NetIQ® eDirectory™

管理ガイド

2019年10月

保証と著作権

保証と著作権、商標、免責事項、保証、輸出およびその他の使用制限、米国政府の規制による権利、特許に関する方針、およびFIPSコンプライアンスの詳細については、https://www.netiq.com/company/legal/を参照してください。

本書およびライブラリについて

この*管理ガイド*では、NetIQ eDirectory (eDirectory)製品を管理および設定する方法について説明します。

本書の読者

このマニュアル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。

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。

Linuxプラットフォーム用チューニングガイド

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

これらのガイドは、NetIQ eDirectory 9.2マニュアルのWebサイトで入手できます。

eDirectory管理ユーティリティの詳細については、『*NetIQ iManager 3.2 Administration Guide*』を参照してください。

NetIQ社について

当社はグローバルなエンタープライズソフトウェア企業であり、お客様の環境において絶えず挑戦となる変化、複雑さ、リスクという3つの要素に焦点を当て、それらをお客様が制御するためにどのようにサポートできるかを常に検討しています。

当社の観点

変化に適応すること、複雑さとリスクを管理することは普遍の課題

実際、直面するあらゆる課題の中で、これらは、物理環境、仮想環境、およびクラウドコンピューティング環境の安全な評価、監視、および管理を行うために必要な制御を脅かす最大の要因かもしれません。

重要なビジネスサービスの改善と高速化を可能にする

当社は、IT組織に可能な限りの制御能力を付与することが、よりタイムリーでコスト効率の高いサービス提供を実現する唯一の方法だと信じています。組織が継続的な変化を遂げ、組織を管理するために必要なテクノロジが実質的に複雑さを増していくにつれ、変化と複雑さという圧力はこれからも増え続けていくことでしょう。

当社の理念

単なるソフトウェアではなく、インテリジェントなソリューションを販売する

確かな制御手段を提供するために、まずお客様のIT組織が日々従事している現実のシナリオを把握することに努めます。そのようにしてのみ、実証済みで測定可能な結果を成功裏に生み出す、現実的でインテリジェントなITソリューションを開発することができます。これは単にソフトウェアを販売するよりもはるかにやりがいのあることです。

当社の情熱はお客様の成功を推し進めること

お客様が成功するためにわたしたちには何ができるかということが、わたしたちのビジネスの核心にあります。製品の着想から展開まで、当社は次のことを念頭に置いています。お客様は既存資産とシームレスに連動して動作するITソリューションを必要としており、展開後も継続的なサポートとトレーニングを必要とし、変化を遂げるときにも共に働きやすいパートナーを必要としています。究極的に、お客様の成功こそがわたしたちの成功なのです。

当社のソリューション

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

- ワークロード管理
- サービス管理

セールスサポートへのお問い合わせ

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

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

テクニカルサポートへのお問い合わせ

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

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

マニュアルサポートへのお問い合わせ

弊社の目標は、お客様のニーズを満たすマニュアルの提供です。改善のためのご提案は、www.netiq.com/documentationに掲載されている本マニュアルのHTML版で、各ページの下にある［**コメントを追加**］をクリックしてください。Documentation-Feedback@netiq.com宛てに電子メールを送信することもできます。貴重なご意見をぜひお寄せください。

オンラインユーザコミュニティへのお問い合わせ

NetIQのオンラインコミュニティであるQmunityは、他のユーザやNetIQのエキスパートとやり取りできるコラボレーションネットワークです。より迅速な情報、有益なリソースへの役立つリンク、NetIQエキスパートとのやり取りを提供するQmunityは、頼みにしているIT投資が持つ可能性を余すことなく実現するために必要な知識の習得に役立ちます。詳細については、http://community.netiq.comを参照してください。

1 NetIQ eDirectoryについて

単純化して言えば、NetIQ eDirectoryとはネットワークユーザ、サーバ、プリンタ、プリントキュー、アプリケーションなどのネットワークリソースを表すオブジェクトのリストです。NetIQ eDirectoryは、スケーラブルで高性能、安全性の高いディレクトリサービスです。ユーザ、アプリケーション、ネットワークデバイス、およびデータなど、多量のオブジェクトを格納および管理できます。NetIQ eDirectoryが提供するセキュア識別情報管理ソリューションは、複数のプラットフォーム間で実行され、インターネットスケーラブルであり、拡張可能です。

また、NetIQ eDirectoryは、中央型識別情報管理、インフラストラクチャ、社内ネットワーク全体をカバーするセキュリティ、およびスケーラビリティを、ファイアウォールの内外で実行するすべてのアプリケーションに提供します。NetIQ eDirectoryには、Webベースのワイヤレス管理機能が含まれており、Webブラウザや各種ハンドヘルドデバイスから、ディレクトリやユーザ、アクセス権、およびネットワークリソースにアクセスしたり、それらを管理したりすることができます。

NetIQ eDirectoryでは、ディレクトリ標準LDAP (Lightweight Directory Access Protocol)バージョン3がネイティブでサポートされ、OpenSSLソースコードに基づいたTLS/SSLサービスへのサポートが提供されています。

eDirectoryエンジンの詳細については、「eDirectory Process Requests (http://support.novell.com/techcenter/articles/anp20020801.html)」を参照してください。

図 1-1は、NetIQ iManager管理ユーティリティで表示されるオブジェクトの一部を示しています。

図 1-1 *iManager でのeDirectoryオブジェクト*

eDirectoryサーバに設定された実際のスキーマやeDirectoryを実行するオペレーティングシステムによっては、使用できないオブジェクトクラスもあります。

オブジェクトの詳細については、25 ページの 「オブジェクトクラスとプロパティ」を参照してください。

ネットワークに複数のeDirectoryサーバがある場合、ディレクトリは複数のサーバに複製できます。

このセクションでは、次の情報について説明します。

- 22 ページの 「NetIQ iManagerの便利な管理機能」

- 25 ページの 「オブジェクトクラスとプロパティ」
- 48 ページの 「コンテキストと命名規則」
- 51 ページの 「スキーマ」
- 58 ページの 「パーティション」
- 61 ページの 「レプリカ」
- 67 ページの 「レプリカリングでのサーバの同期」
- 67 ページの 「リソースへのアクセス」
- 68 ページの 「eDirectoryでの権利」

NetIQ iManagerの便利な管理機能

NetIQ eDirectoryでは、ネットワークリソースを容易に、強力に、そしてフレキシブルに管理することができます。eDirectoryは、グループウェアやその他アプリケーションのユーザ情報のリポジトリとしても機能します。これらのアプリケーションは、業界標準のLDAP(Lightweight Directory Access Protocol)を使用して、ディレクトリにアクセスします。

eDirectoryの便利な管理機能には、強力なツリー構造、統合管理ユーティリティ、およびシングルログインと認証機能があります。

NetIQ iManagerを使用して、Webブラウザやさまざまなハンドヘルドデバイスから、ディレクトリやユーザ、ディレクトリ内のアクセス権やネットワークリソースを管理できます。iManagerのeDirectoryプラグインを使用すると、基本的なディレクトリ管理タスクにアクセスしたり、DSRepair、DSMerge、バックアップおよび復元など、以前はeDirectoryサーバで実行する必要のあったeDirectory管理ユーティリティにアクセスしたりできます。

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

強力なツリー構造

NetIQ eDirectoryではオブジェクトがツリー構造に編成されます。最上位のTreeオブジェクトにはツリー名が付けられます。

eDirectoryサーバで動作するオペレーティングシステムがLinux、Windowsのどちらであっても、すべてのリソースを同じツリー内に保管できます。オブジェクトの作成や、権利の許可、パスワードの変更、アプリケーションの管理のために、それぞれのサーバやドメインに個別にアクセスする必要はありません。

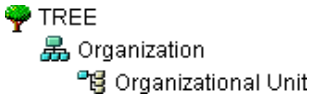
ツリーの階層構造によって、極めて柔軟で強力な管理が可能になっています。このような管理機能は、主に次の2つの機能で実現できます。

- 22 ページの 「コンテナオブジェクト」
- 23 ページの 「継承」

コンテナオブジェクト

コンテナオブジェクトを利用することによって、オブジェクトを個々に扱うのではなく、オブジェクトのまとまりとして扱うことができます。に示すように、コンテナオブジェクトには、3つの共通クラスがあります。図 1-2

図 1-2 コンテナオブジェクトの共通クラス



ツリーオブジェクトは、ツリー内の最上位のコンテナオブジェクトです。通常、このコンテナには、その会社の組織オブジェクトが格納されます。

組織は通常、ツリーオブジェクトの直下に位置するコンテナクラスです。一般に、組織オブジェクトには会社名に基づく名前が付けられます。小規模な会社の場合は、管理を容易化するために、他のオブジェクトをすべて組織オブジェクトの直下に配置します。

組織の下に部門オブジェクトを作成し、異なった地区、ネットワークキャンパス、または個々の部署を表すことができます。部門の下にさらに部門を作成して、ツリーを細分化することもできます。

その他、コンテナオブジェクトには、カントリクラスと地域クラスがあります。これらのクラスは通常、複数の国にまたがるネットワークでのみ使用されます。

ドメインオブジェクトは、ツリーオブジェクトの下、または組織、部門、国、地域オブジェクトの下に作成できます。

コンテナ内のすべてのオブジェクトに対してなんらかの処理を行う場合、コンテナオブジェクトに処理を行えば1回の実行で済みます。Accountingコンテナ(Databaseアプリケーション、Bookkeepersグループ、LaserPrinterプリンタ、およびAmy、Bill、Bobというユーザが含まれている)内の全オブジェクトに対する完全な管理権限をユーザAmyに与える必要があるとします。

これを行うには、iManagerの［オブジェクトの表示］タブに移動し、左側のペインで**Accounting**オブジェクトの親ツリーを選択します。右側のペインで［**Accounting**］を選択して、［**アクション**］>［**トラスティの変更**］をクリックします。［**トラスティの追加**］をクリックして、Amyをトラスティとして追加します。次に、［**割り当てられた権利**］をクリックして、Amyに与える権利を選択します。これでAmyには、Databaseアプリケーション、Bookkeepersグループ、LaserPrinterプリンタ、および自分自身とユーザBill、Bobを管理する権利が与えられました。

継承

eDirectoryのもう1つの強力な機能は、権利の継承です。継承とは、ツリー内の上位層のコンテナの権利が、それぞれの下位層のすべてのコンテナに受け継がれることを意味します。この機能によって、権利の割り当て回数を少なくすることができます。たとえば、23 ページの 図 1-3に示すオブジェクトに対する管理権を与えるとします。

図 1-3 eDirectoryオブジェクトの例

次の割り当てのいずれかを行うことができます。

- ユーザにAllentownに対する権利を与えると、そのユーザはAllentownコンテナ内のオブジェクトのみ管理できます。
- ユーザにEastに対する権利を与えると、そのユーザはEast、Allentown、およびYorktownコンテナ内のオブジェクトを管理できます。
- ユーザにYourCoに対する権利を与えると、そのユーザは図中のすべてのコンテナのすべてのオブジェクトを管理できます。

権利の割り当ての詳細については、68 ページの 「eDirectoryでの権利」を参照してください。

Webベースの管理ユーティリティ

iManagerはブラウザベースのツールで、eDirectoryオブジェクトを運用、管理、設定するために使用します。iManagerでは、ユーザに特定のタスクや責任を割り当て、それらのタスクを実行するために必要なツール(およびそれに伴う権利)だけをユーザに付与することができます。

iManagerを実行するには、Microsoft Internet Explorer 6.0 SP1以降(推奨)、Mozilla 1.7以降、またはMozilla Firefox 0.9.2以降がインストールされているワークステーションが必要です。

重要: これら以外のWebブラウザでもiManagerにアクセスできる場合がありますが、完全な機能は保証されません。

---

iManagerを使用すると、次のようなスーパバイザの作業を実行できます。

- eDirectoryへのLDAPおよびXMLベースのアクセス設定
- ネットワークユーザ、デバイス、およびリソースを表すオブジェクトの作成
- 新規ユーザアカウント作成用のテンプレートの定義
- ネットワークオブジェクトの検索、変更、移動、および削除
- 管理権を委託する権利と職種の定義
- カスタムオブジェクトタイプとプロパティを作成するためのeDirectoryスキーマの拡張
- 複数のサーバでのeDirectoryデータベースのパーティション化とレプリカの作成
- DSRepair、DSMerge、バックアップおよび復元などのeDirectory管理ユーティリティの実行

その他にも、iManagerにロードされたプラグインに基づいた管理機能を実行できます。iManager 2.7には、次のeDirectoryプラグインがバンドルされています。

- eDirectory Backup and Restore
- eDirectory Log Files
- eDirectory Merge
- eDirectory Repair
- eDirectory Service Manager
- eGuideコンテンツ
- iManager基本コンテンツ
- インポート/エクスポート変換ウィザード
- インデックス管理

- iPrint
- LDAP
- ユニバーサルパスワードの強制
- 優先度同期
- 暗号化属性
- 暗号化レプリケーション
- NetIQ Licensing Services (NLS)
- NetIQモジュラー認証サービス(NMAS)
- PKI/Certificate
- フィルタ処理済レプリカ環境設定ウィザード
- ［SNMP］
- WAN Traffic Manager

iManagerのインストール、設定、および実行についての詳細は、『*NetIQ iManager 2.7 Administration Guide (NetIQ iManager 2.7管理ガイド)* (https://www.netiq.com/documentation/imanager/imanager_admin/data/bookinfo.html)』を参照してください。

シングルログインと認証

eDirectoryでは、ユーザはグローバルディレクトリにログインするため、ユーザごとに複数のサーバやドメインを管理する必要はありません。また、ドメイン間の信頼関係や通過時の認証を管理する必要もありません。

ディレクトリのセキュリティ機能の1つは、ユーザの認証です。ユーザがログインするためには、あらかじめユーザオブジェクトがディレクトリ内に作成されている必要があります。ユーザオブジェクトには、名前やパスワードといった、特定のプロパティがあります。

ユーザがログインすると、eDirectoryは入力されたパスワードとディレクトリに格納されているそのユーザのパスワードを照合し、一致した場合にアクセスを許可します。

オブジェクトクラスとプロパティ

eDirectoryオブジェクトの各タイプの定義を、オブジェクトクラスといいます。たとえば、「ユーザ」や「組織」は、オブジェクトクラスです。オブジェクトの各クラスには、それぞれ特定のプロパティがあります。たとえば、ユーザオブジェクトでは、名、姓、および他の多くのプロパティがあります。

スキーマでは、オブジェクトクラスとプロパティ、および包含ルール(どのコンテナにどのオブジェクトを保管するか)が定義されます。eDirectoryにはベーススキーマが付属しています。このベーススキーマは、ユーザまたはユーザが使用するアプリケーションによる拡張が可能です。スキーマの詳細については、51 ページの 「スキーマ」を参照してください。

コンテナオブジェクトは、他のオブジェジェクトを格納し、ツリーをさまざまな分岐に分割するために使用されます。一方、リーフオブジェクトはネットワークリソースを表します。

オブジェクトのリスト

次の表に、eDirectoryのオブジェクトクラスを示します。サービスを追加した場合は、表内のオブジェクトクラス以外のオブジェクトクラスがeDirectory内に新たに作成されることがあります。

eDirectoryコンテナオブジェクトクラス

iManagerアイコン	コンテナオブジェクト(略語)	説明
	ツリー	ツリーの開始点を表します。詳細については、28 ページの「ツリー」を参照してください。
	カントリ(C)	ネットワークが存在する国を表します。その下には、国内の他のディレクトリオブジェクトが編成されます。詳細については、30 ページの 「国」を参照してください。
	ライセンスコンテナ(LC)	NLS (NetIQ Licensing Services)技術を使用してライセンス許可証をインストールした場合やメータリング許可証を作成した場合に、自動的に作成されます。NLS対応のアプリケーションをインストールすると、LCコンテナオブジェクトがツリーに追加され、ライセンス許可証リーフオブジェクトがそのコンテナに追加されます。
	組織(O)	ディレクトリ内の他のオブジェクトの編成に使用されます。組織オブジェクトは、カントリオブジェクトの直下に配置されます(カントリオブジェクトを作成している場合)。詳細については、28 ページの 「組織」を参照してください。
	部門(OU)	ディレクトリ内の他のオブジェクトをさらに細かく編成するために使用されます。部門オブジェクトは、組織オブジェクトの直下に配置されます。詳細については、29 ページの 「部門」を参照してください。
	ドメイン(DC)	ディレクトリ内の他のオブジェクトをさらに細かく編成するために使用されます。ドメインオブジェクトは、Treeオブジェクトの下、または組織、部門、カントリ、および地域オブジェクトの下に作成されます。詳細については、31 ページの 「ドメイン」を参照してください。

eDirectoryリーフオブジェクトクラス

iManagerアイコン	Leaf Object (リーフオブジェクト)	説明
	AFPサーバ	eDirectoryネットワーク内のノードとして機能する、AppleTalk*ファイリングプロトコルサーバを表します。通常、複数のMacintosh*コンピュータに対するルータおよびAppleTalkサーバとしても機能します。
	別名	ディレクトリ内にあるオブジェクトの実際の位置を指します。別名を使用することによって、ディレクトリ内のディレクトリオブジェクトを、実際の場所とは異なる場所に存在するように表示できます。詳細については、46 ページの 「別名」を参照してください。

iManagerアイコン	Leaf Object (リーフオブジェクト)	説明
	Application (アプリケーション)	ネットワークアプリケーションを表します。アプリケーションオブジェクトによって、権利の割り当て、ログインスクリプトのカスタマイズ、およびアプリケーションの起動のような、管理作業を簡素化できます。
	コンピュータ	ネットワーク内のコンピュータを表します。
	ディレクトリマップ	ファイルシステム内のディレクトリを表します。詳細については、47 ページの 「ディレクトリマップ」を参照してください。
	グループ	ディレクトリ内のユーザオブジェクトのリストに名前を割り当てます。権利をそれぞれのユーザに割り当てる代わりに、グループに割り当てることができます。こうすると、グループ内の各ユーザに権利が与えられます。詳細については、35 ページの 「グループ」を参照してください。
	ライセンス許可証	プロダクトライセンス許可証をデータベースのオブジェクトとしてインストールするために、NLS技術とともに使用されます。NLS対応アプリケーションをインストールすると、ライセンス許可証オブジェクトがライセンスプロダクトコンテナに追加されます。
	職種	組織内での地位や職種を定義します。
	プリントキュー	ネットワークのプリントキューを表します。
	Print Server	ネットワークのプリントサーバを表します。
	プリンタ	ネットワークのプリンタを表します。
	プロファイル	共通のログインスクリプトコマンドを共有するユーザグループが使用するログインスクリプトを表します。これらのユーザは同じコンテナに属する必要はありません。詳細については、48 ページの 「プロファイル」を参照してください。
	サーバ	任意のオペレーティングシステムが動作するサーバを表します。詳細については、32 ページの 「サーバ」を参照してください。
	テンプレート	新しいユーザオブジェクトに適用する標準のユーザオブジェクトプロパティを表します。
	不明	iManagerにカスタムアイコンが存在しないオブジェクトを表します。
	User (ユーザ)	ネットワークを使用する人を表します。詳細については、33 ページの 「User (ユーザ)」を参照してください。
	ボリューム	ネットワーク上の物理的なボリュームを表します。詳細については、32 ページの 「ボリューム」を参照してください。

