティリティに表示されます。

次の表では、nds-installユーティリティのパラメータを説明します。

nds-installパラメータ	説明
-hまたは--help	nds-installのヘルプを表示します。
-i	アップグレード時にDIBが検出された場合、nds-installスクリプトがndsconfig upgradeコマンドを呼び出さないようにします。
-j	eDirectoryインストール前のヘルスチェックオプションをジャンプまたは無効化します。ヘルスチェックの詳細については、「159 ページの付録 B「eDirectoryヘルスチェック」」を参照してください。
-m	設定するモジュール名を指定します。新しいツリーを設定するときは、DSモジュールのみを設定できます。DSモジュールを設定してから、addコマンドを使用して、NMAS、LDAP、SAS、SNMP、HTTPの各サービス、およびSecretStore (ss)を追加することができます。モジュール名が指定されていない場合は、すべてのモジュールがインストールされます。
-u	無人インストールモードオプションを指定します。
-f	このオプションは、eDirectoryのいずれかのバージョンに対して、強制的にアップグレード/ダウングレードを行う場合に使用します。

インストールプログラムによって、次のRPMがインストールされます。

eDirectoryコンポーネント	インストールされるパッケージ	説明
eDirectoryサーバ	◆ novell-NDSbase ◆ novell-NDScommon ◆ novell-NDSmasv ◆ novell-NDSserv ◆ novell-NDSimon ◆ novell-NDSrepair ◆ novell-NDSdexvnt ◆ novell-NOVLsubag ◆ novell-NOVLsnmp ◆ novell-NOVLpkit ◆ novell-NOVLpkis ◆ novell-NOVLpkia ◆ novell-NOVLembox ◆ novell-NOVLlmgnt ◆ novell-NOVLxis ◆ novell-NLDAPsdk ◆ novell-NLDAPbase ◆ novell-NOVLsas ◆ novell-NOVLntls ◆ novell-NOVLnmas ◆ novell-NOVLldif2dib ◆ novell-NOVLncp ◆ novell-eba	指定したサーバに、eDirectoryレプリカサーバがインストールされます。
管理ユーティリティ	◆ novell-NOVLice ◆ novell-NDSbase ◆ novell-NLDAPbase ◆ novell-NLDAPsdk ◆ novell-NOVLpkia ◆ novell-NOVLxis ◆ novell-NOVLlmgnt	指定したワークステーションに、NetIQインポート/エクスポート変換ユーティリティおよびLDAPツール管理ユーティリティがインストールされます。

2 画面の指示に従って、ライセンスファイルの完全パスを入力します。

インストールプログラムがデフォルトの位置でライセンスファイルを見つけることができなかった場合のみ、ライセンスファイルの完全パスを入力するためのプロンプトが表示されます。デフォルトの位置は、/var、マウントされたライセンスディスク、またはカレントディレクトリです。

入力したパスが有効でない場合、正しいパスを入力するようプロンプトが出されます。

3 インストールが完了したら、eDirectoryユーティリティを現在のセッションで使用するために次の環境変数を更新してエクスポートします。

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

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

export TEXTDOMAINDIR=/opt/novell/eDirectory/share/locale
```

インストール後にeDirectoryサーバを設定するには、ndsconfigユーティリティを使用します。

サーバコンポーネントの一部として、NMAS (NetIQ Modular Authentication Service)がインストールされます。デフォルトでは、ndsconfigを使用してNMASを設定します。また、インストール後にNMASサーバを設定するには、nmasinstユーティリティを使用します。NMASサーバの設定は、ndsconfigを使用してeDirectoryの設定を行ってから実行する必要があります。

デフォルトでは、eDirectoryサーバはFIPSモードで実行されます。FIPSモードを無効にするには、ndsconfig setコマンドでn4u.server.fips_tls=0を渡し、サーバを再起動します。たとえば、ndsconfig set n4u.server.fips_tls=0と指定します。

eDirectory環境でFIPSモードを有効にすると、OpenSSLを使用するすべてのeDirectoryのアプリケーションまたはモジュールが、常にFIPSモードでOpenSSLを使用します。FIPSモードでeDirectoryを動作させると、SSLv3経由の通信が許可されず、サイファの使用が強度の高いサイファのみに制限されます。詳細については、『NetIQ eDirectory管理ガイド』の「LDAPオブジェクトを環境設定する」および「*HTTP サーバオブジェクトの設定*」を参照してください。

ndsconfigユーティリティの詳細については、「125 ページの 「ndsconfigユーティリティ」」を参照してください。

nmasinstユーティリティの詳細については、「53 ページの 「nmasinstユーティリティを使用してNMASを設定する」」を参照してください。

注: eDirectoryをインストールした後、eDirectoryサーバのDIBディレクトリは、ウィルス対策ソフトウェアやバックアップソフトウェアのプロセスから除外することをお勧めします。DIBディレクトリのバックアップは、eDirectoryバックアップツールを使って行えます。

eDirectoryのバックアップの詳細については、『「NetIQ eDirectory管理ガイド」』の*NetIQ eDirectoryのバックアップと復元*を参照してください。

非ルートユーザによるeDirectory 9.2のインストール

非ルートユーザは、tarballを使用してeDirectory 9.2をインストールできます。

前提条件

- ❒ nds-installユーティリティではなくtarballを使ってeDirectoryをインストールする場合は、NICIがインストールされていることを確認してください。NICIのインストールについては、「37 ページの 「NICI のインストール」」を参照してください。
- ❒ rpm -qp *<SNMP サブエージェント RPM のパス>*コマンドを使って、SNMPサブエージェントがインストールされていることを確認します。
- ❒ SLPおよびSNMPを使用する場合は、それらがルートユーザによってインストールされていることを確認します。

❒ eDirectoryのインストール先ディレクトリに対する書き込み権。

管理者以外のユーザについては、「23 ページの 「前提条件」」セクションに示されている権限を持っていることを確認します。

NICI のインストール

eDirectoryのインストールに進む前に、NICIをインストールする必要があります。必須NICIパッケージはシステム全体で使われるため、ルートユーザを使って、必要なパッケージをインストールすることをお勧めします。

eDirectory 9.2では、1つのシステムに32ビットと64ビットのアプリケーションを共存させることができます。

ルートユーザによるNICIのインストール

64ビットのNICIをインストールするには、次のコマンドを入力します。

rpm -ivh NICI_rpm_absolute_path/nici64-3.2.0-0.00.x86_64.rpm

NICIをサーバモードに設定するには、ルートユーザとして次のように入力します。

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

SLES 12以上でユーザサービスを設定する

これらのプラットフォームで非ルートユーザ向けのサービスをサポートするには、systemdをそのユーザに対しワンタイムアクティビティとして開始します。

非ルートユーザとしてサービスを開始する利点を次に示します。

- システム管理者がサービスを監視できます。
- コンピュータが再起動時にサービスを開始します。

特定のユーザに対してsystemdを開始するには、次のコマンドを実行します。

```
systemctl start user@<uid>.service
```

ここでuidは、そのユーザのユーザIDです。

たとえば、systemctl start user@1001.serviceと指定します。

持続的なsystemdユーザインスタンスを有効にするには、次のコマンドを実行します。

```
loginctl enable-linger user
```

注: SLES 12以上でeDirectoryを設定した後にdatadirを新しい場所に移動する場合は、次の手順を実行してください。

- 場所/usr/lib/systemd/system/にあるサービスファイル内で、ndsd.pidファイルを新しい場所に更新します。

  たとえば、nds.confファイルがもともと/etc/opt/novell/eDirectoryに置かれている場合は、次のようにサンプルのサービスファイルが作成されます。

  /usr/lib/systemd/system/ndsdtmpl-etc-opt-novell-eDirectory-conf-ds.conf@.service。

- systemctl daemon-reloadコマンドを使用して、デーモンを再ロードします。
- eDirectoryサーバを再起動します。

eDirectoryをインストールする

1. eDirectoryをインストールするディレクトリに移動します。
2. 次のコマンドを実行して、tarファイルを展開します。

   ```
   tar xvf /tar_file_name
   ```

   etc、opt、varの各ディレクトリが作成されます。
3. 次を実行して、パスをエクスポートします。
   - **環境変数を手動でエクスポートするには、次のコマンドを入力します。**

     ```
     export LD_LIBRARY_PATH=custom_location/eDirectory/opt/novell/eDirectory/
     lib64:custom_location/eDirectory/opt/novell/eDirectory/lib64/nds-
     modules:custom_location/eDirectory/opt/novell/lib64:$LD_LIBRARY_PATH

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

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

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

     ndspathスクリプトを使って環境変数をエクスポートするには、次の手順を実行します。

     手動でパスをエクスポートしない場合は、ndspathスクリプトをユーティリティの前に指定します。
     - 次のように、必要なユーティリティを実行します。

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

     - 次のとおり、現在のシェル内のパスをエクスポートします。

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

       注: 上記のコマンドは、必ず*custom_location*/eDirectory/optディレクトリから入力してください。

       上記のコマンドを入力したら、通常どおりにユーティリティを実行します。
     - プロファイル内のスクリプト(bashrc、または同様のスクリプト)を呼び出します。こうすることで、ログインするか新しいシェルを開けば、直接ユーティリティを使い始めることができます。
4. 通常の方法でeDirectoryを設定します。

   eDirectoryは次の方法で設定できます。
   - 次のとおり、ndsconfigユーティリティを使用します。

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

次に例を示します。

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

入力するポート番号は、1024～65535の範囲内にする必要があります。1024より小さいポート番号は通常、スーパユーザと標準アプリケーション用に予約されています。そのため、eDirectoryアプリケーションには、デフォルトのポート524は使用できません。

これが原因で、次のアプリケーションで問題が発生する可能性があります。

- ターゲットサーバポートを指定するオプションがないアプリケーション。
- NCPを使用し、ポート524でルートとして動作する古いアプリケーション。

- ndsmanageユーティリティを使用して、新しいインスタンスを設定します。詳細については、「49 ページの 「ndsmanageによるインスタンスの作成」」を参照してください。

拡張バックグラウンド認証を有効にするには、ndsconfig upgradeコマンドの--configure-eba-nowスイッチで*yes*を指定します。有効にしない場合は、*no*を指定して後から設定します。--configure-eba-nowスイッチをndsconfigコマンドに渡さなかった場合は、選択を求めるプロンプトが出されます。デフォルトでは、この設定はnoです。

画面の指示に従って、設定を完了します。

詳細については、「39 ページの 「ndsconfigユーティリティを使用してeDirectoryレプリカサーバを追加または削除する」」を参照してください。

注: eDirectoryをインストールした後、eDirectoryサーバのDIBディレクトリは、ウィルス対策ソフトウェアやバックアップソフトウェアのプロセスから除外することをお勧めします。DIBディレクトリのバックアップは、eDirectoryバックアップツールを使って行えます。

eDirectoryのバックアップの詳細については、『「NetIQ eDirectory管理ガイド」』の*NetIQ eDirectoryのバックアップと復元*を参照してください。

---

ndsconfigユーティリティを使用してeDirectoryレプリカサーバを追加または削除する

eDirectoryをインストールした後、ndsconfigユーティリティを使って、eDirectoryレプリカサーバを設定します。ndsconfigユーティリティを使用するには、管理者の権利を持っている必要があります。引数付きでこのユーティリティを使用した場合は、すべての引数が確認され、管理者の権利を持つユーザのパスワード入力を要求するプロンプトが表示されます。引数なしでndsconfigユーティリティを使用した場合は、このユーティリティに関する説明と利用可能なオプションが表示されます。このユーティリティでは、eDirectoryレプリカサーバを削除したり、eDirectoryサーバの現在の設定を変更することもできます。詳細については、「125 ページの 「ndsconfigユーティリティ」」を参照してください。

特定の場所でeDirectoryを設定するための前提条件

特定の場所にeDirectoryを設定する場合は、eDirectoryの設定を行う前に、その場所にLC_ALLおよびLANGをエクスポートする必要があります。たとえば、eDirectoryのロケールを日本に設定する場合は、次のコマンドを入力します。

export LC_ALL=ja

export LANG=ja

新しいツリーの作成

使用する構文は次のとおりです。

```
ndsconfig new [-m <modulename>] [-i] [-S <server name>] [-t <tree_name>] [-n
<server context>] [-d <path_for_dib>][-P <LDAP URL(s)>] [-L <ldap_port>] [-l
<ssl_port>] [-o http port] [-O https port] [-e] -a <admin FDN> [-R] [-c] [-w <admin
password>] [-b <port to bind>] [-B <interface1@port1, interface2@port2,..>] [-D
<path_for_data>] [--config-file <configuration file>] [--configure-eba-now <yes/
no>] [--pki-default-rsa-keysize <2048/4096/8192>] [--pki-default-ec-curve <P256/
P384/P521>] [--pki-default-cert-life <in years>]
```

指定したツリー名とコンテキストの新しいツリーがインストールされます。

tree_name、*admin FDN*、および*server FDN*の変数には、文字数制限があります。これらの変数に使用できる最大文字数は次のとおりです。

- *tree_name*: 32文字
- *admin-FDN*: 255文字
- *server FDN*: 255文字

重要: eDirectoryでは、NCPサーバオブジェクトのFDNを最大256文字までで設定できますが、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。

コマンドラインにパラメータが指定されていない場合、指定されていない各パラメータに値を入力するよう求めるプロンプトがndsconfigによって表示されます。

また、次の構文も使用できます。

```
ndsconfig def [-t <treename>] [-n <server context>] [-a <admin FDN>] [-w <admin
password>] [-c] [-i] [-S <server name>] [-d <path for dib>] [-m <module>] [-e] [-L
<ldap port>] [-l <SSL port>] [-o <http port>] [-O <https port>] [-D
<custom_location>] [--config-file <configuration_file>] [--configure-eba-now <yes/
no>]
```

指定したツリー名とコンテキストの新しいツリーがインストールされます。コマンドラインにパラメータが指定されていない場合、ndsconfigによって、指定されていない各パラメータにデフォルト値が適用されます。

たとえば、新しいツリーを作成するには、次のようにコマンドを入力します。

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

注: 新しいツリーの作成時に使用するeDirectory 9.2のndsconfigコマンドに--enable-pbkdf2という名前の新しいオプションが追加されました。このオプションが設定されている場合は、パスワードポリシーが作成され、ツリー全体に自動的に割り当てられます。このパスワードポリシーにより、ツリー内のすべてのユーザに対して、NDSパスワードのPBKDF2パスワードとの同期が可能になります。詳細については、『NetIQ eDirectory管理ガイド』の「非可逆パスワードストレージを理解する」を参照してください。

デフォルトサーバ証明書のデフォルトのパラメータを指定する

eDirectoryには、新しいeDirectoryツリーを設定しながら、CA証明書とデフォルトサーバ証明書のデフォルトRSAキーサイズ、楕円曲線、および証明書の有効期限を指定するオプションが用意されています。以下のコマンドを使用して、ndsconfig newを使用して新しいeDirectoryツリーを設定しながら、CAおよびデフォルトサーバの証明書のデフォルトパラメータを指定できます。

- **pki-default-rsa-keysize:** 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。
- **pki-default-ec-curve:** EC証明書の曲線の制限を指定します。使用可能な値はP256、P384、およびP521です。
- **pki-default-cert-life:** 証明書の有効期限を年数で指定します。

これらの属性は、新しいeDirectoryサーバのインストール中にndsconfig newで設定できます。

ここで指定される値は、新しいツリーが構成されるときに組織のCAオブジェクトの対応する属性に設定されます。

詳細については、『*NetIQ eDirectory管理ガイド*』の「組織の認証局オブジェクトを作成する」を参照してください。

既存のツリーにサーバを追加する

使用する構文は次のとおりです。

```
ndsconfig add [-t <treename>] [-n <server context>] [-a <admin FDN>] [-w <admin password>] [-e] [-P <LDAP URL(s)>][-L <ldap port>] [-l <SSL port>] [-o <http port>] [-O <https port>] [-S <server name>] [-d <path for dib>] [-m <module>] [-p <IP address:[port]>] [-R] [-c] [-b <port to bind>] [-B <interface1@port1>, <interface2@port2>,..] [-D <custom_location>] [-config-file <configuration_file>] [-E] [--configure-eba-now <yes/no>]
```

指定したコンテキストで既存のツリーにサーバが追加されます。サーバオブジェクトの追加先として指定したコンテキストが存在しない場合は、ndsconfigによって該当するコンテキストが作成され、サーバが追加されます。

拡張バックグラウンド認証(EBA)を有効にするには、ndsconfig upgradeコマンドの--configure-eba-nowスイッチで*yes*を指定します。有効にしない場合は、*no*を指定して後から設定します。--configure-eba-nowスイッチをndsconfigコマンドに渡さなかった場合は、選択を求めるプロンプトが出されます。デフォルトでは、この設定は*no*です。

EBAを有効にしたセカンダリサーバをツリーに追加するには、ツリーでEBA CAを設定しておく必要があります。EBACAが存在しない場合は、EBAを有効にせずにサーバを追加してから、EBACAをホストするようにサーバをアップグレードします。この操作を行わないと、セカンダリサーバの設定が失敗します。

既存のツリーへeDirectoryをインストールした後で、LDAPおよびセキュリティサービスを追加することもできます。

たとえば、新しいツリーをサーバに追加するには、次のようにコマンドを入力します。

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

-Eオプションを使用して、追加するサーバの暗号化レプリケーションを有効にできます。暗号化レプリケーションの詳細については、『「NetIQ eDirectory管理ガイド」』の「*暗号化レプリケーション*」を参照してください。

ツリーからサーバオブジェクトとディレクトリサービスを削除する

使用する構文は次のとおりです。

```
ndsconfig rm [-a <admin FDN>] [-w <admin password>] [-p <IP address:[port]>] [-c]
```

サーバからeDirectoryおよびデータベースが削除されます。

注: iMonitorを使用して作成したHTMLファイルは削除されません。これらのファイルは、eDirectoryを削除する前に、/var/opt/novell/eDirectory/data/dsreportsから手動で削除する必要があります。

たとえば、eDirectoryサーバオブジェクトとディレクトリサービスをツリーから削除するには、次のコマンドを入力します。

```
ndsconfig rm -a cn=admin.o=company
```

ndsconfigユーティリティパラメータ

ndsconfigのパラメータ	説明
new	新しいeDirectoryツリーを作成します。コマンドラインにパラメータが指定されていない場合、指定されていない各パラメータに値を入力するよう求めるプロンプトがndsconfigによって表示されます。
def	新しいeDirectoryツリーを作成します。コマンドラインにパラメータが指定されていない場合、ndsconfigによって、指定されていない各パラメータにデフォルト値が適用されます。
add	既存のツリーにサーバを追加します。また、既存のツリーでeDirectoryの設定が完了した後、LDAPおよびSASサービスを追加します。
rm	サーバオブジェクトとディレクトリサービスをツリーから削除します。 **注:** このオプションを指定しても、キーマテリアルオブジェクトは削除されません。これらのオブジェクトは、手動で削除する必要があります。
アップグレード	eDirectoryを使用中のバージョンよりも新しいバージョンにアップグレードします。
-i	新しいツリーを設定するときに、同じ名前のツリーが存在するかのチェック結果を無視します。複数の同じ名前を持つツリーが存在できます。

ndsconfigのパラメータ	説明
-S *server name*	サーバ名を指定します。サーバ名にはドットも使用できます(例:netiq.com)。ndsconfigはコマンドラインユーティリティのため、名前にドットを含むコンテナを使用する場合はそれらのドットをエスケープする必要があります。また、ドットを含むコンテキストが含まれたパラメータは二重引用符で囲む必要があります。 たとえば、Oの名前としてnetiq.comを使用しているLinuxサーバに新しいeDirectoryツリーをインストールするには、次のコマンドを使用します。 ndsconfig new -a "admin.novell\\.com" -t netiq_tree -n "OU=servers.O=netiq\\.com" 管理者名のパラメータ、コンテキストとサーバコンテキストのパラメータは、二重引用符で囲みます。netiq.comの「.」だけを「\\」(円記号)文字を使ってエスケープします。このフォーマットは、既存のツリーにサーバをインストールする場合にも使用できます。 **注:** 名前の最初にドットを使用することはできません。たとえば、ドット(.)で始まる「.novell」という名前のサーバをインストールすることはできません。
-t *treename*	サーバの追加先のツリー名です。最大で32文字の名前を付けることができます。このパラメータを指定しない場合、ndsconfigは/etc/opt/novell/eDirectory/conf/nds.confファイル内のn4u.nds.tree-nameパラメータに指定されているツリー名を採用します。デフォルトのツリー名は$LOGNAME-$HOSTNAME-NDStreeです。
-n *server context*	サーバオブジェクトを追加するサーバのコンテキストを指定します。最大で64文字の名前を付けることができます。このコンテキストが指定されていない場合、ndsconfigは/etc/opt/novell/eDirectory/conf/nds.confファイルのn4u.nds.server-context環境設定パラメータに指定されているコンテキストを採用します。サーバコンテキストはタイプつきの形式で指定する必要があります。デフォルトのコンテキストはorgです。
-d *path for dib*	データベースファイルの格納先になる場所のディレクトリパスです。
-r	このオプションを使用すると、サーバにすでに追加されているサーバの数にかかわらず、サーバのレプリカが強制的に追加されます。
-L *ldap_port*	LDAPサーバのTCPポート番号を指定します。デフォルトのポートである389が使用中の場合は、新しいポート番号を要求するプロンプトが表示されます。
-l *ssl_port*	LDAPサーバのSSLポート番号を指定します。デフォルトのポートである636が使用中の場合は、新しいポート番号を要求するプロンプトが表示されます。
-a *admin FDN*	サーバオブジェクトとディレクトリサービスの作成先のコンテキストに対するスーパバイザ権を持つ、ユーザオブジェクトの完全識別名を指定します。admin名はタイプつきの形式で指定する必要があります。最大で64文字の名前を付けることができます。デフォルトのadmin名はadmin.orgです。
-e	LDAPオブジェクトのクリアテキストパスワードを有効にします。
-m *modulename*	設定するモジュール名を指定します。新しいツリーを設定するときは、DSモジュールのみを設定できます。DSモジュールを設定してから、addコマンドを使用して、NMAS、LDAP、SAS、SNMP、HTTPの各サービス、およびSecretStore(ss)を追加することができます。モジュール名が指定されていない場合は、すべてのモジュールがインストールされます。 **注:** nds-installを使ったeDirectoryアップグレード中にSecretStoreを設定しない場合は、このオプションにno_ssという値を渡します。たとえば、nds-install '-m no_ss'などです。

ndsconfigのパラメータ	説明
-o	HTTPクリアポート番号を指定します。
-O	HTTPセキュアポート番号を指定します。
-p <*IPアドレス:[ポート]*>	このオプションは、セカンダリサーバをツリーに追加する場合(addコマンド)に使われます。このサーバを追加するパーティションのレプリカを保持するリモートホストのIPアドレスを指定します。デフォルトのポート番号は524です。これにより、SLPルックアップが回避されるため、ツリーのルックアップが高速化されます。
-R	デフォルトでは、サーバの追加先のパーティションのレプリカは、ローカルサーバに複製されます。このオプションを使用すると、レプリカをローカルサーバに追加することは許可されません。
-c	このオプションを使用すると、ndsconfig操作中(操作を続行するためのyes/noの選択など)のプロンプトや、競合が発生した場合にポート番号の再入力を求めるプロンプトなどが表示されなくなります。コマンドラインで必須パラメータを渡さなかった場合のみ、必須パラメータの入力を求めるプロンプトが表示されます。
-w <*管理パスワード*>	このオプションを使用すると、管理ユーザパスワードをクリアテキストで渡すことができます。 **注:** パスワードをクリアテキストで渡すと、安全が確保できないため、このオプションは推奨されません。
-E	追加するサーバに対して暗号化レプリケーションを有効にします。
-j	eDirectoryインストール前のヘルスチェックオプションをジャンプまたは無効化します。
-b *port to bind*	特定のインスタンスが監視に使用するデフォルトのポート番号を設定します。これにより、n4u.server.tcp-portとn4u.server.udp-portにデフォルトのポート番号が設定されます。-bオプションを使用してNCPポートが渡されると、デフォルトのポートと見なされ、それに応じてTCPとUDPのパラメータが更新されます。 **注:** -bと-Bは排他的に使われます。

-B *interface1@port1*, *interface2@port2*,...	ポート番号をIPアドレスまたはインタフェースとともに指定します。次に例を示します。
	
	`-B eth0@524`
	
	または
	
	`-B 100.1.1.2@524`
	
	注: -bと-Bは互いに排他的です。

--config-file *configuration file*	nds.conf環境設定ファイルを保存するための絶対パスとファイル名を指定します。たとえば、環境設定ファイルを/etc/opt/novell/eDirectory/ディレクトリに保存する場合には、--config-file /etc/opt/novell/eDirectory/nds.confと入力します。
-P <*LDAP URL*>	LDAPURLで、LDAPサーバオブジェクト上のLDAPインタフェースを設定できるようにします。 例: -P ldap://1.2.3.4:1389,ldaps://1.2.3.4:1636
-D *path_for_data*	指定したパスにdata、dib、およびlogのディレクトリを作成します。

ndsconfigのパラメータ	説明
set valuelist	指定したeDirectory環境設定パラメータに対して値を設定します。ツリーを設定する前に、ブートストラップパラメータの設定に使用します。環境設定パラメータを変更した場合、新しい値を有効にするにはndsdを再起動する必要があります。ただし、環境設定パラメータによってはndsdを再起動する必要がない場合があります。 再起動の必要のないパラメータは次のとおりです。 ◆ n4u.nds.inactivity-synchronization-interval ◆ n4u.nds.synchronization-restrictions ◆ n4u.nds.janitor-interval ◆ n4u.nds.backlink-interval ◆ n4u.nds.drl-interval ◆ n4u.nds.flatcleaning-interval ◆ n4u.nds.server-state-up-threshold ◆ n4u.nds.heartbeat-schema ◆ n4u.nds.heartbeat-data ◆ n4u.server.fips_tls ◆ n4u.server.eba_enabled
get help paramlist	指定したeDirectory環境設定パラメータに関するヘルプを表示します。パラメータリストが指定されていない場合は、ndsconfigはすべてのeDirectory環境設定パラメータに関するヘルプ文字列を表示します。
set valuelist	指定したeDirectory環境設定パラメータに対して値を設定します。ツリーを設定する前に、ブートストラップパラメータの設定に使用します。 環境設定パラメータを変更した場合、新しい値を有効にするにはndsdを再起動する必要があります。
get paramlist	指定したeDirectory環境設定パラメータの現在の値を表示します。パラメータリストが指定されていない場合は、ndsconfigはすべてのeDirectory環境設定パラメータを表示します。
configure-eba-now	拡張バックグラウンド認証用にeDirectoryサーバを設定するには、このスイッチを使用します。

ndsconfigの使用によるeDirectory 9.2の複数インスタンスの設定

単一のホスト上でeDirectory 9.2の複数インスタンスを設定できます。eDirectory 9.2では複数インスタンスの機能がサポートされるため、次の設定が可能です。

- 1台のホスト上に複数インスタンスのeDirectoryを設定する
- 1台のホスト上に複数のユーザ用に複数のツリーを設定する
- 1台のホスト上に同じツリーまたはパーティションの複数のレプリカを設定する

警告: 同じユーザに対して複数のツリーを設定することはできません。1ユーザに対する複数のツリーでサーバのインスタンスを設定することはできません。複数のツリーにサーバを設定する場合は、別々のユーザアカウントを使用してください。

次の表に、複数インスタンスをサポートするプラットフォームを示します。

機能	Linux	Windows
複数インスタンスのサポート	✓	✗

複数インスタンスの設定方法は、1つのインスタンスを複数回設定する場合と同様です。各インスタンスは、次のように固有のインスタンス識別子を持つ必要があります。

- 異なるデータとログファイルの場所

  ndsconfig --config-file、-d、および-Dオプションを使用して、これを実行できます。
- リスン対象インスタンスの固有のポート番号

  ndsconfigの-bと-Bオプションを使って、これを実行できます。
- インスタンスの一意なサーバ名

  ndsconfig -S server nameオプションを使用して、これを行えます。

重要: eDirectoryの設定中、デフォルトのNCPサーバ名がホストサーバ名として設定されます。複数のインスタンスを設定する場合、NCPサーバ名を変更する必要があります。ndsconfigのコマンドラインオプションである-S <*server_name*>を使って、別のサーバ名を指定します。

同じツリーまたは複数の異なるツリーのどちらであっても、複数インスタンスを設定する場合は、NCPサーバ名が固有でなければなりません。

複数インスタンスの必要性

複数インスタンスは、次のことを行う必要性から提供されるようになりました。

- eDirectoryのインスタンスを複数設定することによって、ハイエンドのハードウェアを活用する。
- 必要なハードウェアに投資する前に、1台のホスト上でセットアップをテスト運用する。

複数インスタンスを展開する場合のシナリオ

同じツリーまたは複数のツリーに属する複数インスタンスは、次のようなシナリオで効果的に使用できます。

大企業におけるeDirectoryの使用

- 大企業では、eDirectoryの負荷分散と高い可用性を提供することができます。

たとえば、ポート1524、2524、および3524でLDAPサービスを実行するレプリカサーバ3台がある場合、eDirectoryの新しいインスタンスを設定し、新しいポート636で高い可用性のLDAPサービスを提供できます。

- 1台のホストに複数インスタンスを設定すると、組織内の複数の部門にまたがってハイエンドのハードウェアを活用できます。

評価用セットアップにおけるeDirectoryの使用

- **大学:** 大勢の熱心なユーザ(学生)が、複数インスタンスを使用して1台のホストからeDirectoryを評価できます。
- **eDirectory管理のトレーニング:**
  - 参加者は、複数インスタンスを使用して、実際に管理を行ってみることができます。
  - 講師は、1台のホストを使用してクラスの受講者に教えることができます。各受講者に専用のツリーを用意できます。

複数インスタンスの使用

eDirectory 9.2によって、複数インスタンスの設定が容易になります。複数インスタンスを効果的に使用するためには、セットアップを慎重に計画してから、複数インスタンスを設定する必要があります。

- 51 ページの 「セットアップの計画」
- 47 ページの 「複数インスタンスを設定する」

セットアップの計画

この機能を有効に使用するためには、eDirectoryのインスタンスを複数計画し、各インスタンスが、ホスト名、ポート番号、サーバ名、または環境設定ファイルのように、確定的なインスタンス識別子を持つように設定することをお勧めします。

複数インスタンスの設定時には、次のことについて計画したかどうかを確認する必要があります。

- 環境設定ファイルの場所
- 変数データの場所(ログファイルなど)
- DIBの場所
- NCPインタフェース、各インスタンスを識別する一意のポート、および他のサービスのポート(LDAP、LDAPS、HTTP、HTTPSポートなど)
- 各インスタンスの一意なサーバ名

複数インスタンスを設定する

複数インスタンスのeDirectoryは、ndsconfigユーティリティを使用して設定できます。次の表に、複数インスタンスの設定時に指定する必要があるndsconfigオプションを示します。

注: すべてのインスタンスは同じサーバキー(NICI)を共有します。

オプション	説明
--config-file	nds.conf環境設定ファイルを保存するための絶対パスとファイル名を指定します。 たとえば、環境設定ファイルを/etc/opt/novell/eDirectory/ディレクトリに保存する場合には、--config-file /etc/opt/novell/eDirectory/nds.confを使用します。
-b	新しいインスタンスが監視するときのポート番号を指定します。 **注:** -bと-Bは排他的に使われます。
-B	ポート番号をIPアドレスまたはインタフェースとともに指定します。次に例を示します。 -B eth0@524 または -B 100.1.1.2@524 **注:** -bと-Bは排他的に使われます。
-D	data、dib、およびlogのディレクトリを、新しいインスタンス用に指定したパスに作成します。
S	サーバ名を指定します。

オプションを使用して、eDirectoryの新しいインスタンスを設定できます。

ndsmanageユーティリティを使用して、新しいインスタンスを設定することもできます。詳細については、「49 ページの 「ndsmanageによるインスタンスの作成」」を参照してください。

複数インスタンスを管理する

このセクションでは、次の情報を紹介します。

ndsmanageユーティリティ

ndsmanageユーティリティを使用すると、次の操作を実行できます。

- 設定したインスタンスの表示
- 新しいインスタンスの作成
- 選択したインスタンスに対する次の操作の実行:
  - サーバ上にあるレプリカの表示
  - インスタンスの開始
  - インスタンスの停止

- インスタンスに対するDSTrace (ndstrace)の実行
- インスタンスの設定解除

- すべてのインスタンスの開始と停止

インスタンスの表示

次の表で、eDirectoryインスタンスを表示する方法について説明します。

表 2-1 インスタンスを表示するためのndsmanageの使用

構文	説明
ndsmanage	設定したすべてのインスタンスを表示します。
ndsmanage -a|--all	eDirectoryの特定のインストールを使用しているすべてのユーザのインスタンスを表示します。
ndsmanage*ユーザ名*	特定のユーザによって設定されたインスタンスを表示します。

各インスタンスについて、次のフィールドが表示されます。

- 環境設定ファイルのパス
- サーバのFDNおよびポート
- ステータス(インスタンスがアクティブか非アクティブか)

注: このユーティリティは、単一のバイナリに対して設定されたすべてのインスタンスを表示します。

ndsmanageによるインスタンスの作成

ndsmanageを使用して新しいインスタンスを作成するには、次の手順を実行します。

1 次のコマンドを入力します。

```
ndsmanage
```

2 新しいインスタンスを作成するには、「c」と入力します。

新しいツリーを作成するか、既存のツリーにサーバを追加できます。画面の指示に従って、新しいインスタンスを作成します。

特定のインスタンスに対する操作の実行

各インスタンスについて、次の操作を実行できます。

下記の操作以外に、選択したインスタンスに対してDSTraceを実行することもできます。

特定のインスタンスの開始

自分が設定したインスタンスを開始するには、次の操作を実行します。

1 次のように入力します。

```
ndsmanage
```

2 開始するインスタンスを選択します。

メニューが拡張し、特定のインスタンスに対して実行可能なオプションが表示されます。

図 2-1 ndsmanageユーティリティのインスタンスオプションの出力画面

3 インスタンスを開始するには、「s」と入力します。

または、コマンドプロンプトに次のコマンドを入力することもできます。

ndsmanage start --config-file *configuration_file_of_the_instance_configured_by_you*

特定のインスタンスの停止

自分が設定したインスタンスを停止するには、次の操作を実行します。

1 次のように入力します。

```
ndsmanage
```

2 停止するインスタンスを選択します。

メニューが拡張し、特定のインスタンスに対して実行可能なオプションが表示されます。詳細については、「(50 ページ) ndsmanageユーティリティのインスタンスオプションの出力画面」を参照してください。

3 インスタンスを停止するには、「k」と入力します。

または、コマンドプロンプトに次のコマンドを入力することもできます。

ndsmanage stop --config-file *configuration_file_of_the_instance_configured_by_you*

インスタンスの設定解除

インスタンスの設定を解除するには、次の手順を実行します。

1 次のように入力します。

