

Novell eDirectory

8.8

www.novell.com

新機能ガイド

2005年9月15日

N

Novell®

法令通知

米国 Novell, Inc. およびノベル株式会社は、本書の内容または本書を使用した結果について、いかなる保証、表明または約束も行っておりません。また、本書の商品性、および特定の用途への適合性について、いかなる黙示的保証も否認し、排除します。また、本書の内容は予告なく変更されることがあります。

米国 Novell, Inc. およびノベル株式会社は、すべてのノベル製ソフトウェアについて、いかなる保証、表明または約束も行っておりません。また、ノベル製ソフトウェアの商品性、および特定の用途への適合性について、いかなる黙示的保証も否認し、排除します。米国 Novell, Inc. およびノベル株式会社は、ノベル製ソフトウェアの内容を変更する権利を常に留保します。

本契約の締結に基づいて提供されるすべての製品または技術情報には、米国の輸出管理規定およびその他の国の貿易関連法規が適用されます。お客様は、取引対象製品の輸出 § 再輸出または輸入に関し § 国内外の輸出管理規定に従うこと、および必要な許可、または分類に従うものとし。お客様は、現在の米国の輸出除外リストに掲載されている企業、および米国の輸出管理規定で指定された輸出禁止国またはテロリスト国に本製品を輸出または再輸出しないものとし。お客様は、取引対象製品を、禁止されている核兵器、ミサイル、または生物化学兵器を最終目的として使用しないものとし。Novell ソフトウェアを国外へ輸送する詳細については、www.novell.com/info/exports/ を参照してください。弊社は、お客様が必要な輸出承認を取得しなかったことに対し如何なる責任も負わないものとし。

Copyright © 2005, Novell, Inc. All rights reserved. 本書の一部または全体を無断で複写・転載することは、その形態を問わず禁じます。

本書に記載された製品で使用されている技術に関連する知的所有権は、弊社に帰属します。これらの知的所有権は、<http://www.novell.com/company/legal/patents/> に記載されている 1 つ以上の米国特許、および米国ならびにその他の国における 1 つ以上の特許または出願中の特許を含む場合があります。

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.

www.novell.com

Novell eDirectory 8.8 新機能ガイド
2005 年 9 月 15 日

オンラインドキュメント：本製品およびその他の Novell 製品のオンラインマニュアルにアクセスする場合や、アップデート版を取得する場合は、<http://www.novell.com/documentation/japanese> を参照してください。

Novell の商標

Client32 は、米国 Novell, Inc. の商標です。

eDirectory は、米国 Novell, Inc. の商標です。

NetWare は、米国 Novell, Inc. の米国ならびに他の国々における登録商標です。

NetWare Core Protocol および NCP は、米国 Novell, Inc. の商標です。

NMAS は、米国 Novell, Inc. の商標です。

Novell は、米国 Novell, Inc. の米国ならびに他の国々における登録商標です。

Novell Client は、米国 Novell, Inc. の商標です。

Novell Directory Services および NDS は、米国 Novell, Inc. の米国ならびに他の国々における登録商標です。

Ximiam は、米国 Novell, Inc. の米国ならびに他の国々における登録商標です。

ZENworks は、米国 Novell, Inc. の米国ならびに他の国々における登録商標です。

Third-Party Materials

サードパーティ各社とその製品の商標は、所有者であるそれぞれの会社に所属します。

この製品には、OpenSSL プロジェクトが開発した OpenSSL Toolkit (<http://www.openssl.org>) で使用するソフトウェアが含まれています。

目次

このガイドについて	9
1 インストールとアップグレードの拡張機能	11
eDirectory 8.8 インストール用の複数のパッケージ形式	12
自動展開	12
アップグレードの配布	12
容易な展開	13
YaST を使用した eDirectory のインストールと設定	14
任意の場所に eDirectory 8.8 をインストールする	14
アプリケーションファイルに任意の場所を指定する	14
データファイルに任意の場所を指定する	15
環境設定ファイルに任意の場所を指定する	15
ルート以外のユーザによるインストール	16
ルート以外のユーザ	16
管理者以外のユーザ	16
標準の準拠	16
FHS の準拠	16
LSB の準拠	17
サーバのヘルスチェック	18
ヘルスチェックの必要性	18
サーバが正常であることの確認基準	18
ヘルスチェックを実行する	18
ヘルスチェックのタイプ	19
状態のカテゴリ	20
ログファイル	22
SecretStore と eDirectory との統合	23
詳細情報	24
2 複数のインスタンス	25
複数インスタンスの必要性	26
複数インスタンスを展開する場合のシナリオ	26
複数インスタンスの使用	26
セットアップの計画	27
複数インスタンスを設定する	27
複数インスタンスを管理する	28
ndsmanage ユーティリティ	28
特定のインスタンスの識別	31
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	31
複数インスタンスのシナリオ	32
セットアップの計画	32
インスタンスの設定	32
インスタンスに対するユーティリティの呼び出し	32
インスタンスの表示	33
詳細情報	33

3	SASL-GSSAPI を使用した eDirectory に対する認証	35
	概念	35
	Kerberos について	35
	SASL について	36
	GSSAPI について	36
	eDirectory における GSSAPI の動作	36
	GSSAPI の設定	37
	LDAP での GSSAPI の使用方法	38
	よく使用される用語	38
4	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	39
	大文字と小文字を区別するパスワードの必要性	40
	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	40
	前提条件	40
	パスワードの大文字と小文字が区別されるようにする	41
	大文字と小文字を区別するパスワードの管理	41
	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	41
	大文字と小文字を区別するパスワードへの移行	42
	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	43
	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	43
	NDS ログイン設定の管理	43
	パーティション操作	47
	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	47
	詳細情報	47
5	優先度同期	49
	優先度同期の必要性	49
	優先度同期の使用	50
	詳細情報	50
6	データの暗号化	51
	属性を暗号化する	51
	暗号化属性の必要性	51
	属性を暗号化する方法	52
	暗号化属性にアクセスする	52
	複製を暗号化する	52
	暗号化複製の必要性	52
	暗号化複製を有効にする	53
	詳細情報	53
7	バルクロードのパフォーマンス	55
8	iManager ICE プラグインによる設定	57
	不足しているスキーマの追加	57
	スキーマをファイルから追加する	58
	スキーマをサーバから追加する	58
	スキーマの比較	59
	スキーマファイルを比較する	59
	サーバとファイルの間でスキーマを比較する	59
	順序ファイルを生成する	59
9	LDAP ベースのバックアップ	61
	LDAP ベースのバックアップの必要性	61
	詳細情報	62

10 eDirectory 8.8 のエラーログを管理する	63
メッセージの重大度レベル	63
致命的エラー	63
警告	64
Error	64
情報	64
デバッグ	64
エラーログを設定する	65
Linux、UNIX の場合	65
Windows の場合	66
NetWare の場合	67
DSTrace メッセージ	69
NetWare、Linux、および UNIX	69
Windows の場合	70
iMonitor メッセージのフィルタ	72
SAL メッセージのフィルタ	72
重大度レベルの設定	72
ログファイルパスを設定する	73
11 その他	75
セキュリティオブジェクトのキャッシュ	75
サブツリー検索のパフォーマンスの向上	76
localhost の変更点	76
Solaris の 256 個のファイルハンドラ	76
Solaris のメモリマネージャ	76