コンテナオブジェクトクラス

- 28 ページの 「ツリー」
- 28 ページの 「組織」

- 29 ページの 「部門」
- 30 ページの 「国」
- 31 ページの 「ドメイン」

ツリー

 ネットワーク内のサーバにeDirectoryを初めてインストールすると、ツリーコンテナ(以前の［ルート］)が作成されます。最上位のコンテナであるTreeコンテナには、通常、組織オブジェクト、カントリオブジェクト、または別名オブジェクトが格納されます。

Treeが表す内容

Treeコンテナはツリーの最上部を表します。

使用法

Treeは、包括的な権利の割り当てに使用します。Treeに対して行った権利の割り当ては、継承機能によって、ツリー内のすべてのオブジェクトに適用されます。68 ページの 「eDirectoryでの権利」を参照してください。デフォルトで、トラスティ［Public］はTreeに対するブラウズ権を所有し、AdminはTreeに対するスーパバイザ権を所有します。

重要なプロパティ

- Treeオブジェクトは名前プロパティを持っています。名前プロパティは、最初のサーバのインストール時に指定されたツリー名を表します。ツリー名はiManagerの階層に表示されます。
- ツリー名は32文字以下にする必要があります。

組織

 ネットワーク内のサーバにeDirectoryを初めてインストールすると、組織コンテナオブジェクトが作成されます。通常、組織コンテナは最上部のTreeコンテナの直下に作成され、コンテナ内には部門オブジェクトとリーフオブジェクトが格納されます。

デフォルトでは、最初の組織コンテナに、Adminという名のユーザオブジェクトが作成されます。

組織オブジェクトが表す内容

通常、組織オブジェクトは会社を表しますが、Treeの下に組織オブジェクトを追加作成することもできます。一般的に、組織オブジェクトの追加作成は、さまざまな地区で構成されるネットワークや、独立した複数のeDirectoryツリーがマージされているネットワークで行われます。

使用法

ツリーでの組織オブジェクトの運用方法は、ネットワークのサイズと構造により異なります。小規模のネットワークでは、1つの組織オブジェクトの下にすべてのリーフオブジェクトを配置します。

大規模なネットワークでは、組織オブジェクトの下に部門オブジェクトを作成します。これにより、リソースの検索と管理を容易化できます。たとえば、社内の各部署や事業部ごとに部門オブジェクトを作成できます。

複数のサイトがあるネットワークでは、組織オブジェクトの下に各サイトを表す部門オブジェクトを作成します。ディレクトリを分割するためのサーバ数が十分にあれば(または設置の計画があれば)、このようにサイトの境界で論理的にパーティションを区切ることができます。

プリンタ、ボリューム、アプリケーションといった、社内全体で使用するリソースを共有しやすくするために、組織の直下に、対応するプリンタ、ボリューム、アプリケーションのオブジェクトを作成します。

重要なプロパティ

組織オブジェクトの最も有用なプロパティを次に示します。名前プロパティは必須です。すべてのプロパティの一覧を表示するには、iManagerで組織オブジェクトを選択します。プロパティの各ページの説明を表示するには、［ヘルプ］をクリックします。

- 名前

  通常、名前プロパティは会社名と同じです。簡素化のために短くすることもできます。たとえば、会社名がYour Shoe Companyの場合、YourCoとすることができます。

  組織名は、その下に作成されるすべてのオブジェクトのコンテキストの一部として使用されます。
- ログインスクリプト

  ログインスクリプトプロパティには、組織の直下にあるユーザオブジェクトが実行するコマンドが格納されます。これらのコマンドは、ユーザのログイン時に実行されます。
- 組織名の長さは64文字以下にする必要があります。

部門

 ツリーを細分化するために部門(OU)コンテナオブジェクトを作成することができます。部門は、iManagerで、組織、カントリ、または別の部門オブジェクトの下に作成されます。

部門には、ユーザオブジェクトやアプリケーションオブジェクトといった、他の部門やリーフオブジェクトを格納できます。

部門オブジェクトが表す内容

通常は、部門オブジェクトは1つの部署を表し、互いにアクセスする必要があるオブジェクトのセットを格納します。部門オブジェクトの主な格納内容として、ユーザのセット、およびユーザが使用するプリンタ、ボリューム、アプリケーションなどを挙げることができます。

部門オブジェクトの最上位レベルに配置された各部門は、WANリンクごとに区切られたネットワークの各サイトを表します。

使用法

ツリーでの部門オブジェクトの運用方法は、ネットワークのサイズと構造により異なります。小規模のネットワークでは、部門オブジェクトを作成する必要がない場合もあります。

大規模なネットワークでは、組織オブジェクトの下に部門オブジェクトを作成します。これにより、リソースの検索と管理を容易化できます。たとえば、社内の各部署や事業部ごとに部門オブジェクトを作成できます。ユーザオブジェクトと、ユーザが頻繁に使用するリソースを一緒に部門オブジェクトに格納すると、管理が最も容易になります。

複数のサイトがあるネットワークでは、組織オブジェクトの下に各サイトを表わす部門オブジェクトを作成します。ディレクトリを分割するためのサーバ数が十分にあれば、このようにサイトの境界で論理的にパーティションを区切ることができます。

重要なプロパティ

部門オブジェクトの最も有用なプロパティを次に示します。名前プロパティは必須です。すべてのプロパティの一覧を表示するには、iManagerで部門オブジェクトを選択します。プロパティの各ページの説明を表示するには、［ヘルプ］をクリックします。

- 名前

  通常、名前プロパティは部署名と同じです。簡素化のために短くすることもできます。たとえば、部署名がAccounts Payableの場合、省略してAPとすることができます。

  部門名は、その下に作成されるすべてのオブジェクトのコンテキストの一部として使用されます。
- ログインスクリプト

  ログインスクリプトプロパティには、部門の直下にあるユーザオブジェクトが実行するコマンドが格納されます。これらのコマンドは、ユーザのログイン時に実行されます。
- 部門名は64文字まで指定できます。

国

 iManagerを使用して、国オブジェクトをツリーオブジェクトの直下に作成できます。国オブジェクトは、特定のX.500グローバルディレクトリに接続する場合にのみ必要です。

国オブジェクトが表す内容

国オブジェクトは、ツリーの分岐の国名を表します。

使用法

ネットワークが複数の国に渡っている場合でも、管理者は通常、国オブジェクトを作成しません。これは、国オブジェクトがツリーに不要なレベルを追加するだけだからです。ネットワークが複数の国家で構成されている場合は、必要に応じて、Treeオブジェクトの下に1つ以上の国オブジェクトを作成できます。国オブジェクトには、組織オブジェクトのみ格納できます。

国オブジェクトを作成していない場合でも、後で必要になった時には、随時ツリーを変更して国オブジェクトを追加できます。

重要なプロパティ

- 国オブジェクトには、2文字の名前プロパティがあります。国オブジェクト名には、US、UK、またはDEといった、2文字の標準コードが使用されます。
- カントリ名は2文字を超えることができません。

ドメイン

 iManagerを使用して、ドメインオブジェクトをツリーオブジェクトの直下に作成できます。また、組織、部門、国、および地域オブジェクトの下にも作成できます。

ドメインオブジェクトが表す内容

ドメインオブジェクトは、DNSドメインのコンポーネントを表します。ドメインオブジェクトを使用すると、ドメインネームシステムによって示されるサービスリソースレコードの場所(DNS SRV)に基づいて、ツリー内のサービスを検索できます。

ドメインオブジェクトを使用すると、ツリーは次のように表されます。

DS=Novell.DC=Provo.DC=USA

この例では、すべてのサブコンテナがドメインになっています。次のように、異なるツリーが混在する場合にもドメインオブジェクトを使用できます。

DC=Novell.O=Provo.C=USA

または

OU=Novell.DC=Provo.C=USA

通常、先頭のドメインはTree全体を表し、サブドメインはそのTreeの下位の部分を表します。たとえばmachine1.novell.comをツリーで表すと、DC=machine1.DC=novell.DC=comとなります。ドメインは、eDirectoryツリーの設定で使用される一般的な方法です。コンテナおよびサブコンテナがすべてDCオブジェクトである場合は、オブジェクトを検索するときに、C、O、またはOUを意識する必要はありません。

使用法

ドメイン名の長さは64文字以下にする必要があります。

リーフオブジェクトクラス

サーバ

 サーバにeDirectoryをインストールすると、そのサーバのオブジェクトがツリー内に自動作成されます。このオブジェクトクラスは、eDirectoryが動作しているいずれかのサーバを表します。

サーバオブジェクトが表す内容

サーバオブジェクトは、eDirectoryを実行しているサーバまたはバインダリベースのサーバを表します。

使用法

サーバオブジェクトはレプリケーション処理のリファレンスポイントの役目を果たします。バインダリベースのサーバを表すサーバオブジェクトでは、iManagerでそのサーバのボリュームを管理できます。

重要なプロパティ

サーバオブジェクトの主なプロパティとして、ネットワークアドレスプロパティがあります。ネットワークアドレスプロパティには、そのサーバのプロトコルとアドレス番号が表示されます。これはパケットレベルでのトラブルシューティングに役立ちます。

すべてのプロパティの一覧を表示するには、iManagerでサーバオブジェクトを選択します。プロパティの各ページの説明を表示するには、［**ヘルプ**］をクリックします。

ボリューム

 サーバ上に物理ボリュームを作成すると、ツリー内にボリュームオブジェクトが自動作成されます。デフォルトでは、サーバ名にアンダースコアと物理ボリューム名を追加したものが、ボリュームオブジェクトの名前になります(たとえばYOSERVER_SYS)。

Linuxファイルシステムのパーティションは、ボリュームオブジェクトを使用して管理することはできません。ボリュームオブジェクトはOES Linuxでのみサポートされます。

ボリュームオブジェクトが表す内容

ボリュームオブジェクトは、サーバ上の物理ボリューム(書き込み可能ディスクやCDなどのストレージメディア)を表します。eDirectory内のボリュームオブジェクトには、そのボリューム内のファイルやディレクトリに関する情報は含まれませんが、iManagerを使用すれば、それらの情報にアクセスできます。ファイルおよびディレクトリに関する情報は、ファイルシステム自体に保存されます。

使用法

iManagerで［**ボリューム**］アイコンをクリックすると、そのボリュームにあるファイルやディレクトリを管理できます。ボリュームの空きディスク容量、ディレクトリエントリ領域、および圧縮の統計に関する情報がiManagerによって提供されます。

重要なプロパティ

必須の名前プロパティおよびホストサーバプロパティに加えて、ボリュームオブジェクトには他にも重要なプロパティがあります。

- 名前

  ツリー内のボリュームオブジェクトの名前です。デフォルトでは、この名前は物理ボリュームの名前に基づいて付けられますが、変更も可能です。
- Host Server

  ボリュームが存在するサーバの名前です。
- バージョン

  これは、ボリュームをホストしているサーバのeDirectoryのバージョンです。

User (ユーザ)

 ユーザオブジェクトは、ログインで必要とされます。ツリーに最初のサーバがインストールされると、Adminというユーザオブジェクトが作成されます。初回ログイン時には、Adminとしてログインします。

ユーザオブジェクトの作成またはインポートには、次の機能を使用できます。

- iManager

  iManagerの詳細については、『*NetIQ iManager 2.7 Administration Guide (NetIQ iManager 2.7管理ガイド)* (https://www.netiq.com/documentation/imanager/imanager_admin/data/bookinfo.html)』を参照してください。

- データベースファイルからのバッチ処理

  バッチファイルの使用の詳細については、82 ページの 「eDirectoryツリーの設計」を参照してください。

ユーザオブジェクトが表す内容

ユーザオブジェクトはネットワークを使用するユーザを表します。

使用法

ネットワークを使用するユーザ全員に対して、ユーザオブジェクトを作成します。ユーザオブジェクトは個別に管理することもできますが、次のようにすると時間の節約になります。

- テンプレートオブジェクトを使用して、通常のユーザオブジェクトのデフォルトのプロパティを設定する。新しく作成するユーザに対して、自動的にテンプレートが適用されます(既存のユーザには適用されません)。
- ユーザのセットを一括管理するためのグループオブジェクトを作成する。
- コンテナオブジェクトをトラスティとして使用して、権利を割り当てる。これにより、権利の割り当てをコンテナ内のユーザオブジェクトすべてに適用できます。
- 複数のユーザオブジェクトは、<Shift>または<Ctrl>を押してクリックすると選択できます。これにより、選択したすべてのユーザオブジェクトのプロパティ値を一度に変更できます。

重要なプロパティ

ユーザオブジェクトには80を超えるプロパティがあります。すべてのプロパティの一覧を表示するには、iManagerでユーザオブジェクトを選択します。プロパティの各ページの説明を表示するには、［ヘルプ］をクリックします。

ログイン名プロパティと姓プロパティは必須です。これら必須のプロパティおよび、他の有用なプロパティを次に示します。

- ［Account Expiration Date］では、ユーザアカウントの有効期限を設定できます。有効期限を過ぎた後は、アカウントはロックされ、ユーザはログインできなくなります。
- ［アカウント使用不可］には、アカウントがロックされ、ユーザがログインできない状態であることを示すシステム生成の値があります。ロックは、アカウントの有効期限が切れた場合や、ユーザが不正なパスワードを連続して何度も入力した場合などに発生します。
- ［定期的なパスワード強制変更］によって、一定期間ごとにパスワードの変更をユーザに要求し、セキュリティの強化を図ることができます。

- ［グループメンバーシップ］は、ユーザがメンバーとして含まれているすべてのグループオブジェクトを示します。
- ［最終ログイン時刻］はシステムが生成するプロパティで、ユーザが最後にログインした日時を示します。
- ［姓］は必須ですが、eDirectoryが直接使用することはありません。eDirectoryネームベースを利用するアプリケーションが、名、役職、位置、Fax番号など、他の識別プロパティとともに、このプロパティを使用する場合があります。
- ［同時接続数の制限］では、ユーザがネットワークで開くことができるセッションの最大数を設定できます。
- ［ログイン名］はiManagerで［ユーザ］アイコンによって表示される名前です。また、ログイン時にユーザが入力する名前でもあります。

  eDirectoryでは、各コンテナ内で固有のログイン名を使用する必要がありますが、ネットワーク内の別のコンテナ間では同じログイン名を使用できます。ただし、社内全体で固有のログイン名を使用した方が、管理を単純化できます。

  一般に、ログイン名には姓と名の組み合わせが使用されます。たとえば、Steve Jonesの場合は、STEVEJやSJONESのようになります。
- ［ログインスクリプト］では、個々のユーザオブジェクトの特定のログインコマンドを作成できます。ユーザのログイン時には、最初にコンテナログインスクリプトが実行されます。次に、ユーザオブジェクトがプロファイルオブジェクトのメンバーシップリストに登録されている場合は、プロファイルログインスクリプトが実行されます。最後に、ユーザのログインスクリプトが実行されます(スクリプトが存在する場合)。

  管理に要する時間を節約するため、ログインコマンドのほとんどの部分はコンテナのログインスクリプトに保管するようにします。ユーザログインスクリプトを編集すると、共通の必要条件に対する例外に対処できます。
- ［ログイン時間制限］では、ユーザがログインできる時刻と曜日を設定できます。
- ［ネットワークアドレス］には、ユーザのログイン元であるIPX™アドレスやIPアドレスをすべて示すシステム生成の値が格納されます。これらの値は、パケットレベルでのネットワークの問題のトラブルシューティングに役立ちます。
- ［パスワード要求］では、パスワードの入力をユーザに要求するかどうかを指定できます。他の関連プロパティでは、パスワード長などの一般的なパスワード制限を設定できます。
- ［Rights to Files and Directories］は、ユーザに割り当てられた、ファイルシステムに対するすべての権利を示します。iManagerを使用して、ファイルおよびディレクトリに対するユーザの有効な権利(他のオブジェクトから継承されたものを含む)を確認することもできます。

グループ

 グループオブジェクトを作成すると、ユーザオブジェクトをセットで管理できます。

グループオブジェクトが表す内容

グループオブジェクトは、ユーザオブジェクトのセットを表します。

使用法

コンテナオブジェクトではコンテナ内のすべてのユーザオブジェクトを管理でき、グループオブジェクトでは1つまたは複数のコンテナ内のサブセットを管理できます。

グループオブジェクトは、次の2つの主な目的に対して使用されます。

- 多数のユーザオブジェクトに、一度に権利を与える。
- IF MEMBER OF構文を使用して、ログインスクリプトコマンドを指定する。

スタティックグループ

スタティックグループでは、メンバーオブジェクトを明示的に指定します。各メンバーは、グループに明示的に割り当てられます。

これらのグループでは固定したメンバーのリストが示され、また、グループのメンバーリストと、オブジェクト上で属性を持つメンバーとの間の参照整合性を提供します。グループメンバーシップは、メンバーの属性によって明示的に管理されます。

