NetIQ® eDirectory™ 8.8 SP8

新機能ガイド

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

*新機能ガイド*では、NetIQ eDirectory の新機能について説明しています。

『*NetIQ eDirectory 8.8 SP8 新機能ガイド*』の最新版については、NetIQ eDirectory 8.8 オンラインヘルプの 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 のインストール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。

トラブルシューティングガイド

eDirectory の問題を解決する方法について説明します。

Linux プラットフォーム用チューニングガイド

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

これらのガイドは、NetIQ eDirectory 8.8 documentation の Web サイト (https://www.netiq.com/documentation/edir88/) 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* (https://www.netiq.com/documentation/imanager/)』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 サービスパック 8 の機能と機能拡張

この章では、eDirectory 8.8 SP8 の機能と機能拡張の概要について説明します。

1.1 スケーラビリティの機能拡張

より高速なデータ同期化、破損通知処理、およびジャーナルイベント処理におけるメモリフットプリントの削減を実現するために、以下で説明されるスケーラビリティの機能拡張が eDirectory 8.8 SP8 で行われています。

このリリースでは、大規模でダイナミックな環境の要求に応えるために、一部のバックグラウンドプロセスが再設計されました。既存のバックグラウンドプロセスが最適化され、システムを調整して環境に適合させるための環境設定オプションが提供されています。

1.1.1 バックグラウンドプロセスの制御

管理者は、NetIQ iMonitor の［バックグラウンドプロセスの設定］ウィンドウで、以下のバックグラウンドプロセス遅延設定ポリシーの設定により、バックグラウンドプロセスを制御できます。

- **CPU** は、同一プロセス (Skulker、Purger、または破損通知) に対してコンピュータリソースの最大使用率と最大スリープ時間を指定します。
- **ハード制限**は、各 Skulker、Purger、および破損通知プロセスの静的遅延設定を指定します。

バックグラウンドプロセスの設定の詳細については、『*NetIQ eDirectory 8.8 SP8 Administration Guide*』の「Configuring Background Processes」を参照してください。

1.1.2 Skulker プロセス

より多くのサーバに同時に複製するためのスレッド数を増やすには、Skulker プロセスを用いて最大スレッド作成数を手動で設定できます。この設定は、サーバ上のすべてのパーティションに適用できます。

Skulker プロセスの設定の詳細については、『*NetIQ eDirectory 8.8 SP8 Administration Guide*』の「Manually Configuring Synchronization Threads」を参照してください。

1.1.3 非同期レプリケーション

レプリケーションに必要となる時間を短縮するために、以下の処理を並行して実行されるようになりました。

- キャッシュ変更処理
- リモートサーバへのパケット送信

新規の**非同期アウトバンド同期設定 (ミリ秒)** オプションで、受信サーバの過負荷を回避できます。デフォルトでは、このオプションはオフになっています。環境によって設定は異なります。このオプションを有効にする場合は、まず 100 を設定して必要に応じて上下に調整します。

非同期アウトバンド同期設定の詳細については、『*NetIQ eDirectory 8.8 SP8 Administration Guide*』の「Configuring Asynchronous Outbound Synchronization」を参照してください。

1.1.4 ポリシーベースのレプリケーション

管理者は、ポリシー (XML ファイル) を作成して変更の複製方法を指定できます。たとえば、このポリシーは多数の場所に分散配置されたレプリカリングに有効です。ポリシーにタイプミスや構文の誤りがある場合、レプリケーションはデフォルトの方法に戻ります。

詳細については、『*NetIQ eDirectory 8.8 SP8 Administration Guide*』の「Policy Based Replication」を参照してください。

1.1.5 破損通知

eDirectory の以前のリリースより高速にオブジェクトの削除、名前変更、移動処理が行われるため、破損通知が生成されます。たとえば、以前のリリースで 5 サイクル必要だった更新が、現在は 2 サイクルのみで済む場合があります。

また、現行リリースでは破損通知プロセスを Skulker プロセスと並行して実行できます。

1.1.6 iMonitor による破損通知カウントと変更キャッシュのトラッキング

iMonitor には、破損通知の各状態にあるオブジェクト数が表示されます。また、任意のサーバの iMonitor でパーティションオブジェクトを表示すると、パーティションの変更キャッシュにあるオブジェクト数が確認できます。これにより、さらに詳しく同期と破損通知処理の状態がモニターできます。

1.1.7 分散リファレンスリンク (DRL)

破損通知処理を最適化するために、eDirectory では次の DRL 属性を使用しなくなりました。

- UsedBy
- ObitUsedBy

1.1.8 ジャーナルイベントのキャッシング

ジャーナルイベントシステムは変更され、メモリとディスクを組み合わせて使い、キューにイベントを保存できるようになりました。これにより、ndsd プロセスのメモリ使用量の急激な増加が軽減されます。

ジャーナルイベントでの機能拡張 :

- キャッシング

  ジャーナルイベントキューがメモリ使用量のある点 (32MB= 最大 8x4MB ブロック) を超えると、eDirectory はハードディスクキャッシュを使い始めます。

- 変数

ジャーナルイベントでは、ユーザが設定可能な次の変数を使っています。

- NDSD_EVENT_DISK_CACHE
- NDSD_EVENT_DISK_CACHE_DIR

- 圧縮

  拡張圧縮機能は、ハードディスク上のデータサイズを最小化します。圧縮比はおおよそ 20:1 です。

1.1.9 半導体ディスク (SSD) のサポート

このリリースでは、IO 処理を改善するためにエンタープライズ SSD をサポートしています。

1.1.10 詳細参照コスト (ARC)

このリリースでは、ARC がデフォルトで有効となっています。

詳細については、『*NetIQ eDirectory 8.8 SP8 Administration Guide*』の「Advanced Referral Costing」を参照してください。

1.1.11 ログイン更新間隔

新規のログイン更新無効間隔オプションで、管理者は eDirectory がログイン属性を更新しない時間の間隔 (秒) を指定できます。

注 : このオプションは、NetIQ ディレクトリサービス (NDS) のログインだけに適用されます。

詳細については、『*NetIQ eDirectory 8.8 SP8 Administration Guide*』の「Controlling and Configuring the DS Agent」を参照してください。

1.2 LDAP 拡張機能

このリリースは、次の LDAP 拡張機能を含みます。

1.2.1 許容変更制御

このオプションを使って現行 LDAP の変更処理の機能拡張ができます。存在しない属性を削除したり、既存の属性に属性値を追加しようとすると、エラーメッセージを表示しないで操作が完了します。

詳細については、『*NetIQ eDirectory 8.8 SP8 Administration Guide*』の「Configuring Permissive Modify Control」を参照してください。

1.2.2 汎用タイムサポート

汎用タイムサポートオプションによって、時間を YYYYMMDDHHmmSS.0Z 形式で表示できます。

0Z は、Active Directory と同様な秒の小数部のサポートを示しています。eDirectory は秒の小数部分の表示をサポートしていないので、このオプションは共存する環境の機能を損なわないように、秒の小数部分を *0* と表示します。

詳細については、『*NetIQ eDirectory 8.8 SP8 Administration Guide*』の「Configuring Generalized Time Support」を参照してください。

1.2.3 サブツリー削除制御

このリリースでは、コンテナオブジェクトの削除が可能なサブツリー削除制御をサポートしています。以前のリリースでは、リーフオブジェクトのみ削除できました。ただし、サブツリー削除制御はパーティションコンテナの削除はサポートしていません。

1.3 IPv6 のサポート

このリリースは、IPv4 と IPv6 の両方のネットワークをサポートしています。eDirectory をインストールすると、デフォルトで、IPv6 が自動的に有効になります。以前のバージョンの eDirectory からアップグレードした場合は、IPv6 サポートを手動で有効にする必要があります。

eDirectory 8.8 SP8 は以下の IPv6 モードをサポートしています。

- デュアルスタック
- トンネリング
- ピュア IPv6

eDirectory 8.8 SP8 は以下の IPv6 アドレスタイプをサポートしていません。

- リンクローカルアドレス
- IPv4 マップド IPv6 アドレス
- IPv4 互換 IPv6 アドレス

eDirectory 8.8 SP8 は以下のアドレス指定形式をサポートしています。

- [::]
- [::1
- [2015::12]
- [2015::12]:524

1.4 監査の機能拡張

このリリースでは、イベントのクライアント IP アドレスをサポートすることで、XDAS の監査機能を強化しています。

2 eDirectory のインストールがサポートされるプラットフォーム

eDirectory 8.8 SP8 は、eDirectory の安定性強化を目指したクロスプラットフォームのリリースです。

2.1 サポートされないプラットフォーム

eDirectory 8.8 SP8 は以下のプラットフォームをサポートしていません。

- NetWare
- Solaris 上の 32 ビットおよび 64 ビット eDirectory
- AIX 上の 32 ビット eDirectory
- Linux 上の 32 ビット eDirectory
- Windows 上の 32 ビット eDirectory

2.2 Linux

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

- SLES 11 SP1、SP2、および SP3 64 ビット
- SLES 10 SP4 64 ビット
- RHEL 5.7、5.8、および 5.9
- RHEL 6.2、6.3、および 6.4

これらのオペレーティングシステムは次の hypervisor 上で仮想モードで実行できます。

- VMware ESXi
- (SLES 10 および SLES 11 とそのサポートパック上の)Xen

注 : eDirectory 8.8 SP8 は、SLES 10 ゲスト OS を実行している SLES 10 XEN 仮想化サービスでサポートされています。NetIQ Update Web サイト (https://update.novell.com) から、次のアップデートを入手できます。

- SUSE-Linux-Enterprise-Server-X86_64-10-0-20061011-020434
- SLES10-Updates

SUSE Linux Enterprise 10 の登録と更新については、「Registering SUSE Linux Enterprise with the NetIQ Customer Center (http://www.suse.com/products/register.html)」を参照してください。最新の更新プログラムをインストールした後、インストールした更新の最小パッチレベルが 3.0.2_09763-0.8 であることを確認してください。

- Hyper-V を使用した Windows Server 2008 R2 仮想化

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

Red Hat システムに、Red Hat Errata (http://rhn.redhat.com/errata) から配布されている最新の glibc パッチが適用されていることを確認してください。glibc ライブラリの必要最小限のバージョンは、バージョン 2.1 です。

2.3 Windows

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

- Windows Server 2008 (x64) (Standard/Enterprise/Data Center エディション) およびサービスパック
- Windows Server 2008 R2 (Standard/Enterprise/Data Center エディション) およびサービスパック
- Windows 2012 Server

重要

- Windows Server 2008 R2 に eDirectory 8.8 SP8 をインストールするには、管理権限を有するアカウントを使用する必要があります。
- Windows デスクトップバージョンはサポートされていません。

3 インストールとアップグレードの拡張機能

この章では、NetIQ eDirectory 8.8 のインストールとアップグレードに関する新機能と拡張機能について説明します。

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

機能	Linux	Windows
eDirectory 8.8 のインストール用に複数のパッケージ形式を用意	✓	✗
任意の場所へのアプリケーションファイルのインストール	✓	✓
任意の場所へのデータファイルのインストール	✓	✓
任意の場所への環境設定ファイルのインストール	✓	✗
ルート以外のユーザによるインストール	✓	✗
高可用性クラスタへのインストールに対する強化されたサポート	✓	✓
FHS の準拠	✓	✗
LSB の準拠	✓	✗
サーバのヘルスチェック	✓	✓
SecretStore の統合	✓	✓
eDirectory Instrumentation インストール	✓	✓

このセクションでは、次の情報について説明します。

3.1 eDirectory 8.8 インストール用の複数のパッケージ形式

Linux では、eDirectory 8.8 のホストへのインストール時にさまざまなファイル形式を選択するオプションが用意されています。選択できるファイル形式を次の表に示します。

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

tarball を使用したインストールの詳細については、『*NetIQ eDirectory 8.8 SP8 インストールガイド*』を参照してください。

3.2 任意の場所に eDirectory 8.8 をインストールする

eDirectory 8.8 では、アプリケーション、データ、および環境設定ファイルをインストールする場所を自由に選択できます。

eDirectory 8.8 を任意の場所にインストールするシナリオの 1 つは、ホストに以前のバージョンの eDirectory がインストールされており、それをアップグレードする前に eDirectory 8.8 をテストする場合です。このようにすると、既存の eDirectory 設定を変更せずに、この新しいバージョンをテストすることもできます。その後で、既存のバージョンを保持するか、eDirectory 8.8 にアップグレードするかを決定できます。

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

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

- 18 ページのセクション 3.2.1「アプリケーションファイルに任意の場所を指定する」
- 19 ページのセクション 3.2.2「データファイルに任意の場所を指定する」
- 19 ページのセクション 3.2.3「環境設定ファイルに任意の場所を指定する」

3.2.1 アプリケーションファイルに任意の場所を指定する

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

Linux

eDirectory 8.8 を任意の場所にインストールする場合、tarball インストールファイルを使用して、eDirectory 8.8 を選択した場所に展開することができます。

Windows

eDirectory 8.8 以前でも、インストールウィザードの間にアプリケーションファイルに任意の場所を指定することができました。

3.2.2 データファイルに任意の場所を指定する

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

Linux

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

オプション	説明
-d *任意の場所*	指定したパスに DIB(eDirectory データベース) ディレクトリを作成します。 **注 :** このオプションは、eDirectory 8.8 以前にも存在しました。
-D *任意の場所*	data(pid やソケット ID などのデータを含む)、dib、および log ディレクトリを、指定したパスに作成します。