```
ndsmanage
```

2 設定解除するインスタンスを選択します。

メニューが拡張し、特定のインスタンスに対して実行可能なオプションが表示されます。詳細については、「(50 ページ) ndsmanageユーティリティのインスタンスオプションの出力画面」を参照してください。

3 インスタンスを設定解除するには、「d」と入力します。

すべてのインスタンスの開始と停止

自分が設定したすべてのインスタンスを開始および停止できます。

すべてのインスタンスの開始

自分が設定したすべてのインスタンスを開始するには、コマンドプロンプトで次のコマンドを入力します。

ndsmanage startall

特定のインスタンスを開始するには、「49ページの 「特定のインスタンスの開始」」を参照してください。

特定のインスタンスの識別

複数インスタンスの設定中に、ホスト名、ポート番号、および一意な環境設定ファイルのパスを、各インスタンスに割り当てます。このホスト名とポート番号が、インスタンスの識別子になります。

ほとんどのユーティリティには、特定のインスタンスを指定することができる「-h*ホスト名:ポート*」オプションまたは「--config-file*環境設定ファイルの場所*」オプションが用意されています。詳細については、ユーティリティのマニュアルページを参照してください。

特定のインスタンスに対するユーティリティの呼び出し

特定のインスタンスに対してユーティリティを実行する場合は、ユーティリティのコマンドにインスタンスの識別子を含める必要があります。インスタンスの識別子になるのは、環境設定ファイルのパス、ホスト名、およびポート番号です。「--config-file*環境設定ファイルの場所*」または「-h*ホスト名:ポート*」を使用すると、特定のインスタンスに対してユーティリティを実行できます。

コマンドにインスタンス識別子を指定しないと、ユーザが所有するさまざまなインスタンスが表示され、ユーティリティの実行対象にするインスタンスを選択するように求められます。

たとえば、--config-fileオプションを指定して特定のユーティリティに対してDSTraceを実行する場合は、次のように入力します。

```
ndstrace --config-file configuration_filename_with_location
```

複数インスタンスのシナリオ

非ルートユーザであるMaryが、1台のホストマシン上で、1つのバイナリに対し2つのツリーを設定しようとしています。

セットアップの計画

Maryは次のインスタンス識別子を指定します。

- **インスタンス1:**

インスタンスが監視するポート番号	1524
環境設定ファイルのパス	/home/maryinst1/nds.conf
DIBディレクトリ	/home/mary/inst1/var

- **インスタンス2:**

インスタンスが監視するポート番号	2524
環境設定ファイルのパス	/home/mary/inst2/nds.conf
DIBディレクトリ	/home/mary/inst2/var

インスタンスの設定

前述のインスタンス識別子に基づいてインスタンスを設定するために、Maryは次のコマンドを入力する必要があります。

- **インスタンス1:**

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

- **インスタンス2:**

```
ndsconfig new -t corptree -n o=novell -a cn=admin.o=company -b 2524 -D
/home/mary/inst2/var --config-file /home/mary/inst2/nds.conf
```

インスタンスに対するユーティリティの呼び出し

Maryは、ポート1524でリスンしているインスタンス1に対してDSTraceユーティリティを実行しようと思っています。環境設定ファイルは/home/mary/inst1/nds.confにあり、DIBファイルは/home/mary/inst1/varにあります。この場合、以下のようにユーティリティを実行することができます。

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

または

```
ndstrace -h 164.99.146.109:1524
```

インスタンス識別子を指定しないと、Maryが所有するすべてのインスタンスが表示され、インスタンスを選択するように求められます。

インスタンスの表示

Maryがホストのインスタンスの詳細を知りたい場合は、ndsmanageユーティリティを実行できます。

- Maryが所有するすべてのインスタンスを表示するには、次のコマンドを実行します。

  ```
  ndsmanage
  ```

- John(ユーザ名john)が所有するすべてのインスタンスを表示するには、次のコマンドを実行します。

  ```
  ndsmanage john
  ```

- eDirectoryの特定のインストールを使用しているすべてのユーザのインスタンスをすべて表示するには、次のコマンドを実行します。

  ```
  ndsmanage -a
  ```

ndsconfigを使用してコンテナ名にドットを使用したツリーにLinuxサーバをインストールする

ndsconfigを使用して、名前にドットを使用したコンテナ(novell.comなど)を含むeDirectoryツリーにLinuxサーバをインストールできます。

ndsconfigはコマンドラインユーティリティのため、名前にドットを含むコンテナを使用する場合はそれらのドットをエスケープする必要があります。また、ドットを含むコンテキストが含まれたパラメータは二重引用符で囲む必要があります。たとえば、名前をOとして"O=netiq.com"を使用しているLinuxサーバに新しいeDirectoryのツリーをインストールするには、次のコマンドを使用します。

```
ndsconfig new -a 'admin.netiq.com' -t netiq_tree -n 'OU=servers.O=netiq.com'
```

管理者名のパラメータ、サーバとサーバコンテキストのパラメータを二重引用符で囲み、novell.comのドット(「.」)だけを「\」(円記号)文字を使用してエスケープします。

このフォーマットは、既存のツリーにサーバをインストールする場合にも使用できます。

注: DSRepair、Backup、DSMerge、DSLogin、およびldapconfigなどのユーティリティを使用する際に、ドットを含む管理者名やコンテキストを入力する場合も、この形式を使用してください。

---

nmasinstユーティリティを使用してNMASを設定する

デフォルトでは、ndsconfigを使用してNMASを設定します。nmasinstを使用してNMASを設定することもできます。

ndsconfigが行うのはNMAS設定のみです。ログインメソッドのインストールは行いません。ログインメソッドのインストールには、nmasinstを使用できます。

重要: NMASログインメソッドをインストールする前に、ndsconfigを使用してeDirectoryを設定する必要があります。ツリーに対する管理権限も必要です。

- 53 ページの 「NMASの設定」
- 54 ページの 「ログインメソッドのインストール」

NMASの設定

デフォルトでは、ndsconfigを使用してNMASを設定します。nmasinstを同じ目的で使用することもできます。

NMASを設定し、eDirectoryにNMASオブジェクトを作成するには、サーバコンソールのコマンドラインで次のコマンドを入力します。

```
nmasinst -i admin.context tree_name
```

nmasinstからパスワードの入力が要求されます。

このコマンドではNMASに必要なセキュリティコンテナ内にオブジェクトが作成され、eDirectory内のLDAPサーバオブジェクトのNMASに対するLDAP拡張がインストールされます。

ツリー内で最初のNMASをインストールする場合、セキュリティコンテナ内にオブジェクトを作成できる十分な権利を持ったユーザがインストールする必要があります。ただし、それ以降のインストールはセキュリティコンテナに対して読み込み専用の権利のみを持つコンテナ管理者も実行できます。nmasinstは、NMASオブジェクトを作成しようとする前に、セキュリティコンテナ内にNMASオブジェクトが存在していることを確認します。

nmasinstではスキーマを拡張できません。NMASスキーマはeDirectoryのベーススキーマの一部としてインストールされます。

ログインメソッドのインストール

nmasinstを使用してログインメソッドをインストールするには、サーバコンソールのコマンドラインで次のコマンドを入力してください。

```
nmasinst -addmethod admin.context tree_name config.txt_path
```

最後のパラメータで、インストールするログインメソッドのconfig.txtファイルを指定します。各ログインメソッドに対して、config.txtファイルが1つ提供されています。

-addmethodコマンドの一例を次に示します。

```
nmasinst -addmethod admin.netiq MY_TREE ./nmas-methods/novell/Simple Password/
config.txt
```

ログインメソッドがすでに存在する場合は、nmasinstによって更新されます。

詳細については、『NetIQ eDirectory管理ガイド』の「ログインおよびポストログインメソッドとシーケンスを管理する」を参照してください。

非ルートユーザのSNMP設定

NICIとNOVLsubagは、ルートユーザとしてインストールする必要があります。

1. ルートユーザによるNICIのインストール。「37 ページの 「ルートユーザによるNICIのインストール」」を参照してください。
2. ルートユーザによるNOVLsubagのインストール。

   NOVLsubagをインストールするには、次の手順を実行します。

   次のコマンドを入力します。

   ```
   rpm -ivh --nodeps NOVLsubag_rpm_file_name_with_path
   ```

   次に例を示します。

   ```
   rpm -ivh --nodeps novell-novell-NOVLsubag-9.2.0-0.x86_64.rpm
   ```

3. 次を実行して、パスをエクスポートします。

   手動による環境変数のエクスポート.

   ```
   export LD_LIBRARY_PATH=custom_location/opt/novell/eDirectory/lib64:/opt/
   novell/eDirectory/lib64/nds-modules:/opt/novell/lib64:$LD_LIBRARY_PATH

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

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

ログファイルの場所

ndsd.log

ndsd.logファイルには、サーバシャットダウンおよび開始メッセージ、PKIやLDAPサービスの開始およびシャットダウンメッセージといったeDirectoryサーバ関連のメッセージに関する情報が含まれます。デフォルトでは、ファイルは/var/opt/novell/eDirectory/logディレクトリ内に格納されています。

/etc/opt/novell/eDirectory/conf/nds.confファイルで、nds.confファイル内の次の変数を変更することにより、ndsd.logファイルのデバッグレベルを大きくすることができます。

n4u.server.log-levels=Logxxxx

ndsdのログレベルの詳細については、「eDirectoryのエラーログを管理する」を参照してください。

Linuxでのログファイルサイズの指定

ログファイルのサイズを指定するには、nds.confファイルでn4u.server.log-file-sizeパラメータを使用します。最大ファイルサイズは2GBで、デフォルトのファイルサイズは1MBです。ただし、1MBより小さいサイズをファイルサイズに設定することもできます。

この設定はndsd.logファイルには適用できません。

ログファイルのサイズが指定した制限値に到達した場合は、ログファイルの先頭から上書きされます。

3 NetIQ eDirectoryのWindowsへのインストールまたはアップグレード

WindowsプラットフォームでNetIQ eDirectory 9.2をインストールまたはアップグレードするには、次の情報を参照してください。

重要: NetIQ eDirectory 9.2では、Novell Clientがなくてもeディレクトリ for Windowsをインストールできます。すでにNovell Clientが組み込まれたコンピュータにeDirectory 9.2をインストールすると、eDirectoryは既存のClientを使用します。詳細については、「62 ページの 「Windowsサーバで eDirectory 9.2をインストールまたは更新する」」を参照してください。

システム要件

eDirectoryは以下のいずれかのプラットフォームにインストールする必要があります。

- Windows Server 2016 (最小要件)およびWindows Server 2019

重要: Windowsデスクトップバージョンはサポートされていません。

eDirectoryには、次のような要件もあります。

システム要件に関する最新情報については、『リリースノート』を参照してください。

- 割り当て済みのIPアドレス
- Windowsサーバに対する管理権、およびeDirectoryツリー内でドメインユーザオブジェクトを格納する全コンテナに対する管理権。既存のツリー内にインストールする場合は、スキーマを拡張しオブジェクトを作成するために、そのTreeオブジェクトに対する管理権が必要です。

ご使用のWindowsサーバのOS推奨ハードウェア要件を参照してください。

前提条件

重要: 既存のeDirectory環境をアップグレードする前に、現在インストールされているNetIQアプリケーションとサードパーティ製アプリケーションをチェックして、eDirectory 9.2に対応しているかどうかを確認してください。NetIQ製品の現在のステータスは、「TID 7003446 (http://www.novell.com/support/kb/doc.php?id=7003446)」で確認できます。何らかのアップグレードを実行する前に、eDirectoryをバックアップすることを強くお勧めします。

- ❒ FATファイルシステムの場合、NTFSに比べてトランザクション処理の安全性が低いため、eDirectoryはNTFSパーティションにのみインストールできます。FATファイルシステムしかない場合は、次のいずれかを実行します。
  - 新しいパーティションを作成し、NTFSとしてフォーマットする。

    この作業には、Windowsの「ディスクの管理」を使用します。詳細については、Windowsサーバのマニュアルを参照してください。
  - CONVERTコマンドを使って、既存のFATファイルシステムをNTFSに変換する。

    詳細については、Windowsサーバのマニュアルを参照してください。

  サーバにFATファイルシステムしか存在しないときに上記の措置をとらなかった場合は、インストールプログラムによってNTFSパーティションを作成するよう指示されます。
- ❒ (状況によって実行) NICI 3.2およびeDirectory 9.2でサポートされている最大のキーサイズは、RSA暗号化用の8192ビットです。8Kのキーサイズを使用するには、すべてのサーバがeDirectory 9.2にアップグレードされている必要があります。また、iManagerなどの管理ユーティリティを使用しているすべてのワークステーションにNICI 3.2がインストールされている必要があります。

  認証局(CA)サーバをeDirectory 9.2にアップグレードする場合、キーサイズは変わらず、2Kのままです。8Kのキーサイズを作成するには、eDirectory 9.2サーバでCAを再作成する必要があります。また、CAを作成する際に、デフォルトのキーサイズを2Kから8Kに変更する必要があります。

  注: Windows Silent Installerを使用するには、システムにNICI 3.2がインストールされている必要があります。
- ❒ eDirectory 9.2にアップグレードする場合は、ツリー内にあるeDirectory 9.2以外のすべてのサーバに最新のeDirectoryパッチがインストールされていることを確認してください。eDirectoryパッチは、NetIQ Support (http://support.novell.com) Webサイトから入手できます。
- ❒ .NET Management Framework 4.0以降が必要です。
- ❒ 最新のWindows 2012 R2 Service Packがインストールされていることを確認します。最新のWindowsServicePackは、WindowsSNMPサービスのインストール後にインストールする必要があります。
- ❒ 以前のバージョンのeDirectoryからアップグレードする場合は、eDirectory 8.8.8.x以降である必要があります。eDirectoryバージョンの確認方法の詳細については、60 ページの「eDirectoryのバージョンの確認」を参照してください。
- ❒ (状況によって実行)管理者以外のeDirectoryユーザとしてセカンダリサーバを既存のツリーにインストールしている場合は、次の権限を持っていることを確認します。
  - サーバのインストール先となるコンテナに対するスーパバイザ権。

- サーバを追加するパーティションに対するスーパバイザ権。

  注: この権限は、レプリカ数が3未満の場合にレプリカを追加するために必要です。

- すべての属性権: W0.KAP.Securityオブジェクトに対する読み込み権、比較権、および書き込み権。
- エントリ権: Securityコンテナオブジェクトに対するブラウズ権。
- すべての属性権: Securityコンテナオブジェクトに対する読み込み権、比較権。
- (状況によって実行)W1.KAP.Securityオブジェクトが存在する場合は、すべての属性権: このオブジェクトに対する読み込み権、比較権、および書き込み権。W1.KAP.Securityオブジェクトの詳細については、『NICI Administration Guide (NICI管理ガイド)』の「*Creating an AES 256-Bit Tree Key (AES 256 ビットツリーキーを作成する)*」を参照してください。

❒ (状況によって実行)管理者以外のユーザとしてセカンダリサーバを既存のツリーにインストールしている場合、ツリー内の少なくとも1台のサーバのeDirectoryバージョンが、コンテナ管理者として追加しているセカンダリのeDirectoryバージョンと同じかそれ以上である必要があります。追加しているセカンダリの方が新しいバージョンである場合、ツリーの管理者がスキーマを拡張してから、コンテナ管理者でセカンダリを追加する必要があります。

❒ セカンダリサーバを追加できるように、eDirectoryの設定中に、SLPサービスとファイアウォールのNCPポート(デフォルトは 524)を必ず有効にしてください。NCPポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を許可するように設定する必要があります。

必要に応じて、さらに以下のサービスポートも有効にできます。

- LDAP (クリアテキスト) - 389
- LDAP (セキュリティ保護) - 636
- HTTP (クリアテキスト) - 8028
- HTTP (セキュリティ保護) - 8030

ユーザ定義ポートを有効にした場合、eDirectoryの設定時にそのポートを指定する必要があります。

❒ DHCPアドレスが設定された仮想マシン、またはSLPがブロードキャストでない物理マシンまたは仮想マシンにeDirectoryをインストールしている場合、ディレクトリエージェントがネットワークで設定されていることを確認します。

❒ eDirectory 9.2へのアップグレード中に最新のプラットフォームエージェント(PA)がインストールされていない場合、場所<C:\NetIQ\eDirectory\auditds/から Novell_Audit_PlatformAgent_Win64.exeファイルを実行してインストールしてください。

❒ NetIQ eDirectory管理ツールボックス(eMBox)を使用すると、サーバ上でもリモートでもeDirectoryのバックエンドユーティリティすべてにアクセスできます。コマンドラインクライアントは、Javaアプリケーションです。これを実行するには、Oracle Javaの最新バージョン(1.8以上)をインストールする必要があります。また、古いバージョンのJavaすべてで、使用可能なパッチアップグレードをインストールしてアップグレードしてください。最新バージョンのJavaをインストールしたら、次の環境変数をエクスポートします。

- EDIR_JAVA_HOME
- JAVA_HOME
- JRE_HOME

注: eDirectory 9.0 SP4より前のバージョンを使用している場合、コマンドラインクライアントを実行するには、eDirectoryと一緒にインストールされたJavaランタイム環境(Oracle Java 1.8)にアクセスできなければなりません。

eDirectoryのバージョンの確認

eDirectoryのバージョンを確認するには、次のいずれかの手順を実行します。

- iMonitorを実行する。

  エージェントの概要ページで［認識サーバ］をクリックします。次に、［データベースで認識されているサーバ］の下にある［認識サーバ］をクリックします。［エージェントリビジョン］カラムに各サーバの内部ビルド番号が表示されます。たとえば、eDirectory 9.2のエージェントリビジョン番号は40101.xなどです。

  iMonitorの実行の詳細については、『「NetIQ eDirectory管理ガイド」』の「*iMonitorへのアクセス*」を参照してください。

- NDSCons.exeを実行する。

  Windowsの［コントロールパネル］で、［NetIQ eDirectory Services］をダブルクリックします。［サービス］カラムで、ds.dlmを選択し、［設定］をクリックします。［エージェント］タブに、マーケティング文字列(NetIQ eDirectory 9.2など)および内部ビルド番号(40101.xなど)が表示されます。

- ds.dlmファイルのプロパティを表示する。

  Windowsエクスプローラーの.dlmファイルを右クリックし、［プロパティ］ダイアログボックスの［バージョン］タブをクリックします。これにより、ユーティリティのバージョン番号が表示されます。ds.dlmファイルのデフォルトの場所はC:\NetIQ\eDirectoryです。

スタティックIPアドレスを設定する

eDirectoryを効率的に実行するには、サーバでスタティックIPアドレスが設定されている必要があります。DHCPアドレスのサーバにeDirectoryを設定すると、予期しない結果が発生することがあります。

ハードウェア要件

ハードウェア要件は、eDirectoryの実装条件によって異なります。

たとえば、標準スキーマを使用する基本的なeDirectoryのインストールでは、50,000ユーザごとに約74MBの空きディスク容量が必要です。ただし、新しい属性のセットを追加したり、既存の属性をすべて使用すると、オブジェクトのサイズは拡大します。それに対応して、必要な空きディスク容量、プロセッサ、およびメモリが変わります。

キャッシュメモリの量とプロセッサの速さという、2つの要因によってパフォーマンスが向上します。

最適な結果を得るためには、ハードウェアで可能な限り多くのDIBセットをキャッシュに入れるようにします。

eDirectoryはシングルプロセッサ上で良好に動作します。しかし、NetIQ eDirectory 9.2なら、マルチプロセッサの利点を活用できます。プロセッサを追加すると、ログインなど、一部の領域のパフォーマンスが向上します。また、複数のプロセッサ上で複数のスレッドをアクティブにすることでもパフォーマンスは上がります。eDirectory自体は、プロセッサ集約型ではなく、入出力集約型です。

次の表に、NetIQ eDirectory for Windows の一般的なシステム要件を示します。

オブジェクト	メモリ	ハードディスク
10,000	384MB	144MB
100万	2GB	1.5GB
1,000万	2GB以上	15GB

プロセッサの要件は、コンピュータで利用できる追加サービス、およびコンピュータが処理している認証と読み書きの数によって決まります。暗号化や索引付けなどの処理では、プロセッサが集中して使用されることがあります。

バックリンク処理の強制実行

eDirectoryにアップグレードすると内部eDirectory識別情報が変わるため、オブジェクトの整合性を保つために、バックリンクされたオブジェクトを更新するバックリンク処理を行う必要があります。

バックリンクでは、他のサーバ上のオブジェクトへの外部参照が追跡されます。バックリンク処理は、サーバ上の各外部参照について、実オブジェクトが正しい位置に存在することを確認するほか、マスタレプリカのすべてのバックリンク属性を確認します。バックリンク処理はデータベースがオープンされた2時間後に実行され、その後780分(13時間)ごとに実行されます。実行間隔には、2分から10,080分(7日)までの任意の値を設定できます。

eDirectoryにマイグレーションした後、次の手順を完了して、強制的にバックリンクを実行することをお勧めします。バックリンク処理の実行は、レプリカが存在しないサーバ上では特に重要です。

1. ［**スタート**］>［**設定**］>［**コントロールパネル**］>［**NetIQ eDirectoryサービス**］の順にクリックします。
2. ［**サービス**］タブで［**ds.dlm**］を選択します。
3. ［**設定**］をクリックします。
4. ［**トリガ**］タブの［**バックリンカ**］をクリックします。

eDirectoryをWindowsにインストールする

このセクションでは、次のことを説明します。

- 62 ページの 「Windowsサーバで eDirectory 9.2をインストールまたは更新する」
- 63 ページの 「サーバのヘルスチェック」
- 64 ページの 「LDAPを介したeDirectoryとの通信」
- 65 ページの 「NMASサーバソフトウェアのインストール」

- 65 ページの 「コンテナ名にドットを使用したツリーへのインストール」
- 66 ページの 「WindowsでのeDirectory 9.2の無人インストールと設定」
- 73 ページの 「ログファイルの場所」

Windowsサーバで eDirectory 9.2をインストールまたは更新する

eDirectory 9.2 for Windowsは、Novell Clientがなくてもインストールできます。すでにNovell Clientがあるマシンにe Directory 9.2をインストールする場合、eDirectoryは既存のClientを使用するか、それが最新のバージョンでなければ更新します。

1. Windowsサーバで、管理者または管理特権を持つユーザとしてログインします。
2. Autorunがオフになっている場合は、eDirectory 9.2 CD内のwindowsフォルダまたはダウンロードしたファイルから、eDirectory_920_Windows_x86_64.exeを実行します。
3. (新規インストールのみ) eDirectoryのインストールの種類を［基本］タブの下から選択します。
   - **新しいeDirectoryツリーの作成** 新しいツリーを作成します。ツリーに最初のサーバをインストールする場合、またはこのサーバに個別のツリーが必要となる場合は、このオプションを使用します。新しいツリー上で使用可能となるリソースは、別のツリーにログインしているユーザからは使用できません。
   - **既存のツリーへのeDirectoryのインストール** このサーバをeDirectoryネットワークに組み入れます。サーバはツリーのどのレベルにでもインストールできます。
4. eDirectoryインストール画面で情報を入力します。
   - 新しいeDirectoryサーバをインストールする場合は、新しいツリーのツリー名、サーバオブジェクトのコンテキスト、および管理者のログイン名とパスワードを指定します。

     重要: eDirectoryでは、NCPサーバオブジェクトのFDNを最大256文字までで設定できますが、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。
   - インストール先が既存のツリーの場合は、既存のツリーのIPアドレス、ツリー名、サーバオブジェクトのコンテキスト、および管理者のログイン名とパスワードを指定します。
   - eDirectoryサーバをアップグレードする場合は、管理者のパスワードを指定します。

     注: eDirectory 9.2では、すべてのユーティリティに大文字と小文字を区別するパスワードを使用できます。

   コンテナ名にドットを使用する場合の詳細については、65 ページの 「コンテナ名にドットを使用したツリーへのインストール」を参照してください。
5. インストールパスを指定するか、確認します。デフォルトの場所は、C:\NetIQ\eDirectoryです。
6. DIBのパスを指定するか確認します。デフォルトの場所は、C:\NetIQ\eDirectory\DIBFilesです。
7. ［詳細］タブで、次の情報を指定します。
   - IPv6アドレスを使用する場合は、[**IPV6を有効にする**]を選択します。

     注: インストールプロセス中にIPv6アドレスを有効にせず、後から使用することにした場合は、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。

  注: インストールプロセス中にEBAを有効にせず、後から有効にすることにした場合は、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。

  EBAを有効にしたセカンダリサーバをツリーに追加するには、ツリーでEBACAを設定しておく必要があります。EBACAが存在しない場合は、EBAを有効にせずにサーバを追加してから、EBA CAをホストするようにサーバをアップグレードします。この操作を行わないと、セカンダリサーバの設定が失敗します。

- eDirectory管理HTTPサーバで使用する［**HTTPスタックポート**］を指定します。

  重要: eDirectoryのインストール中に設定するHTTPスタックポートは、NetIQ iManagerで使用しているか、使用予定のHTTPスタックポートとは別のポートを指定してください。詳細については、『*iManager管理ガイド* (https://www.netiq.com/documentation/imanager/imanager_admin/data/bookinfo.html)』を参照してください。

- 使用する［**LDAPポート**］を指定します。

  詳細については、「64ページの「LDAPを介したeDirectoryとの通信」」を参照してください。

8 ［**インストール**］をクリックします。

  eDirectoryをインストールする前に、インストールプログラムによって次のコンポーネントがチェックされます。コンポーネントが検出されなかったり、バージョンが正しくない場合は、該当するコンポーネントのインストールが自動的に開始されます。

  - NICI 3.2

    Novell International Cryptographic Infrastructure (NICI)の詳細については、『*NICI Administration Guide (NICI管理ガイド)*』を参照してください。

9 すべての必須コンポーネントがeDirectoryによって自動的にインストールおよび設定されます。

10 インストーラがインストールが完了したら、［**完了**］をクリックしてウィザードを終了します。

重要: eDirectoryがインストールされているサーバにログインできるのはeDirectory管理者だけでなければなりません。

注: eDirectoryをインストールした後、eDirectoryサーバのDIBディレクトリは、ウィルス対策ソフトウェアやバックアップソフトウェアのプロセスから除外することをお勧めします。DIBディレクトリのバックアップは、eDirectoryバックアップツールを使って行えます。

eDirectoryのバックアップの詳細については、『「NetIQ eDirectory管理ガイド」』の*NetIQ eDirectoryのバックアップと復元*を参照してください。

サーバのヘルスチェック

eDirectory 9.2の場合、eDirectoryのアップグレードの際に、デフォルトでサーバヘルスチェックが実行され、サーバをアップグレードしても安全かどうかが確認されます。

- 161 ページの 「パーティションとレプリカの状態」

ヘルスチェックの結果に基づいて、次のようにアップグレードが継続または中止されます。

- すべてのヘルスチェックに成功すると、アップグレードは継続されます。
- あまり重大でないエラーの場合、アップグレードを継続するか中止するかを問うメッセージが表示されます。
- 重大なエラーの場合、アップグレードは中止されます。

あまり重大でないエラーと重大なエラーの一覧については「159 ページの付録 B「eDirectoryヘルスチェック」」を参照してください。

LDAPを介したeDirectoryとの通信

eDirectoryをインストールする場合、LDAPサーバが監視するポートを選択して、LDAP要求を処理できるようにする必要があります。次の表では、さまざまなインストールオプションを示します。

インストール	オプション	結果
eDirectory 9.2	クリアテキスト(ポート389)	ポート389を選択します。
eDirectory 9.2	暗号化(ポート636)	ポート636を選択します。

ポート389(業界標準のLDAPクリアテキストポート)

ポート389を通じた接続は暗号化されません。このポートへの接続を通して送信されるすべてのデータはクリアテキストです。このため、セキュリティの問題が伴います。たとえば、単純バインド要求でLDAPパスワードが見られる可能性があります。

LDAP単純バインドでは、DNおよびパスワードのみが要求されます。パスワードは平文形式です。ポート389を使用する場合、すべてのパケットはクリアテキスト形式です。デフォルトでは、eDirectoryインストールの実行中にこのオプションは使用できません。

ポート389ではクリアテキストが使用できるため、LDAPサーバサービスではこのポートを通じてeDirectoryへの読み込みおよび書き込みを処理します。このポートの使用は開放性が高く、通信に妨害を受けることがなく、パケットが不正受信されない信頼性の高い環境に適しています。

ポート636に対してセキュリティ保護された接続を行い、単純バインドを実行する場合は、接続はその時点ですでに暗号化されています。このため、パスワード、データパケット、またはバインド要求を閲覧することはできません。

ポート636(業界標準のセキュリティ保護されたポート)

ポート636を通じた接続は暗号化されます。TLS(以前のSSL)によって暗号化が管理されます。デフォルトでは、eDirectoryのインストールではこのポートが選択されます。

ポート636への接続では、自動的にハンドシェークをインスタンス生成します。ハンドシェークが失敗した場合、接続は拒否されます。

重要: この設定をデフォルトで選択することで、ローカルLDAPサーバに問題が発生する場合があります。eDirectoryがインストールされる前にホストサーバにロードされているサービスがポート636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。

eDirectoryのインストールでは、nldap.nlmファイルがロードされ、dstrace.logファイルにエラーメッセージが記録され、セキュアポートを使用せずに実行されます。

シナリオ: ポート636がすでに使用されている場合: ローカルサーバでActive Directoryを実行しています。Active Directoryでは、ポート636を使用してLDAPプログラムを実行しています。eDirectoryをインストールします。インストールプログラムによってポート636がすでに使用されていることが検出されるため、NetIQ LDAPサーバにポート番号は割り当てられません。LDAPサーバはロードを開始し、実行されているように見えますが、。LDAPサーバではすでに開いているポートを複製または使用できないため、複製されたポートでの要求はLDAPサーバで処理されません。

ポート389またはポート636がNetIQ LDAPサーバに割り当てられているかどうか不明な場合は、ICEユーティリティを実行してください。［**ベンダバージョン**］フィールドにNetIQが指定されていない場合は、eDirectoryのLDAP Serverを再設定し、別のポートを選択する必要があります。詳細については、『「NetIQ eDirectory管理ガイド」』の「*LDAP サーバが実行されているか確認する*」を参照してください。

シナリオ: Active Directoryが実行中の場合: Active Directoryが実行中です。クリアテキストポート389が開かれています。ポート389にICEコマンドを実行して、ベンダバージョンを確認してください。レポートにMicrosoft*が表示されます。次に、別のポートを選択してNetIQ LDAPサーバを再設定します。eDirectory LDAPサーバがLDAPの要求を処理できるようになります。

またNetIQ iMonitorでは、ポート389または636がすでに開かれていることも表示されます。LDAPサーバが動作していない場合、NetIQ iMonitorを使って、詳細を特定します。詳細については、『「NetIQ eDirectory管理ガイド」』の「*LDAP サーバが実行されているか確認する*」を参照してください。

NMASサーバソフトウェアのインストール

NMAS (Novell Modular Authentication Service)サーバコンポーネントは、eDirectoryインストールプログラムを実行すると自動的にインストールされます。NDSログインメソッドはデフォルトで設定されます。

ログインメソッドの詳細については、『NetIQ eDirectory管理ガイド』の「ログインとポストログインのメソッドとシーケンスの管理」を参照してください。

コンテナ名にドットを使用したツリーへのインストール

Windowsサーバは、名前にドット(.)が含まれるコンテナ(O=netiq.comまたはC=u.s.aなど)を保持しているeDirectoryツリーにインストールできます。名前にドットが含まれているコンテナを使用するには、ドットを円記号(\)でエスケープする必要があります。ドットをエスケープするには、コンテナ名に含まれるすべてのドットの前に円記号を挿入します。

名前の最初にドットを使用することはできません。たとえば、「.netiq」という名前のコンテナは作成できません。名前がドット(「.」)で始まっているためです。

重要: 名前にドットが含まれるコンテナがツリー内に存在する場合、 iMonitor、iManager、DHost iConsoleなどのユーティリティにログインする際、その名前をエスケープする必要があります。 たとえば、ツリーにOの名前として「netiq.com」がある場合、iMonitorにログインするときは［*ユーザ名*］フィールドに、ユーザ名**.netiq\.com**と入力します。

WindowsでのeDirectory 9.2の無人インストールと設定

eDirectory 9.2では、eDirectoryのインストールとアップグレードは自動化されているため、ユーザが操作しなくても、eDirectoryがWindowsサーバにサイレントでインストールまたはアップグレードされます。

WindowsのeDirectoryの無人インストールでは、無人インストールまたは無人アップグレードを円滑に実行できるように、事前定義されたテキストファイルが使用されます。eDirectoryの無人インストールを使用して、次のいずれかのセットアップを実行できます。

- eDirectoryのスタンドアロンインストールまたはアップグレード(eDirectoryの完全インストールかどうかによる)。スタンドアロンアップグレード処理は、インストールされているファイルだけをアップグレードします。
- インストールされているeDirectoryの設定。eDirectoryをインストールすると、eDirectoryの設定がすべて実行されます。インストールではなく、eDirectoryをアップグレードする場合、インストーラはアップグレードされたファイルだけを設定します。

無人インストールのセットアップ方法の詳細については、「67 ページの 「自動インストールに機能を追加する」」を参照してください。

前提条件

- .NET Management Framework 4.0以降が必要です
- Windows 2012 R2サーバが最新のWindowsパッチで更新されるようにします

次のセクションでは、インストール先、スプラッシュ画面の非表示、ポート設定、その他のNMAPメソッド、SNMPサービスの停止と開始など、無人インストールの設定に使用できるさまざまな機能について説明します。

- 66 ページの 「レスポンスファイル」
- 67 ページの 「自動インストールに機能を追加する」
- 71 ページの 「自動インストールを制御する」
- 72 ページの 「レスポンスファイルを使ったeDirectoryの無人インストール」

レスポンスファイル

Windowsオペレーティングシステムでのeディレクトリ 9.2のインストールまたはアップグレードでは、次の内容に対してレスポンスファイルを使うと、メッセージが表示されなくなり、より柔軟に作業することができます。

- 必要なすべてのユーザ入力が用意された完全無人インストール
- コンポーネントのデフォルト設定
- インストール中のすべてのプロンプトのバイパス

レスポンスファイルとは、Windows.iniファイルのようなセクションとキーが記述されているテキストファイルです。任意のASCIIテキストエディタを使って、レスポンスファイルの作成と編集ができます。eDirectoryアップグレードでは、レスポンスファイルからインストールパラメータが直接読み込まれ、デフォルトのインストール値がレスポンスファイルの値に置き換えられます。インストールプログラムはレスポンスファイルからの値を使って、プロンプトなしでインストールを続行します。

レスポンスファイルのセクションとキー

eDirectory9.2のインストールでは、レスポンスファイル内のセクションを変更して、ツリー名、管理者コンテキスト、管理者資格情報(ユーザ名とパスワードを含む)、インストール先など、インストールするeDirectoryインスタンスに関する情報を追加する必要があります。キーとそのデフォルト値の全リストは、eDirectoryのインストール時に提供されるサンプルのレスポンスファイルから入手できます。eDirectoryのインストール時に<eDirectoryInstallPath>\NetIQ\eDirectory\Sample_Response_Fileから4つのレスポンスファイルを入手できます。

- newtree.ni:このファイルは、新しいeDirectoryツリーの設定に使用されます。
- existingtree.ni:このファイルは、既存のeDirectoryツリーにサーバを追加するために使用されます。
- upgrade.ni:このファイルは、eDirectoryサーバをアップグレードするために使用されます。
- deconfigure.ni:このファイルは、eDirectoryツリーの設定を解除するために使用されます。

注: eDirectoryのインストール時に提供されるレスポンスファイルのいずれかを使用してください。必須のパラメータがあり、デフォルトでこれらのファイルで設定されます。これらのファイルを編集する場合は、キーと値のペアを結ぶ等号記号(「=」)の前後にスペースが入らないようにしてください。