ダイナミックグループ

ダイナミックグループでは、LDAPURLを使用して規則のセットを定義します。この規則に従って、eDirectoryのユーザオブジェクトに一致したときに、グループのメンバーが定義されます。ダイナミックグループのメンバーは、URLに指定された検索フィルタによって定義される共通の属性を共有します。LDAP URLの形式に関する詳細は、RFC 2255 (http://www.ietf.org/rfc/rfc2255.txt)を参照してください。

ダイナミックグループを使用すると、グループのメンバーシップを評価する際に使用される条件を指定できます。グループの実際のメンバーは、eDirectoryによって動的に評価されます。つまり、論理的にグループ化することでグループのメンバーを定義するため、eDirectoryはグループのメンバーを自動的に追加または削除できます。この拡張性の高いソリューションによって、管理コストを低減でき、LDAPの通常のグループに高い柔軟性を補うことができます。

eDirectoryでは、任意の属性に基づいてユーザを自動的にグループ化したり、一致する識別名(DN)を含む特定のグループに対してACLを適用したりする場合に、ダイナミックグループを作成できます。たとえば、部署=マーケティングという属性を持つすべてのDNを自動的に含むグループを作成できます。部署=マーケティングという検索フィルタを適用すると、部署=マーケティングの属性を持つすべてのDNを含むグループが検索結果として返されます。その後、このフィルタに基づく検索結果からダイナミックグループを定義できます。部署=マーケティングという条件に一致するユーザがディレクトリに追加されると、このグループにも自動的に追加されます。部署が他の値に変更されたユーザ(またはディレクトリから削除されたユーザ)は、グループから自動的に削除されます。

eDirectoryでダイナミックグループを作成するには、objectclass=dynamicGroupというタイプのオブジェクトを作成します。スタティックグループオブジェクトをダイナミックグループに変換するには、補助クラスdynamicGroupAuxをグループオブジェクトに関連付けます。ダイナミックグループは、グループに関連付けられたmemberQueryURL属性を持ちます。

dgIdentity属性は、ダイナミックグループオブジェクト上で、グループのダイナミックメンバーを拡張するために使用される証明書と権利を持つエントリの識別名に設定することができます。

グループは、memberQueryURLを使用して管理されます。基本的なmemberQueryURLには、ベースDN、スコープ、フィルタ、およびオプション拡張があります。ベースDNは検索ベースを指定します。スコープはベース内の検索レベルを指定します。フィルタは、指定したスコープ内で選択されたエントリに基づく検索フィルタです。

注: memberQueryURLによって作成されたリストに例外を設定するため、ダイナミックグループでもユーザを明示的に含めたり、除外したりできます。

ダイナミックグループは、NetIQ iManagerを使用して作成および管理できます。［役割およびタスク］ページの［**グループ**］役割をクリックすることで、グループ管理タスクにアクセスできます。

また、LDAPコマンドを使用してもグループを管理できます。ダイナミックグループに関連付けられた最も有用なプロパティは、dgIdentityおよびmemberQueryURLです。

重要なプロパティ

グループオブジェクトの最も有用なプロパティは、メンバープロパティとファイル/ディレクトリへの権利プロパティです。すべてのプロパティの一覧を表示するには、iManagerでグループオブジェクトを選択します。プロパティの各ページの説明を表示するには、［**ヘルプ**］をクリックします。

- dgAllowDuplicates

  ダイナミックグループメンバーの印刷で重複が許されるかどうかを指定します。デフォルトでは、［TRUE］が選択されています。

- dgIdentity

  このプロパティはDNを保持します。ダイナミックグループは、このDNの識別子を検索時の認証用に使用します。識別子は、ダイナミックグループと同じパーティション上に存在する必要があります。dgIdentityによって指定されたオブジェクトは、memberQueryURL属性で指定された検索を実行するのに必要な権利を持っている必要があります。

  たとえば、memberQueryURLが次のような値であるとします。

  ```
  l"dap:///o=nov??sub?(title=*)
  ```

  この場合、dgIdentityは、コンテナo=nov以下の属性タイトルに対する読み込み/比較権利を持っている必要があります。

- dgTimeout

  このプロパティは、サーバがタイムアウトになるまでにかかるメンバーの属性の読み込みまたは比較の最大所要時間を指定します。サーバがこのdgTimeout値を超えると、-6016エラーが表示されます。

- memberQueryURL

  このプロパティは、グループメンバーの属性と照合する規則のセットを定義します。

  memberQueryURLは、そのスキーマ定義に従って複数の値を持つ属性です。memberQueryURLは複数の値を持ちますが、eDirectory 8.6.1では、memberQueryURLの最初の値のみが使用されていました。

  次に例を示します。

  管理者によって作成されたダイナミックグループに、次のような2つのmemberQueryURL値があるとします。

  ```
  l"dap:///o=nov??sub?cn=*
  ```

  ```
  l"dap:///o=org??sub?cn=*
  ```

  eDirectory 8.6.*x*サーバは、グループのメンバーの計算に「ldap:///o=nov??sub?cn=*」を使用します。複数のクエリが許可されますが、読み込まれるのは最初のクエリだけです。

この制約事項はeDirectory 8.7以降で解消されました。eDirectoryサーバは、すべてのmemberQueryURL値に基づいてメンバーを計算するようになったため、そのメンバーセットは個々のmemberQueryURL値を使って計算されたメンバーの和集合になります。

上の例では、結果としてダイナミックグループのメンバーは、o=orgおよびo=novの場合にcn値を持つすべてのエントリとなります。

- member

  このプロパティは、グループ内のすべてのオブジェクトを示します。グループオブジェクトに割り当てられた権利は、そのグループのすべてのメンバーに適用されます。ダイナミックグループのmemberプロパティに値を追加すると、ダイナミックグループにスタティックメンバーが追加されます。この方法は、個別にメンバーを追加する場合に使用できます。

- excludedMember

  このプロパティは、ダイナミックグループのメンバーシップリストから特に除外されたDNを格納します。これは、ダイナミックグループの除外リストを作成するのに使用できます。

  excludedMemberによって、DNをダイナミックグループのダイナミックメンバーから除外されるようにします。

  こうすると、memberQueryURLによって指定されたメンバーの基準で選択された場合にのみ、DNはダイナミックグループのダイナミックメンバーになり、excludedMemberとしてリストされたり、uniqueMemberやmemberに明示的に追加されたりすることはありません。

- staticMember

  このプロパティは、ダイナミックグループのスタティックメンバーを読み込むだけではなく、DNがダイナミックグループのスタティックメンバーかどうかも判断します。また、DNが唯一のスタティックメンバーであるダイナミックグループを探し、ダイナミックメンバーを持っているが、スタティックメンバーを持たないグループを探すこともできます。

  このプロパティを既存のダイナミックグループに追加するには、dgstatic.schを使用してスキーマを拡張します。

eDirectory 8.6.1より前のデータベースのダイナミックグループを更新する

ダイナミックグループがローカルで作成されるか、同期の一部として取得されると、ダイナミックグループオブジェクトが作成されますが、ダイナミックグループの機能は、それらのオブジェクトに格納されるいくつかの内部値を必要とします。

古いサーバでもダイナミックグループを格納できますが、値を生成することはできません。ダイナミックグループはeDirectory 8.6.1で導入されたためです。

eDirectory 8.6.2では、eDirectory 8.6.1データベースに適合させるために、8.6.1以前のデータベースのダイナミックグループオブジェクトが自動で更新されました。

memberQueryURLの追加構文のサポート

memberQueryURL属性は、ダイナミックグループのメンバーを計算するためにeDirectoryサーバが使用する検索フィルタを格納できます。

eDirectory 8.6.1では、フィルタで使用される属性の構文は、次の基本的な文字列型にのみ制限されていました。

- SYN_CE_STRING
- SYN_CI_STRING
- SYN_PR_STRING

- SYN_NU_STRING
- SYN_CLASS_NAME
- SYN_TEL_NUMBER
- SYN_INTEGER
- SYN_COUNTER
- SYN_TIME
- SYN_INTERVAL
- SYN_BOOLEAN
- SYN_DIST_NAME
- SYN_PO_ADDRESS
- SYN_CI_LIST
- SYN_FAX_NUMBER
- SYN_EMAIL_ADDRESS

eDirectory 8.7.3以降では、次の属性構文がmemberQueryURLの値として追加でサポートされています。

- SYN_PATH
- SYN_TIMESTAMP
- SYN_TYPED_NAME

eDirectory 8.6.1およびeDirectory 8.7.xの両方では、SYN_OCTET_STRINGやSYN_NET_ADDRESSのようなバイナリ構文は、memberQueryURL検索フィルタでサポートされません。

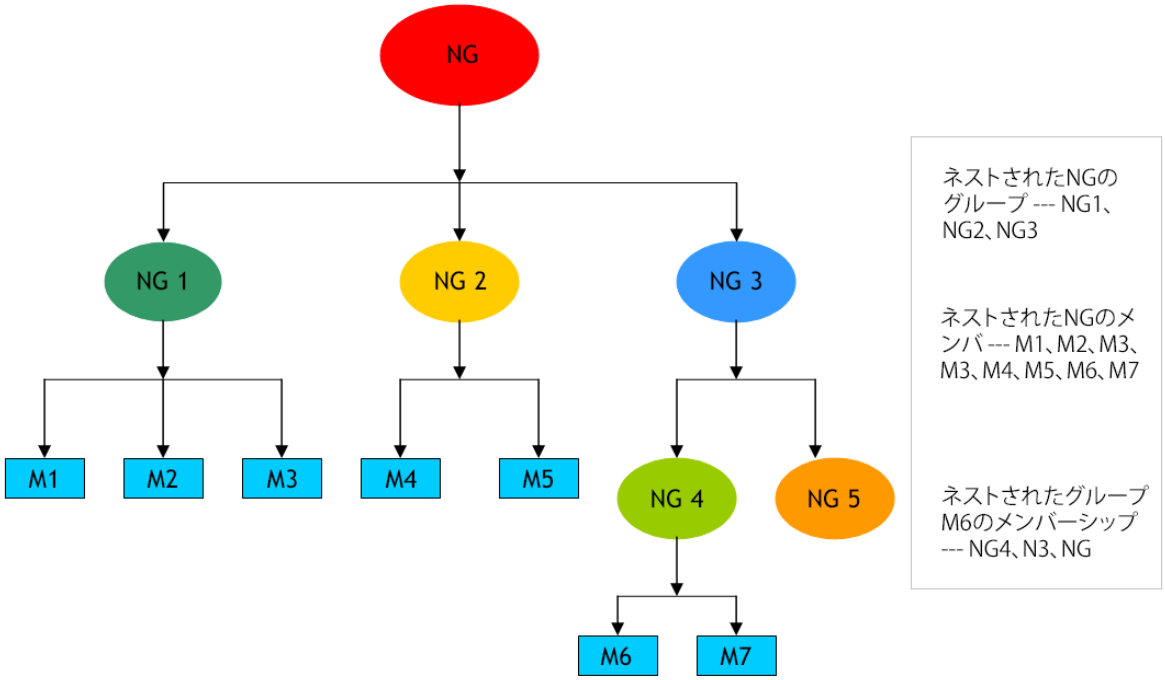
詳細については、「「How to Manage and Use Dynamic Groups in NetIQ eDirectory (NetIQ eDirectoryでダイナミックグループを管理および使用する方法)」 (http://support.novell.com/techcenter/articles/ana20020405.html)」を参照してください。

ネストされたグループ

ネストされたグループにより、グループをグループ化することができ、より構造化された形態のグループ化が可能になります。groupMember属性はネストされたグループを指定し、そのメンバーは、それを含有するネストされたグループオブジェクトのネストされたメンバーになります。グループオブジェクトはgroupMember属性で静的に指定されます。他のグループを含んでいるグループを「含有するグループ」といい、このグループに含まれているグループを「含有されるグループ」といいます。eDirectoryは、スタティック(静的)グループとダイナミック(動的)グループの両方のネストをサポートしています。最大で200レベルまでのネストが可能です。

重要: ネストは、ローカルサーバ内のみでサポートされます。含有されるグループがローカルサーバ上に見つからない場合、そのメンバーは、含有するグループのネストされたメンバーとしてリストされません。

図1-4 ネストされたグループ



iManagerまたはLDAPのツールを使用して、ネストされたグループを作成できます。

- 39 ページの 「LDAPツールを使用してネストされたグループを作成する」
- 40 ページの 「iManagerを使用してネストされたグループを作成する」

LDAPツールを使用してネストされたグループを作成する

LDAPツールを使用して、ネストされたグループを作成することができます。新しい補助クラスnestedGroupAuxを構造化クラスGroupと一緒に用いると、nestedGroupAuxはネストされたグループを表します。この補助クラスを既存のスタティックグループオブジェクトに追加すると、それがネストされたグループに変換されます。

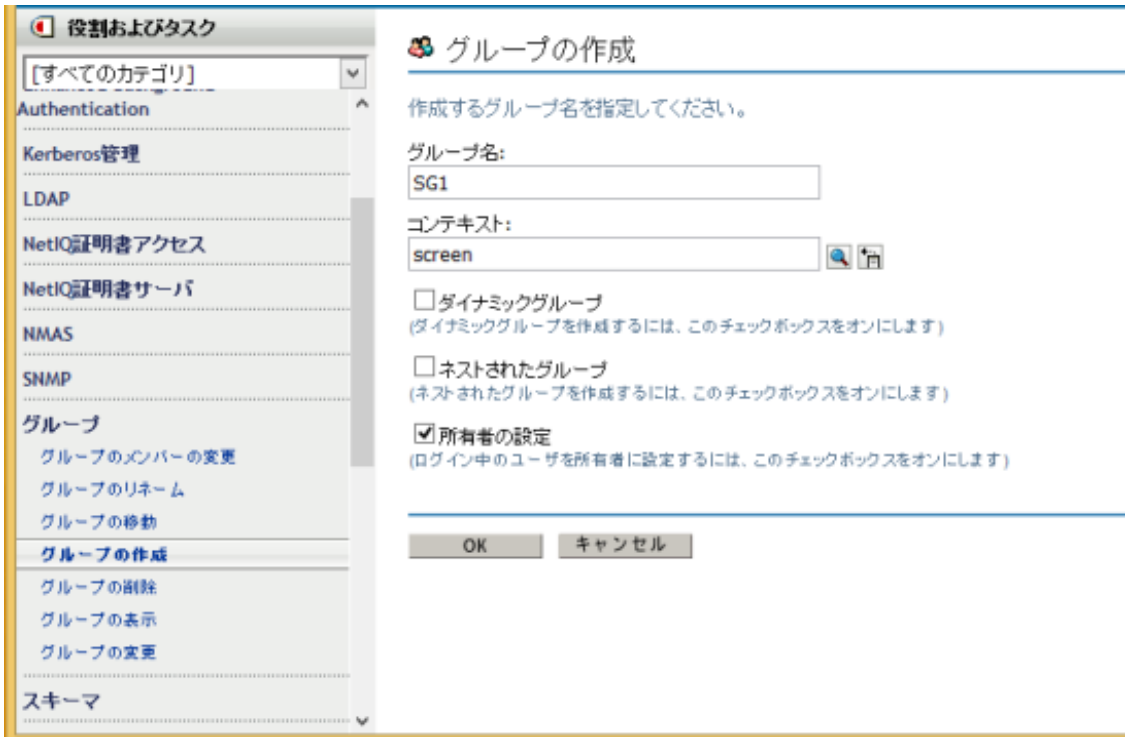
含有されるグループと含有するグループの両方が、ネストされたグループオブジェクトでなければなりません。含有されるグループがネストされたグループである場合にのみ、それにgroupMembership属性(groupMembership属性はスタティックグループには含まれません)を設定して、含有するグループを指定することができます。含有されるグループのタイプが含有するグループと同じでない場合は、含有されるグループのスタティックメンバーのみが、ネストされたメンバーとしてリストされます。

LDIFファイルおよびLDAPツールを使用して、そのようなグループを管理できます。ネストされたグループに関連する最も役立つプロパティは、groupMemberおよびnestedConfigです。

iManagerを使用してネストされたグループを作成する

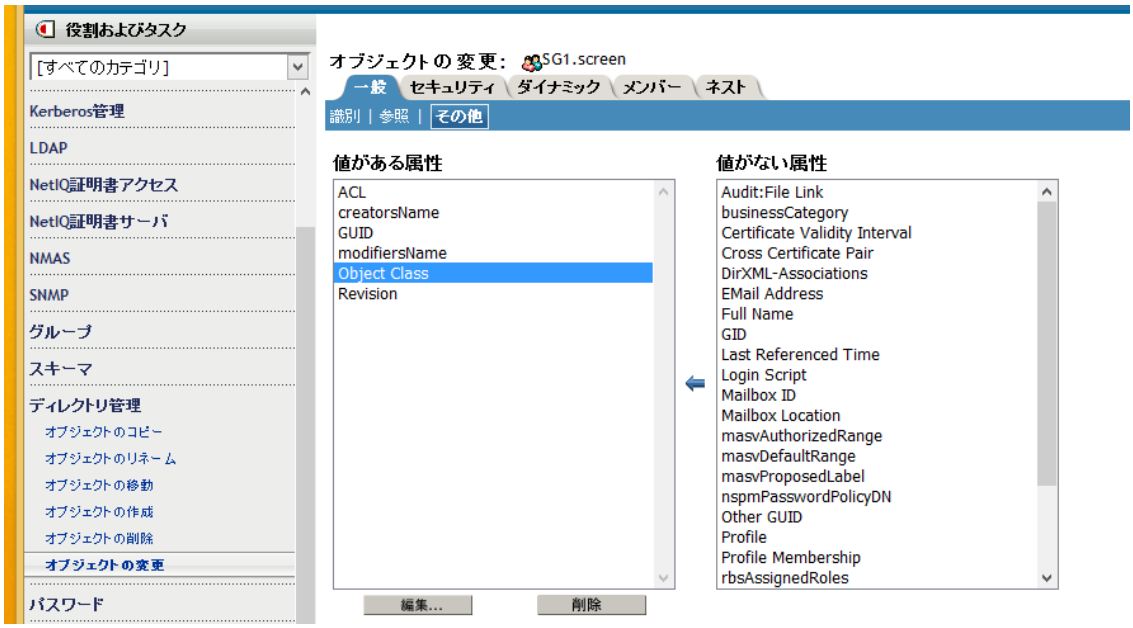
iManagerプラグインを使用して、ネストされたグループを作成したり、スタティックグループをネストされたグループに変更して別のグループにそれを関連付けたりすることができます。