Windows

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

3.2.3 環境設定ファイルに任意の場所を指定する

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

Linux

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

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

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

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

Windows

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

3.3 ルート以外のユーザによるインストール

eDirectory 8.8 以上では、ルート以外のユーザによる eDirectory サーバのインストールと設定がサポートされています。eDirectory の以前のバージョンでは、ホストで実行される eDirectory のシングルインスタンスによってのみ、ルートユーザだけがインストールと設定を行うことができました。

eDirectory 8.8 以上では、ルート以外のユーザが tarball ビルドを使って eDirectory をインストールできます。同一または異なるユーザによる eDirectory のバイナリインストールの複数インスタンスが存在できます。ただし、ルート以外のユーザのインストールに対しても、Novell International Cryptographic Infrastructure (NICI)、SNMP、および SLP などのシステムレベルのサービスはルート権限によってのみインストールが可能です。eDirectory の機能のために、NICI は必須のコンポーネントで、SNMP と SLP はオプションのコンポーネントです。また、パッケージのインストールについては、シングルインスタンスのみがルートユーザによってインストール可能です。

インストール後に、ルート以外のユーザは個々の tarball インストールやバイナリインストールを用いて、eDirectory サーバインスタンスの設定ができます。つまり、1 つのホストで eDirectory サーバの複数のインスタンスが実行できます。なぜなら、ルートユーザもルート以外のユーザも、パッケージや tarball インストールを用いることで、異なる eDirectory サーバインスタンスを 1 つのホスト上で設定できるからです。複数インスタンスの機能の詳細については、『*NetIQ eDirectory 8.8 SP8 インストールガイド*』の「複数インスタンス」および「複数インスタンスのアップグレード」を参照してください。

ルート以外のユーザによるインストールと設定は、Linux プラットフォームでのみ適用可能です。ルート以外のユーザによるインストールと設定の詳細については、『*NetIQ eDirectory 8.8 SP8 インストールガイド*』の「ルート以外のユーザによる eDirectory 8.8 のインストール」を参照してください。

3.4 高可用性クラスタへのインストールに対する強化されたサポート

eDirectory 8.8 SP8 によって Linux と Windows クラスタ上の eDirectory のインストールと管理が簡略化され、クラスタリングのサポートを強化し高可用性を実現しています。eDirectory はまた、レプリカ同期による高可用性を提供していますが、クラスタリングと組み合わさって高レベルの可用性を達成しています。

クラスタへの eDirectory インストールの詳細については、『*NetIQ eDirectory 8.8 SP8 インストールガイド*』を参照してください。

3.5 標準の準拠

eDirectory 8.8 は次の標準に準拠しています。

- 21 ページのセクション 3.5.1「FHS の準拠」
- 22 ページのセクション 3.5.2「LSB の準拠」

3.5.1 FHS の準拠

他製品のアプリケーションファイルとのファイル競合を回避するため、eDirectory 8.8 は FHS(Filesystem Hierarchy Standard) に従っています。この機能は、Linux のみで使用できます。

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

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

次の表に、ディレクトリ構造の変更を示します。

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

環境変数のエクスポート

eDirectory 8.8 で FHS 実装を使用する場合は、パスの環境変数を更新してエクスポートする必要があります。これによって次の問題が生じます。

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

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

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

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

- 次のとおり、現在のシェル内のパスをエクスポートします。

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

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

3.5.2 LSB の準拠

eDirectory 8.8 は LSB(Linux Standard Base) に準拠するようになりました。LSB では、FHS に準拠することも推奨されています。Linux の eDirectory パッケージにはすべて、*novell* というプリフィックスが付けられています。たとえば、NDSserv の名前は novell-NDSserv になっています。

3.6 サーバのヘルスチェック

eDirectory 8.8 には、アップグレード前にサーバが安全な状態であるかどうかを判断するのに役立つ、サーバのヘルスチェックが導入されています。

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

3.6.1 ヘルスチェックの必要性

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

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

3.6.2 サーバが正常であることの確認基準

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

3.6.3 ヘルスチェックを実行する

サーバのヘルスチェックは次の 2 種類の方法で実行できます。

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

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

アップグレードと同時に実行

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

Linux

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

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

Windows

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

スタンドアロンユーティリティとして実行

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

表 3-1 *ヘルスチェックユーティリティ*

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

3.6.4 ヘルスチェックのタイプ

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

- 基本的なサーバの状態
- パーティションとレプリカの状態

ndscheck ユーティリティを実行すると、ヘルスチェックの結果は画面に表示され、ndscheck.log に記録されます。ログファイルの詳細については、「25 ページのセクション 3.6.6「ログファイル」」を参照してください。

アップグレードの一部としてヘルプチェックを実行した場合、ヘルスチェックの後にエラーの深刻度に基づいて、アップグレードを続行するかどうかの確認が求められるか、または処理が中断されます。エラーの詳細については、「24 ページのセクション 3.6.5「状態のカテゴリ」」に記載されています。

基本的なサーバの状態

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

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

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

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

パーティションとレプリカの状態

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

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

3.6.5 状態のカテゴリ

サーバの状態は、チェック中に検出されるエラーに基づいて、次の 3 つカテゴリに分類されます。ヘルスチェックのステータスは、ログファイルに記録されます。詳細については、「25 ページのセクション 3.6.6「ログファイル」」を参照してください。

ヘルスチェックのステータスは、正常、警告、および重大の 3 つに分類されます。

正常

ヘルスチェックが成功した場合、サーバの状態は正常です。

アップグレードは中断されずに続行されます。

警告

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

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

警告は通常、次の状況で発生します。

1. サーバが LDAP ポートと HTTP ポート (通常、セキュリティ保護、または両方) を監視していない。

2. レプリカリング内のいずれの非マスタサーバにも接続できない。
3. レプリカリング内のサーバが同期していない。

重大

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

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

重大な状態は通常、次の状況で発生します。

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

3.6.6 ログファイル

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

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

ヘルスチェックのログファイルには、次のものが含まれています。

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

次の表に、さまざまなプラットフォームでのログファイルの場所を示します。

表 3-2 *ヘルスチェックのログファイルの場所*

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

3.7 SecretStore と eDirectory との統合

eDirectory 8.8 には、eDirectory の環境設定中に Novell SecretStore 3.4 を設定するオプションが用意されています。eDirectory 8.8 以前は、SecretStore を手動でインストールする必要がありました。

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

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

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

- **Linux:**

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

- **Windows:**

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

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

3.8 eDirectory Instrumentation インストール

以前の eDirectory Instrumentation は、Novell Audit に組み込まれていました。eDirectory 8.8 SP3 バージョン以降では、eDirectory Instrumentation は単独でインストールする必要があります。

eDirectory Instrumentation のインストール、設定、アンインストールの詳細については、『*NetIQ eDirectory 8.8 SP8 インストールガイド*』の「eDirectory Instrumentation」セクションを参照してください。

3.9 その他の情報

この章で説明している機能の詳細については、次のいずれかを参照してください。

- *NetIQ eDirectory 8.8 SP8 インストールガイド*
- *NetIQ eDirectory 8.8 SP8 管理ガイド*
- Linux について : nds-install、ndsconfig、および ndscheck のマニュアルページ

4 NICI バックアップと復元

NICI (Novell International Cryptography Infrastructure) は、ファイルシステム内と、システムおよびユーザ固有のディレクトリやファイルに、キーとユーザデータを保存します。これらのディレクトリとファイルは、オペレーティングシステムによって提供されるメカニズムを使用して適切なアクセス権を設定することによって保護されます。この設定は、NICI インストールプログラムによって行われます。

システムから NICI をアンインストールしても、システムまたはユーザ固有のディレクトリとファイルは削除されません。したがって、これらのファイルを以前の状態に復元することが必要になるのは、重大なシステム障害や人為的エラーから回復する場合のみです。既存の NICI ユーザディレクトリおよびファイルを上書きすると、既存のアプリケーションで問題が発生する可能性があることを理解しておくことが重要です。

DIB を開くためのデータベースキーは NICI キーでラップします。したがって、NICI のバックアップから独立して行った eDirectory のバックアップは役に立ちません。

以前の NICI バックアップと復元からの変更点

以前は、NICI バックアップと復元は手動で行いました。今回のリリースでは、新たな NICI バックアップと復元のソリューションが加わりました。eDirectory バックアップソリューション (eMBox バックアップおよび DSBK) にスイッチ (-e) が付け加えられましたが、その機能は :

1. eDirectory バックアップを実行中に NICI キーをバックアップします。
2. eDirectory 復元を実行中に NICI キーを復元します。

『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「NICI のバックアップと復元」を参照してください。

5 ndspassstore ユーティリティ

ndspassstore は新規のユーティリティで、SAdmin ユーザや eDirectory ユーザのために暗号化パスワードを保管します。このユーティリティは、Linux と Windows プラットフォームで利用可能です。このユーティリティは、ユーザ名とパスワードを入力データとして取得し、暗号化したキー値のペアとして保管します。

今回のリリースでは、このユーティリティは SAdmin ユーザのパスワード設定に使われています。

このユーティリティは、Windows の C:\Novell\NDS および Linux の /opt/novell/eDirectory/bin においてデフォルトで利用できます。

コマンド概要

サーバコンソールに次のコマンドを入力することによって、ndspassstore ユーティリティが使えます。

ndspassstore -a < 管理者コンテキスト > -w < パスワード >

オプション	使用率
-a adminContext	このオプションは、管理者権限を持つユーザの完全識別名である adminContext を受け入れるために使われます。
-w password	このオプションは、認証のためにパスワード (ユーザパスワード) を受け入れるために使われます。

6 複数のインスタンス

従来は、1 台のホスト上で設定することができる NetIQ eDirectory のインスタンスは 1 つだけでした。eDirectory 8.8 では複数インスタンスの機能がサポートされるため、次の設定が可能です。

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

eDirectory 8.8 では、インスタンスを簡単に追跡できるユーティリティ (ndsmanage) も提供されます。

次の表に、複数インスタンスをサポートするプラットフォームを示します。

機能	Linux	Windows
複数インスタンスのサポート	✓	✗

このセクションでは、次の情報について説明します。

6.1 複数インスタンスの必要性

複数インスタンスは、次のことを行う必要性から提供されるようになりました。

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

6.2 複数インスタンスを展開する場合のシナリオ

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

大企業における eDirectory の使用

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

  たとえば、ポート 1524、2524、および 3524 で LDAP サービスを実行するレプリカサーバ 3 台がある場合、eDirectory の新しいインスタンスを設定し、新しいポート 636 で高い可用性の LDAP サービスを提供できます。
- 1 台のホストに複数インスタンスを設定すると、組織内の複数の部門にまたがってハイエンドのハードウェアを活用できます。

評価用セットアップにおける eDirectory の使用

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

6.3 複数インスタンスの使用

eDirectory 8.8 によって、複数インスタンスの設定が容易になります。複数インスタンスを効果的に使用するためには、セットアップを慎重に計画してから、複数インスタンスを設定する必要があります。

- 32 ページのセクション 6.3.1「セットアップの計画」
- 32 ページのセクション 6.3.2「複数インスタンスを設定する」

6.3.1 セットアップの計画

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

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

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

6.3.2 複数インスタンスを設定する

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

注 : すべてのインスタンスは同じサーバキー (NICI) を共有します。

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

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

ndsmanage ユーティリティを使用して、新しいインスタンスを設定することもできます。詳細については、「34 ページの 「ndsmanage によるインスタンスの作成」」を参照してください。

6.4 複数インスタンスを管理する

このセクションでは、次の情報を紹介します。

6.4.1 ndsmanage ユーティリティ

ndsmanage ユーティリティを使用すると、次の操作を実行できます。

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

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

- すべてのインスタンスの開始と停止

インスタンスの表示

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

表 6-1　インスタンスを表示するための ndsmanage の使用

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

各インスタンスについて、次のフィールドが表示されます。

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

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

詳細については、「35 ページの 図 6-1」を参照してください。

ndsmanage によるインスタンスの作成

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

1. 次のコマンドを入力します。

   ```
   ndsmanage
   ```

   2 つのインスタンスを設定した場合、次の画面が表示されます。

図 6-1　ndsmanage ユーティリティの出力画面

```
edirscrteem1:~ #
edirscrteem1:~ # ndsmanage
サーバインスタンス管理ユーティリティ  NetIQ eDirectory環境設定ユーティリティ  8.8 SP8 v20801.42

次のユーザが設定したインスタンスのリストです。ユーザ：root

[1] /etc/opt/novell/eDirectory/conf/nds.conf : .EDIRSCRTEEM1.SCREENS1.TREE_SCREENS1. : 10.21.3.1
16@524 : アクティブ

[2] /root/Desktop/nds.conf : .SERVER2.SCREENS1.. : 10.21.3.116@524 : アクティブ

入力 [r] リストを更新するには，[1 - 2] その他のオプションについて、 [c] 新規インスタンスの作成に
ついて または [q] 中止するには：
```

