NetIQ® eDirectory™ 8.8 SP8

トラブルシューティングガイド

2013 年 9 月

保証と著作権

目次

本書およびライブラリについて

『*トラブルシューティングガイド*』は、NetIQ eDirectory (eDirectory) 製品で起きる問題を解決する方法を説明します。

『*NetIQ eDirectory 8.8 SP8 トラブルシューティングガイド*』の最新版については、NetIQ eDirectory 8.8 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。

XDASv2 管理ガイド

eDirectory と NetIQ Identity Manager を監査するための XDASv2 の設定と使用方法について説明します。

インストールガイド

eDirectory をインストールする方法について説明します。ネットワーク管理者を対象としています。

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。

新機能ガイド

eDirectory の新機能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 8.8 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 2.7 Administration Guide*』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る。究極的に、お客様の成功こそがわたしたちの成功なのです。

当社のソリューション

- ID およびアクセスのガバナンス
- アクセス管理
- セキュリティ管理
- システムおよびアプリケーション管理

- ワークロード管理
- サービス管理

セールスサポートへのお問い合わせ

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

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

テクニカルサポートへのお問い合わせ

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

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

マニュアルサポートへのお問い合わせ

弊社の目標は、お客様のニーズを満たすマニュアルの提供です。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 エラーコードの解決

eDirectory エラーコードの完全なリストおよび説明については、NetIQ エラーコード Web ページ (http://www.novell.com/documentation/nwec/) を参照してください。

2 インストールと環境設定

2.1 インストール

このセクションでは、eDirectory 8.8 インストール時に発生する可能性のあるさまざまな問題およびトラブルシューティングのためのヒントについて説明します。

2.1.1 SLES 11 マシンのツリーに 2 番目の eDirectory Server をインストールすると、スキーマの同期に致命的なエラーが発生する

eDirectory ツリーの設定およびツリーへの別のサーバのインストール。両方の場合で、使用可能なすべてのインタフェースを使用するオプションを選択します。両方のサーバに同じインタフェースを使用します。たとえば、127.0.0.2 を使用します。最初のサーバで SCMA、SKLK、および SYNC オプションを指定して DSTrace を開始します。

2.1.2 インストールの失敗

- /var/adm/messages ディレクトリで、次のエラーメッセージを確認します。

```
Unable to bind to SLP Multicast Address. Multicast route not added?
```

Linux または Solaris のコンピュータがマルチキャストルートアドレスに設定されていない場合、このメッセージが表示されます。

マルチキャストルートアドレスを追加して、slpuasa デーモンを再起動します。

- インストール中に「-632: エラーの説明 システムエラー」というエラーメッセージが表示されたら、インストール処理を終了します。

  /etc/opt/novell/eDirectory/conf/nds.conf ファイルで n4u.base.slp.max-wait パラメータを 50 などの大きい値に設定してから、インストール処理をもう一度開始します。

- インストール中に「ツリー名が見つかりません」というエラーメッセージが表示された場合は、次の手順を実行します。

1. 製品をインストールしようとしている Solaris ホストでマルチキャストルーティングが有効に設定されていることを確認します。
2. ツリーパーティションのマスタサーバの IP アドレスを指定します。

2.1.3 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
```

2.1.4 コンテナ管理者の eDirectory インストールの失敗

eDirectory 8.8 インストールプログラムでは、サーバが存在するコンテナにスーパバイザ権を持つ管理者によるインストールをサポートしています。これを実行するには、eDirectory 8.8 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ために [Root] に対する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 8.8 では、最初に eDirectory 8.8 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 8.8 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 8.8 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 8.8 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。

2.1.5 NICI インストールエラー - 1497

NetIQ International Cryptographic Infrastructure (NICI) の初期化が失敗したことを警告するメッセージは、NFK ファイルが正しくないということを意味します。NFK ファイルが正しいか確認してください。Linux プラットフォーム上では、デフォルトで NFK ファイルが NICI パッケージの一部であるため、この問題は発生しない可能性があります。

2.1.6 オブジェクトの命名

オブジェクト名に特殊文字を使用すると、-671 該当するペアレントはありませんというエラーメッセージが表示されます。オブジェクト名には、次の特殊文字を使用しないでください。

\ /, * ? .

2.1.7 NICI がサーバモードで Windows にインストールされない

NICIFK ファイルの［プロパティ］ダイアログボックスに、［セキュリティ］というタブがあります。［グループ］または［ユーザ名］フィールドに名前が入力されていない場合、この問題が発生します。

この問題を回避するには、次の手順を実行します。

1. NICIFK ファイルを削除します。

   このファイルは、システムのルートディレクトリが C:/Windows/system32 の場合は、C:/Windows/system32/novell/nici に存在します。システムのルートディレクトリが F:/Windows/system32 の場合は、このファイルは F:/Windows/system32/novell/nici に存在します。

2. eDirectory をインストールします。

2.1.8 Tarball アップグレードが「Cannot open or remove a file containing a running program」エラーメッセージを出して失敗する

AIX で Tarball アップグレードを実行中に、ファイルコピーの段階で「Cannot open or remove a file containing a running program」エラーメッセージを受け取った場合は、以下のステップを実行して問題を解決してください。

1. ルートユーザとして /usr/sbin/slibclean を実行します。
2. ファイルコピーの段階からアップグレードを続行します。

2.1.9 eDirectory と YUM に関する問題

YUM パッケージマネージャがインストールされている Red Hat Enterprise Linux サーバに eDirectory 8.8 SP6 以降をインストールすると、YUM の使用時に問題が発生する場合があります。

YUM と eDirectory 8.8 はどちらも libexpat.so.0 ライブラリを使用するので、1 つ以上のオプションを使用して YUM を実行すると、YUM はコンソールでエラーを返します。このエラーを回避するには、テキストエディタで /etc/ld.so.conf.d/novell-NDSbase.conf ファイルの次の行をコメントアウトし、ldconfig を実行してください。

```
/opt/novell/eDirectory/lib64
```

行をコメントアウトして ldconfig を実行した後、eDirectory を起動するたびにターミナルウィンドウで次のコマンドを実行してください。

```
source /opt/novell/eDirectory/bin/ndspath
```

同じターミナルを使って eDirectory を再起動します。ndspath が必要なパスの依存性を解決します。

2.1.10 BTRFS 内の eDirectory を実行中にパフォーマンス上の問題が発生する

eDirectory を BTRFS ファイルシステム内の SLE サーバにインストールすると、LDAP 操作の実行や、NetIQ インポート / エクスポート変換ユーティリティの使用で、パフォーマンス関連の問題が発生することがあります。パフォーマンス上の理由から、eDirectory サーバには ext3 ファイルシステムを使うことをお勧めします。

2.2 環境設定

このセクションでは、eDirectory 8.8 環境設定時に発生する可能性のある問題を扱います。

- 18 ページのセクション 2.2.1「ループバック参照がディレクトリサーバから返される」
- 19 ページのセクション 2.2.2「Linux 上で eDirectory 8.8 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」
- 19 ページのセクション 2.2.3「新規サーバの追加」
- 19 ページのセクション 2.2.4「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」
- 19 ページのセクション 2.2.5「eDirectory ndsconfig が RHEL 32 ビットプラットフォームでエラーを表示する」
- 20 ページのセクション 2.2.6「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」

2.2.1 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。

対処方法 : eDirectory から通信可能なインタフェースを 1 つだけ選択します。インストール時にはループバックインタフェースを選択しないでください。

2.2.2 Linux 上で eDirectory 8.8 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 8.8 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
   ```

2.2.3 新規サーバの追加

完全修飾 DN の長さが 255 文字を超える場合は、新しいサーバをコンテキストに追加できません。長さの制限は完全修飾 DN に適用され、コンテキストの長さには適用されません。オブジェクトの完全修飾 DN の最大文字数は 255 文字です。

2.2.4 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 FFFFFD96 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 eDirectory 8.8 SP8 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。

2.2.5 eDirectory ndsconfig が RHEL 32 ビットプラットフォームでエラーを表示する

eDirectory ndsconfig が RHEL 32 ビットプラットフォームで次のエラーを表示します。

```
/opt/novell/eDirectory/lib/libsal.so.1.0.0
```

```
error while loading shared libraries: /opt/novell/lib/libccs2.so: cannot
restore segment prot after reloc: Permission denied
```

問題の対処方法 : 次のコマンドを実行します。

chcon -t textrel_shlib_t '/opt/novell/eDirectory/lib/libsal.so.1.0.0'

chcon -t textrel_shlib_t '/opt/novell/lib/libccs2.so.2.7.6'

2.2.6 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 8.8 SP8 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。

2.3 アップグレード

- 20 ページのセクション 2.3.1「マウントポイントが /var/opt/novell/eDirectory/data に設定されているとアップグレードが失敗する」
- 20 ページのセクション 2.3.2「Windows システムでパッチ適用後に eDirectory をアップグレードすると、パッチバージョンが削除されない」

2.3.1 マウントポイントが /var/opt/novell/eDirectory/data に設定されているとアップグレードが失敗する

マウントポイントが /var/opt/novell/eDirectory/data に設定されていると、ndsconfig upgrade コマンドを使用した eDirectory のアップグレードが失敗します。アップグレードは停止して、次のエラーメッセージが表示されます。

```
ERROR: Unable to check if the directory "/var/opt/novell/eDirectory/data_upg_bak"
already exists. If the directory exists, delete it and execute `ndsconfig upgrade -
-config-file /etc/nds.conf`to restart the upgrade operation.
```

アップグレード中は、カスタマデータが失われることのないように、/var/opt/novell/eDirectory/data ディレクトリの名前が /var/opt/novell/eDirectory/data_upg_bak に変更されます。これが問題の起きる理由です。前述の例の場合、マウントポイントは /var/opt/novell/eDirectory/data ディレクトリですが、このディレクトリは名前を変更することができません。

この問題の対処方法としては、次のいずれかを行います。

- マウントポイントを /var/opt/novell/eDirectory に変更します。
- 以下を実行します。
  1. /var/opt/novell/eDirectory/data_upg_bak ディレクトリを作成します。
  2. /var/opt/novell/eDirectory/data のファイルを /var/opt/novell/eDirectory/data_upg_bak に移動します。

重要 : アップグレードが円滑に行われるようにするため、/var/opt/novell/eDirectory/data ディレクトリは空にしておいてください。

2.3.2 Windows システムでパッチ適用後に eDirectory をアップグレードすると、パッチバージョンが削除されない

パッチ適用後に eDirectory をアップグレードすると、パッチバージョンはアップグレードされませんが、製品の基本バージョンはアップグレードされます。

この問題は、次のようにアップグレードした場合にみられ、問題は再現します。

表 2-1　eDirectory のバージョン

基本製品バージョン	パッチバージョン	アップグレード済みのバージョン
eDirectory 873	87310	eDirectory 88 SP3
eDirectory 873		eDirectory 88 SP3
eDirectory 873		eDirectory 873 SP10
eDirectory 88 SP6	任意のパッチ	eDirectory 88 SP8

この問題の原因は、eDirectory インストーラとパッチインストーラが Windows では異なることにあります。eDirectory の基本製品は NIS フレームワーク経由でインストールされ、eDirectory 8.8 SP5 Patch 2 などのパッチは Nulsoft インストーラスクリプト (NSIS) を使用してインストールされます。インストーラが異なるため、製品の基本バージョンのみがアップグレードされ、NSIS でインストールされたパッチはアップグレードされません。

この問題の対処方法として、アップグレード中にパッチ (eDirectory 8.7.3 SP9/eDirectory 8.7.3 SP10/eDirectory 8.8 SP5 パッチ 2 および eDirectory 8.8 SP5 パッチ 3 など) のレジストリエントリを削除します。

2.4　複数のインスタンス

eDirectory の複数のインスタンスを処理中に、次の問題が発生する可能性があります。

- 21 ページのセクション 2.4.1「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」
- 21 ページのセクション 2.4.2「eDirectory が設定済みインタフェースを全部は監視しない」

2.4.1　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。

2.4.2　eDirectory が設定済みインタフェースを全部は監視しない

eDirectory が設定されているすべてのインタフェースが実行され、接続されていることを確認してください。

2.4.3 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。

2.4.4 .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
```

3 eDirectory バージョン番号の確認

次のセクションでは、サーバにインストールされている eDirectory のバージョンを確認する方法を示します。

- 23 ページのセクション 3.1「Windows」
- 24 ページのセクション 3.2「Linux」

3.1 Windows

- 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 8.7.1 のエージェントリビジョン番号は 10510.64 などです。

  iMonitor の実行の詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「Accessing iMonitor(iMonitor 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 8.8.1 など) および内部ビルド番号 (10510.64 など) が表示されます。

- eDirectory ユーティリティを実行する。

  ほとんどの eDirectory ユーティリティの［ヘルプ］メニューには［バージョン情報］オプションがあり、該当するユーティリティのバージョン番号 (Merge Graft Utility 10510.35 など) が表示されます。内部ビルド番号が、ユーティリティのメインラベル (DSRepair - Version 10510.37 など) に表示される場合もあります。

  eDirectory ユーティリティ (DSMerge または DSRepair など) をロードするには、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、ユーティリティを選択し、［開始］をクリックします。

- eDirectory .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。eDirectory の .dlm ファイルがデフォルトで格納される場所は、C:\novell\NDS です。

3.2 Linux

- 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 8.7.1 は製品バージョン (マーケティング文字列) を示し、10510.65 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: 10510.65
  Root Most Entry Depth: 0
  Product Version: NDS/Linux - NDS eDirectory v8.8.8 [DS]
  ```

  ndsstat の実行方法の詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「NetIQ eDirectory の Linux 用コマンドとその使用法」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 8.8 SP8 管理ガイド*』の「NetIQ eDirectory の Linux 用コマンドとその使用法」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 8.8.1 のエージェントリビジョン番号は 10510.64 などです。

  iMonitor の実行の詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「Accessing iMonitor(iMonitor 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。

4 ログファイル

このセクションには、次のログファイルに関する情報が含まれています。

4.1 modschema.log

modschema.log ファイルには、eDirectory サーバを既存のツリーにインストールするときに適用されるすべてのスキーマ拡張の結果が含まれています。ログの各行は、どのクラスまたは属性が追加または変更されたか、および更新の試行のステータスを示します。

このログは、インストール処理を実行するたびに、作成されるか上書きされます。したがって、このログは、最後に行われた試行の結果だけを表します。このログには、eDirectory スキーマ拡張に加えて、新しい eDirectory サーバを追加する前に DSINSTALL フロントエンドによって適用された他のスキーマ拡張 (LDAP、SAS など) の結果も含まれます。

スタンドアロンサーバをインストールする場合またはターゲットサーバの eDirectory バージョンが 7.0.1 以降である場合は、このログは生成されません。

4.2 dsinstall.log

dsinstall.log ファイルの最初の部分は、設定されている環境変数を表示します。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。

4.3 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、『*NetIQ eDirectory 8.8 SP8 What's New Guide*』の「Managing Error Logging in eDirectory 8.8」を参照してください。

4.4 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。

5 LDIF ファイルのトラブルシューティング

NetIQ インポート / エクスポート変換ユーティリティを使用すると、eDirectory との間での LDIF ファイルのインポートおよびエクスポートが簡単になります。詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「NetIQ インポート / エクスポート変換ユーティリティ」を参照してください。

LDIF インポートを正しく機能させるには、NetIQ インポート / エクスポート変換ユーティリティが読み込み、および処理できる LDIF ファイルを最初に作成する必要があります。このセクションでは、LDIF ファイル形式および構文について説明し、正しい LDIF ファイルの例を示します。

- 27 ページのセクション 5.1「LDIF について」
- 35 ページのセクション 5.2「LDIF ファイルのデバッグ」
- 40 ページのセクション 5.3「LDIF を使用してスキーマを拡張する」
- 44 ページのセクション 5.4「ldif2dib の制限」

5.1 LDIF について

LDIF は、広く一般的に使用されているファイル形式で、ディレクトリ情報およびディレクトリで実行可能な変更操作について記述します。LDIF は、実際のディレクトリ内で使用されている記憶フォーマットとは完全に独立していて、通常は、LDAP サーバとの間でディレクトリ情報をエクスポートまたはインポートするために使用します。

一般的に、LDIF は簡単に生成できます。そのため、awk や perl などのツールを使用して、固有の形式のデータを LDAP ディレクトリに移動できます。また、LDIF 形式でテストデータを生成するスクリプトを作成することもできます。

5.1.1 LDIF ファイル形式

NetIQ インポート / エクスポート変換ユーティリティを使用してインポートするファイルの形式は、LDIF 1 である必要があります。次に LDIF 1 形式のファイルの基本ルールを示します。

- コメント行以外の第 1 行目には、「version: 1」と記述します。
- バージョンの指定の後に、1 つ以上のレコードを定義します。
- 各レコードは、フィールドで構成されます。1 行に 1 フィールドずつ指定します。
- 各行は、改行またはキャリッジリターンと改行の組み合わせのどちらかで区切られます。
- レコードは、1 行以上の空白行で区切られます。

- LDIF レコードには、内容レコードと変更レコードの 2 つのタイプがあります。LDIF ファイルに記述するレコード数に制限はありませんが、記述されたすべてのレコードのタイプが一致している必要があります。同じ LDIF ファイル内に、内容レコードと変更レコードの両方を記述することはできません。
- シャープ記号 (#) で始まる行はコメント行です。この行は、LDIF ファイルの処理時には無視されます。

5.1.2 LDIF 内容レコード

LDIF 内容レコードは、エントリ全体の内容を表します。次に、4 つの内容レコードが定義された LDIF ファイルの例を示します。

```
 1  version: 1
 2  dn: c=US
 3  objectClass: top
 4  objectClass: country
 5
 6  dn: l=San Francisco, c=US
 7  objectClass: top
 8  objectClass: locality
 9  st: San Francisco
10
11 dn: ou=Artists, l=San Francisco, c=US
12 objectClass: top
13 objectClass: organizationalUnit
14 telephoneNumber: +1 415 555 0000
15
16 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
17 sn: Michaels
18 givenname: Peter
19 objectClass: top
20 objectClass: person
21 objectClass: organizationalPerson
22 objectClass: iNetOrgPerson
23 telephonenumber: +1 415 555 0001
24 mail: Peter.Michaels@aaa.com
25 userpassword: Peter123
26
```

この LDIF ファイルは、次の部分から構成されています。

コンポーネント	説明
バージョン指定子	LDIF ファイルの第 1 行目にはバージョンが記述されます。コロンとバージョン番号 (現在の定義は 1) の間には、1 つ以上のスペースを指定できますが、スペースを指定しなくても問題はありません。 バージョンを指定した行がない場合、LDIF ファイルを処理するアプリケーションはそのファイルのバージョンを 0 とみなすことができます。また、構文エラーとして LDIF ファイルが拒否される可能性もあります。LDIF を処理する NetIQ のユーティリティは、バージョンを指定する行がない場合、ファイルのバージョンを 0 とみなします。

コンポーネント	説明
識別名指定子	各内容レコードの先頭の行 (この例では、2、6、11、および 16 行目) には、そのレコードが表すエントリの DN(識別名) を指定します。 DN 指定子は、次の 2 つのどちらかの形式をとる必要があります。 ◆ dn: *safe_UTF-8_distinguished_name* ◆ dn:: *Base64_encoded_distinguished_name*
行区切り記号	行区切り記号としては、改行、またはキャリッジリターンと改行の組み合わせのどちらかを使用できます。これにより、行区切りとして改行を使用する Linux および Solaris テキストファイルと、キャリッジリターンと改行の組み合わせを使用する MS-DOS* および Windows テキストファイルとの間の非互換性を解決できます。
レコード区切り記号	レコード区切りとしては、空白行 (この例では 5、10、15 および 26 行目) を使用します。 LDIF ファイル内の各レコード (最後のレコードも含む) の終わりには、レコード区切り記号として 1 行以上の空白行を挿入する必要があります。一部のアプリケーションでは、レコード区切りを指定していない LDIF ファイルもそのまま受け入れられますが、LDIF の仕様ではレコード区切りは必須です。
属性値指定子	内容レコード内のその他すべての行は、値指定子です。値指定子は、次の 3 つの形式のいずれかをとる必要があります。 ◆ 属性の記述 : *value* ◆ 属性の記述 :: *Base64_encoded_value* ◆ 属性の記述 : < *URL*

5.1.3 LDIF 変更レコード

LDIF 変更レコードには、ディレクトリに加えられる変更が記述されます。LDAP の更新操作 (追加、削除、変更、および DN の変更) はすべて、LDIF 変更レコードに記述できます。

LDIF 変更レコードでは、LDIF 内容レコードと同じ形式の識別名指定子、属性値指定子、およびレコード区切り記号を使用します。(詳細については、28 ページの 「LDIF 内容レコード」を参照してください)LDIF 内容レコードとの違いは、LDIF 変更レコードには changetype フィールドがあることです。changetype フィールドは、変更レコードが指定する操作を識別します。

changetype フィールドは、次の 5 つの形式のいずれかである必要があります。

フォーム	説明
changetype: add	この変更レコードで LDAP の追加操作が指定されていることを示すキーワードです。
changetype: delete	この変更レコードで LDAP の削除操作が指定されていることを示すキーワードです。

フォーム	説明
changetype: moddn	この変更レコードで、LDIF プロセッサがバージョン 3 クライアントとして LDAP サーバにバインドされている場合は LDAP の DN 変更操作が、バージョン 2 クライアントとして LDAP サーバにバインドされている場合は RDN 変更操作が指定されていることを示すキーワードです。
changetype: modrdn	moddn 変更タイプと同義です。
changetype: modify	この変更レコードで LDAP の変更操作が指定されていることを示すキーワードです。

「追加」変更タイプ

追加変更レコードは、内容変更レコード (「28 ページの 「LDIF 内容レコード」」を参照) に、changetype: add フィールドを属性値フィールドの直前に追加したものと同じです。

すべてのレコードのタイプが一致している必要があります。内容レコードと変更レコードを同じファイルに記述することはできません。

```
 1 version: 1
 2 dn: c=US
 3 changetype: add
 4 objectClass: top
 5 objectClass: country
 6
 7 dn: l=San Francisco, c=US
 8 changetype: add
 9 objectClass: top
10 objectClass: locality
11 st: San Francisco
12
14 dn: ou=Artists, l=San Francisco, c=US
15   changetype: add
16 objectClass: top
17 objectClass: organizationalUnit
18 telephoneNumber: +1 415 555 0000
19
20 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
21 changetype: add
22 sn: Michaels
23 givenname: Peter
24 objectClass: top
25 objectClass: person
26 objectClass: organizationalPerson
27 objectClass: iNetOrgPerson
28 telephonenumber: +1 415 555 0001
29 mail: Peter.Michaels@aaa.com
30 userpassword: Peter123
31
```

「削除」変更タイプ

削除変更レコードはエントリの削除を指定するので、削除変更レコードに必要なフィールドは識別名指定子と「削除」変更タイプだけです。

次に、「30 ページの 「「追加」変更タイプ」」の LDIF ファイルで作成した 4 つのエントリを削除する LDIF ファイルの例を示します。

重要 : 以前に追加したエントリを削除するには、エントリの指定順序を逆にする必要があります。順序を逆にしないと、コンテナ内のエントリが空でないため削除操作が失敗します。

```
 1 version: 1
 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
 3 changetype: delete
 4
 5 dn: ou=Artists, l=San Francisco, c=US
 8   changetype: delete
 9
10 dn: l=San Francisco, c=US
11 changetype: delete
12
13 dn: c=US
14 changetype: delete
15
```

「変更」変更タイプ

「変更」変更タイプでは、すでに存在するエントリに対して属性値の追加、削除、および置換を指定できます。変更指定子は、次の 3 つの形式のいずれかをとる必要があります。