1 管理者の資格情報を使ってiManagerにログインし、左側のパネルから［**グループ**］>［**グループの作成**］を選択して、スタティックグループを作成します。たとえば、SG1とします。



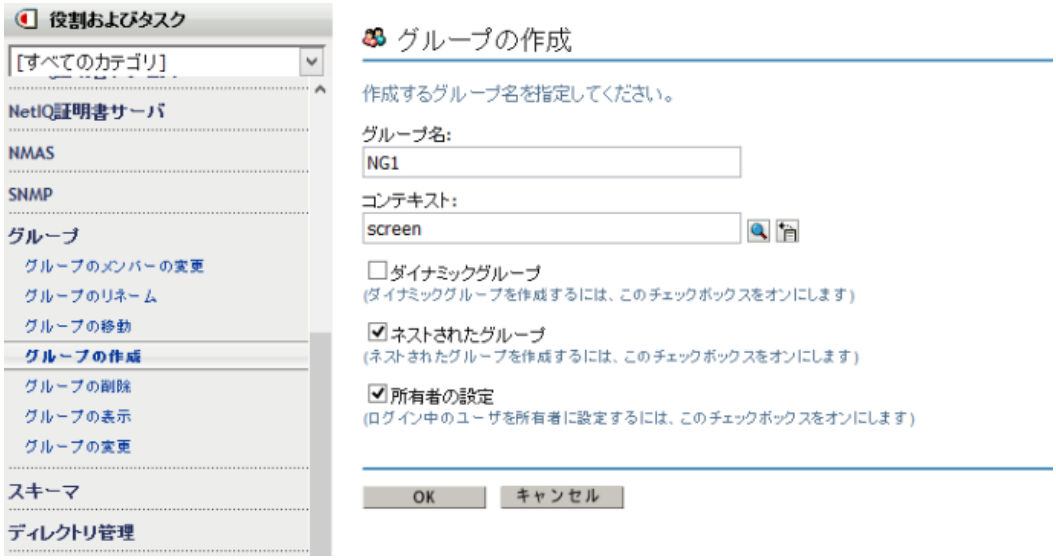
2 左側のパネルから［ディレクトリ管理］>［オブジェクトの変更］を選択し、ブラウズして*SG1.novell*オブジェクトを選択します。

3 ［その他］タブをクリックし、［値がない属性］リストから［オブジェクトクラス］を選択します。

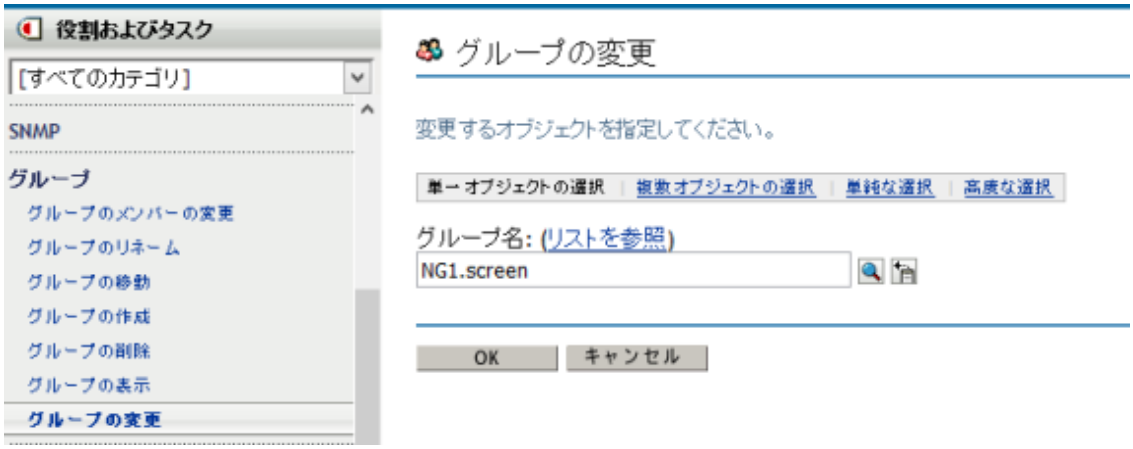


4 値nestedGroupAuxを［オブジェクトクラス］に追加して、［OK］および［適用］をクリックします。

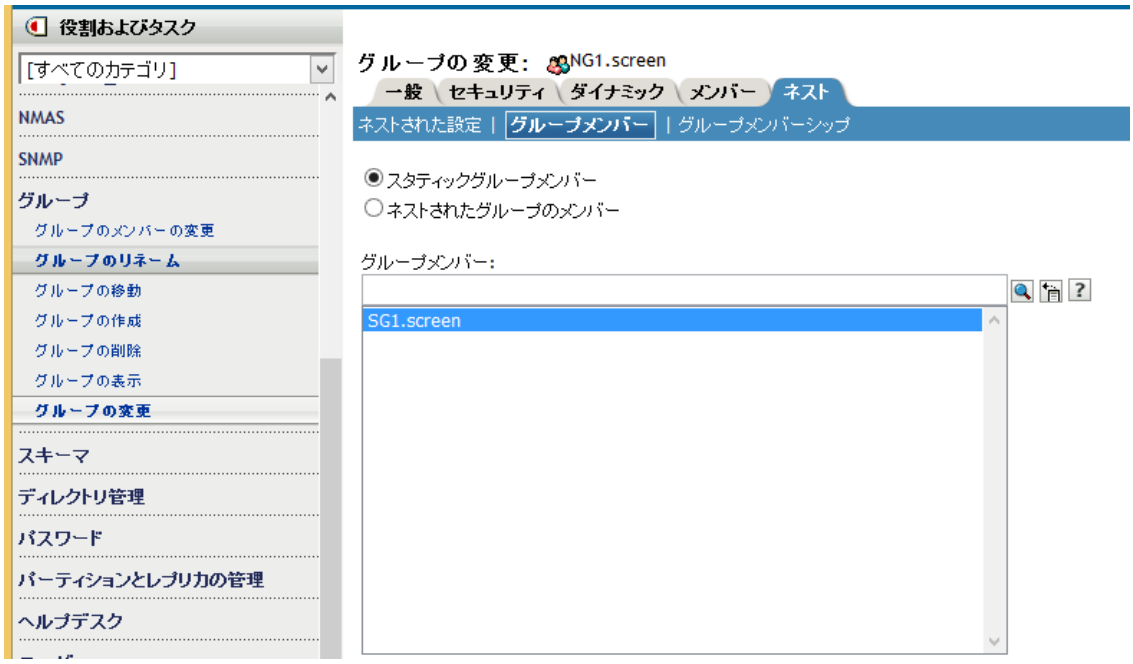
5 左側のパネルから［**グループ**］>［**グループの作成**］を選択し、［**ネストされたグループ**］チェックボックスを選択したうえで、作成するネストされたグループの名前としてNG1を指定し、［**OK**］をクリックします。



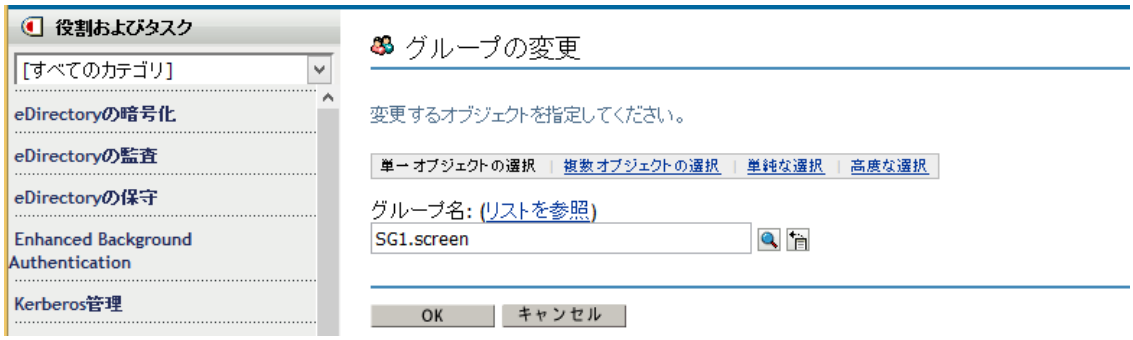
6 左側のパネルから［**グループ**］>［**グループの変更**］を選択し、［**ネストされたグループ**］チェックボックスを選択したうえで、変更するネストされたグループの名前としてNG1を指定し、［**OK**］をクリックします。



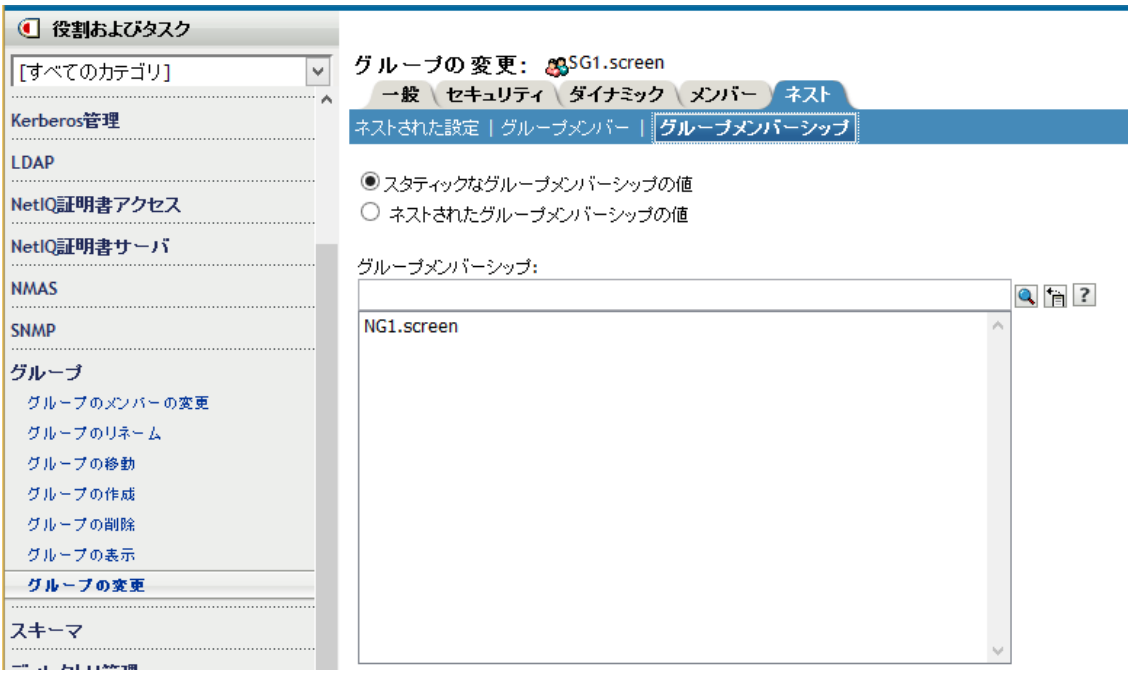
7 ネストされたグループを変更するために、［**グループ**］>［**グループの変更**］を選択し、**NG1.novell**をブラウズして選択します。



8 スタティックグループをNG1に関連付けるために、［ネスト］タブ>［グループメンバー］タブを選択し、SG1スタティックグループをブラウズして選択します。



9 ［適用］をクリックして［OK］をクリックすると、スタティックグループSG1がネストされたグループNG1に変換されます。



ネストされたグループに変換されたスタティックグループが、スタティックグループのメンバーになります。

SG1のメンバーシップの詳細を確認するには、左側のパネルから［グループ］>［グループの変更］を選択して、SG1.novellを選択します。［ネスト］>［グループメンバーシップ］タブを選択して、スタティックグループのメンバーシップ情報がNG1.novellであることを確認します。

ネストされたグループのプロパティ

- groupMember

  デフォルトで、ネストされたグループのメンバーには、すべてのネストされたメンバーが含まれます。したがって、member属性のリスト表示では常にすべてのネストされたメンバーが返され、member属性のアサーションではすべてのネストされたグループオブジェクトが返されます。設定を1 (ネストなし)にした場合は、直下のメンバーだけが対象となります。

- グループメンバーシップ

  groupMembershipは、このオブジェクト(通常はユーザオブジェクト)が属するグループを指定します。この属性はnestedGroupAuxクラスに関連付けられ、このグループがグループメンバーとなっているネストされたグループのDNを保持します。グループオブジェクトに関連付けられている場合、この属性は、そのグループがメンバー(正確にはgroupMember)になっているネストされたグループを示します。memberおよびgroupMemberと似た点として、groupMembershipのリストには、ネスト関係を通してそのグループがgroupMembershipを持っているすべてのネストされたグループが含まれます。さらに、groupMembership属性には、nestedConfigも適用されます。グループメンバーオブジェクト以外に対しては、個々のグループのnestedConfigが使用されます。

- nestedConfig

  nestedConfigは、ネストされたグループオブジェクトの環境設定を設定します。現在サポートされている設定値は、0 (ローカルサーバのネスト)および1 (ネストなし)です。デフォルトでは、常にローカルサーバをネストします。member、groupMember、groupMembershipなどの直接の値だけをその属性でリストするには、設定値を1にすることができます。

- excludedMember

  nestedGroupAuxクラスにはexcludedMemberが含まれていますが、この属性は現在使用されていません。ネストされたグループとダイナミックグループのクラスが両方とも同じグループに含まれている場合、excludedMemberはそのグループレベルのダイナミックメンバーにのみ適用されます。

ネストされたグループの操作

1. groupMember属性を使用して、あるグループを別のグループのメンバーにすることができます。含有されるグループと含有するグループのどちらのグループオブジェクトにも、ネストされたグループ補助クラスが関連付けられている必要があります。

   ```
   dn: cn=finance,o=nov

   objectclass: group

   objectclass: nestedGroupAux

   groupMember: cn=accounts,o=nov

   member: cn=jim,o=nov


   dn: cn=accounts,o=nov

   objectclass: group

   objectclass: nestedGroupAux

   member: cn=allen,o=nov

   member: cn=ESui,o=nov

   member: cn=YLi,o=nov
   ```

2. 含有されるグループと含有するグループの両方がサーバ上にローカルに存在する場合は、ネストされたグループのmember属性を読み込むと、含有されるグループのメンバーも返されます。

   ```
   dn: cn=finance,o=nov
   member: cn=jim,o=nov
   member: cn=allen,o=nov
   member: cn=ESui,o=nov
   member: cn=YLi,o=nov
   ```

   groupMember属性に関してもこれが当てはまります。

3. groupMembershipは、member属性の相互性属性です。つまり、ユーザオブジェクトcn=allen,o=novは、cn=accounts,o=novというグループDNが設定されたgroupMembership属性を持つ必要があります。cn=accounts,o=novグループのgroupMembershipには、cn=finance,o=novが設定されている必要があります。cn=allen,o=novユーザオブジェクトのgroupMembership属性を読み込むと、両方のグループが返されます。

   ```
   dn: cn=allen,o=nov
   groupMembership: cn=accounts,o=nov
   groupMembership: cn=finance,o=nov
   ```

4. ネストされたグループにACLを割り当てることができます。その場合、ネストされたグループのメンバーであるすべてのオブジェクトが権利を獲得します。［割り当てられた権利］フィールドでは、割り当てられている権利に加えて、ネストされたACLのビット(0x80000000)をさらに設定する必要があります。

```
dn: cn=finance,o=nov
groupMember: cn=accounts,o=nov


dn: cn=accounts,o=nov
member: cn=allen,o=nov


dn: ou=MyCo,o=nov
objectclass: Organizational Unit
ACL: 2147483650#entry#cn=finance,o=nov#[All Attributes Rights]
```

権利の値「–2147483650(0x80000002)」には、ネストされたACL(0x80000000)と読み取り権限ビット(0x00000002)が設定されています。したがって、ユーザオブジェクトcn=allen,o=novには、ネストされたグループcn=finance,o=novを介して、MyCoオブジェクトのすべての属性に対する読み取り権限が付与されます。

5. アプリケーションでは、member、groupMember、およびgroupMembership属性に対するフィルタアサーションを使用できます。上記の例では、member=cn=allen,o=novのアサーションによって以下が返されます。

   ```
   dn: cn=accounts,o=nov
   dn: cn=finance,o=nov
   ```

   groupMembership=cn=finance,o=novのアサーションによって次のオブジェクトが返されます。

   ```
   dn: cn=allen,o=nov
   dn: cn=jim,o=nov
   dn: cn=ESui,o=nov
   dn: cn=YLi,o=nov
   dn: cn=accounts,o=nov
   ```

注: 上記の例ではいずれも、ネストのレベルに制限はありません。上記のいずれの属性を読み込むときにも、ネストされたグループでループ検出が実行されます。

制限

- ネストされた関係の範囲がローカルサーバを超えることはありません。関係するオブジェクト、ユーザ、グループはサーバ上にローカルに存在する必要があります。
- メンバーシップリストでは、重複排除は行われません。
- 古いeDirectoryサーバ(バージョン8.8 SP1またはそれ以前)では、ネストされたACLもネストセマンティックもサポートされません。

別名

ツリー内の別のオブジェクトをポイントする別名オブジェクトを作成できます。別名オブジェクトによって、ユーザは自分の属するコンテナの外部にあるオブジェクトに、ローカル名を付けることができます。

コンテナの名前を変更するときには、必要に応じて、元のコンテナの位置に新しい名前をポイントする別名を作成できます。これにより、コンテナ内のオブジェクトを参照するログインスクリプトコマンドやワークステーションは、コンテナ名が更新されていなくても対象のオブジェクトにアクセスできます。