2 新しいインスタンスを作成するには、「c」と入力します。

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

特定のインスタンスに対する操作の実行

各インスタンスについて、次の操作を実行できます。

- 35 ページの 「特定のインスタンスの開始」
- 36 ページの 「特定のインスタンスの停止」
- 36 ページの 「インスタンスの設定解除」

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

特定のインスタンスの開始

自分が設定したインスタンスを開始するには、次の操作を実行します。

1 次のように入力します。

```
ndsmanage
```

2 開始するインスタンスを選択します。

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

図 6-2　ndsmanage ユーティリティのインスタンスオプションの出力画面

```
次のユーザが設定したインスタンスのリストです。ユーザ：root

[1] /etc/opt/novell/eDirectory/conf/nds.conf : .EDIRSCRTEEM1.SCREENS1.TREE_SCREENS1. : 10.21.3.1
16@524 : アクティブ

[2] /root/Desktop/nds.conf : .SERVER2.SCREENS1.. : 10.21.3.116@524 : アクティブ

入力 [r] リストを更新するには，[1 - 2] その他のオプションについて、 [c] 新規インスタンスの作成に
ついて または [q] 中止するには：1

選択されたインスタンス：
[1] /etc/opt/novell/eDirectory/conf/nds.conf : .EDIRSCRTEEM1.SCREENS1.TREE_SCREENS1. : 10.21.3.1
16@524 : アクティブ

[l] サーバ上のレプリカの一覧表示
[s] インスタンスの開始
[k] インスタンスの停止
[t] ndstraceの実行
[d] 設定解除
[b] 前のメニューに戻る
[q] 終了

このインスタンスの処理を上から選択してください。
```

3 インスタンスを開始するには、「s」と入力します。

または、コマンドプロンプトに次のコマンドを入力することもできます。

ndsmanage start --config-file *configuration_file_of_the_instance_configured_by_you*

特定のインスタンスの停止

自分が設定したインスタンスを停止するには、次の操作を実行します。

1 次のように入力します。

```
ndsmanage
```

2 停止するインスタンスを選択します。

メニューが拡張し、特定のインスタンスに対して実行可能なオプションが表示されます。詳細については、「(36 ページ) ndsmanage ユーティリティのインスタンスオプションの出力画面」を参照してください。

3 インスタンスを停止するには、「k」と入力します。

または、コマンドプロンプトに次のコマンドを入力することもできます。

ndsmanage stop --config-file *configuration_file_of_the_instance_configured_by_you*

インスタンスの設定解除

インスタンスの設定を解除するには、次の手順を実行します。

1 次のように入力します。

```
ndsmanage
```

2 設定解除するインスタンスを選択します。

メニューが拡張し、特定のインスタンスに対して実行可能なオプションが表示されます。詳細については、「(36 ページ) ndsmanage ユーティリティのインスタンスオプションの出力画面」を参照してください。

3 インスタンスを設定解除するには、「d」と入力します。

すべてのインスタンスの開始と停止

自分が設定したすべてのインスタンスを開始および停止できます。

すべてのインスタンスの開始

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

ndsmanage startall

特定のインスタンスを開始するには、「35 ページの 「特定のインスタンスの開始」」を参照してください。

すべてのインスタンスの停止

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

ndsmanage stopall

特定のインスタンスを停止するには、「36 ページの 「特定のインスタンスの停止」」を参照してください。

6.4.2 特定のインスタンスの識別

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

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

6.4.3 特定のインスタンスに対するユーティリティの呼び出し

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

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

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

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

6.5 複数インスタンスのシナリオ

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

6.5.1 セットアップの計画

Mary は次のインスタンス識別子を指定します。

- **インスタンス 1:**

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

- **インスタンス 2:**

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

6.5.2 インスタンスの設定

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

- **インスタンス 1:**

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

- **インスタンス 2:**

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

6.5.3 インスタンスに対するユーティリティの呼び出し

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

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

または

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

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

6.5.4 インスタンスの表示

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

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

  ```
  ndsmanage
  ```

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

  ```
  ndsmanage john
  ```

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

  ```
  ndsmanage -a
  ```

6.6 その他の情報

複数インスタンスのサポートの詳細については、次を参照してください。

- *NetIQ eDirectory 8.8 SP8 インストールガイド*
- Linux 用 : ndsconfig および ndsmanage マニュアルページ

7 SASL-GSSAPI を使用して eDirectory を認証

NetIQ eDirectory 8.8 の SASL-GSSAPI メカニズムを使用すると、LDAP 経由で Kerberos チケットを使用して eDirectory に対する認証を行えます。eDirectory のユーザパスワードを入力する必要はありません。Kerberos チケットは、Kerberos サーバに対する認証を行うことによって取得されます。

この機能は主に、Kerberos インフラストラクチャがすでに配置された環境がある LDAP アプリケーションユーザにとって便利です。このため、このようなユーザは、個別の LDAP ユーザパスワードを入力することなく、LDAP サーバへの認証を行うことができます。

この認証を容易に行えるように、eDirectory には SASL-GSSAPI メカニズムが導入されています。

SASL-GSSAPI の現在の実装は、RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222) に準拠しており、認証メカニズムとしては Kerberos v5 のみをサポートしています。

このセクションでは、次の情報について説明します。

7.1 概念

7.1.1 Kerberos について

Kerberos は、ネットワーク上でエンティティを認証する手段を提供する標準プロトコルです。このプロトコルは、信頼されるサードパーティのモデルに基づいています。このモデルでは、共有されるシークレットが必要で、対称型のキー暗号化が使用されます。

詳細については、RFC 1510 (http://www.ietf.org/rfc/rfc1510.txt?number=1510) を参照してください。

7.1.2 SASL について

SASL(Simple Authentication and Security Layer) は、認証の抽象化を行う層をアプリケーションに提供します。これは、認証モジュールをプラグインで接続できるフレームワークです。

詳細については、RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222) を参照してください。

7.1.3 GSSAPI について

GSSAPI(Generic Security Services Application Program Interface) は、API の標準セットを通して認証とその他のセキュリティサービスを提供します。さまざまな認証メカニズムがサポートされていますが、最も一般的なのは Kerberos v5 です。

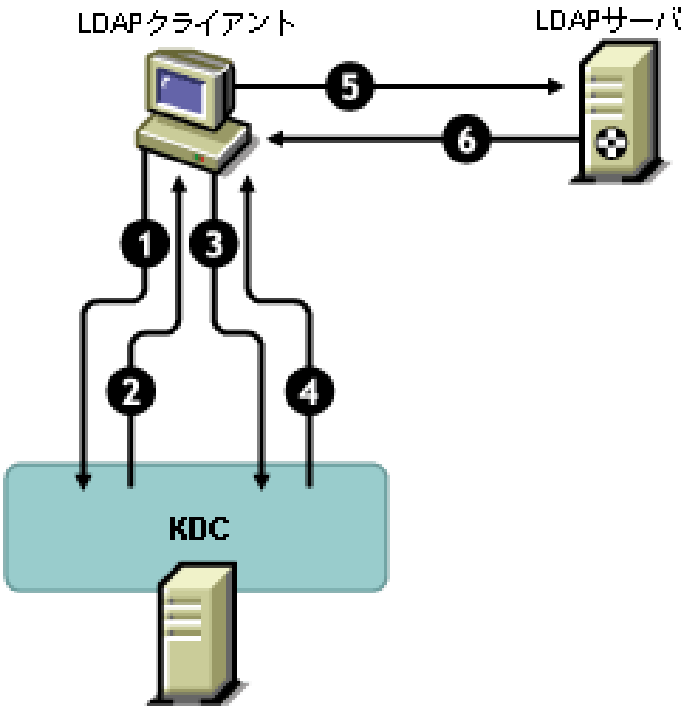
GSS API の形式に関する詳細については、RFC 1964 (http://www.ietf.org/rfc/rfc1964.txt?number=1964) を参照してください。

この SASL-GSSAPI 実装は、RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222) セクション 7.2 に規定されているものです。

7.2 eDirectory における GSSAPI の動作

次の図は、GSSAPI が LDAP サーバとともにどのように動作するかを示しています。

図 7-1 *GSSAPI の動作*



この図の数字は、それぞれ次のことを示しています。

1 eDirectory ユーザは、チケット認可チケット (TGT) と呼ばれる初期チケットの要求を、LDAP クライアントを通して Kerberos KDC(Key Distribution Center) サーバに送信します。

Kerberos KDC としては、MIT または Microsoft* のいずれかのものを使用できます。

2 KDC は、TGT を送って LDAP クライアントに応答します。

3 LDAP クライアントは TGT を KDC に返信し、LDAP サービスチケットを要求します。

4 KDC は、LDAP サービスチケットを送って LDAP クライアントに応答します。

5 LDAP クライアントは LDAP サーバに対して ldap_sasl_bind を実行し、LDAP サービスチケットを送信します。

6 LDAP サーバは GSSAPI メカニズムを利用して LDAP サービスチケットを確認し、その結果に基づいて、ldap_sasl_bind が成功したか失敗したかを LDAP クライアントに返信します。

7.3 GSSAPI の設定

1 eDirectory への接続に SSL/TLS 接続を使用するように iManager が設定されていない場合、SASL-GSSAPI 用の iManager プラグインは動作しません。レルムのマスタキーとプリンシパルキーを保護するために、安全な接続が必要です。

   通常、iManager は eDirectory への接続に SSL/TLS 接続を使用するようにデフォルトで設定されています。iManager 設定をホストしているツリーとは別のツリーで GSSAPI 用に Kerberos ログインメソッドを設定する場合は、SSL/TLS 接続で eDirectory に接続するように iManager を設定する必要があります。

   SSL/TLS 接続を利用して eDirectory へ接続するように iManager を設定する方法については、『*NetIQ iManager 2.7 管理ガイド* (https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html)』を参照してください。

   SASL-GSSAPI (kerberosPlugin.npm) に対する iManager のプラグインは、eDir_88_iMan26_Plugins.npm および eDir_88_iMan27_Plugins.npm ファイルの一部として提供しています。Novell ダウンロード Web サイト (http://download.novell.com) から NPM をダウンロードします。

2 Kerberos チケットを使用して eDirectory サーバへの認証を行うには、次の操作を実行します。

   2a Kerberos スキーマを拡張する。

   2b レルムコンテナを作成する。

   2c KDC からサービスプリンシパルキーまたは共有キーを抽出する。

   2d LDAP サービスプリンシパルオブジェクトを作成する。

   2e Kerberos のプリンシパル名をユーザオブジェクトに関連付ける。

以上のステップについては、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「eDirectory による GSSAPI の設定」を参照してください。

7.4 LDAP での GSSAPI の使用方法

GSSAPI を設定すると、GSSAPI が他の SASL 方式と共に rootDSE の supportedSASLMechanisms 属性に追加されます。ルート DSE (DSE は DSA (Directory System Agent) Specific (固有) Entry(エントリ) の略) とは、ディレクトリ情報ツリー (DIT) のルートにあるエントリです。詳細については、「NetIQ eDirectory 8.8 SP8 管理ガイド」の『*「eDirectory における LDAP の動作について」*』を参照してください。

LDAP サーバは、SASL に問い合わせて環境設定時にインストールしたメカニズムを検索し、インストールされたメカニズムを自動でサポートします。また、supportedSASLMechanisms 属性を使って rootDSE で現在サポートされている SASL メカニズムをレポートします。

そのため、GSSAPI をインストールすると、GSSAPI がデフォルトのメカニズムになります。ただし、明示的に SASL GSSAPI メカニズムを使用して LDAP の操作を行う場合は、コマンドラインで GSSAPI を指定できます。

たとえば、OpenLDAP で GSSAPI メカニズムを使用して検索を行うには、次のように入力します。

```
ldapsearch -Y GSSAPI -h 164.99.146.48 -b "" -s base
```

7.5 よく使用される用語

次の表に、Kerberos と GSSAPI でよく使用される用語の定義を示します。

表 7-1 *Kerberos/GSSAPI の用語*

用語	定義
KDC (Key Distribution Center)	ユーザを認証してチケットを発行する Kerberos サーバ。
プリンシパル	KDC に登録されているエンティティ (ユーザまたはサービスインスタンス)。
レルム	複数の KDC によって管理されるドメインまたはプリンシパルのグループ。
サービスチケット (ST)	特定のサービスプリンシパルの共有キーを使って暗号化されたクライアント情報、サービス情報、およびセッションキーを格納しているレコード。
チケット認可チケット (TGT)	チケットのタイプの 1 つで、クライアントはそれを使用すると追加の Kerberos チケットを入手できる。

8 大文字と小文字を区別するユニバーサルパスワードを適用

NetIQ eDirectory 8.8 では、ユニバーサルパスワードを有効にして、次のクライアントやユーティリティから eDirectory 8.8 サーバにアクセスするときに、パスワードの大文字と小文字が区別されるようにすることができる。

- Novell Client 4.9 以降
- eDirectory 8.8 にアップグレードした管理ユーティリティ
- NetIQ iManager 2.7 以降、ただし Windows で実行される場合を除く

任意のバージョンの LDAP SDK を使用して、大文字と小文字を区別するパスワードを適用できます。

次の表に、大文字と小文字を区別するパスワード機能がサポートされるプラットフォームを示します。

機能	Linux	Windows
大文字と小文字を区別するユニバーサルパスワードの適用	✓	✓

このセクションでは、次の情報について説明します。

8.1 大文字と小文字を区別するパスワードの必要性

パスワードの大文字と小文字を区別することで、ディレクトリへのログインのセキュリティが向上します。たとえば、大文字と小文字が区別されるパスワード「aBc」がある場合、abc、Abc、ABC のような組み合わせでログインを試みてもすべて失敗します。

eDirectory 8.8 以降では、eDirectory 8.8 にアップグレードされたすべてのクライアントについて、パスワードの大文字と小文字を区別できます。

大文字と小文字を区別するパスワードの使用を強制することで、Novell のレガシークライアントが eDirectory 8.8 サーバにアクセスできないようにします。詳細については、「48 ページのセクション 8.4「Novell レガシークライアントの eDirectory 8.8 サーバへのアクセスを防止する」」を参照してください。

8.2 パスワードの大文字と小文字が区別されるようにする方法

eDirectory 8.8 以降では、ユニバーサルパスワードを有効にすることで、すべてのクライアントについてパスワードの大文字と小文字を区別できるようになりました。ユニバーサルパスワードは、デフォルトでは無効になっています。

8.2.1 前提条件

デフォルトでは、LDAP およびその他のサーバ側ユーティリティでは NDS ログインを最初に使用します。NDS ログインに失敗した場合は、簡易パスワードログインを使用します。大文字と小文字を区別するパスワード機能を動作させるには、Novell モジュラー認証サービス (NMAS) を使用してログインする必要があります。したがって、NDSD_TRY_NMASLOGIN_FIRST 環境変数を設定して、大文字と小文字を区別するパスワード機能を有効にします。

大文字と小文字を区別するパスワード機能を使用できるようにするには、次の手順を完了させます。

1 環境変数を設定する
   - Linux:

     以下を /opt/novell/eDirectory/sbin/pre_ndsd_start の最後に付け加えます。

     ```
     NDSD_TRY_NMASLOGIN_FIRST=true
     export NDSD_TRY_NMASLOGIN_FIRST
     ```

   - Windows:

     ［マイコンピュータ］を右クリックして、［プロパティ］を選択します。［詳細設定］タブの［環境変数］をクリックします。［システム環境変数］に変数を追加して、値を True に設定します。
2 eDirectory サーバを再起動します。

注 : 認証に NMAS を用いるとログインにかかる時間が長くなります。

8.2.2 パスワードの大文字と小文字が区別されるようにする

1 既存のパスワードを使用して eDirectory にログインします。

   新規インストールの場合は、eDirectory 8.8 の設定中に指定したパスワードが既存のパスワードになります。

   たとえば、パスワードが「novell」だとします。

   注 : このパスワードの大文字と小文字は区別されません。

2 ユニバーサルパスワードを有効にする .