このガイドについて

Novell® eDirectory™ 8.8 へようこそ。このガイドでは、本製品の機能を紹介します。

eDirectory 8.8 は、ディレクトリ市場での eDirectory の主導的地位をさらに強化する新機能と拡張機能を多数備えています。

このガイドでは次のことについて紹介します。

- ◆ 11 ページの第 1 章「インストールとアップグレードの拡張機能」
- ◆ 25 ページの第 2 章「複数のインスタンス」
- ◆ 35 ページの第 3 章「SASL-GSSAPI を使用した eDirectory に対する認証」
- ◆ 39 ページの第 4 章「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」
- ◆ 49 ページの第 5 章「優先度同期」
- ◆ 51 ページの第 6 章「データの暗号化」
- ◆ 55 ページの第 7 章「バルクロードのパフォーマンス」
- ◆ 57 ページの第 8 章「iManager ICE プラグインによる設定」
- ◆ 61 ページの第 9 章「LDAP ベースのバックアップ」
- ◆ 63 ページの第 10 章「eDirectory 8.8 のエラーログを管理する」

補足マニュアル

eDirectory 8.8 の詳細については、次を参照してください。

- ◆ Novell eDirectory 8.8 インストールガイド
- ◆ Novell eDirectory 8.8 管理ガイド
- ◆ Novell eDirectory 8.8 トラブルシューティングガイド

これらのガイドは、[Novell eDirectory 8.8 documentation の Web サイト](http://www.novell.com/documentation/edir88/index.html) (<http://www.novell.com/documentation/edir88/index.html>) で入手できます。

eDirectory 管理ユーティリティに関する情報については、『[Novell iManager 2.5 管理ガイド](http://www.novell.com/documentation/imanager25/index.html)』 (<http://www.novell.com/documentation/imanager25/index.html>) を参照してください。

マニュアルの更新

このガイドの最新版については、『[Novell eDirectory 8.8 新機能ガイド](http://www.novell.com/documentation/edir88/edir88new/data/front.html)』 (<http://www.novell.com/documentation/edir88/edir88new/data/front.html>) を参照してください。

マニュアルの表記規則

このマニュアルでは、不等号 (>) を使用して、操作手順の動作、およびクロスリファレンスパス内の項目を区切ります。

「®」、「™」などの商標記号は、Novell の商標を示します。アスタリスク (*) はサードパーティの商標を示します。

パス名に円記号 (\) が使用されるプラットフォームやスラッシュ (/) が使用されるプラットフォームがありますが、パス名は円記号で表記されています。Linux* や UNIX* など、スラッシュを必要とするプラットフォームでは、ソフトウェアの必要に応じてスラッシュを使用してください。

1

インストールとアップグレードの拡張機能

この章では、Novell® 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	NetWare の場合	Linux の場合	UNIX	Windows の場合
eDirectory 8.8 インストール用の複数のパッケージ形式	✗	✓	✓	✗
Ximian® ZENworks® Linux Management 2.2 による自動展開	✗	✓	✗	✗
YaST を使用した eDirectory のインストールと設定	✗	✓	✗	✗
インストール場所を指定した、アプリケーションファイルのインストール	✗	✓	✓	✓
インストール場所を指定した、データファイルのインストール	✗	✓	✓	✓
インストール場所を指定した、環境設定ファイルのインストール	✗	✓	✓	✗
ルート以外へのインストール	✗	✓	✓	✗
FHS への準拠	✗	✓	✓	✗
LSB への準拠	✗	✓	✗	✗
サーバのヘルスチェック	✓	✓	✓	✓
SecretStore の統合	✓	✓	✓	✓

この章では次の機能について説明します。

- ◆ [eDirectory 8.8 インストール用の複数のパッケージ形式 \(12 ページ\)](#)
- ◆ [自動展開 \(12 ページ\)](#)
- ◆ [YaST を使用した eDirectory のインストールと設定 \(14 ページ\)](#)
- ◆ [任意の場所に eDirectory 8.8 をインストールする \(14 ページ\)](#)
- ◆ [ルート以外のユーザによるインストール \(16 ページ\)](#)
- ◆ [標準の準拠 \(16 ページ\)](#)
- ◆ [サーバのヘルスチェック \(18 ページ\)](#)
- ◆ [SecretStore と eDirectory との統合 \(23 ページ\)](#)

eDirectory 8.8 インストール用の複数のパッケージ形式

Linux* と UNIX 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 の場合	Solaris の場合	AIX の場合	HP-UX の場合
ルートユーザ :				
デフォルトの場所	RPM	パッケージ	ファイルセット	Depot
任意の場所	Tarball	パッケージと Tarball	Tarball	Depot と Tarball
ルート以外のユーザ :				
任意の場所	Tarball	Tarball	Tarball	Tarball

tarball を使用したインストールの詳細については、『[Novell eDirectory 8.8 インストールガイド](#)』(<http://www.novell.com/documentation/edir88/edirin88/data/a79kg0w.html#bs6a3gs>) を参照してください。

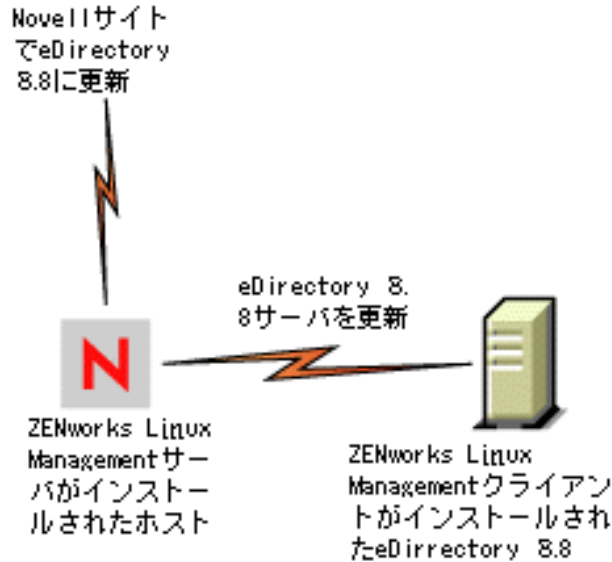
自動展開

Linux 上の eDirectory 8.8 では、ZENworks Linux Management を使用してアップグレードの配布と展開を容易に行うことができます。詳細については、[Ximian 製品 Web サイト](#) (<http://www.ximian.com/products/redcarpet>) を参照してください。

アップグレードの配布

eDirectory 8.8 を使用すると、eDirectory が備える機能を指定して、加入することができます。この機能に対する更新 (アップグレードまたはパッチ) が Novell サイト上にある場合は常に、その更新は自動的に取得されます。