別名オブジェクトが表す内容

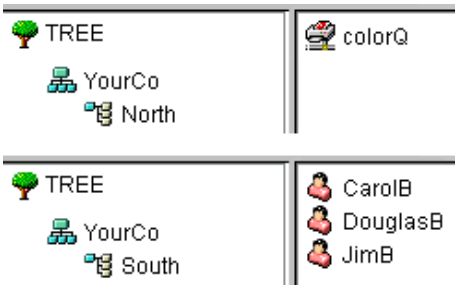
別名オブジェクトは、コンテナやユーザなど、ツリー内の別のオブジェクトを表します。別名オブジェクト自体にはトラスティ権はありません。別名オブジェクトに与えられたトラスティ権は、その別名オブジェクトが示している実際のオブジェクトに適用されます。ただし、別名をトラスティ割り当ての対象とすることもできます。

使用法

別名オブジェクトを作成すると、名前の解決が容易になります。オブジェクトの命名規則では、現在のコンテキストのオブジェクトに対する命名が最も簡単なため、現在のコンテキストに、現在のコンテキストの外部のリソースをポイントする別名オブジェクトを作成します。

たとえば、図 1-5に示すように、ユーザがSouthコンテナにログインし、現在のコンテキストを確立する場合に、NorthコンテナのColorQというプリントキューオブジェクトにアクセスする必要があるとします。

図 1-5 *コンテナの例*



に示されるように、Southコンテナに別名オブジェクトを作成できます。図 1-6

図 1-6 *eDirectoryコンテナの別名オブジェクト*

別名オブジェクトによって、元のColorQオブジェクトがポイントされるため、Southコンテナでは ColorQをローカルオブジェクトとして印刷設定できます。

重要なプロパティ

別名オブジェクトには別名元オブジェクトプロパティがあり、このプロパティによって、別名オブジェクトと元のオブジェクトとが関連付けられます。

ディレクトリマップ

ディレクトリマップオブジェクトは、サーバのファイルシステム内のパスへのポインタです。これにより、ディレクトリをより簡単に参照できます。

ネットワークにボリュームがない場合は、ディレクトリマップオブジェクトを作成することはできません。

ディレクトリマップオブジェクトが表す内容

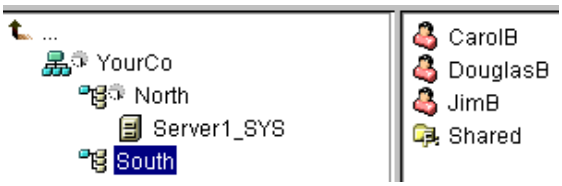
ディレクトリマップオブジェクトは、ボリューム上のディレクトリを表しますそれに対し、別名オブジェクトはオブジェクトを表します。

使用法

ディレクトリマップオブジェクトは、ログインスクリプトでのドライブマッピングを単純化するために作成します。ディレクトリマップオブジェクトを使用すると、複雑なファイルシステムパスを簡単な名前にすることができます。

また、ファイルの場所を変更した場合でも、新しい場所を参照するように、ログインスクリプトやバッチファイルを変更する必要がありません。ディレクトリマップオブジェクトを編集するだけです。たとえば、図 1-7に示すように、Southコンテナのログインスクリプトを編集するとします。

図 1-7 eDirectoryコンテナの例



ドライブをボリュームsys:上のSharedディレクトリにマッピングするコマンドは、次のようになります。

```
MAP N:=sys.North.:Shared
```

共有ディレクトリマップオブジェクトを作成した場合、マップコマンドは、次のようにさらに簡単になります。

```
MAP N:=Shared
```

重要なプロパティ

ディレクトリマップオブジェクトには、次のようなプロパティがあります。

- 名前

ディレクトリ内のオブジェクト(たとえば、Shared)を指定します。名前プロパティはMAPコマンドで使用されます。

- ボリューム

  Sys.North.YourCoのような、ディレクトリマップオブジェクトが参照するボリュームオブジェクトの名前が格納されます。

- パス

  ボリュームのルートからのパスでディレクトリを指定します(例: public\winnt\nls\english)。

プロファイル

 プロファイルオブジェクトは、ログインスクリプトの管理に役立ちます。

プロファイルオブジェクトが表す内容

プロファイルオブジェクトは、コンテナログインスクリプトの後、およびユーザログインスクリプトの前に実行されるログインスクリプトを表します。

使用法

特定のユーザのみを対象にログインスクリプトコマンドを実行したい場合は、プロファイルオブジェクトを作成します。対象のユーザには、同一コンテナ内のユーザだけでなく、異なるコンテナ内のユーザも指定できます。プロファイルオブジェクトを作成した後は、プロファイルのログインスクリプトプロパティにコマンドを指定します。続いて、該当のユーザオブジェクトをプロファイルオブジェクトのトラスティに指定し、それらのユーザオブジェクトのプロファイルメンバーシッププロパティにそのプロファイルオブジェクトを追加します。

重要なプロパティ

プロファイルオブジェクトには、次の2つの重要なプロパティがあります。

- ログインスクリプト

  そのプロファイルのユーザに対して実行するコマンドを格納します。

- ファイル/ディレクトリへの権利

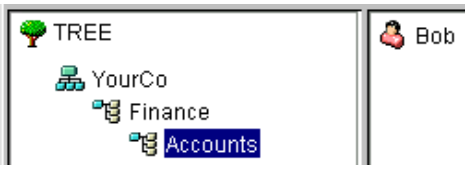
  ログインスクリプトにINCLUDEステートメントを使用した場合は、プロファイルオブジェクトに、ファイル/ディレクトリへの権利プロパティに指定されているファイルに対する権利を与える必要があります。

コンテキストと命名規則

オブジェクトのコンテキストは、ツリー内でのそのオブジェクトの位置を表します。コンテキストは、DNSドメインとほぼ同じです。

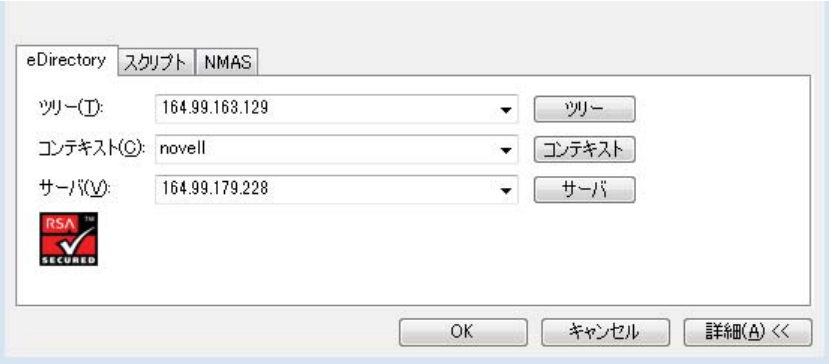
図 1-8は、ユーザBobが、YourCoという組織のFinance部門の中のAccounts部門に所属していることを示しています。

図 1-8 eDirectoryコンテナの例



ただし、オブジェクトのコンテキストをeDirectoryユーティリティで表現する必要がある場合もあります。たとえば、図 1-9に示すように、Bobのワークステーションを設定するときには、名前のコンテキストを指定する必要があります。

図 1-9 Novell ClientのNDSページ



コンテキストは、対象のオブジェクトとツリーの最上部との間に存在する各コンテナをピリオドで区切ったリストとして指定します。

識別名

オブジェクトの識別名とは、オブジェクト名にコンテキストを付けたものです。たとえば、ユーザオブジェクトBobの識別名は、Bob.Accounts.Finance.YourCoです。

タイプ付きの名前

タイプ付きの名前が、eDirectoryユーティリティに表示されることがあります。タイプつきの名前には、次の表に示されたようなオブジェクトタイプの略語があります。

オブジェクトクラス	タイプ	省略形
すべてのリーフオブジェクトクラス	Common Name	CN
組織	組織	O
部門	部門	OU
国	国	C
地域	地域または都道府県	LまたはS

eDirectoryでは、タイプ付きの名前の作成に、タイプの略語、等号、およびオブジェクト名を使用します。たとえば、Bobのタイプ付きの名前は、CN=Bobとなります。Bobのタイプ付きの完全な名前は、CN=Bob.OU=Accounts.OU=Finance.O=YourCoとなります。eDirectoryユーティリティにおいて、タイプ付きの名前は、タイプなしの名前と互換性があります。

ネームレゾリューション

ディレクトリツリー内のオブジェクトの位置を見つけるためにeDirectoryが使用するプロセスのことを、ネームレゾリューション(名前解決)といいます。eDirectoryユーティリティでオブジェクト名を使用すると、eDirectoryは、現在のコンテキストまたはツリーの最上部を基準として名前の解決を行います。

現在のワークステーションのコンテキスト

ネットワークソフトウェアの実行時には、ワークステーションにはコンテキストが設定されます。このコンテキストによって、ネットワーク内のワークステーションの位置が相対的に指定されます。たとえば、Bobのワークステーションでは、現在のコンテキストが次のように設定されます。

```
Accounts.Finance.YourCo
```

次のセクションで説明するように、現在のコンテキストは、先頭のピリオド、相対命名、および後続ピリオドの使用法を理解するうえで重要です。

先頭ピリオド

現在のコンテキストがどこに設定されているかに関わりなく、ツリーの最上部から名前を解決するには、先頭ピリオドを使用します。次の例では、先頭ピリオドがCX(コンテキストの変更)ユーティリティに、ツリーの最上部を基準として名前を解決するよう指定しています。

```
CX .Finance.YourCo
```

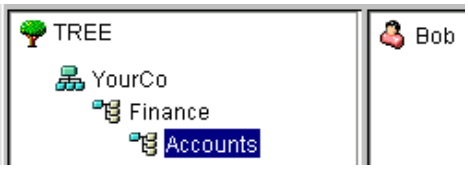
eDirectoryはこのコマンドを、「ツリーの最上部から名前の解決を行い、YourCoコンテナにあるFinanceコンテナにコンテキストを変更する」と解釈します。

相対命名

相対命名とは、ツリーの最上部ではなく、ワークステーションの現在のコンテキストを基準に、名前を解決することを意味します。先頭ピリオドはツリーの最上部からの名前解決を表すため、相対命名の場合は先頭ピリオドを使用しません。

たとえば、ワークステーションの現在のコンテキストがFinanceに設定されているとします。詳細については、図 1-10を参照してください。

図 1-10 *eDirectoryコンテナの例*



Bobの相対オブジェクト名は、次のようになります。

```
Bob.Accounts
```

eDirectoryは、この名前を「現在のコンテキストFinanceから解決されるAccountsに属するBob」と解釈します。

後続ピリオド

後続ピリオドは、相対命名でのみ使用されます。したがって、先頭ピリオドと後続ピリオドの両方を使用することはできません。後続ピリオドは、eDirectoryが名前解決を開始するコンテナを変更します。

後続ピリオド1つにつき、解決地点がツリーの上部に向かって1コンテナずつ引き上げられます。たとえば、図 1-11の例は、ワークステーションの現在のコンテキストをTimminsからAllentownに変更する場合を示しています。

図 1-11 *eDirectoryコンテナの例*

この場合の適切なCXコマンドでは、次に示すように、後続ピリオドを付けた相対命名を使用します。

```
CX Allentown.East..
```

eDirectoryはこのコマンドを、「現在のコンテキストの2つ上にあるコンテナから名前の解決を行い、EastにあるAllentownにコンテキストを変更する」と解釈します。

同様に、BobがAllentownコンテナに属し、ワークステーションの現在のコンテキストがTimminsの場合、Bobの相対名は次のようになります。

```
Bob.Allentown.East..
```

Linuxでのコンテキストと名前付け

LinuxのユーザアカウントをeDirectoryに移行する場合、ユーザの名前付けにeDirectoryのコンテキストは使用されません。

スキーマ

スキーマは、ツリー内で作成できるオブジェクトのタイプ(ユーザ、プリンタ、グループなど)、およびオブジェクトの作成時に使用する必須情報とオプション情報を定義します。各オブジェクトには、そのオブジェクトタイプのスキーマクラスが定義されています。

製品に元から付属しているスキーマは、ベーススキーマといいます。新しいクラスや新しい属性の追加など、なんらかの形でベーススキーマが変更されると、そのスキーマは拡張スキーマと見なされます。

スキーマを必ずしも拡張する必要はありませんが、拡張することも可能です。iManagerのスキーマ役割を使用すれば、運用条件に合わせてスキーマを拡張できます。たとえば、組織の従業員たちに特殊な履き物が必要で、従業員の靴のサイズを把握しておく必要があるとします。この場合は、Shoe Sizeという新しい属性を作成し、この属性を補助クラスに追加することができます。その後、その補助クラスを使用して、ユーザオブジェクトを必要に応じて拡張できます。補助クラスの作成の詳細については、142 ページの 「補助クラスを作成する」を参照してください。

eDirectoryスキーマの操作の詳細については、139ページの第5章「スキーマの管理」を参照してください。

スキーマ管理

NetIQ iManagerのスキーマ役割を通して、ツリーに対するスーパバイザ権を持っているユーザがそのツリーのスキーマをカスタマイズすることができます。スキーマ役割、およびその関連タスクは、iManagerの役割およびタスクページに表示されています。

スキーマ役割の使用目的

- スキーマ内のすべてのクラスおよび属性の一覧を表示する。
- 構文やフラグなどの属性についての情報を表示する。
- 既存のスキーマにクラスまたは属性を追加して、スキーマを拡張する。
- 名前を付けてから、属性、フラグ、追加できるコンテナ、および属性の継承元のペアレントクラスを指定して、クラスを作成する。
- 名前を付けてから、構文およびフラグを指定して、属性を作成する。
- 既存のクラスにオプションの属性を追加する。
- 使用されていない、または必要のなくなったクラスや属性を削除する。

スキーマクラス、属性、および構文

Classes (クラス)

クラスとは、ディレクトリオブジェクトのテンプレートのようなものです。ディレクトリオブジェクトとは、データを挿入されたクラスです。つまり、次のように表すことができます。

CLASS + DATA = DIRECTORY OBJECT

各クラスは、クラス名、継承クラス(そのクラスがクラス階層の最上位である場合を除く)、クラスフラグ、および属性のグループを持っています。クラスは、ディレクトリオブジェクト(ユーザ、プリンタ、キュー、サーバなど)と同じように命名されますが、単なる構造であり内容はありません。

継承クラスとは、他のオブジェクトクラスを定義するときの開始点となるクラスです。継承クラスの属性はすべて、クラス階層でそのクラスの下位に位置するクラスへ継承されます。

クラス階層は、あるクラスがどのようにペアレントクラスと関連付けられているかを示します。クラス階層により、類似したクラスが関連付けられ、属性の継承が可能になります。また、クラスを格納できる有効なコンテナのタイプも定義されます。

クラスの作成時には、クラス階層と追加属性を使用して各クラスをカスタマイズできます。継承クラスを指定することによって、階層内の上位のクラスからその属性とフラグのすべてを新しいクラスに継承できます。さらに、継承された属性クラスに追加する属性を1つまたは複数選択することによって、新しいクラスをカスタマイズできます。追加の属性は、必須属性、ネーミング属性、またはオプション属性として選択できます。

オプションの属性を追加して、既存のクラスを変更することもできます。

属性

属性とは、eDirectoryデータベース内のデータフィールドのことです。たとえば、クラスが記入用紙のようなものだとすれば、属性は記入用紙における1つの記入欄です。属性の作成時に、名前(*姓*や*社員番号*など)と、構文タイプ(*文字列*や*数字*など)が指定されます。その後、その属性はスキーママネージャの属性リストで使用できるようになります。

注: eDirectoryでは、レプリケーションの問題のため、ストリーム属性タイプ以外の属性に60KBまたは30,000文字を超える値を含めることができません。ユーザやアプリケーションが、その制限を超える文字列またはバイナリ属性の値を設定すると、eDirectoryは値が長すぎることを示す-649エラーを返します。

構文

構文にはいくつかの選択可能なオプションがあります。これらの構文オプションは、各属性で入力するデータのタイプを指定するために使用されます。構文は属性の作成時にのみ指定できます。後から構文を変更することはできません。利用可能な構文は次のようなものです。

- Back Link (バックリンク)

  オブジェクトを参照する他のサーバの追跡に使用されます。また、eDirectoryの内部管理目的で使用されます。

- ブール

  TRUE(1)またはFALSE(0)の値をとる属性に使用されます。この構文タイプには、単一の値のフラグが設定されます。

- Case Exact String (大/小文字一致文字列)

  比較演算で大文字/小文字が区別されるUnicode文字列を値としてとる属性に使用されます。2つの「大文字小文字を区別する文字列」は、長さが等しく、対応する文字(大文字/小文字の区別を含む)が同一の場合に一致とみなされます。

- Case Ignore List (大/小文字無視リスト)

  比較演算で大文字/小文字が区別されないUnicode文字列の順序列を値としてとる属性に使用されます。2つの「大文字小文字を無視するリスト」は、文字列の数が等しく、対応するすべての文字列が同じ場合(つまり、長さと対応する文字が同一の場合)に一致とみなされます。

- Case Ignore String (大/小文字無視文字列)

  比較演算で大文字/小文字が区別されないUnicode文字列を値としてとる属性に使用されます。2つの「大文字小文字を無視する文字列」は、長さが等しく、対応する文字があらゆる面で(ただし、大文字/小文字の区別を除く)同一の場合に一致とみなされます。

- クラス名

  オブジェクトクラスの名前を値としてとる属性に使用されます。2つのクラス名は、長さが等しく、対応する文字があらゆる面で(ただし、大文字/小文字の区別を除く)同一の場合に一致とみなされます。

- カウンタ

  増分変更された符号付き整数を値としてとる属性に使用されます。カウンタによって定義された属性は、単一の値の属性です。カウンタは、この構文の属性に値が追加されると足し算で合計に追加され、この構文の属性から値が削除されると引き算で合計から差し引かれるという点で、整数とは異なります。

- 識別名

  eDirectoryツリー内のオブジェクト名を値としてとる属性に使用されます。DN(識別名)では大文字/小文字が区別されませんが、ネーミング属性の1つでは大文字/小文字が区別されます。

- EMail Address (電子メールアドレス)