   詳細については、『*Novell パスワード管理 3.3 管理ガイド*』の「ユニバーサルパスワードの配備」セクションを参照してください (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html)。

3 eDirectory からログアウトします。

4 任意の大文字と小文字で記述した既存のパスワードを使用して、eDirectory にログインします。

ここで指定するパスワードでは、大文字と小文字が区別されます。

たとえば、「NoVELL」と入力します。

これでパスワードは「NoVELL」に設定されます。「NoVELL」ではなく、「novell」や他の大文字と小文字の組み合わせを入力すると、すべて無効になります。

大文字と小文字を区別するパスワードに移行する場合は、「48 ページのセクション 8.3.1「大文字と小文字を区別するパスワードへの移行」?v を参照してください。

設定する新しいパスワードはすべて、有効にしたユニバーサルパスワードのレベル (オブジェクトまたはパーティション) に応じて、大文字と小文字が区別されます。

8.2.3 大文字と小文字を区別するパスワードの管理

iManager からユニバーサルパスワードを有効または無効にすることによって、パスワードの大文字と小文字をどのレベルまで区別するかを管理できます。詳細については、『*NetIQ パスワード管理 3.3 管理ガイド*』の「ユニバーサルパスワードの配備」セクションを参照してください (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html)。

8.3 Novell レガシークライアントおよびユーティリティのアップグレード

最新バージョンの Novell クライアントおよび NetIQ ユーティリティを次に示します。

- Novell Client 4.9
- eDirectory 8.8 に付属の管理ユーティリティ
- NetIQ iManager 2.7 以降

これらのバージョンより前のクライアントとユーティリティは、Novell レガシークライアントになります。

Novell レガシークライアントに対しては、最新バージョンにアップグレードした後に、大文字と小文字が区別されるパスワードを使用できます。eDirectory 8.8 では、容易で柔軟性の高い方法で、既存のパスワードから大文字と小文字が区別されるパスワードに移行できます。詳細については、「48 ページのセクション 8.3.1「大文字と小文字を区別するパスワードへの移行」」を参照してください。

レガシークライアントを最新バージョンにアップグレードしない場合、レガシークライアントによる eDirectory 8.8 の使用が、サーバレベルでブロックされることがあります。詳細については、「48 ページのセクション 8.4「Novell レガシークライアントの eDirectory 8.8 サーバへのアクセスを防止する」」を参照してください。

8.3.1 大文字と小文字を区別するパスワードへの移行

ユニバーサルパスワードはデフォルトで無効になっているため、iManager でユニバーサルパスワードを有効にするまで、既存のパスワードは影響を受けません。詳細な手順については、「46 ページのセクション 8.2「パスワードの大文字と小文字が区別されるようにする方法」」を参照してください。

次の例では、大文字と小文字を区別するパスワードへの移行について説明します。

ログインセッション 1: ユニバーサルパスワードはデフォルトで無効になっています。

- 既存のパスワードを使用してログインします。たとえば、パスワードが「netiq」だとします。
- このパスワードの大文字と小文字は区別されません。そのため、「netiq」と「NetIQ」はどちらも有効なパスワードです。
- ログイン後、ユニバーサルパスワードを有効にします。『*NetIQ パスワード管理 3.3 管理ガイド*』の「ユニバーサルパスワードの配備」を参照してください (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html)。

ログインセッション 2: 前のセッションでユニバーサルパスワードが有効になりました。

- 既存のパスワードを使用してログインします。たとえば、「noVell」とパスワードを入力したとします。
- ユニバーサルパスワードが有効にされていると、このパスワードの大文字と小文字が区別されるようになります。そのため、パスワードをどのように入力したかを記憶しておく必要があります。

ログインセッション 3、および以後のログイン :

- パスワードとして「netIQ」を使用してログインする場合、パスワードは有効です。
- パスワードとして「NetIQ」(または「noVell」以外の大文字と小文字の組み合わせ) を使用してログインする場合、パスワードは無効になります。

8.4 Novell レガシークライアントの eDirectory 8.8 サーバへのアクセスを防止する

eDirectory 8.7.1 および 8.7.3 では、Novell レガシークライアントが NDS パスワードの設定や変更を行うことを防止できました。eDirectory 8.8 では、レガシークライアントが eDirectory 8.8 にログインすること、およびパスワードを検証することも防止できます。

eDirectory 8.8 の使用を Novell レガシークライアントに許可または禁止するには、iManager または LDAP のいずれかを使用して、NDS ログインを設定する必要があります。

このセクションでは、次の情報を紹介します。

8.4.1 Novell レガシークライアントによる eDirectory 8.8 サーバへのアクセスを防止することの必要性

Novell レガシークライアントのパスワードは、大文字と小文字が区別されません。このため eDirectory 8.8 以降では、大文字と小文字が区別されるパスワードの使用を適用する場合、レガシークライアントによるディレクトリへのアクセスをブロックする必要が生じる可能性があります。

Novell Client 4.9 より前のバージョンでは、ユニバーサルパスワードはサポートされていませんでした。ログインとパスワードの変更が、NMAS に対してではなく NDS パスワードに直接反映されていたためです。ユニバーサルパスワードを使用している場合、レガシークライアントがパスワードを変更すると、パスワードドリフトと呼ばれる問題が発生することがあります。これは、NDS パスワードとユニバーサルパスワードが同期されないことを意味します。この問題を防止するには、1 つのオプションとして、バージョンが 4.9 より前のクライアントによってパスワードが変更されるのをブロックするという方法があります。

レガシークライアントによる eDirectory 8.8 サーバへのアクセスをブロックする方法の詳細については、次のセクションの「NDS ログイン設定の管理」を参照してください。

8.4.2 NDS ログイン設定の管理

NDS ログインを設定すると、Novell レガシークライアントによる eDirectory 8.8 サーバへのアクセスを、許可または禁止することができます。NDS ログイン設定は、iManager 2.6 と LDAP を通して管理できます。

eDirectory 8.8 以降では、iManager はもちろん、LDAP を使用してパスワードの設定や変更を行うことができます。

このセクションでは、次の情報について説明します。

- 49 ページの 「異なるレベルでの NDS 設定」
- 51 ページの 「iManager を使用して NDS 設定を管理する」
- 51 ページの 「LDAP を使用して NDS 設定を管理する」
- 53 ページのセクション 8.4.4「大文字と小文字を区別するパスワードを混在ツリーで適用する」

異なるレベルでの NDS 設定

NDS ログインは、次の 1 つまたはすべてのレベルで設定することができます。

- パーティションレベル
- オブジェクトレベル

設定をどのレベルにも指定しない場合、NDS ログイン設定はすべてのレベルで有効になります。

オブジェクトレベルの設定はパーティションレベルの設定を常に上書きます。次の表に各レベルでの設定を示します。

表 8-1 NDS 設定

オブジェクトレベルでの設定	パーティションレベルでの設定	環境設定
指定されていない	有効	有効
有効	指定されていない	有効
指定されていない	無効	無効
無効	指定されていない	無効
有効	有効	有効
有効	無効	有効
無効	有効	無効
無効	無効	無効

すべてのレベル (オブジェクトおよびパーティション) で、NDS ログインについて次のことを設定できます。

- NDS パスワードを使用したディレクトリへのログイン、または NDS パスワードの検証
- 新しいパスワードの設定と既存のパスワードの変更

ディレクトリへのログインまたは NDS パスワードの検証

NDS パスワードを使用したログイン / 検証とは、次のことを意味します。

- NDS パスワードを使用してディレクトリにログインする。
- ディレクトリで既存のパスワードを検証する。

NDS パスワードを使用したログイン / 検証は、デフォルトで有効になっています。ログイン / 検証キーを無効にすると、最新バージョンの eDirectory へのログインや、パスワードの検証ができなくなります。NDS パスワードを使用したログイン / 検証は、パーティションおよびオブジェクトのレベルで有効または無効にできます。ログイン / 検証が無効にされた場合、NDS パスワードの設定や変更ができなくなります。

NDS パスワードを使用したログイン / 検証は、iManager 2.5 と LDAP を通して設定できます。詳細については、51 ページの 「iManager を使用して NDS 設定を管理する」および51 ページの 「LDAP を使用して NDS 設定を管理する」を参照してください。

新しいパスワードの設定および NDS パスワードの変更

NDS パスワードの設定 / 変更とは、次のことを意味します。

- オブジェクトに対して新しいパスワードを設定する。
- オブジェクトの既存のパスワードを変更する。

NDS パスワードの設定 / 変更は、デフォルトで有効になっています。キーの設定 / 変更を無効にすると、新しいパスワードの設定や既存のパスワードの変更を eDirectory で行えなくなります。NDS パスワードを使用した設定 / 変更は、パーティションおよびオブジェクトのレベルで有効または無効にできます。ログイン / 検証が無効にされた場合、パスワードの設定 / 変更が行えなくなります。

NDS パスワードの設定および変更は、以前は LDAP を通してのみ行われました。現在は、iManager でも管理できるようになりました。詳細については、51 ページの 「iManager を使用して NDS 設定を管理する」および51 ページの 「LDAP を使用して NDS 設定を管理する」を参照してください。

iManager を使用して NDS 設定を管理する

このセクションでは、次の情報を紹介します。

- 51 ページの 「パーティションの NDS 環境設定を有効 / 無効にする」
- 51 ページの 「オブジェクトの NDS 設定を有効 / 無効にする」

ログイン / 検証キーや設定 / 変更キーは、NDS ログイン設定で有効にすることができます。

パーティションの NDS 環境設定を有効 / 無効にする

eDirectory 8.8 以前のクライアントに対して NDS ログインを有効にする :

1. iManager の *[役割およびタスク]* ボタンをクリックします。『 』。
2. *［NMAS］* > *［ユニバーサルパスワードの強制］* の順に選択します。
3. ［ユニバーサルパスワードの強制］プラグインで、*［NDS Configuration for a Partition (パーティションの NDS 環境設定)］* を選択します。
4. ［NDS Configuration for a Partition (パーティションの NDS 環境設定)］ウィザードの指示に従って、パーティションレベルでログインとパスワード管理を設定します。

   ウィザードの各段階で、［ヘルプ］が利用できます。

オブジェクトの NDS 設定を有効 / 無効にする

eDirectory 8.8 以前のクライアントに対して NDS ログインを有効にする :

1. iManager の *[役割およびタスク]* ボタンをクリックします。『 』。
2. *［NMAS］* > *［ユニバーサルパスワードの強制］* の順に選択します。
3. ウィザードで *［NDS Configuration for an Object (オブジェクトクラスの NDS 環境設定)］* を選択します。
4. ［NDS Configuration for an Object (オブジェクトの NDS 環境設定)］ウィザードの指示に従って、オブジェクトレベルでログインとパスワード管理を設定します。

   ウィザードの各段階で、［ヘルプ］が利用できます。

LDAP を使用して NDS 設定を管理する

重要 : NDS 設定の管理には、LDAP ではなく、iManager を使用することを強くお勧めします。

NDS 設定は、パーティションのルートコンテナまたはオブジェクトの eDirectory 属性を使用して、LDAP 経由で管理することができます。これらの属性は eDirectory 8.7.1 以降のスキーマの一部であり、eDirectory 8.7 以前ではサポートされていません。

レガシークライアントで NDS ログイン設定に使用される方法は NDAP ログイン管理と呼ばれ、NDS パスワード設定に使用される方法は NDAP パスワード管理と呼ばれています。