自動インストールに機能を追加する

eDirectoryインストーラの細かな設定はほとんど、手動インストールのにデフォルト設定になっています。ただし無人インストール中は、各環境設定パラメータは明示的に設定されていなければなりません。このセクションでは、インストールの順番や追加機能に関係のない基本設定について説明します。

eDirectoryサーバの詳細情報

アップグレードか、プライマリ/セカンダリサーバのインストールかにかかわらず、インストールまたはアップグレード対象のサーバの詳細情報が、インストーラに提供される必要があります。この情報のほとんどは、タグ[NWI:NDS]で設定されます。

```
[NWI:NDS]
```

- **mode:** デフォルトでは、modeキーはconfigureに設定されています。これによってeDirectoryが設定されます。
- **Tree Name:** プライマリサーバのインストールでは、これはインストールする必要があるツリーの名前です。セカンダリサーバのインストールでは、サーバの追加先となるツリーになります。
- **Server Name:** インストールするサーバの名前です。
- **Server Container:** ツリーに追加されたサーバにはサーバオブジェクトがあり、そこにサーバ固有の詳細な設定情報がすべて入っています。このパラメータは、サーバオブジェクトの追加先となるツリーのコンテナオブジェクトです。プライマリサーバのインストールでは、このコンテナはサーバオブジェクトと共に作成されます。
- **Admin Login Name:** 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名前(RDN)。ツリー内のすべての操作は、このユーザとして実行されます。

- **Admin Context:** ツリーに追加されたユーザにはユーザオブジェクトがあり、そこにユーザ固有の詳細情報がすべて入っています。このパラメータは、管理者オブジェクトの追加先となるツリーのコンテナオブジェクトです。プライマリサーバのインストールでは、このコンテナはサーバオブジェクトと共に作成されます。
- **Admin password:** 前述のパラメータで作成された管理者オブジェクトのパスワード。このパスワードは、プライマリサーバのインストール時に管理者オブジェクトに対して設定されます。セカンダリサーバのインストールでは、これは新しいサーバの追加先となるコンテキストに対して権限を持っているプライマリサーバの管理者オブジェクトのパスワードである必要があります。

  環境変数で管理者のパスワードを設定し、レスポンスファイルで環境変数の名前を指定することをお勧めします。サイレント設定が完了したら、環境変数からパスワードを削除します。

  重要: 無人インストールで使用するレスポンスファイルに管理者ユーザ資格情報を入力します。このため、管理者資格情報が漏洩しないように、インストール後にこのファイルを完全に削除する必要があります。

- **DataDir:** デフォルトでは、DIBはNDSロケーション内のFilesサブフォルダにインストールされますが、管理者はこのパラメータを変更して別の場所を指定することができます。このパラメータに値が指定されない場合、値はデフォルトで<Install location>/DIBFilesに設定されます。
- **EBA:** 拡張バックグラウンド認証(EBA)は、ツリー内のNCPサーバを認証するため、改良され安全性の高まったバックグラウンド認証プロトコルを提供します。eDirectoryには、eDirectoryツリーの設定中または設定後にEBAを有効にするためのオプションが用意されています。レスポンスファイルを変更しない限り、EBAはデフォルトではeDirectory上には設定されません。EBAを有効にするには、［Require EBA］を［Yes］に設定します。
- **FIPS:** NetIQは、連邦情報処理標準(FIPS)モードで実行するeDirectoryをサポートしています。FIPSモードで実行するeDirectoryを有効にするには、［Require FIPS for TLS］を［Yes］に設定します。
- **Enable PBKDF2:** 新しい環境設定パラメータEnable PBKDF2が、eDirectory 9.2のnewtree.niレスポンスファイルに追加されました。このオプションを「yes」に設定すると、パスワードポリシーが作成され、ツリー全体に自動的に割り当てられます。このパスワードポリシーにより、ツリー内のすべてのユーザに対して、NDSパスワードのPBKDF2パスワードとの同期が可能になります。詳細については、『NetIQ eDirectory管理ガイド』の「非可逆パスワードストレージを理解する」を参照してください。

前述の基本パラメータをすべて記述したレスポンスファイルのテキスト例を次に示します。

```
[NWI:NDS]
mode=configure
New Tree=Yes
Tree Name=ENEWTREE
Server Name=ENEWSERVER
Server Container=myorg
Admin Context=myorg
Admin Login Name=Admin
Admin Password=env: PASSWORD_VAR
Require IPV6=NO
Require EBA=NO
Require FIPS for TLS=NO
DataDir=C:\NetIQ\eDirectory\DIBFiles
LDAP TCP Port=389
LDAP SSL Port=636
Require TLS=No
Require SS=YES
Enable PBKDF2=No
```

NMASメソッドを追加する

eDirectoryのインストールでもアップグレードでも、複数のNMASメソッドのインストールがサポートされています。手動インストール中に、インストールして設定するNMASメソッドを選択できます。自動インストールでも、NMASメソッドの選択ができます。

NMAS関連の環境設定は、[NWI:NMAS]タグ内で指定します。タグには、設定するキーが2つあり、どちらも必須です。

- **Choices:** このキーは、インストールする必要があるNMASメソッドの数を、eDirectoryインストールコンポーネントに通知します。
- **Methods:** このキーは、インストールする必要があるNMASメソッドオプションを一覧表示します。現在、サポートされているNMASメソッドが6つあります。メソッド名とそのタイプは以下の通りです。

表 3-1 *NMASメソッド*

メソッド名	メソッドタイプ
CertMutual	証明書相互ログインメソッド
Challenge Response	NetIQチャレンジ/レスポンス方式NMASメソッド
DIGEST-MD5	ダイジェストMD5ログインメソッド
SAML	Security Assertion Markup Languageの認証メソッド
NDS	NDSログインメソッド(デフォルト)
Simple Password	シンプルパスワードNMASログインメソッド
SCRAM	Salt Challenge Response Authentication Mechanism(SCRAM)では、PBKDF2ハッシュベースのパスワードを使用します。

注: メソッド名は、Methodキーに対するオプションとして、上の表に表示された名前と正確に一致する必要があります。インストーラは、インストールするNMASメソッドを選択するため、文字列の正確な比較(大文字/小文字を含む)を行います。

MSNMASメソッドは必須で、NMASメソッドのリストが無い場合に自動的にインストールされます。明示的リストが作成する場合も、リストからこのメソッドを削除しないでください。

この手法を使ってレスポンスファイルにNMASメソッドが設定されている場合、eDirectoryはユーザ入力のプロンプトを出さずに、インストール中にステータスメッセージを表示します。

NMASメソッドを選択するレスポンスファイルのサンプルテキストを次に示します。

```
[NWI:NMAS]
Methods=CertMutual,Challenge Response,DIGEST-MD5,NDS,Simple Password,SAML
```

HTTPポート

eDirectoryは、Webを介したアクセスのために事前設定されたHTTPポートをリスンします。たとえば、iMonitorはWebインタフェースを介してeDirectoryにアクセスします。適切なアプリケーションにアクセスするには、具体的な名前を指定する必要があります。eDirectoryを特定のポートに設定するには、インストールの前に設定できるキーが2種類あります。

- **クリアテキストHTTPポート:** クリアテキストのHTTP操作のためのポート番号。
- **SSL HTTPポート:** セキュアソケットレイヤ操作のためのHTTPポート番号。

HTTPポート番号を設定するレスポンスファイルのテキスト例を次に示します。

```
[eDir:HTTP]

Clear Text HTTP Port=8028

SSL HTTP Port=8030
```

LDAP環境設定

eDirectoryは、LDAP操作をサポートしています。eDirectoryは、2つの異なるポート上で、クリアテキストとSSLのLDAPリクエストをリスンします。インストール前にこれらのポートをレスポンスファイルで設定すれば、eDirectoryの起動時に設定されたポートをリスンすることができます。

［NWI:NDS］タグには、LDAPポートを設定する以下の3つのキーがあります。

- **LDAP TCP Port:** eDirectoryが平文のLDAPリクエストをリスンするポート。ポートが指定されない場合、デフォルトで389が使用されます。
- **LDAP SSL Port:** eDirectoryがSSLのLDAPリクエストをリスンするポート。バインドリクエストが平文でパスワードを送信する際にセキュリティ保護された接続をeDirectoryが必須とするかどうか、キーを使って設定することもできます。ポートが指定されない場合、デフォルトで636が使用されます。
- **Require TLS:** eDirectoryがLDAPリクエストを平文で受信する場合、TLSを必須とするかどうか指定します。このパラメータに値が指定されない場合、デフォルトで［はい］に設定されます。

LDAP環境設定のレスポンスファイルのテキスト例を次に示します。

```
[NWI:NDS]

Require TLS=Yes

LDAP TLS Port=389

LDAP SSL Port=636
```

自動インストールを制御する

レスポンスファイルを編集して、自動インストールのフローを制御することもできます。

SNMPサービスを停止する

これは、WindowsでのeDirectoryインストールに固有の機能です。ほとんどのWindowsサーバでは、SNMPが設定され、動作しています。eDirectoryをインストールする時は、SNMPサービスをダウン状態にして、インストール後に再起動する必要があります。手動インストールの場合、インストールを続行する前にSNMPサービスを停止するよう求めるプロンプトがインストーラの画面に表示されます。[NWI:SNMP]タブのキーを次のように設定することで、自動インストール中にこのプロンプトを表示しないようにすることができます。

- **Stop service:** この値を「Yes」に設定すると、プロンプトを表示せずにSNMPサービスを停止します。状態が画面上に表示されます。

SNMPサービスを停止するレスポンスファイルのテキスト例を次に示します。

```
[NWI:SNMP]

Stop service=yes
```

SLPサービス

eDirectoryはインストール時やアップグレード時、SLPサービスを使って、サブネット内の他のサービスやツリーを特定します。eDirectoryのインストールによってサーバですでにSLPサービスがインストールされている場合、eDirectoryの現行バージョンはSLPを検出して最新バージョンにアップグレードします。 SLPがインストールされていない場合、サイレントインストール時にeDirectoryによってSLPサービスがインストールされます。

デフォルトサーバ証明書のデフォルトのパラメータを指定する

eDirectoryには、新しいeDirectoryツリーを設定しながら、CA証明書とデフォルトサーバ証明書のデフォルトRSAキーサイズ、楕円曲線、および証明書の有効期限を指定するオプションが用意されています。レスポンスファイルの新しいeDirectoryツリーのサイレントインストール時にCA証明書とデフォルトサーバ証明書のために次のデフォルトパラメータを指定できます。

- **RSA Key Size:** 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。
- **EC Curve:** EC証明書の曲線の制限を指定します。使用可能な値はP256、P384、およびP521です。
- **Certificate Life:** 証明書の有効期限を年数で指定します。

ここで指定される値は、新しいツリーが構成されるときに組織のCAオブジェクトの対応する属性に設定されます。

これらの属性は、以下の例に示すように、新しいeDirectoryサーバのインストール中にnewtree.inファイルの[NWI:PKI]タグで設定できます。

```
[NWI:PKI]
RSA KeySize=4096
EC Curve=P521
Certificate Life=4
```

詳細については、『*NetIQ eDirectory管理ガイド*』の「組織の認証局オブジェクトを作成する」を参照してください。

プライマリ/セカンダリサーバのインストール

eDirectoryインストーラには、プライマリサーバまたはセカンダリサーバをネットワークに無人インストールする際に使用できるオプションがあります。プライマリサーバのインストールか、セカンダリサーバのインストールかを決定するキーが1つあります。

- **プライマリサーバ:** [NWI:NDS]タグで［新しいツリー］キーを使用し、newtree.niファイル、または新しいサーバのセットアップに必要な類似のレスポンスファイルで新規/プライマリツリーのインストールをYesに設定します。
- **セカンダリサーバ:** [NWI:NDS]タグで［新しいツリー］キーを使用し、existingtree.niファイル、またはセカンダリサーバのセットアップに必要な類似のレスポンスファイルでセカンダリツリーのインストールをNoに設定します。

たとえば、新しいツリーにプライマリサーバをインストールする場合は、次のようになります。

```
[NWI:NDS]

New Tree=Yes
```

既存ツリーにセカンダリサーバをインストールする場合は、次のようになります。

```
[NWI:NDS]

New Tree=No
```

レスポンスファイルを使ったeDirectoryの無人インストール

WindowsでeDirectoryインストーラを起動することは簡単です。eDirectoryリリースで配布されているeDirectory_920_Windows_x86_64.exeは、追加パラメータを指定してコマンドラインから起動します。

指定したセットアップモードに応じて、次のコマンドのどちらかを使用します。

インストール

<*Download Location Path*>\eDirectory_920_Windows_x86_64.exe /qn

例: D:\builds\eDirectory_920_Windows_x86_64.exe /qn

注: 以下のコマンドを実行して、任意の場所にeDirectoryをインストールします。

eDirectory_920_Windows_x86_64.exe /qn INSTALLDIR="C:\<*Install Location*>

設定

<*eDirectoryのインストール場所*>。/EConfig.ps1 -rfile <サンプルレスポンスファイルの場所>\newtree.ni

たとえば、C:\NetIQ\eDirectory>。/EConfig.ps1 -rfile C:\Sample_Response_Files\newtree.ni

---

注: ログファイルには、以下の場所からアクセスできます。

- C:\Program Files\NetIQ\eDirectory\installlogs
- C:\Program Files\NetIQ\eDirectory\logs

ログファイルの場所

dsinstall.log

<Windows Drive>\NetIQ\eDirectoryから入手可能なdsinstall.logファイルの最初の部分には、設定される環境変数の一覧が示されます。2番目の部分には、eDirectoryインストール処理を記録するステータスメッセージが含まれています。

WindowsでのeDirectoryのアップグレード

eDirectoryのアップグレードでは、eDirectory 8.8.8.x 64ビットからeDirectory 9.2 64ビットへのアップグレードが可能です。

注: 32ビットバージョンのeDirectoryを64ビットバージョンのeDirectoryにアップグレードするには、まず32ビットバージョンをeDirectory 8.8.x 64ビットバージョンにアップグレードし、次にそれをeDirectory 9.2にアップグレードします。64ビットのeDirectoryをeDirectory 9.2にアップグレードする場合と同じ手順に従います。

次のセクションでは、インストール済みの既存のeDirectoryを現在のバージョンにアップグレードするのに役立つ情報を提供します。

- 73 ページの 「Windowsインストーラを使用してeDirectoryをアップグレードする」
- 73 ページの 「WindowsでのeDirectoryの無人アップグレード」

Windowsインストーラを使用してeDirectoryをアップグレードする

Windowsインストーラを使用して、eDirectoryサーバをアップグレードすることができます。eDirectoryサーバをアップグレードするには、次の手順を実行します。

1. Windowsサーバで、管理者または管理特権を持つユーザとしてログインします
2. eDirectory 9.2 CDのwindowsフォルダから、またはダウンロードしたファイルから、eDirectory_920_Windows_x86_64.exeを実行します。
3. インストーラの画面に既存のeDirectoryツリー名が表示され、［**基本**］タブにサーバのFDNが表示されます。ツリー管理者の資格情報を入力し、［**アップグレード**］ボタンをクリックしてアップグレードプロセスを続行します。
4. ［**詳細**］タブでは、eDirectoryのインストール中に設定された既存の設定を変更できます。詳細については、62 ページの 「Windowsサーバで eDirectory 9.2をインストールまたは更新する」を参照してください。

WindowsでのeDirectoryの無人アップグレード

Windows上でeDirectoryをアップグレードする場合は、サイレントモードで実行することができます。

Windowsでは、アップグレードの前に、既存のeDirectoryサーバのツリー名、サーバ名、および管理者の資格情報をupgrade.niレスポンスファイルに指定する必要があります。

次に示すのは、アップグレードの設定を指定したupgrade.niレスポンスファイルのサンプルです。

```
[NWI:NDS]
mode=configure
Tree Name=enewtree
Server Name=enewserver
Server Container=org
Admin Context=org
Admin Login Name=Admin
Admin Password=env:PASSWORD_VAR
Require IPV6=NO
Require EBA=NO
Require FIPS for TLS=YES
LDAP TCP Port=389
LDAP SSL Port=636
Require TLS=Yes
Require SS=Yes
Existing Server=172.65.156.167
Existing Server Port=524

[NWI:SNMP]
Stop service=No

[NWI:NMAS]
Methods=CertMutual,Challenge Response,DIGEST-MD5,NDS,Simple Password,SAML
```

必要なeDirectoryサーバの詳細を指定して、upgrade.niレスポンスファイルの更新が済んだら、次のコマンドを実行して、eDirectoryサーバをアップグレードします。

<*eDirectory installed location*> ./EConfig.ps1 -rfile <Sample_Response_Files location>\upgrade.ni

例: C:\NetIQ\eDirectory> ./EConfig.ps1 -rfile C:\Sample_Response_Files\upgrade.ni。

4 Microsoft AzureでのeDirectoryのデプロイ

eDirectoryは、Microsoft Azure仮想マシンにデプロイできます。

eDirectoryでは、Azureで次のオペレーティングシステムがサポートされています。

- SUSE Linux Enterprise Server (SLES) 12 SP3
- SUSE Linux Enterprise Server (SLES) 12 SP4
- SUSE Linux Enterprise Server (SLES) 15
- Red Hat Enterprise Linux (RHEL) 7.5
- Red Hat Enterprise Linux (RHEL) 7.6

前提条件

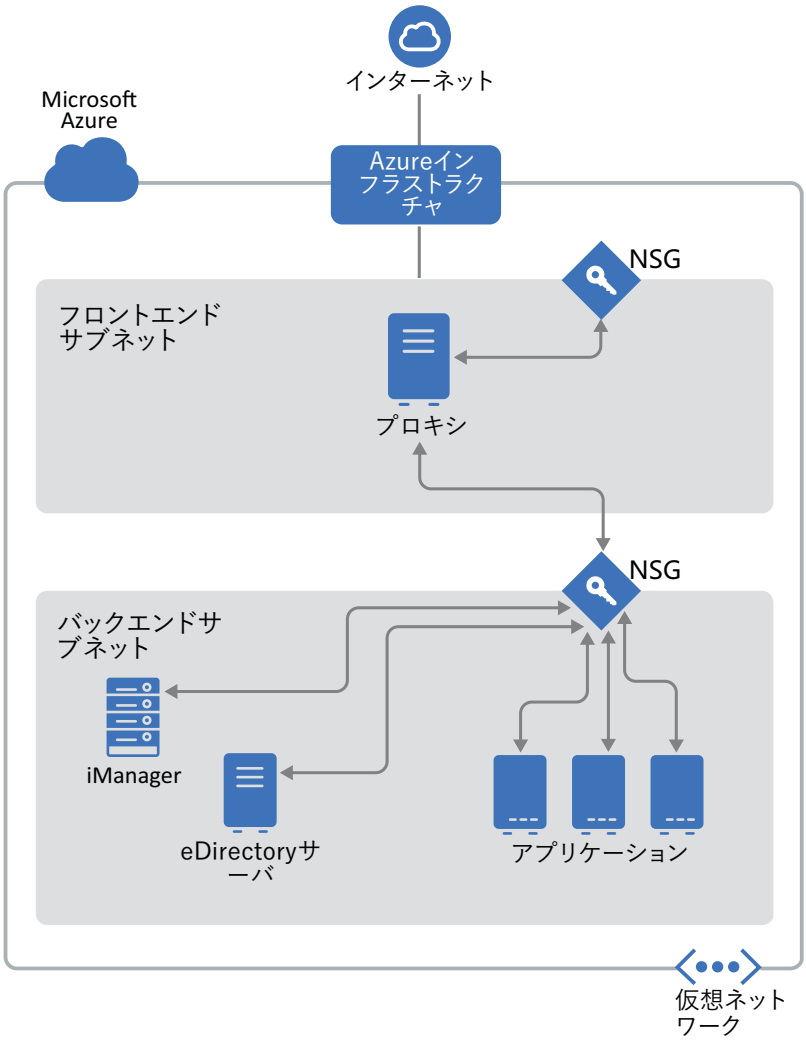
eDirectoryのシステム要件に加えて、次の要件を満たしていることを確認してください。

- Azureの管理アカウント。
- 仮想マシンにコピーできるように、eDirectoryインストーラ(tarballファイル)をダウンロードし、展開してあること。
- クライアントマシンからAzure仮想マシンに接続するSSHクライアント。

デプロイメントの手順

eDirectoryは、必ずAzure Virtual Networkのバックエンドサブネット内にデプロイする必要があります。図4-1は、後続のセクションで説明されているデプロイメントのサンプルを示しています。

図 4-1 Azure上でのeDirectoryのデプロイメント



注

- プロキシは、管理者がSSHを使用して接続し、SSHエージェント転送を使用してバックエンドサブネット内の他のインスタンスに接続する、フロントエンドサブネット内の要塞ホストです。
- eDirectoryにアクセスする必要があるアプリケーションは、バックエンドサブネットにデプロイする必要があります。これらのアプリケーションにインターネットからアクセスする必要がある場合は、フロントエンドサブネット内にAzureロードバランサーを設定して、アクセスを可能にします。詳細については、「Azure portalを使用してBasic Load Balancerを作成する」を参照してください。

デプロイメント手順は、次のステップで構成されます。

- 77 ページの 「Azureサービスの準備」
- 77 ページの 「アプリケーションセキュリティグループ(ASG)の設定」
- 78 ページの 「サブネット用のネットワークセキュリティグループ(NSG)の設定」
- 80 ページの 「仮想マシン用のネットワークセキュリティグループの設定」

- 82 ページの 「SSHキーペアを作成する」
- 82 ページの 「仮想マシンの作成とデプロイ」
- 83 ページの 「eDirectoryデータを格納するためのデータディスクの設定」
- 84 ページの 「eDirectoryとiManagerのインストール」
- 87 ページの 「監査サービスのデプロイ」
- 88 ページの 「障害復旧」

Azureサービスの準備

このセクションでは、eDirectoryで使用するAzureサービスを作成するための一般的な手順について概説します。これには、リソースグループ、仮想ネットワーク(VNet)、およびサブネットの作成が含まれます。

重要: 仮想ネットワーク、セキュリティグループ、仮想マシンなどのサービスを作成する際には、［**場所**］に同じ値を指定していることを確認してください。

リソースグループの作成

リソースグループは、Azureソリューションに関連するリソースを保持するコンテナです。リソースグループには、ソリューションのすべてのリソースを含めるか、またはグループとして管理するリソースのみを含めることができます。たとえば、AzureにeDirectoryをデプロイしている間は、リソースグループには仮想マシン、仮想ネットワーク、アプリケーションセキュリティグループ、ネットワークセキュリティグループ、パブリックIPアドレス、ネットワークインターフェイス、およびディスクが含まれている必要があります。リソースグループの作成方法の詳細については、「Azure portalを使用したAzureリソースの管理」を参照してください。

注: すべての管理者が、新しいリソースグループを作成する権限を持っているわけではありません。

仮想ネットワークの作成

Azure Virtual Networkを使用すると、Azure仮想マシン(VM)などの多くの種類のAzureリソースが、相互に、インターネットと、そしてオンプレミスのネットワークと安全に通信することができます。詳細については、「Azure Virtual Networkとは」を参照してください。

仮想ネットワークを作成する際には、デフォルトで1つのサブネットが作成されます。複数のサブネットを作成する場合は、新しく作成された**仮想ネットワーク**から、［**サブネット**］>［**サブネットの追加**］に移動します。

アプリケーションセキュリティグループ(ASG)の設定

アプリケーションセキュリティグループを使用すると、アプリケーション構造の自然な拡張としてネットワークセキュリティを設定できます。さらに、仮想マシンをグループ化し、それらのグループに基づいてネットワークセキュリティポリシーを定義することもできます。詳細については、「アプリケーションセキュリティグループ」を参照してください。

ネットワークセキュリティグループを設定する前に、次のアプリケーションセキュリティグループを作成する必要があります。

表 4-1 アプリケーションセキュリティグループ

名前	説明
SSH_Proxy	SSH_Proxyを設定する仮想マシンのネットワークインターフェイスが含まれます
eDirectory	eDirectoryを設定するすべての仮想マシンのネットワークインターフェイスが含まれます
eDirectory_CA	ツリー認証局(CA)をホストするeDirectoryサーバが設定される仮想マシンのネットワークインターフェイスが含まれます
iManager	iManagerが設定される仮想マシンのネットワークインターフェイスが含まれます

サブネット用のネットワークセキュリティグループ(NSG)の設定

NSGを使用して、サブネットのインバウンドおよびアウトバウンドのネットワークトラフィックをフィルタすることができます。NSGには、ネットワークトラフィックを、IPアドレス、ポート、およびプロトコルによってフィルタするセキュリティルールが含まれています。

このセクションでは、フロントエンドサブネット用にNSGを作成するためのルールについて概説します。デフォルトのセキュリティルールの上に、次のルールを設定します。

- インバウンドルール:

表 4-2 フロントエンドサブネットのインバウンドルール

優先度	名前	ポート範囲	ソース	宛先	アクション	説明
100	SSH	TCP 22	すべて(Any)	SSH_Proxy (ASG)	許可	インターネットからプロキシサーバへのSSH接続を許可します
110	Allow Subnet Traffic	すべて(Any)	すべて	フロントエンドサブネット	許可	(オプション)すべてのサブネット内トラフィックを許可します。 **注:** このルールは、相互に通信する必要のある他の仮想マシンがフロントエンドサブネット内にある場合にのみ設定します。

優先度	名前	ポート範囲	ソース	宛先	アクション	説明
120	All Traffic	すべて(All)	すべて	すべて	拒否	前のルールによってまだ処理されていないすべてのインバウンドトラフィックを拒否します

このセクションでは、バックエンドサブネットでNSGを作成するためのルールについて概説します。ネットワークセキュリティグループに対して、次のルールを設定します。

- インバウンドルール:

***表 4-3** バックエンドサブネットのインバウンドルール*

優先度	名前	ポート範囲	ソース	宛先	アクション	説明
100	SSH	TCP 22	プロキシ (ASG)	バックエンドサブネット	許可	SSHプロキシからのインバウンドSSHトラフィックを許可します
110	iManager	TCP 8443	プロキシ (ASG)	iManager (ASG)	許可	SSHプロキシからiManagerにアクセスするためのHTTPSトラフィックを許可します
120	HTTP CRL	TCP 8028	仮想ネットワーク	eDirectory_CA (ASG)	許可	ツリーCAによって発行された証明書を使用して設定されているVNetにサービスが存在する場合に、VNetからeDirectoryツリーのCRLにアクセスするために必要です。
130	Allow Subnet Traffic	すべて(Any)	バックエンドサブネット	バックエンドサブネット	許可	すべてのサブネット内トラフィックを許可します
140	All Traffic	すべて(All)	すべて	すべて	拒否	すべてのインバウンドトラフィックを拒否します

仮想マシン用のネットワークセキュリティグループの設定

セキュリティグループは、仮想ネットワーク内の1つまたは複数の仮想マシンに割り当てることができる仮想ファイアウォールルールのセットです。

デフォルトでは、新しいセキュリティグループではポート22の着信トラフィックのみが許可されるので、インスタンスにはSSHを使用してのみ接続できます。

詳細については、「セキュリティグループ」を参照してください。

AzureにeDirectoryをデプロイするには、次のネットワークセキュリティグループを作成します: eDirectory_NSG_1、eDirectory_NSG_2、およびiManager_NSG。これらのセキュリティグループを作成して次のポートルールを設定し、デフォルトのセキュリティルールを上書きします。

1. **eDirectory_NSG_1:** このNSGは、eDirectoryツリーのCAをホストする仮想マシンに関連付ける必要があります。

優先度	名前	ポート範囲	ソース	宛先	アクション	説明
100	SSH	TCP 22	SSHプロキシ (ASG)	eDirectory (ASG)	許可	SSHプロキシからのSSHトラフィックを許可します
110	NCP	TCP 524	バックエンドサブネット	eDirectory (ASG)	許可	バックエンドサブネット内でeDirectoryに対するNCPトラフィックを許可します
120	HTTP CRL	TCP 8028	仮想ネットワーク	eDirectory_CA (ASG)	許可	ツリーCAによって発行された証明書を使用して設定されているVNetにサービスが存在する場合に、VNetからeDirectoryツリーのCRLにアクセスするために必要です。
130	LDAPS	TCP 636	バックエンドサブネット	eDirectory (ASG)	許可	バックエンドサブネット内でセキュリティ保護されたLDAPトラフィックを許可します

優先度	名前	ポート範囲	ソース	宛先	アクション	説明
140	SLP	Any 427	バックエンドサブネット	eDirectory (ASG)	許可	バックエンドサブネット内のSLPトラフィックを許可します
150	All Traffic	すべて(All)	すべて	すべて	拒否	すべてのインバウンドトラフィックを拒否します

注: eDirectoryサーバは、LDAPポート389でリスンするように設定してはならず、eDirectoryに割り当てられているセキュリティグループに対してポート389へのアクセスを許可してはなりません。また、HTTPポートへのアクセスを許可するのは、ツリーのCAをホストしているeDirectoryサーバに割り当てられたセキュリティグループに対してのみにする必要があります。

2. **eDirectory_NSG_2:** このNSGは、eDirectoryツリーCA以外のeDirectoryサーバをホストしているすべての仮想マシンに関連付ける必要があります。

優先度	名前	ポート範囲	ソース	宛先	アクション	説明
100	SSH	TCP 22	SSHプロキシ (ASG)	eDirectory (ASG)	許可	SSHプロキシからのSSHトラフィックを許可します
110	NCP	TCP 524	バックエンドサブネット	eDirectory (ASG)	許可	バックエンドサブネット内でeDirectoryに対するNCPトラフィックを許可します
120	LDAPS	TCP 636	バックエンドサブネット	eDirectory (ASG)	許可	バックエンドサブネット内でセキュリティ保護されたLDAPトラフィックを許可します
130	SLP	Any 427	バックエンドサブネット	eDirectory (ASG)	許可	バックエンドサブネット内のSLPトラフィックを許可します
140	All Traffic	すべて(All)	すべて	すべて	拒否	すべてのインバウンドトラフィックを拒否します

3. **iManager_NSG:** このNSGは、iManagerをホストする仮想マシンに関連付ける必要があります。次のNSGルールを使用すると、プロキシサーバのみからiManagerサーバにアクセスできるようになります。

優先度	名前	ポート範囲	ソース	宛先	アクション	説明
100	SSH	TCP 22	SSHプロキシ(ASG)	iManager(ASG)	許可	プロキシからのSSHトラフィックを許可します
110	HTTPS	TCP 8443	SSHプロキシ(ASG)	iManager(ASG)	許可	プロキシからiManagerにアクセスする、セキュリティ保護されたHTTPトラフィックを許可します
120	All Traffic	すべて(All)	すべて	すべて	拒否	すべてのインバウンドトラフィックを拒否します

SSHキーペアを作成する

Azure VMを設定する前に、SSHキーペアを作成する必要があります。キーペアを作成するには、次の手順を実行します。

1 次のコマンドを使用して、クライアント上で4096ビットのRSA SSHキーペアを作成します。

```
ssh-keygen -t rsa -b 4096
```

ssh-keygenにより、新しく作成された公開鍵が~/.ssh/id_rsa.pubに置かれます。

2 このSSH公開鍵をAzureアカウントに提供します。詳細については、「SSH公開鍵を提供する」を参照してください。

重要: SSH秘密鍵を使用してのみ、仮想マシンに接続して管理できます。そのため、SSH秘密鍵を紛失しないようにしてください。

仮想マシンの作成とデプロイ

サポートされているプラットフォームのいずれかで仮想マシン(VM)を作成して起動します。VMを作成して起動する方法の詳細については、「Azure portalでLinux仮想マシンを作成する」を参照してください。インスタンスを作成および起動する際には、次の手順も実行する必要があります。

1 最初のeDirectoryサーバを設定するVMにeDirectory_NSG_1を関連付け、その他のすべてのeDirectoryサーバを設定するVMにeDirectory_NSG_2を関連付け、iManagerを設定するVMにiManager_NSGを関連付けます。セキュリティグループの詳細については、80 ページの 「仮想マシン用のネットワークセキュリティグループの設定」を参照してください。

2 82 ページの 「SSHキーペアを作成する」セクションで作成した公開鍵をインスタンスに関連付けます。

注: 選択したAzureの場所に対して複数の可用性ゾーンが使用可能な場合は、レプリカサーバをマスタeDirectoryサーバと同じ可用性ゾーンにデプロイしないでください。

eDirectoryデータを格納するためのデータディスクの設定

Azure VMのクラッシュが発生した場合にeDirectoryのデータと設定が失われるのを防ぐには、データディスクを設定する必要があります。eDirectoryのデータと設定を復元する方法の詳細については、88 ページの 「障害復旧」を参照してください。VMを作成した後、次の手順を実行して、eDirectoryをデプロイできるようにVMを準備します。

1. データディスクを作成して接続するために、「ポータルを利用し、データディスクをLinux VMに接続する」の手順を実行します。
2. VMにログインし、ext4ファイルシステムを使用してデータディスクをフォーマットし、データディスクをマウントします。データディスクをフォーマットしてマウントする方法の詳細については、「Linux VMを接続して新しいディスクをマウントする」を参照してください。
3. ディレクトリを、データディスクからeDirectoryデータディレクトリとNICIデータディレクトリにバインドマウントします。ルートユーザとして次の手順を実行して、バインドマウントします。

   3a 次のコマンドを使用して、eDirectoryデータディレクトリを作成します。

   ```
   mkdir <mount_point>/eDirectory_data
   ```

   3b 次のコマンドを使用して、NICIデータディレクトリを作成します。

   ```
   mkdir <mount_point>/nici_data
   ```

   3c 次のコマンドを使用して、NICIおよびeDirectoryの環境設定ディレクトリを作成します。

   ```
   mkdir <mount_point>/eDirectory_nici_conf
   ```

   3d 次のコマンドを使用して、eDirectoryに必要なディレクトリを作成します。

   ```
   mkdir --parents /var/opt/novell/eDirectory
   mkdir –-parents /var/opt/novell/nici
   mkdir –-parents /etc/opt/novell/eDirectory
   ```

   3e ディレクトリをバインドマウントするために、次の内容を/etc/fstabに追加します。

   ```
   <mount_point>/eDirectory_data /var/opt/novell/eDirectory none
   defaults,bind 0 0

   <mount_point>/nici_data /var/opt/novell/nici none defaults,bind 0 0

   <mount_point>/eDirectory_nici_conf /etc/opt/novell/eDirectory none
   defaults,bind 0 0
   ```

注: VM内でのすべての操作は、ルートユーザとして実行する必要があります。

eDirectoryとiManagerのインストール

前提条件

- ❒ 「システム要件」に記載されている要件を満たしていることを確認します。
- ❒ 80 ページの 「仮想マシン用のネットワークセキュリティグループの設定」で説明されているように、セキュリティグループを作成します。
- ❒ プロキシVMは、強化され、セキュリティ保護されたサーバである必要があります。バックエンドサブネット内のVMおよびプロキシVMへのアクセスに必要なSSH秘密鍵は、VNet内には保存しないでください。クライアント上にのみ保存してください。このインスタンスに適したパフォーマンスとメモリを提供するVMサイズを選択します。
- ❒ プロキシVMに対する追加のネットワークインターフェイスを作成し、そのインターフェイスにスタティックなパブリックIPアドレスを割り当てます。
- ❒ プロキシVM内にVNCサーバを設定します。VNCサーバは、強力なパスワードを使用して強化する必要があります。セキュリティ保護された通信を可能にするために、SSHトンネルを使用してVNCサーバに接続します。VNCサーバは、localhostからの接続についてのみリスンするように設定する必要があります。セッションのロックアウトを防止するために、画面ロックを無効にします。VNCサーバを使用した後、セッションを終了する必要があります。
- ❒ VMの/etc/hostsファイルを手動で更新して、IP-Address Full-Qualified-Hostname Short-Hostnameエントリを設定します。これは、逆引きDNS検索を実行する際のAzureの制限を回避するためです。
- ❒ eDirectory/iManagerを設定するバックエンドサブネット内のVMには、SSHプロキシを使用して接続します。

  ```
  ssh -i edir_key.pem -A -J azureuser@<ssh_proxy_ip>
  azureuser@<instance_private_ip>
  ```