要素	説明
add: 属性タイプ	この属性タイプに対する後続の属性値指定子がエントリに追加されるように指定する必要があることを示すキーワードです。
delete: 属性タイプ	この属性タイプの値が削除されることを示すキーワードです。delete フィールドの後に属性値指定子が続く場合は、その指定された値が削除されます。 delete フィールドの後に属性値指定子がない場合は、すべての値が削除されます。属性に値がない場合、この操作は失敗しますが、属性には削除する値がないので結果的にはこの操作が成功したときと同じです。
replace: 属性タイプ	属性タイプの値が置き換えられることを示すキーワードです。replace フィールドに続く属性値指定子が、その属性タイプの新しい値になります。 replace フィールドの後に属性値指定子がない場合は、現在の値のセットが空の値のセットに置き換えられます (結果的に、属性が削除されます)。delete 変更指定子とは異なり、属性に値が設定されていない場合でも replace は成功します。どちらの場合も実際に得られる結果は同じです。

次の「変更」変更タイプの例では、cn=Peter Michaels エントリに別の電話番号を追加します。

```
 1 version: 1
 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
 3 changetype: modify
 4 # add the telephone number to cn=Peter Michaels
 4 add: telephonenumber
 5 telephonenumber: +1 415 555 0002
 6
```

1 つの LDAP 変更要求にさまざまな変更を組み合わせて指定できるのと同じように、1 つの LDIF レコードに複数の変更指定子を指定できます。ハイフン (-) だけが記述されている行は、各変更指定子に対する属性値指定の終わりを示します。

次の LDIF ファイルの例では、複数の変更を組み合わせて指定しています。

```
 1 version: 1
 2
 3 # An empty line to demonstrate that one or more
 4 # line separators between the version identifier
 5 # and the first record is legal.
 6
 7 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
 8 changetype: modify
 9 # Add an additional telephone number value.
10 add: telephonenumber
11 telephonenumber: +1 415 555 0002
12 -
13 # Delete the entire fascimiletelephonenumber attribute.
14 delete: facsimileTelephoneNumber
15 -
16 # Replace the existing description (if any exists)
17 # with two new values.
18 replace: description
19 description: guitar player
20 description: solo performer
21 -
22 # Delete a specific value from the telephonenumber
23 # attribute.
24 delete: telephonenumber
25 telephonenumber: +1 415 555 0001
26 -
27 # Replace the existing title attribute with an empty
28 # set of values, thereby causing the title attribute to
29 # be removed.
30 replace: title
31 -
32
```

「DN 変更」変更タイプ

「DN 変更」変更タイプでは、エントリのリネーム、移動、またはその両方ができます。この変更タイプは、2 つの必須フィールドと 1 つのオプションフィールドで構成されます。

フィールド	説明
newrdn (必須)	このレコードの処理の実行中にエントリに割り当てられる新しい名前を指定します。新規 RDN(newrdn) 指定子は、次の 2 つのどちらかの形式をとる必要があります。 ◆ newrdn: *safe_UTF-8_relative_distinguished_name* ◆ newrdn:: *Base64_encoded_relative_ distinguished_name* 新規 RDN 指定子は、「DN 変更」変更タイプが指定されたすべての LDIF レコードで指定されている必要があります。

フィールド	説明
deleteoldrdn (必須)	旧 RDN 削除 (deleteoldrdn) 指定子は、古い RDN を newrdn(新規 RDN) に置き換えるか、残しておくかを指定するフラグです。これは、次の 2 つのどちらかの形式をとります。 ◆ deleteoldrdn: 0 リネーム後も古い RDN の値をエントリ内に残しておくことを指定します。 ◆ deleteoldrdn: 1 エントリのリネーム後に古い RDN の値を削除することを指定します。
newsuperior (オプション)	新規スーペリア (newsuperior) 指定子は、この DN 変更レコードの処理時にエントリに割り当てる新しいペアレントの名前を指定します。新規スーペリア指定子は、次の 2 つのどちらかの形式をとります。 ◆ newsuperior: *safe_UTF-8_distinguished_name* ◆ newsuperior:: *Base64_encoded_distinguished_ name* 新規スーペリア指定子は、「DN 変更」変更タイプが指定された LDIF レコードでオプションとして使用できます。これは、エントリのペアレントを変更する場合のみ指定します。

次の「DN 変更」変更タイプの例で、エントリの名前を変更する方法を示します。

```
 1 version: 1
 2
 3 # Rename ou=Artists to ou=West Coast Artists, and leave
 4 # its old RDN value.
 5 dn: ou=Artists,l=San Francisco,c=US
 6 changetype: moddn
 7 newrdn: ou=West Coast Artists
 8 deleteoldrdn: 1
 9
```

次の「DN 変更」変更タイプの例で、エントリを移動する方法を示します。

```
 1 version: 1
 2
 3 # Move cn=Peter Michaels from
 4 # ou=Artists,l=San Francisco,c=US to
 5 # ou=Promotion,l=New York,c=US and delete the old RDN.
 5 dn: cn=Peter Michaels,ou=Artists,l=San Francisco,c=US
 6 changetype: moddn
 7 newrdn: cn=Peter Michaels
 8 deleteoldrdn: 1
 9 newsuperior: ou=Promotion,l=New York,c=US
10
```

次の「DN 変更」変更タイプの例では、エントリを移動し、同時に名前を変更する方法を示します。

```
 1 version: 1
 2
 3 # Move ou=Promotion from l=New York,c=US to
 4 # l=San Francisco,c=US and rename it to
 5 # ou=National Promotion.
 5 dn: ou=Promotion,l=New York,c=US
 6 changetype: moddn
 7 newrdn: ou=National Promotion
 8 deleteoldrdn: 1
 9 newsuperior: l=San Francisco,c=US
10
```

重要 : LDAP 2 の RDN 変更操作では、エントリの移動はサポートされません。LDAP 2 クライアントで LDIF newsuperior 構文を使用してエントリを移動しようとすると、その要求は失敗します。

5.1.4 LDIF ファイル内での行の折り返し

LDIF ファイル内で行を折り返すには、行を折り返したい場所で単に行区切り記号 (改行、またはキャリッジリターンと改行の組み合わせ) を挿入し、その後にスペースを追加します。行の先頭にスペースがある場合、LDIF パーサではスペースの後のデータとその前の行のデータを結合して解析します。したがって、先頭のスペースは無視されます。

マルチバイトの UTF-8 文字の途中では、行を折り返さないでください。

次に、行の折り返しを含む (13 および 14 行目)LDIF ファイルの例を示します。

```
 1 version: 1
 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
 3 sn: Michaels
 4 givenname: Peter
 5 objectClass: top
 6 objectClass: person
 7 objectClass: organizationalPerson
 8 objectClass: iNetOrgPerson
 9 telephonenumber: +1 415 555 0001
10 mail: Peter.Michaels@aaa.com
11 userpassword: Peter123
12 description: Peter is one of the most popular music
13  ians recording on our label. He’s a big concert dr
14  aw, and his fans adore him.
15
```

5.1.5 LDIF ファイル内でのハッシュ化パスワードの表記

LDIF ファイル内では、ハッシュ化パスワードは Base64 データとして表記されます。属性名 userpassword に続けて、パスワードをハッシュ化するために使用される暗号化方式の名前を記述する必要があります。この名前は、次に示すように中カッコ「{ }」で囲んで記述します。

例 1

SHA ハッシュ化パスワードの場合 :

```
1 version: 1 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US 3 sn:
Michaels 4 userpassword: {SHA}xcbdh46ngh37jsd0naSFDedjAS30dm5 objectclass:
inetOrgPerson
```

例 2

SSHA ハッシュ化パスワードの場合 :

```
1 version: 1 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US 3 sn:
Michaels 4 userpassword: {SSHA}sGs948DFGkakdfkasdDF34DF4dS3skl5DFS5 objectclass:
inetOrgPerson
```

例 3

Digest MD5 ハッシュ化パスワードの場合 :

```
1 version: 1 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US 3 sn:
Michaels 4 userpassword: {MD5}a45lkSDF234SDFG62dsfsf2DG2QEvgdmnk4305 objectclass:
inetOrgPerson
```

5.2 LDIF ファイルのデバッグ

- 35 ページの 「前方参照を有効化する」
- 38 ページの 「LDIF ファイルの構文をチェックする」
- 39 ページの 「LDIF エラーファイルを使用する」
- 39 ページの 「LDAP SDK デバッギングフラグを使用する」

LDIF ファイルで問題が発生した場合、次のことを考慮してください。

5.2.1 前方参照を有効化する

LDIF ファイルで、あるエントリを追加するレコードを、そのエントリのペアレントを追加するレコードの前に記述してしまう場合があります。この場合、LDAP サーバが新しいエントリを追加しようとすると、そのエントリのペアレントが存在しないためエラーが発生します。

この問題は、前方参照の使用を有効にするだけで解決できます。前方参照の作成を有効にすると、エントリを作成するときにそのペアレントがまだ存在していない場合でも、このペアレント用に前方参照というプレースホルダが作成されるため、エントリを正常に作成できます。以後の操作で親が作成されると、前方向参照は通常のエントリに変更されます。

LDIF のインポートが完了した後でも、1 つ以上の前方参照が残っている場合があります (たとえば、LDIF ファイルでエントリのペアレントが作成されなかった場合など)。この場合、前方参照は ConsoleOne および iManager に不明オブジェクトとして表示されます。前方参照エントリを検索することはできますが、前方参照エントリには属性も属性値もないため、objectClass 以外の属性を読み込むことはできません。ただし、前方参照の下に位置する実オブジェクトエントリ上では、すべての LDAP 操作が正常に機能します。

前方参照エントリを識別する

前方参照エントリは「不明」のオブジェクトクラスを持ち、また、内部 NDS EF_REFERENCE エントリにフラグが設定されています。ConsoleOne および iManager では、「不明」のオブジェクトクラスを持つエントリは、中央に疑問符が表示される丸い黄色のアイコンで示されます。LDAP を使用して不明オブジェクトクラスのオブジェクトを検索することもできますが、現時点では LDAP からエントリフラグの設定にアクセスしてそれが前方参照エントリであることを確認する方法はありません。

前方参照エントリを通常オブジェクトへ変更する

(LDIF ファイルまたは LDAP クライアント要求などを使用して) オブジェクトを作成するだけで、前方参照エントリを通常のオブジェクトに変更できます。eDirectory で作成するように指定したエントリが前方参照としてすでに存在する場合、eDirectory では既存の前方参照エントリが、作成を指定したオブジェクトに変換されます。

NetIQ eDirectory インポート / エクスポート変換ウィザードを使用する

LDIF のインポート時に前方参照を有効にするには、次の手順に従ってください。

1. NetIQ iManager で、［*役割およびタスク*］ボタン をクリックします。
2. ［*eDirectory の保守*］>［*インポート / エクスポート変換ウィザード*］の順にクリックします。
3. ［*ディスク上のファイルからデータをインポート*］をクリックし、［*次へ*］をクリックします。
4. インポートするファイルのタイプに［*LDIF*］を指定します。
5. インポートするデータが含まれているファイルの名前を指定し、適切なオプションを指定してから［*次へ*］をクリックします。
6. データのインポート先になる LDAP サーバを指定します。
7. 次の表の説明を参照して、適切なオプションを追加します。

オプション	説明
サーバの DNS 名 /IP アドレス	相手 LDAP サーバの DNS 名または IP アドレス
ポート	相手 LDAP サーバのポート番号 (整数)
DER ファイル	SSL 認証に使用するサーバキーが格納されている DER ファイルの名前
ログイン方法	［認証ログイン］または［匿名ログイン］(［ユーザ DN］フィールドに指定したエントリのログイン方法)
ユーザ DN	サーバで指定されたバインド操作に使用されるエントリの識別名
パスワード	［ユーザ DN］フィールドで指定したエントリのパスワード属性

8. ［*詳細設定*］で、［*前方参照を許可する*］をクリックします。
9. ［*次へ*］をクリックし、［*終了*］をクリックします。

データをデータサーバへ移行するときに前方参照を有効にするには、次の手順に従ってください。

1. NetIQ iManager で、［*役割およびタスク*］ボタン をクリックします。
2. ［*eDirectory の保守*］>［*インポート / エクスポート変換ウィザード*］の順にクリックします。
3. ［*サーバ間でデータを移行*］>［*次へ*］の順にクリックします。
4. 移行するエントリが格納されている LDAP サーバを指定します。
5. 次の表の説明を参照して、適切なオプションを追加します。

オプション	説明
サーバの DNS 名 /IP アドレス	ソース LDAP サーバの DNS 名または IP アドレス
ポート	ソース LDAP サーバのポート番号 (整数)
DER ファイル	SSL 認証に使用するサーバキーが格納されている DER ファイルの名前
ログイン方法	［認証ログイン］または［匿名ログイン］(［ユーザ DN］フィールドに指定したエントリのログイン方法)
ユーザ DN	サーバで指定されたバインド操作に使用されるエントリの識別名
パスワード	［ユーザ DN］フィールドで指定したエントリのパスワード属性

6 ［*詳細設定*］で、［*前方参照を許可する*］をクリックします。

7 ［*次へ*］をクリックします。

8 移行するエントリの検索条件を次のように指定します。

オプション	説明
ベース DN	検索要求のベース識別名 このフィールドを指定しなかった場合、デフォルトのベース DN である ""(空の文字列) が使用されます。
スコープ	検索要求のスコープ
フィルタ	RFC 2254 準拠の検索フィルタ デフォルトは「objectclass=*」です。
属性	検索エントリごとに取得する属性

9 ［*次へ*］をクリックします。

10 データを移行する LDAP サーバを指定します。

11 ［*次へ*］をクリックし、［*終了*］をクリックします。

注 : スキーマが各 LDAP サービスで整合性を保っていることを確認します。

NetIQ インポート / エクスポート変換ユーティリティのコマンドラインインタフェースの使用

コマンドラインインタフェースで前方参照を有効にするには、-F LDAP ターゲットハンドラオプションを使用します。

詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「LDIF ターゲットハンドラのオプション」を参照してください。

5.2.2 LDIF ファイルの構文をチェックする

ファイル内のレコードを処理する前に、［操作を表示するが実行しない］LDIF ソースハンドラオプションを使用して LDIF ファイルの構文をチェックできます。

LDIF ソースハンドラは、LDIF ファイル内のレコードを処理するときに常に構文をチェックします。このオプションを使用すると、レコードの処理を無効にして、構文を検証できます。

NetIQ eDirectory インポート / エクスポート変換ウィザードを使用する

1. NetIQ iManager で、［*役割およびタスク*］ボタン をクリックします。
2. ［*eDirectory の保守*］>［*インポート / エクスポート変換ウィザード*］の順にクリックします。
3. ［*ディスク上のファイルからデータをインポート*］をクリックし、［*次へ*］をクリックします。
4. インポートするファイルのタイプに［*LDIF*］を指定します。
5. インポートするデータが含まれているファイルの名前を指定し、適切なオプションを指定します。
6. ［*詳細設定*］で、［*操作を実行せずに表示*］をクリックし、［*次へ*］をクリックします。
7. データのインポート先になる LDAP サーバを指定します。
8. 次の表の説明を参照して、適切なオプションを追加します。

オプション	説明
サーバの DNS 名 /IP アドレス	相手 LDAP サーバの DNS 名または IP アドレス
ポート	相手 LDAP サーバのポート番号 (整数)
DER ファイル	SSL 認証に使用するサーバキーが格納されている DER ファイルの名前
ログイン方法	［認証ログイン］または［匿名ログイン］(［ユーザ DN］フィールドに指定したエントリのログイン方法)
ユーザ DN	サーバで指定されたバインド操作に使用されるエントリの識別名
パスワード	［ユーザ DN］フィールドで指定したエントリのパスワード属性

9. ［*次へ*］をクリックし、［*終了*］をクリックします。

NetIQ インポート / エクスポート変換ユーティリティのコマンドラインインタフェースの使用

コマンドラインインタフェースで LDIF ファイルの構文をチェックするには、-n LDIF ソースハンドラオプションを使用します。

詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「LDIF ソースハンドラのオプション」を参照してください。

5.2.3 LDIF エラーファイルを使用する

NetIQ インポート / エクスポート変換ユーティリティは、ターゲットハンドラによる処理に失敗したレコードをすべてリストした LDIF ファイルを自動的に作成します。ユーティリティによって生成された LDIF エラーファイルを編集してエラーを修正し、サーバに再適用することで、失敗したレコードに含まれているインポートまたはデータの移行を完了できます。

NetIQ eDirectory インポート / エクスポートウィザードを使用する

この機能は ConsoleOne のみで使用できます。

1. ConsoleOne で、［*ウィザード*］>［*NDS インポート / エクスポート*］の順にクリックします。
2. 実行するタスクをクリックします。
3. ［*詳細*］をクリックします。
4. ［*ログファイル*］フィールドに、出力メッセージ (エラーメッセージを含む) を記録するファイル名を指定します。
5. ［*失敗したレコードの LDIF 出力ファイル*］フィールドに、失敗したエントリを LDIF 形式で出力するファイル名を指定します。

   このファイルは、エラーの確認や訂正に使用できます。このファイルを修正 (訂正) して、もう一度ディレクトリに適用することもできます。
6. ［*閉じる*］をクリックします。
7. 表示される指示に従って、選択したタスクを完了します。

NetIQ インポート / エクスポート変換ユーティリティのコマンドラインインタフェースの使用

コマンドラインユーティリティでエラーログオプションを設定するには、-l 一般オプションを使用します。

詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「一般オプション」を参照してください。

5.2.4 LDAP SDK デバッギングフラグを使用する

一部の LDIF の問題を理解するには、LDAP クライアント SDK がどのように機能するかを理解する必要があります。LDAP ソースハンドラ、LDAP ターゲットハンドラ、またはその両方に、次のデバッギングフラグを設定できます。

値	説明
0x0001	LDAP ファンクションコールをトレースします。
0x0002	パケットに関する情報を出力します。
0x0004	引数に関する情報を出力します。
0x0008	接続情報を出力します。
0x0010	BER のエンコーディングおよびデコーディング情報を出力します。

値	説明
0x0020	検索フィルタ情報を出力します。
0x0040	設定情報を出力します。
0x0080	ACL 情報を出力します。
0x0100	統計情報を出力します。
0x0200	追加の統計情報を出力します。
0x0400	シェル情報を出力します。
0x0800	解析情報を出力します。
0xFFFF (10 進数では、-1)	すべてのデバッギングオプションを有効にします。

この機能を有効にするには、LDAP ソースハンドラおよびターゲットハンドラで-e オプションを使用します。-e オプションに指定する整数の値は、LDAP SDK でさまざまな種類のデバッグ情報を有効にするビットマスクです。

詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「LDAP ソースハンドラのオプション」および「LDAP ターゲットハンドラのオプション」を参照してください。

5.3 LDIF を使用してスキーマを拡張する

LDIF では LDAP 更新操作を表すことができるので、LDIF を使用してスキーマを変更できます。

5.3.1 新しいオブジェクトクラスを追加する

クラスを追加するには、単に、NDSObjectClassDescription の仕様に従った属性値を subschemaSubentry の objectClasses 属性に追加します。

```
NDSObjectClassDescription = "(" whsp
   numericoid whsp
   [ "NAME" qdescrs ]
   [ "DESC" qdstring ]
   [ "OBSOLETE" whsp ]
   [ "SUP" oids ]
   [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ]
   [ "MUST" oids ]
   [ "MAY" oids ]
   [ "X-NDS_NOT_CONTAINER" qdstrings ]
   [ "X-NDS_NONREMOVABLE" qdstrings ]
   [ "X-NDS_CONTAINMENT" qdstrings ]
   [ "X-NDS_NAMING" qdstrings ]
   [ "X-NDS_NAME" qdstrings ]
   whsp ")"
```

次の LDIF ファイルの例では、person objectClass をスキーマに追加します。

```
 1 version: 1
 2 dn: cn=schema
 3 changetype: add
 4 objectClasses: ( 2.5.6.6 NAME 'person' DESC 'Standard
 5   ObjectClass' SUP ndsLoginProperties STRUCTURAL MUST
 6   (cn $ sn) MAY (description $ seeAlso $ telephoneNum
 7  ber $ fullName $ givenName $ initials $ uid $ userPa
 8  ssword) X-NDS_NAMING ('cn' 'uid') X-NDS_CONTAINMENT
 9  ('organization' 'organizationalUnit' 'domain') X-NDS
10  _NAME 'Person' X-NDS_NOT_CONTAINER '1' X-NDS_NONREMO
11  VABLE '1')
12
```

必須属性

必須属性は、オブジェクトクラス記述の MUST セクションにリストします。person オブジェクトクラスの場合、必須属性は cn と sn です。

オプション属性

オプション属性のリストは、オブジェクトクラス記述の MAY セクションに記述します。person オブジェクトクラスのオプション属性は、description、seeAlso、telephoneNumber、fullName、givenName、initials、uid、および userPassword です。

注 : userPassword 属性は、オプション (MAY) 属性には使用できません。この LDIF 形式を使用して、新しい objectClass でこの属性を必須 (MUST) 属性に使用してスキーマを拡張しようとしても、操作は失敗します。

包含ルール

定義されているオブジェクトクラスを包含するオブジェクトクラスは、オブジェクトクラス記述の X-NDS_CONTAINMENT セクションで指定します。person オブジェクトクラスを包含するオブジェクトクラスは、organization、organizationalUnit、および domain です。

5.3.2 新しい属性を追加する

属性を追加するには、NDSAttributeTypeDescription の仕様に従って属性値を subschemaSubentry の attributes 属性に追加します。

```
NDSAttributeTypeDescription = "(" whsp
  numericoid whsp  ; AttributeType identifier
  [ "NAME" qdescrs ]  ; name used in AttributeType
  [ "DESC" qdstring ]  ; description
  [ "OBSOLETE" whsp ]
  [ "SUP" woid ]  ; derived from this other AttributeType
  [ "EQUALITY" woid]  ; Matching Rule name
  [ "ORDERING" woid]  ; Matching Rule name
  [ "SUBSTR" woid ]  ; Matching Rule name
  [ "SYNTAX" whsp noidlen whsp ] ;  Syntax OID
  [ "SINGLE-VALUE" whsp ]  ; default multi-valued
  [ "COLLECTIVE" whsp ]  ; default not collective
  [ "NO-USER-MODIFICATION" whsp ] ;  default user modifiable
  [ "USAGE" whsp AttributeUsage ] ;  default userApplications
  [ "X-NDS_PUBLIC_READ" qdstrings ]
                              ; default not public read ('0')
  [ "X-NDS_SERVER_READ" qdstrings ]
```

```
                              ; default not server read ('0')
  [ "X-NDS_NEVER_SYNC" qdstrings ]
                               ; default not never sync ('0')
  [ "X-NDS_NOT_SCHED_SYNC_IMMEDIATE" qdstrings ]
                            ;  default sched sync immediate ('0')
  [ "X-NDS_SCHED_SYNC_NEVER" qdstrings ]
                                 ;  default schedule sync ('0')
  [ "X-NDS_LOWER_BOUND" qdstrings ]
                              ;  default no lower bound('0')
                                     ;(upper is specified in SYNTAX)
  [ "X-NDS_NAME_VALUE_ACCESS" qdstrings ]
                          ; default not name value access ('0')
  [ "X-NDS_NAME" qdstrings ]  ; legacy NDS name
  whsp ")"
```