このセクションでは、次の情報について説明します。

- 52 ページの 「パーティションの NDS 環境設定を有効 / 無効にする」
- 52 ページの 「オブジェクトの NDS 設定を有効 / 無効にする」

パーティションの NDS 環境設定を有効 / 無効にする

ログインおよびパスワード管理の検証

ndapPartitionLoginMgmt 属性を使用し、パーティションに対して NDS ログインを有効 / 無効にしたり、パスワード管理を検証したりします。

ndapPartitionLoginMgmt 属性値	説明
存在しないか指定されていない	NDAP ログイン管理が有効になります。
0	NDAP ログイン管理が無効になります。
1	NDAP ログイン管理が有効になります。

NDS パスワードの設定と変更

ndapPartitionPasswordMgmt 属性を使用し、パーティションに対して NDS パスワードの設定および変更を有効にしたり、無効にしたりします。

ndapPartitionPasswordMgmt 属性値	説明
存在しないか指定されていない	NDAP パスワード管理が有効になります。
0	NDAP パスワード管理が無効になります。
1	NDAP パスワード管理が有効になります。

オブジェクトの NDS 設定を有効 / 無効にする

NDS パスワードを使用したログインおよび検証

ndapLoginMgmt 属性を使用し、NDS ログインを有効 / 無効にしたり、オブジェクト管理を検証したりします。

ndapLoginMgmt 属性値	説明
存在しないか指定されていない	NDAP ログイン管理はパーティションレベルでの設定に依存します。
0	パーティションレベルで NDAP ログイン管理が無効にされている場合、NDAP ログイン管理は無効になります。
1	NDAP ログイン管理は、パーティションレベルでの環境設定に関係なく、有効になります。

NDS パスワードの設定と変更

ndapPasswordMgmt 属性を使用すると、オブジェクトに対する NDS パスワードの設定および変更を有効にしたり、無効にしたりすることができます。

ndapPasswordMgmt 属性値	説明
存在しないか指定されていない	NDAP パスワード管理はパーティションレベルでの設定に依存します。
0	パーティションレベルで NDAP パスワード管理が無効にされている場合、NDAP パスワード管理は無効になります。
1	NDAP パスワード管理は、パーティションレベルでの環境設定に関係なく、有効になります。

注 : 優先度同期ポリシーの作成と管理の詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「Linux の LDAP ツール」および「NetIQ インポート変換エクスポートユーティリティ」を参照してください。

8.4.3 パーティション操作

パーティションを分割すると、NDS 設定はチャイルドパーティションに継承されません。パーティションをマージすると、マージ後のパーティションではペアレントの NDS 設定が保持されます。

8.4.4 大文字と小文字を区別するパスワードを混在ツリーで適用する

eDirectory 8.8 以降のサーバと eDirectory 8.7 以前のサーバが含まれるツリーが存在し、2 台のサーバがパーティションを共有している場合、そのパーティションで NDS ログイン設定を無効にすると、予期しない結果が生じることがあります。8.8 サーバは設定を適用して、レガシークライアントによるディレクトリへのアクセスを防止します。ただし、8.7 サーバは設定を適用しないので、8.7 サーバを通してディレクトリにアクセスすることができます。

8.5 その他の情報

大文字と小文字を区別するパスワードの詳細については、次を参照してください。

- iManager オンラインヘルプ
- 『*NetIQ パスワード管理ガイド 3.3* 』の「ユニバーサルパスワードの配備」セクション (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html)

9 Microsoft Windows Server 2008 パスワードポリシーをサポート

eDirectory の以前のリリースでは、ユーザはデフォルトで Microsoft の複雑性ポリシーや Novell のレガシーな構文が使えました。ただし、NetIQ eDirectory 8.8 SP8 では、Microsoft Windows Server 2008 のパスワードポリシーの複雑性の要求事項に適合するパスワードポリシーをサポートしていますが、この要求事項は以前の Microsoft の複雑性ポリシーの要求事項とは異なります。iManager で、新しい Microsoft Server 2008 パスワードポリシーの構文オプションを使ってポリシーを作成し、ユーザ環境に必要なポリシー設定を行えます。

このセクションでは、次の情報について説明します。

9.1 Windows Server 2008 パスワードポリシーの作成

iManager で、Microsoft Windows Server 2008 の複雑性の要求事項を使ったパスワードポリシーを作成し、eDirectory 環境のユーザに新しいポリシーを割り当てることができます。パスワードポリシー作成の詳細については、『*NetIQ パスワード管理 3.3.2 管理ガイド* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html)』を参照してください。

注

- Microsoft Server 2008 パスワードポリシー構文を使って新しいパスワードポリシーを作成する前に、Novell iManager パスワード管理プラグインの最新バージョンがインストールされていることを確認してください。iManager プラグインモジュールインストールの詳細については、『*NetIQ iManager 2.7 管理ガイド* (https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html)』を参照してください。
- ポリシーの作成や設定に対して、ユニバーサルパスワードと拡張パスワードルールが有効になっていることも確認する必要があります。

9.2 Windows Server 2008 パスワードポリシーの管理

iManager を用いて、Windows Server 2008 のパスワードポリシーの複雑性の要求事項を使ったポリシーを管理できます。詳細については、『*Novell パスワード管理 3.3.2 管理ガイド*』の「パスワードポリシーを使用したパスワードの管理」セクションを参照ください (http://www.netiq.com/documentation/password_management33/pwm_administration/data/ampxjj0.html)。

9.3 その他の情報

eDirectory のパスワードポリシーの詳細については、次を参照してください。

- iManager オンラインヘルプ
- *Novell パスワード管理 3.3.2 管理ガイド* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html)
- *Novell モジュラー認証サービス 3.3.4 管理ガイド* (http://www.netiq.com/documentation/nmas33/admin/data/a20gkue.html)

10 優先度同期

優先度同期は、eDirectory の現在の同期処理を補う NetIQ eDirectory 8.8 の新しい機能です。優先度同期によって、変更された重要なデータ (パスワードなど) を即座に同期することができます。

通常の同期を待てない場合は、優先度同期によって重要なデータを同期できます。優先度同期プロセスは通常の同期プロセスより高速です。優先度同期は、同じパーティションをホストしている 2 台以上の eDirectory 8.8 以降のサーバ間でのみサポートされます。

次の表に、優先度同期機能をサポートするプラットフォームを示します。

機能リスト	Linux	Windows
優先度同期	✓	✓

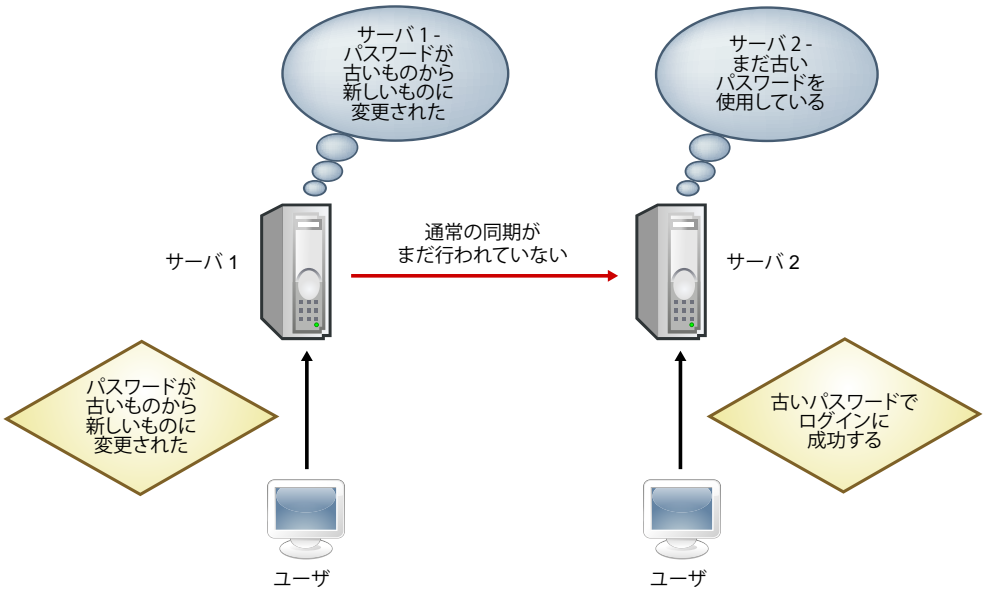
このセクションでは、次の情報について説明します。

- 57 ページのセクション 10.1「優先度同期の必要性」
- 58 ページのセクション 10.2「優先度同期の使用」
- 58 ページのセクション 10.3「その他の情報」

10.1 優先度同期の必要性

通常の同期では時間がかかる場合がありますが、その間、変更されたデータは他のサーバで使用できません。たとえば、ディレクトリと通信している異なるアプリケーションがあるとします。サーバ 1 でパスワードを変更します。通常の同期では、この変更がサーバ 2 と同期されるまでしばらく時間がかかります。このため、ユーザはまだ古いパスワードを使用して、サーバ 2 と通信するアプリケーションを通してディレクトリへの認証を行うことができます。

図 10-1　優先度同期の必要性



大規模な展開においては、オブジェクトの重要なデータが変更されたときに、変更が直ちに同期される必要があります。優先度同期プロセスはこの問題を解決します。

10.2　優先度同期の使用

優先度同期を使用して日付の変更を同期するには、次の操作を行う必要があります。

1. 優先度同期を有効にして、スレッド数を設定します。次に、iMonitor から優先度同期キューサイズを設定します。
2. iManager を使用して重要な属性を指定し、優先度同期ポリシーを定義します。
3. iManager を使用して、優先度同期ポリシーをパーティションに適用します。

10.3　その他の情報

優先度同期の詳細については、次を参照してください。

- *NetIQ eDirectory 8.8 SP8 管理ガイド*
- iManager および iMonitor のオンラインヘルプ

11 データの暗号化

NetIQ eDirectory 8.8 以降では、特定のデータをディスクに保存したり、2 台以上の eDirectory 8.8 サーバ間でデータを転送する場合に、データを暗号化できます。そのため、機密データのセキュリティを強化できます。

次の表に、データの暗号化機能をサポートするプラットフォームを示します。

機能	Linux	Windows
暗号化属性	✓	✓
暗号化レプリケーション	✓	✓

このセクションでは、次の情報について説明します。

- 59 ページのセクション 11.1「属性を暗号化する」
- 60 ページのセクション 11.2「複製を暗号化する」
- 61 ページのセクション 11.3「その他の情報」

11.1 属性を暗号化する

eDirectory 8.8 では、ディスクに保存された重要データを暗号化することができます。暗号化属性はサーバ固有の機能です。

暗号化属性には、クリアテキストチャネルでのアクセスも提供するよう選択した場合以外は、セキュリティ保護されたチャネルでのみアクセスできます。詳細については、「60 ページのセクション 11.1.3「暗号化属性にアクセスする」」を参照してください。

このセクションでは、次の情報を紹介します。

- 59 ページのセクション 11.1.1「暗号化属性の必要性」
- 60 ページのセクション 11.1.2「属性を暗号化する方法」
- 60 ページのセクション 11.1.3「暗号化属性にアクセスする」

暗号化属性機能は、eDirectory 8.8 以降のサーバでのみサポートされています。

11.1.1 暗号化属性の必要性

eDirectory 8.8 以前は、データはクリアテキストでディスクに保存されました。データを保護し、セキュリティ保護されたチャネルでのみデータへのアクセスを提供する必要がありました。

この機能は、銀行顧客のクレジットカード番号のような機密データを保護する必要がある場合に使用できます。

11.1.2 属性を暗号化する方法

属性を暗号化するには、暗号化属性ポリシーを作成および定義し、サーバにポリシーを適用します。暗号化属性は、iManager および LDAP を使用して、作成、定義、適用、および管理することができます。

1 暗号化属性ポリシーを作成および定義します。
   - 1a 暗号化する属性を決定します。
   - 1b 属性の暗号化スキームを決定します。
2 サーバに暗号化属性ポリシーを適用します。

11.1.3 暗号化属性にアクセスする

暗号化属性には、LDAP SSL ポートや HTTPS ポートのように、セキュリティ保護されたチャネル経由でのみアクセスできます。iManager プラグインを用いた平文のチャネルを通して、暗号化された属性へのアクセスを提供できます。詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』を参照してください。

11.2 複製を暗号化する

暗号化複製とは、2 台以上の eDirectory 8.8 サーバ間で転送されるデータを暗号化することです。

暗号化複製は、eDirectory での通常の同期を補うものです。

このセクションでは、次の情報を紹介します。

- 60 ページのセクション 11.2.1「暗号化複製の必要性」
- 60 ページのセクション 11.2.2「暗号化複製を有効にする」

11.2.1 暗号化複製の必要性

eDirectory 8.8 以前は、データは複製中に、クリアテキストでネットワークに転送されました。レプリカが地理的に離れており、インターネット経由で接続されている場合は特に、ネットワーク上で機密データを暗号化して保護する必要がありました。

この機能は、次のような状況で使用できます。

- ディレクトリサーバがWANやインターネットを介して地理的に複数の場所にわたって広がっており、ネットワーク上で重要データを暗号化する必要がある。
- ツリーのパーティションの一部だけを保護する場合は、複製のために暗号化する重要データを保持しているパーティションを選択的に指定できます。
- 重要データを含むパーティションの特定のレプリカ間で暗号化複製が必要な場合。
- 現在のネットワーク環境が安全ではないと思われる場合は、複製中に重要データを保護することもできます。