  注

  - 上記のサンプルコマンドで、edir_key.pemは、サーバキーを含むサンプルファイル名です。
  - SSH-Addコマンドを使用してエージェント内に識別情報ファイルを追加すれば、ログインするたびに識別情報ファイルを使用しないで済みます。

  VMのプライベートIPアドレスを表示するには、［**インスタンス**］> *［インスタンス］* >［**説明**］をクリックします。
- ❒ バックエンドサブネット内のVMにSLPディレクトリエージェント(DA)サーバを設定します。SLP DAがデプロイされているVMに対して、NSGのインバウンドルールでポート427を開きます。slp.confファイルを編集して、DA操作を有効にします。詳細については、『*NetIQ eDirectory管理ガイド*』の「OpenSLP for eDirectoryの設定」を参照してください。

インストールと環境設定の手順

このセクションでは、Azure環境にeDirectoryとiManagerをインストールして設定する手順について説明します。eDirectoryをインストールした後、次の条件を満たしていることを確認する必要があります。

- EBAが有効になっている
- SNMPが無効になっている

- eDirectoryがポート389でリスンしていない
- LDAPおよびHTTPサービスは、ECDSA証明書のみを使用するように設定されている
- バックエンドサブネット内のAzure VMのSSHポートへのアクセスは、不使用時は無効になっている
- iMonitor、eMBox、およびDHostモジュールを無効にして、セキュリティを強化する。これらのモジュールを無効にした後、これらのモジュールに関係するすべてのアクティビティは、NDSユーティリティのみを使用して実行する必要があります。

eDirectoryのインストールと設定

1. eDirectoryを設定するバックエンドサブネット内のVMに、セキュアコピー(scp)を使用してeDirectory_<*version*>_Linux_x86_64.tar.gzファイルをコピーします(SSHプロキシを使用します)。

   ```
   scp -i <keyname> -o ProxyJump=vm-user@<ssh_proxy_ip>
   eDirectory_<version>_Linux_x86_64.tar.gz vm-user@<instance_ip>:/<directory>
   ```

2. eDirectoryをインストールします。詳細については、「nds-installユーティリティを使用してeDirectoryコンポーネントをインストールする」を参照してください。
3. eDirectoryを設定します。詳細については、「ndsconfigユーティリティを使用してeDirectoryレプリカサーバを追加または削除する」を参照してください。たとえば、eDirectoryをインストールして設定するためのコマンドのサンプルを次に示します。

   ```
   ndsconfig  new [-t <tree_name>] [-n <server context>] -a <admin FDN> [-w <admin
   password>] -P ldaps://<instance_ip> --configure-eba-now yes
   ```

4. openslp-serverをインストールして、SLPDサービスを始動します。

iManagerのインストールと設定

iManager管理コンソールを使用すると、Azure環境上でのeDirectoryの操作を管理できます。iManagerは、eDirectoryをインストールした後で、Azure VMにインストールする必要があります。

1. iManagerを設定するバックエンドサブネット内のインスタンスに、セキュアコピー(scp)を使用してiMan_<*version*>_linux_x86_64.tgzファイルをコピーします(SSHプロキシを使用します)。

   ```
   scp -i <keyname> -o ProxyJump=vm-user@<ssh_proxy_ip>
   iMan_<version>_linux_x86_64.tgz vm-user@<instance_ip>:/<directory>
   ```

2. iManagerをインストールして設定します。詳細については、「LinuxでのiManagerサーバのインストール」を参照してください。iManagerをインストールする前に、『*iManagerインストールガイド*』の「システム要件」セクションに記載されているシステム要件を参照してください。
3. iManagerが実行されているVMに、EBA CA証明書をダウンロードします。詳細については『*NetIQ eDirectory管理ガイド*』の「iManagerを使用したEBA CAの管理」を参照してください。
4. iManagerを実行しているVMの自己署名証明書を、セキュアCA署名証明書で置き換えます。詳細については、「iManager用の一時的な自己署名証明書の置き換え」を参照してください。

注: iManagerサーバは、ECDSA証明書のみを使用するように設定してください。iManagerをインストールした後、権限を持ったユーザと、このユーザが管理する適切なeDirectoryツリー名を指定します。

iManagerの起動

次の手順を実行して、iManagerを起動します。

1. SSHトンネルを使用して、プロキシVMのlocalhost上で実行されているVNCサーバに接続します。
2. 同じインスタンスにブラウザをインストールして起動します。
3. IPアドレスまたはツリー名を使用して、eDirectoryツリーを起動して接続します。

設定後のタスク

1. EBAが有効になっているかどうかを確認するため、『*NetIQ eDirectory管理ガイド*』「EBAに関する情報の表示」を参照してください。
2. 証明書サーバでSuite Bを有効にします。詳細については、『*NetIQ eDirectory管理ガイド*』の「証明書サーバでのSuite Bの有効化」を参照してください。
3. 1番目のeDirectoryサーバに対してAES 256ビットツリーキーを設定します。詳細については、『*NICI Administration Guide (NICI管理ガイド)*』の「Creating an AES 256-Bit Tree Key (AES 256ビットツリーキーを作成する)」を参照してください。
4. 1番目のeDirectoryサーバにあるCRL配布ポイントを削除します。ポート389でのセキュリティ保護されていないLDAPアクセスはすべてのeDirectoryサーバで無効化されているため、ツリーCAのCRLはHTTPのみでダウンロードできるようにする必要があります。次の手順を実行して、CRL配布ポイントを削除します。
   - **4a** 管理者としてiManagerにログインします。
   - **4b** ［**役割およびタスク**］>［**NetIQ証明書サーバ**］>［**認証局の環境設定**］に移動します。
   - **4c** ［**CRL**］をクリックします。
   - **4d** ［**One**］をクリックします。HTTP CRL配布ポイント(http://<instance_ip>:8028/crl/one.crl)以外のすべての［**CRL配布ポイント**］を選択して削除します。
   - **4e** ［**適用**］をクリックし、［**閉じる**］をクリックします。
   - **4f** ［**OneEC**］をクリックします。HTTP CRL配布ポイント(http://<instance_ip>:8028/crl/oneec.crl)以外のすべての［**CRL配布ポイント**］を選択して削除します。
   - **4g** ［**適用**］をクリックし、［**OK**］をクリックします。
5. iManager証明書サーバプラグインを使用して、サーバのデフォルト証明書を修復します。デフォルト証明書を修復するには、次の手順を実行します。
   - **5a** 管理者としてiManagerにログインします。
   - **5b** ［**役割およびタスク**］>［**NetIQ証明書サーバ**］>［**デフォルト証明書の修復**］に移動します。
   - **5c** 証明書を所有するサーバを選択して、［**次へ**］をクリックします。
   - **5d** ［**デフォルト証明書はすべて上書きされます**］を選択し、［**次へ**］をクリックします。
   - **5e** 実行するタスクを確認し、［**完了**］を選択します。

6 ECDSA証明書とSuiteB暗号化を使用するようにLDAPサービスとHTTPサービスを設定します。詳細については『*NetIQ eDirectory管理ガイド*』の「ECDSA証明書とSuite B Cipherを使用するためのLDAPサービスとHTTPサービスの設定」を参照してください。完了したら、eDirectory を再起動します。

7 SNMPサブエージェントがアンロードされているかどうかを確認する方法について、『*NetIQ eDirectory管理ガイド*』の「SNMPサーバモジュールのロードとアンロード」を参照します。

8 eDirectoryがポート389でリスンしていないことを確認します。

9 iMonitor、eMBox、DHost、およびHTTPスタックを無効にします。

9a 次の手順を実行して、ツリーCAをホストしているeDirectoryサーバのiMonitor、eMBox、およびDHostを無効にします。

9a1 ndsmodules.confファイルを編集して、hconserv、imon、およびemboxをコメント化します。

9a2 eDirectoryを再起動します。

9b 次の手順を実行して、eDirectoryレプリカサーバのHTTPスタックを無効にします。

9b1 ndsmodules.confファイルを編集して、httpstk、hconserv、imon、およびemboxをコメント化します。

9b2 eDirectoryを再起動します。

注: httpstkは、コメント化の前に、ndsmodules.confファイル内でndsより上に配置されている必要があります。これにより、ndsモジュールはHTTPスタックを有効にしなくなります。

---

10 アドバタイジング方式としてユニキャストを使用することをeDirectoryに強制するように、SLPを設定します。バックエンドサブネット内のDAサーバのIPアドレスを提供するように、slp.confファイルを編集します。詳細については、『*NetIQ eDirectory管理ガイド*』の「環境設定パラメータ」を参照してください。

注: すべてのeDirectory VMとiManagerの設定が完了したら、SSHポートへのアクセスを拒否し、必要な場合にのみ許可するように、Azureバックエンドサブネットのセキュリティルールを設定してください。

監査サービスのデプロイ

AzureにCommon Event Format (CEF)監査サービスをデプロイして、さまざまなeDirectoryイベントを監査することができます。CEF監査サービスをデプロイするには、次の手順を実行します。

1 VNetに監査サーバをインストールします。

2 ポート上でリスンするように監査サーバを設定します

注: 監査サーバとしてはSentinelを使用することをお勧めします。

---

3 フロントエンドサブネットに新しいネットワークセキュリティグループルールを作成して次のように設定し、監査サーバが実行されているVMに関連付けます。

名前	ポート	ソース	宛先	説明
Auditing Server Port	TCP (監査サーバポート)	バックエンドサブネット	監査サーバのIP	eDirectoryサーバからのイベントの受信を許可します

4 すべてのeDirectoryインスタンスで、次のように/etc/opt/novell/eDirectory/conf/auditlogconfig.propertiesファイルを更新します。

```
log4j.appender.S.Host=<Auditing server ip>
log4j.appender.S.Port=<auditing server port>
```

5 iManagerから、対応するCEFイベントを有効にします。詳細については、「監査するCEFイベントの設定」を参照してください。有効にされたイベントは、監査サーバに転送されます。

障害復旧

障害復旧は、eDirectoryが実行されているVMでクラッシュが発生した場合に実行します。障害復旧を行うには、次の手順を実行します。

1 クラッシュしたVMを停止し、データディスクとの関連付けを解除します。詳細については、「データディスクをLinux仮想マシンから切断する方法」を参照してください。

2 クラッシュしたVMと同じオペレーティングシステムを使用して、新しいVMを設定します。

3 新しいVMに同じバージョンのeDirectoryをインストールします。

4 データディスクを新しいVMに接続し、ファイルシステムをマウントします。詳細については、「ポータルを利用し、データディスクをLinux VMに接続する」を参照してください。

5 ディレクトリをバインドマウントします。

ディレクトリをバインドマウントするには、/etc/fstabを次のように更新します。

```
<mount_point>/eDirectory_data /var/opt/novell/eDirectory none defaults,bind 0
0

<mount_point>/nici_data /var/opt/novell/nici none defaults,bind 0 0

<mount_point>/eDirectory_nici_conf /etc/opt/novell/eDirectory none
defaults,bind 0 0
```

6 /etc/opt/novell/eDirectory/conf/nds.conf内のIPアドレスを、現在のVMのIPアドレスに変更します。

7 eDirectoryをアップグレードしてヘルスチェックをスキップします。詳細については、『NetIQ eDirectoryインストールガイド』の「*eDirectoryをアップグレードする*」を参照してください。

8 ndsrepairユーティリティを使用して、ネットワークアドレスを修復します。詳細については、『NetIQ eDirectory管理ガイド』の「*DSRepairオプション*」を参照してください。

9 ツリーCAのIPアドレスが変更された場合は、CRL配布ポイントのIPアドレスを変更します。IPアドレスの変更方法の詳細については、『NetIQ eDirectory管理ガイド』の「CRL環境設定オブジェクトのプロパティの表示と変更」を参照してください。

10 iManager証明書サーバプラグインを使用して、サーバのデフォルト証明書を修復します。デフォルト証明書を修復するには、次の手順を実行します。

10a 管理者としてiManagerにログインします。

10b ［**役割およびタスク**］>［**NetIQ証明書サーバ**］>［**デフォルト証明書の修復**］に移動します。

10c 証明書を所有するサーバを選択して、［**次へ**］をクリックします。

10d ［**デフォルト証明書はすべて上書きされます**］を選択し、［**次へ**］をクリックします。

10e 実行するタスクを確認し、［**完了**］を選択します。

11 新しいECDSA証明書を使用するようにLDAPおよびHTTPサービスを設定します。

5 Amazon Web Services EC2でのeDirectoryのデプロイ

eDirectoryは、Amazon Web Services (AWS) EC2インスタンスにデプロイできます。

eDirectoryでは、AWS EC2で次のオペレーティングシステムがサポートされています。

- SUSE Linux Enterprise Server (SLES) 12 SP3
- SUSE Linux Enterprise Server (SLES) 12 SP4
- SUSE Linux Enterprise Server 15
- Red Hat Enterprise Linux (RHEL) 7.5
- Red Hat Enterprise Linux (RHEL) 7.6

前提条件

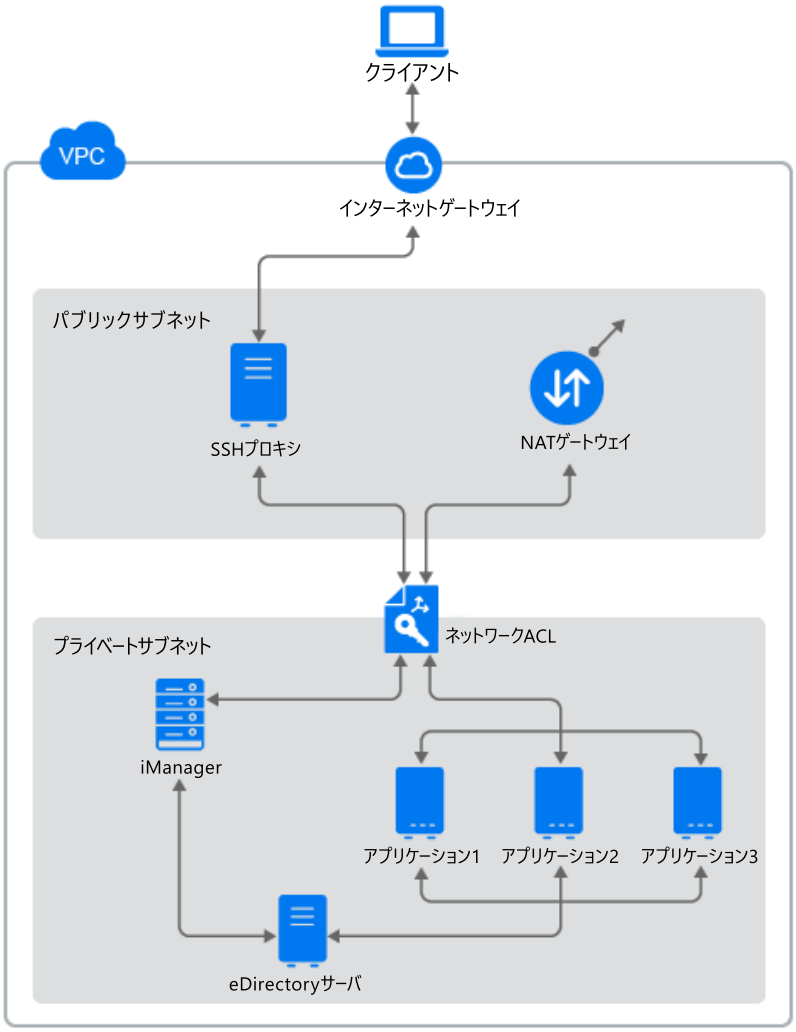
eDirectoryのシステム要件に加えて、次の要件を満たしていることを確認してください。

- AWS EC2の管理アカウント。
- インスタンスにコピーできるように、eDirectoryインストーラ(tarballファイル)をダウンロードし、展開してあること。
- クライアントマシンからAWS EC2インスタンスに接続するSSHクライアント。

デプロイメントの手順

eDirectoryは、Amazon VPC内のプライベートサブネットにのみデプロイされる必要があります。図4-1は、後続のセクションで説明されているデプロイメントのサンプルを示しています。

図 5-1 AWS EC2上でのeDirectoryのデプロイメント



注

- SSHプロキシは、管理者がSSHを使用して接続し、SSHエージェント転送を使用してプライベートサブネット内の他のインスタンスに接続する、パブリックサブネット内の要塞ホストです。
- eDirectoryにアクセスする必要があるアプリケーションは、プライベートサブネットにデプロイする必要があります。これらのアプリケーションにインターネットからアクセスする必要がある場合は、パブリックサブネット内にAWS EC2ロードバランサーを設定して、アクセスを可能にします。詳細については、「Application Load Balancerの作成」を参照してください。

デプロイメント手順は、次のステップで構成されます。

- 93 ページの 「AWS仮想プライベートクラウドの準備」
- 94 ページの 「ネットワークACLの設定」
- 96 ページの 「セキュリティグループの設定」
- 97 ページの 「SSHキーペアを作成する」
- 97 ページの 「インスタンスの作成とデプロイ」

- 98 ページの 「eDirectoryデータの保存用にEBSボリュームを設定する」
- 98 ページの 「eDirectoryとiManagerのインストール」
- 102 ページの 「監査サービスのデプロイ」
- 103 ページの 「障害復旧」

AWS仮想プライベートクラウドの準備

このセクションでは、eDirectoryで使用するためにAWS VPCを設定する一般的な手順について概説します。詳細については、「Amazon Elastic Compute Cloudドキュメント」を参照してください。

次の手順を実行し、AWS VPCサービスを作成します。

1 AWS管理コンソールにログインします。

2 次のサービスを作成します。

サービス	説明
VPC	Amazon VPCコンソールを使用して、VPCを作成することができます。VPCの作成方法の詳細については、「VPCの作成」を参照してください。 VPCの概要に関する詳細については、「Amazon Virtual Private Cloud ドキュメント」を参照してください。
重要: ［VPCウィザードの起動］を使用してVPCを作成すると、VPC用に2つのサブネット、インターネットゲートウェイ、およびルートテーブルとNATゲートウェイが作成されます。これらの項目を表示または編集するには、次の手順に従います。	
サブネット	VPC作成の一環として、2つのサブネットが作成されます。パブリックおよびプライベートサブネットです。eDirectoryは、プライベートサブネットにデプロイする必要があります。図 4-1に示したとおり、eDirectoryにアクセスするすべてのアプリケーションは、同じプライベートサブネットにデプロイする必要があります。プライベートサブネット内のインスタンスへのSSHアクセスは、パブリックサブネット内のSSHプロキシを経由して行う必要があります。詳細については、「VPCとサブネット」を参照してください。
インターネットゲートウェイ	インターネットゲートウェイは、図 4-1に示したとおり、SSHプロキシへのSSH接続を可能にするために必要です。VPCを使用してインターネットゲートウェイを作成および接続する方法の詳細については、「インターネットゲートウェイ」を参照してください。
ルートテーブル	ルートテーブルを作成する方法の詳細については、「ルートテーブル」を参照してください。
NATゲートウェイ	オペレーティングシステムの更新をダウンロードするためのプライベートサブネット内のインスタンスには、NATゲートウェイが必要です。NATゲートウェイの作成に関する詳細については、「NATゲートウェイ」を参照してください。
Elastic IPアドレス	Elastic IPアドレスは、SSHプロキシおよびNATゲートウェイを実行するインスタンスに割り当てる必要のあるパブリックなスタティックIPアドレスです。Elastic IPアドレスを作成する方法の詳細については、「Elastic IPアドレスの操作」を参照してください。

ネットワークACLの設定

ネットワークアクセス制御リスト(ACL)は、1つまたは複数のサブネットに対するトラフィックを制御するファイアウォールとして機能する、VPC用のセキュリティのオプション層です。詳細については、「ネットワークACL」を参照してください。

このセクションでは、プライベートサブネットにネットワークACLを作成するためのルールについて概説します。プライベートサブネットのネットワークACLに対して、次のルールを設定してください。

- インバウンドルール:

表 5-1

ルール	タイプ	ポート範囲	ソース	アクション	説明
10	SSH	TCP 22	*<SSH Proxy IP Address>*/32	許可	パブリックサブネット内のSSHプロキシのIPアドレスからのインバウンドSSHトラフィックを許可します
15	HTTPS	TCP 8443	*<SSH Proxy IP Address>*/32	許可	パブリックサブネット内のSSHプロキシのIPアドレスからのインバウンドHTTPSトラフィックを許可します
20	カスタムTCPルール	TCP 32768-65535	0.0.0.0/0	許可	サブネットからの要求に対するインターネット上のホストからのインバウンド返信トラフィックを許可します
*	All Traffic	すべて(All)	0.0.0.0/0	拒否	前のルールによってまだ処理されていないすべてのインバウンドIPv4トラフィックを拒否します(変更不可能)

- アウトバウンドルール:

表 5-2

ルール	タイプ	ポート範囲	宛先	アクション	説明
10	カスタム TCPルール	TCP 32768-65535	*<SSH Proxy IP Address>*/32	許可	プライベートサブネットからパブリックサブネット内のSSHプロキシに対するアウトバウンドSSHトラフィックを許可します
12	カスタム TCPルール	TCP 32768-65535	*<SSH Proxy IP Address>*/32	許可	パブリックサブネットからiManagerにアクセスするためのアウトバウンドトラフィックを許可します
15	HTTPS	TCP 443	0.0.0.0/0	許可	プライベートサブネットからインターネットへのアウトバウンドHTTPSトラフィックを許可します
20	HTTP	TCP 80	0.0.0.0/0	許可	プライベートサブネットからインターネットへのアウトバウンドHTTPトラフィックを許可します
25	HTTPS	監査サーバがリスンしているポート番号	*<IP Address of the audit server>*	許可	eDirectoryイベントの監査を許可します。 **注:** このルールは、監査サーバがプライベートサブネットの外部にある場合にのみ適用されます。
*	All Traffic	すべて(All)	0.0.0.0/0	拒否	前のルールによってまだ処理されていないすべてのアウトバウンドIPv4トラフィックを拒否します(変更不可能)

セキュリティグループの設定

セキュリティグループは、VPC内の1つまたは複数のインスタンスに割り当てることができる仮想ファイアウォールルールのセットです。

デフォルトでは、新しいセキュリティグループではポート22の着信トラフィックのみが許可されるので、インスタンスにはSSHを使用してのみ接続できます。

詳細については、「LinuxインスタンスのAmazonEC2セキュリティグループ」を参照してください。

AWSにeDirectoryをデプロイするには、3つのセキュリティグループを作成します。たとえば、Security Group 1、Security Group 2、Security Group 3のようにします。次のポートルールを使用して、これらのセキュリティグループを作成します。

1. **Security Group 1 (eDirectory用):**

ポート	ソース	説明
TCP 22	パブリックサブネット	パブリックサブネットからのSSHトラフィックを許可します
TCP 636	プライベートサブネット	プライベートサブネット内でLDAPSトラフィックを許可します
TCP 524	プライベートサブネット	プライベートサブネット内でeDirectoryのNCPトラフィックを許可します
UDP 427	プライベートサブネット	プライベートサブネット内のSLPトラフィックを許可します

注: eDirectoryに割り当てられているセキュリティグループでは、LDAPポート389を有効にしないでください。HTTPポートは、ツリーCAをホストするeDirectoryサーバに割り当てられているセキュリティグループでのみ有効にする必要があります。

2. **Security Group 2 (eDirectory用):**

ポート	ソース	説明
TCP 8028	VPC	ツリーCAによって発行された証明書を使用して設定されているVPCにサービスが存在する場合に、VPCからeDirectoryツリーのCRLにアクセスするために必要です。このセキュリティグループは、ツリーCAをホストしているeDirectoryサーバに割り当てます。

3. **Security Group 3 (iManager用):**

ポート	ソース	説明
TCP 22	パブリックサブネット	パブリックサブネットからのSSHトラフィックを許可します
TCP 8443	パブリックサブネット	パブリックサブネットからiManagerにアクセスするためのHTTPSトラフィックを許可します

SSHキーペアを作成する

AmazonEC2インスタンスを設定する前に、SSHキーペアを作成する必要があります。キーペアを作成するには、次の手順を実行します。

1 次のコマンドを使用して、クライアント上で4096ビットのRSA SSHキーペアを作成します。

```
ssh-keygen -t rsa -b 4096
```

ssh-keygenにより、新しく作成された公開鍵が~/.ssh/id_rsa.pubに置かれます。

2 ご使用のAmazonEC2アカウントにSSH公開鍵をインポートします。詳細については、「独自の公開鍵をAmazon EC2にインポートする」を参照してください。

重要: SSH秘密鍵を使用してのみ、インスタンスに接続して管理できます。そのため、SSH秘密鍵を紛失しないようにしてください。

インスタンスの作成とデプロイ

サポートされているプラットフォームのいずれかにEC2インスタンスを作成して起動します。インスタンスを作成して起動する方法の詳細については、「EC2リソースを作成しEC2インスタンスを起動する」を参照してください。インスタンスを作成および起動する際には、次の手順も実行する必要があります。

1 最初のeDirectoryサーバを設定するインスタンスにSecurity Group 1を関連付け、その他のすべてのeDirectoryサーバを設定するインスタンスにSecurity Group 2を関連付け、iManagerを設定するインスタンスにSecurity Group 3を関連付けます。セキュリティグループの詳細については、80 ページの 「仮想マシン用のネットワークセキュリティグループの設定」を参照してください。

2 82 ページの 「SSHキーペアを作成する」セクションで作成した公開鍵をインスタンスに関連付けます。

eDirectoryデータの保存用にEBSボリュームを設定する

EC2インスタンスのクラッシュが発生した場合にeDirectoryのデータと設定が失われるのを防ぐには、EBSボリュームを設定する必要があります。eDirectoryのデータと設定を復元する方法の詳細については、88 ページの 「障害復旧」を参照してください。EC2インスタンスを作成した後、次の手順を実行して、eDirectoryデプロイできるようにインスタンスを準備します。

1. EBSボリュームを作成するために、「Amazon EBSボリュームの作成」にある手順を実行します。
2. EC2インスタンスにEBSボリュームを関連付けます。詳細については、「インスタンスへのAmazon EBSボリュームのアタッチ」を参照してください
3. インスタンスにログインし、EBSボリュームをext4ファイルシステムでフォーマットし、EBSボリュームをマウントします。EBSボリュームをフォーマットしてマウントする方法の詳細については、「LinuxでAmazon EBSボリュームを使用できるようにする」を参照してください。
4. ディレクトリをEBSボリュームからeDirectoryデータおよびNICIデータディレクトリにバインドマウントします。ルートユーザとして次の手順を実行して、バインドマウントします。

   4a 次のコマンドを使用して、eDirectoryデータディレクトリを作成します。

   ```
   mkdir <mount_point>/eDirectory_data
   ```

   4b 次のコマンドを使用して、NICIデータディレクトリを作成します。

   ```
   mkdir <mount_point>/nici_data
   ```

   4c 次のコマンドを使用して、NICIおよびeDirectoryの環境設定ディレクトリを作成します。

   ```
   mkdir <mount_point>/eDirectory_nici_conf
   ```

   4d 次のコマンドを使用して、eDirectoryに必要なディレクトリを作成します。

   ```
   mkdir –-parents /var/opt/novell/eDirectory
   mkdir –-parents /var/opt/novell/nici
   mkdir –-parents /etc/opt/novell/eDirectory
   ```

   4e ディレクトリをバインドマウントするために、次の内容を/etc/fstabに追加します。

   ```
   <mount_point>/eDirectory_data /var/opt/novell/eDirectory none
   defaults,bind 0 0

   <mount_point>/nici_data /var/opt/novell/nici none defaults,bind 0 0

   <mount_point>/eDirectory_nici_conf /etc/opt/novell/eDirectory none
   defaults,bind 0 0
   ```

注: インスタンス内でのすべての操作は、ルートユーザとして実行する必要があります。

eDirectoryとiManagerのインストール

前提条件

- ❒ 「システム要件」に記載されている要件を満たしていることを確認します。
- ❒ 80 ページの 「仮想マシン用のネットワークセキュリティグループの設定」で説明されているように、セキュリティグループを作成します。

- ❒ SSHプロキシインスタンスは、強化され、セキュリティ保護されたサーバである必要があります。このインスタンスについてはSSHポート22のみを開き、適切なパフォーマンスとメモリを持つAWSインスタンスタイプを選択します。プライベートサブネット内のインスタンスとSSHプロキシが実行されているインスタンスへのアクセスに必要なSSH秘密鍵は、VPC内には保存しないようにしてください。クライアント上にのみ保存してください。SSHプロキシサーバにはElastic IPアドレスを関連付けて、スタティックなIPアドレスを設定します。
- ❒ SSHプロキシインスタンス内にVNCサーバを設定します。VNCサーバは、強力なパスワードを使用して強化する必要があります。セキュリティ保護された通信のみを可能にするために、SSHトンネルを使用してVNCサーバに接続します。VNCサーバは、localhostからの接続についてのみリスンするように設定する必要があります。セッションのロックアウトを防止するために、画面ロックを無効にします。VNCサーバを使用した後、セッションを終了する必要があります。
- ❒ eDirectory/iManagerを設定するプライベートサブネット内のインスタンスには、SSHプロキシを使用して接続します。

  ```
  ssh -i edir_key.pem -A -J ec2-user@<ssh_proxy_ip> ec2-
  user@<instance_private_ip>
  ```

  注

  - 上記のサンプルコマンドで、edir_key.pemは、サーバキーを含むサンプルファイル名です。
  - SSH-Addコマンドを使用してエージェント内に識別情報ファイルを追加すれば、ログインするたびに識別情報ファイルを使用しないで済みます。

  インスタンスのプライベートIPアドレスを表示するには、［**インスタンス**］>［*インスタンス*］>［**説明**］をクリックします。
- ❒ バックエンドサブネット内のVMにSLPディレクトリエージェント(DA)サーバを設定します。SLP DAがデプロイされているVMに対して、NSGのインバウンドルールでポート427を開きます。slp.confファイルを編集して、DA操作を有効にします。詳細については、『*NetIQ eDirectory管理ガイド*』の「OpenSLP for eDirectoryの設定」を参照してください。

インストールと環境設定の手順

このセクションでは、AWS EC2環境にeDirectoryとiManagerをインストールして設定する手順について説明します。eDirectoryをインストールした後、次の条件を満たしていることを確認する必要があります。

- EBAが有効になっている
- SNMPが無効になっている
- eDirectoryがポート389でリスンしていない
- LDAPおよびHTTPサービスは、ECDSA証明書のみを使用するように設定されている
- 使用されていない場合は、AWS EC2プライベートインスタンスのSSHポートへのアクセスを無効にする必要があります。
- iMonitor、eMBox、およびDHostモジュールを無効にして、セキュリティを強化する。これらのモジュールを無効にした後、これらのモジュールに関係するすべてのアクティビティは、NDSユーティリティのみを使用して実行する必要があります。

eDirectoryのインストールと設定

1. eDirectoryを設定するプライベートサブネット内のインスタンスに、セキュアコピー(scp)を使用してeDirectory_<*version*>_Linux_x86_64.tar.gzファイルをコピーします(SSHプロキシを使用します)。

   ```
   scp -i <keyname> -o ProxyJump=ec2-user@<ssh_proxy_ip>
   eDirectory_<version>_Linux_x86_64.tar.gz ec2-user@<instance_ip>:/<directory>
   ```

2. eDirectoryをインストールします。詳細については、「nds-installユーティリティを使用してeDirectoryコンポーネントをインストールする」を参照してください。
3. eDirectoryを設定します。詳細については、「ndsconfigユーティリティを使用してeDirectoryレプリカサーバを追加または削除する」を参照してください。たとえば、eDirectoryをインストールして設定するためのコマンドのサンプルを次に示します。

   ```
   ndsconfig  new [-t <tree_name>] [-n <server context>] -a <admin FDN> [-w <admin
   password>] -P ldaps://<instance_ip> --configure-eba-now yes
   ```

4. openslp-serverをインストールして、SLPDサービスを始動します。

iManagerのインストールと設定

iManager管理コンソールを使用すると、AWS環境上でeDirectoryの操作を管理できます。iManagerは、eDirectoryをインストールした後で、AWSインスタンスにインストールする必要があります。

1. iManagerを設定するプライベートサブネット内のインスタンスに、セキュアコピー(scp)を使用してiMan_<*version*>_linux_x86_64.tgzファイルをコピーします(SSHプロキシを使用します)。

   ```
   scp -i <keyname> -o ProxyJump=ec2-user@<ssh_proxy_ip>
   iMan_<version>_linux_x86_64.tgz ec2-user@<instance_ip>:/<directory>
   ```

2. iManagerをインストールして設定します。詳細については、「LinuxでのiManagerサーバのインストール」を参照してください。iManagerをインストールする前に、『*iManagerインストールガイド*』の「システム要件」セクションに記載されているシステム要件を参照してください。
3. iManagerが実行されているインスタンスに、EBACA証明書をダウンロードします。詳細については『*NetIQ eDirectory管理ガイド*』の「iManagerを使用したEBA CAの管理」を参照してください。
4. iManagerを実行しているVMの自己署名証明書を、セキュアCA署名証明書で置き換えます。詳細については、「iManager用の一時的な自己署名証明書の置き換え」を参照してください。

注: iManagerサーバは、ECDSA証明書のみを使用するように設定してください。iManagerをインストールした後、権限を持ったユーザと、このユーザが管理する適切なeDirectoryツリー名を指定します。

---

iManagerの起動

次の手順を実行して、iManagerを起動します。

1 SSHトンネルを使用して、SSHプロキシのlocalhost上で実行されているVNCサーバに接続します。
2 同じインスタンスにブラウザをインストールして起動します。
3 iManagerを起動し、IPアドレスまたはツリー名を使用してeDirectoryツリーに接続します。