次の LDIF ファイルの例では、title 属性タイプをスキーマに追加します。

```
1 version: 1
2 dn: cn=schema
3 changetype: add
4 attributeTypes: ( 2.5.4.12 NAME 'title' DESC 'Standa
5  rd Attribute' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{
6  64} X-NDS_NAME 'Title' X-NDS_NOT_SCHED_SYNC_IMMEDIA
7  TE '1' X-NDS_LOWER_BOUND '1')
8
```

単一値と複数値

属性は、明示的に単一値として定義されない限り、デフォルトでは複数値です。次の LDIF ファイルの例では、SYNTAX セクションの後に SINGLE-VALUE キーワードを追加することによって、title を単一値として定義しています。

```
1 version: 1
2 dn: cn=schema
3 changetype: add
4 attributeTypes: ( 2.5.4.12 NAME 'title' DESC 'Standa
5  rd Attribute' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{
6  64} SINGLE-VALUE X-NDS_NAME 'Title' X-NDS_NOT_SCHED
7  _SYNC_IMMEDIATE '1' X-NDS_LOWER_BOUND '1')
8
```

既存のオブジェクトクラスへオプション属性を追加する

新しいスキーマエレメントを追加する場合は問題ありませんが、通常、既存のスキーマエレメントを変更または拡張する場合には注意が必要です。すべてのスキーマエレメントは OID によって固有に識別されるため、標準スキーマエレメントを拡張すると、元の OID を使用する場合でも実際にはそのエレメントに対して 2 つめの定義が作成されます。このため、不整合が発生することがあります。

スキーマエレメントの変更が必要な場合もあります。たとえば、開発しながらスキーマエレメントを洗練していくときに、新しいスキーマエレメントの拡張または修正が必要な場合があります。次のような場合は、クラスに直接新しい属性を追加せずに、通常は補助クラスのみを使用します。

- 既存のオブジェクトクラスに新しい属性を追加する場合。
- 既存のオブジェクトクラスのサブクラスを作成する場合。

5.3.3 補助クラスを追加または削除する

次のサンプル LDIF ファイルは、2 つの新しい属性、およびこの新しい属性に付随する補助クラスを作成してから、inetOrgPerson エントリをエントリのオブジェクトクラスとして auxiliary クラスと auxiliary クラスの属性値に追加します。

```
version: 1
# Add an attribute to track a bear's hair. The attribute is
# multi-valued, uses a case ignore string syntax,
# and has public read rights
# Values may include: long hair, short, curly, straight,
# none, black, and brown
# X-NDS_PUBLIC_READ '1' The 1 allows public read,
# 0 denies public read
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.186.4.10 NAME
'bearHair' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
X-NDS_PUBLIC_READ '1' )

# add an attribute to store a bear's picture
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.186.4.11 NAME
'bearPicture' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE )

# create an Auxiliary class for the bearfeatures
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: (2.16.840.1.113719.1.186.6.101 NAME
'bearFeatures' MAY (bearHair $ bearPicture) AUXILIARY)

# now create a user named bobby
dn: cn=bobby,o=bearcave
changetype: add
cn: bobby
sn: bear
givenName: bobby
bearHair: Short
bearHair: Brown
bearHair: Curly
bearPicture:< file:///c:/tmp/alien.jpg
objectClass: top
objectClass: person
objectClass: inetOrgPerson
objectClass: bearFeatures

# now create a person named john that will later be changed
# into a bear when bearFeatures is added to its objectClass
# list
dn: cn=john,o=bearcave
changetype: add
cn: John
sn: bear
givenName: john
objectClass: top
objectClass: person
objectClass: inetOrgPerson

# now morph john into a bear by adding bearFeatures
dn: cn=john,o=bearcave
changetype: modify
add: objectClass
```

```
objectClass: bearFeatures
-
add: bearHair
bearHair: long
bearHair: black
#bearPicture:< file:///c:/tmp/john.jpg>
-

# to morph john back to a person, simply delete the
# objectClass bearFeatures
dn: cn=john,o=bearcave
changetype: modify
delete: objectClass
objectClass: bearFeatures
```

補助クラスの削除にあたって、objectClass リストから auxiliary クラスを削除する場合には、auxiliary クラスに関連するすべての値を削除する必要はありません。この処理は eDirectory によって自動的に行われます。

auxiliary クラスに MUST 属性がある場合、auxiliary クラスを objectClass リストへ追加する変更操作でもこれらの属性を指定する必要があります。これらの属性が指定されていない場合、変更は失敗します。

XML 解析で発生する既知の問題

個々のレコードが XML ファイルで指定されたすべての XML ルールを遵守していない場合、LDIF レコード (LDAP サーバで生成された LDIF 形式またはレコード) の XML 処理は成功しません。

5.4 ldif2dib の制限

5.4.1 簡易パスワード LDIF

Windows では、簡易パスワードを持つ LDIF をアップロードするときに、system フォルダおよび *Administrator* フォルダに格納されている NICI キーが同期されていない場合、ldif2dib が失敗することがあります。

この問題を回避するには、次の手順で nici/system フォルダ内のキーにアクセスします。

1. C:\Windows\system32\novell\nici\ フォルダに移動します (32 ビット NICI の場合)。

   または

   C:\Windows\SysWOW64\novell\nici\ フォルダに移動します (64 ビット NICI の場合)。
2. *Administrator* フォルダのファイルをバックアップします。
3. System フォルダの［プロパティ］ウィンドウにある *［セキュリティ］* タブに移動します。
4. *［詳細設定］* を選択し、*［所有者］* タブに移動します。
5. *Administrator* を選択します。

6 *［セキュリティ］*タブに戻り、Administrator を一覧に追加します。

7 手順ステップ 3 ～ステップ 6 を繰り返し、system フォルダ内にあるすべてのファイルに対して読み取りアクセス権を取得します。

8 *Administrator* フォルダのファイルを system フォルダのファイルで上書きします。

9 アップロードした後に、バックアップファイルを *Administrator* フォルダにコピーします。

10 system フォルダおよびフォルダ内のファイルへの Administrator のアクセス権を変更します。

5.4.2 スキーマ

LDIF ファイルには、エントリが属するすべてのオブジェクトクラスを記述する必要があります。また、クラスの継承によってエントリが属することになるクラスも記述する必要があります。たとえば、inetOrgPerson タイプのエントリの構文は LDIF ファイルでは次のようになります。

- objectclass: inetorgperson
- objectclass: organizationalPerson
- objectclass: person
- objectclass: top

5.4.3 ACL テンプレート

ldif2dib ユーティリティを使用してバルクロード処理を行ったオブジェクトは、指定された ACL と一緒にオブジェクトのオブジェクトクラス用の ACL テンプレートには追加されません。

5.4.4 シグナルハンドラ

s キーまたは S キーを押すと、オフラインのバルクロード処理を一時的に停止することができます。バルクロード処理を停止する際はエスケープキー (Esc) を使用することができます。

6 SNMP のトラブルシューティング

このセクションには、すべてのプラットフォーム上の SNMP のトラブルシューティングについての情報が含まれています。

6.1 必要なトラップが生成されない

トラップは、対応するバーブの要求がサーバで受信された場合にのみ送信されます。それ以外の場合にトラップは送信されません。たとえば、ndsRemoveEntry (トラップ番号 108) の要求が送信された場合にのみ、ndsDeleteAttribute が送信されます。ただし、アプリケーションでは常に ACL が読み込まれ、そのユーザに削除操作を実行する十分な権利があるかどうかが確認されます。この場合、ndsDeleteAttribute トラップは生成されません。ただし、iMonitor を使用して特定のサーバにバーブ統計情報を表示できます。

すべてのイベントの発生時にトラップを取得するには、時間間隔を 0 に設定します。

トラップを有効にすると、失敗した場合にのみ送信できます。トラップを有効にすると、すべての状態でトラップを取得できます。

マスタエージェントが再起動される際に、ndssnmpsa を再起動する必要があります

ndssnmpsa を再起動するには、ndssnmpsa を停止した後に再度開始します。

ndssnmpsa を停止するには、次のように入力します。

Linux: /etc/init.d/ndssnmpsa stop

ndssnmpsa を開始するには、次のように入力します。

Linux: /etc/init.d/ndssnmpsa start

6.2 SNMP グループオブジェクト

SNMP グループオブジェクトのインストールが失敗した場合、サーバコンソールで次のコマンドを実行すると、この問題を修正できます。

ndsconfig *add -m snmp*

6.3 SNMP 初期化エラー

eDirectory SNMP 初期化コンポーネント。エラーコード : -255

または

初期化に失敗しました。エラーコード : -255

原因としては、eDirectory SNMP 環境設定ファイル内で hostname:port または IP_address:port を SERVER コマンドのパラメータとして指定しなかったことが考えられます。

eDirectory SNMP 環境設定ファイルは ndssnmp.cfg です。これは次のディレクトリにあります。

- Linux: /etc/opt/novell/eDirectory/conf/ndssnmp/
- Windows: *install_directory*\SNMP\

6.4 SNMP サブエージェントが起動しない

SNMP サブエージェントの起動時に、セグメンテーションエラーが発生する可能性があります。このエラーは、ndssnmp.cfg ファイル内の余分なスペースが原因で発生する場合があります。スペースを削除して ndssnmpsa を起動してください。

6.5 LDAP SNMP 統計が報告されない

匿名バインドが無効になっていると、LDAP SNMP 統計が報告されません。

この問題を解決するには、次の操作を行います。

1. 匿名バインドを許可します。
2. サブエージェントを起動します。
3. 匿名バインドを無効にします。

6.6 サブエージェントにアクセスする際のセグメント化失敗エラー

誤った eDirectory パスワードでユーザがサブエージェント (ndssnmpsa) を起動しようとすると、セグメント化失敗のエラーが発生します。

このエラーを回避するには、サブエージェントの起動時に、必ず正しい eDirectory パスワードを使用します。

6.7 SNMP に関する問題

6.7.1 eDirectory 8.7.3 から eDirectory 8.8 にアップグレードした後に発生するの問題

eDirectory 8.7.3 から eDirectory 8.8 にアップグレードした後に、次のようなエラーが発生する可能性があります。

```
%%% Attempting to restart the NetIQ eDirectory SNMP subagent (ndssnmpsa)...
Starting NDS SNMP Subagent ...
Initialization failure. Error code : -255
Please Wait...
Done
```

```
%%% Unable to start ndssnmpsa... Please try starting it manually...
```

eDirectory 8.8 では eDirectory が localhost を監視しないため、このエラーが発生します。以前のバージョンの ndssnmp.cfg ファイルには、デフォルトで SERVER localhost が設定されていました。

このエラーを解決するには、ndssnmp.cfg ファイルを手動で編集し、監視対象となる eDirectory サーバのホスト名を指定する必要があります。

たとえば、ndssnmp.cfg ファイルに次のように入力します。

```
SERVER test-server
```

test-server は、デフォルトの NCP ポート (524) で実行されている eDirectory のホスト名です。eDirectory が別のポート (例 :1524) で実行されている場合は、次のように入力します。

```
SERVER test-server:1524
```

6.7.2 NDS サブエージェントの起動時のエラー

サブエージェントが失敗して次のメッセージが表示される場合があります。

```
Unable to load library: libnetsnmp.so
```

この問題を解決するには、net-snmp ライブラリ (libnetsnmp.so) のメジャーバージョン番号を使用して、環境変数 SNMP_MAJOR_VERSION をエクスポートします。例 : 次のコマンドを使用できます。

export SNMP_MAJOR_VERSION=10

6.7.3 ndssnmpsa の再起動

Linux 上でマスタエージェントが再起動される際に、ndssnmpsa を再起動する必要があります。

ndssnmpsa を再起動するには、ndssnmpsa を停止した後に再度開始します。

ndssnmpsa を停止するには、次のコマンドを入力します。

/etc/init.d/ndssnmpsa stop

ndssnmpsa を開始するには、次のように入力します。

/etc/init.d/ndssnmpsa start

6.7.4 ndssnmpsa の起動時のエラー

Linux 上で ndssnmpsa を開始する際に、次のエラーが発生する可能性があります。

```
Error: eDirectory SNMP Initialization component. Error code: -168
Error: eDirectory SNMP Initialization component. Error code: 9
```

この問題を解決するには、次のコマンドを使用して ndssnmp をアンロードしてからロードします。

/opt/novell/eDirectory/bin/ndssnmp -u

/opt/novell/eDirectory/bin/ndssnmp -l

6.7.5 ndssnmpsa の停止時のエラー

SLES 9 で ndssnmpsa が停止されると、「*** glibc detected *** double free or corruption (!prev): 0x0819cdd0 ***」のようなエラーメッセージが画面上に表示されます。

これらのメッセージは無視することができます。

6.7.6 edir.mib のコンパイル

Windows の eDirectory MIB ファイル (<*eDirectoryInstallRootDir*>\snmp\edir.mib) では、コンパイル時に HP-OpenView でいくつかのエラーおよび警告が出されます。これらのエラーは無視することができます。

6.7.7 SNMP 設定ファイルの変更

LDAP がクリアテキストモードで実行されるように設定されていない場合は、eDirectory SNMP サブエージェントを起動する前に、SNMP 環境設定ファイル (SSLKEY C:\Novell\nds\trust.der など) でルート認証局証明書ファイルの名前を指定する必要があります。

ndssnmp.cfg は、Windows 上の C:\novell\nds\snmp にあります。

6.7.8 新しいツリーをインストールした後の SNMP の使用

eDirectory 8.8 SP8 を初めてインストールする (新しいツリーを作成する) 際に、サーバにインストールされている Windows SNMP サービスに依存するサービスが 1 つ以上ある場合、eDirectory は SNMP サービスをシャットダウンできません。このような場合は、eDirectory をインストールした後に SNMP を使用することができません。

次の手順に従って、SNMP サービスを再起動してください。

1. *［スタート］* > *［設定］* > *［コントロールパネル］* > *［管理ツール］* > *［サービス］* の順にクリックします。
2. *［名前］* の一覧で *［SNMP サービス］* を右クリックし、*［停止］* をクリックします。
3. ［Yes to All］をクリックします。
4. *［名前］* の一覧で *［SNMP サービス］* を右クリックし、*［開始］* をクリックします。

6.7.9 Windows サーバでの SNMP オブジェクト作成エラー

対応している Windows プラットフォームのサーバに eDirectory をインストールしている間に、SNMP グループオブジェクトの作成エラーが発生した場合は、SNMP グループオブジェクトを手動で作成する必要があります。SNMP オブジェクトを手動で作成する手順は、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「eDirectory and SNMP (http://www.netiq.com/documentation/edir88/edir88/data/ag7hr1h.html)」セクションを参照してください。

6.7.10 eDirectory のアンインストール時に SNMP をアンインストールする方法

Windows SNMP サービスがサーバにインストールされ、SNMP サービスに依存するサービスが 1 つ以上ある場合は、eDirectory のアンインストールによって C:\novell\nds フォルダ内の SNMP ファイルがすべて削除されるわけではありません。ただし、SNMP レジストリエントリの削除や、NetIQ SNMP エージェントが DS および SNMP サービスによって行う設定解除プロセスなど、その他のアンインストールプロセスは正常に完了します。

アンインストールを完了するには、次の手順を実行します。

1. *［スタート］* > *［設定］* > *［コントロールパネル］* > *［管理ツール］* > *［サービス］* の順にクリックします。
2. *［名前］* の一覧で *［SNMP サービス］* を右クリックし、*［停止］* をクリックします。
3. *［Yes to All］* をクリックします。
4. *［名前］* の一覧で *［SNMP サービス］* を右クリックし、*［開始］* をクリックします。
5. C:\novell\nds フォルダに残っている SNMP ファイルを手動で削除します。

7 iMonitor

7.1 iMonitor を使用しての 2 バイト文字を含むオブジェクトの参照

iMonitor を使用して eDirectory ツリー内のオブジェクトを参照する際、名前に 2 バイト文字が含まれているオブジェクトについては、オブジェクトプロパティへのハイパーリンクが正しく設定されないことがあります。

7.2 単一のサーバツリーでのエージェントヘルスチェック

iMonitor のエージェントヘルスチェック機能を単一のサーバツリーで実行すると、破損しやすいデータのステータスが原因で、［結果］カラムに［警告］アイコンが表示されます。これは、ツリーが正常でないということでも、エージェントヘルスチェックが設計どおりに機能していないということでもありません。破損しやすいデータとは、現在のところ少なくとも 1 つのレプリカにも同期されていないデータです。単一のサーバツリーは、その性質上、別の場所にデータのレプリカを作成していないため、このようなデータには常に重大な障害が発生する危険性があります。ハードディスクに障害が発生した場合、データを失うことになります。

単一のサーバツリーの破損しやすいデータまたは読み込み可能なレプリカ数に関するヘルスチェック警告を表示させたくない場合は、ndsimonhealth.ini ファイルを編集することにより、これらのヘルスチェックを無効にすることができます。ヘルスチェックを無効にするには、次のエントリを変更します。

perishable_data-active: OFF

および

ring_readable-Min_Marginal: 1 または ring_readable-active: OFF

この設定により、読み込み可能なレプリカ数および破損しやすいデータに関する警告が無効になります。

7.3 iMonitor レポートで 1 時間ごとのレコードが保存されない

iMonitor のカスタムレポート機能は、カスタムレポートを作成するときに、ユーザが指定した URL を保存対象のレポート (保存される HTML ファイル) に挿入するように設計されています。このため、保存された実行済みのカスタムレポートを開くと、カスタムレポートが実行された時点で URL によって取得されたデータではなく、アクティブな (現在の) データが表示されます。この問題は iMonitor の今後のリリースで解決される予定です。

7.4 作成および変更のタイムスタンプ

Linux プラットフォームではファイルの作成時刻が保持されないため、iMonitor で作成時刻と変更時刻が両方とも同じように表示されます。

7.5 古いバージョンの Mozilla での iMonitor に関する問題

1.5 より前のバージョンの Mozilla を使用して iMonitor にアクセスすると、DSTrace フラグ選択中に iMonitor に問題が起きる可能性があります。Mozilla では、一部の操作がサポートされていない場合があります。

7.6 iMonitor で整列されていないレポート画面レイアウトの実行

ナビゲーションフレームとアシスタントフレームは Linux で 2 回表示されます。

この問題に対処するには、ページを更新します。

7.7 iMonitor がエラー -672 を表示する

特定のデバッグツールが iMonitor と同時に実行されていると、いくつかの操作が失敗してエラー -672 が表示されます。

Linux の場合

dsdump ツールが iMonitor と同時に実行されていると、iMonitor がエラー -672 を表示します。

この問題を解決するには、dsdump ツールを終了してから、iMonitor を開始します。

Windows の場合

dsbrowse ツールまたは dsedit ツールが iMonitor と同時に実行されていると、iMonitor がエラー -672 を表示します。

この問題を解決するには、dsbrowse ツールおよび dsedit ツールを終了してから、iMonitor を開始します。

7.8 タイムスタンプが 16 進数形式で表示される

Time 構文属性を 1970 年 1 月 1 日より前の値に設定すると、iMonitor はこの属性のタイムスタンプを標準の日時形式ではなく 16 進数形式で表示します。iMonitor は、1970 年 1 月 1 日以降の値をとるすべての属性を日時形式で表示します。

7.9 Internet Explorer 10 での iMonitor トレース設定の問題

iMonitor のトレース設定を Internet Explorer 10 で使用できません。

この問題を回避するには、Internet Explorer 10 を互換モードで起動し、iMonitor のアドレスを［信頼済みサイト］のリストに追加してから、ブラウザを再起動します。

8 iManager

8.1 Quick Create を使用した新しい LDAP グループの作成後に LDAP 操作に失敗する

Quick Create は、ユーザが後で変更できるダミー属性を持つ LDAP グループオブジェクトのみを作成します。Quick Create では、バージョン 12 ではなくバージョン 11 によって LDAP グループオブジェクトが作成されます。そのため、すべての LDAP 操作は失敗します。これは、バージョンに互換性がないことによってどの LDAP サーバとも関連付けることができないためです。

この問題を回避するには、Quick Create を使用して LDAP を作成した後、LDAP グループオブジェクトバージョン番号を 12 に変更します。

9 破損通知

破損通知は、削除、移動、名前変更、復元などの操作中に、eDirectory が参照整合性を保持するためにオブジェクトに付加する操作属性です。たとえば、グループ A にユーザ B というメンバーが含まれているとき、ユーザ B が削除されると、ディレクトリは自動的にグループ A からユーザ B への参照を削除します。eDirectory 8.8 SP8 では、削除、移動、および名前変更の操作によって生成される破損通知が、デフォルトで最適化されます。

注 : 破損通知を含むオブジェクトは、エージェントのアウトバウンド同期の実行時、およびインバウンド同期サイクルの最後に実行されるようにスケジュールされている破損通知処理の実行時に調査の対象となります。

破損通知には大きく分類して 3 つの種類があります。

- プライマリ破損通知には、停止 (0001)、復元 (0000)、移動 (0002)、新規 RDN(0005)、およびツリーの新規 RDN(0008) の各種類がありあます。
- セカンダリ破損通知は、一般的にプライマリ破損通知に関連付けられており、プライマリ破損通知で指定された操作の通知が必要なエージェントおよびパーティションを表します。セカンダリ破損通知には、バックリンク (0006)、使用中 (000C)、およびツリーの移動 (000a) の各種類があります。
- トラッキング破損通知には移動禁止 (0003)、古い RDN(0004)、およびツリーの古い RDN(0007) の各種類があります。

トラッキング破損通知以外の破損通知は、次の同期ステータスのセットを使用して移動する必要があります。

- 初期化ステータスまたは発行済み (0)
- 通知済み (1)
- パージ準備完了 (2)
- パージ可能 (4)

ステータスは破損通知属性のフラグフィールドで記録されます。破損通知が次のステータスに進む前に、現在のステータスは必ず実オブジェクトのすべてのレプリカに同期されます。リング内のすべてのレプリカが破損通知ステータスを与えられているかどうかを判断するために、遷移ベクトルからベクトルが計算されます。eDirectory 8.6 以降では、保存されていない破損通知ベクトルが使用されます。以前のバージョンの eDirectory では、パージベクトルが使用されます。破損通知の変更タイムスタンプ (MTS) が計測ベクトルよりも古い場合、担当サーバは該当する破損通知を次のステータスに進めることができます。

「バックリンク」のセカンダリ破損通知の場合、該当する破損通知を含むオブジェクトのマスタレプリカを持つエージェントがステータスを進めます。「使用中」のセカンダリ破損通知の場合、レプリカが存在している間は該当する破損通知を作成したエージェントがステータスを進めます。レプリカが存在しない場合、パーティションのマスタを保持しているエージェントが「使用中」の破損通知のステータスを進めます。「ツリーの移動」の破損通知の場合、ルートパーティションのマスタがステータスを進めます。

プライマリ破損通知は、すべてのセカンダリ破損通知が最後のステータスまで進められた後でのみ、ステータスを進めることができます。プライマリ破損通知が最後のステータスまで進んだ後で、そのステータスがリング内のすべてのサーバに同期されると、残っているのは属性を持たないオブジェクトであるオブジェクトハスクのみとなり、これらはシステムのパージプロセスによってパージされます。トラッキング破損通知は、プライマリ破損通知の削除の準備が完了した後か、Inhibit_move の場合はプライマリ破損通知がマスタレプリカの OBF_NOTIFIED ステータスに移動された後で削除されます。

破損通知の処理を担当するレプリカは、指定したパーティションがインバウンド同期サイクルを終了した後で、パーティションごとにスケジュールされているバックグラウンド処理 (破損通知処理) を実行します。パーティションにその他のレプリカがない場合、アウトバウンドレプリケーション処理がハートビート間隔でスケジュールされたままになります。その後、アウトバウンドレプリケーション処理によって破損通知処理が開始されます。破損通知処理は手動ではスケジュールできず、また、その必要もありません。同期化が実行されると、遷移ベクトルが更新され、パージベクトルおよび Obit ベクトルを進めます。これらのベクトルが進められると、破損通知のステータスを進めることができます。これと同時に、インバウンド同期に自動スケジュールが実行されると、破損通知処理サイクルが完了します。すなわち、破損通知処理の起動要因はオブジェクト同期です。