11.2.2 暗号化複製を有効にする

暗号化複製を有効にするには、iManager を使用します。暗号化複製は、パーティションレベルとレプリカレベルで有効にすることができます。

重要 : 暗号化複製を有効にする前に、複製元と複製先の両方のサーバがデフォルト証明書を持っていることを確認します。名前変更など証明書に変更を加えている場合は、暗号化複製に失敗します。

11.3 その他の情報

eDirectory のデータ暗号化の詳細については、次を参照してください。

- *NetIQ eDirectory 8.8 SP8 管理ガイド*
- iManager および iMonitor のオンラインヘルプ

12 バルクロードのパフォーマンス

NetIQ eDirectory 8.8 には、バルクロードのパフォーマンスを向上させるための拡張機能が用意されています。

バルクロードのパフォーマンスを向上させる方法の詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の次のセクションを参照してください。

- 「eDirectory キャッシュの設定」
- 「LBURP トランザクションサイズの設定」
- 「ICE の非同期要求の数を増やす」
- 「LDAP 書き込みスレッド数の増加」
- 「ICE のスキーマ検証を無効にする」
- 「ACL テンプレートを無効にする」
- 「バックリンカ」
- 「インラインキャッシュを有効 / 無効にする」
- 「LBURP のタイムアウト周期の拡大」
- 「オフラインのバルクロードユーティリティ」

13 iManager ICE プラグインによる設定

NetIQ eDirectory 8.8 以前は、iManager プラグイン内に、Novell インポート / エクスポート変換 (ICE) ユーティリティのコマンドラインオプションの一部に相当するオプションがありませんでした。

次の表に、この機能をサポートするプラットフォームを示します。

機能	Linux	Windows
ICE iManager 拡張機能	✓	✓

eDirectory 8.8 に付属する iManager 2.7 の ICE ウィザードは、次の機能を備えています。

- 不足しているスキーマの追加
- スキーマの比較
- 順序ファイルの生成

13.1 不足しているスキーマの追加

eDirectory 8.8 の iManager には、不足しているスキーマをサーバのスキーマに追加するためのオプションが用意されています。このプロセスには、ソースとターゲットの比較が含まれます。ソーススキーマに追加のスキーマがある場合、このスキーマがターゲットスキーマに追加されます。ソースはファイルまたは LDAP サーバのいずれかになります。ターゲットは LDAP サーバであることが必要です。

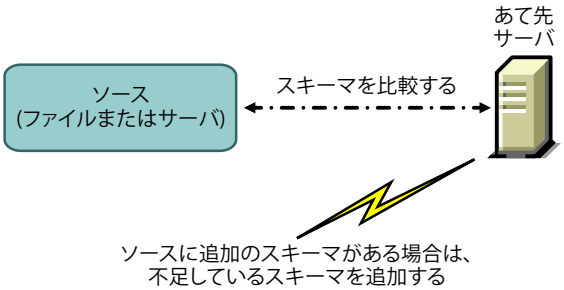
iManager の ICE ウィザードからは、不足しているスキーマを次のオプションを使って追加できます。

- スキーマをファイルから追加する
- スキーマをサーバから追加する

13.1.1 スキーマをファイルから追加する

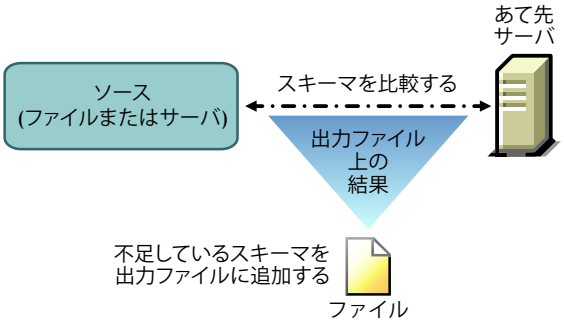
ICE はソースとターゲットのスキーマを比較できます。ソースはファイルまたは LDAP サーバのいずれかで、ターゲットは LDAP サーバです。ソースのスキーマファイルは、LDIF 形式または SCH 形式のいずれかになります。

図 13-1　ファイルにあるスキーマを比較して追加する



あて先サーバにスキーマを追加せずに、スキーマの比較だけをする場合は、*[スキーマを追加しないで比較]* オプションを選択します。この場合、追加のスキーマは追加先サーバに追加されず、処理の最後に表示されるリンクからスキーマの相違点を確認できます。

図 13-2　スキーマを比較して出力ファイルに結果を追加する



詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「NetIQ eDirectory 管理ユーティリティ」を参照してください。

13.1.2　スキーマをサーバから追加する

ソースとターゲットは LDAP サーバです。

あて先サーバにスキーマを追加せずに、スキーマの比較だけをする場合は、*[スキーマを追加しないで比較]* オプションを選択します。この場合、追加のスキーマは追加先サーバに追加されず、処理の最後に表示されるリンクからスキーマの相違点を確認できます。

詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「NetIQ eDirectory 管理ユーティリティ」を参照してください。

13.2　スキーマの比較

iManager で、ソースとターゲット間のスキーマの比較ができます。ソースはファイルでもサーバでもよいですが、ターゲットは LDIF ファイルでないといけません。

iManager はソースとターゲットのスキーマを比較し、結果を出力ファイルに保存します。

iManager の ICE マネージャからは、次のオプションを使ってスキーマを比較できます。

- スキーマファイルを比較する
- サーバとファイルの間でスキーマを比較する

13.2.1 スキーマファイルを比較する

[スキーマファイルの比較] オプションはソースファイルとターゲットファイルのスキーマを比較し、結果を出力ファイルに保存します。不足しているスキーマをターゲットファイルに追加するには、出力ファイルのレコードをターゲットファイルに適用します。

詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「NetIQ eDirectory 管理ユーティリティ」を参照してください。

13.2.2 サーバとファイルの間でスキーマを比較する

*サーバとファイル間のスキーマ比較*オプションで、コピー元サーバとコピー先ファイル間でスキーマの比較ができ、その結果をファイルに出力できます。不足しているスキーマをターゲットファイルに追加するには、出力ファイルのレコードをターゲットファイルに適用します。

詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「NetIQ eDirectory 管理ユーティリティ」を参照してください。

13.3 順序ファイルを生成する

このオプションは、区切りデータファイルからデータをインポートするために、delim ハンドラを使用する順序ファイルを生成します。ウィザードでは、特定のオブジェクトクラスの属性リストを含む順序ファイルを作成できます。

詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「NetIQ eDirectory 管理ユーティリティ」を参照してください。

13.4 その他の情報

この機能の詳細については、次を参照してください。

- *NetIQ eDirectory 8.8 SP8 管理ガイド*
- iMonitor のオンラインヘルプ

14 LDAP ベースのバックアップ

LDAP ベースのバックアップ機能が NetIQ eDirectory 8.8 とともに導入されました。この機能で一度に 1 つのオブジェクトの属性と属性値をバックアップできます。

次の表に、この機能をサポートするプラットフォームを示します。

機能	Linux	Windows
LDAP ベースのバックアップ	✓	✓

この機能を使用すれば、変更が加えられている場合にだけオブジェクトをバックアップする、インクリメンタルバックアップを実行できます。

LDAP ベースのバックアップでは、LDAP 拡張オペレーションを通じて、LDAP Libraries for C によって提供される eDirectory オブジェクトのバックアップ / 復元用インタフェースを使用できます。

LDAP Libraries for C SDK の詳細については、LDAP Libraries for C のマニュアル (http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html) を参照してください。

LDAP を使用して eDirectory オブジェクトのバックアップと復元を行う方法の例については、backup.c のサンプルコード (http://developer.novell.com/ndk/doc/samplecode/cldap_sample/extensions/backup.c.html) を参照してください。

14.1 LDAP ベースのバックアップの必要性

LDAP ベースのバックアップは、現在のバックアップと復元を使用して問題の解決を試みます。

この機能で解決される問題には次のようなものがあります。

- サードパーティのバックアップアプリケーションまたは開発者が使用して、サポートされるすべてのプラットフォームで eDirectory をバックアップできるような、一貫性のあるインタフェースを提供する。
- オブジェクトのインクリメンタルバックアップを行うバックアップソリューションを提供する。

14.2 その他の情報

この機能の詳細については、次を参照してください。

- LDAP Libraries for C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html)
- サンプルコード : backup.c (http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/backup.c.html)

15 LDAP の有効権限リスト取得

LDAP の有効権限リスト取得 API は、NetIQ eDirectory 8.8 SP6 とともに導入されました。

次の表に、この機能をサポートするプラットフォームを示します。

機能	Linux	Windows
LDAP の有効権限リスト取得	✓	✓

この機能によって、任意の属性セットに対応する任意のターゲット DN 上の任意のサブジェクト DN の有効な権限を取得できます。この機能により、LDAP の拡張操作と C のためのライブラリを通して、権限リストを取得するためのインタフェースを提供しています。

LDAP Libraries for C SDK の詳細については、LDAP Libraries for C のマニュアル (http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html) を参照してください。

15.1 LDAP の有効権限リスト取得インタフェースの必要性

LDAP の有効権限リスト取得インタフェースは、有効権限取得 API によって問題の解決を試みます。

この機能で解決される問題には次のようなものがあります。

- 複数属性に関する有効な権利を取得するために、ディレクトリに対して単一の要求のみが必要となります。
- 複数属性に関する有効な権利を取得するために、ディレクトリに対しての往復時間を縮小します。
- 要求やディレクトリへの入力誤りを識別します。

15.2 その他の情報

この機能の詳細については、次を参照してください。

- LDAP Libraries for C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html)。
- サンプルコード : getpriv.c (http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/getpriv.c.html)。

16 eDirectory 8.8 のエラーログを管理する

多くの顧客は、一般的な問題を識別して解決する際に、NetIQ eDirectory のエラーログがあまり役立たないと報告しています。エラーログは、eDirectory のインストール中に自動的に開始されます。

この章では次のセクションについて説明します。

16.1 メッセージの重大度レベル

すべてのメッセージには重大度レベルが添付されており、そのメッセージがどれだけ重要であるかを判断する助けになります。レベルは、重大度が高い順から次のとおりです。

16.1.1 Fatal

致命的エラーのメッセージは、データや機能の損失のような重大な問題を示します。

例 :

- eDirectory サーバが、モジュールのロード中に、NCPEngine や DSLoader などのシステムモジュールのロードに失敗した場合は、致命的エラーが報告され、ログに記録されます。
- eDirectory サーバがセキュアポート 636 でのバインドに失敗すると、致命的エラーが報告され、ログに記録されます。

16.1.2 警告

重大とは限らないメッセージですが、将来的に問題を引き起こす原因になる可能性があります。

例 :

- ツリー内のいずれか 2 台のサーバ間で接続エラーが発生し、結果的にサーバが不正アドレスのキャッシュに追加された。サーバは、不正アドレスのキャッシュをリセットすると、この状態から回復できます。
- LDAP クライアントアプリケーションがバインドを実行し、バインドを解除しないで接続を閉じた場合、LDAP サーバは適切な警告メッセージを記録する必要があります。
- eDirectory サーバがファイル記述子をすべて消費してしきい値に達した場合、結果としてサーバは受信要求を処理して応答することができず、アプリケーションのエラーが発生します。

16.1.3 エラー

無効と見なされる操作が原因で示されるメッセージです。問題の発生を警告するものではありません。

例 :

- クライアントアプリケーションがオブジェクトを追加しようとしたときに、そのオブジェクトの属性定義がスキーマに定義されていない場合、eDirectory サーバは ERR_NO_SUCH_ATTRIBUTE エラーを通知します。
- 無効なパスワードを使用してユーザがログインしようとすると、eDirectory サーバは ERR_FAILED_AUTHENTICATION エラーを通知します。

16.1.4 情報

操作が正常に完了したことや、eDirectory サーバ内のイベントについて説明するメッセージです。

例 :

- モジュールが正常にロードまたはアンロードされたときに、操作に関する情報を示すメッセージを記録しておきたい場合があります。
- データベースキャッシュの設定が変更された場合、設定が正常に保存されたことことを示す情報メッセージをログに記録する必要があります。

16.1.5 デバッグ

開発者がプログラムをデバッグする際に役立つ情報が含まれるメッセージです。

例 :

ダイナミックグループの検索時に、エントリ ID、パーティション ID、およびメンバーの DN とともに、すべてのダイナミックグループメンバーを表示します。この情報は、すべてのメンバーが eDirectory レベルで返されることを確認する際に役立ちます。

16.2 エラーログを設定する

- 75 ページのセクション 16.2.1「Linux」
- 75 ページのセクション 16.2.2「Windows」

16.2.1 Linux

サーバ側メッセージに対してエラーログ設定を行う場合は、/etc/opt/novell/eDirectory/conf/nds.conf 環境設定ファイルで、n4u.server.log-levels パラメータと n4u.server.log-file パラメータを使用できます。

重大度レベルの設定

使用できる重大度レベルは、LogFatal、LogWarn、LogErr、LogInfo、および LogDbg です (重大度が高い順)。重大度のレベルの詳細については、「73 ページのセクション 16.1「メッセージの重大度レベル」」を参照してください。

デフォルトでは重大度レベルは「LogFatal」に設定されます。このため、重大度レベルが致命的エラーであるメッセージのみがログに記録されます。

重大度レベルを設定するには、nds.conf ファイル内で、n4u.server.log-levels パラメータを次のように設定します。

n4u.server.log-levels= *重大度レベル*

次に例を示します。

- 重大度レベルを LogInfo 以上に設定するには、次のように入力します。

  ```
  n4u.server.log-levels=LogInfo
  ```