図1 アップグレードの配布

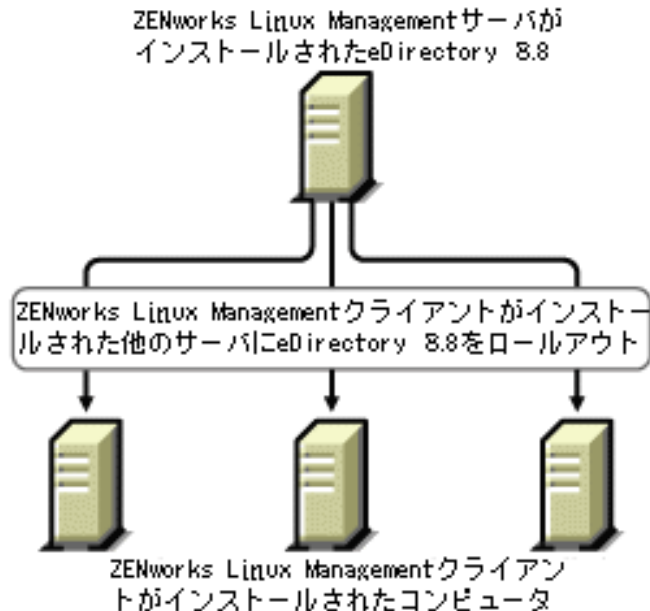


アップグレードを容易に配布するには、eDirectory 8.8 が存在するホストに ZENworks Linux Management クライアントをインストールし、更新がある場合に通知を受け取るために ZENworks Linux Management サーバに登録する必要があります。

容易な展開

eDirectory 8.8 では、ZENworks Linux Management サーバがインストールされているホストに eDirectory をインストールし、その後で ZENworks Linux Management クライアントがインストールされている他のサーバに eDirectory を展開することができます。

図2 RedCarpet からの eDirectory の配布



YaST を使用した eDirectory のインストールと設定

Open Enterprise Server (OES) とも呼ばれる SLES 9.1 では、YaST を使用して eDirectory 8.8 をインストールおよび設定できます。

YaST を使用した eDirectory のインストールと設定の詳細については、『*Novell eDirectory 8.8 インストールガイド*』(<http://www.novell.com/documentation/edir88/edirin88/data/a79kg0w.html#bv1lx18>) を参照してください。

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。

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

アプリケーションファイルに任意の場所を指定する

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

Linux、UNIX の場合

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。

NetWare の場合

NetWare では、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はできません。

Windows の場合

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。

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、データ、dib、およびログのディレクトリが含まれます。

Linux、UNIX の場合

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
<code>-d 任意の場所</code>	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。
<code>-D 任意の場所</code>	データ (pid やソケット ID などのデータを含む)、dib、およびログのディレクトリを、指定したパスに作成します。

NetWare の場合

eDirectory のアップグレード中に DIB の任意の場所を選択することはできません。NetWare では、eDirectory のインストールは常にアップグレードです。そのため、NetWare 上では DIB の任意のパスを選択できません。

Windows の場合

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

環境設定ファイルに任意の場所を指定する

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

Linux、UNIX の場合

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
```

NetWare、Windows の場合

NetWare と 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。

ルート以外のユーザによるインストール

ルート権限を持っていないユーザは、この機能によって Linux および UNIX で eDirectory 8.8 をインストールできます。ルートユーザが eDirectory をインストールする場合、ルート以外のユーザは eDirectory を使用できます。

この機能は、NetWare と Windows ではサポートされていません。

重要: ルート以外のユーザは、SLP や SNMP サブエージェントをインストールできません。

一般的には、次のように 2 種類のルート以外のユーザが存在します。

- ◆ UNIX コンピュータでルートではないユーザ。詳細については、[16 ページの「ルート以外のユーザ」](#)を参照してください。
- ◆ eDirectory の管理者ではないユーザ。詳細については、[16 ページの「管理者以外のユーザ」](#)を参照してください。

ルート以外のユーザ

eDirectory をインストールするルート以外のユーザ

このユーザはホストマシン上でルートではありません。ルート以外のユーザが eDirectory をインストールする権利は、ユーザがそのホストマシンで持っている権利に結び付いています。

eDirectory を設定するルート以外のユーザ

このユーザはホストマシン上でルートではありません。ルート以外のユーザが eDirectory を設定する権利は、ユーザがそのホストマシンで持っている権利に結び付いています。

管理者以外のユーザ

このユーザは eDirectory の管理者ではありません。管理者以外のユーザが eDirectory を設定する権利は、eDirectory でそのユーザのオブジェクトに割り当てられている権利によって異なります。

標準の準拠

eDirectory 8.8 は次の標準に準拠しています。

- ◆ [16 ページの「FHS の準拠」](#)
- ◆ [17 ページの「LSB の準拠」](#)

FHS の準拠

他製品のアプリケーションファイルとの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 および UNIX 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 および UNIX のマニュアルページ	/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。

任意の場所 /opt/novell/eDirectory/bin/ndspath ユーティリティ名とパラメータ

- ◆ 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。

. 任意の場所 /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。そのため、ログインするか新しいシェルを開くときにはいつでも、直接ユーティリティの使用を開始できます。

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。

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 (NetWare では dscheck) を実行してヘルスチェックを行うこともできます。

ヘルスチェックの必要性

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

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

サーバが正常であることの確認基準

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

ヘルスチェックを実行する

サーバのヘルスチェックは次の 2 種類の方法で実行できます。

- ◆ 18 ページの「アップグレードと同時に実行」
- ◆ 19 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。

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、UNIX の場合

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。

NetWare、Windows の場合

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

スタンドアロンユーティリティとして実行

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

表 1 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 および UNIX	ndscheck 構文： ndscheck -h ホスト名:ポート -a 管理者 FDN -F ログファイルのパス --config-file 環境設定ファイルの名前とパス 注: -h または --config-file のいずれかを指定できます。これらを両方とも指定することはできません。
NetWare	dscheck
Windows	ndscheck

ヘルスチェックのタイプ

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

- ◆ **基本的なサーバの状態**
- ◆ **パーティションとレプリカの状態**

ndscheck ユーティリティを実行すると、ヘルスチェックの結果は画面に表示され、ndscheck.log (NetWare では dscheck.log) に記録されます。ログファイルの詳細については、[22 ページの「ログファイル」](#)を参照してください。

アップグレードの一部としてヘルプチェックを実行した場合、ヘルスチェックの後にエラーの深刻度に基づいて、アップグレードを続行するかどうかの確認が求められるか、または処理が中断されます。エラーの詳細については、[20 ページの「状態のカテゴリ」](#)に記載されています。

基本的なサーバの状態

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

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

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

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

パーティションとレプリカの状態

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

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

状態のカテゴリ

サーバの状態は、チェック中に検出されるエラーに基づいて、次の3つカテゴリに分類されます。ヘルスチェックのステータスは、ログファイルに記録されます。詳細については、[22 ページの「ログファイル」](#)を参照してください。

ヘルスチェックのステータスは、**正常**、**警告**、および **Critical** 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。

詳細については、次の図を参照してください。

図 3 警告が発生したヘルスチェック