削除されたオブジェクトの場合、「停止」のプライマリ破損通知に関連するすべての破損通知が最後のステータス (パージ可能) まで進められ、そのステータスがすべてのレプリカに同期された後で、新しい処理がデータベースに残っているエントリハスクの削除を担当します。これらのハスクを削除するために、パージ処理が自動的に実行されます。パージプロセスのスケジュールおよび自動スケジュール間隔の調整は、iMonitor のエージェント環境設定ページを使用して手動で設定することができます。

9.1 例

このセクションでは、次の例を紹介します。

- 60 ページの 「オブジェクトの削除」
- 61 ページの 「オブジェクトの移動」

9.1.1 オブジェクトの削除

1. プライマリ破損通知 OBT_DEAD を追加します。

   バックリンクの属性には、このオブジェクトに関連し、このエントリに対する変更を通知する必要のあるサーバのリストが含まれています。バックリンクの属性のリストに含まれる各 DN およびエントリのパーティションレプリカ属性のリストに含まれるすべてのサーバに対して、eDirectory はバックリンク破損通知を追加します。プライマリ破損通知 (OBT_DEAD) の作成時刻は、セカンダリ破損通知に保存されます。

   使用中の属性には、このオブジェクトに関連し、このエントリに対する変更を通知する必要のあるパーティションのリストが含まれています。使用中の属性のリストに含まれているすべての DN に対して、eDirectory は使用中の破損通知を追加します。プライマリ破損通知 (OBT_DEAD) の作成時刻は、セカンダリ破損通知に保存されます。

2. 破損通知以外のすべての属性を削除します。

   次に、アウトバウンドレプリケーションプロセスによって、レプリカリング内にある他のすべてのサーバに変更が同期されます。

このパーティションの次回のインバウンド同期が実行されるときに、破損通知処理が開始され、次の処理が実行されます。

- 最小遷移ベクトルである時間ベクトルを計算し、パージベクトルとして参照されます。比較的新しいバージョンの eDirectory では、2 番目に小さいベクトルが計算されます。このベクトルは、サブオーディネートリファレンスのレプリカではなく、破損通知ベクトルと呼ばれます。
- このパーティション内にあるそれぞれの破損通知が検査されます。

  該当する破損通知がプライマリ破損通知で、セカンダリ破損通知がなく、破損通知の属性変更タイムスタンプ (MTS) がパージベクトルよりも古い場合、すべてのサーバが変更を確認済みとしてこの破損通知は削除されます。

  該当する破損通知がバックリンク破損通知で、このサーバがマスタの場合、このサーバが破損通知の処理を担当します。

  重要 : ステータスが完了していない場合、このステータスに必要な操作を実行します。これは外部参照を通知するときに最も頻繁に実行されます。

  該当する破損通知が使用中の破損通知で、(破損通知の MTS のレプリカ番号とローカルのレプリカ番号の比較から判断して) このサーバで削除が発生している場合、このサーバがこの破損通知の処理を担当します。
- このサーバが特定のセカンダリ破損通知のタイプ (バックリンクまたは使用中) の処理を担当し、1 つのエントリ内にある該当するタイプのすべてのセカンダリ破損通知が同じステータスであり、該当するステータスに必要な処理 (たとえば、サーバへの通知) がすべての破損通知で完了していて、さらにその破損通知のタイプの MTS が破損通知ベクトルよりも古い場合、該当するタイプのすべてのセカンダリ破損通知を次のステータスに進めることができます。

9.1.2 オブジェクトの移動

移動は削除と非常によく似ていますが、次に挙げる操作が違います。

- プライマリ破損通知が移動元に配置される前に、エントリの一部が移動先のコンテナに作成され、そのエントリの一部にトラッキング破損通知 (OBT_INHIBIT_MOVE) が配置されます。このトラッキング破損通知は、エントリが移動元から完全に移動される前にエントリが移動されたり、パーティション操作に加わるのを防ぐために配置されます。
- ソースエントリでは、プライマリ破損通知は OBT_MOVED です。
- プライマリ破損通知(OBT_MOVED)のステータスが通知済み(ソースのすべてのレプリカにエントリが移動されたことを通知した状態) になり、すべての外部参照に通知が完了すると、トラッキング破損通知 (OBT_INHIBIT_MOVE) が移動先エントリから削除されます。

9.2 予防策

定期的に iMonitor サーバ情報レポートを実行してください。このレポートは、ツリー全体を調べて、検索可能な各 NCP サーバと通信し、検知したすべてのエラーをレポートします。このレポートを使用して、時刻同期および Limber の問題を診断できます。また、現在のサーバ自体が他のすべてのサーバと通信可能であると認識しているかどうかも知ることができます。環境設定ページで選択

されている場合、サーバはツリー内にある各サーバの NDS エージェントヘルス情報を生成することもできます。サーバ情報レポートの実行に関する詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「レポートの設定と表示」を参照してください。

iMonitor2.0 以降のバージョンを使用する場合は、[Errors and Health sub-report] のレポートオプションが有効になっていることを確認してください。レポートでは次の項目が確認されます。レポートを参照し、エラーがないことを確認してください。

- iMonitor に保存されている ndsimonhealth 環境設定ファイルの情報に基づき (『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「環境設定ファイル」を参照)、ツリー全体で正しいディレクトリパッチを実行していることを確認するために eDirectory エージェントのバージョンをチェックする。
- すべてのサーバが Timesync の許容範囲内にある。
- このサーバが他のすべてのサーバと通信できる。
- このツリーから不適切または不完全に削除されたサーバがない。
- ヘルスサブレポートで、レプリケーション同期時刻の許容範囲外にパーティションがあるかどうかを確認する。

iMonitor1.5 を使用する場合はエラーレポートオプションを選択します。レポートでは次の項目が確認されます。レポートを参照し、エラーがないことを確認してください。

- エージェントのバージョンが表示される。ツリー内のすべてのサーバで、NetIQ Support の Web サイト (http://support.novell.com) から入手できる最新の eDirectory Support Pack が実行されている。
- すべてのサーバが Timesync の許容範囲内にある。
- このサーバが他のすべてのサーバと通信できる。
- このツリーから不適切または不完全に削除されたサーバがない。

iMonitor 破損通知リスティングレポートまたは iMonitor オブジェクト統計情報レポートを使用して、システムにある破損通知を検索できます。処理が実行されていないと思われる破損通知を見つけた場合は、「62 ページのセクション 9.3「トラブルシューティングのヒント」」を参照してください。

9.3 トラブルシューティングのヒント

破損通知が処理されない一般的な理由が 2 つあります。それは、破損通知が孤立している場合 (破損通知がすべてのサーバではなく一部のサーバにのみ存在する場合)、または破損通知が停止している場合 (破損通知がすべてのサーバに存在するが、ステータスが何らかの理由で進まない場合) です。

次の項目を参照して、孤立または停止した破損通知の問題を解決してください。

- ❒ 慌てないでください！
- ❒ オブジェクトの破損通知がこのサーバに保存されていない(該当するオブジェクトが外部参照の) 場合、次を実行します。
  - 一致する破損通知が実オブジェクトに含まれているかどうかをチェックします。一致する破損通知が含まれていない場合、この破損通知は孤立しています。詳細については、64 ページの 「外部参照の孤立した破損通知の解決」を参照してください。
  - 一致する破損通知が実オブジェクトに含まれている場合、実オブジェクトの破損通知の問題を解決してから、外部参照にある破損通知の問題を特定してください。

- ❒ 破損通知が正確に同期されていることを確認してください。
  - iMonitor のエージェント同期のページを使用して同期エラーをチェックおよび解決してください。
  - 破損通知は、レプリカリングのコピーを保持するすべてのエージェントがステータスの変更を確認した後でのみステータスを変更できます。すべてのレプリカがデータを認識したことを確認するには、次のようないくつかの方法があります。

    破損通知を含むエントリを参照しながら、エントリ同期リンクをクリックします。すべてのレプリカに同期されていない属性がすべて表示されます。

    破損通知属性値の中で、最も古いタイムスタンプを検索します。検索されたタイムスタンプの時刻と現在時刻の差が、パーティション同期ページの最大リングデルタフィールドの間隔よりも大きい必要があります。

    遷移ベクトルを調査します。
- ❒ すべてのサーバ通信が機能していることを確認するには、iMonitor のサーバ情報レポートを実行します。
- ❒ エラーを検索するには、エージェントプロセスステータス : 破損通知を検査してください。
  - エージェントプロセスステータス : 破損通知で起こりうる一般的な問題には、次のものがあります。

    -625、-622、-634、および -635 の通信エラー。詳細については、サーバ情報レポートを参照してください。

    -601 および -603 は、適切に削除されていないサーバ、またはサーバオブジェクトに不明なベースクラスが含まれるサーバを示します。
  - このページに表示されるエラーは致命的なものではありません。そのパーティションで破損通知処理が次回実行されるときに、この操作が再試行されます。このページに表示された問題を解決して、再試行まで待機してください。
- ❒ 破損通知オブジェクトを表示した状態で、リング周辺の破損通知を比較しながらレプリカリングを調べます。
  - 破損通知のコピーがないレプリカがあり、すべての属性値がパージ可能ではない場合、このオブジェクトはレプリカリング周辺で矛盾しており、破損通知が孤立していると考えられます。詳細については、64 ページの 「孤立した破損通知の解決」を参照してください。
  - オブジェクトがすべてのレプリカに矛盾なく存在している場合、同期エラー、または破損通知処理にエラーが発生しているために次のステータスに進まない可能性があります。
- ❒ 必要に応じて Trace の［破損通知］オプションを有効にして、破損通知処理の詳細を検査してください。
- ❒ 今後、破損通知の問題を回避するには、eDirectory 8.6 の最新のサポートパックにアップグレードしてください。破損通知についての既知の問題がすべて修正されています。

9.3.1 解決方法

「62 ページのセクション 9.3「トラブルシューティングのヒント」」を参照して、適切な解決方法を使用してください。

これらの解決方法を使用する前に、データが安全であることを確認してください。ディレクトリデータベースファイル、サーバ環境設定、およびトラスティのバックアップが必要となる場合があります。成功率を高め、今後生じる問題を最小限に抑えるためには、最新の eDirectory サポートパックにアップグレードしてください。

孤立した破損通知の解決

- **推奨される方法 :** レプリカリング内のサーバのいずれかに eDirectory 8.6 以降のバージョンを使用する場合、iMonitor のオブジェクトを参照し、［Send Single Entry］を選択します。これにより、その他のすべてのレプリカに信頼されていない送信が実行されます。
- **避けるべき方法 :** 孤立した破損通知のコピーを持つレプリカリングにあるすべてのサーバが eDirectory 8.6 よりも前のバージョンの場合、DSBrowse を -a オプションでロードして、オブジェクトを参照し、エントリにタイムスタンプを設定します。これにより、このサーバに存在するオブジェクトを信頼されたコピーとして指定します。Novell では、実際にはオブジェクトを信頼されたオブジェクトとして指定することはお勧めしません。

外部参照の孤立した破損通知の解決

- **推奨されない方法 :** タイムスタンプオプションが選択されている DSRepair を実行します。
- **推奨されない方法 :** 実レプリカをサーバに移動し、使用可能な状態になってから破損通知が処理されるのを待ちます。破損通知が処理されない場合は、「62 ページのセクション 9.3「トラブルシューティングのヒント」」にある情報を参照して実レプリカに移動されたオブジェクトの問題を解決してください。破損通知が処理されたら、レプリカは削除してもかまいません。

9.3.2 以前の操作

過去には、停止した破損通知を解決するためにいくつかの異なる手段をとりました。これらの手段の一部は、費用のかかるパーティション操作、または将来的に問題の原因となる可能性のあるドキュメント化されていない機能の使用に関連しています。

1 つ目に使用されていたのは、マスタを保持しているレプリカを切り替える方法です。マスタはさまざまなステータスを通じてバックリンクの破損通知の移動を担当しているエージェントなので、この手段が有効な場合もあります。レプリカに矛盾がありマスタが削除されたオブジェクトを保持していない場合、該当するマスタを、破損通知と一緒に削除されたエントリを保持していたエージェントに切り替えると、新規エージェントに破損通知のステータスを次に進めてパージすることのできるライセンスが与えられます。［Send Single Entry］を選択すると、より確実で危険性の低い方法で、レプリカの矛盾が原因で停止している破損通知の問題を解決します。

2 つ目に使用されていたのは、DSRepair を実行してすべての破損通知を削除するスイッチを使用する方法です。(DSRepair を起動して、停止している破損通知を解決するサードパーティ製のアプリケーションがあります。) この方法はお勧めできません。これらのスイッチを使用すると、このエージェントにあるすべての破損通知が削除されます。したがって停止していない破損通知も削除される可能性があり、レプリカの矛盾性がさらに深まり、より多くの停止している破損通知が作成される場合があります。これは分散された操作ではないので、停止している破損通知のあるすべてのサーバで DSRepair を実行する必要があります。この操作は、これらのサーバの 1 つで処理未了のまま削除されてしまうパーティションの破損通知を取得する可能性を高めます。処理未了のまま破損通知を削除すると、孤立した破損通知を新たに生み出す可能性があり、その結果として数年後にレプリカタイプの変更、新規レプリカの追加、またはその他のパーティション操作を実行したときに問題が生じる場合があります。

3 つ目に使用されていたのは、カスタムモード操作で DSBrowse を使用してエントリにタイムスタンプを設定するか、または RSRepair で -0T スイッチを使用してオブジェクトを信頼されたオブジェクトに指定する方法です。この操作によりエントリは信頼されたエントリに指定され、他のすべてのレプリカにこのエントリを同期します。その他のサーバで変更されたデータを失う可能性があるので、この操作の実行には細心の注意を払う必要があります。破損通知のクリーンアップの方法としては、なるべく使用しないことをお勧めします。

10 NetIQ eDirectory への移行

この章では、次の製品から NetIQ eDirectory に移行する方法について説明します。

- 65 ページのセクション 10.1「Sun One スキーマの NetIQ eDirectory への移行」
- 68 ページのセクション 10.2「ICE を使用した、アクティブディレクトリスキーマの NetIQ eDirectory への移行」

10.1 Sun One スキーマの NetIQ eDirectory への移行

Sun One スキーマを NetIQ eDirectory に移行するには、次の手順に従ってください。

65 ページの 「手順 1: スキーマキャッシュの更新操作を実行する」
65 ページの 「手順 2: エラーを解決するためにエラー LDIF ファイルを訂正する」
68 ページの 「手順 3: LDIF ファイルをインポートする」

10.1.1 手順 1: スキーマキャッシュの更新操作を実行する

次のコマンドを使用して、スキーマの比較中に検出されたエラーをエラーファイルに書き込むことができます。

```
ice -e LDIF error file name -C -a -SLDAP -s Sun ONE server -p Sun ONE port -DLDAP -
s eDirectory server -p eDirectory port
```

次に例を示します。

```
ice -e err.ldf -C -a -SLDAP -s sun_srv1 -p sun_port1 -DLDAP -s edir_srv2 -p
edir_port2
```

スキーマの比較中に検出されたエラーはすべてエラーファイル (例では err.ldf) に書き込まれます。Root DSE を読み込むためにサーバから認証が要求されない限り、この操作を実行するためにログインする必要はありません。Microsoft アクティブディレクトリでは、Root DSE を読み込むための認証が要求されます。

10.1.2 手順 2: エラーを解決するためにエラー LDIF ファイルを訂正する

- Sun ONE では、eDirectory では定義されていないいくつかのスキーマ定義が公式に定義されています。これらの定義には、objectClasses、attributeTypes、ldapSyntaxes および subschemSubentry などの属性が含まれます。これらの定義は内部に存在し、スキーマにとって非常に重要です。したがって、これらの定義を変更することはできません。これらの定義を変更しようとすると、次のエラーが発生します。

  LDAP エラー : 53 (DSA が動作しません)

  これらの定義の参照が含まれるすべてのレコードに対して、次のエラーが表示されます。

LDAP エラー : 16 : (該当する属性はありません)

したがって、これらのオブジェクトへの参照が含まれるレコードまたはこれらの定義の変更を試行するレコードは、LDIF エラーファイル (例では err.ldf) にコメントとして記入されている必要があります。

- 一部の Sun ONE の objectClasses 定義にはネーミング属性がありません。これらの objectClasses を追加すると、eDirectory で次のエラーが発生することがあります。

  LDAP エラー : 80 (NDS エラー : ネーミングがあいまいです (-651)

  このエラーは、Sun ONE では eDirectory とは異なるネーミングルールの決定のメソッドが使用されていることが原因で発生します。

  これを解決するには、次の 3 つのいずれかのオプションを使用できます。

  オプション 1:

  エラーの原因となっている各 objectClasses を確認し、それぞれに有効なネーミング属性を追加します。

  次に例を示します。

  ネーミング属性［cn］をオブジェクトクラス netscapeMachineData に追加するには、X-NDS_NAMING フラグが包含されるように err.ldf ファイル内のエントリ (次の例で*強調表示*されている部分) を次のように変更します。

```
dn: cn=schemachangetype: modifyadd: objectClassesobjectClasses: (
2.16.840.1.113730.3.2.32 NAME 'netscapeMachineData'
    DESC 'iPlanet defined objectclass' SUP top STRUCTURAL MAY 'cn'     X-
NDS_NAMING 'cn' )-
```

  オプション 2:

  エラーの原因となっている各 objectClasses を確認し、該当するものをすべて AUXILIARY または ABSTRACT に変更します。

  次に例を示します。

  netscapeMachineData のオブジェクトクラス定義を “STRUCTURAL” から “AUXILIARY” に変更するには、次のように err.ldf ファイルのエントリ (次の例で*強調表示*されている部分) を変更します。

```
dn: cn=schemachangetype: modifyadd: objectClassesobjectClasses: (
2.16.840.1.113730.3.2.32 NAME 'netscapeMachineData'
   DESC 'iPlanet defined objectclass' SUP top AUXILIARY )-
```

  netscapeMachineData のオブジェクトクラス定義を “STRUCTURAL” から “ABSTRACT” に変更するには、次のように err.ldf ファイルのエントリ (次の例で*強調表示*されている部分) を変更します。

```
dn: cn=schemachangetype: modifyadd: objectClassesobjectClasses: (
2.16.840.1.113730.3.2.32 NAME 'netscapeMachineData'
   DESC 'iPlanet defined objectclass' SUP top ABSTRACT )-
```

  オプション 3:

  eDirectory の Top の定義に cn を追加すると、すべての objectClasses の潜在的なネーミング属性になります。

  cn を Top に追加するには 2 つの方法があります。

  - **方法 1:**

    次のようなファイルを作成し、topsch.ldf と命名します。

```
version : 1

dn:cn=schema

changetype :modify

delete : objectclasses

objectclasses : ( 2.5.6.0 NAME 'top' STRUCTURAL )

-

add:objectclasses

objectclasses : (2.5.6.0 NAME 'top' STRUCTURAL MAY cn)
```

次の NetIQ インポート / エクスポート変換コマンドラインを使用します。

```
ice -SLDIF -f LDIF_file_name -DLDAP -s eDirectory_server -p eDirectory_port
-d eDirectory_Admin_DN -w eDirectory_password
```

次に例を示します。

```
ice -SLDIF -f topsch.ldf -DLDAP -s edir_srv2 -p edir_port2 -d
cn=admin,o=org -w pwd1
```

- **方法 2:**

  1. NetIQ iManager で、［*役割およびタスク*］ボタン をクリックします。
  2. ［*スキーマ*］>［*属性の追加*］の順にクリックします。
  3. ［*使用可能なクラス*］リストで［*トップ*］を選択してから、［*OK*］をクリックします。
  4. ［*使用可能なオプション属性*］リストで、［*CN*］をダブルクリックします。
  5. [*OK*] をクリックします。

- 一部の objectClass 定義には、必須属性リストとして userPassword が含まれる場合があります。これらの objectClasses を eDirectory に追加すると、次のエラーが発生します。

  LDAP エラー : 16 (該当する属性はありません)

  このエラーを解決するには、objectClass 定義を変更して、ndsLoginProperties から新しい objectClass を継承し、必須属性リストから userPassword 属性を削除します。

  次に例を示します。

  必須属性リストに userPassword が含まれる objectClass の場合 :

```
version : 1
dn: cn=schemaz
changetype: modify
add: objectClasses
objectClasses: ( 0.9.2342.19200300.100.4.19 NAME 'simpleSecurityObject' DESC '
 Standard LDAP objectClass' SUP top STRUCTURAL MUST userPassword )
```

  次のように変更する必要があります (最終行の変更に注意してください):

```
version : 1
dn: cn=schema
changetype: modify
add: objectClasses
objectClasses: ( 0.9.2342.19200300.100.4.19 NAME 'simpleSecurityObject' DESC '
 Standard LDAP objectClass' SUP (ndsLoginProperties $ top) STRUCTURAL )
```

10.1.3 手順 3: LDIF ファイルをインポートする

次の NetIQ インポート / エクスポート変換コマンドを使用して変更されたスキーマ比較 LDIF ファイル (例では err.ldf) をインポートします。

```
ice -e error_file -SLDIF -f modified_LDIF_file -DLDAP -s eDirectory_server -p
eDirectory_port -d eDirectory_Admin_DN -w eDirectory_password
```

次に例を示します。

```
ice -e errors.ldf -SLDIF -f err.ldf -DLDAP -s edir_srv2 -p edir_port2 -d
cn=admin,o=org -w pwd1
```

10.2 ICE を使用した、アクティブディレクトリスキーマの NetIQ eDirectory への移行

ICE を使用して、スキーマをアクティブディレクトリから NetIQ eDirectory に移行すると、あいまいなネーミングエラー (-651) というエラーメッセージが表示され、スキーマの Computer オブジェクトクラスへの移行が失敗します。

これを解決するには、次の手順を実行します。

65 ページの 「手順 1: スキーマキャッシュの更新操作を実行する」
65 ページの 「手順 2: エラーを解決するためにエラー LDIF ファイルを訂正する」
68 ページの 「手順 3: LDIF ファイルをインポートする」

10.2.1 手順 1: スキーマキャッシュの更新操作を実行する

ICE を使用して、スキーマをアクティブディレクトリから NetIQ eDirectory へ移行し、次のように ICE のエラーログオプション (-e) が提供されていることを確認します。

```
ice -e error_file -S ldap -s Active_Directory_server -p Active_Directory_port -d
Active_Directory_full_admin_context -w Active_Directory_password -D ldap -s
eDirectory_server -p eDirectory_port -d eDirectory_full_admin_context -w
eDirectory_password
```

次に例を示します。

```
ice -e err.ldf -S ldap -s activesrv1 -p activeport1 -d cn=admin,o=company -w
activepwd -D ldap -s edirsrv2 -p edirport2 -d cn=admin,o=company -w edirpwd
```

10.2.2 手順 2: エラーを解決するためにエラー LDIF ファイルを訂正する

失敗したエントリは次のように err.ldf ファイルに記述されています。

```
dn: cn=schema

changetype: modify

delete: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' )

-

add: objectclasses
```

```
objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' SUP (device $
 user ) STRUCTURAL MAY (operator $ server $ status $ cn $ networkAddress $
 local PolicyFlags $ defaultLocalPolicyObject $ machineRole $ location $
 netbootInitialization $ netbootGUID $ netbootMachineFilePath $ siteGUID $
 operatingSystem $ operatingSystemVersion $ operatingSystemServicePack $
 operatingSystemHotfix $ volumeCount $ physicalLocationObject $ dNSHostName
 $ policyReplicationFlags $ managedBy $ rIDSetReferences $ catalogs $
 netbootSIFFile $ netboot MirrorDataFile ) X-NDS_NOT_CONTAINER '1' X
 -NDS_NONREMOVABLE '1' X-NDS_NAME 'Computer' )