  この設定を使用すると、重大度レベルが LogInfo 以上 (つまり、LogFatal、LogWarn、および LogErr) のメッセージが、ログファイルに記録されます。
- 重大度レベルを LogWarn 以上に設定するには、次のように入力します。

  ```
  n4u.server.log-levels=LogWarn
  ```

  この設定を使用すると、重大度レベルが LogWarn 以上 (LogFatal) のメッセージが、ログファイルに記録されます。

ログファイル名の指定

メッセージの記録先にするログファイルの場所を指定するには、nds.conf ファイル内で n4u.server.log-file パラメータを使用します。デフォルトでは、ndsd.log ファイルにメッセージが書き込まれます。

たとえば、メッセージを /tmp/edir.log に記録するには、次のように入力します。

```
n4u.server.log-file=/tmp/edir.log
```

システムのログにメッセージを記録するには、次のように n4u.server.log-file パラメータを使用します。

```
n4u.server.log-file=syslog
```

16.2.2 Windows

- 76 ページの 「重大度レベルの設定」
- 76 ページの 「ログファイル名とパスの指定」
- 76 ページの 「ログファイルサイズの指定」

重大度レベルの設定

使用できる重大度レベルは、LogFatal、LogWarn、LogErr、LogInfo、および LogDbg です (重大度が高い順)。重大度のレベルの詳細については、「73 ページのセクション 16.1「メッセージの重大度レベル」」を参照してください。

重大度レベルを設定するには、次の操作を行います。

1. ［*スタート*］>［*設定*］>［*コントロールパネル*］>［*NetIQ eDirectory サービス*］の順にクリックします。
2. ［*サービス*］タブで、［*dhlog.dlm*］を選択します。
3. ［*開始パラメータ*］ボックスにログのレベルを入力します。

   たとえば、ログのレベルを LogErr 以上に設定するには、次のように入力します。

   ```
   LogLevels=LogErr
   ```

4. ［*設定*］をクリックします。
5. ［*ACS 環境設定*］タブで、［*DhostLogger*］のプラス記号をクリックします。

   設定した値で LogLevel パラメータが更新されます。

ログファイル名とパスの指定

1. ［*スタート*］>［*設定*］>［*コントロールパネル*］>［*NetIQ eDirectory サービス*］の順にクリックします。
2. ［*サービス*］タブで、［*dhlog.dlm*］を選択します。
3. ［*開始パラメータ*］に、ログファイルのパスを次のように入力します。

   ```
   LogFile=file_path
   ```

   たとえば、ログファイルのパスを /tmp/Err.log に設定するには、［開始パラメータ］に次のように入力します。

   ```
   LogFile=/tmp/Err.log
   ```

4. ［*設定*］をクリックします。
5. ［*ACS 環境設定*］タブで、［*DhostLogger*］のプラス記号をクリックします。

   設定した値で LogFile パラメータが更新されます。

ログファイルサイズの指定

1. ［*スタート*］>［*設定*］>［*コントロールパネル*］>［*NetIQ eDirectory サービス*］の順にクリックします。
2. ［*サービス*］タブで、［*dhlog.dlm*］を選択します。
3. ［*開始パラメータ*］に、ログファイルのパスを次のように入力します。

   ```
   LogSize=size
   ```

   デフォルトのファイルサイズは 1MB です。

4. ［*設定*］をクリックします。
5. ［*ACS 環境設定*］タブで、［*DhostLogger*］のプラス記号をクリックします。

   設定した値で LogSize パラメータが更新されます。

16.3 DSTrace メッセージ

スレッド ID、接続 ID、およびメッセージの重大度に基づいて、トレースメッセージをフィルタすることができます。

メッセージにフィルタを指定すると、フィルタに一致するメッセージだけが画面に表示されます。FILE が ON に設定されている場合、タグが有効になっている他のメッセージはすべて ndstrace.log に記録されます。

一度に適用できるのは 1 つのフィルタだけです。フィルタは、DSTrace のセッションごとに指定する必要があります。

デフォルトでは、重大度レベルは INFO に設定されます。これは、重大度レベルが INFO 以上のメッセージはすべて表示されることを意味します。重大度レベルは、svty タグを有効にすると表示できます。

iMonitor を使用しても、トレースメッセージをフィルタすることができます。詳細については、「79 ページのセクション 16.4「iMonitor メッセージのフィルタ」」を参照してください。

16.3.1 Linux

次の手順を完了してトレースメッセージをフィルタします。

1 次のコマンドでフィルタを有効にします。

```
ndstrace tag filter_value
```

フィルタを無効にするには、次のコマンドを入力します。

```
ndstrace tag
```

フィルタを有効にする場合の例 :

- スレッド ID が 35 の場合にフィルタを有効にするには、次のように入力します。

  ```
  ndstrace thrd 35
  ```

- 重大度レベルが致命的エラーの場合にフィルタを有効にするには、次のように入力します。

  ```
  ndstrace svty fatal
  ```

  重大度レベルとして、FATAL、WARN、ERR、INFO、および DEBUG を指定できます。

- 接続 ID が 21 の場合にフィルタを有効にするには、次のように入力します。

  ```
  ndstrace conn 21
  ```

フィルタを無効にする場合の例 :

- スレッド ID に基づいてフィルタを無効にするには、次のように入力します。

  ```
  ndstrace thrd
  ```

- 接続 ID に基づいてフィルタを無効にするには、次のように入力します。

  ```
  ndstrace conn
  ```

- 重大度に基づいてフィルタを無効にするには、次のように入力します。

  ```
  ndstrace svty
  ```

図 16-1　フィルタを適用したトレースメッセージのサンプル画面

```
NCPEng  : INFO    : NCP Reply to tcp:164.99.148.243, conn 14, task 0, seq 241, size 121, flags 0, ncperr
0.
NCPEng  : INFO    : NCP Request from tcp:164.99.148.243, conn 22, task 0, seq 120, size 32, err 0.
NCPEng  : INFO    : NCP: 104 (1) - Novell eDirectory Services (Novell eDirectory Ping).
NCPEng  : INFO    : NCP Reply to tcp:164.99.148.243, conn 22, task 0, seq 120, size 54, flags 0, ncperr
0.
NCPEng  : INFO    : NCP Request from tcp:164.99.148.243, conn 22, task 0, seq 121, size 248, err 0.
NCPEng  : INFO    : NCP: 104 (2) - Novell eDirectory Services (Fragged Request).
Agent   : DEBUG   : Calling DSAResolveName conn:22 for client .[Public].
Reslv   : DEBUG   : ConvertDNToID: dn=\T=WIN-0510\O=novell\CN=OSG-NTS-2-NDS, cts=4281a5dc:01:001
NCPCli  : DEBUG   : DCCreateContext context 3464002c moduleHandle 60000000 C:\Novell\NDS\ds.dlm, idHandle
00000000
Reslv   : DEBUG   : Connect to tcp:164.99.148.219:524 succeeded
DRL     : INFO    : Primary object is ID_INVALID
NCPCli  : DEBUG   : DCFreeContext context 3464002c idHandle 00000000, connHandle 00001b00, C:\Novell\NDS
\ds.dlm
NCPEng  : INFO    : NCP Reply to tcp:164.99.148.243, conn 22, task 0, seq 121, size 74, flags 0, ncperr
0.
NCPEng  : INFO    : NCP Request from tcp:164.99.148.243, conn 14, task 0, seq 242, size 32, err 0.
NCPEng  : INFO    : NCP: 104 (1) - Novell eDirectory Services (Novell eDirectory Ping).
NCPEng  : INFO    : NCP Reply to tcp:164.99.148.243, conn 14, task 0, seq 242, size 46, flags 0, ncperr
0.
NCPEng  : INFO    : NCP Request from tcp:164.99.148.243, conn 14, task 0, seq 243, size 196, err 0.
NCPEng  : INFO    : NCP: 104 (2) - Novell eDirectory Services (Fragged Request).
Agent   : DEBUG   : Calling DSAStartUpdateReplica conn:14 for client .OSG-NTS-2-NDS.novell.WIN-0510.
Reslv   : DEBUG   : ConvertDNToID: dn=\T=WIN-0510, cts=4281a5dc:01:001
SyncI   : INFO    :  ** SYNCHRONIZATION DISABLED! .WIN-0510., .OSG-NTS-2-NDS.novell.WIN-0510.
Agent   : DEBUG   : DSAStartUpdateReplica failed, synchronization disabled (-701).
NCPEng  : INFO    : NCP Reply to tcp:164.99.148.243, conn 14, task 0, seq 243, size 32, flags 0, ncperr
0.
```

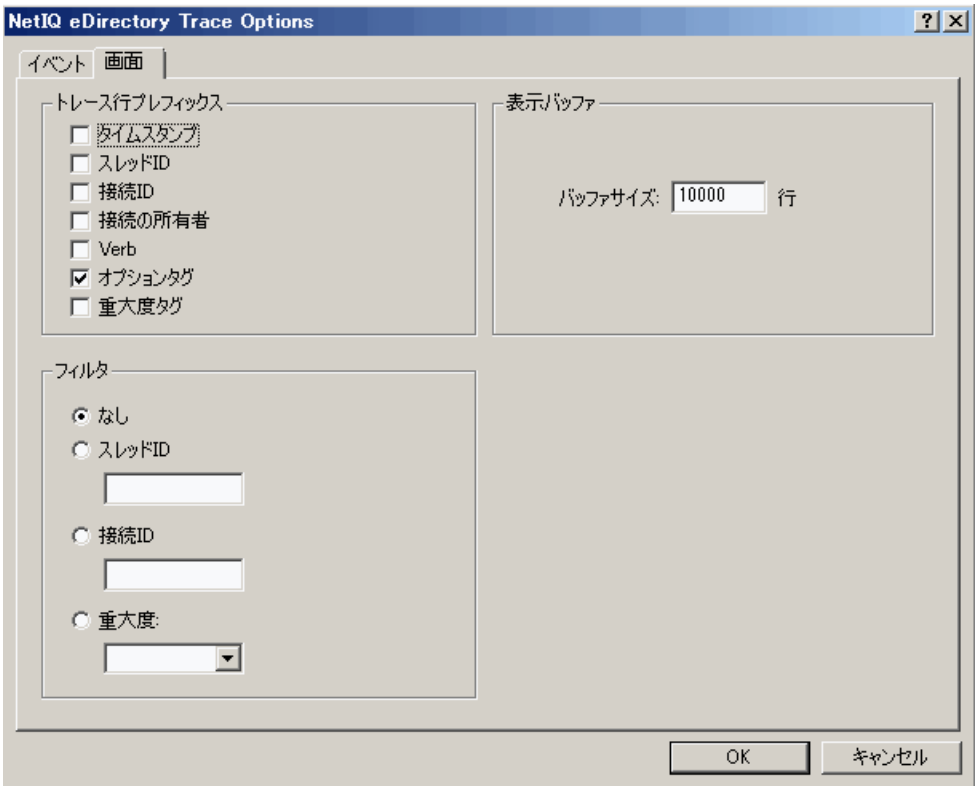
16.3.2　Windows

次の手順を完了してトレースメッセージをフィルタします。

1. *［スタート］*>*［コントロールパネル］*>*［NetIQ eDirectory サービス］*の順にクリックします。
2. *［サービス］*タブで、*［dstrace.dlm］*を選択します。
3. ［トレース］ウィンドウで、*［編集］*>*［オプション］*の順にクリックします。

   ［NetIQ eDirectory トレースオプション］ダイアログボックスが表示されます。

図 16-2　Windows でのトレースオプション画面



4 *［画面］*タブをクリックします。

5 *［フィルタ］*グループからフィルタオプションを選択し、フィルタの値を入力します。

次の項目に基づいてメッセージをフィルタできます。

- スレッド ID
- 接続 ID
- 重大度

いずれかのフィルタを選択する前に、*［トレース行プレフィックス］*でそのフィルタが有効にされていることを確認します。

*［なし］*を選択するか、フィルタオプションの選択を解除すると、フィルタを無効にすることもできます。

注 : フィルタオプションとして*スレッド ID* または*接続 ID* を選択し、存在しない値を入力した場合、メッセージは画面に表示されません。ただし、他のメッセージはすべて ndstrace.log ファイルに記録されます。

16.4　iMonitor メッセージのフィルタ

接続 ID、スレッド ID、またはエラー番号に基づいて、iMonitor のトレースメッセージをフィルタできます。

接続 ID やスレッド ID に基づいてフィルタを行う場合は、［トレースの環境設定］タブでこれらを有効にしたことを確認します。

詳細については、iMonitor のオンラインヘルプを参照してください。

16.5 SAL メッセージのフィルタ

SAL は、エラーに関する包括的な情報を、オンデマンドでログに記録するために拡張されてきました。デバッグビルドでは、引数を使用してファンクションコールをトレースすることができます。

16.5.1 重大度レベルの設定

SAL_LogLevels パラメータを使用すると、SAL メッセージの重大度レベルを設定できます。SAL_LogLevels は、必要なログレベルから構成されたコンマ区切りのリストです。

下の表では、ログレベルについて説明します。

表 16-1 *SAL メッセージのフィルタパラメータ*

パラメータ名	説明
LogCrit	致命的なメッセージ。 デフォルトでは、このレベルは有効になっています。致命的エラーが記録されると、システムはシャットダウンされます。
LogErr	すべてのエラーメッセージ。 システムは機能し続けますが、結果は予測できません。
LogWarn	警告メッセージ。 発生する可能性のあるエラーの存在について通知される警告です。
LogInfo	情報メッセージ。
LogDbg	開発時のデバッグ用に使用されるデバッグメッセージです。 これらのメッセージは、バイナリサイズを削減するため、コンパイル時にリリースビルドから削除されます。
LogCall	ファンクションコールをトレースします。これらはデバッグメッセージのサブセットです。
LogAll	LogCall 以外のメッセージをすべて有効にします。