設定後のタスク

1 EBAが有効になっているかどうかを確認するため、『*NetIQ eDirectory管理ガイド*』「EBAに関する情報の表示」を参照してください。
2 証明書サーバでSuite Bを有効にします。詳細については、『*NetIQ eDirectory管理ガイド*』の「証明書サーバでのSuite Bの有効化」を参照してください。
3 1番目のeDirectoryサーバに対してAES 256ビットツリーキーを設定します。詳細については、『*NICI Administration Guide (NICI管理ガイド)*』の「Creating an AES 256-Bit Tree Key (AES 256ビットツリーキーを作成する)」を参照してください。
4 1番目のeDirectoryサーバにあるCRL配布ポイントを削除します。ポート389でのセキュリティ保護されていないLDAPアクセスはすべてのeDirectoryサーバで無効化されているため、ツリーCAのCRLはHTTPのみでダウンロードできるようにする必要があります。次の手順を実行して、CRL配布ポイントを削除します。
   4a 管理者としてiManagerにログインします。
   4b ［**役割およびタスク**］>［**NetIQ証明書サーバ**］>［**認証局の環境設定**］に移動します。
   4c ［**CRL**］をクリックします。
   4d ［**One**］をクリックします。HTTP CRL配布ポイント(http://<instance_ip>:8028/crl/one.crl)以外のすべての［**CRL配布ポイント**］を選択して削除します。
   4e ［**適用**］をクリックし、［**閉じる**］をクリックします。
   4f ［**OneEC**］をクリックします。HTTP CRL配布ポイント(http://<instance_ip>:8028/crl/oneec.crl)以外のすべての［**CRL配布ポイント**］を選択して削除します。
   4g ［**適用**］をクリックし、［**OK**］をクリックします。
5 iManager証明書サーバプラグインを使用して、サーバのデフォルト証明書を修復します。デフォルト証明書を修復するには、次の手順を実行します。
   5a 管理者としてiManagerにログインします。
   5b ［**役割およびタスク**］>［**NetIQ証明書サーバ**］>［**デフォルト証明書の修復**］に移動します。
   5c 証明書を所有するサーバを選択して、［**次へ**］をクリックします。
   5d ［**デフォルト証明書はすべて上書きされます**］を選択し、［**次へ**］をクリックします。
   5e 実行するタスクを確認し、［**完了**］を選択します。
6 ECDSA証明書とSuiteB暗号化を使用するようにLDAPサービスとHTTPサービスを設定します。詳細については『*NetIQ eDirectory管理ガイド*』の「ECDSA証明書とSuite B Cipherを使用するためのLDAPサービスとHTTPサービスの設定」を参照してください。完了したら、eDirectory を再起動します。
7 SNMPサブエージェントがアンロードされているかどうかを確認する方法について、『*NetIQ eDirectory管理ガイド*』の「SNMPサーバモジュールのロードとアンロード」を参照します。

8 eDirectoryがポート389でリスンしていないことを確認します。

9 iMonitor、eMBox、DHost、およびHTTPスタックを無効にします。

9a 次の手順を実行して、ツリーCAをホストしているeDirectoryサーバのiMonitor、eMBox、およびDHostを無効にします。

9a1 ndsmodules.confファイルを編集して、hconserv、imon、およびemboxをコメント化します。

9a2 eDirectoryを再起動します。

9b 次の手順を実行して、eDirectoryレプリカサーバのHTTPスタックを無効にします。

9b1 ndsmodules.confファイルを編集して、httpstk、hconserv、imon、およびemboxをコメント化します。

9b2 eDirectoryを再起動します。

注: httpstkは、コメント化の前に、ndsmodules.confファイル内でndsより上に配置されている必要があります。これにより、ndsモジュールはHTTPスタックを有効にしなくなります。

---

10 アドバタイジング方式としてユニキャストを使用することをeDirectoryに強制するように、SLPを設定します。バックエンドサブネット内のDAサーバのIPアドレスを提供するように、slp.confファイルを編集します。詳細については、『*NetIQ eDirectory管理ガイド*』の「環境設定パラメータ」を参照してください。

注: すべてのeDirectoryインスタンスとiManagerの設定が完了したら、SSHポートへのアクセスを拒否し、必要な場合にのみ許可するように、AWSプライベートサブネットのネットワークACLを設定してください。

監査サービスのデプロイ

AWS EC2にCommon Event Format (CEF)監査サービスをデプロイして、さまざまなeDirectoryイベントを監査することができます。CEF監査サービスをデプロイするには、次の手順を実行します。

1 VPCに監査サーバをインストールします。

2 ポート上でリスンするように監査サーバを設定します

注: 監査サーバとしてはSentinelを使用することをお勧めします。

---

3 次の設定を使用して新しいセキュリティグループを作成し、監査サーバが実行されているインスタンスに関連付けます。

ポート	ソース	説明
TCP (監査サーバポート)	プライベートサブネット	eDirectoryサーバからのイベントの受信を許可します

4 すべてのeDirectoryインスタンスで、次のように/etc/opt/novell/eDirectory/conf/auditlogconfig.propertiesファイルを更新します。

```
log4j.appender.S.Host=<Auditing server ip>
log4j.appender.S.Port=<auditing server port>
```

5 iManagerから、対応するCEFイベントを有効にします。詳細については、「監査するCEFイベントの設定」を参照してください。有効にされたイベントは、監査サーバに転送されます。

障害復旧

障害復旧は、eDirectoryが実行されているインスタンスでクラッシュが発生した場合に実行します。障害復旧を行うには、次の手順を実行します。

1 クラッシュしたインスタンスを停止し、EBSボリュームとの関連付けを解除します。詳細については、「インスタンスからのAmazon EBSボリュームのデタッチ」を参照してください。

2 クラッシュしたインスタンスと同じオペレーティングシステムを使用して、新しいEC2インスタンスを設定します。

3 新しいEC2インスタンスに同じバージョンのeDirectoryをインストールします。

4 新しいインスタンスにEBSボリュームをアタッチし、ファイルシステムをマウントします。詳細については、「インスタンスへのAmazorEBSボリュームのアタッチ」を参照してください。

5 ディレクトリをバインドマウントします。

ディレクトリをバインドマウントするには、/etc/fstabを次のように更新します。

```
<mount_point>/eDirectory_data /var/opt/novell/eDirectory none defaults,bind 0
0

<mount_point>/nici_data /var/opt/novell/nici none defaults,bind 0 0

<mount_point>/eDirectory_nici_conf /etc/opt/novell/eDirectory none
defaults,bind 0 0
```

6 /etc/opt/novell/eDirectory/conf/nds.conf内のIPアドレスを、現在のインスタンスのIPアドレスに変更します。

7 eDirectoryをアップグレードしてヘルスチェックをスキップします。詳細については、『NetIQ eDirectoryインストールガイド』の「*eDirectoryをアップグレードする*」を参照してください。

8 ndsrepairユーティリティを使用して、ネットワークアドレスを修復します。詳細については、『NetIQ eDirectory管理ガイド』の「*DSRepairオプション*」を参照してください。

9 ツリーCAのIPアドレスが変更された場合は、CRL配布ポイントのIPアドレスを変更します。IPアドレスの変更方法の詳細については、『NetIQ eDirectory管理ガイド』の「CRL環境設定オブジェクトのプロパティの表示と変更」を参照してください。

10 iManager証明書サーバプラグインを使用して、サーバのデフォルト証明書を修復します。デフォルト証明書を修復するには、次の手順を実行します。

10a 管理者としてiManagerにログインします。

10b ［**役割およびタスク**］>［**NetIQ証明書サーバ**］>［**デフォルト証明書の修復**］に移動します。

10c 証明書を所有するサーバを選択して、［**次へ**］をクリックします。

10d ［**デフォルト証明書はすべて上書きされます**］を選択し、［**次へ**］をクリックします。

10e 実行するタスクを確認し、［**完了**］を選択します。

11 新しいECDSA証明書を使用するようにLDAPおよびHTTPサービスを設定します。

6 Dockerコンテナを使用したeDirectoryのデプロイ

この章では、Dockerコンテナを使用してeDirectoryをデプロイする方法について説明します。

Dockerの利点

Dockerは、最も一般的なアプリケーションのコンテナ化技術です。これは、コンテナを使用してアプリケーションを簡単に作成、デプロイ、および実行できるように設計されたプラットフォームです。コンテナにより、アプリケーションは独自のオペレーティングシステムと、その他のすべての依存関係(ライブラリやパッケージ)と一緒にカプセル化されます。Dockerコンテナを使用したeDirectoryのデプロイには、次のような利点があります。

- **移植性の高さ:** コンテナで実行されているアプリケーションは、Dockerでサポートされている任意のオペレーティングシステムおよびハードウェアプラットフォームに容易にデプロイできます。
- **デプロイが簡単。** コンテナを使用すると、オーケストレーションツールにより、アプリケーションをより迅速にデプロイ、アップグレード、さらにはスケールすることができます。
- **一貫性:** どこにコンテナをデプロイするかに関係なく、eDirectoryの機能に影響を与えません。

Dockerとそのコンポーネントの詳細については、「Docker Overview」を参照してください。

Dockerコンテナを使用してeDirectoryをデプロイするための計画

このセクションでは、eDirectory Dockerコンテナをデプロイするためのシステム要件と前提条件について説明します。

システム要件

プラットフォームの要件

❒ eDirectory Dockerコンテナのデプロイには、Docker Community Editionバージョン18.06以上があれば十分です。

- ❒ 推奨されるDockerストレージドライバはoverlay2です。BTRFSは、Dockerをインストールできるホストでサポートされているファイルシステムではありません。
- ❒ Linuxカーネルバージョン3.10以降。

ハードウェア要件

- ❒ Dockerホストマシンには、最低でも4GBのRAMと30GBのハードディスク容量をプロビジョニングする必要があります。

注: メモリ、CPU、およびハードディスクの要件は、デプロイメントのタイプとデプロイするコンテナの数によって異なります。将来のスケールアップの可能性に備えるため、常に、現在の要件よりも多いリソースをプロビジョニングするようにしてください。

前提条件

- ❒ Dockerホストマシンにはスタティックアドレスが設定されている必要があります。
- ❒ Dockerがインストールされている必要があります。サポートされているプラットフォームの詳細については、Dockerのマニュアルを参照してください。
- ❒ Dockerデーモンが稼動している必要があります。
- ❒ eDirectory DockerイメージのtarballをNetIQダウンロードWebサイトからダウンロードする必要があります。
- ❒ Dockerでコンテナ管理を実行する必要があるユーザは、dockerグループに追加する必要があります。

Docker CLI

Docker CLIで使用されるさまざまなコマンドの説明は、こちらを参照してください。

eDirectoryコンテナのデプロイ

eDirectory DockerイメージのOSベースイメージはopenSUSE Leap 15.1です。eDirectoryイメージのtarファイルをDockerホストマシンにダウンロードする必要があります。tarballをダウンロードした後、次のコマンドを使用して、そのイメージをDockerのローカルレジストリにロードする必要があります。

```
# tar xf eDirectory_920.tar.gz
# docker load --input edir920.tar
```

eDirectory Dockerコンテナは、Docker Runコマンドでndsconfigユーティリティのすべてのパラメータを受け入れます。ndsconfigユーティリティの詳細については、39 ページの 「ndsconfigユーティリティを使用してeDirectoryレプリカサーバを追加または削除する」を参照してください。

注: Docker Runコマンドでndsconfigユーティリティの-wオプションを使用してパスワードを設定することはお勧めできません。このオプションを使用して設定したパスワードは、Docker inspectコマンドを使用してプレーンテキストで表示できます。管理者の資格情報を設定するには、管理者のFDNと管理者パスワードをプロンプトで指定する方法がより安全です。

---

eDirectory Dockerコンテナでは、次のndsconfigパラメータに対してデフォルト値が使用されます。したがって、Docker runコマンドではこれらのパラメータを設定しないでください。

- **設定ファイル:** /config/eDirectory/inst/conf/nds.conf
- **インスタンスの場所:** /config/eDirectory/inst/data/data
- **DIB保存先:** /config/eDirectory/inst/data/data/dib

注: インスタンスデータと環境設定をコンテナの/configフォルダに含めることが大切です。これは、eDirectoryコンテナの永続的な保存とアップグレードの機能を有効にするためです。詳細については、113 ページの 「eDirectoryデータストレージの管理」を参照してください。

---

eDirectoryコンテナのデフォルトのログファイルの場所は、/config/eDirectory/inst/data/logです。

eDirectoryをデプロイする前に、次の推奨事項を考慮する必要があります。

- Dockerコンテナには、デフォルトではリソースの制約がありません。そのため、すべてのコンテナには、ホストのカーネルによって提供されるすべてのCPUリソースおよびメモリリソースへのアクセスが提供されます。コンテナで使用できるリソースの量に制限を設定することにより、実行中の1つのコンテナによってより多くのリソースが消費され、実行中の他のコンテナがリソース不足になることがないようにする必要があります。
  - Docker runコマンドの--memoryフラグを使用して、Dockerコンテナで、コンテナによって使用されるメモリに対してハード制限が適用されるようにする必要があります。
  - Docker runコマンドの--cpuset-cpusフラグを使用して、Dockerコンテナで、実行中のコンテナによって使用されるCPUの容量に制限が適用されるようにする必要があります。
  - --pids-limitには300を設定して、任意の時点でコンテナ内で生成されるカーネルスレッドの数を制限する必要があります。これは、DoS攻撃を防ぐためです。
- Docker runコマンドの--restartフラグを使用して、障害発生時のコンテナ再起動ポリシーを5に設定する必要があります。
- eDirectoryコンテナは、必ず、コンテナの起動後にヘルスステータスが［**正常**］と表示されてから使用する必要があります。コンテナのヘルスステータスを確認するには、次のコマンドを実行します。

  ```
  docker ps <container_name/ID>
  ```

- 通常、DockerコンテナではLinux機能のデフォルトリストが有効になっています。eDirectoryコンテナで次の機能のみが有効になっていることを確認し、その他の機能をドロップする必要があります。
  - AUDIT_WRITE
  - CHOWN
  - DAC_OVERRIDE
  - SETGID
  - SETUID
  - NET_BIND_SERVICE
  - SYS_CHROOT (SLPサービスを有効にしている場合のみ)
  - SYS_PTRACE (Linux ptraceを活用するユーティリティを使用する場合のみ。gdbなど)

機能の追加とドロップの詳細については、「Runtime privilege and Linux capabilities」を参照してください。

- eDirectoryコンテナは、常にroot以外のユーザ(nds)として起動されます。追加のセキュリティ対策として、デーモンでのユーザ名前空間の再マッピングを有効にして、コンテナ内からの特権昇格攻撃を防止します。ユーザ名前空間の再マッピングの詳細については、「ユーザ名前空間でコンテナを分離する」を参照してください。

注: 以前のバージョンのスタンドアロンeDirectoryを使用している場合は、eDirectory 9.2 Dockerコンテナを使用して、セットアップをDocker環境に移行することはできません。

---

eDirectory Dockerコンテナでは、マルチホストのDocker環境にデプロイするためのホストおよびオーバーレイネットワークドライバがサポートされています。

- 108 ページの 「ホストネットワークでのeDirectoryコンテナのデプロイ」
- 109 ページの 「ユーザ定義のオーバーレイネットワークでのeDirectoryコンテナのデプロイ」

ホストネットワークでのeDirectoryコンテナのデプロイ

eDirectoryコンテナは、Linux上でのみホストネットワークドライバを使用してハイブリッド環境にデプロイできます。Dockerネットワークの詳細については、「ConfigureNetworking」を参照してください。

注: ホストネットワークはWindowsではサポートされていません。

ハイブリッド環境は、同じツリーにeDirectoryサーバのレガシデプロイメントおよびコンテナベースのデプロイメントの両方を組み合わせたものです。ハイブリッドネットワークを使用すると、レガシeDirectoryデプロイメントをすでにホストしている既存の運用環境に、eDirectory Dockerコンテナをシームレスに導入できます。Dockerホストネットワーキングでは、ホストのネットワークスタックがレガシeDirectoryデプロイメントとコンテナ化されたeDirectoryデプロイメントの両方によって共有されているため、サービスポートを再使用することはできません。また、コンテナ化されたeDirectoryサーバは、クライアントとツリー内の他のサーバに対して、レガシeDirectoryサーバとして表示されます。

次の例は、eDirectoryコンテナを使用して新しいツリーを作成する方法を示しています。

```
docker run -it --name eDir-container-1 --restart on-failure:5 --memory="700M" --
cpuset-cpus="1" --pids-limit="300" --volume eDir-volume1:/config --network=host
edirectory:9.2.0 new -t docker-tree1 -n novell -S m1 -B 164.99.1.1@1524 -o 1028 -O
1030 -L 1389 -l 1636 --configure-eba-now yes
```

次の例は、eDirectoryコンテナレプリカサーバを既存のツリーに追加する方法を示しています。

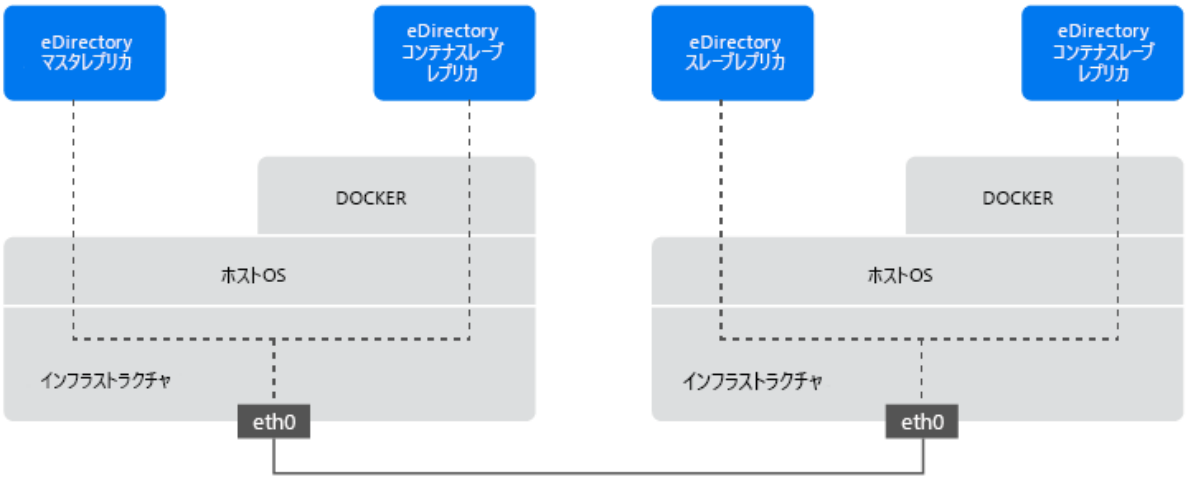
```
docker run -it --name eDir-container-2 --restart on-failure:5 --memory="700M" --
cpuset-cpus="1" --pids-limit="300" --volume eDir-volume2:/config --network=host
edirectory:9.2.0 add -t docker-tree1 -n novell -S m2 -B 164.99.10.10@2524 -o 2028 -
O 2030 -L 2389 -l 2636 --configure-eba-now yes -p 164.99.1.1@1524
```

注

- --networkフラグは、ホストネットワーキングドライバを使用してコンテナをデプロイするために使用します。

- 同じDockerホスト上で実行されているeDirectoryコンテナ間で、サービスのポート番号を繰り返すことはできません。
- 上記のコマンドで使用するIPアドレスは、コンテナが実行されることを想定しているDockerホストマシンのものです。

図6-1 ホストネットワークでのeDirectoryコンテナのデプロイ



ユーザ定義のオーバーレイネットワークでのeDirectoryコンテナのデプロイ

ユーザ定義のオーバーレイネットワークを使用して、複数のDockerデーモンホスト上で実行される、eDirectoryコンテナの分散ネットワークを作成できます。ユーザ定義のオーバーレイネットワーク内のeDirectoryコンテナは、LinuxとWindowsの両方にデプロイできます。DockerホストをSwarmに参加させ、それらのホスト上で実行されているeDirectoryコンテナがシームレスに通信できるようにするには、DockerSwarmサービスを使用する必要があります。Dockerオーバレイネットワークドライバの詳細については「Use Overlay Networks」を参照してください。

注: Docker Swarmのスケーリングとスケジューリングの機能は、eDirectoryコンテナでは認定されていません。Swarmサービスによるホスト間でのeDirectoryコンテナのマイグレーションもサポートされていません。

前提条件

- ❒ 少なくとも1つのDockerホストをmanagerとして設定し、他のホストをworkerとして設定してDocker Swarmを作成する必要があります。
- ❒ myOverlayという名前のアタッチ可能なオーバーレイネットワークを作成します。
- ❒ DockerSwarm内でクラスタ管理と通信を行うため、Dockerホスト間のファイアウォールで次のポートを開きます。
  - TCPポート2377

- TCPおよびUDPポート7946
- UDPポート4789

❒ オーバーレイネットワークにデプロイされたコンテナには、myOverlayサブネットに属するスタティック内部IPアドレスを割り当てる必要があります。

Swarmをデプロイし、ユーザ定義のオーバーレイネットワークを作成する方法については、「Networking with overlay networks」を参照してください。

ユーザ定義のオーバーレイネットワークにeDirectoryコンテナをデプロイする前に、次の推奨事項を考慮する必要があります。

- eDirectoryコンテナのマスタレプリカサーバとそのR/Wレプリカを同じオーバレイネットワーク内にデプロイする必要があります。オーバーレイネットワークの外部で実行されている他のスタンドアロンのeDirectoryサーバまたはコンテナとの通信はサポートされません。
- iManager Dockerコンテナは、eDirectory管理用の同じユーザ定義のオーバーレイネットワークにデプロイすることをお勧めします。iManager Dockerコンテナのデプロイ方法の詳細については、「Deploying iManager Using Docker Container」を参照してください。
- 次のコマンドを実行すると、ユーザ定義のオーバーレイネットワークのネットワークに関する詳細を確認できます。

  ```
  docker inspect myOverlay
  ```

次のコマンドは、eDirectoryコンテナを使用して新しいツリーを作成する方法を示しています。

```
docker run -it --name eDir-container-1 --restart on-failure:5 --memory="700M" --
cpuset-cpus="1" --pids-limit="300" --volume eDir-volume1:/config --
network=myOverlay --ip=10.0.0.5 edirectory:9.2.0 new -t docker-tree1 -n novell -S
m1 –b 524 -o 8028 -O 8030 -L 389 -l 636 --configure-eba-now yes
```

次のコマンドは、上で作成したeDirectoryコンテナのIPアドレスを取得する方法を示しています。

```
docker inspect eDir-container-1 --format
{{.NetworkSettings.Networks.myOverlay.IPAddress}}
```

表示されたIPアドレスは、eDirectoryコンテナのレプリカサーバをツリーに追加するときに、remote_IP_Addressとして使用できます。

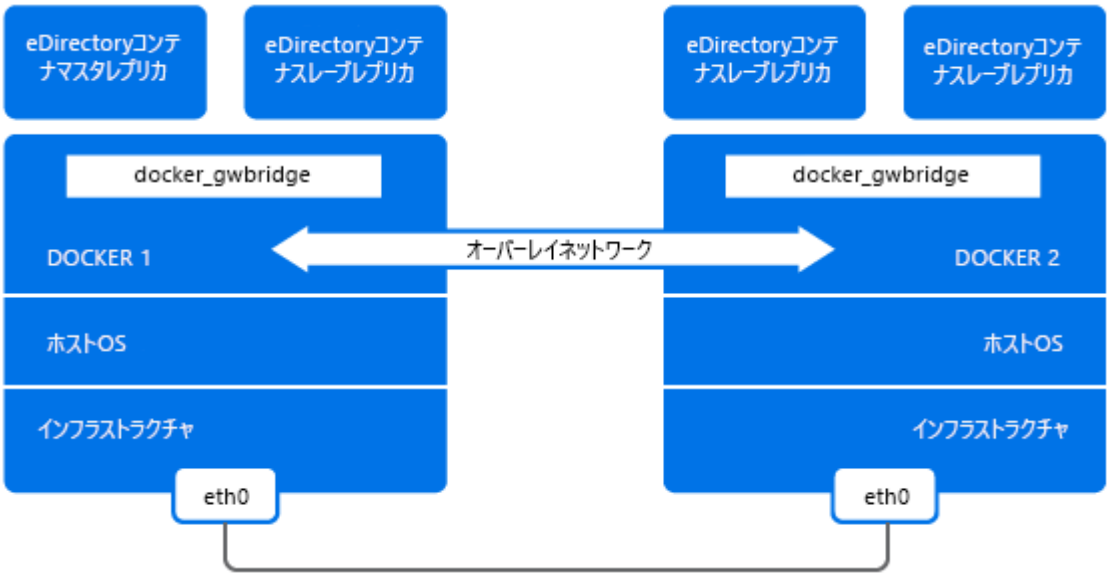
次のコマンドは、eDirectoryコンテナレプリカサーバを既存のツリーに追加する方法を示しています。

```
docker run -it --name eDir-container-2 --restart on-failure:5 --memory="700M" --
cpuset-cpus="1" --pids-limit="300" --volume eDir-volume2:/config --
network=myOverlay --ip=10.0.0.6 edirectory:9.2.0 add -t docker-tree1 -n novell -S
m2 –b 524 -o 8028 -O 8030 -L 389 -l 636 --configure-eba-now yes -p
<remote_IP_Address>
```

注

- --networkフラグは、オーバーレイネットワークドライバを使用してmyOverlayというユーザ定義のオーバーレイネットワーク内にコンテナをデプロイするために使用されます。
- 上の例では、--ipフラグを使用して、myOverlayサブネットに属するコンテナにスタティック内部IPアドレスを割り当てます。

図 6-2 ユーザ定義のオーバーレイネットワークでのeDirectoryコンテナのデプロイ



デプロイメント後のタスク

次のタスクを、eDirectoryコンテナのデプロイ後に実行する必要があります。

- 111 ページの 「実行中のeDirectoryコンテナでのコマンドの実行」
- 112 ページの 「OpenSLP for eDirectory Dockerコンテナの設定」
- 112 ページの 「eDirectory Dockerコンテナ内のNMASメソッドのインストール」

実行中のeDirectoryコンテナでのコマンドの実行

Dockerホストマシンで次のコマンドを実行すると、eDirectory Dockerコンテナでbashシェルを使用できます。

```
bash# docker exec -it eDir-container-1 /bin/bash
```

上記のコマンドでは、eDirectoryバイナリパスを/opt/novell/eDirectory/binに設定します。

NDSユーティリティコマンドは、コンテナプロンプトで実行できます。以下に例を示します。

```
nds@abbae7c93b1c:~> ndsstat

[1] Instance at /config/eDirectory/inst/conf/nds.conf:  m1.O=novell.DOCKER-TREE1
Tree Name: DOCKER-TREE1
Server Name: .CN=m1.O=novell.T=DOCKER-TREE1.
Binary Version: 40201.14
Root Most Entry Depth: 0
Product Version: eDirectory for Linux x86_64 v9.2 [DS]
```

上記のコマンドはホストマシンから直接実行できます。以下に例を示します。

```
bash# docker exec -it eDir-container-1 /opt/novell/eDirectory/bin/ndsstat
```

```
[1] Instance at /config/eDirectory/inst/conf/nds.conf:  m1.O=novell.DOCKER-TREE1
Tree Name: DOCKER-TREE1
Server Name: .CN=m1.O=novell.T=DOCKER-TREE1.
Binary Version: 40201.14
Root Most Entry Depth: 0
Product Version: eDirectory for Linux x86_64 v9.2 [DS]
```

OpenSLP for eDirectory Dockerコンテナの設定

実行中のeDirectoryコンテナでSLPサーバを起動するには、次の手順を実行します。

1 次のコマンドを実行して、slpdを起動します。

```
docker exec --user root eDir-container-1 /usr/sbin/slpd
```

2 次のコマンドを実行して、eDirectoryを再起動します。

```
docker exec eDir-container-1 /opt/novell/eDirectory/bin/ndsmanage stopall
```

```
docker exec eDir-container-1 /opt/novell/eDirectory/bin/ndsmanage startall
```

注

- コンテナを停止して再起動すると、SLPデーモンが停止します。手動で再起動する必要があります。/var/run/slpd.pidに古いPIDファイルが存在する場合は、そのPIDファイルを削除してからデーモンを起動する必要があります。
- 古いPIDファイルは、停止したプロセスまたは強制終了されたプロセス(この例では、SLPデーモンプロセス)のPIDを持つファイルです。
- オーバーレイ環境では、SLP DAを同じオーバレイネットワーク内で実行する必要があります。

eDirectory Dockerコンテナ内のNMASメソッドのインストール

eDirectoryコンテナにNMASメソッドをインストールするには、次のタスクを実行します。

注: NMASメソッドは、デフォルトでは/home/nds/eDirectory/nmasで使用できます。

1 次のコマンドを実行して、eDirectoryコンテナにログインします。

```
docker exec -it eDir-container-1 bash
```

2 NMASメソッドを追加します。

```
cd /home/nds/eDirectory/nmas/NmasMethods/Novell/<method-name>
```

```
nmasinst -addmethod admin.novell docker-tree1 ./config.txt
```

注: NMASメソッドを追加する方法の詳細については、『*NetIQ eDirectory 管理ガイド*』の「nmasinstユーティリティを使用したログインメソッドのインストール」を参照してください。

3 コンテナコンソールを終了します。

```
exit
```

4 eDirectoryコンテナを再起動します

```
docker restart eDir-container-1
```

eDirectoryデータストレージの管理

eDirectoryのデータと環境設定を永続的に保存するには、Docker Volumeを使用することをお勧めします。永続的に保存することの詳細については「Manage data in Docker」参照してください。

永続的に保存する必要のあるeDirectoryアプリケーションデータは、起動時にコンテナ内の/configディレクトリの下に配置されます。Dockerホストファイルシステム上のデータをコンテナの外部に永続的に保存するには、Dockerボリュームをeコンテナ内の/configパスにマウントする必要があります。管理目的でコンテナが停止または削除されても、ボリューム内のアプリケーションデータは保持されます。

この方法は、eDirectoryコンテナのアップグレード時に古い設定とデータを保持する場合に便利です。eDirectoryコンテナのアップグレードの詳細については、113 ページの 「Dockerコンテナを使用したeDirectoryのアップグレード」を参照してください。

次の例は、eDir-volume-1という名前のDockerボリュームを作成する方法を示しています。

```
docker volume create eDir-volume-1
```

次の例は、保存する目的でボリュームをマウントしてeDirectoryコンテナを起動する方法を示しています。

```
docker run -it --name eDir1-Host --restart on-failure:5 --memory="700M" --cpuset-cpus="1" --pids-limit="300" --volume eDir-volume1:/config --network=host edir920:latest new -t docker-tree1 -n novell -S m1 -B 164.99.179.213@1524 -o 1028 -O 1030 -L 1389 -l 1636 --configure-eba-now yes
```

上記のコマンドでは、eDir-volume1というDockerボリュームが作成され、eDirectoryコンテナ内の場所/configにマウントされます。

Dockerコンテナを使用したeDirectoryのアップグレード

eDirectoryイメージの新しいバージョンが使用可能になった場合、管理者は、最新バージョンのeDirectoryをコンテナにデプロイするためのアップグレード手順を実行できます。アップグレードを実行する前に、すべての必要なアプリケーション関連データをDockerボリュームに永続的に保存するようにしてください。Dockerコンテナを使用してeDirectoryをアップグレードするには、次の手順を実行します。

1 実行中のeDirectoryコンテナを停止して削除します。実行中のコンテナは、新しいイメージを使用できないため、アップグレードを実行する前に停止して削除する必要があります。

2 新しいeDirectory Dockerイメージと、Docker Volumeに保存されている古いコンテナのアプリケーションデータを使用して、新しいコンテナを起動します。

次の例は、保存する目的でボリュームをマウントしてeDirectoryコンテナを起動する方法を示しています。

```
docker run -it --name eDir1-Host --restart on-failure:5 --memory="700M" --
cpuset-cpus="1" --pids-limit="300" --volume eDir-volume1:/config --
network=host <eDirectory_image> new -t docker-tree1 -n novell -S m1 -B
<Host_IP_Address>@1524 -o 1028 -O 1030 -L 1389 -l 1636 --configure-eba-now yes
```

次の例は、手順2で作成したeDirectoryコンテナをアップグレードする方法を示しています。

```
docker run -it --name eDir1-Host --restart on-failure:5 --memory="700M" --
cpuset-cpus="1" --pids-limit="300" --volume eDir-volume1:/config --
network=host <Latest_eDirectory_image> upgrade
```

eDir-volume1は、古いeDirectoryコンテナのアプリケーションデータを保持している同じボリュームです。

注

- eDirectoryコンテナをアップグレードするには、その前に、古いバージョンのイメージが実行されているコンテナを削除する必要があります。
- ndsconfigコマンドの-aオプションと-wオプションを使用しないでください。コンテナのアップグレード時には、画面上のプロンプトを使用して管理者の資格情報を入力してください。

eDirectory Dockerコンテナの復旧

不明な理由が原因で、実行中のeDirectoryコンテナにアクセスできなくなったり、コンテナが削除されたり、使用不能になったりした場合は、コンテナ復旧を実行する必要があります。このような場合には、影響を受けたコンテナを停止して削除する必要があります。新しいコンテナは、影響を受けたコンテナと同じeDirectoryイメージとDockerボリュームを使用して開始する必要があります。eDirectoryコンテナを復旧するには、次の手順を実行します。

1. 影響を受けたコンテナを停止して削除します。
2. ホストマシンのパス/var/lib/docker/volumes/eDir-volume1/_data/eDirectory/inst/confにあるnds.versionファイル内のエポックタイムスタンプを編集して、より小さい値を指定します。
3. 影響を受けたコンテナと同じeDirectoryイメージとのボリュームを使用して、新しいコンテナを起動します。次の例は、影響を受けたコンテナを復旧する方法を示しています。

   ```
   docker run -it --name eDir1-Host --restart on-failure:5 --memory="700M" --
   cpuset-cpus="1" --pids-limit="150" --volume eDir-volume1:/config --
   network=host <same_eDirectory_image> upgrade
   ```

   eDir-volume1は、影響を受けたeDirectoryコンテナのアプリケーションデータを保持している同じボリュームです。

7 IPv6アドレスを使用するLinuxとWindowsでのeDirectoryのインストール

eDirectory 9.2ではIPv4アドレスとIPv6アドレスの両方がサポートされています。eDirectoryのインストール処理中にIPv6アドレスを有効にできます。以前のバージョンからアップグレードしている場合、IPv6アドレスを手動で有効にする必要があります。

eDirectory 9.2では、デュアルIPスタック方式、トンネリング方式、およびピュアIPv6移行方式をサポートしています。グローバルのIPアドレスのみがサポートされます。次に例を示します。

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

IPv6アドレスは角括弧[ ]内に指定しなければならないということを除けば、eDirectoryの機能はIPv6でもIPv4と同じです。IPアドレスの代わりにホスト名を使用することもできます。ホスト名を用いる場合、etc\hostsファイルでホスト名を指定し、それをIPv6アドレスと関連付ける必要があります。

IPv6アドレスを使用しているeDirectoryユーティリティの例を以下に示します。

```
ndsstat -h [6015:abc:def:123:456:12:0:123]

ndsstat -h [6015:abc:def:123:456:12:0:123]:524

ndslogin -h [2015::4] admin.organization

ndscheck -h [6015:abc:def:123:456:12:0:123] -a admin.organization -w password

ldapadd -h [2015::4] -p 389 -D cn=admin,o=organization -w password -f adduser.ldif

ldapdelete -h [6015:abc:def:123:456:12:0:123] -p 389 -D cn=admin,o=organization -w
password cn=user21,o=organization

ldapmodify -h [2015::4] -p 389 -D cn=admin,o=organization -w password -f
modify.ldif

ldapsearch -h [6015:abc:def:123:456:12:0:123] -p 389 -D cn=admin,o=organization -w
password -b o=organization objectclass=inetorgperson

http://[2015::3]:8028/nds
```

eDirectory 9.2ではリンクローカルアドレスタイプ、IPv4マップドIPv6アドレスタイプ、およびIPv4互換IPv6アドレスタイプはサポートしていません。

以下のセクションでは、IPv6がすでに設定されているLinuxおよびWindowsにNetIQ eDirectory 9.2をインストールして設定する方法を示します。

- 116 ページの 「IPv6を使用するLinuxでのeDirectoryの設定」
- 117 ページの 「IPv6を使用するWindowsでのeDirectoryのインストールもしくはアップグレード」