-
```

次の例で強調表示されている部分のように、エラーファイル (例では err.ldf) でこのエントリを編集して、Computer オブジェクトクラスの定義にあるスーペリアオブジェクトクラスのリストから user オブジェクトクラスを削除します。

```
dn: cn=schema

changetype: modify

delete: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' )

-

add: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' SUP device
 STRUCTURAL MAY (operator $ server $ status $ cn $ networkAddress $ local
 PolicyFlags $ defaultLocalPolicyObject $ machineRole $ location $
 netbootInitialization $ netbootGUID $ netbootMachineFilePath $ siteGUID $
 operatingSystem $ operatingSystemVersion $ operatingSystemServicePack $
 operatingSystemHotfix $ volumeCount $ physicalLocationObject $ dNSHostName
 $ policyReplicationFlags $ managedBy $ rIDSetReferences $ catalogs $
 netbootSIFFile $ netbootMirrorDataFile ) X-NDS_NOT_CONTAINER '1' X
 -NDS_NONREMOVABLE '1' X-NDS_NAME 'Computer' )

-
```

10.2.3 手順 3: LDIF ファイルをインポートする

次の ICE コマンドを使用して、変更されたエントリをインポートします。

```
ice -S ldif -f LDIF_file -D ldap -s Novell_eDirectory_server -p port_number -d
full_admin_context -w password
```

次に例を示します。

```
ice -S ldif -f err.ldf -D ldap -s edirsrv1 -p edirport1 -d cn=admin,o=company -w
pwd1
```

10.3 OpenLDAP から NetIQ eDirectory への移行

10.3.1 前提条件

OpenLDAP サーバから移行したデータは、MD5 パスワードを含んでいることがあります。この場合、適切な NetIQ モジュラー認証サービス (NMAS) メソッドがインストールされていないと、アプリケーションが中断することがあります。NMAS メソッドの SimplePassword を、次に示すコマンドを使用して NetIQ eDirectory 用にインストールする必要があります。

nmasinst -addmethod *admin_contexttreenameconfigfile* -h *Hostname*:*port*-w *password*

例 : nmasinst -addmethod admin.novell eDir-Tree /Linux/eDirectory/nmas/NmasMethods/Novell/SimplePassword/config.txt -h eDir_srv:524 -w secret

10.3.2 OpenLDAP スキーマの eDirectory への移行

OpenLDAP スキーマを eDirectory に移行するには、次の手順に従ってください。

- 70 ページの 「手順 1: スキーマキャッシュの更新操作を実行する」
- 70 ページの 「手順 2: エラーを解決するためにエラー LDIF ファイルを訂正する」

手順 1: スキーマキャッシュの更新操作を実行する

次のコマンドを使用して、スキーマの比較中に検出されたエラーをエラーファイルに書き込むことができます。

```
ice -e error_file -C -a -S ldap -s OpenLDAP_server -p Open_LDAP_port - D ldap -s
eDirectory_server -p eDirectory_port -d eDirectory_full_admin_context -w
eDirectory_password
```

次に例を示します。

```
ice -e err.ldf -C -a -SLDAP -s open_srv1 -p open_port1 -DLDAP -s edir_srv2 -p
edir_port2 -d cn=admin,o=novell -w secret
```

スキーマの比較中に検出されたエラーはすべてエラーファイル (例では err.ldf) に書き込まれます。

手順 2: エラーを解決するためにエラー LDIF ファイルを訂正する

Open LDAP では、いくつかのスキーマ定義が公式に定義されています。これらの定義には、objectClasses、attributeTypes、ldapSyntaxes、および subschemSubentry などの属性が含まれます。これらの定義は内部に存在し、スキーマにとって非常に重要です。したがって、これらの定義を変更することはできません。これらの定義を変更しようとすると、次のエラーが発生します。

```
LDAP error : 53 (DSA is unwilling to perform)
```

これらの定義の参照が含まれるすべてのレコードに対して、次のエラーが表示されます。

```
LDAP error : 16 ( No such attribute )
```

したがって、これらのオブジェクトへの参照が含まれるレコードまたはこれらの定義の変更を試行するレコードは、LDIF エラーファイル (例では err.ldf) にコメントとして記入されている必要があります。

10.3.3 Open LDAP データの NetIQ eDirectory への移行

次のコマンドを実行してデータを移行します。

```
ice -e error_data.ldif -SLDAP -s OpenLDAP_server -p OpenLDAP_port  -d admin_context
-w password -t -b dc=blr,dc=novell,dc=com -F objectclass=* -DLDAP -d  admin_context
-w password  -l  -F
```

次に例を示します。

```
ice -e err_data.ldif -SLDAP -s open_srv1 -p open_port1  -d
cn=administrator,dc=blr,dc=novell,dc=com -w secret1 -t -b dc=blr,dc=novell,dc=com
-F objectclass=* -DLDAP -d cn=admin,o=novell -w secret2 -l -F
```

オブジェクトによっては、前方参照やオブジェクトへの内部依存のために失敗するものもありますが、アプリケーションが中断することはほとんどありません。

10.3.4 移行後に PAM を NetIQ eDirectory で動作可能にする

OpenLDAP から eDirectory に移行したら、PAM が eDirectory で動作するようにするため、いくつか変更する必要があります。

/etc/ldap.conf ファイルの変更

```
# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
  binddn cn=admin,o=acme
  ...
# The credentials to bind with.
# Optional: default is no credential.
  bindpw secret
  ...
# The search scope.
  scope sub
  ...
# Filter to AND with uid=%s
  pam_filter objectclass=inetorgperson
  ...
# Remove old password first, then update in
# cleartext. Necessary for use with Novell
# Directory Services (NDS)
  pam_password nds
  ...
  ssl off
  ...
```

ディレクトリ内のデータの変更

この変更は、OpenLDAP のユーザオブジェクトでパスワードのハッシュアルゴリズムとして CRYPT を使用するシナリオにのみ行います。

iManager を使用して、規定値のある次の属性を、すべてのユーザオブジェクトを持つコンテナに追加します。

属性 : sasDefaultLoginSequence

値 : 単純パスワード

11 スキーマ

このセクションには、スキーマのトラブルシューティングについての情報が含まれています。

スキーマのトラブルシューティング

オブジェクトから補助クラスを分離しても、値が即時に削除されることはなく、存在しないというマークが付けられます。オブジェクトの実際の検証中に DRL プロセスがそれらの値をクリーンアップするまで、補助クラスはエントリに関連付けられています。

DRL はリソースを消費するバックグラウンドプロセスであるため、このクリーンアップの間は他の操作が遅くなります。クリーンアッププロセスに要する時間は、システム内に実際にあるオブジェクトおよび外部参照の数によって決まります。この処理は CPU とメモリに負荷がかかるため、頻繁に実行しないでください。デフォルトでは、Backlinker バックグラウンドプロセスは、ndsd が開始した 50 分後に実行され、その後 13 時間ごとに実行されます。

エントリから補助クラスをクリアするには 0 ～ 13 時間かかることがあり、それに加えてシステム内でそのエントリを処理するにも時間がかかります。

この問題を回避するには、DSTrace または iMonitor から Backlinker をトリガーして、補助クラスのエントリを削除します。

注 : オブジェクトが削除されると、値は即時にパージされます。この削除は他のバックグラウンドプロセスによって処理されるからです。

---

12 DSRepair

12.1 Linux 上の NFS マウントされた DIB での DSRepair の実行

Linux システム上の NFS マウントされた DIB で ndsrepair (DSRepair) 操作を実行しようとすると、-732 エラーまたは -6009 エラーが表示される可能性があります。

12.2 -R オプションを指定して DSRepair を実行したときにハングアップする

インデックス化された属性で暗号化属性を有効化した後に、-R オプションを指定して ndsrepair (DSRepair) を実行すると、ハングアップします。

12.3 アップグレードまたは移行後の DSRepair の実行

8.7.3.x サーバからのアップグレードまたは移行後に DSRepair 標準を実行すると、［エントリの先祖 ID リストが無効です］というエラーメッセージが表示されます。

先祖 ID アップグレードは、DIB のアップグレードまたは移行のプロセス終了後、バックグラウンドプロセスの一環として行われるため、このエラーは無視することができます。

13 複製

eDirectory では、NetIQ の強力なディレクトリサービス、および複製による障害対策が提供されています。複製により、eDirectory データベースまたはその一部のコピーを、複数のサーバで同時に保持できます。

13.1 暗号化された複製に関する問題

13.1.1 iManager を使用した暗号化複製の設定

レプリカリング内のいずれかのサーバが停止している場合は、iManager を使用して暗号化複製を設定することはできません。

13.1.2 暗号化複製が有効になっているツリーのマージに失敗する

暗号化複製が有効になっている場合、ツリーのマージに失敗します。マージを行う前に、各ツリーでセキュリティ保護された複製を無効にします。

13.2 eDirectory レプリカ問題から回復する

eDirectory パーティションのレプリカは、常に複数作成しておいてください。レプリカを複数作成しておくことで、あるレプリカがハードディスクの故障で破損したり失われたりした場合でも、ConsoleOne または NetIQ iManager を使用してそのレプリカを削除し、破損していないレプリカから作成した新しいレプリカに置き換えることができます。

レプリケーションの削除の詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「レプリカを管理する (Administering Replicas) (http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html)」を参照してください。

14 クローン DIB に関する問題

14.1 クローン DIB の -601 および -603 エラーによる失敗

暗号化属性および暗号化複製がツリーレベルで有効になっている場合、クローン DIB は次のエラーにより失敗します。

- SAS の設定時に、ターゲットサーバ上でクローン DIB が -601 エラーにより失敗します。
- クローン DIB の後で、新たに作成されたクローンオブジェクトが -603 エラーにより失敗します。

これらの問題を回避するには、暗号化属性と暗号化複製を無効にします。

14.2 オフラインのバルクロード処理の直後にクローン DIB に失敗する

オフラインのバルクロード処理の直後にサーバのクローンを作成する場合、バルクロード処理がインデックスの無効化オプション付きで行われていると、クローン作成に失敗することがあります。

ただしこの問題は、バルクロード処理の完了後数時間以内に dibclone を実行した場合は発生しません。

14.3 暗号化複製機能を有効にしたクローン作成における問題

ソースサーバで暗号化複製機能を有効にしてクローンを作成する際に、クローン作成されたサーバを一時的に除外するように ER ポリシーを変更します。この設定は、クローン作成されたサーバの設定が完了した後で変更できます。

15 NetIQ パブリックキーインフラストラクチャサービス

15.1 PKI 操作が機能しない

ConsoleOne または iManager で PKI 操作が機能しない場合、NetIQ PKI サービスが Linux で実行されていないことが考えられます。「npki - 1」と入力して PKI サービスを開始してください。

証明書を作成できない場合は、NICI モジュールが正しくインストールされているか確認する必要があります。『*Novell eDirectory 8.8 SP8 管理ガイド*』の「サーバ上の NICI モジュールを初期化する」を参照してください。「」NICI がインストールされているかどうかを確認するには、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「サーバ上に NICI がインストールおよび初期化されているかどうかを確認する」を参照してください。

15.2 重要なレプリカというエラーコードが表示され、既存の eDirectory オブジェクトの別のサーバへの移動が失敗した後に、マルチサーバツリー内でツリーキーサーバとして機能している eDirectory サーバの削除。

この操作を完了するには、［セキュリティコンテナ］>［KAP］以下にある W0 オブジェクトで、キーサーバ DN 属性をこのサーバからツリーキーをダウンロードしたツリー内にある別のサーバに変更します。

1. NetIQ iManager で、［*役割およびタスク*］ボタン をクリックします。
2. ［*eDirectory 管理*］>［*オブジェクトの変更*］の順にクリックします。
3. W0 オブジェクト名およびコンテキスト (通常は、W0.KAP.Security) を指定して、［*OK*］をクリックします。
4. ［*値がある属性*］カラムで、［*NDSPKI:SD キーサーバ DN*］を選択してから、［*編集*］をクリックします。

5 ［*セキュリティドメインキーサーバの DN*］フィールドで別のサーバの名前とコンテキストを指定してから、［*OK*］をクリックします。

6 ［*適用*］をクリックし、［*OK*］をクリックします。

15.3 CA を保持している eDirectory サーバのアンインストール中に、サーバに作成された KMO がツリー内の別のサーバに移動されて無効になる

この場合、ツリーの CA および KMO をもう一度作成する必要があります。詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「組織の認証局オブジェクトを作成する」および「サーバ認証オブジェクトを作成する」を参照してください。

ツリーの CA を保持する eDirectory は、アンインストールしないことをお勧めします。

16 Linux でのユーティリティのトラブルシューティング

16.1 NetIQ インポート / エクスポート変換ユーティリティ

LDAP サーバがリフレッシュまたはアンロードされると、Novell インポート / エクスポート変換操作の実行中に「LBURP operation is timed out」というメッセージが画面上に表示されます。LBURP 操作がタイムアウトした場合、サーバは後で復元されます。

16.2 ndsconfig ユーティリティ

このセクションでは次について説明します。

16.2.1 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。

16.2.2 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。

16.2.3 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。

16.3 ndsmerge ユーティリティ

マージ操作後は、PKI サーバはアクティブになっていません。したがって、npki -l コマンドを使用して再起動する必要があります。

異なるバージョンの製品では、マージ操作が成功しないことがあります。サーバで古いバージョンの NDS または eDirectory が実行されている場合は、最新バージョンの eDirectory にアップデートしてからマージ操作を続行してください。

ツリーに付随する同じ名前のコンテナがソースツリーおよびターゲットツリーの両方にある場合、2 つのツリーのマージは成功しません。どちらかのコンテナ名を変更してから、マージ操作を続行してください。

結合操作の実行中に、「-611 不正な包含ルールです」というエラーメッセージが表示される場合があります。ndsrepair を実行してスキーマを変更します。次に、ndsrepair -S を実行し、［*オプションスキーマ拡張機能*］を選択します。

16.4 DSTrace ユーティリティ

DSTrace 画面をオンにすると、参照リンクに対するプライマリオブジェクトが不正であることを示すエラーメッセージが表示される場合があります。eDirectory が正常に機能している場合は、このメッセージを無視してください。

16.5 ndsbackup ユーティリティ

eDirectory のバックアップの実行中に、「NDS エラー : NDS サーバへの接続に失敗しました」というエラーメッセージが表示される場合があります。これは、デフォルトのポート 524 以外のポートで監視している eDirectory が原因である可能性があります。コマンドラインで、eDirectory が設定されているポート番号を入力します。たとえば、eDirectory がポート番号 1524 に設定されている場合は次のように入力します。

ndsbackup sR 164.99.148.82:1524

eDirectory 8.8 以降で、データのバックアップ中に「NDS エラー : パスワードが必要です」と表示されることがある。これは、サーバに暗号化をマークする属性があるのに、-E オプションを有効にしてバックアップデータを暗号化または復号化していないためです。

16.6 DSRepair の使用

このセクションでは次について説明します。

- 85 ページの 「構文」
- 92 ページのセクション 16.6.2「DSRepair のトラブルシューティング」

サーバコンソールでの DSRepair ユーティリティの用途は次のとおりです。

- 不正なレコード、スキーマの不一致、不正なサーバアドレス、外部参照など、eDirectory の問題を修正する。
- eDirectory スキーマに詳細な変更を加える。
- eDirectory データベースで次の操作を実行する。
  - データベースの終了やデータベースの介入を伴わない、自動的なデータベースの構造チェック。
  - データベースインデックスを確認する。
  - データベースの終了やユーザのロックアウトを伴わず、データベースを修復する。
  - 空のレコードを破棄して、空き領域を増量する。

16.6.1 構文

DSRepair を実行するには、次の構文を使用します。

```
ndsrepair {-U| -P| -S| -C| -E| -N| -T| -J entry_id}
[-A yes|no] [-O yes|no] [-F filename] [-Ad]
```

または

```
ndsrepair -R [-l yes|no [-u yes|no] [-m yes|no] [-i yes|no] [-f yes|no] [-d yes|no]
[-t yes|no] [-o yes|no] [-r yes|no] [-v yes|no] [-c yes|no] [-A yes|no] [-O yes|no]
[-F filename]
```

重要 : -Ad オプションは、NetIQ サポート担当者からの事前の指示がない限り使用しないでください。

DSRepair オプション

オプション	説明
-R	ローカル eDirectory データベースを修復します。eDirectory でオープンおよびアクセスできるように、この修復操作を使用してローカルデータベースの矛盾を解決します。このオプションには、データベースの修復操作を容易にするサブオプションがあります。このオプションにはファンクション修飾子があります。ファンクション修飾子については、「87 ページの 「-R オプションで使用するファンクション修飾子」」で説明されています。NetIQ サポート担当者から特定の操作を手動で実行するように指示された場合を除き、修復にこのオプションを (サブオプションを指定せずに) 使用することをお勧めします。
-P	［レプリカ操作とパーティション操作］オプションです。現在のサーバの eDirectory データベースファイルにレプリカが保存されているパーティションが表示されます。［レプリカオプション］メニューには、「レプリカの修復」、「パーティション操作のキャンセル」、「同期のスケジュール」、および「ローカルレプリカをマスタレプリカとして指定」を実行するオプションがあります。 詳細については、「88 ページの 「［レプリカ操作とパーティション操作］オプション」」を参照してください。
-S	［グローバルスキーマの操作］オプションです。このオプションには、このサーバのスキーマを Tree オブジェクトのマスタに準拠させるのに必要なスキーマ操作がいくつか含まれています。ただし、これらの操作は必要な場合にのみ使用してください。スキーマは、ローカル修復操作および標準修復操作によってすでに検査されています。
-C	［外部参照オブジェクトのチェック］オプションです。各外部参照オブジェクトをチェックして、そのオブジェクトを含むレプリカがあるかどうかを調べます。オブジェクトのあるパーティションレプリカを含むすべてのサーバがアクセス不能の場合、オブジェクトは見つかりません。オブジェクトが見つからない場合、警告が表示されます。
-E	［レプリカ同期のレポート］オプションです。現在のサーバ上にレプリカを持つすべてのパーティションのレプリカ同期ステータスをレポートします。この操作により、パーティションのレプリカを保持する各サーバ上にあるレプリカのツリーオブジェクトから、同期ステータス属性が読み込まれます。レポートには、すべてのサーバに対して正常に同期が行われた最終時刻と、最終同期以降発生したエラーが表示されます。12 時間以内に同期が完了していない場合は、警告メッセージが表示されます。
-N	［このデータベースに認識されているサーバ］オプションです。ローカル eDirectory データベースに認識されているすべてのサーバが表示されます。現在のサーバに Tree パーティションのレプリカがある場合、このサーバには eDirectory ツリー内のすべてのサーバのリストが表示されます。サーバオプションを実行するサーバを 1 つ選択します。
-J	ローカルサーバ上の 1 つのオブジェクトを修復します。修復するオブジェクトのエントリ ID(16 進形式で) を指定する必要があります。破損している 1 つの特定のオブジェクトを修復する場合、標準修復 (-U) オプションの代わりに、このオプションを使用できます。データベースのサイズによっては、［標準修復］オプションの完了に何時間もかかる場合があります。このオプションを使用して、時間を節約することができます。

オプション	説明
-T	［時刻同期］オプションです。ローカル eDirectory データベースに登録されているすべてのサーバにアクセスして、各サーバの時刻同期ステータスの情報を要求します。このサーバに Tree パーティションのレプリカがある場合は、eDirectory ツリー内のすべてのサーバがポーリングされます。各サーバで実行されている eDirectory のバージョンもレポートされます。
-A	既存のログファイルに付加します。情報は既存のログファイルに追加されます。デフォルトでは、このオプションは有効です。
-O	出力をファイルに記録します。デフォルトでは、このオプションは有効です。
-F *filename*	出力を指定したファイルに記録します。
-U	［標準修復］オプションです。ユーザの操作なしに DSRepair を実行または終了します。このオプションはデータベースをロックし、サーバ参照を更新します。修復が完了したらログファイルをチェックして、DSRepair で変更された内容を確認します。

-R オプションで使用するファンクション修飾子

変更者	説明
-l	修復操作中に eDirectory データベースをロックします。
-u	修復操作中に一時 eDirectory データベースを使用します。
-m	修復されていない元のデータベースを維持します。
-i	eDirectory データベース構造とインデックスをチェックします。
-f	データベースの空き領域を増やします。
-d	データベース全体を再構築します。
-t	ツリー構造のチェックを実行します。データベース内での接続状況が正しいかどうかを調べるため、ツリー構造のリンクをすべてチェックするには、「はい」を設定します。チェックを省略するには、「いいえ」を設定します。 デフォルト値は「はい」です。
-o	オペレーショナルスキーマを再構築します。
-r	すべてのローカルレプリカを修復します。
-v	ストリームファイルを確認します。
-c	ローカル参照をチェックします。

グローバルスキーマの操作

ndsrepair -S(［-Ad］*詳細設定スイッチ*) オプションを使用して、実行できるすべてのスキーマ操作のリストを表示できます。次の表では、使用可能なオプションについて説明します。

オプション	説明
マスタサーバからスキーマを要求	このサーバのスキーマを同期するようツリーのルートのマスタレプリカに要求します。スキーマの変更内容は、Tree オブジェクトのマスタレプリカからこのサーバに 24 時間以内に伝えられます。すべてのサーバがマスタレプリカのスキーマを要求すると、ネットワークトラフィックが増加します。
ローカルスキーマをリセット	ローカルスキーマのタイムスタンプをクリアし、インバウンドスキーマの同期を要求するスキーマリセット機能が呼び出されます。Tree パーティションのマスタレプリカから実行する場合、このオプションは使用できません。これは、ツリー内のすべてのサーバが同時にリセットされないようにするためです。
オプションスキーマ拡張機能	包含やその他の拡張機能をスキーマに追加し、変更します。このオプションを使用するには、このサーバが Tree パーティションのレプリカを保持し、レプリカのステータスがオンである必要があります。
リモートスキーマのインポート (詳細設定スイッチオプション)	現在のツリーのスキーマに追加するスキーマを含む eDirectory ツリーを選択します。ツリーを選択すると、Tree パーティションのマスタレプリカを保持するサーバに接続されます。現在のツリー上にあるスキーマを拡張するには、そのサーバのスキーマが使用されます。
新規エポックの宣言 (詳細設定スイッチオプション)	新規スキーマエポックを宣言すると、Tree パーティションのマスタレプリカにアクセスし、そのサーバで宣言されるスキーマの無効なタイムスタンプが修復されます。他のすべてのサーバは、修復されたタイムスタンプを保持する新しいスキーマのコピーを受け取ります。受け取る側のサーバが新規エポック内に存在しなかったスキーマを含む場合は、古いスキーマを使用するオブジェクトおよび属性が「不明」オブジェクトクラスまたは属性に変更されます。

［レプリカ操作とパーティション操作］オプション

サーバに保存された各レプリカの情報を表示するには、次のコマンドを入力します。

```
ndsrepair -P
```

必要なレプリカを選択します。次のオプションが表示されます。

- すべてのレプリカの修復

  レプリカテーブルに表示されたレプリカをすべて修復します。

- 選択したレプリカの修復

  レプリカテーブルに表示されているレプリカのうち、選択したレプリカのみを修復します。

  重要 : レプリカの修復では、レプリカ内の各オブジェクトとスキーマとの整合性のチェック、データと属性構文との整合性のチェックが行われます。レプリカに関連する他の内部データ構造もチェックされます。過去 30 分間にローカル eDirectory データベースを修復していない場合は、レプリカを修復する前にローカル eDirectory データベースを修復する必要があります。