```

osg-dt-srv27</>ndsconfig upgrade -a admin.org
[1] Instance at /etc/opt/novell/eDirectory/conf/nds.conf: osg-dt-srv27.org.$OLTI
0615
Enter the password for admin.org:
Starting health check...
Mon Jun 21 08:20:48 2004
Performing health check on the eDirectory server ".CN=osg-dt-srv27.0=org.T=$OLTI0
615." ...
-----
Checking the LDAP and HTTP configuration...
WARNING: eDirectory server is not listening on the LDAP port 389
WARNING: eDirectory server is not listening on the LDAP port 636
Checking health of partitions ...
Status of partition ".T=$OLTI0615." ... [OK]
Checking the status of the replica ring...
Number of replicas = 2
-----+-----+-----+-----+-----+
Server Name                Status   Time Sync   Time Delta   Replica S
tate
-----+-----+-----+-----+-----+
.CN=osg-dt-srv27.0=org.T=$OLTI0615.    UP      YES        0 m:0 s      ON
.CN=osg-dt-srv9.0=org.T=$OLTI0615.     UP      YES        0 m:23 s     ON
-----+-----+-----+-----+-----+
Checking replication delta on the partition...
Maximum replica ring delta "0:3:35 (hh:mm:ss)"
Perishable delta on this server: "0:3:35 (hh:mm:ss)"
eDirectory health check completed.
Errors were detected during the server health check. Refer log file "/var/opt/no
vell/eDirectory/data/./log/ndscheck.log" for more details.
For a possible solution refer the following locations -
1. Cool solutions: http://www.novell.com/cool solutions/nds/
2. Support forums: http://support.novell.com/forums/2ed.html
3. Documentation (trouble shooting section): http://www.novell.com/documentati
on/edirectory.html
4. Error codes: http://www.novell.com/documentation/lg/nwec/index.html
5. Patches: http://support.novell.com/filefinder/5069/index.html
WARNING: Errors were detected during the server health check.
Continue (y/n)? _

```

Critical

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。

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、アップグレード操作は中止されます。

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。

詳細については、次の図を参照してください。

図 4 重大なエラーが発生したヘルスチェック

```
osg-dt-srv27</>ndsconfig upgrade -a admin.org
[!] Instance at /etc/opt/novell/eDirectory/conf/nds.conf: osg-dt-srv27.org.SOLT0615
Enter the password for admin.org:

Starting health check...
Mon Jun 21 08:14:46 2004
Performing health check on the eDirectory server ".CN=osg-dt-srv27.0=org.T=SOLT0615." ...

-----
Checking the LDAP and HTTP configuration... [OK]
Checking health of partitions ...
Status of partition ".T=SOLT0615." ... [OK]
Checking the status of the replica ring...
Number of replicas = 2
-----+-----+-----+-----+-----+
+-----+
Server Name                               Status   Time Sync   Time Delta   Replica S
state
-----+-----+-----+-----+-----+
.CN=osg-dt-srv27.0=org.T=SOLT0615.        UP       YES         0 m:0 s      ON
.CN=osg-dt-srv9.0=org.T=SOLT0615.        DOWN    -           -            ON
-----+-----+-----+-----+-----+
Checking replication delta on the partition...
Maximum replica ring delta "0:0:23 (hh:mm:ss)"
Perishable delta on this server: "0:0:0 (hh:mm:ss)"

eDirectory health check completed.

Errors were detected during the server health check. Refer log file "/var/opt/novell/eDirectory/data/./log/ndscheck.log" for more details.

For a possible solution refer the following locations -
1. Cool solutions: http://www.novell.com/cool solutions/nds/
2. Support forums: http://support.novell.com/forums/2ed.html
3. Documentation (trouble shooting section): http://www.novell.com/documentation/edirectory.html
4. Error codes: http://www.novell.com/documentation/lg/nwec/index.html
5. Patches: http://support.novell.com/filefinder/5069/index.html

ERROR 2: Check the errors before continuing with the eDirectory upgrade.
osg-dt-srv27</>_
```

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。例については、[図 3](#) および [図 4](#) を参照してください。

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)
- ◆ Novell 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 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 および UNIX	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。
NetWare	dscheck.log	sys:\system
Windows	ndscheck.log	インストールディレクトリ

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、UNIX、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、適切なログイン認証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 および UNIX :**

ndsconfig -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。

◆ **NetWare、Windows の場合 :**

デフォルトで、eDirectory のインストールとともにインストールされます。

SecretStore の使用方法に関する詳細については、『[Novell SecretStore 管理ガイド](http://www.novell.com/documentation/secretstore33/index.html)』(<http://www.novell.com/documentation/secretstore33/index.html>) を参照してください。

詳細情報

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。

- ◆ 『Novell eDirectory 8.8 インストールガイド』 (<http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html>)
- ◆ 『Novell eDirectory 8.8 管理ガイド』 (<http://www.novell.com/documentation/edir88/edir88/data/fbadjaeh.html#fbadjaeh>)
- ◆ Linux および UNIX の場合: nds-install、ndsconfig、および ndscheck のマニュアルページ

2

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 Novell® 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
注：このベータ版では、複数のインスタンスを設定できるのは eDirectory 8.8 のみで、その他のバージョンの eDirectory については設定できません。
- ◆ 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	NetWare の場合	Linux の場合	UNIX	Windows の場合
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。

- ◆ [26 ページの「複数インスタンスを展開する場合のシナリオ」](#)
- ◆ [26 ページの「複数インスタンスの使用」](#)
- ◆ [28 ページの「複数インスタンスを管理する」](#)
- ◆ [32 ページの「複数インスタンスのシナリオ」](#)

複数インスタンスの必要性

複数インスタンスは、次のことを行う必要性から提供されるようになりました。

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

複数インスタンスを展開する場合のシナリオ

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

大企業における eDirectory の使用

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

評価用セットアップにおける eDirectory の使用

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

複数インスタンスの使用

eDirectory 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。

- ◆ [27 ページの「セットアップの計画」](#)
- ◆ [27 ページの「複数インスタンスを設定する」](#)

セットアップの計画

この機能を有効に使用するためには、eDirectory のインスタンスを複数計画し、各インスタンスが、ホスト名、ポート番号、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)

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。

すでに説明したように、設定を始める前には、環境設定ファイルの場所、DIB、ポート番号などのインスタンス識別子を決定しておく必要があります。

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 だけが使用されます。
-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。例： -B eth0@524 または -B 100.1.1.2@524 注: -b と -B だけが使用されます。
-D	データ、dib、およびログのディレクトリを、新しいインスタンス用に指定したパスに作成します。

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、[29 ページの「ndsmanage を使用してインスタンスを作成する」](#)を参照してください。

複数インスタンスを管理する

このセクションでは、次の情報について説明します。

- ◆ 28 ページの「**ndsmanage ユーティリティ**」
- ◆ 31 ページの「**特定のインスタンスの識別**」
- ◆ 31 ページの「**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**」

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。

- ◆ **設定されているインスタンスの表示**
- ◆ **新しいインスタンスの作成**
- ◆ **選択され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 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および停止**

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 3 インスタンスを表示する際の ndsmanage の使用法

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、29 ページの「**ndsmanage ユーティリティの出力画面**」を参照してください。

ndsmanage を使用してインスタンスを作成する

ndsmanage を使用して新しいインスタンスを作成する。

- 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 5 ndsmanage ユーティリティの出力画面