特定のログレベルの先頭に「-」を指定すると、そのレベルが無効になります。

例

LogInfo と LogDbg を除いたすべてのログレベルに基づいてフィルタを行う場合は、次の手順を完了させます。

Linux

1. ndsd を停止します。
2. 次のコマンドを入力します。

```
export SAL_LogLevels=LogAll,-LogInfo,-LogDbg
```

3 ndsd を起動します。

Windows

1 DHost をシャットダウンします。

2 次のコマンドをコマンドプロンプトの指示にしたがって入力します。

```
set SAL_LogLevels=LogAll,-LogInfo,-LogDbg
c:\novell\nds>dhost.exe /datadir=c:\novell\nds\DIBFiles\
```

3 DHost を再起動します。

16.5.2 ログファイルパスを設定する

SAL_LogFile 環境変数を使用すると、ログファイルの場所を指定できます。場所として指定できるのは、有効なパスの有効なファイル名、または次のいずれかです。

- コンソール : すべてのメッセージはコンソールに出力されます。
- syslog: Linux では、メッセージは syslog に記録されます。Windows では、メッセージは syslog という名前のファイルに記録されます。これはログのデフォルトの動作です。

  致命的なエラーはすべて、明確に無効にされている場合以外は、常に syslog に記録されます。

17 オフラインバルクロードユーティリティ：ldif2dib

ldif2dib は、NetIQ eDirectory 8.8 とともに導入された新しいユーティリティで、LDIF ファイルから eDirectory データベースへデータをバルクロードします。オフラインユーティリティで、他のオンラインツールと比べるとより高速にバルクロードできます。

次の一覧表は、ldif2dib をサポートするプラットフォームです。

機能	Linux	Windows
ldif2dib	✓	✓

17.1 ldif2dib の必要性

LDIF ファイルから入力してユーザの大きなデータベースを作成する場合は、dif2dib ユーティリティが必要です。ice や ldapmodify などのオンラインツールはオンラインでのバルクロード時にスキーマチェックやプロトコル変換やアクセスコントロールチェックなどのオーバーヘッド処理を伴うため、この点においては ldif2dib より処理が遅いです。ldif2dib は、ユーザの大きなデータベースを構築し、初期のダウンタイムが問題とならないときは、高速な動作可能時間を実現します。

17.2 その他の情報

詳細については、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「オフラインバルクロードユーティリティ」を参照してください。

18 SMS による eDirectory バックアップ

Novell Storage Management Services(SMS) は、バックアップアプリケーションが完全なバックアップソリューションを提供するために使用する API フレームワークです。SMS は、2 つの主要なコンポーネントで構成されています。

- Storage Management Data Requester (SMDR)
- ターゲットサービスエージェント (TSA:Target Service Agent)

eDirectory 用の TSA(tsands) は、eDirectory のターゲットにサービスを提供し、ディレクトリツリーに Novell Storage Management Services API を実装します。アプリケーションは SMS API のトップに構築し、完結したバックアップサービスが提供されます。

NDS 対応の TSA は、Linux でサポートされます。

19 LDAP 監査

監査機能は、ディレクトリを評価する際に、管理者が興味を持つ主要な機能の 1 つです。eDirectory のイベントメカニズムが、eDirectory の監査機能を促進しています。多くのアプリケーションがディレクトリにアクセスするために LDAP プロトコルを導入しているので、LDAP の処理を監査する必要性が大いに広まっています。

この章では次のセクションについて説明します。

19.1 LDAP 監査の必要性

このイベントメカニズムは、LDAP 情報を十分に提供できない既存の eDirectory LDAP サーバでは明らかに不足していました。NDS イベントシステムは、すべての eDirectory 操作に対するイベントを生成していましたが、アプリケーションが LDAP サーバを監査するためには、この情報のほとんどが不十分または不適切でした。プロトコルやバインドの詳細、ネットワークアドレス、認証方法、認証タイプ、LDAP 検索、トランザクションの詳細などの情報が LDAP サーバの監査に不可欠ですが、NDIS イベントでは利用できませんでした。アプリケーション開発者にとって、従来のイベントをベースにしたアプリケーションで監査機能を実現することは困難でした。

LDAP は eDirectory の重要なインタフェースで、アプリケーションに対して eDirectory LDAP サーバの監査機能を提供しています。NetIQ eDirectory 8.8 SP3 バージョンで、新 LDAP イベントサブシステムが導入されています。このサブシステムは、アプリケーションが LDAP サーバを監査するのに関連のあるすべての情報を含む LDAP 特有のイベントを生成します。これは LDAP 監査として知られています。

19.2 LDAP 監査の利用

LDAP 監査は、アプリケーションが追加、変更、検索などの LDAP の処理を監視 / 監査し、接続情報や LDAP 処理の際にサーバが接続するクライアント IP、メッセージ ID、処理に対する結果コードなどの有用な情報を LDAP サーバから取り込みます。

LDAP 監査は、NDK LDAP Libraries for C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html) により実行されますが、新 LDAP の構造とイベントを通して監査機能をクライアント側のインタフェースとして提供します。

19.3 その他の情報

LDAP 監査イベントについては、次を参照してください。

- 『*NetIQ eDirectory 8.8 SP8 管理ガイド*』の「NetIQ eDirectory のための LDAP サービスの設定」。
- NDK: LDAP ツール (http://developer.novell.com/documentation/cldap/ltoolenu/data/hevgtl7k.html) に関しては、LDAP Libraries for C のマニュアルを参照してください。

LDAP のツール情報に関しては、『LDAP Libraries for C (http://developer.novell.com/ndk/doc/cldap/index.html?ldaplibc/data/a6eup29.html)』を参照してください。

20 XDASv2 を使った監査

XDASv2 の仕様には、監査イベントの標準的な分類が記載されています。グローバルな分散システムレベルにおける一般イベントのセットを定義します。XDASv2 には、一般的なポータブルの監査レコードフォーマットが含まれており、分散システムレベルでの複数のコンポーネントからの監査情報を、簡単にまとめたり、分析したりできます。XDASv2 イベントは、標準または既存のイベント ID セットの拡張に対応した階層型の表記システム内でカプセル化されます。

eDirectory 8.8 SP8 で、XDASv2 エージェントが syslog サーバと通信できない場合は、エージェントが記録した監査イベントをローカルでキャッシュし、監査データの損失を防ぐ設定ができます。エージェントは、その後で監査イベントの再送を試み、通信機能が回復するまでこれを継続します。XDAS のイベントキャッシングはデフォルトでは無効となっています。

詳細については、『*NetIQ XDASv2 管理ガイド*』を参照してください。

21 その他

この章では、NetIQ eDirectory 8.8 に備わる他の新機能について説明します。

21.1 iMonitor キャッシュダンプレポーティング

iMonitor の Change Cache ページには、一時期に 1 つのオブジェクトのみが表示されますが、そのことが全体のキャッシュ変更の確認を困難にしています。eDirectory 8.8 SP8 によって、新しい Change Cache ダンプレポートが、iMonitor とともにデフォルトレポートとして追加されました。このレポートにより、キャッシュ変更の状態を一覧できます。管理者は、このレポートにより特定のサーバで起きている変化を把握できます。

Change Cache ダンプレポートを実行すると、iMonitor がキャッシュにあるすべてのオブジェクトやそのサーバ間で同期を取るのに必要な属性および属性値に関しての XML ダンプも生成します。

iMonitor レポートについての詳細は、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』を参照してください。

21.2 iManager による Microsoft の大きな整数構文のサポート

eDirectory 8.8 SP8 は Microsoft Large Integer 構文をサポートする新しい構文を提供しています。1970 未満や 2038 を超える大きい整数の値または日付を保存するのに、この構文を使用できます。LDAP または iManager を使って、この構文を使った属性を作成し管理できます。

注 : eDirectory は、今もなお既存の構文を使用し、32 ビットデータを内部のタイムスタンプに用いています。

21.3 セキュリティオブジェクトのキャッシュ

セキュリティコンテナは、ツリーに最初のサーバがインストールされたときにルートパーティションから分かれて作成され、グローバルデータ、セキュリティポリシー、キーなどの情報を保持します。

ユニバーサルパスワードが導入された後は、ユーザが NMAS を介して eDirectory にログインするたびに、NMAS がセキュリティコンテナ内の情報にアクセスしてログインを認証していました。セキュリティコンテナがあるパーティションがローカルに存在しない場合、NMAS はそのパーティションを持つサーバにアクセスしていました。このとき、NMAS 認証のパフォーマンスに悪影響が及んでいました。セキュリティコンテナがあるパーティションを持つサーバに WAN リンク経由でアクセスする必要がある状況では、この問題はさらに悪化しました。

この状況を解決するため、eDirectory 8.8 では、セキュリティコンテナのデータはローカルサーバ上にキャッシュされます。このため NMAS は、ユーザがログインするたびに、異なるコンピュータに置かれているセキュリティコンテナにアクセスする必要がありません。セキュリティコンテナには、ローカルで容易にアクセスすることができます。これによってパフォーマンスが向上します。セキュリティコンテナがあるパーティションをローカルサーバに追加することでパフォーマンスは向上しますが、サーバの数が多すぎる場合はそうはいかない可能性があります。

セキュリティコンテナ内の実際のデータが、セキュリティコンテナのパーティションを含むサーバ上で変更された場合、ローカルキャッシュはバックリンカと呼ばれるバックグラウンドプロセスによってリフレッシュされます。デフォルトでは、バックリンカが 13 時間ごとに実行され、変更されたデータがリモートサーバから取得されます。データの即時同期が必要な場合は、iMonitor、Linux 上の ndstrace、または Windows 上の ndscons を用いてバックリンカをローカルサーバにスケジュールできます。詳細については、iMonitor のオンラインヘルプまたは ndstrace のマニュアルページを参照してください。

セキュリティオブジェクトのキャッシュ機能は、デフォルトで有効になっています。バックリンカによってデータをキャッシュしない場合は、NCP サーバオブジェクトから CachedAttrsOnExtRef を削除します。

21.4 サブツリー検索のパフォーマンスの向上

eDirectory では、深い入れ子構造を持つ大規模なツリーに対してサブツリー検索を行う場合、パフォーマンスは検索のベース DN に関係なくフラットな状態であり続けます。この問題は、AncestorID 属性を使用することにより解決されています。AncestorID 属性はすべての祖先の entryID のリストであり、各エントリに関連付けられています。この AncestorID 属性は、サブツリー検索の間に内部で使用されます。したがって、AncestorID は検索のスコープを制限します。

この属性は、DIB のエントリを追加している間やすべてのエントリをアップグレードした後に表示されます。また､サブツリーが移動されると、サブツリーのすべてのエントリに対する属性が再表示されます。ただし、アップグレードやサブツリーの移動を行った後で属性を作成する際は、サブツリー検索時に AncestorID 属性は使用されません。したがって、サブツリーのパフォーマンスは eDirectory 8.8 以前のサブツリー検索のものと同様になります。

AncestorID がアップグレード後に更新されているかどうかを確認するには。

AncestorID が一度作成されると、NDS オブジェクトのアップグレードバージョンが 6 以上に変更されます。エージェント情報の *DIB 履歴*セクションで iMonitor を使用して、このバージョンを表示できます。

AncestorID がサブツリーの移動操作の後に更新されているかどうかを確認するには。

AncestorID が作成されている間、擬似サーバオブジェクトの属性 UpdateInProgress は、サブツリーのパーティションルートのエントリ ID のリストを保持します。AncestorID が一度表示されると、擬似サーバに属性は存在しなくなります。

AncestorID 属性が無効の場合、DSRepair は AncestorID 属性を更新します。

21.5 localhost の変更点

eDirectory 8.8 サーバはループバックアドレスを監視しません。localhost を使用するユーティリティは、ホスト名または IP アドレス解決に変更する必要があります。

サードパーティ製のツールやユーティリティが localhost を使用して解決している場合は、localhost アドレスではなく、ホスト名または IP アドレスを使用して解決する必要があります。

21.6 Solaris 上での 256 個のファイルハンドラ

以前は、Solaris 2.*x* の stdio ストリーム実装で使用できるファイル記述子は、最大で 256 個だけでした。これは、eDirectory が正常に機能するには不十分です。この限界を乗り越えるために、eDirectory 8.8 のスタブライブラリを提供します。

21.7 Solaris 上でのメモリマネージャ

Solaris 上の eDirectory は、以前のリリースではメモリマネージャとして、サードパーティ製品の Geodesic* を使用していました。このリリースの eDirectory 8.8 には、サードパーティ製のメモリ割り当てプログラムは含まれていませんが、ネイティブのメモリマネージャを利用しています。

eDirectory のパフォーマンスには、これによる影響はありません。ほとんどの場合、パフォーマンスは向上しているか、サードパーティ製のメモリ割り当てプログラムと同レベルにとどまっています。

21.8 ネストされたグループ

eDirectory 8.8 SP2 では、グループのグルーピング機能をサポートしますが、これによりグループの構造化がより可能になります。この機能はネストされたグループと呼ばれます。現在ネストはスタティックグループに許可されています。

ネストは最大 200 までの複数レベルが利用できます。

ネストされたグループについては、『*NetIQ eDirectory 8.8 SP8 管理ガイド*』を参照してください。