  バイナリ情報の文字列を値としてとる属性に使用されます。eDirectoryは、この構文の内容の内部構造については想定しません。

- Fax番号

  国際電話番号と、推奨T.20に従って形式設定されたオプションのビット文字列の格納を規定するE.123標準に準拠した文字列を指定します。2つのFax番号値は、長さが等しく、対応する文字列が同一(ただし、比較処理で無視されるスペースとハイフンを除く)の場合に、一致とみなされます。

- ［保持］

  符号付き整数の値を持つアカウント数量の属性に使用されます。この構文は、アカウント数量(トランザクションが完了するまでの間、サブジェクトのクレジット限度に対して暫定的に保持される金額)を表します。保持量は、カウンタ構文と同じように扱われ、新しい値がベース合計に加算されるか、ベース合計から減算されます。計算された保持量が0になると、保持レコードは削除されます。

- 整数

  符号付き数値として表される属性に使用されます。2つの整数値は、値が同一である場合に一致とみなされます。順序付けの比較では、符号付き整数ルールが使用されます。

- 整数64

  64ビット整数値として表される属性に使用されます。整数64属性はMicrosoft Large Integer Syntaxをサポートし、large-integer値や1970年より前または2038年より後の日付を格納するために使用できます。

  注: eDirectoryでは、内部タイムスタンプ用に既存の構文と32ビット値を使用します。

- Interval

  符号付き整数を値としてとり、時間の間隔を表す属性に使用されます。間隔構文では、整数構文と同じ表現が使用されます。Interval (間隔)値は時間間隔の秒数です。

- Net Address (ネットアドレス)

  サーバ環境でのネットワーク層アドレスを表します。このアドレスは、バイナリ形式です。2つのネットアドレスは、各アドレスのタイプ、長さ、および値が一致する場合に、一致とみなされます。

- Numeric String (数値文字列)

CCITT X.208定義で数値文字列として定義されている数値整数を値としてとる属性に使用されます。2つの数値文字列は、長さが等しく、対応する文字が同一の場合に一致とみなされます。数値文字列文字セットにおいて有効な文字は、数字(0～9)およびスペースのみです。

- Object ACL (オブジェクトACL)

  アクセス制御リスト(ACL)エントリを表す値をとる属性に使用されます。Object ACL (オブジェクトACL)値は、オブジェクトまたは属性のいずれかを保護できます。

- Octet List (オクテットリスト)

  バイナリ情報またはオクテット文字列の順序付き文字列シーケンスを表します。オクテットリストは、保存済みリストのサブセットである場合に、保存済みリストと一致するとみなされます。2つのオクテットリストは、長さが等しく、対応するビット列(オクテット)が同一の場合に一致とみなされます。

- Octet String (オクテット文字列)

  eDirectoryによって解釈されないバイナリ情報の文字列を値としてとる属性に使用されます。これらのオクテット文字列は、非Unicode文字列です。2つのオクテット文字列は、長さが等しく、対応するビット列(オクテット)が同一の場合に一致とみなされます。

- パス

  ファイルシステムパスを表す属性であり、サーバ上でファイルを見つけるために必要なすべての情報が格納されます。2つのパスは、長さが等しく、対応する文字(大文字/小文字の区別を含む)が同一の場合に、一致とみなされます。

- Postal Address (住所)

  住所を表すUnicode文字列を値としてとる属性に使用されます。通常、住所の属性値は、勧告F.401に基づいてMHS Unformatted Postal O/R Address Specificationバージョン1から選択された属性で構成されます。この値は6行(各行は30文字)に制限されます(郵送先国名を含む)。2つの住所は、文字列の数が等しく、対応するすべての文字列が同じ場合(つまり、長さと対応する文字が同一の場合)に一致とみなされます。

- 印刷可能文字列

  CCITT X.208に定義されている印刷可能文字列を値としてとる属性に使用されます。印刷可能文字セットは、次のものから構成されます。

  - 英大文字および英小文字
  - 数字(0～9)
  - スペース
  - アポストロフィ (')
  - 左カッコおよび右カッコ( )
  - プラス記号(+)
  - カンマ(,)
  - ハイフン(-)
  - ピリオド(.)
  - スラッシュ(/)
  - コロン(:)
  - 等号(=)
  - 疑問符(?)

2つの印刷可能文字列は長さが等しく、対応する文字が同一の場合に一致とみなされます。大文字/小文字は区別されます。

- Replica Pointer (レプリカポインタ)

  パーティションレプリカを表す値をとる属性に使用されます。eDirectoryツリーのパーティションでは、複数のサーバにレプリカを置くことができます。この構文は、次の6つのコンポーネントで構成されます。

  - サーバ名
  - レプリカタイプ(マスタ、セカンダリ、読み込み専用、サブオーディネートリファレンス)
  - レプリカ番号
  - レプリカルートID
  - アドレスの数
  - アドレスレコード

- Stream (ストリーム)

  任意のバイナリ情報を表します。ストリーム構文を使用すると、ファイルサーバ上のファイルからeDirectory属性を作成できます。この構文は、ログインスクリプトやその他のストリーム属性で使用されます。ストリームファイルに格納されているデータは、いかなる種類の構文強制も受けません。この構文は単に任意のデータであり、個別のアプリケーションで作成、定義および使用されます。

- Telephone Number (電話番号)

  電話番号を値としてとる属性に使用されます。2つの電話番号は、長さが等しく、対応する文字列が同一(ただし、比較処理で無視されるスペースとハイフンを除く)の場合に、一致とみなされます。

- 時刻

  符号なし整数を値としてとり、秒単位の時間を表す属性に使用されます。

- Timestamp (タイムスタンプ)

  特定のイベントが発生した時刻を示す値をとる属性に使用されます。特定のイベントが発生すると、eDirectoryサーバによってタイムスタンプ値が生成され、そのイベントに関連付けられます。各タイムスタンプ値は、eDirectoryパーティション内で固有です。これにより、同一パーティションのレプリカを保持しているすべてのサーバで発生したイベントを1つにまとめて順序付けできます。

- Typed Name (タイプ付きの名前)

  オブジェクトに関連付けられたレベルおよび間隔を表す値をとる属性に使用されます。この構文は、eDirectoryオブジェクトを指定し、次の2つの数値を当該オブジェクトにアタッチします。

  - 優先番号を示す属性レベル
  - イベント間の秒数、または参照の頻度を表す間隔

- 不明

  スキーマから削除されている属性定義をもつ属性に使用されます。この構文は、バイナリ情報の文字列を表します。

必須属性およびオプション属性について

オブジェクトにはどれも、オブジェクトのタイプに合わせて定義されたスキーマクラスがあります。クラスとは、意味のある方法で組織された属性のグループを指します。これらの属性の一部は必須で、一部はオプションです。

必須属性

必須属性とは、オブジェクトの作成時に指定する必要がある属性です。たとえば、社員番号が必須属性であるユーザクラスで新しいユーザを作成する場合、社員番号を入力せずに新しいユーザオブジェクトを作成することはできません。

オプション属性

オプション属性とは、必要に応じて指定できる属性を指します。たとえば、ニックネームがオプション属性となっているユーザクラスで新しいユーザオブジェクトを作成するとします。この場合、この属性が入力されてもされなくてもユーザオブジェクトは作成できます。属性を入力するかどうかは、新しいユーザにニックネームが付けられているかどうかに左右されます。

例外的にオプション属性が命名に使用される場合がありますが、その場合は属性が必須になります。

スキーマのサンプル

図 1-12は、スキーマの一部の例で、基本のスキーマに類似しているかもしれません。この図は、組織クラスについての情報を表しています。この画面に表示されているほとんどの情報は、クラスが作成されたときに指定されたものです。オプションの属性のいくつかは後に追加されました。

 このアイコンは、ベーススキーマの拡張であるすべてのクラスと属性に割り当てられます。

図 1-12 iManagerのクラス情報ページ

スキーマを設計する

最初にスキーマの設計を行うと、長期的に見た場合、時間と労力を節約できます。ベーススキーマを表示して、それが実際の必要条件に見合うか、あるいは変更が必要かを判断できます。変更が必要な場合は、スキーママネージャを使用してスキーマを拡張します。詳細については、「140ページの 「スキーマの拡張」」と「144 ページの 「スキーマの表示」」を参照してください。

パーティション

パーティションは、eDirectoryデータベースの論理区分です。各ディレクトリパーティションは、ディレクトリ情報を格納するツリー内の個別のデータユニットとなります。

パーティションを分割すると、ディレクトリの一部を1つのサーバから切り離し、別のサーバに置くことができます。

WANリンクが遅い場合や信頼性に乏しい場合、またはディレクトリに多量のオブジェクトがあるためにサーバが処理しきれず、アクセスが遅くなる場合は、ディレクトリをパーティション分割することを検討してください。パーティションの詳細な説明については、151ページの第6章「パーティションおよびレプリカの管理」を参照してください。

各ディレクトリパーティションは、コンテナオブジェクト、それに含まれるすべてのオブジェクト、およびそれらのオブジェクトに関するデータのセットから構成されます。eDirectoryパーティションには、ファイルシステムに関する情報、またはパーティションに含まれるディレクトリやファイルに関する情報は格納されません。

パーティション分割はNetIQ iManagerを使用して行います。iManagerでは、パーティションアイコン()によってパーティションが識別されます。

図1-13 サーバのレプリカビュー

この上の例では、［パーティション］アイコンはTreeオブジェクトの横にあります。この場合は、Treeオブジェクトが、パーティション内の最上位のコンテナであることを意味します。他のコンテナではパーティションが表示されていないため、このパーティションが唯一のパーティションになります。

これはデフォルトのeDirectoryパーティションで、ディレクトリ全体を1つのパーティションにまとめています。

この例では、Server1のレプリカビューが表示されていることに注意してください。iManagerでサーバのレプリカビューを表示すると、そのサーバに保持されているすべてのレプリカが右に表示されます。この場合、Server1には唯一のパーティションのレプリカが保持されています。詳細については、61 ページの 「レプリカ」および160 ページの 「eDirectoryサーバのレプリカを表示する」を参照してください。

パーティション

パーティションには、その最上位のコンテナの名前が付けられます。では、TreeおよびFinanceという名前の2つのパーティションがあります。図 1-14パーティションFinanceはTreeから分割されたため、このパーティションはTreeのチャイルドパーティションと呼ばれます。またTreeは、Financeのペアレントパーティションと呼ばれます。

***図1-14** パーティションのレプリカビュー*

ディレクトリに大量のオブジェクトがあるためにサーバが処理しきれず、eDirectoryへのアクセスが遅くなる場合、このように新しいパーティションを作成すると便利です。新しいパーティションを作成すると、データベースを分割し、その分岐のオブジェクトを異なるサーバに渡すことができます。

上の例では、Financeパーティションのレプリカビューが表示されています。iManagerでパーティションのレプリカビューを表示すると、そのパーティションのレプリカを持つサーバはすべて右側に表示されます。この場合、Server1には、Financeパーティションの読み書き可能レプリカが保持されています。詳細については、162 ページの 「パーティションレプリカを表示する」を参照してください。

パフォーマンス向上のためにレプリカを分散する

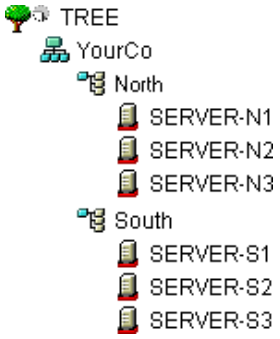
前の例で、Server1サーバに、TreeパーティションとFinanceパーティションの両方のレプリカが保管されているとします。この場合、パーティション分割後もServer1はディレクトリ全体(両パーティションのレプリカ)をまだ保持しているため、パーティション分割によるeDirectoryのパフォーマンスの向上は実現されません。

パフォーマンスを向上させるには、レプリカの1つを別のサーバに移動する必要があります。たとえば、TreeパーティションをServer2へ移動すると、TreeおよびYourCoコンテナにあるすべてのオブジェクトがServer2に移動します。Server1は、FinanceおよびAccountsコンテナのオブジェクトだけを格納することになります。Server1とServer2への負荷は、パーティション分割を行っていないときに比べて、いずれも軽くなります。

パーティションとWANリンク

ネットワークが、WANリンクで分割されたNorthサイトとSouthサイトの2つのサイトに渡っている場合を考えてみます。各サイトには、それぞれ3つのサーバがあります。

図 1-15 *eDirectoryコンテナの例*



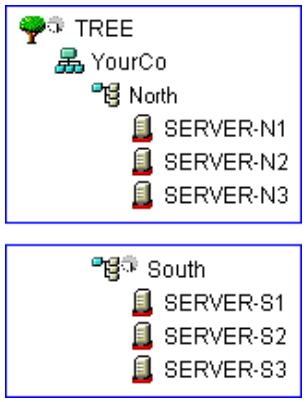
このケースでは、ディレクトリを2つのパーティションに分割すると、eDirectoryはより高速になり、信頼性も向上します。

パーティションが1つしかないと、レプリカは1つのサイトに保存されるか、2つのサイトに分散されます。この場合、次の2つの問題点があります。

- たとえば、Northサイトにすべてのレプリカが保存されているとすると、Southサイトでは、ログインやリソースへのアクセスに時間がかかります。また、リンクが停止した場合、Southサイトのユーザは、ログインまたはリソースにアクセスすることができなくなります。
- レプリカが2つのサイトに分散されていると、ユーザはローカルでディレクトリにアクセスできます。ただし、サーバ間のレプリカの同期はWANリンクを通して行われるので、リンクの信頼性が低い場合には、eDirectoryエラーが発生する可能性があります。ディレクトリに加えられた変更をWAN経由で伝えるには、時間がかかります。

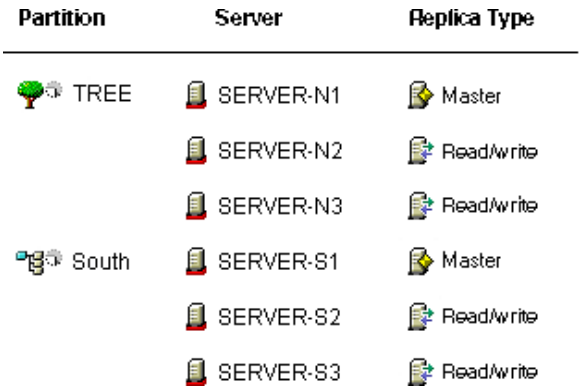
に示した2つのパーティションによるソリューションは、WANリンクでのパフォーマンスと信頼性の問題を解決します。図 1-16

図 1-16 *パーティションの例*



Treeパーティションのレプリカは、Northサイトのサーバに保存されています。Southパーティションのレプリカは、図 1-17に示すように、Southサイトのサーバに保存されています。

図1-17 パーティション、サーバ、およびレプリカの例



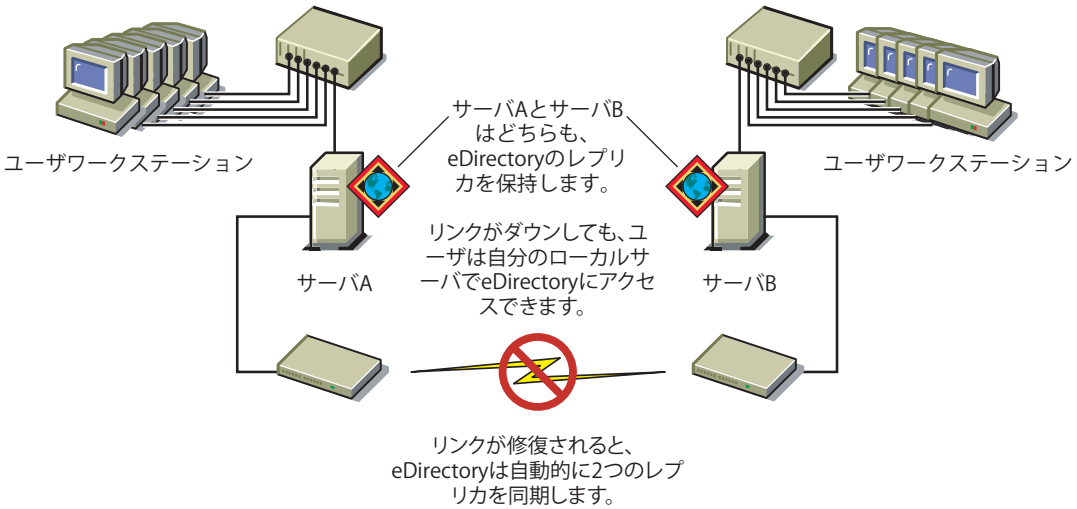
各サイトでは、ローカルリソースを表すオブジェクトは、ローカルで保存されています。サーバ間の同期トラフィックは、通信速度が遅く信頼性の低いWANリンクではなく、LAN上でローカルに行われます。

ただし、異なるサイトのオブジェクトにユーザや管理者がアクセスする場合は、wanリンク上でのeDirectoryトラフィックが発生します。

レプリカ

レプリカは、eDirectoryサーバに分配されたユーザ定義済みのパーティションのコピーまたはインスタンスです。ネットワークに複数のeDirectoryサーバがある場合、ディレクトリのレプリカ(コピー)を複数保存しておくことができます。これにより、あるサーバやそのサーバに対するネットワークリンクが機能しなくなった場合でも、ユーザが残りのネットワークリソースにログインして使用できます(図 1-18を参照)。

図1-18 eDirectoryレプリカ



それぞれのサーバは65,000を超えるeDirectoryレプリカを格納できます。ただし、同じユーザ定義パーティションのレプリカを、同じサーバ上に2つ以上格納することはできません。レプリカの詳細な説明については、151ページの第6章「パーティションおよびレプリカの管理」を参照してください。

eDirectoryの障害対策として、レプリカを3つ保存しておくことをお勧めします(レプリカを保存するeDirectoryサーバが3箇所あると想定した場合)。単独のサーバに、複数のパーティションのレプリカを保存することもできます。

レプリカサーバは、eDirectoryレプリカのみを格納する専用サーバです。このタイプのサーバは、DSMASTERサーバとも呼ばれます。この環境設定は、多くの単一サーバリモートオフィスを使用する企業などでよく利用されます。レプリカサーバを使用すると、リモートオフィスの場所のパーティション用として追加のレプリカを格納できます。