IPv6のLinuxおよびWindowsプラットフォームにおける違いについては 『「NetIQ eDirectory Troubleshooting Guide (NetIQ eDirectoryトラブルシューティングガイド)」』の「*Listeners for Unspecified IPv6 Addresses in Linux and Windows (LinuxおよびWindowsの未指定のIPv6アドレスのリスナ)*」を参照してください。

IPv6を使用するLinuxでのeDirectoryの設定

このセクションではIPv6アドレスをすでにサポートしているLinuxコンピュータ上にeDirectoryを設定する方法について説明します。

新しいeDirectoryツリーを作成する

ndsconfigコマンドで-Bオプションを用いてIPv6アドレスを指定することで、IPv6アドレスを用いたeDirectoryツリーを新しく設定することができます。次に例を示します。

```
ndsconfig new -t CORP-TREE -B [2015::3]@524 -P ldap://[2015::3]:389,ldaps://
[2015::3]:636
```

LDAPリスナーに自動的にIPvアドレスの認識を開始させるには、eDirectoryの設定中に-PオプションでLDAP URLを指定する必要があります。初期設定の段階で指定しない場合は、後からldapconfigコマンドまたはiManagerを用いてldapInterfaces属性に追加できます。詳細については、「11ページの 「IPV6のLDAPURLのLDAPサーバオブジェクトへの追加」」を参照してください。

既存のeDirectoryツリーへのサーバの追加

ndsconfigコマンドの-Bオプションを用いてIPv6アドレスを指定することで、既存のIPv6のツリーにサーバを追加できます。次に例を示します。

```
ndsconfig add -t CORP-TREE -B [2015::4]@524 -P ldap://[2015::4]:389,ldaps://
[2015::4]:636
```

LDAPリスナーに自動的にIPvアドレスの認識を開始させるには、eDirectoryの設定中に-PオプションでLDAP URLを指定する必要があります。初期設定の段階で指定しない場合は、後からldapconfigコマンドまたはiManagerを用いてldapInterfaces属性に追加できます。詳細については、「11ページの 「IPV6のLDAPURLのLDAPサーバオブジェクトへの追加」」を参照してください。

既存のもしくはアップグレードしたeDirectoryサーバでのIPv6アドレスの有効化

1 /etc/opt/novell/eDirectory/conf/nds.confファイルに、ポート番号を含むIPv6インタフェースアドレスを追加します。コンピュータに複数のインスタンスが設定されている場合は、それぞれの環境設定ファイルにこのアドレスを追加する必要があります。

次に例を示します。

```
n4u.server.interfaces=164.99.90.148@524,[2015::4]@524,[2015:1234:2345:3456:abc
d:bcde:cdef:aaaa]@524
```

```
http.server.interfaces=164.99.90.148@8028,[2015::4]@8028,[2015:1234:2345:3456:
abcd:bcde:cdef:aaaa]@8028
```

```
https.server.interfaces=164.99.90.148@8030,[2015::4]@8030,[2015:1234:2345:3456
:abcd:bcde:cdef:aaaa]@8030
```

2 以下のコマンドを使用して、ndsdを再起動します。

```
ndsmanage stopall
ndsmanage startall
```

IPV6のLDAP URLのLDAPサーバオブジェクトへの追加

eDirectoryの初期設定の段階でLDAP URLを指定しない場合は、後からldapconfigコマンドまたはiManagerを用いて、ldapInterfaces属性にLDAP URL追加できます。

以下は、ldapconfig setおよびldapconfig-sコマンドの使用例です。

```
ldapconfig set "ldapInterfaces=ldap://[2015::3]:389,ldaps://[2015::3]:636"
```

```
ldapconfig -s
"ldapInterfaces=ldap://[2015::3]:389,ldapInterfaces=ldaps://[2015::3]:636"
```

iManagerでLDAP URLを追加する：

1 NetIQ iManagerで［**役割およびタスク**］をクリックする。
2 ［**LDAP**］ > ［**LDAPオプション**］をクリックする。
3 ［**LDAPサーバの表示**］をクリックし、LDAPサーバオブジェクトの名前をクリックして設定します。
4 ［**接続**］をクリックし、［**LDAPインタフェース**］フィールドで**LDAP URLを追加する**。
5 ［**適用**］をクリックし、［**OK**］をクリックします。

IPv6を使用するWindowsでのeDirectoryのインストールもしくはアップグレード

このセクションではIPv6アドレスをすでにサポートしているWindowsコンピュータ上にeDirectoryを設定する方法について説明します。

eDirectoryのインストール中またはアップグレード中に行うIPv6の有効化

IPv6アドレスを使用する場合は、eDirectoryのインストール中に［**IPV6の初期設定**］の下の［**IPV6を有効にする**］チェックボックスを選択します。選択するとDHostがIPv6アドレスの認識を開始します。インストールプロセス中にIPv6アドレスを有効にせず、後から使用することにした場合は、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。

既存のサーバ上でのIPv6の有効化

設定済みのeDirectoryサーバでIPv6アドレスを使用する場合はインストールを再実行し、［**IPV6の初期設定**］の下の［**IPV6を有効にする**］チェックボックスを選択する必要があります。それによりIPv6アドレスの、NCP、HTTP、およびHTTPSプロトコルが有効になります。

iMonitorへのアクセス

IPv6アドレスを介してiMontiorにアクセスするためのリンクは以下の通りです：

```
http://[2015::3]:8028/nds
```

8 FIPSモードでのeDirectoryの運用

eDirectory 9.2は、非常にセキュアな環境を使用している米国連邦政府機関や顧客のセキュリティ要件を満たすため、FIPS (連邦情報処理規格)に準拠した機能を利用しています。本章では、FIPSモードのeDirectoryの環境設定と運用について説明します。

NICIおよびOpenSSLモジュールでサポートされるFIPS 140-2モードでeDirectoryを実行できます。

- 119 ページの 「OpenSSL用にFIPSモードのeDirectoryを設定」

OpenSSL用にFIPSモードのeDirectoryを設定

eDirectoryサーバでFIPSモードを有効にすると、OpenSSLを使用してeDirectory内で実行されるすべてのアプリケーションおよびモジュールが、常にFIPSモードでOpenSSLを使用します。たとえば、LDAP、HTTP、EBA内のすべての暗号化処理などがこれに該当します。FIPSモードでeDirectoryを動作させると、SSLv3経由の通信が許可されず、サイファの使用が強度の高いサイファのみに制限されます。詳細については、『NetIQ eDirectory管理ガイド』の「LDAPオブジェクトを環境設定する」および「*HTTPサーバオブジェクトの設定*」を参照してください。

デフォルトで、すべてのeDirectory 9.2サーバはLinuxとWindowsのどちらのプラットフォームでもOpenSSLのFIPSモードで実行されます。eDirectoryには、要件に合わせてFIPSモードを設定するためのスイッチが用意されています。

OpenSSLに対してFIPSモードを有効にするには:

- **Windows:** デフォルトでFIPSモードがeDirectory環境で有効になり、OpenSSLを使用するすべてのeDirectoryのアプリケーションまたはモジュールが、常にFIPSモードでOpenSSLを使用します。FIPSモードでeDirectoryを動作させると、SSLv3経由の通信が許可されず、サイファの使用が強度の高いサイファのみに制限されます。詳細については、『NetIQ eDirectory管理ガイド』の「LDAPオブジェクトを環境設定する」および「*HTTPサーバオブジェクトの設定*」を参照してください。
- **Linux:** Linux上でFIPSモードでeDirectoryを実行するためにその他の設定を行う必要はありません。eDirectoryのインストールでは、FIPSモードがデフォルトでオンになります。

OpenSSLに対してFIPSモードを無効にするには:

- **Windows:** HKLM\SOFTWARE\Novell\NDS\FipsModeレジストリ値に移動し、**FipsMode**を**0**に設定します。
- **Linux:** ndsconfig setコマンドで**n4u.server.fips_tls=0**を渡し、サーバを再起動します。

  たとえば、ndsconfig set n4u.server.fips=0と指定します。

9 DIBの移動

NetIQ eDirectoryをインストールして設定した後、DIBの移動が必要な場合は、DIBを移動できます。DIBの移動が必要となる理由はさまざまです。たとえば、ツリー内のオブジェクト数の増加が予想されるが、DIBがある現在のファイルシステムに十分な容量がない場合などが挙げられます。

Linux

DIBを移動するには、次の手順を実行します。

1. コマンドラインで次のコマンドを入力して、サーバの状態を確認します。

   ndscheck

2. 次のようにして、ndsmanagを使用してeDirectoryサービスを停止します。

   2a コマンドプロンプトで「ndsmanage」と入力します。

   2b 停止するインスタンスを選択します。

   メニューが拡張し、特定のインスタンスに対して実行可能なオプションが表示されます。

   2c インスタンスを停止するには、「k」と入力します。

3. 次のコマンドを使用して、DIBの現在位置を取得します。

   ```
   ndsconfig get n4u.nds.dir
   ```

4. 次のとおり、DIBを新しい場所にコピーします。

   ```
   cp -rp current_location new_location
   ```

   たとえば、DIBを/home/nds/にコピーするには、次のコマンドを入力します。

   ```
   cp -rp /var/opt/novell/eDirectory/data//* /home/nds//
   ```

5. インスタンス固有のnds.conf環境設定ファイルを編集して、次のようにn4u.nds.dirのパラメータ値を変更します。

   ```
   n4u.nds.dir=new_location
   ```

   たとえば、DIBのパスを/var/nds/から/home/nds/に変更する場合は、次のように入力します。

   ```
   n4u.nds.dir=/home/nds/
   ```

6. 次のとおり、eDirectoryサービスを開始します。

   6a コマンドプロンプトで「ndsmanage」と入力します。

   6b 開始するインスタンスを選択します。

   メニューが拡張し、特定のインスタンスに対して実行可能なオプションが表示されます。

   6c インスタンスを開始するには、「s」と入力します。

7. サーバステータスを次のようにチェックします。

   ndscheck

Windows

DIBの移動は現在サポートされていません。ただし、eDirectoryのインストール中に、DIBを任意の場所に配置することができます。

10 eDirectory 9.2のアップグレード要件

eDirectoryの独特の機能の1つとして、厳格なリファレンス整合性を維持することができるようになっています。最上位から派生しているオブジェクトクラスのクラス定義はどれも、リファレンス属性を持つようになります。これは、eDirectoryが内部的に維持しているすべてのリファレンス先オブジェクトに追加される隠し属性です。リファレンス先オブジェクトとリファレンス元オブジェクト間のリンクをチェックするバックグラウンドプロセスは、継続的に実行されます。

リファレンス先オブジェクトのパーティションがサーバ内でローカルに保持されていたオブジェクトのパーティションと異なる場合、そのオブジェクトへの外部参照が外部参照パーティション内のローカルで作成されます。外部参照とは、eDirectoryツリー内に存在するオブジェクトを表現したものです。ただし、外部参照はオブジェクトとそのオブジェクトの割り当てられた属性のコピーではありません。

eDirectoryからリファレンス属性を削除することはできますが、ツリーの後方互換性を維持するため、クラス定義を操作することは今のところできません。

この章では、eDirectory 9.2の変更点、および考えられるアップグレードシナリオについて説明します。

9.2以降のバージョンのリファレンスに関する変更点

リファレンス属性は隠し属性で、リファレンス先オブジェクトごとに保持されます。これは、DSによって作成および保持されます。DSの新しいリファレンスコードは、Flexible Adaptable Information Manager (FLAIM)インデックスをベースにしています。これはDSが作成するLocalEntryIDIndexと呼ばれています。FLAIMはインデックスを維持しますが、使用方法はDSが決定します。DN値が追加または削除されると、FLAIMはインデックスを自動的に更新します。インデックス内の各キーは合成キー(リファレンス先のオブジェクトのDN+リファレンス元オブジェクトのエントリID)です。たとえば、エントリID343のオブジェクトがあり、オブジェクト#899をポイントする「メンバー」値が存在する場合、FLAIMは899+343というインデックスでキーを自動生成します。これでDSはインデックス内のルックアップを実行し、オブジェクト#899をポイントしているすべてのオブジェクトを検索できるようになります。参照元のすべてのオブジェクトを記憶するために、オブジェクト#899自体がリファレンス属性を保持する必要はありません。実際、FLAIMはインデックスがどのように使われるかを認識せずにインデックスを保持しますが、DSにはインデックスの使用方法を認識しているコードが存在します。

ただし、リファレンスを維持する新しい方法では、既存のeDirectoryインスタンスを9.2以降のバージョンにアップグレードするときにデータベースをアップグレードする必要があります。アップグレードでは、新しいインデックスの作成が必要で、そこでデータベースの各エントリを詳細に検証することが必要になります。また、データベース内の各エントリから「リファレンス」属性をすべて削除することも必要です。さらに、DNを埋め込んでいたDSが使用する内部オクテット文字列属性が、オクテット文字列値と一緒に保存する新しいDN値を生成する必要も出てきます。これらの処理はすべて、大規模なデータベースでは非常に時間のかかるプロセスです。DSは新しいFLAIM機能を使ってリファレンスの整合性を保持するように変更されており、それが新しいイン

デックスに依存しているため、この変換が完了するまで、DSを実際に稼働できません。したがって、初めて既存データベースを開いたときに、すべてのリファレンス属性を新しいインデックスに変更する必要があります。大型データベースの場合、実際に開いてアプリケーションが使用できる状態になるまで数時間かかることがあります。

9.2のアップグレードプロセス

ndsconfig upgradeコマンドは、HTTP、LDAP、SNMP、SAS、およびNMASなどのコンポーネントで必要な環境設定をアップグレードするために使用します。eDirectory 8.8 SP1より前のeDirectoryバージョンをeDirectory 9.2にアップグレードすると、eDirectoryデータベースは新しいフォーマットにアップグレードされます。

強制オプションを使ってLinuxのeDirectoryを旧バージョンからアップグレードする

Linuxでは、eDirectory 9.2は、8.8.8以降のバージョンからのアップグレードのみに対応しています。

eDirectoryバージョン8.7.3～8.8.8からアップグレードする場合は、次のいずれかの手順を実行します。

- 最初にeDirectory 8.8.8にアップグレードし、次にeDirectory9.2にアップグレードする。

または

- switch -fの強制コマンドを使って、直接アップグレードする。

  このオプションを使用した場合、DIBアップグレードのためのヘルスチェックやディスク容量チェックなど、一部のチェックが実行されません。また、古いRPMが削除され、新しいRPMがインストールされます。

重要: Identity Manager変更ログモジュールがすでにインストールされている場合、eDirectoryを9.2にアップグレードするときに、環境変数NDSD_IGNORE_IDM_CHECKを1に設定する必要があります。次に例を示します。

- Linuxの場合: NDSD_IGNORE_IDM_CHECK=1 ./nds-install
- Windowsの場合: setup.exeを実行する前にNDSD_IGNORE_IDM_CHECKをtrueに設定します。

---

11 Linux上でのNetIQ eDirectoryの設定

NetIQ eDirectoryには、Linuxコンピュータ上でのさまざまなeDirectoryコンポーネントの設定を容易にする設定ユーティリティが含まれています。次のセクションでは、eDirectory環境設定コンポーネントの機能および使用法について説明します。

- 125 ページの 「環境設定ユーティリティ」
- 128 ページの 「環境設定パラメータ」
- 134 ページの 「セキュリティ上の考慮事項」

環境設定ユーティリティ

このセクションでは、次のeDirectory環境設定ユーティリティの使用法について説明します。

- 125 ページの 「ndsconfigユーティリティ」
- 126ページの「LDAPツールを使用してLDAPサーバとLDAPグループオブジェクトを背呈する」
- 126 ページの 「nmasinstユーティリティを使用してNetIQ Modular Authentication Serviceを設定する」
- 126 ページの 「eDirectoryのカスタマイズ」

ndsconfigユーティリティ

ndsconfigユーティリティを使用して、eDirectoryを設定できます。このユーティリティは、既存のツリーにeDirectoryレプリカサーバを追加するときや新しいツリーを作成するときにも使用できます。詳細については、「39 ページの 「ndsconfigユーティリティを使用してeDirectoryレプリカサーバを追加または削除する」」を参照してください。

注

- NCPサーバ名がネットワーク内で一意であることを確認してください。
- SLES12SP2およびRHEL7.2でndsconfigユーティリティが失敗する。この問題はランダムに発生します。この問題のトラブルシュートの詳細については、「TID 18366」を参照してください。

インストールされているコンポーネントの現在の設定を変更するには、次の構文を使用します。

```
ndsconfig {set value_list | get [parameter_list] | get help [parameter_list]}
```

ndsconfigパラメータの説明については、「128ページの「環境設定パラメータ」」を参照してください。

重要: インストール後、ndsconfigユーティリティをサーバのインストール場所から実行します。この場所はデフォルトでは/opt/novell/eDirectory/binです。インストールパッケージからndsconfigを実行しないでください。

LDAPツールを使用してLDAPサーバとLDAPグループオブジェクトを背呈する

Linuxコンピュータ上でLDAPサーバおよびグループオブジェクトの属性を変更、表示、およびリフレッシュするには、eDirectoryに同梱されているLADPツールを使用できます。

詳細については、『「NetIQ eDirectory管理ガイド」』の「*Linux でのLDAP ツールの使用*」を参照してください。

nmasinstユーティリティを使用してNetIQ Modular Authentication Serviceを設定する

eDirectory 9.2では、デフォルトで、ndsconfigを使用してNMASを設定します。nmasinstを使用してNMASを設定することもできます。

ndsconfigが行うのはNMAS設定のみです。ログインメソッドのインストールは行いません。ログインメソッドのインストールには、nmasinstを使用できます。詳細については、「53 ページの「nmasinstユーティリティを使用してNMASを設定する」」を参照してください。

eDirectoryのカスタマイズ

ndsd initスクリプトを使用する

システムが起動すると、デフォルトの環境設定ファイル/etc/opt/novell/eDirectory/conf/nds.conf の環境設定パラメータを使用して、ndsd initスクリプトがデーモンを開始します。

注: systemd環境では/etc/init.d/ndsdスクリプトを使用しないでください。Systemdは現在、SLES 12およびRHEL 7プラットフォームのみでサポートされています。詳細については、127 ページの「SLES 12およびRHEL 7プラットフォームでeDirectoryを使用する」を参照してください。

---

ndsdを開始する前に、すべてのSLP (Service Location Protocol)エージェントがホスト上で実行されていることを確認してください。OpenSLP、ご利用のオペレーティングシステムで使用可能なSLP、またはNetIQ SLPがインストール可能です。

注: eDirectoryを開始するには、ndsmanageユーティリティを使用します。

---

ndsdを開始するには、/etc/init.d/ndsd startを実行します。

ndsdを停止するには、/etc/init.d/ndsd stopを実行します。

注: 以下のコマンドを実行して、SLES 12およびRHEL7でeDirectoryを開始および停止してください。

- ndsdを開始するには、systemctl start ndsd*を実行します
- ndsdを停止するには、systemctl stop ndsd*を実行します

eDirectoryの設定によって、/opt/novell/eDirectory/sbin内に次のシェルスクリプトが作成されます。

- pre_ndsd_start
- post_ndsd_start
- pre_ndsd_stop
- post_ndsd_stop

名前が示すように、ndsdバイナリが/etc/init.d/ndsdスクリプトによって起動される前に、pre_ndsd_startスクリプトが実行されます。post_ndsd_startスクリプトは、/etc/init.d/ndsdスクリプトによってndsdバイナリが起動された後に実行されます。同様に、pre_ndsd_stopとpost_ndsd_stopスクリプトも、ndsdプロセスを停止する前と後にそれぞれ実行されます。

選択したコマンドをこれらのスクリプトに追加して、実行することができます。デフォルトでは、LDAPサービスが起動した後/etc/init.d/ndsdを実行するコマンドがpost_ndsd_startスクリプトに記述されています。

注: /etc/opt/novell/eDirectory/confディレクトリにあるenv_customスクリプトで、eDirectoryサービスに必要なすべての環境変数を追加する必要があります。端末または/etc/init.d/ndsdスクリプトでの環境変数のエクスポートは、eDirectoryでは使用されません。環境変数の詳細については、「TID 7018431」を参照してください。

SLES 12およびRHEL 7プラットフォームでeDirectoryを使用する

システムが起動すると、デフォルトの環境設定ファイル/etc/opt/novell/eDirectory/conf/nds.confの環境設定パラメータを使用して、eDirectoryがデーモンを開始します。

ndsdを開始する前に、すべてのSLP (Service Location Protocol)エージェントがホスト上で実行されていることを確認してください。OpenSLP、ご利用のオペレーティングシステムで使用可能なSLP、またはNetIQ SLPがインストール可能です。

eDirectoryを開始または停止するには、ndsmanageユーティリティを使用します。

eDirectoryの設定によって、/opt/novell/eDirectory/sbin内に次のシェルスクリプトが作成されます。

- pre_ndsd_start_custom: eDirectoryを実行する前にこのスクリプトを使用して、コマンドをカスタムで追加します。
- post_ndsd_start_custom: eDirectoryを実行した後でこのスクリプトを使用して、コマンドをカスタムで追加します。
- post_ndsd_stop_custom: eDirectoryを停止した後でこのスクリプトを使用して、コマンドをカスタムで追加します。

注

- /opt/novell/eDirectory/sbinにある工場出荷時のスクリプトは使用しないでください。eDirectoryの設定では、工場出荷時のスクリプトが使用されます。選択したコマンドを含めるには、カスタムスクリプトを使用してください。
- オペレーティングシステムをアップグレードした後、ndsconfig upgradeユーティリティを実行します。

サーバのブートでeDirectoryの非ルートインスタンスを開始できるようにする

非ルートインストールからのeDirectoryインスタンスは、自動では開始しません。サーバを再起動したときにeDirectoryの非ルートインスタンスを自動で開始できるようにするには、次の手順を実行します。

1. 開始スクリプトを作成します。
2. スクリプトに次のコマンドを入力します。

   ```
   su - user1 -c"/home/user1/eDirectory/opt/novell/eDirectory/bin/ndsmanage
   startall
   ```

   上記の例では、eDirectoryは、/home/user1/eDirectory/opt/novell/eDirectory/bin/ndsmanageパスのndsmanageスクリプトを使用して非ルートのuser1として実行されます。
3. ファイルを保存します。
4. スクリプトを実行するための適切な許可をルートユーザに付与します。
5. 次のコマンドを使用して開始スクリプトへのシンボリックリンクを作成します。

   ```
   ln -s /etc/init.d/ndsstart /sbin/rcndsstart

   ln -s /etc/init.d/ndstart /etc/init.d/rc2.d/S10ndsstart

   ln -s /etc/init.d/ndstart /etc/init.d/rc3.d/S10ndsstart

   ln -s /etc/init.d/ndsstart /etc/init.d/rc5.d/S10ndsstart
   ```

サーバが再起動すると、eDirectoryのすべての非ルートインスタンスが自動的に開始されるようになります。

環境設定パラメータ

eDirectory環境設定パラメータはnds.confファイルに格納されています。

環境設定パラメータを変更した場合、新しい値を有効にするにはndsdを再起動する必要があります。ndsdを再起動するには、ndsmanageを使用してください。

ただし、環境設定パラメータによってはndsdを再起動する必要がない場合があります。再起動の必要のないパラメータは次のとおりです。

- n4u.nds.inactivity-synchronization-interval
- n4u.nds.synchronization-restrictions
- n4u.nds.janitor-interval

- n4u.nds.backlink-interval
- n4u.nds.drl-interval
- n4u.nds.flatcleaning-interval
- n4u.nds.server-state-up-thresholdn4u.nds.heartbeat-scheman4u.nds.heartbeat-data

次の表では、すべての環境設定パラメータの説明を示します。

パラメータ	説明
n4u.nds.preferred-server	eDirectoryを格納するコンピュータのホスト名です。 デフォルト値はNULLです。
n4u.base.tree-name	AccountManagementが使用するツリー名です。この必須パラメータは、AccountManagementのインストーラによって設定されます。このパラメータを設定することはできません。
n4u.base.dclient.use-udp	DClientでは、eDirectoryサーバとの通信に、TCPのほかにUDPも使用できます。このパラメータにより、UDP転送機能が使用できるようになります。 デフォルト値は0です。 範囲は0または1です。
n4u.base.slp.max-wait	SLP (Service Location Protocol) API呼び出しのタイムアウトです。 デフォルト値は30です。 範囲は3～100です。 この値は秒単位で表します。 このオプションは、NetIQ SLPによってのみサポートされ、OpenSLPではサポートされません。
n4u.nds.advertise-life-time	指定の時間が過ぎると、eDirectoryはディレクトリエージェントに再び自己登録します。 デフォルト値は3600です。 範囲は1～65535です。 この値は秒単位で表します。
n4u.server.signature-level	これにより、拡張セキュリティサポートのレベルが決まります。この値を大きくするとセキュリティは向上しますが、パフォーマンスは低下します。 デフォルト値は1です。 範囲は0～3です。

パラメータ	説明
n4u.nds.dir	eDirectoryディレクトリ情報データベースです。 デフォルト: `/var/opt/novell/eDirectory/data/` ndsconfig setコマンドを使用してこのパラメータを設定することはできません。DIBを再配置する場合は、このパラメータを手動で変更できます。ただし、この操作はお勧めできません。
n4u.nds.server-guid	eDirectoryサーバ全体で固有の識別子です。 デフォルト値はNULLです。
n4u.nds.server-name	eDirectoryサーバの名前です。 デフォルト値はNULLです。
n4u.nds.bindery-context	バインダリコンテキストの文字列です。 デフォルト値はNULLです。
n4u.nds.server-context	eDirectoryサーバの追加先コンテキストです。このパラメータを設定または変更することはできません。
n4u.nds.external-reference-life-span	使用されていない外部参照を削除するまでの時間数です。 デフォルト値は192です。 範囲は1～384です。
n4u.nds.inactivity-synchronization-interval	レプリカの完全同期の実行後、サーバ上のeDirectoryに格納されている情報が最初に変更されてから次にレプリカの完全同期を実行するまでの時間間隔(分)です。 デフォルト値は60です。 範囲は2～1440です。
n4u.nds.synchronization-restrictions	値をOffに設定すると、eDirectoryの任意のバージョンと同期できます。値をOnに設定すると、同期するバージョン番号がパラメータで指定した値(ON,420,421など)に制限されます。 デフォルト=オフ
n4u.nds.janitor-interval	eDirectory janitor処理の実行間隔(分)です。 デフォルト値は2です。 範囲は1～10080です。
n4u.nds.backlink-interval	eDirectoryバックリンクの整合性チェックの実行間隔(分)です。 デフォルト値は780です。 範囲は2～10080です。

パラメータ	説明
n4u.nds.drl-interval	eDirectory分散リファレンスリンクの整合性チェックの実行間隔(分)です。 デフォルト値は780です。 範囲は2～10080です。
n4u.nds.flatcleaning-interval	flatcleaner処理によるデータベースからのエントリの自動パージおよび削除の実行間隔(分)です。 デフォルト値は720です。 範囲は1～720です。
n4u.nds.server-state-up-threshold	サーバの状態のUPしきい値(分)です。このしきい値に達すると、eDirectoryはサーバの状態をチェックし、その後-625エラーを戻します。 デフォルト値は30です。 範囲は1～720です。
n4u.nds.heartbeat-schema	Heartbeatベーススキーマの同期間隔(分)です。 デフォルト値は240です。 範囲は2～1440です。
n4u.nds.heartbeat-data	Heartbeat同期間隔(分)です。 デフォルト値は60です。 範囲は2～1440です。
n4u.nds.dofsync	このパラメータを0に設定すると、大規模なデータベースで更新のパフォーマンスが大幅に上がります。しかし、システムがクラッシュした場合にはデータベースが破損する危険があります。
n4u.server.configdir	eDirectory環境設定ファイルがここに配置されます。 デフォルト値は/etcです。
n4u.server.vardir	eDirectoryおよびユーティリティのログファイルがここに配置されます。 デフォルト値は/var/opt/novell/eDirectory/logです。
n4u.server.libdir	eDirectory固有のライブラリは、nds-modulesディレクトリのこの場所に配置されます。 デフォルト値は/opt/novell/eDirectory/libです。
n4u.server.sid-caching	SSLセッションIDの変更を有効にします。SSLのセッションIDのキャッシュの詳細については、『SSL v3.0 RFC』を参照してください。
n4u.server.tcp-port	n4u.server.interfacesパラメータでポート番号が指定されない場合に使われるデフォルトポートです。

パラメータ	説明
n4u.server.interfaces	eDirectoryサーバがクライアント接続をリスンするIPアドレスおよびポート番号です。設定の組み合わせを複数指定する場合は、値をコンマ区切りのリスト形式で指定できます。例: n4u.server.interfaces=101.1.2.3@524,100.1.2.3@1524
n4u.server.max-interfaces	このパラメータは、eDirectoryが使用するインタフェースの最大数を指定します。 デフォルト値は128です。 範囲は1～2048です。
n4u.server.max-openfiles	このパラメータは、eDirectoryが使用できるファイルデスクリプタの最大数を指定します。 デフォルト値は、管理者によって設定される最大値です
n4u.server.max-threads	eDirectoryサーバが開始するスレッドの最大数です。この数は、eDirectoryサーバ内で同時に実行できる操作の数です。 デフォルト値は64です。 範囲は32～512です。 最適値を設定するには、『*NetIQ eDirectory Troubleshooting Guide (NetIQ eDirectory トラブルシューティングガイド)*』を参照してください。
n4u.server.idle-threads	eDirectoryサーバで許可されるアイドル状態のスレッドの最大数です。 デフォルト値は8です。 範囲は1～128です。
n4u.server.start-threads	最初に開始されるスレッドの数です。 デフォルト値は8です。
n4u.server.log-levels	このパラメータは、サーバ側のメッセージのエラーログを設定するときに役立ちます。メッセージログのレベルはLogFatal、LogWarn、LogErr、LogInfo、LogDbgのいずれかに設定されます。
n4u.server.log-file	このパラメータは、メッセージを書き込むログファイルの場所を指定します。デフォルトでは、ndsd.logファイルにメッセージが書き込まれます。

パラメータ	説明
n4u.ldap.lburp.transize	1つのLBURPパケットでNetIQインポート/エクスポートクライアントからLDAPサーバに送られるレコード数です。トランザクションのサイズを増やし、1つの要求で確実に複数の追加操作を実行することができます。 デフォルト値は25です。 範囲は1～250です。
n4u.server.listen-on-loopback	ブール値のパラメータで、デフォルトで有効になっています。最近のいくつかのLinux配布パッケージでは、/etc/hostsファイル内のホスト名がループバックアドレスに関連付けられています。SLESシステムで提供される共通アドレスは127.0.0.2ですが、127.0.0.0から127.255.255.255までの任意の値(有効なループバックアドレス)にすることができます。
http.server.interfaces	HTTPサーバが使用するインタフェースのカンマ区切りのリストです。
http.server.request-io-buffer-size	デフォルトのIOバッファサイズです。
http.server.request_timeout-seconds	サーバ要求のタイムアウトです。
http.server.keep-timeout-seconds	同じ接続上にある同じクライアントからの次の要求を待つ秒数です。
http.server.threads-per-processor	プロセッサごとのHTTPスレッドプールのサイズです。
http.server.session-exp-seconds	セッションの有効期間(秒)です。
http.server.sadmin-passwd	セッション管理者のパスワードです。
http.server.module-base	HTTPサーバのWebルートです。
https.server.cached-cert-dn	HTTPSサーバがキャッシュした証明書のDNです。
https.server.cached-server-dn	HTTPSサーバがキャッシュしたDNです。
http.server.trace-level	HTTPサーバの診断追跡レベルです。
http.server.auth-req-tls	HTTPサーバ認証にTLSが必要です。
http.server.clear-port	HTTPプロトコルのサーバポートです。
http.server.tls-port	HTTPSプロトコルのサーバポートです。
n4u.server.fips	eDirectoryサーバをFIPSモードで実行するかどうかを指定します。 デフォルトは1です。この場合、eDirectoryはFIPSモードで実行されます。 FIPSモードを無効にするには、ndsconfig setコマンドでn4u.server.fips=0を渡し、サーバを再起動します。

注: eDirectoryの環境設定パラメータの詳細については、nds.confのマニュアルページを参照してください。

セキュリティ上の考慮事項

次のセキュリティ上の検討事項を推奨します。

- ツリーのブラウズ権限を認証されたユーザだけに割り当ててください。これを制限するには、次の操作を実行します。
  - ツールルートの［パブリック］のブラウズ権限を削除します。
  - ツリールートの［ルート］のブラウズ権限を割り当てます。
- LDAPサーバオブジェクトのldapBindRestrictions属性を、［匿名単純バインドを不許可にする］に設定します。これにより、クライアントが匿名バインドをしなくなります。

12 eDirectory 9.2へのマイグレーション

本書では、オペレーティングシステムも併せてアップグレードする必要がある場合に、NetIQ eDirectory 8.8.8.xサーバをeDirectory 9.2にマイグレートする方法を説明します。

eDirectory 9.2でサポートされるオペレーティングシステムの変更があったため、以前はeDirectory 8.8.8.xでサポートされていたものの、eDirectory 9.2ではサポートされていないバージョンがいくつか存在します。

eDirectory 9.2へのマイグレーションには、次の2種類のシナリオがあります。

- **プラットフォームのアップグレードが可能な場合のeDirectory 9.2へのマイグレーション**

  このシナリオでは、オペレーティングシステムをサポート対象バージョンにアップグレードした後、eDirectoryをeDirectory 9.2にアップグレードします。
- **プラットフォームのアップグレードが実行できない場合のeDirectory 9.2へのマイグレーション**

  このシナリオでは、オペレーティングシステムのマイグレーションパスが実行不可のため、オペレーティングシステムをサポート対象のバージョンにアップグレードすることができません。

オペレーティングシステムをアップグレードしてeDirectory 9.2へマイグレートする

ここでは、オペレーティングシステムをアップグレードした後、eDirectory 9.2にマイグレートできる場合のシナリオで説明します。たとえば、32ビットのオペレーティングシステムから64ビットのオペレーティングシステムにアップグレードできます。次の表に、マイグレーションパスを示します。

重要

- eDirectory 8.7.3を最新のパッチセットでアップグレードしていることを確認します。
- BTRFSを使用している場合は、サポートされているファイルシステムにマイグレートすることをお勧めします。マイグレートする方法の詳細については、136 ページの 「オペレーティングシステムをアップグレードしないでeDirectory 9.2へマイグレートする」を参照してください。

表 12-1 マイグレーションのパス

オペレーティングシステム	開始状態	中間状態	中間状態	最終状態
Windows	Windows 2008 SP2 + eDirectory 8.8 SP8	Windows 2012 + eDirectory 8.8 SP8		Windows 2012 R2 + eDirectory 9.2
	注意: Linux上でeDirectoryをアップグレードする前に、ホスト名が/etc/hostsファイル内のループバックアドレスではなく、有効なIPアドレスに設定されていることを確認してください。			
Linux	SLES 10 + eDirectory 8.8.8.x	SLES 11 SP4 + eDirectory 8.8.8.x	SLES 12 + eDirectory 8.8 SP8	SLES 12 + eDirectory 9.2.x

重要: ndsconfig upgradeは必ず、eDirectory 8.8 SP8からeDirectory 9.2にアップグレードした後で実行してください。

推奨事項

1 1 オペレーティングシステムをアップグレードする前に、eDirectory 8.8.8.xのファイルをバックアップしてください。eDirectoryを停止し、次のファイルをバックアップします。

- dibディレクトリ
- nds.rflディレクトリ (デフォルトでは、このディレクトリはdibディレクトリの下にあります)
- nds.confファイル
- niciディレクトリ(ルートユーザの場合は、/var/opt/novell/nici/0で見つかったディレクトリがNICIユーザディレクトリになります)
- ログファイル

2 2 eDirectoryのバージョンが中間状態の特定オペレーティングシステムでサポートされていない場合、eDirectoryのアップグレード以外の操作を中間状態で実行しないでください。

オペレーティングシステムをアップグレードしないでeDirectory 9.2へマイグレートする

この方法は、サポートされているeDirectory 9.2バージョンへのオペレーティングシステムのアップグレードパスが存在しないシナリオで使われます。

たとえば、SLES 10にeDirectory 8.8がインストールされている場合です。SLES 10を使用する顧客がSLES 12上のeDirectory 9.2にアップグレードしようとすると、SLES 10からSLES 12へのアップグレードパスがありません。

eDirectory 9.2へマイグレートするには、次の手順を実行します。

1 eDirectoryサーバを停止します。

2 次のeDirectory 8.8ファイルのバックアップを作成します。

- dibディレクトリ

- nds.rfl ディレクトリ(デフォルトでは、このディレクトリはdibディレクトリの下にあります)
- nds.confファイル
- NICIユーザディレクトリ(ルートユーザの場合は、/var/opt/novell/nici/0で見つかったディレクトリがNICIユーザディレクトリになります)
- ログファイル

3 オペレーティングシステムをインストールします。.