- 即時同期のスケジューリング

すべてのレプリカの同期を直ちに行うようにスケジュールします。この操作は、同期が予定通り実行されるまで待たずに、その同期プロセスの eDirectory 情報を DSTrace 画面で参照したい場合に便利です。

- パーティション操作のキャンセル

  選択したパーティション上でのパーティション操作をキャンセルします。このオプションは、サーバの検出不可や通信リンクの不良など、eDirectory ツリーに問題があるために操作が完了できない場合に必要になります。操作がある程度以上進行していると、キャンセルできない場合があります。

- このサーバを新しいマスタレプリカに設定

  選択したパーティションのローカルレプリカをマスタレプリカとして設定します。元のマスタレプリカが失われた場合、このオプションを使用して新しいマスタレプリカを設定します。

- すべてのサーバの同期ステータスのレポート

  現在のサーバ上にあるすべてのパーティションのレプリカ同期ステータスをレポートします。レポートには、すべてのサーバに対して正常に同期が行われた最終時刻と、最終同期以降発生したエラーが表示されます。

- すべてのサーバ上のレプリカの同期

  選択したパーティションのレプリカを持つすべてのサーバ上で、完全な同期ステータスを特定します。このオプションにより、パーティションの状態を確認できます。該当するパーティションのレプリカを保持するすべてのサーバが正常に同期されていれば、そのパーティションは正常に機能していると判断できます。各サーバは、レプリカリング内の他のすべてのサーバに対して即時同期を実行します。サーバは、そのサーバ自身とは同期されません。したがって、現在のサーバが所有するレプリカのステータスは「ホスト」と表示されます。

- すべてのレプリカのリングの修復

  レプリカテーブルに表示されたすべてのレプリカのレプリカリングを修復します。

- 選択したレプリカのリングの修復

  レプリカテーブルから選択したレプリカのレプリカリングを修復します。

重要 : レプリカリングの修復では、指定したパーティションのレプリカを含む各サーバ上のレプリカリング情報がチェックされ、リモート ID 情報が検証されます。過去 30 分間にローカル eDirectory データベースを修復していない場合は、すべてのリングまたは選択したリングを修復する前に、ローカル eDirectory データベースを修復する必要があります。ローカルデータベースを修復するには、-R オプションを使用します。詳細については、「86 ページの 「-R」」を参照してください。

- レプリカリングの表示

  選択したパーティションのレプリカを含むすべてのサーバのリストを表示します。このサーバのセットをレプリカリングと呼びます。レプリカリングのリストには、レプリカのタイプに関する情報およびリング内にある各サーバの現在のステータスが表示されます。レプリカリングを表示してからサーバを選択すると、サーバオプションが表示されます。

  サーバオプション

  - 選択したサーバの同期ステータスのレポート

    選択したサーバ上にレプリカを保持する選択したパーティションのレプリカ同期ステータスをレポートします。この操作により、パーティションのレプリカを保持する各サーバ上のレプリカルートオブジェクトから、同期ステータス属性が読み込まれます。レポートには、すべてのサーバに対して正常に同期が行われた最終時刻と、最終同期以降発生したエラーが表示されます。12 時間以内に同期が完了していない場合は、警告メッセージが表示されます。

- 選択したサーバのレプリカの同期

  選択したパーティションのレプリカを保持する選択したサーバ上で、完全な同期ステータスを確保します。このオプションにより、パーティションの状態を確認できます。該当するパーティションのレプリカを持つサーバが正常に同期されていれば、そのパーティションが正常に機能していると判断されます。該当するサーバは、直ちにレプリカリング内の他のすべてのサーバに同期されます。サーバは、そのサーバ自身とは同期されません。したがって、現在のサーバが所有するレプリカのステータスは「ホスト」として表示されます。

- リング内のすべてのレプリカにすべてのオブジェクトを送信

  レプリカリング内で選択したサーバから、パーティションのレプリカを含む他のすべてのサーバに、すべてのオブジェクトを送信します。この操作を行うと、大量のネットワークトラフィックが発生する可能性があります。レプリカリング内で選択したサーバ上の選択したパーティションのレプリカが、レプリカリング内の他のすべてのサーバと同期されていることを確かめるには、このオプションを使用します。該当するパーティションのサブオーディネートリファレンスレプリカのみを含むサーバでは、この操作は実行できません。

- マスタからこのレプリカへのすべてのオブジェクトの受信

  選択したサーバ上のレプリカで、マスタレプリカのすべてのオブジェクトを受信します。この操作を行うと、大量のネットワークトラフィックが発生する可能性があります。レプリカリング内で選択したサーバ上の選択したパーティションのレプリカが、マスタレプリカと同期していることを確かめるには、このオプションを使用します。マスタレプリカのみを保持するサーバ上ではこの操作は実行できません。

- サーバのフルネームを表示

  このオプションは、サーバ名が長すぎてサーバテーブル内にすべてを表示できない場合に、完全なサーバ名を表示するために使用します。

- レプリカリングからのサーバの削除

  (詳細設定スイッチオプション) 現在のサーバに保存されているレプリカのうち選択したレプリカから選択したサーバを削除します。レプリカリング内に表示されるサーバがすでに eDirectory ツリーの一部ではない場合や、パーティションのレプリカを保持していない場合は、iManager を使用してこのサーバオブジェクトを削除します。サーバオブジェクトが削除されると、そのオブジェクトは最終的にレプリカリングから除外されます。

  警告 : この操作を誤用すると、eDirectory データベースで致命的な破損が生じることがあります。NetIQ サポート担当者の指示がない限り、このオプションは使用しないでください。

- フルパーティション名の表示

  このオプションは、パーティション名が長すぎてレプリカテーブル内にすべてを表示できない場合に、完全なパーティション識別名を確認するために使用します。

- タイムスタンプの修復と新規エポックの宣言

  (詳細設定スイッチオプション) 選択したパーティションのレプリカをすべて最新版に更新するために、マスタレプリカの新しい参照ポイントを指定します。この操作は、常にパーティションのマスタレプリカ上で実行されます。マスタレプリカは、このサーバのローカルレプリカにある必要はありません。オブジェクトが作成または変更されるとタイムスタンプが設定されます。これらのタイムスタンプは固有である必要があります。マスタレプリカのタイムスタンプはすべて検査されます。タイムスタンプが現在のネットワーク時間より遅れている場合は、新しいタイムスタンプに置き換えられます。

- 選択したレプリカの削除

(詳細設定スイッチオプション) このサーバ上の選択したレプリカを削除します。このオプションの使用はお勧めできません。このオプションは、他のユーティリティを使用してレプリカを削除できない場合にのみ使用してください。

- 不明リーフオブジェクトの削除

  (詳細設定スイッチオプション) 不明オブジェクトクラスを持ち、サブオーディネートオブジェクトのないオブジェクトを、ローカル eDirectory データベースからすべて削除します。このオプションによって、不明なオブジェクトが削除対象としてマークされます。削除は、eDirectory ツリーの他のレプリカと同時に、後で行われます。

警告 : このオプションは、ConsoleOne または iManager を使用してオブジェクトの変更や削除ができない場合にのみ使用してください。

[このデータベースに認識されているサーバ] のオプション

サーバでは次の修復オプションが使用できます。

- すべてのネットワークアドレスの修復

  ローカル eDirectory データベース内で、すべてのサーバのネットワークアドレスをチェックします。このオプションでは、使用可能なトランスポートプロトコルに応じて、各サーバ名の SLP ディレクトリエージェントが検索されます。次に、各アドレスが、サーバオブジェクトのネットワークアドレスプロパティ、およびすべてのパーティション Tree オブジェクトの各レプリカプロパティのアドレスレコードと比較されます。アドレスが異なる場合は、同じになるように更新されます。

- 選択したサーバのネットワークアドレスの修復

  ローカル eDirectory データベースファイル内にある特定のサーバのネットワークアドレスをチェックします。このオプションでは、SLP ディレクトリエージェントが、サーバ名に現在関連付けられているトランスポートプロトコルに応じて検索されます。

- サーバのフルネームを表示

  サーバ名が長すぎてサーバテーブル内にすべてを表示できない場合に、完全なサーバ名を表示するのに使用します。このオプションは、-P オプションと同じです。詳細については、「86 ページの 「-P」」を参照してください。

例

標準修復を実行し、/root/ndsrepair.log ファイルにイベントを記録する場合 (またはログファイルがすでに存在していればそのログファイルに追加してイベントを記録する場合) は、次のコマンドを入力します。

```
ndsrepair -U  -A no -F /root/ndsrepair.log
```

すべてのグローバルスキーマ操作とその詳細設定オプションのリストを表示するには、次のコマンドを入力します。

```
ndsrepair -S -Ad
```

データベースを強制ロックしてローカルデータベースを修復するには、次のコマンドを入力します。

```
ndsrepair -R -l yes
```

注 : ndsrepair コマンドの入力内容は、オプションファイルによってリダイレクトできます。オプションファイルは、レプリカおよびパーティション操作に関連するオプションやサブオプションを含むテキストファイルです。これらはサーバに対する認証を必要としません。各オプションまたはサブオプションは改行によって区切られます。ファイルの内容が、適切な順序で指定されていることを確認します。適切な順序になっていないと、予期しない結果が発生する場合があります。

16.6.2 DSRepair のトラブルシューティング

エラー - 786 DSRepair の実行中

DSRepair を使用する場合、マシン内の DSRepair を実行する特定のパーティションに DIB の 3 倍の空き容量が必要になります。

16.7 DSTrace の使用

Linux 環境で DSTrace ユーティリティを使用するには、サーバプロンプトから次のコマンドを実行します。

```
/opt/novell/eDirectory/bin/ndstrace
```

ndstrace コマンドの完全な構文は次のとおりです。

```
ndstrace [-l|-u|-c "command1;......"|--version] [-h <local_interface:port>] [--
config-file <configuration_file_path>] [thrd <thread ID>] [svty <severity_level>]
[conn <connection_ID>]
```

DSTrace ユーティリティは、次の 3 つの主要部分で構成されています。

- 92 ページの 「基本機能」
- 93 ページの 「デバッギングメッセージ」
- 96 ページの 「バックグラウンド処理」

16.7.1 基本機能

DSTrace の基本機能は次のとおりです。

- eDirectory の内部動作および Linux のデバッグメッセージを表示します。
- 一部の同期処理を開始します。

DSTrace ユーティリティは、UI モードまたはコマンドラインモードのいずれかで使用できます。デフォルトでは、DSTrace は UI モードで実行します。UI モードで DSTrace ユーティリティを開始するには、サーバプロンプトで次のコマンドを実行します。

```
/opt/novell/eDirectory/bin/ndstrace
```

コマンドラインモードで DSTrace ユーティリティを開始するには、サーバプロンプトで次のコマンドを実行します。

```
/opt/novell/eDirectory/bin/ndstrace -l
```

DSTrace の基本機能を開始するには、次の構文を使用してサーバプロンプトでコマンドを入力します。

`ndstrace command_option`

次の表では、入力可能なコマンドオプションのリストを示します。

オプション	説明
オン	基本トレースメッセージを含む eDirectory トレース画面を起動します。
オフ	トレース画面を無効にします。
ALL	eDirectory トレース画面を起動し、すべてのトレースメッセージを表示します。
AGENT	ON、BACKLINK、DSAGENT、JANITOR、RESNAME、および VCLIENT フラグと同等のトレースメッセージを含む eDirectory トレース画面を開始します。
DEBUG	デバッグに通常使用する定義済みのトレースメッセージのセットを有効にします。設定されるフラグは、ON、BACKLINK、ERRORS、EMU、FRAGGER、INIT、INSPECTOR、JANITOR、LIMBER、MISC、PART、RECMAN、REPAIR、SCHEMA、SKULKER、STREAMS、および VCLIENT です。
NODEBUG	トレース画面は使用可能なままで、以前に設定したデバッギングメッセージはすべて無効にします。このオプションでは、メッセージも ON のコマンドオプションが設定された状態のままになります。

16.7.2 デバッギングメッセージ

DSTrace 画面が使用可能な場合、デフォルトのフィルタの設定に基づいて情報が表示されます。デフォルトで表示される情報の内容を変更するには、デバッギングメッセージフラグを使用してフィルタを操作します。デバッギングメッセージにより、eDirectory のステータスを確認し、問題が発生していないかどうかを検証できます。

各 eDirectory 処理には、デバッギングメッセージのセットが含まれています。個々の処理中にそのデバッギングメッセージを表示するには、プラス記号 (+)、および該当する処理名またはオプションを使用します。処理を表示しない場合は、マイナス記号 (-)、および該当する処理名またはオプションを使用します。次に例を示します。

メッセージ	説明
set ndstrace = +SYNC	同期メッセージを表示します。
set ndstrace = -SYNC	同期メッセージを非表示にします。
set ndstrace = +SCHEMA	スキーマメッセージを表示します。

また、ブール演算子の & (AND) および | (OR) を使用して、デバッギングメッセージのフラグを結合することもできます。サーバコンソールでデバッギングメッセージを制御する構文は、次のとおりです。

`set ndstrace = <trace_flag> [parameter]`

次の表では、デバッギングメッセージ用のトレースフラグについて説明します。各トレースフラグは略語で入力できます。

トレースフラグ	説明
ABUF	eDirectory 要求との連携、または eDirectory 要求への応答として受信されたデータを含む、インバウンドおよびアウトバウンドパケットバッファに関するメッセージと情報です。
ALOC	メモリ割り当ての詳細について示すメッセージです。
AREQ	他のサーバまたはクライアントからのインバウンド要求に関するメッセージです。
AUTH	認証に関するメッセージとエラーレポートです。
BASE	最小限のデバッギングレベルでのデバッグエラーメッセージ。
BLNK	バックリンクとインバウンドの破損通知メッセージおよびエラーレポートです。
CBUF	アウトバウンド DS クライアント要求に関するメッセージです。
CHNG	キャッシュ変更メッセージです。
COLL	以前に更新内容を受信したときのオブジェクトの更新情報に関するステータスおよびエラーレポートです。
CONN	ローカルサーバが接続を試みている相手のサーバ、およびローカルサーバが接続できない原因となっている可能性のあるエラーとタイムアウトについての情報を示すメッセージです。
DNS	eDirectory 統合 DNS サーバプロセスに関するメッセージです。
DRLK	分散リファレンスリンクメッセージです。
DVRS	eDirectory が機能している可能性のある DirXML® ドライバ固有のエリアを示すメッセージ。
DXML	DirXML イベントの詳細について示すメッセージです。
FRAG	eDirectory メッセージを NCP サイズのメッセージに分解する、NCP™ Fragger からのメッセージ。
IN	インバウンドの要求およびプロセスに関するメッセージです。
INIT	eDirectory の初期化に関するメッセージです。
INSP	ソースサーバのローカルデータベース内のオブジェクトの整合性に関するメッセージです。このフラグを使用すると、ソースサーバのディスクストレージシステム、メモリ、プロセッサの要求量が増加します。オブジェクトが破損しない限り、このフラグは有効に設定しないでください。
JNTR	janitor、レプリカの同期、フラットクリーナなどのバックグラウンド処理に関するメッセージです。
LDAP	LDAP サーバに関するメッセージです。
LMBR	limber 処理に関するメッセージです。
LOCK	ソースサーバのローカルデータベースロックの使用および操作に関するメッセージです。
LOST	消失エントリに関するメッセージです。
MISC	eDirectory 内の異なるソースからのメッセージです。

トレースフラグ	説明
MOVE	パーティションの移動操作、またはサブツリーの移動操作からのメッセージです。
NCPE	NCP レベルの要求を受信したサーバを示すメッセージです。
NMON	iMonitor に関するメッセージです。
OBIT	破損通知処理からのメッセージです。
PART	バックグラウンド処理および要求処理からのパーティション操作に関するメッセージです。
PURG	パージ処理に関するメッセージです。
RECM	ソースサーバのデータベースの操作に関するメッセージです。
RSLV	名前解決要求の処理に関するメッセージです。
SADV	SLP (Service Location Protocol) のツリー名とパーティションの登録に関するメッセージです。
SCMA	スキーマの同期処理に関するメッセージです。
SCMD	スキーマ関連の操作の詳細について示すメッセージです。インバウンド同期とアウトバウンド同期の両方についての詳細を示します。
SKLK	レプリカの同期処理に関するメッセージです。
SPKT	eDirectory NCP サーバレベルの情報に関するメッセージです。
STRM	ストリーム構文の属性の処理に関するメッセージです。
SYDL	レプリケーション処理時の詳細について示すメッセージです。
SYNC	インバウンド同期トラフィック (サーバ側で受信される内容) についてのメッセージです。
TAGS	トレースオプションを識別するタグ文字列が表示されます。このトレースオプションでは、トレース処理で表示される各行のイベントが生成されます。
THRD	バックグラウンド処理 (スレッド) の開始時と終了時を示すメッセージです。
TIME	同期処理時に使用される遷移ベクトルに関するメッセージです。
TVEC	Synchronize Up To、レプリカ、および遷移ベクトルなどの属性に関するメッセージです。
VCLN	他のサーバへの接続の確立または切断に関するメッセージです。

DSTrace でデバッギングメッセージを使用していると、特に便利なトレースフラグがあることが分かります。NetIQ サポートで多く使用されている DSTrace 設定には、次のようなショートカットがあります。

```
set ndstrace = A81164B91
```

この設定を使用すると、複数のデバッギングメッセージを 1 つのグループとして使用できます。

16.7.3 バックグラウンド処理

eDirectory のステータスを確認できるデバッギングメッセージの他に、eDirectory バックグラウンド処理を強制的に実行するコマンドのセットも用意されています。バックグラウンド処理を強制的に実行するには、コマンドの先頭にアスタリスク (*) を付けます。次に例を示します。

```
set ndstrace = *H
```

また、いくつかのバックグラウンド処理のステータス、タイミング、および制御を変更することもできます。これらの値を変更するには、コマンドの先頭に感嘆符 (!) を付けて新しいパラメータまたは値を入力します。次に例を示します。

```
set ndstrace = !H 15 (parameter_value_in_minutes)
```

eDirectory バックグラウンド処理を制御する各ステートメントの構文を次に示します。

```
set ndstrace = <trace_flag> [parameter]
```

次の表では、バックグラウンド処理のトレースフラグ、必要なパラメータ、およびトレースフラグが表示される処理のリストを示します。

トレースフラグ	パラメータ	説明
*A	なし	ソースサーバのアドレスキャッシュをリセットします。
*AD	なし	ソースサーバのアドレスキャッシュを無効にします。
*AE	なし	ソースサーバのアドレスキャッシュを有効にします。
*B	なし	ソースサーバ上で 1 秒後にバックリンク処理の実行を開始するようにスケジュールします。
!B	時刻	バックリンク処理の実行間隔を分単位で設定します。 デフォルト =1500 分 (25 時間)。範囲 =2 ～ 10080 分 (168 時間)
*CT	なし	ソースサーバのアウトバウンド接続テーブルと、テーブルの現在の統計情報を表示します。これらの統計情報には、他のサーバやクライアントからソースサーバへのインバウンド接続に関する情報は含まれていません。
*CTD	なし	コンマ区切りの形式で、ソースサーバのアウトバウンド接続テーブルと、テーブルの現在の統計情報を表示します。これらの統計情報には、他のサーバやクライアントからソースサーバへのインバウンド接続に関する情報は含まれていません。
*D	レプリカ rootEntry ID	指定したローカルエントリ ID をソースサーバの［すべてのオブジェクトを送信］リストから削除します。エントリ ID では、サーバのローカルデータベースで固有のパーティションルートオブジェクトを指定する必要があります。通常、このコマンドは、サーバのアクセス不能が原因で Send All Updates 処理が何度試みられても失敗する場合にのみ使用します。
!D	時刻	インバウンド同期およびアウトバウンド同期の間隔を分単位で指定された値に設定します。 デフォルト =24 分。範囲 =2 ～ 10080 分 (168 時間)

トレースフラグ	パラメータ	説明
!DI	時刻	インバウンド同期の間隔を分単位で指定された値に設定します。 デフォルト =24 分。範囲 =2 〜 10080 分 (168 時間)
!DO	時刻	アウトバウンド同期の間隔を分単位で指定された値に設定します。 デフォルト =24 分。範囲 =2 〜 10080 分 (168 時間)
*E	なし	ソースサーバのエントリキャッシュを再初期化します。
!E	なし	インバウンド同期およびアウトバウンド同期処理の実行を開始するようにスケジュールします。
!EI	なし	インバウンド同期処理の実行を開始するようにスケジュールします。
!EO	なし	アウトバウンド同期処理の実行を開始するようにスケジュールします。
*F	なし	janitor 処理の一部として、フラットクリーナ処理の実行がソースサーバ上で 5 秒後に開始されるようにスケジュールします。
!F	時刻	フラットクリーナ処理の実行間隔を分単位で設定します。 デフォルト =240 分 (4 時間)。範囲 =2 〜 10080 分 (168 時間)
*FL	1-10	DSTrace が使用するローリングログファイルの数を設定します。このパラメータを 1 より大きい値に設定した場合、ソースサーバの ndstrace.log ファイルが設定されている最大ファイルサイズに達すると、DSTrace はログファイルの名前を ndstrace1.log に変更して、新しい ndstrace.log ファイルを作成します。このファイルが最大ファイルサイズに達すると、先ほどの ndstrace1.log ファイルが ndstrace2.log に名前を変更され、それより新しい ndstrace.log ファイルが ndstrace1.log に名前を変更されます。 この処理は、DSTrace がこのオプションによって設定されたローリングログファイルの最大数に達するまで継続します。指定された制限に達すると、一番古いログファイルが削除されて、指定された最大数のローリングログファイルのみが保持されます。 最大 10 個のローリングログファイルを設定できます。デフォルトでは、DSTrace はローリングログファイルを少なくとも 1 個使用する必要があります。このパラメータを 0 に設定すると、DSTrace はパラメータ値として 1 を使用します。
*G	レプリカ rootEntry ID	指定したルートパーティション ID の変更キャッシュを再構築します。
*H	なし	ソースサーバ上で直ちににレプリカ同期処理の実行を開始するようにスケジュールします。

トレースフラグ	パラメータ	説明
!H	時刻	Heatbeat 同期処理の実行間隔を分単位で設定します。 デフォルト =30 分。範囲 =2 ～ 1440 分 (24 時間)
*HR	なし	メモリ内で最後に送信されたベクトルを消去します。
*I	レプリカ rootEntry ID	指定したローカルエントリ ID をソースサーバの［すべてのオブジェクトを送信］リストに追加します。エントリ ID では、サーバのローカルデータベースで固有のパーティションルートオブジェクトを指定する必要があります。レプリカの同期処理では、［すべてのオブジェクトを送信］リストがチェックされます。パーティションのルートオブジェクトのエントリ ID がリスト内に存在する場合、Synchronized Up To 属性の値に関係なく、eDirectory によってパーティション内のすべてのオブジェクトと属性が同期されます。
!I	時刻	Heatbeat 同期処理の実行間隔を分単位で設定します。 デフォルト =30 分。範囲 =2 ～ 1440 分 (24 時間)
*J	なし	レプリカの同期処理の一部として、ソースサーバ上でパージ処理の実行を開始するようにスケジュールします。
!J	時刻	janitor 処理の実行間隔を分単位で設定します。 デフォルト =2 分。範囲 =1 ～ 10080 分 (168 時間)
*L	なし	ソースサーバ上で 5 秒後に limber 処理の実行を開始するようにスケジュールします。
*M	［Bytes］	ソースサーバの ndstrace.log ファイルで使用する最大ファイルサイズを変更します。このコマンドは、デバッグファイルの状態に関係なく使用できます。bytes の値は 10000 バイトと 100MB の間で 10 進の値を指定する必要があります。この範囲外の値が指定された場合、変更は行われません。
!M	なし	eDirectory で使用されるメモリの最大量をレポートします。
!N	0 | 1	名前の形式を設定します。 0=16 進数のみ。1=full dot 形式
*P	なし	調整可能なパラメータとそのデフォルトの設定を表示します。
*R	なし	ndstrace.log ファイルのサイズをゼロバイトに再設定します。このコマンドは、SET パラメータの NDS Trace File Length Set to Zero と同じ働きをします。
*S	なし	サーバ上のレプリカを同期する必要があるかどうかをチェックするスカルク処理をスケジュールします。
!SI	時刻	インバウンドスキーマ同期処理の実行間隔を分単位で設定します。 デフォルト =24 分。範囲 =2 ～ 10080 分 (168 時間)