```
bash-3.00# ndsmanage root
eDirectoryインスタンスの管理用Novellユーティリティ - バージョン: 1.0

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 : .SUN1.SCON.STREE. : 80.85.182.28@524 : ACTIVE
[2] /builds/server2/eDirectory/conf/nds.conf : .SUN1.SCON.STREE. : 80.85.182.28@524 : ACTIVE

<Enter> [1 - 1] 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。

- ◆ 29 ページの「特定のインスタンスの開始」
- ◆ 30 ページの「特定のインスタンスの停止」
- ◆ 30 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 `ndstrace` 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：

- 1 次のコマンドを入力します。

```
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。

```

bash-3.00# ndsmanage root
eDirectoryインスタンスの管理用Novellユーティリティ - バージョン: 1.0

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 : .SUN1.SCON.STREE. : 80.85.182.26@524 : ACTIVE
[2] /builds/server2/eDirectory/conf/nds.conf : .SUN1.SCON.STREE. : 80.85.182.26@524 : ACTIVE

<Enter> [1 - 1] 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
[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
[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 *自分が設定したインスタンスの設定ファイル*

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：

1 次のコマンドを入力します。

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、**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 (30 ページ)** 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
自分が設定したインスタンスの環境設定ファイル

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：

1 次のコマンドを入力します。

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、**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 (30 ページ)** 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、[29 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、[30 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。

特定のインスタンスの識別

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

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

特定のインスタンスに対するユーティリティの呼び出し

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

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

たとえば、**--config-file** オプションを指定して特定のインスタンスに対して **ndstrace** を実行する場合は、次のように入力します。

```
ndstrace --config-file 場所を指定した環境設定ファイル
```

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。

セットアップの計画

Mary は次のインスタンス識別子を指定します。

- ◆ インスタンス 1 :

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

- ◆ インスタンス 2 :

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

インスタンスの設定

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

- ◆ インスタンス 1 :

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

- ◆ インスタンス 2 :

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

インスタンスに対するユーティリティの呼び出し

ポート 1524 を監視しているインスタンス 1 に対して `ndstrace` ユーティリティを実行する必要があります、この環境設定ファイルが `home/mary/inst1/nds.conf` location にあり、DIB ファイルが `/home/mary/inst1/var` にある場合、Mary は次のようにしてユーティリティを実行できます。

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

または

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

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

インスタンスの表示

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

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

```
ndsmanage
```

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

```
ndsmanage john
```

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

```
ndsmanage -a
```

詳細情報

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。

- ◆ 『Novell eDirectory 8.8 インストールガイド』(<http://www.novell.com/documentation/edir88/edirin88/data/a79kg0w.html#bqs8mmt>)
- ◆ Linux および UNIX : `ndsconfig` および `ndsmanage` のマニュアルページ

3

SASL-GSSAPI を使用した eDirectory に対する認証

Novell® eDirectory™ 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。

- ◆ 35 ページの「概念」
- ◆ 36 ページの「eDirectory における GSSAPI の動作」
- ◆ 37 ページの「GSSAPI の設定」
- ◆ 38 ページの「LDAP での GSSAPI の使用方法」
- ◆ 38 ページの「よく使用される用語」

概念

- ◆ 35 ページの「Kerberos について」
- ◆ 36 ページの「SASL について」
- ◆ 36 ページの「GSSAPI について」

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。

Novell Kerberos KDC の詳細については、[Novell Kerberos KDC documentation \(http://www.novell.com/documentation/kdc/index.html\)](http://www.novell.com/documentation/kdc/index.html) を参照してください。

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 \(http://www.ietf.org/rfc/rfc2222.txt?number=2222\)](http://www.ietf.org/rfc/rfc2222.txt?number=2222) を参照してください。

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。

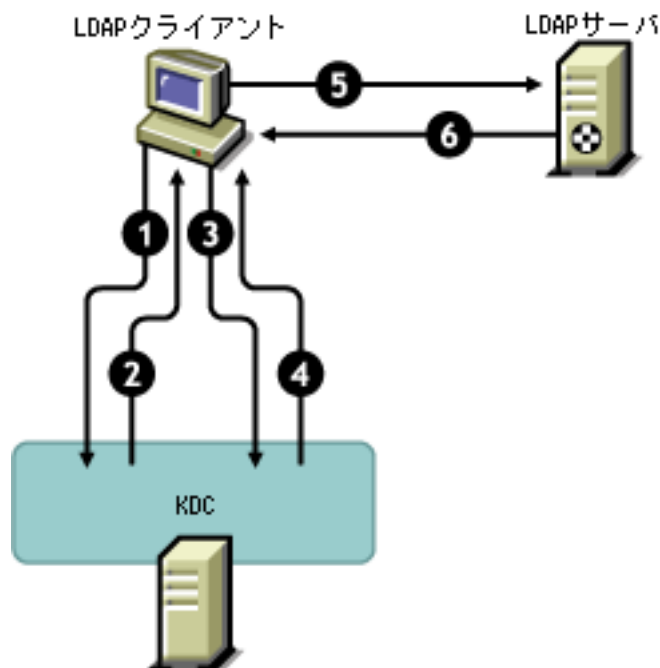
GSS API の形式に関する詳細については、[RFC 1964 \(http://www.ietf.org/rfc/rfc1964.txt?number=1964\)](http://www.ietf.org/rfc/rfc1964.txt?number=1964) を参照してください。

この SASL-GSSAPI 実装は、[RFC 2222 \(http://www.ietf.org/rfc/rfc2222.txt?number=2222\)](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。

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 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、Microsoft*、または Heimdal のいずれかのもを使用できます。
- 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。

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。レルムのマスター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 NMAS 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 接続を使用して eDirectory へ接続するように iManager を設定する方法については、『*iManager 2.5 管理ガイド*』(<http://www.novell.com/documentation/lg/imanager20/index.html?page=/documentation/lg/imanager20/imanager20/data/am4ajce.html#bow4dv4>) を参照してください。

- 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。

上記の手順の詳細については、[Novell Kerberos KDC documentation](http://www.novell.com/documentation/kdc/index.html) (<http://www.novell.com/documentation/kdc/index.html>) を参照してください。

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『[Novell eDirectory 8.8 管理ガイド](http://www.novell.com/documentation/edir88/edir88/data/h0000007.html#a680dyc)』(<http://www.novell.com/documentation/edir88/edir88/data/h0000007.html#a680dyc>) を参照してください。