また、障害復旧計画にそれを含めることもできます(451ページの「DSMASTERサーバによる災害対策」の説明を参照)。

eDirectoryのレプリケーションでは、サーバファイルシステムの障害対策は提供されません。eDirectoryオブジェクトに関する情報のみが、複製されます。TTS™ (トランザクショントラッキングシステム™)、ディスクミラーリング/二重化、RAID、またはNRS (NetIQ Replication Services)を使用することにより、ファイルシステムの耐障害性を得ることができます。

バインダリサービスを提供するサーバでは、マスタレプリカ、または読み書き可能レプリカが必要になります。

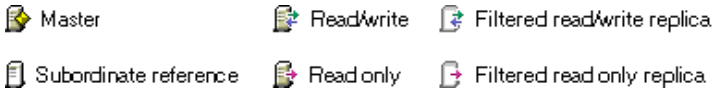
ユーザがWAN経由でeDirectory情報に定期的にアクセスしている場合は、必要な情報を含んだレプリカをサーバに配置し、ユーザがローカルでアクセスできるようにすることで、アクセス時間とWANトラフィックを減らすことができます。

LANにおいても、ある程度は同じことが当てはまります。ネットワーク上の複数のサーバにレプリカを分散すると、情報は、通常、最も近くにある使用可能なサーバから取得されます。

レプリカのタイプ

eDirectoryでは、次の図に示したレプリカのタイプがサポートされます。

図1-19 *レプリカのタイプ*



- 62 ページの 「マスタレプリカ」
- 63 ページの 「読み書き可能レプリカ」
- 63 ページの 「読み込み専用レプリカ」
- 64 ページの 「フィルタ済み読み書き可能レプリカ」
- 64 ページの 「フィルタ済み読み込み専用レプリカ」
- 64 ページの 「サブオーディネートリファレンスレプリカ」

マスタレプリカ


マスタレプリカはオブジェクトやパーティションへの変更を開始するために使用される、書き込み可能なレプリカタイプです。マスタレプリカは、次のタイプのeDirectoryパーティション操作を管理します。

- レプリカのサーバへの追加

- レプリカのサーバからの削除
- eDirectoryツリーの新しいパーティションの作成
- eDirectoryツリーの既存のパーティションの削除
- eDirectoryツリーのパーティションの移動

マスタレプリカは、次のタイプのeDirectoryオブジェクト操作にも使用されます。

- eDirectoryツリーへの新しいオブジェクトの追加
- eDirectoryツリーの既存のオブジェクトの削除、リネーム、または移動
- eDirectoryツリーへのオブジェクトの認証
- eDirectoryツリーへの新しいオブジェクト属性の追加
- 既存の属性の変更または削除

デフォルトでは、ネットワークの最初のeDirectoryサーバが、マスタレプリカを保持します。マスタレプリカは、各パーティションに同時に1つだけ存在します。別のレプリカを作成すると、デフォルトで読み書き可能レプリカになります。

マスタレプリカを保持しているサーバを1～2日以上ダウンさせる場合は、読み書き可能レプリカのうち1つをマスタレプリカにすることができます。オリジナルのマスタレプリカは、自動的に読み書き可能レプリカになります。

eDirectoryで新しいレプリカやパーティションの作成などの操作をするには、ネットワークでマスタレプリカが使用可能である必要があります。

読み書き可能レプリカ

 eDirectoryが、読み書き可能レプリカおよびマスタレプリカのオブジェクト情報にアクセスして、変更できます。すべての変更内容は、すべてのレプリカに自動的に伝えられます。

WANリンクの通信速度が遅い場合やルータがビジー状態の場合など、ネットワークインフラストラクチャで遅延のためeDirectoryのユーザへの反応が遅い場合は、eDirectoryを必要とするユーザの近くに読み書き可能レプリカを作成できます読み書き可能レプリカは、サーバにいくつでも作成できますが、レプリカが増えると、同期を取るためにトラフィックの量が増加します。

読み込み専用レプリカ

 読み込み専用レプリカは、パーティションの境界内にあるすべてのオブジェクトに関する情報を読み込むのに使用される、読み込み可能なレプリカタイプです。読み込み専用レプリカは、マスタレプリカと読み書き可能レプリカからの同期更新は受け入れますが、クライアントからの直接の変更は受け入れません。ログイン更新が有効になっている場合、読み込み専用レプリカへのログインにより属性の更新が発生するため、ログインは失敗します。

このレプリカタイプは、バインダリエミュレーションを提供できませんが、eDirectoryツリーの障害対策を提供しています。マスタレプリカおよびすべての読み書き可能なレプリカが破壊または破損すると、読み込み専用レプリカを新しいマスタレプリカに昇格させることができます。

また、NDSオブジェクトの読み込みやパーティションの境界内のすべてのオブジェクトを含むフォールトトレランス、およびパーティションルートオブジェクトを含むNDSディレクトリツリーへの接続も提供します。

クライアントは常に読み書き可能レプリカにアクセスし、変更を加え続けることができるため、ツリー内のセキュリティポリシーを確立してオブジェクトの変更を制限する目的のために読み込み専用レプリカを使用することは避けてください。権利継承フィルタの使用のように、この目的でディレクトリに存在するメカニズムは他にもあります。詳細については、73 ページの 「IRF(権利継承フィルタ)」を参照してください。

フィルタ済み読み書き可能レプリカ

 フィルタ済み読み書き可能レプリカには、フィルタ済みオブジェクトセットまたはオブジェクトクラスが、それらのオブジェクトのフィルタ済み属性セットおよび値とともに格納されます。それに含まれる内容は、ホストサーバのレプリケーションフィルタに固有のeDirectoryオブジェクトおよびプロパティのタイプに限定されます。ユーザはレプリカの内容を読み取ったり、変更することができ、eDirectoryは選択されたオブジェクト情報にアクセスしたり、変更することができます。選択された変更内容は、すべてのレプリカに自動的に伝えられます。

フィルタ済みレプリカの場合、サーバごとにフィルタを1つだけ指定できます。つまり、あるサーバで定義されているフィルタは、そのサーバ上のすべてのフィルタ済みレプリカに適用されます。フィルタ済みレプリカは、サーバにいくつでも作成できますが、レプリカが増えると、同期を取るためのトラフィックの量が増加してしまいます。

詳細については、65 ページの 「フィルタ済みレプリカ」を参照してください。

フィルタ済み読み込み専用レプリカ

 フィルタ済み読み込み専用レプリカには、フィルタ済みオブジェクトセットまたはオブジェクトクラスが、それらのオブジェクトのフィルタ済み属性セットおよび値とともに格納されます。フィルタ済み読み込み専用レプリカは、マスタレプリカと読み書き可能レプリカからの同期更新は受け入れますが、クライアントからの直接の変更は受け入れません。ユーザはこのレプリカの内容を読み込むことができますが、変更はできません。それに含まれる内容は、ホストサーバのレプリケーションフィルタに固有のeDirectoryオブジェクトおよびプロパティのタイプに限定されます。

詳細については、65 ページの 「フィルタ済みレプリカ」を参照してください。

サブオーディネートリファレンスレプリカ

サブオーディネートリファレンスレプリカは、システム生成のレプリカで、マスタレプリカや読み書き可能レプリカのオブジェクトをすべて含んでいるわけではありません。したがって、サブオーディネートリファレンスレプリカは、障害対策を提供していません。サブオーディネートリファレンスレプリカは、eDirectoryによるパーティションの境界を超えた名前の解決に必要な情報のみを格納するために生成される内部ポインタです。

サブオーディネートリファレンスレプリカを削除することはできません。不要になった時点で、eDirectoryが自動的に削除します。サブオーディネートリファレンスレプリカは、ペアレントパーティションのレプリカを保持し、チャイルドパーティションのレプリカを保持していないサーバでのみ作成されます。

チャイルドパーティションのレプリカが、ペアレントのレプリカを保持するサーバにコピーされた場合、サブオーディネートリファレンスレプリカは自動的に削除されます。

フィルタ済みレプリカ

フィルタ済みレプリカには、オブジェクトまたはオブジェクトクラスのフィルタされたセットが、これらのオブジェクトの属性および値のフィルタされたセットと共に格納されます。たとえば、eDirectoryツリーのさまざまなパーティション内のユーザオブジェクトのみを格納するフィルタ済みレプリカのセットを、1つのサーバ上に作成できます。また、ユーザオブジェクトのデータ(名、姓、電話番号など)のサブセットのみを格納するレプリカを作成することもできます。

フィルタ済みレプリカを使用して、1つのサーバ上にeDirectoryデータのビューを構築できます。そのために、フィルタ済みレプリカでは、スコープとフィルタを作成できます。これにより、ツリー内の数多くのパーティションから1つのeDirectoryサーバに、適切に定義されたデータセットを格納することが可能になります。

サーバのスコープとデータフィルタの説明はeDirectoryに格納され、iManagerのサーバオブジェクトを通して管理できます。

1つまたは複数のフィルタ済みレプリカを格納するサーバは、レプリケーションフィルタを1つだけ保持します。そのため、そのサーバにあるすべてのフィルタ済みレプリカは、それぞれのパーティションからの同じ情報のサブセットを格納します。フィルタ済みレプリカのマスタパーティションレプリカは、eDirectory 8.5以降が動作するeDirectoryサーバでホストされていなければなりません。

フィルタ済みレプリカは、次の目的に使用できます。

- 他のサーバから複製する必要があるデータ量が減ることによる、サーバへの同期トラフィックの削減。
- NetIQ Identity Managerによってフィルタリングする必要があるイベント数の削減。

  NetIQ Identity Managerの詳細については、『*NetIQ Identity Manager Administration Guide (NetIQ Identity Manager管理ガイド)*』を参照してください。
- ディレクトリデータベースのサイズの縮小。

  レプリカの数が増えれば、その分データベースのサイズが増大します。完全なレプリカを作成するのではなく、特定のクラスのデータのみを格納するフィルタ済みレプリカを作成することによって、ローカルデータベースのサイズを小さくすることができます。

  たとえば、ツリーに10,000のオブジェクトが含まれていても、そのうち［ユーザ］オブジェクトの占める割合がわずかであれば、10,000すべてのオブジェクトを格納する完全なレプリカではなく、［ユーザ］オブジェクトのみを含むフィルタ済みレプリカを作成できます。

ローカルデータベースに格納されているデータをフィルタリングできるという特徴を別にすれば、フィルタ済みレプリカは通常のeDirectoryレプリカと同じであり、必要なときはいつでも完全なレプリカに戻すことができます。

注: デフォルトでフィルタ済みのレプリカは、必須のフィルタとして組織および部門を持つことになります。

フィルタ済みレプリカの設定と管理の詳細については、159 ページの 「フィルタ済みレプリカを設定し管理する」を参照してください。

フィルタ済みレプリカへのローカルログインの許可

フィルタ済みレプリカへのローカルログインを許可するには、iManagerで［**ローカルログインの有効化**］オプションを選択することに加えて、クラスndsLoginPropertiesをフィルタに追加する必要もあります。

フィルタ済みレプリカへログインする前に、次の属性を設定する必要があります。

- 不正侵入者を検出する
- 不正ログイン回数のリセット間隔
- 最終ログイン時刻
- 不正侵入者によりロックされました
- 検出後のロックアウト
- ログイン許容時間マップ
- ログインが無効化されました
- ログインの有効期限
- ログイン猶予制限
- 残りのログイン猶予
- ログイン不正侵入者のアドレス
- ログイン不正侵入者の試行
- ログイン不正侵入者の制限
- ログイン不正侵入者のリセット時間
- 同時ログインの最大数
- ログイン時刻
- ネットワークアドレス
- ネットワークアドレスの制限
- パスワード期限間隔
- パスワード期限の時刻
- 秘密鍵
- 公開鍵
- nspmDoNotExpirePassword
- nspmPasswordKey
- nspmPasswordPolicyDN
- pwdAccountLockedTime
- pwdFailureTime
- sasLoginFailureDelay
- sasOTPCounter
- sasOTPDigits
- sasOTPEnabled
- sasOTPReSync

- sasUpdateLoginInfo
- sasUpdateLoginTimeInterval

注: 上記の属性は、ユーザオブジェクト、ペアレントコンテナ、またはログインポリシーで設定できます。

レプリカリングでのサーバの同期

複数のサーバが、同じパーティションのレプリカを保持している場合、それらのサーバはレプリカリングとみなされます。同期は、あるレプリカから他のレプリカへのディレクトリ情報の伝播であるため、各パーティションの情報は他のパーティションの情報と整合性を保ちます。eDirectoryは自動的にそれらのサーバの同期を維持します。詳細については、121 ページの 「同期」を参照してください。

eDirectory同期のタイプは、次のとおりです。

- 通常同期またはレプリカ同期
- 優先度同期

リソースへのアクセス

eDirectoryは、デフォルトの権利に従って基本レベルのネットワークアクセスセキュリティを構築します。アクセス制御をより強化するための方法を、次に示します。

- 権利の割り当て

  ユーザがネットワークリソースへのアクセスを試みると、システムはそのリソースに対するユーザの有効な権利を計算します。明示的なトラスティ割り当て、同等セキュリティの付与、および継承される権利に対するフィルタ処理を行うことによって、ユーザがリソースに対する適切で有効な権利を持つように設定できます。

  権利の割り当てを単純化するため、グループおよび職種オブジェクトを作成した後に、グループや職種にユーザを割り当てることができます。

- ログインセキュリティの追加

  ログインセキュリティは、デフォルトでは設定されていません。ログインセキュリティ方法の設定にはいくつかあります。ログインパスワード、ログインする場所および時間の制限、同時ログインセッションの制限、不正侵入者検出、およびログインの禁止があります。

- ロールベース管理の設定

  特定のオブジェクトプロパティに対して管理者を設定し、これらのプロパティに対してのみ、権利を許可します。これにより、特定の責任を担う管理者を作成できます。この責任はどのコンテナオブジェクトの下位のオブジェクトへも継承できます。ロールベースの管理者は、従業員の情報やパスワードに関連したプロパティのような、特定のプロパティに対して責任を持ちます。

  役割ベースのサービスの設定については、『*NetIQ iManager管理ガイド*(https://www.netiq.com/documentation/imanager-3/imanager_admin/)』の「RBSのインストール」を参照してください。

  管理者がロールベースの管理アプリケーションを実行できるよう、特定のタスクに基づいて役割を定義することもできます。詳細については、役割ベースサービスを設定するを参照してください。

eDirectoryでの権利

ツリーを作成すると、デフォルトの権利割り当てによって、ネットワークへの汎用アクセスとセキュリティが与えられます。デフォルトの割り当てには、次のようなものがあります。

- ユーザAdminはツリーの最上位に対してスーパバイザ権を持ちます。これにより、Adminはディレクトリ全体を完全に制御できます。Adminは、サーバオブジェクトに対してもスーパバイザ権を持ち、サーバ上のどのボリュームに対しても完全に制御できます。
- ［Public］はツリーの最上位のブラウズ権を持ちます。これにより、すべてのユーザが、パブリックアクセスを通して、ツリー内のすべてのオブジェクトを表示する権利を持つことになります。
- アップグレードプロセス、印刷アップグレード、Windowsユーザ移行を通して作成されたオブジェクトは、ほとんどの状況で適切なトラスティ割り当てを受け取ります。

トラスティ割り当ておよびターゲット

権利の割り当てには、トラスティとターゲットオブジェクトが関係します。トラスティとは、権限を付与される単一のユーザまたはユーザの集合です。ターゲットとは、ユーザが権利を持っているネットワークリソースです。

- 別名をトラスティにする場合、権利は別名が示すオブジェクトにのみ適用されます。ただし、別名オブジェクトを明示的にターゲットにすることは可能です。
- ファイルシステム権はeDirectory内ではなく、ファイルシステム自体に保存されていますが、ファイルシステム内のファイルまたはディレクトリも、ターゲットにすることができます。

注: ［Public］トラスティは、オブジェクトではありません。すべてのネットワークユーザに対して与えられる、権利割り当てに関連するトラスティです。

［This］は特殊な種類のトラスティです。これは、その名前がアクセス対象のエントリと一致する場合に、認証されたオブジェクトになるよう定義されています。これにより管理者は、［This］をトラスティとして、ツリー最上位で1つのACLを使用することで、簡単に権利(「各ユーザが自分の電話番号を管理する」など)を指定できます。

---

eDirectoryでの権利の概念

eDirectoryでの権利についてより良く理解していただくために、次に各権利の概念について説明します。

- 69 ページの 「オブジェクト(エントリ)権」
- 69 ページの 「プロパティ権」
- 70 ページの 「有効な権利」
- 70 ページの 「有効な権利を計算する方法」
- 72 ページの 「同等セキュリティ」
- 73 ページの 「ACL(アクセス制御リスト)」
- 73 ページの 「IRF(権利継承フィルタ)」

オブジェクト(エントリ)権

トラスティ割り当てを作成するときには、オブジェクト権とプロパティ権を与えることができます。オブジェクト権はオブジェクト全体の操作に適用されますが、プロパティ権は一定のオブジェクトプロパティにのみ適用されます。オブジェクト権は、eDirectoryデータベース内でエントリが提供されるため、エントリ権と呼ばれます。

各権利について、次に説明します。

- **スーパバイザ** には、オブジェクトおよびそのオブジェクトのすべてのプロパティに対する、すべての権利が含まれます。
- **参照** とは、ツリー内のオブジェクトを参照する権利です。オブジェクトのプロパティを参照する権利は含まれていません。
- **作成** は、ターゲットオブジェクトがコンテナの場合にのみ適用されます。トラスティがコンテナの下に新規オブジェクトを作成する権利のことで、ブラウズ権も含まれます。
- **削除** とは、ディレクトリからターゲットを削除する権利です。
- **リネーム** とは、ターゲット名を変更する権利です。

プロパティ権

トラスティ割り当てを作成するときには、オブジェクト権とプロパティ権を与えることができます。オブジェクト権はオブジェクト全体の操作に適用されますが、プロパティ権は一定のオブジェクトプロパティにのみ適用されます。

iManagerでは、プロパティ権の管理用に次の2つのオプションが用意されています。

- ［**All Attributes Rights**］項目が選択されている場合は、すべてのプロパティを同時に管理できます。
- 特定のプロパティが選択されている場合は、選択された個々のプロパティを管理できます。