トレースフラグ	パラメータ	説明
!SO	時刻	アウトバウンドスキーマ同期処理の実行間隔を分単位で設定します。 デフォルト =24 分。範囲 =2 ～ 10080 分 (168 時間)
!SIO	時刻	時間を分単位で指定し、その間のインバウンドスキーマ同期処理を無効にします。 デフォルト =24 分。範囲 =2 ～ 10080 分 (168 時間)
!SO0	時刻	時間を分単位で指定し、その間のインバウンドスキーマ同期処理を無効にします。 デフォルト =24 分。範囲 =2 ～ 10080 分 (168 時間)
*SS	なし	強制的に即時スキーマの同期を実行します。
*SSA	なし	スキーマの同期処理の実行を即時に開始するようにスケジュールします。過去 24 時間以内に同期が行われていた場合でも、すべてのターゲットサーバでスキーマの同期が強制的に実行されます。
*SSD	なし	ソースサーバの［ターゲットスキーマ同期］リストをリセットします。このリストでは、スキーマの同期処理の実行中にソースサーバと同期する必要のあるサーバが識別されます。レプリカを保持していないサーバは、サーバオブジェクトとレプリカを保持しているサーバのターゲットリストに包含されるように要求を送信します。
*［SSL］	なし	ターゲットサーバのスキーマ同期リストを印刷します。
*ST	なし	ソースサーバ上のバックグラウンド処理のステータス情報を表示します。
*STX	なし	ソースサーバ上のバックリンク処理 (外部参照) のステータス情報を表示します。
*STS	なし	ソースサーバ上のスキーマ同期処理のステータス情報を表示します。
*STO	なし	ソースサーバ上のバックリンク処理 (破損通知) のステータス情報を表示します。
*STL	なし	ソースサーバ上の limber 処理のステータス情報を表示します。
!T	時刻	サーバの稼動状態のチェックの実行間隔を分単位で設定します。 デフォルト =30 分。範囲 =1 ～ 720 分 (12 時間)
*U	サーバのオプションの ID	コマンドにエントリ ID が含まれていない場合は、以前に「**down**」から「**up**」にラベルが付加された任意のサーバのステータスを変更します。コマンドにローカルエントリ ID が含まれている場合は、指定されたサーバのステータスを「**down**」から「**up**」に変更します。エントリ ID は、ソースサーバのデータベースで固有であり、サーバを表すオブジェクトを参照する必要があります。

トレースフラグ	パラメータ	説明
!V	リスト	制限のある eDirectory バージョンのリストを表示します。バージョンが表示されない場合は、制限がないことを示します。各バージョンはコンマで区切られます。
*Z	なし	現在、スケジュールされているタスクを表示します。

17 Linux での NMAS

17.1 どのメソッドを使用してもログインできない

NMAS をインストールおよび設定した後で、eDirectory サーバを再起動します。

メソッドの以前のインスタンスをアンインストールしてからメソッドを再インストールした後で、eDirectory サーバを再起動します。

17.2 ICE ユーティリティを使用して追加したユーザが、簡易パスワードを使用してログインできない

NetIQ インポート / エクスポート変換ユーティリティを使用して簡易パスワードを使用するユーザを追加する場合は、-l オプションを使用します。

18 Windows のトラブルシューティング

18.1 eDirectory for Windows サーバが起動しない場合

Windows サーバのブート時に eDirectory サーバが起動に失敗すると、サービスの開始に失敗したことを示すメッセージが通知されます。

他に eDirectory データベースのレプリカがない場合、ユーザはログインできません。

他にレプリカがある場合は、ログインが遅くなります。また、これらのレプリカを保持しているサーバ上に通信エラーおよび同期エラーが表示されます。

- Windows レジストリ内の eDirectory サーバエントリが編集されたか、Windows レジストリが破損している可能性があります。
- eDirectory データベースファイルが破損しているか、削除された可能性があります。
- 他のサービスが開始されていないために eDirectory サーバが起動できない場合、［*スタート*］>［*プログラム*］>［*管理ツール*］>［*イベントビューア*］の順にクリックして詳細を参照できます。

  eDirectory サーバを起動する前に、他の必要なサービスにおける問題を解決する必要があります。
- レジストリまたは eDirectory 実行可能ファイルが、破損しているか失われています。システムディレクトリにある SAMMIG ユーティリティを実行します。［*Windows NT 上の NDS のアンインストール*］を選択し、NT ドメインに新しい eDirectory 情報を追加します。操作を続行してアンインストールプロセスを完了します。次に、sammig.exe を再起動し、eDirectory のインストールへ進みます。

- データベースファイルが、破損しているか削除されています。NT サーバ上で eDirectory サーバが起動しているのに、サービスが eDirectory データベースファイルを開くことができない場合は、「104 ページのセクション 18.2「Windows サーバが eDirectory データベースファイルを開けない場合」」を参照してください。
- eDirectory サーバがハブまたはスイッチに接続されていないか、クロスケーブルを使用してワークステーションに直接接続されていません。サーバをハブまたはスイッチに接続してください。

18.2 Windows サーバが eDirectory データベースファイルを開けない場合

eDirectory サーバがデータベースファイルを開けない場合、Windows サーバ上で、これを示すメッセージが通知されます。

他にデータベースのレプリカがない場合、ユーザはログインできません。

他にレプリカがある場合は、ログインが遅くなります。また、これらのレプリカを保持しているサーバ上に通信エラーおよび同期エラーが表示されます。

- NT/2000 サーバ上のディスクエラーのため、データベースファイルが破損している可能性があります。
- 他のユーザにより、1 つまたは複数のデータベースファイルが削除された可能性があります。

他に eDirectory データベースのレプリカがある場合は、次の手順を実行します。

1. 管理ワークステーションから NetIQ iManager を起動します。
2. 破損したレプリカをレプリカリングから削除します。

   詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「レプリカの削除」を参照してください。
3. NT サーバ上のシステムディレクトリ (通常、C:\WINNT\SYSTEM32) にある SAMMING.EXE ユーティリティを実行するか、［*スタート*］メニューから実行します。
4. eDirectory サーバ上に新しいレプリカを作成するオプションを選択します。

この eDirectory サーバだけにパーティションのレプリカがある場合は、次の手順を実行します。

1. NT サーバ上のシステムディレクトリ (通常、C:\WINNT\SYSTEM32) にある SAMMING.EXE ユーティリティを実行するか、［*スタート*］メニューから実行します。
2. Windows で［*NDS のアンインストール*］を選択して、移行前の Windows ドメインの状態に戻します。
3. 操作を続行してアンインストールプロセスを完了します。
4. Migration Tool を再起動し、Windows に eDirectory をインストールします。
5. ユーザオブジェクトを NT/2000 ドメインから eDirectory ツリーへ移動します。

18.3 Windows マシンで SLP_NETWORK_ERROR(-23) が発生する

サービスロケーションプロトコル (SLP) クエリは、DHCP アドレスを持つ仮想マシン、または SLP がブロードキャストされない物理マシンもしくは仮想マシンで -23 SLP_NETWORK_ERROR を返します。

次のいずれかの方法で、ネットワークにディレクトリエージェントを設定することにより、この SLP エラーを回避することができます。

1. C:\Windows\System32\Novell\eDir\OpenSLP\slp.conf ファイルを c:\Windows\ ディレクトリにコピーします。
2. テキストエディタで slp.conf ファイルを開いて、次の行を変更します。

   ```
   ;net.slp.DAAddresses = myDay1,myDa2,myDa3
   ```

   変更後 :

   ```
   net.slp.DAAddresses = <Give your DA Address>
   ```

3. 変更内容を保存し、ファイルを閉じます。

または

1. C:\Windows\System32\Novell\eDir\OpenSLP\slp.conf ファイルを c:\Windows\ ディレクトリにコピーします。
2. テキストエディタで slp.conf ファイルを開いて、次の行を変更します。

   ```
   ;net.slp.isDA = true
   ```

   変更後 :

   ```
   net.slp.isDA = true
   ```

3. 変更内容を保存し、ファイルを閉じます。

18.4 eDirectory インストール中に、正しくないインストールパスが参照ページに表示される

パスを希望する場所に手動で変更します。

18.5 SLP が Windows で正しく設定されていない場合、サーバの追加が失敗する

SPLD がすでにインストールされていて実行中であると、サーバをツリーに追加するときに (現在のツリーを参照する必要があります)、eDirectory のインストールが失敗します。Windows は［*launch.exe died*］というメッセージを表示します。

eDirectory を正常にインストールするには、システムをリブートせずに次の手順を実行します。

1. サービスロケーションプロトコルサービスを停止します。
2. C:\Windows\slp.conf ファイルを削除します。

3 C:\Windows\System32\Novell\eDir\OpenSLP フォルダを削除します。

4 Registry HKLM\SYSTEM\CurrentControlSet\Services\slpd から SLPD サーバのレジストリキーを削除します。

5 管理者の役割で再度セットアップを実行します。

19 DSがロードされない場合のHTTPSTKへのアクセス

DS がロードされない場合に HTTPSTK(HTTP プロトコルスタック) にアクセスできる管理者ユーザを事前に設定できます。事前に設定された管理者ユーザ (sadmin) には、eDirectory 管理者ユーザオブジェクトと同等の権利があります。サーバが、eDirectory が適切に機能していない状態の場合、このユーザとしてサーバにログインし、eDirectory を使用せずに実行できる必要なすべての診断およびデバッギング作業を実行します。

- 107 ページのセクション 19.1「Windows で sadmin パスワードを設定する」
- 107 ページのセクション 19.2「Linux で sadmin パスワードを設定する」

19.1 Windows で sadmin パスワードを設定する

DHOST リモートマネージャページ (/dhost URL またはルートページからアクセス可能) を使用して、sadmin パスワードを設定します。sadmin パスワードの設定や変更を行うには、eDirectory サーバで dhost.exe を実行している必要があります。

1. Web ブラウザを開きます。
2. アドレス (URL) フィールドに、次の形式で入力します。

   http://*server.name*:*port*/dhost

   たとえば、次のように入力します。

   `http://MyServer:80/dhost`

   DHost iConsole へのアクセスに、サーバの IP アドレスを使用することもできます。次に例を示します。

   `http://137.65.135.150:80/dhost`
3. ユーザ名、コンテキスト、パスワードを指定します。
4. ［*HTTP サーバ*］をクリックしてから、sadmin パスワードを指定します。
5. 指定したパスワードを確認入力して、［*送信*］をクリックします。

19.2 Linux で sadmin パスワードを設定する

sadmin のパスワードの設定には、DHost リモート管理ページまたは ndsconfig ユーティリティを使用できます。

DHost リモート管理ページ

DHost リモートマネージャページ (/dhost URL またはルートページからアクセス可能) を使用して、sadmin パスワードを設定します。sadmin パスワードの設定や変更を行うには、eDirectory サーバで NetIQ eDirectory サーバを実行している必要があります。

1. Web ブラウザを開きます。
2. アドレス (URL) フィールドに、次の形式で入力します。

   http://*server.name*:*port*/dhost

   たとえば、次のように入力します。

   `http://MyServer:80/dhost`

   DHost iConsole へのアクセスに、サーバの IP アドレスを使用することもできます。次に例を示します。

   `http://137.65.135.150:80/dhost`
3. ユーザ名、コンテキスト、パスワードを指定します。
4. ［*HTTP サーバ*］をクリックしてから、sadmin パスワードを指定します。
5. 指定したパスワードを確認入力して、［*送信*］をクリックします。

ndsconfig

ndsconfig ユーティリティを使用して、sadmin パスワードを設定します。sadmin パスワードの設定や変更を行うには、eDirectory サーバで ndsd を実行している必要があります。

サーバコンソールから、次のように入力します。

ndsconfig set http.server.sadmin-pwd=*password*

ここで *password* は、新しい sadmin パスワードです。

ndsconfig ユーティリティの使用に関する詳細については、『*NetIQ eDirectory 8.8 SP8 インストールガイド*』の「sconfig ユーティリティのパラメータ」を参照してください。

20 eDirectory のデータを暗号化する

NetIQ eDirectory 8.8 以降では、特定の重要データをディスクに保存したり、クライアントによってアクセスされたりしている間に、データを暗号化できます。この章では、eDirectory8.8 以降で、暗号化属性やレプリケーション機能を使用しているときに起こるエラーについて情報を提供します。暗号化属性およびレプリケーションの詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド* (http://www.netiq.com/documentation/edir88/edir88/data/a2iii88.html)』を参照してください。

eDirectory の他のエラーメッセージの詳細については、NetIQ エラーコード Web サイト (http://www.novell.com/documentation/nwec/) を参照してください。

20.1 エラーメッセージ

このセクションでは、次のエラーメッセージについて説明します。

- 109 ページのセクション 20.1.1「-6090 0xFFFFE836 ERR_ER_DISABLED」
- 109 ページのセクション 20.1.2「-6089 0xFFFFE837 ERR_REQUIRE_SECURE_ACCESS」
- 110 ページのセクション 20.1.3「-666 FFFFFD66 INCOMPATIBLE NDS VERSION」

20.1.1 -6090 0xFFFFE836 ERR_ER_DISABLED

eDirectory レプリカ同期処理が、ターゲットサーバに対し暗号化されたレプリケーションを開始しようとしました。しかし、ターゲット eDirectory サーバは暗号化されたレプリカ同期処理を無効にしました。

考えられる原因

暗号化されたレプリケーションがターゲット eDirectory サーバで無効になっています。

アクション

ターゲット eDirectory サーバで暗号化されたレプリケーションを有効にします。

20.1.2 -6089 0xFFFFE837 ERR_REQUIRE_SECURE_ACCESS

アプリケーション (クライアントアクセス) が、クリアテキストチャネルから暗号化属性にアクセスしようとしました。

ソース

eDirectory または NDS

考えられる原因

暗号化属性が、セキュリティ保護されたチャネルからのみアクセスできるように設定されています。アプリケーションが、クリアテキストチャネルから暗号化属性にアクセスしようとしています。

アクション

アプリケーションは、LDAP セキュアチャネルまたは HTTP セキュアチャネルなどのような、セキュリティ保護されているチャネルから暗号化属性にアクセスする必要があります。

考えられる原因

このエラーをレプリカの作成中に受け取った場合は、レプリカリングの 1 つ以上のサーバが暗号化用にマークされたいくつかの属性を持ち、セキュアチャネルからのみアクセスできるように設定されています。

アクション

セキュリティ保護されていないチャネルから暗号化属性にアクセスできるように、暗号化属性ポリシーの設定を変更します。詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド* (http://www.netiq.com/documentation/edir88/edir88/data/a2iii88.html)』を参照してください。

考えられる原因

暗号化されたレプリケーションがパーティションレベルまたはパーティションのレプリカ間で設定されているときにこのエラーを受け取った場合は、レプリカリングは eDirectory 8.8 以前のサーバを使用しています。

アクション

レプリカリング内のすべてのサーバを eDirectory 8.8 に対応するバージョンにアップグレードします。

20.1.3 -666 FFFFFD66 INCOMPATIBLE NDS VERSION

本文がここに入ります。

考えられる原因

暗号化されたレプリケーションがパーティションレベルで有効になっている場合、またこのパーティションのレプリカを eDirectory サーバに追加しようとしている場合は、このサーバの eDirectory バージョンがソースサーバのバージョンに対応していません。

アクション

サーバを eDirectory に対応したバージョンにアップグレードします。

考えられる原因

ペアレントパーティションが eDirectory8.8 以前のサーバ (混合バージョンのリング) を使用しており、チャイルドパーティションに有効な ER がある場合は、マージおよび / またはパーティションの結合操作は不許可になり、ERR_INCOMPATIBLE_DS_VERSION エラーが返されます。

この理由は、チャイルドパーティションにパーティションレベルで ER が有効な重要なデータが含まれており、ペアレントパーティションに eDirectory8.8 以前のサーバがあるからです。マージ中に、eDirectory8.8 サーバ間でのみ ER が有効になっていると、重要なデータは eDirectory8.8 以前のサーバに複製しているとき危険にさらされます。

アクション

1. サーバを eDirectory に対応したバージョンにアップグレードします。

   または

2. ペアレントまたはチャイルドパーティションで ER を無効にします。

   注 : ER を無効にしている間、レプリケーションはクリアテキストフォームで行われます。

20.2 重複暗号化アルゴリズムの問題

LDIF を使用して暗号化用の属性を追加する場合は、重複したアルゴリズムを一つの属性に関連付けないでください。

例えば、「タイトル」を AES および DES 暗号化アルゴリズムで暗号化された属性としてマークすると、どちらのアルゴリズムが最終的に考慮されるのか不明瞭になります。LIMBER が実行されるときに毎回、タイトル属性トグルが AES と DES の間に表示されます。そのため、設定変更があったように見えてしまいます。

そのようなことを避けるため、同じ属性に重複してアルゴリズムを割り当てるのを避けることをお勧めします。

これは、iManager を使用して暗号化用の属性をマークした場合は起こりません。

20.3 ストリーム属性の暗号化

ストリーム属性がクリアテキストデータとして存在する可能性があります。この原因は、eDirectory 8.8 ではストリーム属性を暗号化しないことによります。

20.4 iManager を使用した暗号化複製の設定

レプリカリング内のいずれかのサーバが停止している場合は、iManager を使用して暗号化複製を設定することはできません。

20.5 iManager を使用した暗号化属性の表示または変更

オブジェクトの属性が暗号化されている場合、iManager 2.5 では、オブジェクトを表示することも変更することもできません。

この問題を回避するために、セキュアチャネルを通じて暗号化属性の表示や変更を行うことができます。これには、次の 2 つの方法があります。

- LDAP: LDAP 要求は、セキュアチャネルを通じて送信する必要があります。そのため、サーバのルート認証局証明書を使用する必要があります。
- ICE: LDIF スクリプトを使用してオブジェクトを変更することができます。この場合、ICE はセキュアチャネルを使用する必要があります。
- iManager 2.5 FP2、iManager 2.6 以降を使用します。

注 : 暗号化属性の表示または変更を行う場合は、iManager 2.6 以降を使用することをお勧めします。

または、暗号化属性を表示または変更できるように、EA ポリシーの requireSecure 属性を無効にすることにより、［セキュアチャンネルが必要です］オプションを無効にできます。この操作により、クリアテキストチャネルから、いずれのクライアントもオブジェクトと暗号化属性にアクセスできるようになります。これで、iManager がオブジェクトにアクセスできるようになります。

20.6 暗号化複製が有効になっているツリーのマージに失敗する

暗号化複製が有効になっている場合、ツリーのマージに失敗します。マージを行う前に、各ツリーでセキュリティ保護された複製を無効にします。

20.7 Limber で -603 エラーが表示される

暗号化属性ポリシーパーティションのサブリファレンスレプリカのみがサーバにある場合、Limber では、-603 エラーが表示されます。

この問題を回避するには、次のいずれかの手順を実行します。

- NCP サーバオブジェクトへの読み込みアクセスを許可します。この手順は、iManager を使用して、ツリールートにトラスティを追加し、NCP サーバオブジェクトへの読み込みアクセスを許可することで実行できます。属性に attrEncryptionDefinition および attrEncryptionRequiresSecure を指定します。
- LDAP または ndssch を通じて、次の属性へのパブリック読み込みアクセスを許可します。
  - attrEncryptionDefinition
  - attrEncryptionRequiresSecure

21 eDirectory Management Toolbox

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。

eMBox を NetIQ iManager とあわせて使用すると、DSRepair、DSMerge、バックアップと復元、サービスマネージャなどの eDirectory ユーティリティに Web ベースでアクセスできます。

重要 : eMBox タスクを実行するには、iManager を使用して、管理するツリーに役割ベースサービスを設定する必要があります。

すべての機能は、ローカルサーバまたはリモートのいずれからでもコマンドラインクライアントを通じて使用できます。eMBox クライアントを使用して、1 つのサーバまたはワークステーションから複数のサーバに対するタスクを実行できます。バックアップ、DSRepair、DSMerge、スキーマの操作、および eDirectory Service Manager などのすべての eMTool(eDirectory Management Tool) を実行するには、eDirectory サーバに eMBox がロードされ、実行されている必要があります。

21.1 eMTool サービスを停止できない

コマンド serviceStop -n*{service}* を実行しているときに、*{service}* がサービス (libsasl.so、libncpengine.so、libhttpstk.so、または libdsloader.so) の 1 つである場合は、次のエラーが起こります。

```
Service {service} could not be stopped, Error : -660
```

これはエラーではありません。この進行 (具体的には libsasl.so、libncpengine.so、libhttpstk.so、および libdsloader.so) は、他のモジュールがこれらに依存しているため、止めることはできません。

21.2 復元を実行すると -6020 エラーになる

デフォルトの場所にロールフォワードログがある場合、DSBK または eMBox クライアントを使用して復元操作を実行すると -6020 エラーになります。このエラーを回避するには、restore コマンドに -s スイッチを指定する必要があります。

21.3 eDirectory Service Manager に関する問題

iManager で eDirectory Service Manager を使用して eDirectory を停止すると、Service Manager を通じて eDirectory を再起動することはできません。eDirectory サーバで eDirectory サービスユーティリティ (C:\novell\NDS\NDSCons.exe) を使用して、eDirectory を再起動します。

21.3.1 移動したオブジェクトの削除

2 台以上のサーバが含まれるツリーでは、移動したオブジェクトの削除に失敗する場合があります (エラー : 637)。

21.3.2 ダイナミックグループの移動に関する問題

dynamicgroup という Object Class 属性を持つダイナミックグループオブジェクトを他のコンテナに移動すると、ダイナミックグループが機能しなくなります。移動後、ダイナミックメンバーにクエリおよび検索を実行しても機能しません。

21.3.3 eMBox からネットワークアドレスを修復する際の問題

eMBox からネットワークアドレスを修復しているとき、eMBox が修復用の最新フィックスで更新されていないと、次のエラーが発生します。

エラー : このサーバのネットアドレスが見つかりませんでした。エラー : 11004

エラー : 接続できませんでした。エラー : 11004

21.3.4 フランス語のマニュアルページの参照

Red Hat Linux でフランス語のマニュアルページを参照するには、次のようにエクスポートします。

```
export MANPATH=/opt/novell/man/frutf8:/opt/novell/eDirectory/man/frutf8
```

21.3.5 移動したオブジェクトの削除

2 台以上のサーバが含まれるツリーでは、移動したオブジェクトの削除に失敗する場合があります (エラー : 637)。

21.3.6 eDirectory クライアントの制限により eDirectory でログアウトイベントが生成されない

eDirectory では、iManager からログアウトしたときに、ログアウトイベントが生成されません。これは、eDirectory のクライアントに存在する技術上の制限によるものです。