LDAP サーバは、SASL に問い合わせで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
```

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 4 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。

4

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

Novell® 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、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ます。

- ◆ 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
- ◆ Novell iManager 2.5 (Windows で実行されている場合を除く)

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	NetWare の場合	Linux の場合	UNIX	Windows の場合
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	✓	✓	✓	✓

注：このベータ版では、Netware 上の eDirectory を eDirectory 8.8 にアップグレードしないと、iManager を iManager 2.5 にアップグレードした場合でも、iManager ログインで大文字と小文字を区別するパスワードを利用できません。

このセクションでは、次の情報について説明します。

- ◆ [40 ページの「大文字と小文字を区別するパスワードの必要性」](#)
- ◆ [40 ページの「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」](#)
- ◆ [41 ページの「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」](#)
- ◆ [43 ページの「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」](#)

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 8.7.1 および 8.7.3 では、[ユニバーサルパスワード \(http://www.novell.com/documentation/nmas23/admin/data/allq21t.html\)](http://www.novell.com/documentation/nmas23/admin/data/allq21t.html) を有効にすると、Novell Client32™ を使用してログインした場合のみパスワードの大文字と小文字が区別されました。他のクライアント (eDirectory SDK または iManager など) でログインした場合は、パスワードの大文字と小文字は区別されませんでした。

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るようになりました。

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、[43 ページの「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。

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。

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、NMASS を使用してログインする必要があります。したがって、環境変数 `NDS_TRY_NMASLOGIN_FIRST` を `TRUE` に設定する必要があります。こうすることにより、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なります。

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 および UNIX :

`ndsd` スクリプト `/etc/init.d/ndsd` に次のコードを追加します。

```
NDS_TRY_NMASLOGIN_FIRST=true
export NDS_TRY_NMASLOGIN_FIRST
```

- ◆ NetWare:

`sys:\system\Autoexec.ncf` ファイルの冒頭に次のコードを追加します。