4 サーバにeDirectory 9.2をインストールします(新規インストール)。

5 NICIユーザディレクトリを/var/opt/novellに復元します。

NICIユーザディレクトリの詳細については、『*NICI Administration Guide (NICI管理ガイド)*』の「Configuring the Settings for NICI User Directory (NICIユーザディレクトリを設定する)」を参照してください。

6 dibディレクトリおよびnds.rflディレクトリを復元します。

7 nds.confをユーザ指定の場所に復元します。

8 /etc/opt/novell/eDirectory/conf/.edir/instances.0を編集し、nds.confファイルの絶対パスを記述します。

9 nds.confファイルを編集して、次を追加します。

```
n4u.nds.dir=_file_location
n4u.server.libdir=/opt/novell/eDirectory/lib
n4u.server.vardir=var_directory
n4u.server.configdir=/etc/opt/novell/eDirectory/conf
http.server.module-base=http_server_module_base_directory
```

10 次のようにパスを設定します。

/opt/novell/eDirectory/bin/ndspathユーティリティを使用します。

11 パスを設定した後、ndsconfig upgradeを実行します。

13 高可用性クラスタでeDirectoryを展開する

NetIQ eDirectoryが高可用性をサポートする主な方法は、同期により複数サーバを設定する方法です。ただし一部の環境で高可用性を実現する場合、クラスタリングの方が実現性が高い選択肢となることがあります。

このセクションでは、共有ストレージを使って、高可用性クラスタ上でeDirectoryを環境設定するためのガイドラインについて説明します。このセクションでは、サポート対象のWindowsまたはLinuxプラットフォームの、一般的な高可用性クラスタの共有ストレージについて説明しています。特定のクラスタマネージャに特化したものではありません。

eDirectory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。つまり、eDirectoryDIBは、クラスタの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eDirectoryルートインスタンスは、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。

DIBの他に、サーバ固有のキーをクラスタノード間で複製するために、NICI (NetIQ International Cryptographic Infrastructure)のデータも共有する必要があります。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。

その他のeDirectory設定データやログデータも、共有ストレージに常駐する必要があります。

eDirectory 9.2には、LinuxサーバとWindowsサーバの両方で、指定した共有ストレージ場所へのデータコピー、適切な環境設定パラメータの更新、プライマリノード以外のクラスタノード上でのeDirectoryサービスの設定など、クラスタ環境内のeDirectoryを自動的に環境設定するユーティリティが用意されています。

以下のセクションの手順は、以下の前提条件に基づいています。

- ユーザがeDirectoryのインストール手順に精通している。
- 2ノードクラスタを使用している。

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。eDirectory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ないことに注意してください。

この章の構成は次のとおりです。

LinuxでのeDirectoryサービスのクラスタリング

このセクションでは、Linuxの高可用性(HA)クラスタリングを使用して、eDirectory 9.2を環境設定する方法について説明します。

前提条件

- クラスタリングソフトウェアがインストールされた2台以上のLinuxサーバ
- すべてのeDirectoryおよびNICIデータを保存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
- 仮想IPアドレス
- NetIQ eDirectory 9.1以降

注: nds-cluster-configユーティリティは、eDirectoryのルートインスタンスの環境設定だけをサポートしています。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。

---

eDirectoryをインストールして設定する

1 プライマリクラスタノードとして使用するサーバにeDirectoryをインストールして、設定を行います。インストールと環境設定の手順の詳細については、「33 ページの 「nds-installユーティリティを使用してeDirectoryコンポーネントをインストールする」」を参照してください。

注

- eDirectoryを環境設定する場合、デフォルトのNCPサーバは、eDirectoryをインストールしたコンピュータのホストサーバ名になります。eDirectoryはクラスタ環境内の複数のホスト上でホストされているため、デフォルト名を使用する代わりに、クラスタに対して一意となるNCPサーバ名を指定してください。たとえば、プライマリクラスタノード上にeDirectoryを設定した場合、NCPサーバにclusterserverという名前を指定できます。
- 環境設定処理中、eDirectoryのインストールで必ず仮想IPアドレスを設定してください。クラスタ環境では、eDirectoryはシステムのIPアドレスではなく、仮想IPアドレスだけをリスンします。

---

2 eDirectoryのインストールと環境設定を実行した後、/etc/opt/novell/eDirectory/confに格納されているnds.confファイルに移動します。

3 nds.confファイルを編集して、n4u.nds.preferred-server設定の値をクラスタインストールの仮想IPアドレスに設定し、ファイルを保存して閉じます。

4 ndsstatコマンドを使って、eDirectoryのインストールを確認します。

eDirectoryはプライマリクラスタノードで稼働している必要があります。

5 クラスタマネージャを使って、共有ファイルシステムをマウントします。

6 環境設定ユーティリティを実行する前に、次のディレクトリ内のすべてのデータをバックアップします。

- /var/opt/novell/nici
- /var/opt/novell/eDirectory/data (n4u.server.vardir)
- /var/opt/novell/eDirectory/data/dib (n4u.nds.dibdir)
- /etc/opt/novell/eDirectory/conf (n4u.server.configdir)
- /var/opt/novell/eDirectory /log

注: デフォルト以外の場所にeDirectoryをインストールする場合、ndsconfig getコマンドを使って、インストールで使われたvardirやdirパスを検索できます。nds.confはデフォルトの場所 (/etc/opt/novell/eDirectory/conf/nds.conf) に配置する必要があります。

---

7 プライマリクラスタノードサーバで端末を開き、次のコマンドを実行して、eDirectoryサービスを停止します。

```
ndsmanage stopall
```

8 端末で環境設定ユーティリティnds-cluster-configの場所に移動します。 このユーティリティは、/opt/novell/eDirectory/binディレクトリにあります。

9 次のコマンドを実行します。

```
nds-cluster-config -s /<sharedfilesystem>
```

ここで、<*sharedfilesystem*>は、eDirectory共有クラスタデータに使用する場所を指しています。

注: -uオプションを使って、ユーティリティを無人モードで実行することもできます。このオプションを使用すると、クラスタのeDirectoryを設定するときに、ユーティリティによる確認は行われなくなります。

無人オプションを使用する場合、-sオプションを併せて使用し、共有クラスタファイルシステムを指定する必要があります。

---

10 クラスタ共有ストレージが有効であることをユーティリティが確認した後、［**y**］をクリックして、クラスタの環境設定を続行します。

環境設定ユーティリティは、先に示したディレクトリ内のデータを、共有ファイルシステムの次の場所に移動します。

- <*sharedfilesystem*>/nici
- <*sharedfilesystem*>/data
- <*sharedfilesystem*>/data/
- <*sharedfilesystem*>/conf
- <*sharedfilesystem*>/log

11 次のコマンドを実行して、eDirectoryサービスを開始します。

```
ndsmanage startall
```

12 ndsstatを使って、eDirectoryの状態を確認します。eDirectoryサービスは稼働している必要があります。

13 次のコマンドを実行して、eDirectoryサービスを停止します。

```
ndsmanage stopall
```

14 クラスタのセカンダリノードとして、使用するサーバにログインします。

15 クラスタマネージャを使って、共有ストレージをセカンダリノードに移動します。

16 プライマリクラスタノードにインストールしたバージョンと同じeDirectoryのバージョンを、セカンダリクラスタノードにインストールします。ただし、eDirectoryは設定しないでください。

17 端末で、セカンダリノードの環境設定ユーティリティの場所に移動します。このユーティリティは、/opt/novell/eDirectory/binディレクトリにあります。

18 端末を開き、次のコマンドを実行します。

```
nds-cluster-config -s /<sharedfilesystem>
```

ここで、<*sharedfilesystem*>は、クラスタ共有ストレージを指しています。<*sharedfilesystem*>のパスは、プライマリノードの設定時に指定したパスの場所と同じにしてください。

nds-cluster-configユーティリティは、セカンダリクラスタノードを、共有クラスタファイルシステム上に格納されている共有eDirectoryデータにリンクします。

19 次のコマンドを実行して、eDirectoryサービスを開始します。

```
ndsmanage startall
```

ndsstatコマンドを使って、eDirectoryの状態を確認します。

20 ndsmanage stopallコマンドを実行して、セカンダリノード上のeDirectoryサービスを停止します。

21 クラスタの両方のノード上でeDirectoryを正常に環境設定した後、次のコマンドを使って、各ノード上のNDSDサービスのスタートアップモードを変更する必要があります。

```
chkconfig -d ndsd
```

22 環境設定ユーティリティで2番目のノードの環境設定が終了した後、クラスタマネージャを使って、eDirectoryサービスをクラスタに追加できます。

Linuxでのクラスタサービスの詳細については、次のマニュアルを参照してください。

- SUSE Linux Enterprise Server (SLES 12以降)
- SLES 11 SP4

重要: 2台以上のノードが同じDIBを同時にアクセスしていないことをクラスタマネージャがチェックするのが、理想的です。ただし、ユーザが2台以上のクラスタノードから同時にNDSDが実行されないことを確認する必要があります。これは、2台以上のノードを介して同じDIBにアクセスすると、DIBの破損につながるからです。

クラスタ化したLinux環境でSNMPサーバを設定する

1 すべてのノード上でsnmpd.confファイルを変更します。詳細については、『「NetIQ eDirectory管理ガイド」』の「*eDirectoryのSNMPサービスのインストールと設定*」を参照してください。

2 ndssnmpsaを起動します。

3 ［パスワードを保存しますか］オプションに「Yes」を選択します。

4 SNMPサービスを開始するには、次のいずれかの操作を実行します。

- /etc/init.d/ndssnmpsa startをpost_ndsd_startスクリプトに追加し、/etc/init.d/ndssnmpsa stopをpre_ndsd_stopスクリプトに追加します。
- eDirectoryリソースに依存するクラスタリソースとしてndssnmpsaを追加します。

注: eDirectoryは仮想IPアドレスをリスンしているため、トラップにはホストのIPアドレスが設定されます。これはエージェントのIPアドレスになります。

WindowsでのeDirectoryサービスのクラスタリング

このセクションでは、Windowsの高可用性(HA)クラスタリングを使用して、eDirectory 9.2を環境設定する方法について説明します。

- 143 ページの 「前提条件」
- 143 ページの 「eDirectoryをインストールして設定する」
- 145 ページの 「クラスタ化したWindows環境でSNMPサーバを設定する」

前提条件

- クラスタリングソフトウェアをインストールした2台以上のWindowsサーバ
- 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
- 仮想IPアドレス
- NetIQ eDirectory 9.2

eDirectoryをインストールして設定する

1 プライマリクラスタノードとして使用するサーバにeDirectoryをインストールして、設定を行います。インストールと環境設定の手順の詳細については、「62 ページの 「Windowsサーバで eDirectory 9.2をインストールまたは更新する」」を参照してください。

2 クラスタマネージャを使って、共有ボリュームをマウントします。

3 環境設定ユーティリティを実行する前に、すべてのDIBファイルとNICIデータをバックアップします。

4 プライマリクラスタノードで端末を開き、NDSCons.exeユーティリティに移動します。このユーティリティは、デフォルトでは*<eDirectoryのインストールフォルダ>*フォルダにあります。

5 端末で次のコマンドを実行します。

```
NDSCons.exe
```

6 NDSConsユーティリティで［**シャットダウン**］をクリックして、すべてのeDirectoryサービスを停止します。

7 「**Yes**」をクリックして確認します。

8 端末で環境設定ユーティリティdsclusterconfig.exeの場所に移動します。 このユーティリティは、デフォルトでは<eDirectoryのインストールフォルダ>フォルダにあります。

9 次のコマンドを実行します。

```
dsclusterconfig.exe -s /<sharedfilesystem>
```

ここで、<*sharedfilesystem*>は、eDirectory共有クラスタデータに使用する場所を指しています。

注

- -sと-uオプションを使って、無人モードでユーティリティを実行することもできます。
- プライマリクラスタノードにマウントされている共有ドライブ内のフォルダを指定する必要があります。ドライブ名だけを指定することはできません。たとえば、E:を指定するのではなく、E:\Novellを指定する必要があります。

---

10 クラスタ共有ストレージが有効であることをユーティリティが確認した後、［**y**］をクリックして、クラスタの環境設定を続行します。

環境設定ユーティリティは、先に示したディレクトリ内のデータを、共有ファイルシステムの次の場所に移動します。

- <*sharedfilesystem*>/nici
- <*sharedfilesystem*>/Files

共有ファイルシステムへのeDirectoryデータの移動に加え、ユーティリティはeDirectoryサービスのレジストリキーを共有ボリュームにコピーし、キーをndsConfigKeyファイルとして保存します。

また、プライマリノードコンピュータのNDSServerサービスの［起動のタイプ］を、［自動］から［手動］に変更します。

11 NDSConsユーティリティで［**起動**］をクリックすると、すべてのeDirectoryサービスが起動します。

12 すべてのeDirectoryサービスが実行されていることを確認し、NDSConsユーティリティを使って、サービスをもう一度停止します。

13 NDSConsユーティリティを終了します。

14 クラスタのセカンダリノードとして、使用するサーバにログインします。

15 クラスタマネージャを使って、共有ストレージをセカンダリノードに移動します。

16 eDirectoryインストーラを使って、セカンダリノードで無人インストールを実行します。インストールのモードが「Install」であることを確認します。

17 端末で、セカンダリノードの環境設定ユーティリティの場所に移動します。このユーティリティは、デフォルトではeDirectoryのインストールフォルダにあります。

18 次のコマンドを実行します。

```
dsclusterconfig.exe -s /<sharedfilesystem>
```

ここで、<*sharedfilesystem*>は、クラスタ共有ストレージを指しています。<*sharedfilesystem*>のパスは、プライマリノードの設定時に指定したパスの場所と同じにしてください。

19 dsclusterconfigユーティリティはセカンダリクラスタノードのレジストリを、共有クラスタファイルシステム上に格納されている共有eDirectoryデータに更新します。

20 環境設定ユーティリティによるセカンダリノードの環境設定が終了したら、NDSConsユーティリティを実行します。

21 NDSConsユーティリティで［**起動**］をクリックします。

22 「**Yes**」をクリックして確認します。

23 NDSConsがすべてのeDirectoryサービスを開始したら、eDirectoryを確認し、［シャットダウン］をクリックします。

24 ［Yes］をクリックして確認します。

25 クラスタリソースグループでeDirectoryを設定するには、eDirectoryに使用するリソースグループで新しいリソースを作成します。

次の詳細情報を提供する必要があります。

- リソースタイプ-汎用サービス
- 依存先-リソースグループのIPアドレスと共有ディスク
- サービス名- NDS Server0
- 起動パラメータなし
- レジストリキー-SYSTEM\CurrentControlSet\Services\NDS Server0

注: 2台以上のノードが同じDIBを同時にアクセスしていないことをクラスタマネージャがチェックするのが、理想的です。ただし、ユーザが2台以上のクラスタノードから同時にNDSDが実行されないことを確認する必要があります。これは、2台以上のノードを介して同じDIBにアクセスすると、DIBの破損につながるからです。

クラスタ化したWindows環境でSNMPサーバを設定する

1 プライマリクラスタノードで、マスタエージェントを設定し、自動化する起動タイプを設定します。詳細については、『「NetIQeDirectory管理ガイド」』の「*eDirectoryのSNMPサービスのインストールと設定*」を参照してください。

2 パスワードの入力を求めるプロンプトが表示されたら、eDirectoryパスワードを保存します。

3 サブエージェントを起動します。

4 他のノードでステップ 1～ステップ 3を実行します。

クラスタ化環境のトラブルシューティング

クラスタ化ノードのeDirectoryを修復またはアップグレードする

任意のクラスタノードで修復またはアップグレードを実行した場合、自動フェールオーバが発生しないように、他のクラスタノードを一時停止またはスタンバイ状態にする必要があります。

Windowsレジストリキーの作成

Windowsのクラスタ環境での環境設定処理の一部として、環境設定ユーティリティは、クラスタ共有ファイルシステムでレジストリキーHKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NDS Server0\ImagePathを自動作成します。eDirectoryはクラスタノード上でx86 NDS Serverサービスを開始するため、このレジストリキーを必要とします。

ユーティリティでこのレジストリキーが作成できず、環境設定中にエラーメッセージが返された場合は、完了設定ユーティリティが環境設定を正常に完了したように見える場合でも、レジストリエディタを使って、すべてのクラスタノードでレジストリキーを手動作成する必要があります。

すべてのノードで次のレジストリキーを作成します。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NDS Server0\ImagePath
```

ImagePathキーに次の値を割り当てます。

"<*primarynodeinstallfolder*>\NDS\ndsserv.exe" /DataDir="<*sharedstorage*>\Files" ds

ここで、<*primarynodeinstallfolder*>は、プライマリノードにeDirectoryをインストールしたフォルダで、<*sharedstorage*>は、共有ファイルシステムの場所へのパスです。

環境設定ユーティリティのオプション

環境設定ユーティリティで使用可能なオプションを次に示します。

<*configuration utility*> [-h] [-u] [-s /<*sharedfilesystem*>]

ここで、<*configuration utility*>は、プラットフォームによってnds-cluster-configかdsclusterconfig.exeのいずれかになります。<*sharedfilesystem*>は、eDirectory共有クラスタデータに使用する場所を指しています。

パラメータ	説明
-h	環境設定ユーティリティのヘルプを表示します。
-s	クラスタの共有ディレクトリパスを指定します。
-u	ユーティリティがクラスタ上のeDirectoryの環境設定を無人モードで実行できるようにします。 -uオプションを使ってユーティリティを実行した場合、-sオプションも併せて使用し、共有ディレクトリパスを指定してください。次に例を示します。 nds-cluster-config -u -s <*sharedfilesystem*>

14 NetIQ eDirectoryのアンインストール

この章では、次の情報について説明します。

WindowsのeDirectoryをアンインストールする

Windowsの［コントロールパネル］を使用して、WindowsサーバからeDirectory、ConsoleOne、SLP DA、およびNICIを削除します。

重要: eDirectoryを削除すると、ロールフォワードログディレクトリおよびそれに含まれるすべてのログも削除されます。このサーバのeDirectoryの復元にログを使用する予定がある場合は、eDirectoryを削除する前にロールフォワードログを別の場所にコピーする必要があります。ロールフォワードログの詳細については、『「NetIQ eDirectory管理ガイド」』の「*ロールフォワードログを使用する*」を参照してください。

注: iMonitorを使用して作成したHTMLファイルは削除されません。iMonitorを使って作成したHTMLファイルは、eDirectoryを削除する前に、*<インストールディレクトリ>*\novell\NDS\ndsimon\dsreportsから手動で削除してください。

---

eDirectory、ConsoleOne、およびSLP DAのアンインストール

1. eDirectoryがインストールされているWindowsサーバで、［**スタート**］>［**設定**］>［**コントロールパネル**］>［**プログラムの追加と削除**］の順に選択します。
2. リストから［**eDirectory**］、［**ConsoleOne**］、または［**SLPディレクトリエージェント**］を選択し、［**追加と削除**］をクリックします。
3. 選択したアプリケーションの削除を確認するメッセージが表示されたら、「**Yes**」をクリックします。

   インストールウィザードによって、該当するプログラムがサーバから削除されます。

eDirectoryの無人アンインストール

WindowsのeDirectoryの無人アンインストールでは、無人アンインストールを円滑に実行できるように、事前定義されたテキストファイルが使用されます。eDirectoryの無人アンインストールモードを使うことで、以下の操作を実行できます。

- インストールしたeDirectoryの環境設定の解除。
- eDirectoryスタンドアロンアンインストール。
- eDirectoryのアンインストールと設定解除の両方。

以下の節では、eDirectoryの無人アンインストールのさまざまな機能について説明します。

- 148 ページの 「レスポンスファイル」
- 148 ページの 「remove.rspファイルのセクションとキー」
- 149 ページの 「自動アンインストールに機能を追加する」
- 150 ページの 「環境設定ファイルの変更の削除」
- 150 ページの 「レスポンスファイルを使用したeDirectoryの無人アンインストール」

レスポンスファイル

Windowsオペレーティングシステムのeディレクトリのアンインストールは、レスポンスファイル(remove.rsp)を使って、以下のタスクを実行することで、サイレントでかつ柔軟に実行することができます。

- 必要なすべてのユーザ入力が用意された完全無人アンインストール
- コンポーネントのデフォルト設定
- インストール中のすべてのプロンプトのバイパス

レスポンスファイルとは、Windows.iniファイルのようなセクションとキーが記述されているテキストファイルです。任意のASCIIテキストエディタを使って、レスポンスファイルの作成と編集ができます。eDirectoryはレスポンスファイルから直接アンインストールパラメータを読み取り、デフォルトのインストール値をレスポンスファイルの値に置き換えます。アンインストールプログラムは、レスポンスファイルからの値を受け入れ、プロンプトを表示せずにアンインストールを続行します。

remove.rspファイルのセクションとキー

eDirectoryのアンインストールでは、レスポンスファイル内のセクションを変更し、ツリー名、管理コンテキスト、管理者資格情報(ユーザ名やパスワード)などの情報を追加する必要があります。キーとそのデフォルト値の全リストは、eDirectoryのインストール時に提供されるサンプルのremove.rspファイルから入手できます。

注: eDirectoryインストール内のeDirectory\windows\x64\NDSonNT\remove.rspにあるremove.rspファイルを使用する必要があります。必須パラメータはデフォルトで、このファイルで設定されます。remove.rsp ファイルを編集するとき、キーと値のペアを結ぶ等号記号(「=」)の前後にスペースが入らないようにしてください。

無人アンインストールで使用するremove.rspファイルに管理者ユーザ資格情報を入力します。このため、管理者資格情報が漏洩しないように、アンインストール後はファイルを完全に削除してください。

自動アンインストールに機能を追加する

eDirectoryアンインストーラの細かな設定はほとんど、手動アンインストールのデフォルト設定になっています。ただし、無人アンインストール中、各環境設定パラメータを明示的に設定する必要があります。このセクションでは、設定を解除する基本設定について説明します。

eDirectoryサーバの詳細情報

アンインストールするサーバの詳細を、アンインストーラに提供してください。この情報のほとんどは、3つのタグ[Novell:NDSforNT:1.0.0]、[Initialization]、および[Selected Nodes]で設定されます。

remove.rspの[Initialization]および [Selected Nodes]で指定されているすべての値をそのまま使用してください。

[Novell:NDSforNT:1.0.0]

Tree Name: サーバがアンインストールされるツリーの名前。

Admin Login Name: 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名前(RDN)。ツリー内のすべての操作は、このユーザとして実行されます。

Admin Context: ツリーに追加されたユーザにはユーザオブジェクトがあり、そこにユーザ固有の詳細情報がすべて入っています。このパラメータは、管理者オブジェクトの追加先となるツリーのコンテナオブジェクトです。プライマリサーバのインストールでは、このコンテナはサーバオブジェクトと共に作成されます。

Admin Password: 前述のパラメータで作成された管理者オブジェクトのパスワード。このパスワードは、プライマリサーバのインストール時に管理者オブジェクトに対して設定されます。セカンダリサーバのインストールでは、これは新しいサーバの追加先となるコンテキストに対して権限を持っているプライマリサーバの管理者オブジェクトのパスワードである必要があります。

NDS Location: ライブラリとバイナリがコピーされる、ローカルシステムのeDirectoryのインストール場所。レスポンスファイルで変更されていない限り、eDirectoryはデフォルトでC:\Novell\NDSにインストールされます。

DataDir: eDirectoryバージョン9.2までは、DIBはNDSロケーション内にサブフォルダとしてインストールされていました。後に、管理者が別のDIBロケーションを指定するオプションが追加されました。これは、DIBに保存されるデータが多くなりすぎてNDSロケーションに収まらなくなる可能性があるためです。現在デフォルトでは、DIBはNDSロケーション内のFilesサブフォルダにインストールされますが、管理者はこのパラメータを変更して別の場所を指定することができます。

mode: eDirectoryのセットアップタイプ。セットアップには、次の3つのタイプがあります。

- deconfigure: eDirectoryの環境設定解除を実行します。
- uninstall: eDirectoryのアンインストールを実行します。
- full: eDirectoryの設定解除とアンインストールの両方を実行します。

注: 無人インストール時にフルセットアップモードを選択すると、eDirectoryのアンインストール時に、個別の設定解除とアンインストールオプションを選択することはできません。

ConfigurationMode: modeキーで指定したセットアップを設定解除した場合、ConfigurationModeキーのRestrictNodeRemove値を変更していないことを確認してください。

Prompt: アンインストールモードのタイプは、この変数で指定する必要があります。無人アンインストールの場合、デフォルトでは「silent」に設定されます。「silent」以外の値を設定すると、通常のアンインストールが実行されます。

前述の基本パラメータをすべて記述したレスポンスファイルのテキスト例を次に示します。

```
[Novell:NDSforNT:1.0.0]

  Tree Name=SILENTCORP-TREE

  Admin Context=Novell

  Admin Login Name=Admin

  Admin Password=novell

  prompt=silent
```

環境設定ファイルの変更の削除

<Windowsインストールドライブ>\Program Files\Common Files\novell\ni\bin*にある*remove.cfgファイルを次のように変更します。

```
[PARAMETERS]0/OUTPUT_TO_FILE
```

変更後:

```
[PARAMETERS]0/OUTPUT_TO_FILE /SILENT
```

レスポンスファイルを使用したeDirectoryの無人アンインストール

編集したファイルremove.rspを*<Windowsインストールドライブ>*\Program Files\Common Files\novell\ni\dataにコピーします。

eDirectoryにインストールされたinstall.exeは、追加パラメータを指定して、コマンドラインから起動します。必要なセットアップに応じて、次のいずれかのコマンドを実行する必要があります。

設定解除

```
<Windows Installed Drive>\Program Files\Common Files\novell\ni\bin>install.exe -
remove /restrictnoderemove /nopleasewait ..\data\ip.db ..\data\remove.rsp
Novell:NDSForNT:1.0.0 0 NDSonNT
```

アンインストール

1. <Windowsドライブ>\Program Files\Common Files\novell\ni\data*ディレクトリ内にある*ip.dbファイルの名前を別の名前に変更します。
2. <Windowsドライブ>\Program Files\Common Files\novell\ni\data*フォルダの*ip_conf.dbファイルを、ip.dbにコピーします。

3 次のコマンドを実行します。

<*Windowsがインストールされているドライブ*>\Program Files\Common Files\novell\ni\bin>install.exe -remove /nopleasewait ..\data\ip.db ..\data\remove.rsp Novell:NDSForNT:1.0.0 0 NDSonNT

eDirectoryの設定解除とアンインストール

```
<Windows Installed Drive>\Program Files\Common Files\novell\ni\bin>install.exe -
remove /nopleasewait ..\data\ip.db ..\data\remove.rsp Novell:NDSForNT:1.0.0 0
NDSonNT
```

eDirectoryまたはそれに伴うセットアップのアンインストールを実行したら、次のフォルダを削除します。

- C:\Novell\NDS(デフォルトの場所、またはeDirectoryのインストールディレクトリ)
- C:\Novell\NDS\Files (デフォルトの場所、またはeDirectory DIBの格納先)
- <*Windowsがインストールされているドライブ*>:\Program Files\Common Files\Novell\ni
- <*Windowsがインストールされているドライブ*>:\Windows\system32\NDScpa.cpl

NICIのアンインストール

1 eDirectoryがインストールされているWindowsサーバで、［**スタート**］>［**設定**］>［**コントロールパネル**］>［**プログラムの追加と削除**］の順に選択します。

2 リストから［**NICI**］を選択し、［**追加と削除**］をクリックします。

3 NICIの削除を確認するメッセージが表示されたら、［**Yes**］をクリックします。

インストールウィザードによって、サーバからNICIが削除されます。

NICIをアンインストールした後、システムからNICIを完全に削除するには、C:\Windows\system32\novell\nici (32ビット)とC:\Windows\SysWOW64\novell\nici (64ビット)サブディレクトリを削除します。これらを削除するには、いくつかのファイルおよびディレクトリの所有権を持っている必要がある場合があります。

警告: NICIサブディレクトリの削除後は、以前にNICIで暗号かされたすべてのデータまたは情報が失われます。

Microsoft Visual C++ 2005とVisual C++ 2012のランタイムライブラリのアンインストール

Microsoft Visual C++ 2005とMicrosoft Visual C++ 2012のランタイムライブラリがeDirectory以外の製品で使用されていない場合は、次の手順を使用してそれらのランライムライブラリをアンインストールしてください。

1 eDirectoryがインストールされているWindowsサーバの［*プログラムの追加と削除*］または［**プログラムと機能**］に移動します。

2 次の再配布パッケージを削除します。

Microsoft Visual C++ 2012再配布可能モジュールとMicrosoft Visual C++ 2005再配布可能パッケージ (x64)

Linux上でのeDirectoryのアンインストール

Linuxコンピュータからeディレクトリコンポーネントをアンインストールするには、nds-uninstallユーティリティを使用します。このユーティリティはローカルホストからeDirectoryをアンインストールします。nds-uninstallを実行する前に、eDirectoryサーバの設定を解除してください。ndsconfig rm -a <*admin FDN*>を実行して、eDirectoryサーバを削除します。このユーティリティは、/opt/novell/eDirectory/sbin/nds-uninstallで入手できます。

ndsconfig rmをOESサーバ上で実行しないでください。

重要: eDirectoryを削除すると、ロールフォワードログディレクトリおよびそれに含まれるすべてのログも削除されます。このサーバのeDirectoryの復元にログを使用する予定がある場合は、eDirectoryを削除する前にロールフォワードログを別の場所にコピーする必要があります。ロールフォワードログの詳細については、『「NetIQ eDirectory管理ガイド」』の「*ロールフォワードログを使用する*」を参照してください。

---

1. nds-uninstallコマンドを実行します。
2. 使用する構文は次のとおりです。

   ```
   nds-uninstall [-s][-h]
   ```

   コマンドラインに必要なパラメータを入力していない場合、パラメータを要求するプロンプトがnds-installユーティリティに表示されます。

パラメータ	説明
-h	ヘルプを表示します。
-s	インスタンスが設定されている場合でも、eDirectoryパッケージとバイナリを削除します。ただし、このオプションではDIBディレクトリおよびNDS環境設定ファイルは削除されません。 **重要:** このオプションを使用した場合、他のサービスに長時間影響を与えないことを確認してください。

nds-uninstallでは、次のパッケージはアンインストールされません。

パッケージ	削除されない理由
NICIパッケージ	NICIは次のいずれかで使用されている可能性があります。 ◆ その他の製品 ◆ 任意の場所にインストールされたeDirectory ◆ 非ルートユーザによってインストールされたeDirectory
NOVLsubag	NOVLsubagは次のいずれかで使用されている可能性があります。 ◆ 任意の場所にインストールされたeDirectory ◆ 非ルートユーザによってインストールされたeDirectory

Linux上でのeDirectoryの無人アンインストール

1 eDirectoryのインスタンスの削除:

```
ndsconfig rm -a <user name> -w passwd -c
```

2 eDirectoryの設定解除用自動化スクリプトで次のどちらかを使用します。

環境変数からパスワードを渡す場合: ndsconfig rm -a <*ユーザ名*> -w env:<*環境変数*> -c

ファイルからパスワードを渡す場合: ndsconfig rm -a <*ユーザ名*> -w file:<*絶対パス/相対パスで指定したファイル名*> -c

3 (オプション)複数インスタンスの場合、インスタンスごとに次のコマンドを実行します。

```
ndsconfig rm -a <user name> -w passwd  --config-file <absolute path for configuration file>
```

次に例を示します。

```
ndsconfig rm -a admin.novell -w n -c
```

```
ndsconfig rm -a admin.novell -w env:ADM_PASWD -c
```

```
ndsconfig rm -a admin.novell -w file:/Builds/88SP8/adm_paswd -c
```

4 eDirectoryパッケージをアンインストールするには、nds-uninstallスクリプトを実行して、eDirectoryパッケージを削除します。