アプリケーションの監査では、NWDS API を使用してログアウトイベントを受信できます。LDAP を使用するアプリケーションでは、バインド解除イベントでログアウトを監視できます。

21.3.7 DSTrace 実行中に TERM によって生じる問題

TIME および TAGS のタグが有効であるように表示されますが (下線表示)、デフォルトでは有効ではありません。TERM を Linux ターミナルから VT100 または xterm に設定すると、これらのタグが有効であるように表示されます (下線表示)。この問題は、dtterm などの他のターミナルでは発生しません。

21.3.8 eMBox で 2 バイト文字が処理されない

eMBox では、eMBox クライアントおよび iManager を使用してロールフォワードディレクトリを設定するときに 2 バイト文字が処理されません。処理するには、DSBK を使用します。

22 SASL-GSSAPI

このセクションでは、SASL-GSSAPI 認証メカニズムによって記録されたエラーメッセージを説明します。

22.1 SASL GSSAPI に関する問題

22.1.1 複数のユーザオブジェクトによる問題

同一の Kerberos プリンシパルが複数の eDirectory ユーザオブジェクトに関連付けられている場合、SASL GSSAPI との LDAP バインドは失敗します。

22.1.2 認証 ID

RFC2222 では、ユーザおよびクライアントによって送信される認証 ID のサポートについて規定されています。これは、SASL GSSAPI メソッドではサポートされていません。

22.2 ログファイル

Linux インストールでは、エラーメッセージは ndsd.log ファイルに記録されます。

22.3 エラーメッセージ

SASL-GSSAPI: Reading Object *user_FDN* FAILED *eDirectory error code*

原因： このエラーは、eDirectory 内で生成されます。user_FDN オブジェクトは存在しません。

SASL-GSSAPI: Reading principal names for *user_FDN* failed *eDirectory error code*

原因： このエラーは、eDirectory 内で生成されます。ケルベロスのプリンシパル名がユーザオブジェクト (userdn) にアタッチされていません。

SASL-GSSAPI: Reading Object *Realm_FDN* FAILED *eDirectory error code*

原因： このエラーは、eDirectory 内で生成されます。レルムオブジェクトは存在しません。

SASL-GSSAPI: Not enough memory

原因： 特定の操作を行うためのメモリが不足しています。

SASL-GSSAPI: Invalid Input Token

原因： クライアントからのトークンが不良、または無効です。

SASL-GSSAPI: NMAS error *NMAS error code*

原因： このエラーは、NMAS で生成される初期エラーです。

SASL-GSS: Invalid LDAP service principal name *LDAP_service_principal_name*

原因： LDAP サービスのプリンシパル名が無効になっています。

SASL-GSS: eDirectory からの LDAP サービスプリンシパルキーの読み込みに失敗しました

原因： LDAP サービスのプリンシパルオブジェクトが作成されていません。

原因： レルムオブジェクトのマスタキーが変更されています。

原因： LDAP サービスのプリンシパルオブジェクトが、属するレルムのサブツリーで見つかりませんでした。

SASL-GSS: GSS コンテキストの作成に失敗しました

原因： クライアント、KDC、および eDirectory サーバで、時間が同期していません。

原因： LDAP サービスプリンシパルのキーは、ケルベロスデータベースで変更されましたが、eDirectory で更新されていません。

原因： 暗号化タイプがサポートされていません。

SASL GSSAPI: Invalid user FDN = *user_FDN*

原因： クライアントに提供されたユーザ FDN が有効ではありません。

SASL GSSAPI: No user DN is associated with principal *client_principal_name*

原因 : サブツリーの下のユーザオブジェクトが、ケルベロスプリンシパル名にアタッチされていません。

SASL GSSAPI: 複数のユーザ DN がプリンシパル *client_principal_name* に関連付けられています

原因 : サブツリー下の複数のユーザオブジェクトが、同じプリンシパルに関連付けられています。

ldap_simple_bind_s: Invalid credentials major = 1, minor =0

原因 : 原因は、KDC サーバの LDAP サービスプリンシパルと eDirectory サーバの LDAP サービスプリンシパルの間で、バージョンが一致していないことが考えられます。これは、keytab ファイルに LDAP サービスプリンシパルキーを取り出すたびに、キーのバージョンナンバーが増加するためです。

アクション :

次の手順を実行します。

1. バージョン番号が同期するように、eDirectory サーバでキーを更新します。
2. クライアントでチケットを破棄します。
3. プリンシパル用に TGT を再度取得します。
4. LDAP sasl バインド操作を実行します。

23 その他

- 128 ページのセクション 23.26「LDAP 経由の SecretStore」
- 128 ページのセクション 23.27「相互運用性の問題」

23.1 コンテナのバックアップ

ndsbackup を使用しながらオブジェクトを多数 (100 万個程度) 持つコンテナをバックアップするには、コンテナ内のオブジェクトのリストを取得し、個々のバックアップを開始するために、かなりの時間がかかる可能性があります。

23.2 eDirectory への繰り返しログイン

eDirectory に繰り返しログインする場合、すべての使用可能なメモリを使用できます。iMonitor を使用してログイン更新属性を無効にすると、この問題を解決できます。

23.3 イベントシステム統計を有効にする

eDirectory でイベントが発生して消費されるたびに、そのイベントの時刻に関連する統計が保持されます。この情報は、イベントコンシューマの問題を解決するのに役立ちます。この統計はディレクトリの通常の機能に必要ではないため、パフォーマンス上の理由で無効にされています。iMonitor 詳細設定パラメータを使用することで、イベント統計を実行時に有効にすることができます。

イベント統計を表示するには、ENABLE_EVENT_STATISTICS パラメータを設定して、サーバを再起動します。このパラメータは永続的な設定パラメータです。

23.4 Linux でのメモリ破損問題のトラッキング

Linux プラットフォームで、eDirectory はデフォルトのメモリアロケータとして Google malloc (libtcmalloc) を使用します。

メモリ破損の問題をトラッキングするには、ndsd 起動スクリプトに MALLOC_CHECK_ 環境変数を設定します。起動スクリプトはこの変数が設定されているか確認します。設定されている場合は、デフォルトシステムの malloc が使用され、設定されていない場合は、libtcmalloc がロードされます。

ndsd での MALLOC_CHECK_ の設定

- MALLOC_CHECK_ が 0 に設定されている場合、検出されたヒープ破損は無視されて通知されません。
- MALLOC_CHECK_ が 2 に設定されている場合、直ちに中止が呼び出されます。

  このおかげで、メモリ破損の本当の原因を早い段階で特定することができます。さもなければ、原因を後で追求することは難しくなります。

23.5 異常ログアウト後に TCP 接続が終了しない

ワークステーションのクラッシュまたは停電のために突然に停止したクライアントホストを、OES Linux サーバが検出できないことがあります。しかし、接続はアクティブのままで、デフォルトのタイムアウト時間 (12 ～ 15 分間ほど) が経過してから切断されます。同時接続数を 1 に設定している場合は、接続を手動で終了するか、またはタイムアウトまでの時間を予測して待ってから再びログインすることをお勧めします。この状況は、ウォッチドッグプロセスが接続を正常に閉じることができなかったときに発生します。そのため、同時接続数が 1 に設定されていて、接続がウォッチドッグによって正常に閉じられていないと、ユーザはログインすることができません。Linux カーネルには、keepalive プローブのサーバ側動作を変更するための 3 つのパラメータが提供されています。TCP レベルで対処方法を実行するには、これらのパラメータを使用します。

これらのパラメータは /proc/sys/net/ipv4/ ディレクトリにあります。

- tcp_keepalive_time: 接続が使用されていない場合に、接続を生かしておくために TCP keepalive パケットを送信する頻度を指定します。この値は keepalive が有効である場合にのみ使用します。

  tcp_keepalive_time には、秒数を整数で指定します。デフォルト値は 7200 秒すなわち 2 時間です。この値はたいていのホストに適しており、多くのネットワークリソースを必要としません。この値を低く設定すると、不要なトラフィックのためにネットワークリソースを使用することになります。

- tcp_keepalive_probes: 接続が切断されたと判断するまでに TCP keepalive プローブを送信する頻度を指定します。

  tcp_keepalive_probes には整数値を指定します。推奨値は 50 未満で、tcp_keepalive_time 値と tcp_keepalive_interval 値によって決まります。デフォルトは、9 プローブ送信後に接続が切断されているとアプリケーションに通知するよう設定されています。

- tcp_keepalive_intvl: 各 keepalive プローブの応答の持続期間を指定します。この値は、接続の keepalive が停止するまでの時間を計算するために重要です。

  tcp_keepalive_intvl には整数値を指定します。デフォルトは 75 秒です。1 プローブが 75 秒だとすると、9 プローブは約 11 分となります。tcp_keepalive_probes 変数および tcp_keepalive_intvl 変数のデフォルト値を使用して、keepalive によって接続が時間切れになるまでのデフォルト時間を評価できます。

余分なネットワークトラフィックが大量に発生せずかつ問題は解決されるように、これら 3 つのパラメータを変更します。一例として、次のように変更できます (検出時間は 3 分)。

- tcp_keepalive_time set -120
- tcp_keepalive_probes - 3
- tcp_keepalive_intvl - 20

注 : パラメータ設定値に注意し、すでに有効である接続の設定をしないようにします。

設定はファイルが変更された直後に有効になります。どのサービスも再起動する必要はありません。ただし、設定は現行のセッションにのみ有効です。サーバを再起動すると、設定はデフォルト設定に戻ります。

設定を (再起動後も) 永続的なものにするには、以下の手順を行います。

次のエントリを /etc/sysctl.conf に追加します。

- net.ipv4.tcp_keepalive_time=120

- net.ipv4.tcp_keepalive_probes=3
- net.ipv4.tcp_keepalive_intvl=20

すべてのクライアントおよびサーバは LAN 経由で接続されている場合にのみ、上記の設定を推奨します。

23.6 ユーザオブジェクトに対して ldapsearch を実行中に、システムエラー (-632) の NDS エラーが発生する

簡易パスワードを使用してユーザオブジェクトをインポートし、ユーザオブジェクトがインポートされたコンテナのユニバーサルパスワードを有効にします。DS サーバを停止して NDSD_TRY_NMASLOGIN_FIRST=true を環境に設定してから、DS サーバを起動します。簡易パスワードを使用してインポートされたユーザオブジェクトに対して ldapsearch を実行すると、次のようなエラーが発生します。

```
ldap_bind: Unknown error,  additional info: NDS error: system failure (-632)
```

この問題を解決するには、ユーザオブジェクトに対して ldapsearch を実行する前に、デフォルトのログインシーケンスを、ユーザオブジェクトがインポートされたコンテナの簡易パスワードとして設定してください。

LDAP が NMAS にユーザのログインを要求する際、NMAS はデフォルトのログインシーケンスを使用します。これらのユーザに対してデフォルトのログインシーケンスを指定しない場合、NMAS は NDS シーケンスを使用します。ユーザをインポートした際にこれらのユーザに NDS パスワードが割り当てられていない場合は、NDS シーケンスは動作しません。ユニバーサルパスワードを有効にすると、ユーザが簡易パスワードを使用してログインする際に、簡易パスワードは NDS パスワードおよびユニバーサルパスワードと同期されます。

23.7 SecretStore の無効化

eDirectory 管理者は、次の処理を使用して SecretStore を無効化することができます。

23.7.1 Linux の場合

1. nds-modules ディレクトリに移動して、次の SecretStore モジュールの名前を変更して移動します。

   libsss.so

   libssncp.so

   libssldp.so

2. サーバを再起動します。

または、/etc/opt/novell/eDirectory/conf/ndsmodules.conf ファイルの ssncp をロードする行をコメントアウトすることもできます。

23.7.2 Windows の場合

1. novell\nds ディレクトリに移動して、次の SecretStore モジュールの名前を変更するか移動します。

lsss.dll

sss.dlm

ssncp.dlm

ssldp.dlm

2 サーバを再起動します。

23.8 SLP マニュアルページの参照

SLP のマニュアルページを参照するには、マニュアルページのパスを設定する必要があります。たとえば、AIX の場合、/opt/novell/man ではなく /usr/share/man にマニュアルページのパスを設定する必要があります。

23.9 dsbk 環境設定ファイルの場所

dsbk.conf ファイルは、eDirectory の特定のインスタンスに関連した場所ではなく、/etc 内に格納されています。

23.10 OES Linux 上での SLP の相互運用性に関する問題

OpenSLP は SLPv2 を実装しています。一方、Linux および Windows プラットフォーム上の NetIQ SLP (NDSslp) は SLPv1 を実装しています。

SLPv1 UA は SLPv2 SA からの応答を受信しません。また、SLPv2 UA は SLPv1 SA からの応答を受信しません。つまり、OpenSLP を使用しているクライアントは、NDSslp を使用しているツリーを認識することができません。同様に、NDSslp を使用しているクライアントは、OpenSLP を使用しているツリーを認識できません。SLPv1 と SLPv2 の相互運用を可能にするには、SLPv2 を実行しているディレクトリエージェントを設定する必要があります。OES Linux には OpenSLP が付属しています。ただし、Red Hat Linux など他の Linux プラットフォームにインストールされている eDirectory では、eDirectory に付属する NDSslp を使用できます。SLP の 2 つのバージョンの相互運用性に関する問題のため、OpenSLP マルチキャストを使用して通知されたツリーが NDSslp に認識されない場合や、その逆の場合があります。この問題を解決するには、OpenSLP を実行するディレクトリエージェントを設定する必要があります。

23.11 DIB ディレクトリがデフォルト以外のパスにある場合、ldif2dib でエラーログファイルを開けない

dib ディレクトリがデフォルト以外の場所に移動されている場合、ldif2dib ではデフォルトのログファイル (ldif2dib.log) を開くことができません。

この問題を回避するには、-b スイッチを使用してログファイルの場所を明示的に指定します。

23.12 仮想 SLES 10 で eDirectory サーバが自動的に起動しない

パッケージを追加した後に、YaST を使用して eDirectory を設定しない場合は、コマンドラインで次のコマンドを実行する必要があります。

chkconfig -a ndsd

23.13 システムクラッシュの後で ndsd が起動しない

システムクラッシュまたは電源異常の後に、場合によって、eDirectory サービス (ndsd) が起動しないことがあります。eDirectory を再起動するには、次の手順を実行します。

1. /var/opt/novell/eDirectory/data/ndsd.pid ファイルを削除します。
2. /etc/init.d/ndsd start コマンドを入力します。

23.14 Linux コンピュータで、すべてのタグが有効になっている場合に、DSTrace を実行してはいけない

すべてのタグが有効になっている場合、次の場所では DSTRace を実行しないでください。

- **ジャーナルモードでロードされたシステム :** ndsd メモリを構築する可能性があります。
- **インラインモードのサーバ :** ndsd がクラッシュします。

23.15 LDAP が匿名検索要求に関する RFC に準拠していない

匿名バインドが無効になっているときに認証されていない検索をクライアントが行うと、LDAP サーバは検索結果の代わりに、不適切な認証であることを示すバインド結果 operationsError を返します。

23.16 eDirectory 8.8 のカスタムインスタンスでのポートのトラブルシューティング

eDirectory 8.8 で、インスタンスのデフォルトサーバがダウンしたときに、カスタムロケーションに新しいインスタンスを設定する場合、インスタンスのデフォルトポートが取得されます。デフォルトインスタンスのポートはカスタムロケーションのインスタンスに割り当てられるため、デフォルトインスタンスは開始されません。

ホストを再起動する前に「eDirectory 8.8 のカスタムインスタンスでのポートのトラブルシューティング」(http://www.novell.com/coolsolutions/feature/17933.html) の手順に従ってください。

23.17 ホストの再起動

ホストを再起動すると、デフォルトのインスタンスバイナリを使用して作成されたデフォルトインスタンスのみが開始されます。

パスを設定し、ndsmanage を使用して、その他のインスタンスを開始させることができます。

23.18 所定の NCP ポート上のループバックアドレスで ndsd が監視していない

複数の eDirectory インスタンスが存在する場合、2 番目以降のインスタンスは、ループバックアドレス上の NCP ポートではなくデフォルトの 524 ポートで監視しようとします。

この問題を回避するには、2 番目のインスタンスの「n4u.server.tcp-port」パラメータを監視対象のポートに設定します。n4u.server.tcp-port パラメータは nds.conf ファイルに記載されています。

重要 : eDirectory 8.8 SP8 にアップグレードする前に、eDirectory のすべてのインスタンスを起動する必要があります。

23.19 LDAP トランザクション OID

LDAP トランザクションのサポートでは、supportedGroupingTypes と transactionGroupingType OID の値は同じ (2.16.840.1.113719.1.27.103.7) になります。

23.20 LDAP トレースの -5871 エラーおよび -5875 エラー

LDAP トレースの -5871 エラーと -5875 エラーは、通常、LDAP クライアントがアンバインドを実行せずに閉じようとすると起きます。そのため、これらのエラーを心配する必要はなく、無視できます。これらのエラーの詳細については、NetIQ エラーコード Web サイト (http://www.novell.com/documentation/nwec/) を参照してください。

23.21 ツリーの名前が変更されると NDSCons が -625 エラーを出す

プライマリサーバのツリーの名前を変更してセカンダリサーバの DHost をシャットダウンすると、NDSCons ユーティリティはセカンダリサーバに転送失敗エラーメッセージ -625 を表示しますが、DHost はプライマリサーバとセカンダリサーバの両方で実行し続けます。エラーが起きるのは、プライマリサーバでツリーの名前が変更されたときに、NDSCons がセカンダリサーバで実行中であったためです。NDSCons を閉じてから再起動すると、NDSCons は正常に動作します。

23.22 複数の NIC を監視すると eDirectory ldapsearch のパフォーマンスが低下する

この問題を回避するには次の手順に従ってください。

環境設定ファイルで、ldapsearch のパフォーマンスを低下させる NIC を無効にします。

または

DSTrace で set NDSTRACE =!ARC1 コマンドを使用して、詳細参照コスト (ARC) を有効にします。

23.23 Linux プラットフォームで同時接続ユーザ数を制限できない

eDirectory 8.8 SP8 では、Linux プラットフォームの同時接続ユーザ数を制限できません。従来の動作 (厳密なポートベースのチェック) を実行するには、nds.conf ファイルで次のパラメータを設定します。

```
n4u.server.mask-port-number=0
```

23.24 SLP が原因で ndsd がシャットダウンに失敗する

ネットワーク上に SLP ディレクトリエージェント (DA) を設定していない場合、SLP を使用するサービスの検索に時間がかかることがあります。eDirectory シャットダウン中に、ndsd は SLP を使用する操作を実行しようとし、それにかかる時間が init スクリプトによって通常許可されているよりも長いため、強制的にシャットダウンされます。

この問題を解決するには :

1. config ディレクトリに hosts.nds という名前の空のファイルを作成します。サーバの config ディレクトリは、ndsconfig get n4u.server.confdir コマンドを実行して取得できます。
2. /opt/novell/eDirectory/sbin/pre_ndsd_start で export NDS_USESLP=0 を指定することによって、環境変数 NDS_USESLP を 0 に設定します。
3. eDirectory を再起動します。

23.25 Windows での NLDAP の再起動

NLDAP を停止した後に、サーバを再起動して NLDAP をロードする必要があります。

23.26 LDAP 経由の SecretStore

NetIQ SecretStore 機能は、LDAP 経由では動作しません。この問題を解決するには、iManager を通じて LDAP を更新する必要があります。

23.27 相互運用性の問題

- 129 ページのセクション 23.27.1「SecretStore のロック解除後に、パスフレーズを変更できない」
- 129 ページのセクション 23.27.2「SecretStore を使用してユーザの資格情報を変更すると、Null にリセットされる」
- 129 ページのセクション 23.27.3「同じユーザに別の資格情報セットを作成すると、以前の資格情報セットが上書きされる」

23.27.1 SecretStore のロック解除後に、パスフレーズを変更できない

ユーザの資格情報と誤ったパスフレーズでログインして、忘れたパスワードを取得しようとすると、SecretStore はロックされます。SecretStore のロックは、管理者権限で解除できます。また、NetIQ SecureLogin クライアントを使用すると、パスフレーズなしでログインできます。パスフレーズを変更しようとすると、ログインは失敗し、エラーが返されます。

23.27.2 SecretStore を使用してユーザの資格情報を変更すると、Null にリセットされる

iManager プラグインを使用して SecretStore に新しい資格情報を保存しようとすると、iManager で変更が保存されず、空の資格情報列が表示されます。

資格情報を変更できるのは SecretStore iManager プラグインからのみで、管理者ではなく、ユーザとしてログインする必要があります。

23.27.3 同じユーザに別の資格情報セットを作成すると、以前の資格情報セットが上書きされる

別の資格情報セットを保存すると、SecretStore では最初のセットが保持されず、最新の資格情報セットだけが表示されます。

資格情報を変更できるのは SecretStore iManager プラグインからのみで、管理者ではなく、ユーザとしてログインする必要があります。

24 IPV6

このセクションには、すべてのプラットフォーム上の IPv6 に関する問題のトラブルシューティングについての情報が含まれています。

24.1 LDAP セキュア検索は IPv4 または IPv6 の一方と動作し、両方同時には動作しない

クライアントアドレスに IPv4 と IPv6 の両方が指定されていると、LDAP セキュア検索は失敗します。

24.2 ICE プラグインが IPV6 アドレスには使用できない

iManager が IPv4 アドレスのみを監視している場合、このプラグインは次のエラーを出して要求されたサーバに接続できません。

```
Unable to connect to the requested server. Verify the name/address and port.
```

iManager が eDirectory と連携するように IPv6 を設定するには、次の手順に従って IPv6 を有効にする必要があります。

1. catalina.properties ファイルに次のプロパティを設定して、Tomcat を再起動します。

   ```
   java.net.preferIPv4Stack=false
   ```

   ```
   java.net.preferIPv4Addresses=true
   ```

   java.net.preferIPv4Stack は iManager が eDirectory と連携する場合に適用され、java.net.preferIPv4Addresses はブラウザが iManager と連携する場合に適用されます。

2. *［LDAP オプション］* > *［LDAP サーバの表示］* > *［接続］* > *［LDAP サーバ］* の順に移動してから、IPv6 アドレスの LDAP インタフェースをポート番号付きで追加します。

   ```
   ldap://[xx::xx]:389
   ldaps://[xx::xx]:636
   ```

3. 役割ベースサービスを設定して、セッションからログアウトし、再度ログインします。

24.3 Linux および Windows の未指定の IPv6 アドレスのリスナ

未指定の IPv6 アドレスのリスナは、Linux の IPv4 および IPv6 の両方の接続を受け入れます。この動作のため、Linux では IPv4 と IPv6 の両方の未指定のリスナを同時に同じポートで開始できません。そのため、未指定の IPv6 アドレス用にすでに設定されているリスナがあると、未指定の IPv4 アドレスのリスナは開始できません。Linux は、LDAP リスナ用に未指定のアドレスを使用します。

注 : SLES 10 コンピュータで、すでに IPv4 の未指定のユーザがいる場合、同じポートで IPv6 固有の IP リスナを開始できません。SLES 10 では、これは既知の問題です。しかし、SLES 11 ではこの問題は起きません。

Windows の場合、未指定の IPv6 リスナは IPv6 接続のみを受け入れます。したがって、IPv6 接続に加えて IPv4 接続を受け入れるには、別個に IPv4 リスナを設定する必要があります。

デフォルトでは、IPv4 リスナと IPv6 リスナの両方は ldapInterfaces 用に設定されます。ldapInterfaces は、プラットフォームに応じて必要なリスナを開始します。