```
env NDS_TRY_NMASLOGIN_FIRST=true
```

- ◆ 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。変数を追加して値に `TRUE` を設定します。

2 eDirectory サーバを再起動します。

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します。

詳細については、『*Deploying Universal Password*』(<http://www.novell.com/documentation/nmas23/admin/data/allq21t.html>) を参照してください。

- 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、**42 ページの「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。

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。

大文字と小文字を区別するパスワードの管理

Novell 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、『*Deploying Universal Password*』(<http://www.novell.com/documentation/nmas23/admin/data/allq21t.html>) を参照してください。

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
- ◆ Novell iManager 2.5

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、**42 ページの「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、43 ページの「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。

注: このベータ版では、Netware 上の eDirectory を eDirectory 8.8 にアップグレードしないと、iManager を iManager 2.5 にアップグレードした場合でも、iManager ログインで大文字と小文字を区別するパスワードを利用できません。

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、40 ページの「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、デフォルトでは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「novell」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、「novell」と「Novell」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。『*Deploying Universal Password*』(<http://www.novell.com/documentation/nmas23/admin/data/allq21t.html>) を参照してください。

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「noVell」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「Novell」(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。

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、次の情報について説明します。

- ◆ [43 ページの「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」](#)
- ◆ [43 ページの「NDS ログイン設定の管理」](#)
- ◆ [47 ページの「パーティション操作」](#)
- ◆ [47 ページの「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」](#)

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。

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、Novell iManager 2.5 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。

- ◆ [44 ページの「異なるレベルでの NDS 設定」](#)
- ◆ [45 ページの「iManager を使用して NDS 設定を管理する」](#)
- ◆ [46 ページの「LDAP を使用して NDS 設定を管理する」](#)
- ◆ [47 ページの「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 5 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	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、**45 ページの「iManager を使用して NDS 設定を管理する」** および **46 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、[45 ページの「iManager を使用して NDS 設定を管理する」](#) および [46 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、次の情報について説明します。

- ◆ [45 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」](#)
- ◆ [45 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 Novell iManager で、[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 Novell iManager で、[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。

- ◆ 46 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」
- ◆ 47 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。

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。

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。

詳細情報

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
- ◆ 『*Deploying Universal Password*』 (<http://www.novell.com/documentation/nmas23/admin/data/allq21t.html>)

5

優先度同期

優先度同期は、eDirectory の現在の同期処理を補う Novell® 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 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	NetWare の場合	Linux の場合	UNIX	Windows の場合
優先度同期	✓	✓	✓	✓

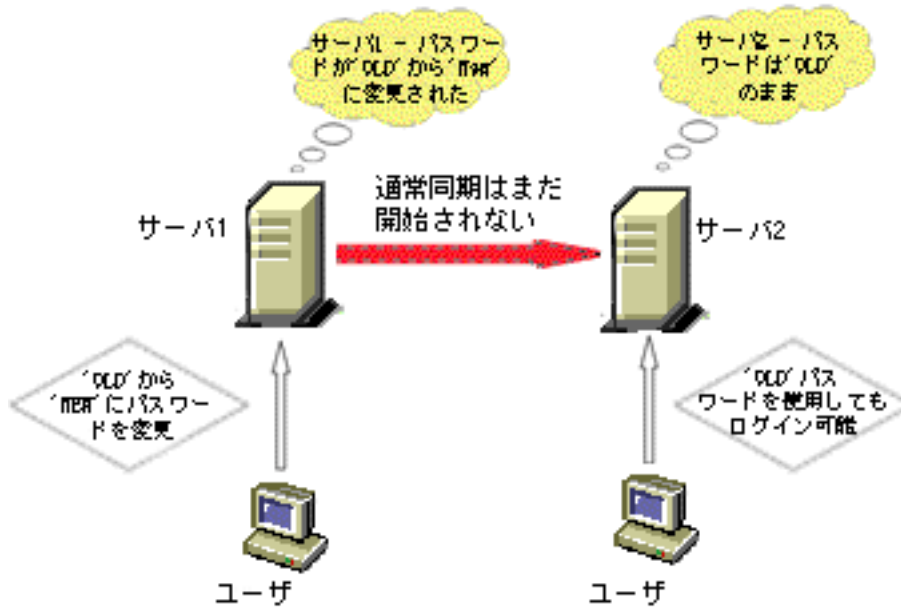
このセクションでは、次の情報について説明します。

- ◆ [49 ページの「優先度同期の必要性」](#)
- ◆ [50 ページの「優先度同期の使用」](#)

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 8 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。

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、Novell iMonitor から優先度同期キューサイズを設定します。
2. Novell 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。

詳細情報

優先度同期の詳細については、次を参照してください。

- ◆ 『Novell eDirectory 8.8 管理ガイド』 (<http://www.novell.com/documentation/edir88/edir88/data/brp2di9.html#brp2z9z>)
- ◆ iManager および iMonitor のオンラインヘルプ

6

データの暗号化

Novell® 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	NetWare の場合	Linux の場合	UNIX	Windows の場合
暗号化属性	✓	✓	✓	✓
暗号化複製	✗	✓	✓	✓

このセクションでは、次の情報について説明します。

- ◆ [51 ページの「属性を暗号化する」](#)
- ◆ [52 ページの「複製を暗号化する」](#)

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に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、[52 ページの「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、次の情報について説明します。

- ◆ [51 ページの「暗号化属性の必要性」](#)
- ◆ [52 ページの「属性を暗号化する方法」](#)
- ◆ [52 ページの「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。

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。

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。

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 プラグインを使用して、クリアテキストチャネルを通して暗号化属性へのアクセスを提供することができます。詳細については、『*Novell eDirectory 8.8 管理ガイド*』(<http://www.novell.com/documentation/edir88/index.html>) を参照してください。

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、次の情報について説明します。

- ◆ 52 ページの「暗号化複製の必要性」
- ◆ 53 ページの「暗号化複製を有効にする」

注：Netware[®] では、暗号化複製機能がサポートされていません。

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ります。
- ◆ 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。

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。

詳細情報

eDirectory におけるデータの暗号化に関する詳細については、次を参照してください。

- ◆ 『*Novell eDirectory 8.8 管理ガイド*』 (<http://www.novell.com/documentation/edir88/index.html>)
- ◆ iManager および iMonitor のオンラインヘルプ

7

バルクロードのパフォーマンス

Novell® 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、『*Novell eDirectory 8.8 管理ガイド*』(<http://www.novell.com/documentation/edir88/edir88/data/bqu6wcq.html>) 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

8

iManager ICE プラグインによる設定

Novell® 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	NetWare の場合	Linux の場合	UNIX	Windows の場合
ICE iManager 拡張機能	✓	✓	✓	✓

eDirectory 8.8 に付属する iManager 2.5 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

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。

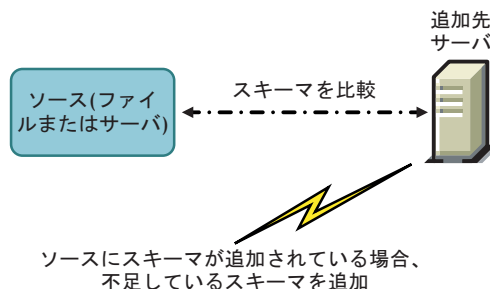
iManager の ICE ウィザードからは、不足しているスキーマを次のオプションを使って追加できます。

- ◆ 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

スキーマをファイルから追加する

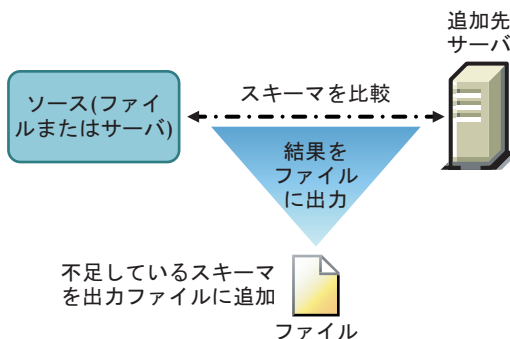
ICE はソースとターゲットのスキーマを比較できます。ソースはファイルまたは LDAP サーバのいずれかで、ターゲットは LDAP サーバです。ソースのスキーマファイルは、LDIF 形式または SCH 形式のいずれかになります。

図 9 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 10 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、『Novell eDirectory 8.8 管理ガイド』の「Novell eDirectory 管理ユーティリティ」(<http://www.novell.com/documentation/edir88/edir88/data/a5hf8rg.html#a5hf8rg>)の章を参照してください。

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、『Novell eDirectory 8.8 管理ガイド』の「Novell eDirectory 管理ユーティリティ」(<http://www.novell.com/documentation/edir88/edir88/data/a5hf8rg.html#a5hf8rg>)の章を参照してください。

スキーマの比較

iManager を使用して、ソースとターゲットの間でスキーマを比較できます。ソースはファイルまたはサーバのいずれかになります。ターゲットは LDIF ファイルである必要があります。

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

スキーマファイルを比較する

この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、『Novell eDirectory 8.8 管理ガイド』の「Novell eDirectory 管理ユーティリティ」(<http://www.novell.com/documentation/edir88/edir88/data/a5hf8rg.html#a5hf8rg>)の章を参照してください。

サーバとファイルの間でスキーマを比較する

このオプションはソースサーバ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、『Novell eDirectory 8.8 管理ガイド』の「Novell eDirectory 管理ユーティリティ」(<http://www.novell.com/documentation/edir88/edir88/data/a5hf8rg.html#a5hf8rg>)の章を参照してください。

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、『Novell eDirectory 8.8 管理ガイド』の「Novell eDirectory 管理ユーティリティ」(<http://www.novell.com/documentation/edir88/edir88/data/a5hf8rg.html#a5hf8rg>)の章を参照してください。

9

LDAP ベースのバックアップ

LDAP ベースのバックアップ機能は Novell® eDirectory™ 8.8 から導入されました。この機能を使用すると、1 回につき 1 つのオブジェクトの属性と属性値がバックアップされます。

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	NetWare の場合	Linux の場合	UNIX	Windows の場合
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 \(http://developer.novell.com/ndk/cldap.htm\)](http://developer.novell.com/ndk/cldap.htm) 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 \(http://developer.novell.com/ndk/doc/samplecode/cldap_sample/extensions/backup.c.html\)](http://developer.novell.com/ndk/doc/samplecode/cldap_sample/extensions/backup.c.html) を参照してください。

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。

詳細情報

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/ndk/cldap.htm>)
- ◆ サンプルコード : backup.c (http://developer.novell.com/ndk/doc/samplecode/cldap_sample/extensions/backup.c.html)

10 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、Novell® 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。

- ◆ 63 ページの「メッセージの重大度レベル」
- ◆ 65 ページの「エラーログを設定する」
- ◆ 69 ページの「DSTrace メッセージ」
- ◆ 72 ページの「iMonitor メッセージのフィルタ」
- ◆ 72 ページの「SAL メッセージのフィルタ」

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。

- ◆ 63 ページの「致命的エラー」
- ◆ 64 ページの「警告」
- ◆ 64 ページの「Error」
- ◆ 64 ページの「情報」
- ◆ 64 ページの「デバッグ」

致命的エラー

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。

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。

Error

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すると、eDirectory サーバは ERR_FAILED_AUTHENTICATION エラーを通知します。

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。

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。

エラーログを設定する

Linux、UNIX の場合

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、[63 ページの「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使用します。

```
n4u.server.log-levels= 重大度レベル
```

例 :

- ◆ 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、`nds.log` ファイルにメッセージが記録されます。

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
```

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 `nds.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。

Windows の場合

- ◆ 66 ページの「重大度レベルの設定」
- ◆ 66 ページの「ログファイル名とパスの指定」
- ◆ 67 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、63 ページの「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] > [Novell 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。
`LogLevel=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] > [Novell 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= ファイルのパス`
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] > [Novell 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= サイズ
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。

NetWare の場合

NetWare では、DSLOG.NLM がサーバ側メッセージを記録します。サーバ側メッセージは sys:\system\ds.log に記録されます。

注: DSLOG.NLM は、DS の移動中には自動的に動作します。DSLOG.NLM は、手動でロードまたはアンロードすることができます。

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、[63 ページの「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、イベントタグとメッセージが ds.log に記録されます。メッセージは次の形式で記録されます。