```
nds-uninstall -u
```

eDirectoryのアンインストールに関する注意

eDirectoryをアンインストールし、再インストールする場合、eDirectoryサーバからネットワーク内の他のサーバにアクセスすることはできません。レプリカがeDirectoryサーバ内に存在するパーティションに対して、同期化や破損通知など、分散型操作を実行することはできません。この状態がしばらく続く場合、すべてのサーバやサーバ上で実行されている処理が影響を受けることがあります。

eDirectoryの新しいバージョンをアンインストールして、以前のバージョンをインストールすることはしないでください。これには次の理由があります。

- スキーマ関連のアップグレードは元に戻りません。
- DIBを新しいバージョンにアップグレードされている場合、eDirectoryが機能しないことがあります。
- nds.confを除き、既存の環境設定ファイルがすべて削除されます。

ただし、eDirectoryの新しいバージョンをアンインストールし、以前のバージョンをインストールする場合、以下の点を考慮してください。

- DIBを新しいバージョンにアップグレードします。DIBをアップグレードしないと、eDirectoryは機能しないことがあります。
- nds.confを除く既存の環境設定ファイルをバックアップし、eDirectoryを再インストールしたときに復元します。
- スキーマ関連のアップグレードは元に戻りません。

A NetIQ eDirectory用のLinuxパッケージ

NetIQ eDirectoryには、Linuxパッケージシステムが含まれています。このパッケージは、さまざまなeDirectoryコンポーネントのインストールとアンインストールを容易にするツールをまとめたものです。パッケージには、特定のeDirectoryコンポーネントの構築に必要な条件を示したMakefileが含まれています。パッケージには、OSと一緒にインストールされた標準のLinuxツールで使用される環境設定ファイル、ユーティリティ、ライブラリ、デーモン、およびマニュアルページも含まれています。

下の表に、NetIQ eDirectoryに含まれているLinuxパッケージに関する情報を示します。

注: Linuxでは、すべてのパッケージの先頭に*novell-*というプレフィックスが追加されます(**eba**を除く)。たとえば、NDSservはnovell-NDSservとなります。

パッケージ	説明
NOVLice	NetIQインポート/エクスポート変換ユーティリティが含まれています。NOVLlmgnt、NOVLxis、およびNLDAPbaseの各パッケージに依存します。
NDSbase	ディレクトリユーザエージェントを表します。このパッケージはNICIパッケージに依存しています。 NDSbaseには、以下のものが含まれています。 ◆ eDirectoryに必要なRSA認証を格納する認証ツールボックス ◆ プラットフォーム独立システム抽象ライブラリ、すべての定義済みディレクトリユーザエージェント機能を格納するライブラリ、およびスキーマ拡張ライブラリ ◆ 統合設定ユーティリティおよびディレクトリユーザエージェントテストユーティリティ ◆ eDirectory環境設定ファイルおよびマニュアルページ
NDScommon	eDirectory環境設定ファイルのマニュアルページと、インストールおよびアンインストールユーティリティが含まれています。このパッケージはDNSbaseパッケージに依存しています。
NDSmasv	必須アクセスコントロールサービス(MASV)に必要なライブラリが含まれています。

パッケージ	説明
NDSserv	eDirectoryサーバが必要とするすべてのバイナリとライブラリが含まれています。また、システム上のeDirectoryサーバを管理するユーティリティも含まれています。このパッケージはNDSbase、NDScommon、NDSmasv、NLDAPsdk、NOVLpkia、およびNOVLpkitの各パッケージに依存しています。 NDSservパッケージには次のものが含まれています。 ◆ NDSインストールライブラリ、FLAIMライブラリ、トレースライブラリ、NDSライブラリ、LDAPサーバライブラリ、LDAPインストールライブラリ、インデックスエディタライブラリ、DNSライブラリ、マージライブラリ、およびLDAP SDK用LDAP拡張ライブラリ ◆ eDirectoryサーバデーモン ◆ DNS用バイナリ、およびLDAPのロード/アンロード用バイナリ ◆ MACアドレスの作成に必要なユーティリティ、サーバの追跡およびサーバの一部のグローバル変数の変更用ユーティリティ、eDirectoryのバックアップと復元用ユーティリティ、およびeDirectoryツリーのマージユーティリティ ◆ DNS、NDSD、およびNLDAPの起動スクリプト ◆ マニュアルページ
NDSimon	eDirectoryサービスからのデータの検索および取得に使用される、ランタイムライブラリおよびユーティリティが含まれています。このパッケージはDNSbaseパッケージに依存しています。
NDSrepair	eDirectoryデータベースの問題を修正する、ランタイムライブラリおよびユーティリティが含まれています。このパッケージはDNSbaseパッケージに依存しています。
NLDAPbase	LDAPライブラリ、LDAPライブラリの拡張、および次のLDAPツールが含まれています。 ◆ ldapdelete ◆ ldapmodify ◆ ldapmodrdn ◆ ldapsearch このパッケージはNLDAPsdkパッケージに依存しています。
NOVLnmas	NMASサーバが必要とする、すべてのNMASライブラリとnmasinstバイナリが含まれています。このパッケージは、NICIおよびNDSmasvのパッケージに依存しています。
NLDAPsdk	LDAPランタイムとセキュリティライブラリ(Client NICI)に対するNetIQ 拡張が含まれています。
NOVLsubag	eDirectory SNMPサブエージェント用のランタイムライブラリおよびユーティリティが含まれています。このパッケージは、NICI、NDSbase、およびNLDAPbaseの各パッケージに依存しています。
NOVLpkit	eDirectoryを必要としないPKIサービスを提供します。このパッケージは、NICIとNLDAPsdkのパッケージに依存しています。
NOVLpkis	PKIサーバサービスを提供します。このパッケージは、NICI、NDSbase、およびNLDAPsdkの各パッケージに依存しています。

パッケージ	説明
NOVLsnmp	SNMP用のランタイムライブラリおよびユーティリティです。このパッケージはNICIパッケージに依存しています。
NDSdexvnt	NetIQ eDirectoryで生成された、他のデータベースに対するイベントを管理するライブラリが含まれています。
NOVLpkia	PKIサービスを提供します。このパッケージは、NICI、NDSbase、およびNLDAPsdkの各パッケージに依存しています。
NOVLembox	eMBoxインフラストラクチャおよびeMToolを提供します。
NOVLlmgnt	NetIQ Language Managementのランタイムライブラリが含まれています。
NOVLxis	NetIQ XIS用ランタイムライブラリが含まれています。
NOVLsas	NetIQ SASライブラリが含まれています。
NOVLntls	NetIQ TLSライブラリが含まれています。 Linux上では、このパッケージはntlsです。
NOVLldif2	NetIQ Offline Bulkloadユーティリティが含まれています。NDSbase、NDSserv、NOVLntls、NOVLlmgnt、およびNICIの各パッケージに依存しています。
NOVLncp	NetIQ Encrypted NCP Services for Linuxが含まれています。このパッケージはNDScommonパッケージに依存します。
novell-eba	拡張バックグラウンド認証をサポートするためのライブラリが含まれています。このパッケージは、NICI、NDSbase、およびNDSServの各パッケージに依存しています。

B eDirectoryヘルスチェック

NetIQ eDirectory 9.2は、使用しているeDirectoryのヘルスが安全かどうかを特定できるようにする診断ツールを提供します。このツールの主な用途は、アップグレード前にサーバの状態をチェックすることです。

eDirectoryヘルスチェックはデフォルトでアップグレードの実行時に必ず実行されます。実際のパッケージアップグレードが開始される前に実行されます。診断ツールndscheckは、ヘルスチェックを確認するために、いつでも実行できます。

ヘルスチェックの必要性

eDirectoryの以前のリリースでは、アップグレードを進める前にサーバの状態はチェックされませんでした。状態が不安定であると、アップグレード処理が失敗し、eDirectoryは不整合な状態になってしまいます。場合によっては、アップグレード前の設定に戻すことができない場合もあります。

新しいヘルスチェックツールによってこの問題が解決され、サーバをアップグレードする準備を確実に整えることができます。

ヘルスチェックの実行

eDirectoryヘルスチェックは2とおりの方法で実行できます。

注: ヘルスチェックユーティリティを実行するには、管理者の権利を持っている必要があります。

- 159 ページの 「アップグレードと同時に実行」
- 160 ページの 「スタンドアロンユーティリティとして実行」

アップグレードと同時に実行

eDirectoryをアップグレードするときは常に、デフォルトでヘルスチェックが実行されます。

Linux

アップグレード時には常にデフォルトで、実際のアップグレード処理が開始される前にヘルスチェックが実行されます。

デフォルトのヘルスチェックをスキップするには、-jオプションを指定してnds-installを実行します。

Windows

eDirectoryヘルスチェックは、インストールウィザードの一部として実行されます。ヘルスチェックは、プロンプトが表示されたときに有効または無効にすることができます。

スタンドアロンユーティリティとして実行

eDirectoryヘルスチェックはいつでも好きなときにスタンドアロンユーティリティとして実行できます。次の表に、プラットフォームごとのヘルスチェックユーティリティ名を示します。

表 B-1 *ヘルスチェックユーティリティ*

プラットフォーム	ユーティリティ名
Linux	ndscheck 構文: `ndscheck [--help | -?] Display command usage ndscheck [--version | -v] Display version information ndscheck [-h <hostname port>] [-a <admin FDN>] [-F <log file>] [-D] [-q] [--config-file <file name>]`
Windows	ndscheck 構文: `ndscheck [--help | -?] Display command usage ndscheck [--version | -v] Display version information ndscheck [-h <hostname port>] [-a <admin FDN>] [-F <log file>] [-D] [-q] [--config-file <file name>]`

ヘルスチェックのタイプ

ndscheckユーティリティを実行またはアップグレードすると、次のタイプのヘルスチェックが実行されます。

- 基本的なサーバの状態
- パーティションとレプリカの状態

ndscheckユーティリティを実行すると、その結果が画面に表示され、ndscheck.logに記録されます。ログファイルの詳細については、「162 ページの 「ログファイル」」を参照してください。

アップグレードの一部としてヘルスチェックを実行した場合、エラーが検出されると、検出されたエラーのタイプに応じて、アップグレードを続行するかどうかの確認が求められるか、または処理が中断されます。エラーの種類については、「161 ページの 「状態のカテゴリ」」で説明します。

基本的なサーバの状態

これは、ヘルスチェックの最初の段階です。ヘルスチェックユーティリティは次の内容をチェックします。

1. eDirectoryサービスが動作している。DIBが開いていて、ツリー名などの基本的なツリー情報を読むことができる。
2. サーバがそれぞれのポート番号を監視している。

LDAPに関しては、TCPポート番号とSSLポート番号を取得して、サーバがこれらのポートを監視しているかどうかをチェックします。

同様に、HTTPセキュアポート番号とHTTPSセキュアポート番号を取得して、サーバがこれらのポートを監視しているかどうかをチェックします。

パーティションとレプリカの状態

基本的なサーバの状態のチェック後は、次のとおり、パーティションとレプリカの状態をチェックします。

1. ローカルに保持されているパーティションのレプリカの状態をチェックします。
2. サーバによって保持されているすべてのパーティションのレプリカリングを読み込み、レプリカリング内のすべてのサーバが動作していて、すべてのレプリカが使用可能な状態であることをチェックします。
3. レプリカリング内のすべてのサーバの時刻同期をチェックし、サーバ間の時刻の違いを表示します。

状態のカテゴリ

eDirectoryサーバのヘルスチェック中に検出されたエラーに応じて、ヘルスには3つの潜在的なカテゴリがあります。

- (161 ページ) 正常
- (161 ページ) 警告
- (162 ページ) 重大

ヘルスチェックの状態は、ログファイルに記録されます。詳細については、「162 ページの 「ログファイル」」を参照してください。

正常

すべてのヘルスチェックに成功し、サーバの状態は正常です。

アップグレードは中断されずに続行されます。

警告

サーバの状態のチェック中に、あまり重大でないエラーが検出されました。

アップグレードの一部としてヘルスチェックが実行されている場合、中止するか続行するかの確認を求められます。

警告は通常、次の状況で発生します。

- サーバがLDAPポートとHTTPポート(通常、セキュリティ保護、または両方)を監視していない。
- レプリカリング内のいずれの非マスタサーバにも接続できない。
- レプリカリング内のサーバが同期していない。

重大

eDirectoryのヘルスチェック中に重大エラーが検出されました。

ヘルスチェックがeDirectoryアップグレードの一部として実行されている場合、アップグレード操作は破棄されます。

重大な状態は通常、次の状況で発生します。

- DIBを開くことができないか読み込むことができない(ロックされているか破損している可能性がある)。
- レプリカリング内のすべてのサーバに接続できない。
- ローカルに保持されているパーティションが使用中である。
- レプリカが使用可能な状態ではない。

ログファイル

アップグレード時に実行するか、スタンドアロンユーティリティとして実行するかかかわらず、eDirectoryヘルスチェック操作を実行するたびに、ヘルスの状態がログファイルに記録されます。

ログファイルの内容は、チェック実行時に画面に表示されるメッセージと同様です。

ヘルスチェックのログファイルには、次のものが含まれています。

- ヘルスチェックのステータス(正常、警告、または重大)。
- 考えられる解決方法を示すURL。
  - サポートフォーラム (http://forums.novell.com/netiq/netiq-product-discussion-forums/edirectory/)
  - ドキュメントのトラブルシューティング (https://www.netiq.com/documentation/edir88/edir88tshoot/data/bookinfo.html)
  - エラー番号 (http://www.novell.com/documentation/nwec/)
  - パッチ (http://support.novell.com/patches.html)
  - Cool Solutions (http://www.novell.com/communities/coolsolutions/edirectory)

次の表は、さまざまなプラットフォームにおけるデフォルトのログファイルの位置を示しています。

***表 B-2** ヘルスチェックのログファイルの場所*

プラットフォーム	ログファイル名	場所
Linux	ndscheck.log	1. -hオプションを指定すると、ndscheck.logファイルはユーザのホームディレクトリに保存されます。 2. --config-fileオプションを指定すると、ndscheck.logファイルはサーバインスタンスのログディレクトリに保存されます。または、インスタンスの一覧からインスタンスを選択することもできます。
Windows	nsdcheck.log	ログファイルは*install_directory*\novell nds\に保存されます。 **注:** *install_directory*は、ユーザが指定するディレクトリです。

C OpenSLP for eDirectoryの設定

この付録では、ネットワーク管理者向けに、Novell Clientが存在しないOpenSLP for NetIQ eDirectoryのインストールに関する適切な環境設定について説明します。

Service Location Protocol

OpenSLPは、IETF Service Location Protocol Version 2.0規格のオープンソースによる実装です。この規格は、IETF Request-For-Comments (RFC) 2608 (http://www.ietf.org/rfc/rfc2608.txt?number=2608)で文書化されました。

SLPv2プロトコルの実装に加え、OpenSLPソースコードが提供するインタフェースは、SLP機能にプログラム的にアクセスするためのもう1つのIETF規格を実装したもので、RFC 2614 (http://www.ietf.org/rfc/rfc2614.txt?number=2614)で文書化されています。

SLPの動作を完全に理解するため、前述の文書を読んで修得することをお勧めします。読みやすい文書ではありませんが、インターネットでのSLPの正しい設定を行うためには重要なドキュメントです。

OpenSLPプロジェクトの詳細については、OpenSLP (http://www.OpenSLP.org)のWebサイトとSourceForge (http://sourceforge.net/projects/openslp)のWebサイトを参照してください。OpenSLPのWebサイトには、環境設定に関する貴重なヒントを含んださまざまな文書があります。ただし、このガイドの作成時点では、これらのドキュメントの多くは未完成です。

SLPの基本

Service Location Protocolでは、次の3種類のコンポーネントが定義されています。

- ユーザエージェント(UA)
- サービスエージェント(SA)
- ディレクトリエージェント(DA)

ユーザエージェントは、クライアントがサービスを問い合わせたり、サービスがそれ自体を通知するためのプログラムインタフェースを提供します。ユーザエージェントはディレクトリエージェントに接続し、指定したスコープ内の指定したサービスクラスに登録されたサービスを問い合わせます。

サービスエージェントは、SLPで登録されたローカルサービスを持続的に格納し、維持する場所を提供します。サービスエージェントは主として、登録済みのローカルサービスをメモリ内データベースとして維持します。この場合、サービスはローカルSAがない限りSLPで登録できません。ク

ライアントがサービスを検出するのはUAライブラリ内のみですが、登録するにはSAが必要です。これは主に、ディレクトリエージェントを受信して登録を維持するためには、登録済みサービスの存在をSAが定期的に表明する必要があるためです。

ディレクトリエージェントは、通知されたサービスに対して長期間持続的にキャッシュを提供し、ユーザエージェントがサービスを検索するためのアクセスポイントとなります。キャッシュ機能を提供するDAは、SAが新しいサービスを通知するのを受信し、これらの通知をキャッシュします。DAのキャッシュは短時間で完了します。ディレクトリエージェントは、期限切れのアルゴリズムを使用してエントリキャッシュを有効期限切れにします。ディレクトリエージェントが起動すると、持続的な格納領域(通常はハードドライブ)からキャッシュを読み込み、アルゴリズムに従ってエントリを有効期限切れにします。新しいDAが起動したり、キャッシュが削除されると、DAはこの条件を検出して受信中のすべてのSAに特別な通知を送信します。SAは、DAが直ちにキャッシュを作成できるようにローカルデータベースをダンプします。

ディレクトリエージェントが存在しない場合、UAはSAが応答できる一般的なマルチキャスト方式のクエリを使用し、DAがキャッシュを作成するのとほぼ同じ方法で、要求されたサービスのリストを作成します。このクエリによって返されるサービスのリストは、DAが提供するリストと比較すると不完全かつ局所的です。特に、多くのネットワーク管理者が使用するマルチキャスト方式でのフィルタ処理では、ブロードキャストおよびマルチキャストの対象がローカルサブネットのみに制限されるためです。

つまり、指定されたスコープに対してユーザエージェントが検索するものは、すべてディレクトリエージェントに依存します。

NetIQ Service Location Providers

NovellのバージョンのSLPでは、強力なサービスアドバータイズ環境を提供するため、SLP標準が一部変更されます。しかし、このために一部の拡張性を犠牲にしています。

たとえば、サービスアドバータイズのフレームワークの拡張性を改善するために、サブネット上でのブロードキャストまたはマルチキャストのパケット数が制限されます。SLPの仕様では、これを管理するために、ディレクトリエージェントのクエリに関してサービスエージェントおよびユーザエージェントに制限を加えています。必要なスコープに対応するための最初に検出されたディレクトリエージェントは、サービスエージェント(つまり結果的にローカルユーザエージェント)がそのスコープ上の将来の要求すべてに使用するエージェントとなります。

NetIQ SLPを実装すると、クエリ情報の検索について既知のディレクトリエージェントをすべてスキャンします。スキャンの所要時間は300ミリ秒とかなり長く、したがって、約3〜5秒以内で10台のサーバしかスキャンできません。SLPがネットワーク上で正しく設定されている場合にはこのような検索の必要はありません。OpenSLPでは、ネットワークが実際にSLPトラフィック用に設定されていると見なされます。OpenSLPの応答タイムアウト値はNetIQのSLPサービスプロバイダの応答タイムアウト値よりも大きい値です。ディレクトリエージェント数は、エージェントの情報が正確で完全であるかどうかに関係なく、最初に応答するディレクトリエージェントに制限されます。

ユーザエージェント

ユーザエージェントの物理形式は、アプリケーションにリンクされたスタティックライブラリまたはダイナミックライブラリです。ユーザエージェントにより、アプリケーションはSLPサービスに対して問い合わせることができます。

ユーザエージェントは、アルゴリズムに従って、クエリの送信先になるディレクトリエージェントのアドレスを取得します。指定したスコープのDAアドレスを取得すると、ユーザエージェントはそのスコープから応答がなくなるまで同じアドレスを使用し続けます。応答がなくなると、ユーザエージェントはそのスコープに対する別のDAアドレスを取得します。ユーザエージェントは、指定されたスコープのディレクトリエージェントのアドレスを次の方法で検索します。

1. 現在の要求のソケットハンドルが、指定したスコープのDAに接続されているかどうかを確認する。複数の要求の場合は、すでにキャッシュ化された接続がある可能性がある。
2. 指定したスコープと一致しているDAの、既知のローカルDAキャッシュをチェックする。
3. 指定したスコープでローカルSAに対してDAを確認する(その後キャッシュに新しいアドレスを追加します)。
4. 指定したスコープに一致するDAのネットワーク設定済みのアドレスをDHCPに問い合わせる(その後キャッシュに新しいアドレスを追加します)。
5. 既知のポートでDAの検出要求をマルチキャストする(その後キャッシュに新しいアドレスを追加します)。

スコープを指定しない場合、指定スコープは「デフォルト」になります。つまり、SLP設定ファイルで静的に定義されたスコープがなく、クエリでスコープを指定していない場合は、使用されるスコープは「デフォルト」という単語になります。また、eDirectoryの登録ではeDirectoryはスコープを指定しないことに注意してください。つまり、eDirectoryで使用されるスコープは常に「デフォルト」というわけではありません。スコープが静的に設定されている場合、そのスコープがすべてのローカルUA要求およびSA登録に対して、指定したスコープがない場合のデフォルトのスコープになります。

サービスエージェント

サービスエージェントの物理形式は、ホストマシン上での個別のプロセスです。Windowsの場合は、slpd.exeがローカルマシン上のサービスとして実行されます。ユーザエージェントは、既知のポート上のループバックアドレスにメッセージを送信することによって、ローカルサービスエージェントを問い合わせます。

サービスエージェントは、潜在DAアドレスにDA検出要求を直接送信することにより、ディレクトリエージェントおよびそれがサポートするスコープリストを検出してキャッシュします。DA検出要求は、次の方法で送信されます。

1. 静的に設定されたDAアドレスをすべてチェックする(その後SAの既知のDAキャッシュに新しいDAアドレスを追加します)。
2. DHCPからDAとスコープのリストを要求する(その後SAの既知のDAキャッシュに新しいリストを追加します)。
3. 既知のポートでDAの検出要求をマルチキャストする(その後SAの既知のDAキャッシュに新しいポートを追加します)。
4. DAによって定期的にブロードキャストされたDAのアドバータイズパケットを受信する(その後SAの既知のDAキャッシュに新しいアドバータイズパケットを追加します)。

ユーザエージェントは常に最初にローカルサービスエージェントに対して問い合わせます。ローカルサービスエージェントの応答によってユーザエージェントが次の検出段階を続行するかどうかが決定されるため、このことは重要な点です(DHCPのこのケースについては、「165ページの「ユーザエージェント」」の手順3および4を参照してください)。

環境設定パラメータ

%systemroot%/slp.confファイル内の各環境設定パラメータも、次のようにしてDAの検出を制御します。

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

useScopesオプションは、SAの通知先のスコープ、および、サービスまたはクライアントアプリケーションで作成された登録またはクエリに指定したスコープが存在しない場合に、クエリが作成されるスコープを示します。eDirectoryは常にデフォルトのスコープに通知し、問い合わせを行うため、このリストがeDirectoryの登録およびクエリのデフォルトのスコープのリストになります。

DAAddressesオプションはコンマで区切られたIPアドレスのリストで、アドレスは10進数とドットで表記されます。このアドレスが他のすべてに対して優先されます。設定されたDAのこのリストが登録またはクエリのスコープをサポートしない場合、検出を無効にしていない限りは、SAおよびUAはマルチキャスト方式でDAを検出します。

passiveDADetectionオプションのデフォルトは「TRUE」です。ディレクトリエージェントは、設定に応じて定期的にそれ自体の存在をサブネットの既知のポート上にブロードキャストします。これらのパケットはDAAdvertパケットと名付けられます。このオプションに「FALSE」を設定した場合、ブロードキャスト方式のすべてのDAAdvertパケットはSAに無視されます。

activeDADetectionオプションのデフォルトも「TRUE」です。この設定により、SAはすべてのDAに対して、指示されたDAAdvertパケットで応答するように、定期的にブロードキャスト方式で要求できます。指示されたパケットはブロードキャストではありませんが、この要求に対する応答ではSAに直接送信されます。このオプションに「FALSE」を設定した場合、SAは定期的なDAの検出要求をブロードキャストしません。

DAActiveDiscoveryIntervalオプションはtry-stateパラメータです。デフォルト値は1です。これは、初期化の際に、SAがDAの検出要求を1回送る設定であることを意味する特別な値です。このオプションに0を設定すると、activeDADetectionオプションに「FALSE」を設定した場合と結果は同じです。その他の値は、検出をブロードキャストする間隔を秒数で表します。

このオプションを正しく使用すると、サービスアドバータイズに使用するネットワーク帯域幅を適切に設定できます。ただし、デフォルト設定は平均的なネットワークで拡張性を最適化するように設計されています。

D 問題のトラブルシューティング

このセクションでは、eDirectoryのインストールおよび設定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。

インストール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。

問題	推奨されるアクション
インストールに長い時間がかかる. eDirectoryを既存のツリーにインストールする場合に、インストールの完了までに長時間かかるときは、サーバのdstrace画面を確認してください。「-625 トランスポートできません」というメッセージが表示された場合は、アドレスキャッシュをリセットする必要があります。	アドレスキャッシュをリセットするには、システムコンソールで次のコマンドを入力します。 `set dstrace = *A`
コンテナ管理者のeDirectoryインストールの失敗 eDirectory 9.0のインストールプログラムでは、サーバが格納されているコンテナのスーパバイザ権を持つ管理者によるインストールがサポートされています。これを実行するには、eDirectory 9.0をインストールする最初のサーバにスキーマを拡張する[Root]のスーパバイザ権がある必要があります。この点から、後続のサーバには［Root］のスーパバイザ権は必要ありません。ただし、eDirectory 9.0では、最初にeDirectory 9.0がインストールされているプラットフォームによっては一部のスキーマが拡張されない場合があり、以降異なるプラットフォームでサーバをインストールするときに、［Root］に対するスーパバイザ権が要求される場合があります。	eDirectory 9.0を複数のプラットフォームにインストールする場合は、各プラットフォームでインストールする最初のサーバの［Root］に対するスーパバイザ権があることを確認してください。たとえば、eDirectory 9.0をインストールする最初のサーバがLinuxで実行されていて、eDirectory 9.0をSolarisでもインストールする場合、各プラットフォームの最初のサーバは［Root］のスーパバイザ権を持っている必要があります。それ以降、各プラットフォームでインストールする場合は、サーバがインストールされているコンテナに対するコンテナ管理者の権利のみが必要になります。 追加情報については、eDirectory 8.7.x Readme Addendumの*ソリューション*NOVL83874 (http://support.novell.com/docs/Tids/Solutions/10073723.html)を参照してください。
新しいネットワークインタフェースのデフォルトリスナ	Windowsでは、eDirectoryはデフォルトで、NCP、HTTP、HTTPS、LDAP、およびLDAPSのコンピュータ上に設定されたすべてのインタフェースをリスンします。コンピュータに新しいネットワークインタフェースアドレスを追加し、eDirectoryを再起動すると、自動的にそのアドレスのリスンが開始され、それに応じて参照も追加されます。 **注:** Linuxでは、インタフェースをn4u.server.interfacesパラメータに手動で追加する必要があります。

問題	推奨されるアクション
アップグレード後の複製に関する問題 eDirectory 9.0 にアップグレードして暗号化複製を有効にしている場合、ごくまれに複製に失敗することがあります。	この問題を解決するには: 1. NetIQ iManagerで、[**オブジェクトの変更**]を選択してから、NCPサーバオブジェクトを選択します。 2. ［全般］タブで［**その他**］を選択します。 3. **NCPKeyMaterialName**を［値がない属性］から、**SSL CertificateDNS**などの証明書の名前が付いた［値がある属性］に追加します。 4. 手順3で属性を変更したサーバでLimberを実行します。Limberの使用方法については、『NetIQ eDirectory Administration Guide』を参照してください。

設定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。

問題	推奨されるアクション
ループバック参照がディレクトリサーバから返される	eDirectoryがループバックアドレスを監視するように設定されていると、ループバックアドレスは格納され、クライアントが検索または他の操作を実行したときにクライアントにループバックアドレスが返されます。サーバ以外のマシンから接続を試行したクライアントには、参照は適用されません。そのため、そのような方法でループバック参照を使用したクライアントは接続に失敗します。しかし、サーバから返されるそれ以外の参照については、クライアントは引き続き正常に使用できます。 各ループバック参照に接続して正しい参照を選択しようとするなら、クライアントのパフォーマンスに影響が出る可能性があります。

Linux上でeDirectory 9.0を設定中に発生する「ツリー名の検索に失敗しました: -632」エラー	Linux上でeDirectory 9.0を設定している間に、「ツリー名の検索に失敗しました: -632」のエラーが発生する可能性があります。この問題を解決するには、次の手順を実行します。
	
	1. SLPパッケージをインストールした後、次のコマンドを入力し、手動でSLPを起動します。
	
	`/etc/init.d/slpuasa start`
	
	2. SLPパッケージをアンインストールした後、次のコマンドを入力し、手動でSLPを終了します。
	
	`/etc/init.d/slpuasa stop`

EBAを有効にしたセカンダリサーバを、EBAを有効にしていないサーバに追加すると、設定が失敗する	この問題を回避するにはまず、EBAを設定せずにセカンダリサーバを設定し、EBA設定を使用するEBAにアップグレードします。

問題	推奨されるアクション
バックアップまたはアンチウィルス処理からのDIBディレクトリの除外 eDirectoryをインストールした後、eDirectoryサーバのDIBディレクトリをアンチウィルスまたはバックアップソフトウェアの処理の対象外となるように環境設定する必要があります。DIBディレクトリをこれらの処理の対象外にしないと、DIBディレクトリの破損や「-618 FFFFD9E INCONSISTENT DATABASE」エラーが発生する可能性があります。	DIBディレクトリのバックアップは、eDirectoryバックアップツールを使って行えます。eDirectoryのバックアップの詳細については、『NetIQ証明書サーバ管理ガイド』の「ロールフォワードログのバックアップと削除」を参照してください。
IP AG 証明書がSLES 11 64ビットプラットフォームで作成されない	eDirectory 9.0 がIPv4とIPv6の両方で設定されていて、その片方(たとえばIPv4)のエントリのみが/etc/hostsファイルにあり、もう片方のインタフェースはリモートマシンからアクセス可能であるとします。両方のIPを監視するようにeDirectoryを設定すると、IP AG証明書は/etc/hostsファイルにリストされているIP用のみが生成されます。この例で生成されるのは、IPv4用となります。
複数のインスタンスのデフォルトのインスタンスパス. ホストでeDirectoryの2つ目のインスタンスを設定する際に、デフォルトのパスに設定するよう求めるメッセージが表示されます。	別のパスを選択し、続行します。

EDirectoryの複数インスタンス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。

問題	推奨されるアクション
最初のインスタンスが停止している場合、HTTPが動作しない Linuxプラットフォーム上で、eDirectoryが複数のNICカードを持つコンピュータ上に設定されており、HTTPが1つ以上のインタフェースにバインドされている場合、最初のインタフェースが停止すると、残りのインタフェースからHTTPにアクセスできなくなります。 これは、残りのインタフェースが要求を最初のインタフェースへリダイレクトしているのに対して、最初のインタフェースが停止しているためです。	この問題を解決するには、最初のインタフェースが停止している場合、eDirectoryを再起動します。

問題	推奨されるアクション
指定されたインタフェースが正しくない場合に、ndsdがデフォルトポートに戻る	eDirectoryの2番目のインスタンスをndsconfig newまたはndsmanageを使用して作成する場合、指定したインタフェースが正しくないと、ndsはデフォルトインタフェースを使用しようとします。デフォルト以外のポート(1524など)を指定し、指定したインタフェースが正しくないと、デフォルトインタフェースおよびデフォルトポート524が使用されます。 n4u.server.interfacesの場合、指定したインタフェースが正しくないと、ndsdは1番目のインタフェースの監視を試行し、ポート番号はn4u.server.tcp-portに指定されているものが使用されます。

.edirディレクトリを再構築する方法	eDirectoryの複数のインスタンスのトラッキングには.edirディレクトリが使用されます。失われたまたは破損したインスタンスファイル(instances.$uidファイル。$uidはシステム内でのユーザのユーザIDを表す)を再作成するには、インスタンスファイルを個別に再作成する必要があります。
	
	これらのファイルには、ユーザによって設定されたすべてのインスタンスのnds.confファイルの絶対位置が含まれています。たとえば、uidが1000であるユーザは、次のエントリを含む/etc/opt/novell/eDirectory/conf/.edir/instances.1000インスタンスファイルを作成する必要があります。
	
	`/home/user1/instance1/nds.conf`
	
	`/home/user1/instance2/nds.conf`

ndsconfigユーティリティ

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。

問題	推奨されるアクション
デフォルト以外の場所から実行するようにndsconfigを設定する	デフォルトの/opt/novell/eDirectory/binディレクトリ以外の場所からndsconfigユーティリティを実行するとエラーを受け取る場合は、ndsconfigを実行する前に必ずndspathをエクスポートしてください。次のコマンドを実行します。 `source /opt/novell/eDirectory/bin/ndspath` コマンドをエクスポートした後、ndsconfigと入力してndsconfigユーティリティを実行します。./ndsconfigとは入力しないでください。

問題	推奨されるアクション
無効な環境設定ファイルパスがndsconfigで検証されない	必要な環境設定ファイルを作成するには、ndsconfigで完全なパスと環境設定ファイル名を使用する必要があります。環境設定ファイルとインスタンスディレクトリの両方に同じパス名が指定されると、ndsconfigは環境設定ファイルを作成できないため、処理を中止します。
ndsconfigで英語以外の文字がジャンク文字で出力される	Linux上でndsconfig getコマンドを実行すると、英字以外の文字を含むパラメータに対しては無意味な文字が出力されます。 この問題に対処するには、表示したい特定のパラメータ名を次のように入力します。 ndsconfig get <*表示する対象のパラメータ*> パラメータの一覧については、nds.confマニュアルページを参照してください。

NMASインストールのトラブルシューティング

- Novell Clientをアンインストールする場合は、別のアプリケーションで使用されているNMASクライアントをアンインストールし、再インストールする必要があります。
- ユーザがNMASを使用するためには、ユーザのオブジェクトの書き込み可能なレプリカを保持するサーバにNMASをインストールしておく必要があります。
- NMAS ソフトウェアを実行する各クライアントワークステーションにNovell International Cryptographic Infrastructure (NICI)クライアントをインストールしておく必要があります。
- NMASをインストールした後でサーバを再起動せずにパスワードをリセットしようとすると、エラーメッセージが表示されます。
- ログインメソッドは最新の状態にしておく必要があります。eDirectoryのOES/Linuxのインストールでは、メソッドをアップグレードする手段が提供されない場合があります。

証明書サーバのインストールのトラブルシューティング

インストール中にファイルデータの競合が発生

以前インストールしたファイルより新しいバージョンのファイルが存在することを示すメッセージを受け取った場合は、常に新しいファイルを上書きするように選択してください。

サーバのリストが不完全

インストール時に表示されるサーバのリストには、IPのみを使用するように設定されたサーバが含まれない可能性があります。テキストボックスにサーバの名前を入力すると、名前が表示されていないサーバにNetIQ証明書サーバをインストールできます。

インストール中に障害が発生

組織の認証局またはサーバ証明書の作成中、またはルート認証局証明書のエクスポート中にインストールに失敗する場合は、インストールを繰り返す必要はありません。この時点では、ソフトウェアは正常にインストールされています。iManagerを使用すれば、組織の認証局およびサーバ証明書を作成でき、ルート認証局をエクスポートできます。

iManager 2.7.6 Patch1以下のバージョンへのインストール時にPKIプラグインがエラーを検出する

この問題を回避するには、次のように、libntls.soを指すlibntls.so.8シンボリックリンクを作成します。

```
ln -sf /var/opt/novell/iManager/nps/WEB-INF/bin/linux/libntls.so
```

```
/var/opt/novell/iManager/nps/WEB-INF/bin/linux/libntls.so.8
```

SLES 11 64ビットプラットフォームでIP自動生成証明書が作成されない

eDirectory 9.0がIPv4とIPv6の両方で設定されていて、その片方(たとえばIPv4)のエントリのみが/etc/hostsファイルにあり、もう片方のインタフェースはリモートマシンからアクセス可能であるとします。両方のIPを監視するようにeDirectoryを設定すると、IP AG証明書は/etc/hostsファイルにリストされているIP用のみが生成されます。この例で生成されるのは、IPv4用となります。

証明書オブジェクトのRDNが最大長を超えているとIP自動生成IPv6証明書が作成されない

eDirectory 9.0のインストール中、IPv4とIPv6の両方のアドレスでリスンしているときには、IP AG <IPv6>証明書(KMO)は作成されません。

これは、証明書オブジェクトのRDNが最大長の64文字を超えたときに発生します。これを処理するために、圧縮形式のIPv6アドレスが使用されます。これにより、最大長を超えている場合でも、要求に合わせてアドレスが分割されます。アドレスは、(逆順で)3番目のコロンから分割されます。

たとえば、2508:f0g0:1003:0061:0000:0000:0000:0002というIPv6アドレスが切り捨てられると、0000:0000:0002となります。これにより、アドレスが切り捨てられても、ホストは正しく識別されます。

CAがホストされていないサーバ用にデフォルトのサーバ証明書が再作成されると、HTTPサーバがIP AG証明書に関連付けられる

デフォルトの関連付けを手動で変更するには、iManagerを使用します。

iManagerにログインし、変更を加えたら、httpサーバオブジェクトを選択し、httpKeyMaterialObject属性を選択し、HTTPサーバオブジェクトの関連付けをSSL CertificateDNSに変更します。