< イベントタグ >:< 時刻 >:< 重大度レベル >: メッセージ

例:

```
INIT:[2005/03/25 15:27:14] INFO:NDS Schema Upgrade Version:DIB 1, Code 1  
PART:[2005/03/25 16:18:10] DEBUG:Merging partition root data during  
partition join success
```

フィルタの設定

フィルタを設定するには、次の構文を入力します。

DSLOG オプション

次の表では、dslog のオプションについて説明します。

表 6 Dslog のオプションの説明

オプション	説明
FILE ON	ログファイルへの記録を有効にします。 デフォルトでは FILE は ON に設定されています。
FILE OFF	ログファイルへの記録を無効にします。
FMAX= サイズ	最大ディスクファイルサイズを指定します。

オプション	説明
SLEVEL= 値	エラーの重大度レベルを指定します。 デフォルトでは SLEVEL は LogFatal に設定されます。
FNAME= 名前	ディスクファイル名を指定します。 デフォルトのファイル名は ds.log です。

例：

- ◆ ログを有効にするには、次のように入力します。

```
DSLOG FILE ON
```

- ◆ ログを無効にするには、次のように入力します。

```
DSLOG FILE OFF
```

- ◆ 最大ファイルサイズを 10,240 バイトに設定するには、次のように入力します。

```
DSLOG FMAX=10240
```

- ◆ 重大度がデバッグメッセージ以上のメッセージをフィルタするには、次のように入力します。

```
DSLOG SLEVEL=LOGDBG
```

- ◆ ログファイル名を指定するには、次のように入力します。

```
DSLOG FNAME=DS.LOG
```

dslog オプションについては、オンラインヘルプを参照してください。その場合は、コマンドラインで次のように入力します。

```
help dslog
```

現在の設定を表示する

次のように GET オプションを使用すると、現在の設定を表示することができます。

```
DSLOG GET
```

たとえば、DSLOG を有効にして重大度レベルをデバッグに設定した場合、出力は次のようになります。

```
DSLOG Configuration:
DSLOG File is ON           File Name: DS.LOGFile
Size: nnnnn(Max: nnnnnn). Severity Level: LOGDBG
```

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、`ndstrace` 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、[72 ページの「iMonitor メッセージのフィルタ」](#)を参照してください。

NetWare、Linux、および UNIX

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。

注: 次のコマンドでは、NetWare の `ndstrace` を `dstrace` に変更します。

- 1 次のコマンドでフィルタを有効にします。

```
ndstrace タグ フィルタの値
```

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 タグ
```

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 11 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\0=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 DSASStartUpdateReplica 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 : DSASStartUpdateReplica 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.

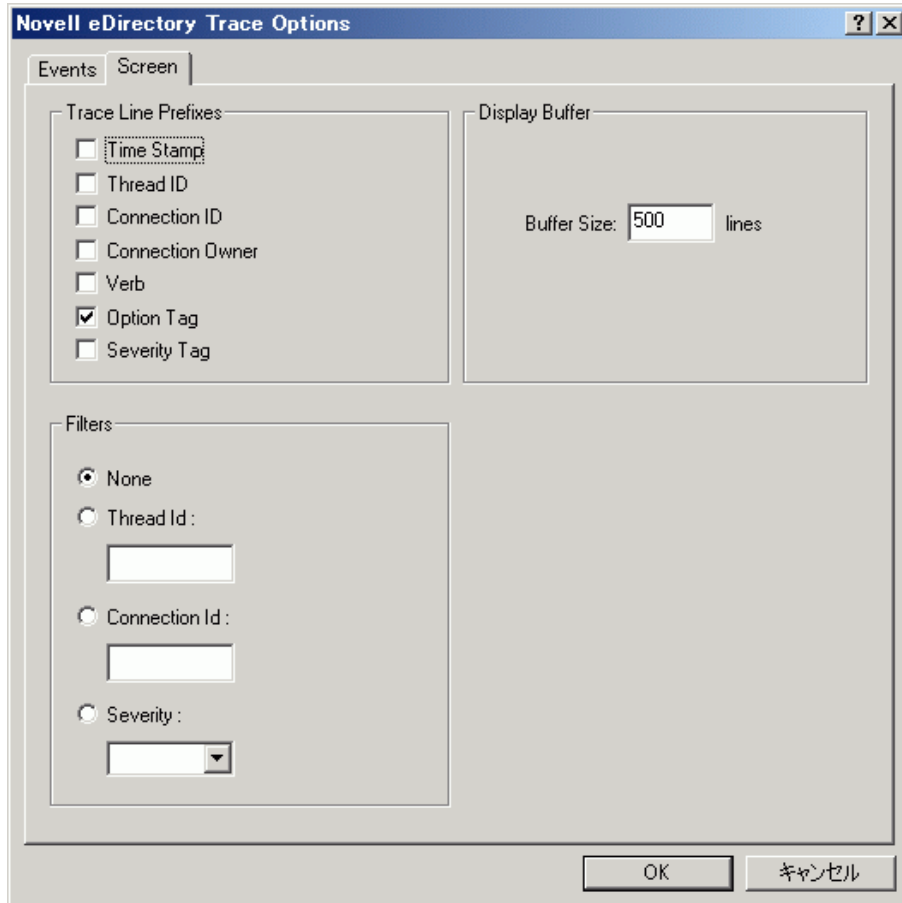
```

Windows の場合

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] > [Novell 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。
[Novell 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 12 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。

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。iMonitor のオンラインヘルプは iMonitor の画面から表示できます。

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。

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 7 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。

たとえば、LogInfo と LogDbg を除くすべてのログレベルに基づいてフィルタを行うには、次のように入力します。

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


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 と UNIX では、メッセージはシステムログに出力されます。NetWare と 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。

11

その他

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

- ◆ 75 ページの「セキュリティオブジェクトのキャッシュ」
- ◆ 76 ページの「サブツリー検索のパフォーマンスの向上」
- ◆ 76 ページの「localhost の変更点」
- ◆ 76 ページの「Solaris の 256 個のファイルハンドラ」
- ◆ 76 ページの「Solaris のメモリマネージャ」

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ク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、バックリンクが 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。データを直ちに同期する必要がある場合は、iMonitor、ndstrace (Linux および UNIX)、dstrace (Netware®)、または ndscons (Windows) を使用して、ローカルサーバでバックリンクを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。バックリンク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。

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 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 は検索の範囲を制限します。

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 以上に更新されます。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、ndsrepair は AncestorID 属性を更新します。

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、ホスト名解決または IP アドレス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。

Solaris の 256 個のファイルハンドラ

以前は、Solaris 2.x の stdio ストリーム実装で利用できるファイル記述子は、最大で 256 個だけでした。この数は、eDirectory が正しく動作するためには不十分でした。eDirectory 8.8 では、スタブライブラリを用意してこの制限を克服しています。

Solaris 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。