重要: あるユーザの［All Attributes Rights］プロパティへの読み取りアクセスをトラスティに付与した場合、そのトラスティには、そのユーザの［PasswoManagement］属性への読み取りアクセスが与えられます。トラスティは、そのユーザのパスワードを読み込むことができるようになります。

パスワードポリシーの作成と管理の詳細については、786 ページの 「パスワードポリシーの作成」を参照してください。

各権利について、次に説明します。

- **スーパバイザ** トラスティにプロパティの完全な制御権を与えます。
- **比較** トラスティは、プロパティの値と任意の値を比較できます。この権利によって検索が可能になります。検索では、TRUEまたはFALSEの結果のみ返されます。トラスティは、プロパティの値を実際に参照することはできません。
- **読み込み** トラスティはプロパティの値を参照することができます。この権利には、比較権が含まれます。
- **書き込み** トラスティはプロパティの値を作成、変更、および削除できます。
- **自己追加** トラスティ自身をプロパティの値として追加または削除する権利です。この権利は、メンバーシップリストまたはACL(アクセス制御リスト)などのような、値としてオブジェクト名を持つプロパティに適用されます。

有効な権利

ユーザは、明示的なトラスティ割り当て、継承、および同等セキュリティなどのさまざまな方法で権利を受け取ることができます。権利は、権利継承フィルタにより制限され、下位レベルのトラスティ割り当てによって変更、または取り消すこともできます。これらのすべてのアクションによる最終結果、つまりユーザが行使できる権利は、*有効な権利*と呼ばれます。

ユーザがいずれかの操作を実行しようとするたびに、該当のオブジェクトに対するそのユーザの有効な権利が計算されます。

有効な権利を計算する方法

ユーザがネットワークリソースにアクセスを試みるたびに、eDirectoryは次の手順でそのターゲットリソースに対するユーザの有効な権利を計算します。

1. 計算で考慮される権利を持ったトラスティをリストします。考慮されるトラスティには次のものがあります。
   - ターゲットリソースにアクセスしようとしているユーザ
   - ユーザが同等セキュリティとなっているオブジェクト
2. リスト内の各トラスティに対して、次のように有効な権利を決定します。

   2a まず、ツリーの最上位に対してトラスティが継承可能な権利を持っているかどうかチェックします。

   eDirectoryはTreeオブジェクトのオブジェクトトラスティ(ACL)プロパティをチェックして、該当のトラスティが登録された項目があるかどうか調べます。該当のトラスティが登録された項目が見つかり、その権利が継承可能な場合、eDirectoryはそれらの項目に指定された権利を、該当のトラスティの有効な権利の初期セットとして使用します。

   2b ツリー内の、ターゲットリソースが含まれている分岐を1レベル下に移動します。

   2c このレベルでフィルタリングされるすべての権利を削除します。

   eDirectoryはこのレベルのACLをチェックし、該当のトラスティの有効な権利のタイプ(オブジェクト、すべてのプロパティ、または特定のプロパティ)と一致するIRF(権利継承フィルタ)がないか調べます。検出された場合は、eDirectoryは該当のトラスティの有効な権利から、これらのIRFによって継承を阻止されるすべての権利を削除します。

   たとえば、上位のレベルで、トラスティの有効な権利にすべてのプロパティに対する書き込み権の割り当てが含まれていても、このレベルのIRFによってその継承を阻止された場合、すべてのプロパティに対する書き込み権はトラスティの有効な権利から削除されます。

   2d このレベルで割り当てられた継承可能な権利があれば追加し、必要に応じて他の割り当てを無効化します。

   eDirectoryはこのレベルのACLをチェックし、該当のトラスティが登録された項目があるかどうかチェックします。該当のトラスティが登録された項目が見つかり、その権利が継承可能な場合、eDirectoryはそれらの項目の権利をトラスティの有効な権利にコピーし、必要に応じて他の割り当てを無効化します。

   たとえば、上位のレベルで、トラスティの有効な権利に作成および削除オブジェクト権が含まれ、プロパティ権についてはまったく含まれていないときに、このレベルのACLに、該当のトラスティに対する0オブジェクト権の割り当てとすべてのプロパティの書き込み権の割り当てが含まれている場合、トラスティの既存のオブジェクト権(作成および削除)は0権利と置き換えられ、新たにすべてのプロパティ権が追加されます。

2e eDirectoryは、ツリーの各レベル(ターゲットリソースのレベルを含む)でフィルタリングと追加の手順(上記のステップ 2cおよびステップ 2d)を繰り返します。

2f ターゲットリソースで割り当てられた継承不可能な権利があれば追加し、必要に応じて他の割り当てを無効化します。

eDirectoryは、上記のステップ 2dと同じ処理を行います。その結果作成される権利セットが、該当のトラスティの有効な権利になります。

3 リスト内のすべてのトラスティの有効な権利を次のように結合します。

3a eDirectoryはリスト内のいずれかのトラスティが所有している権利をすべて含めます。リスト内のどのトラスティも所有していない権利のみ除外します。権利タイプは混在させません。たとえば、特定のプロパティに対する権利を、すべてのプロパティに対する権利に追加したり、その逆を行うことはありません。

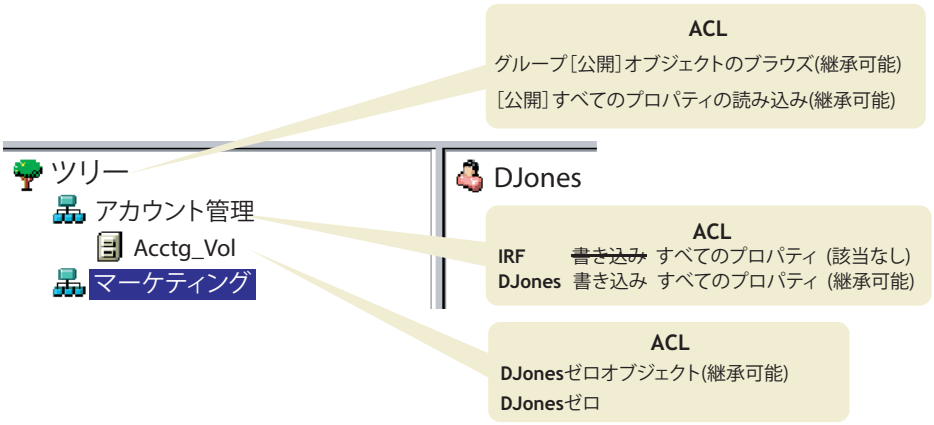
3b 現在有効な権利に暗黙で含まれる権利を追加します。

権利の設定により、ターゲットリソースに対するユーザの有効な権利が作られます。

例

ユーザ「DJones」が、ボリューム「Acctg_Vol」にアクセスしようとしています。図 1-20を参照してください。

図 1-20 トラスティ権の例



次の手順は、eDirectoryがAcctg_Volに対するDJonesの有効な権利を計算する方法を示したものです。

1. 計算で考慮される権利を持ったトラスティは、DJones、Marketing、Tree、および［Public］です。

   ここでは、DJonesがどのグループまたは役割にも所属せず、どの同等セキュリティにも明示的に割り当てられていないと仮定しています。

2. 各トラスティの有効な権利は、次のとおりです。
   - DJones: 0オブジェクト、0すべてのプロパティ

     Acctg_Volで0すべてのプロパティ権を割り当てられることで、Accountingでのすべてのプロパティに対する書き込み権の割り当ては無効化されます。
   - Marketing: 0すべてのプロパティ

     ツリーの最上位にあるすべてのプロパティに対する書き込み権の割り当ては、AccountingでのIRFによって除外されます。

- Tree: 権利なし

  Treeには、関連するどのツリー分岐でも、権利はまったく割り当てられません。

- ［パブリック］: オブジェクトのブラウズ権、すべてのプロパティの読み込み権

  これらの権利はルートで割り当てられ、関連するツリー分岐のどの位置でも、フィルタリングも無効化もされません。

3. これらすべてのトラスティの権利を結合することによって、次のようになります。

   DJones: オブジェクトのブラウズ権、すべてのプロパティの読み込み権

4. すべてのプロパティの読み込み権に伴って暗黙で割り当てられるすべてのプロパティの比較権を追加することで、最終的にAcctg_Volに対するDJonesの有効な権利は次のようになります。

   DJones: オブジェクトのブラウズ権、すべてのプロパティの読み込み、比較権

有効な権利のブロック

有効な権利の計算方法では、IRFに頼らずに特定の権利を特定のユーザに対してブロックする方法は、必ずしも明確ではありません(IRFはすべてのユーザの権利をブロックします)。

特定の権利をIRFに頼らずにユーザに対してブロックするには、次のような方法があります。

- ターゲットリソース、およびツリー内のターゲットリソースよりも上位のレベルで、該当のユーザおよびそのユーザと同等セキュリティになるオブジェクトにそれらの権利を割り当てないようにする。
- 該当のユーザまたはそのユーザが同等セキュリティになるいずれかのオブジェクトにそれらの権利が実際に割り当てられている場合は、ツリーの下位レベルに、それらの権利の割り当てを阻止する何らかの割り当てをそのオブジェクトに対して与えるようにする。不適切な権利を持つすべての(ユーザと関連する)トラスティに対して、これを実行します。

同等セキュリティ

同等セキュリティとは、別のオブジェクトと同じ権利を持つことを意味します。あるオブジェクト(オブジェクトA)を別のオブジェクト(オブジェクトB)に対して同等セキュリティに設定すると、オブジェクトAの有効な権利の計算時にオブジェクトBの権利がオブジェクトAに追加されます。

たとえば、ユーザオブジェクトJoeをAdminオブジェクトと同等セキュリティにするとします。同等セキュリティを割り当てた後は、Joeは、ツリーおよびファイルシステムに対して、Adminが持つ権利と同じ権利を持つことになります。

同等セキュリティには、次の3つのタイプがあります。

- 明示的:割り当てによる
- 自動的: グループまたは役割のメンバーシップによる
- 暗黙的:すべてのペアレントコンテナおよび［パブリック］トラスティと同等

同等セキュリティは、1ステップにかぎり有効です。たとえば、さらに別のユーザを上の例のJoeと同等セキュリティにした場合、このユーザはJoeの権利は受け取りますが、Adminの権利は受け取りません。

同等セキュリティは、該当のユーザオブジェクトの同等セキュリティプロパティの値としてeDirectoryに記録されます。

ユーザオブジェクトを職種オブジェクトにその職種の担当者として追加すると、そのユーザは自動的にその職種オブジェクトと同等セキュリティになります。ユーザをグループオブジェクトに追加した場合も同様です。

ACL(アクセス制御リスト)

ACL(アクセス制御リスト)は、オブジェクトトラスティプロパティとも呼ばれます。トラスティを割り当てると、そのトラスティは値としてターゲットのオブジェクトトラスティ(ACL)プロパティに追加されます。

このプロパティは、次の理由から、ネットワークのセキュリティに大きく影響します。

- オブジェクトのオブジェクトトラスティ(ACL)プロパティに対する書き込み権またはスーパバイザ権を持つユーザは、そのオブジェクトのトラスティが誰であるかを知ることができる。
- オブジェクトのオブジェクトトラスティ(ACL)プロパティに対して自己追加権を持つユーザは、そのオブジェクトに対する自分の権利を変更できる。たとえば、そのユーザは自分にスーパバイザ権を与えることができます。

このため、コンテナオブジェクトのすべてのプロパティに対して自己追加権を与える場合は、慎重に行う必要があります。自己追加権を割り当てられたトラスティは、該当のコンテナ、その中のすべてのオブジェクト、およびその下のコンテナ内のすべてのオブジェクトに対してスーパバイザとなることができます。

IRF(権利継承フィルタ)

権利継承フィルタにより、eDirectoryツリーの下位レベルへの権利の継承をブロックできます。このフィルタの設定の詳細については、78 ページの 「eDirectoryオブジェクトまたはプロパティへの権利継承をブロックする」を参照してください。

新規サーバのデフォルト権

新規サーバオブジェクトをツリーにインストールすると、次のトラスティ割り当てが作成されます。

デフォルトトラスティ	デフォルトの権利
Admin(ツリー内の最初のeDirectoryサーバ)	Treeオブジェクトに対するスーパバイザオブジェクト権。 Adminは、サーバオブジェクトに対してスーパバイザオブジェクト権を持ちます。これは、Adminがサーバ上に存在するあらゆるボリュームのファイルシステムのルートディレクトリに対してもスーパバイザ権を持つことを意味します。
［Public］(ツリー内の最初のeDirectoryサーバ)	Treeオブジェクトに対するブラウズオブジェクト権。
ツリー	すべてのボリュームオブジェクトのホストサーバ名プロパティおよびホストリソースプロパティに対するTree読み込みプロパティ権。 これにより、すべてのオブジェクトが物理ボリューム名および物理サーバ名にアクセスできるようになります。

デフォルトトラスティ	デフォルトの権利
コンテナオブジェクト	sys:\publicフォルダに対する読み込み権およびファイルスキャン権。これにより、コンテナの下のユーザオブジェクトは、\public内のユーティリティにアクセスできるようになります。 **注:** これらの権利は、OES Linuxを実行しているサーバにのみ適用されます。
ユーザオブジェクト	ユーザ用にホームディレクトリが自動的に作成されると、ユーザにはそのディレクトリに対するスーパーバイザ権が与えられます。

管理の委託

eDirectoryでは、自分が管理するツリーの分岐に対する管理権を無効にして、その分岐の管理を他の人物に委託できます。たとえば、特別なセキュリティ要件により、ツリーの分岐を完全に制御する管理者を個別に置かなければならないような場合には、管理権の委託というこの方法をとることが必要になります。

管理権を委託するには、次を実行します。

1 委託先のユーザに、該当のコンテナに対するスーパーバイザオブジェクト権を与えます。

1a NetIQ iManagerで、［**役割およびタスク**］ボタン をクリックします。

1b ［**権利**］>［**トラスティの変更**］の順にクリックします。

1c アクセスを制御するコンテナオブジェクトの名前およびコンテキストを入力して、［**OK**］をクリックします。

1d ［**割り当てられた権利**］をクリックします。

1e 該当するプロパティの［**スーパバイザ**］チェックボックスをオンにします。

1f ［**完了**］をクリックして、［**OK**］をクリックします。

2 継承を阻止したいスーパバイザ権や他の権利をフィルタリングするためのIRFを、そのコンテナに対して作成します。

2a NetIQ iManagerで、［**役割およびタスク**］ボタン をクリックします。

2b ［**権利**］>［**権利継承フィルタの変更**］の順にクリックします。

2c 権利継承フィルタを変更する対象のオブジェクトの名前とコンテキストを指定して、［**OK**］をクリックします。

2d 必要に応じて権利継承フィルタのリストを編集します。

フィルタのリストを編集するには、オブジェクトのACLプロパティに対するスーパバイザ権またはアクセス制御権を持っている必要があります。オブジェクトの継承された権利を全体的にブロックするフィルタは、オブジェクトのすべてのプロパティおよび個々のプロパティに対して設定できます。

注: このオブジェクトのトラスティに明示的に付与された権利は継承されないため、これらのフィルタでそのような権利を阻止することはできません。

2e **OK**をクリックします。

重要: ユーザオブジェクトに管理を委託した後に、そのオブジェクトが削除されると、その分岐を管理する権利を持つオブジェクトはなくなります。

パスワード管理など、特定のeDirectoryプロパティの管理を委任するには、76 ページの 「同等セキュリティを付与する」を参照してください。

ロールベース管理アプリケーションの特定の機能の使用を委託するには、114 ページの 「役割ベースサービスを設定する」を参照してください。

権利の管理

権利を明示的に割り当てる

eDirectoryツリーでデフォルトで割り当てられた権利によって、ユーザが必要以上にリソースにアクセスできたり、アクセスが不十分であったりする場合は、権利を明示的に作成して割り当てたり、それを変更したりできます。権利の割り当てを作成または変更するには、まず最初にアクセスを制御しているリソースやトラスティ(権利を所有している、またはこれから所有するeDirectoryオブジェクト)を選択します。

ヒント: ユーザの権利を個別にではなく、まとめて管理するには、グループ、役割、またはコンテナオブジェクトをトラスティにします。すべてのユーザについてリソースへのアクセスを全体的に制限するには、78 ページの 「eDirectoryオブジェクトまたはプロパティへの権利継承をブロックする」を参照してください。

リソースに基づいてNetIQ eDirectoryへのアクセスを制御する

1 NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。

2 ［**権利**］>［**トラスティの変更**］の順にクリックします。

3 制御するアクセス権の対象となるeDirectoryリソース(オブジェクト)の名前とコンテキストを指定して、［**OK**］をクリックします。

コンテナの下のすべてのオブジェクトへのアクセスを制御するには、そのコンテナを選択します。

4 トラスティのリストおよび権利の割り当てを必要に応じて編集します。

4a トラスティの権利の割り当てを変更するには、トラスティを選択し、［**割り当てられた権利**］をクリックし、必要に応じて権利の割り当てを変更して、［**完了**］をクリックします。

4b オブジェクトをトラスティとして追加するには、［**トラスティの追加**］をクリックし、オブジェクトを選択し、［**OK**］をクリックします。次に、［**割り当てられた権利**］をクリックしてトラスティの権利を割り当て、［**完了**］をクリックします。

権利の割り当てを作成または変更する場合、オブジェクト全体に対しても、オブジェクトのすべてのプロパティまたは個々のプロパティに対しても、アクセスを付与したり拒否したりすることができます。

4c トラスティとなっているオブジェクトを削除するには、そのトラスティを選択し、［**トラスティの削除**］をクリックします。

削除されたトラスティには、オブジェクトやプロパティに対する明示的な権利はすでにありませんが、継承や同等セキュリティによる有効な権利はまだ存在する可能性があります。

5 **OK**をクリックします。

トラスティに基づいてNetIQ eDirectoryへのアクセスを制御する

1 NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。

2 ［**権利**］>［**他のオブジェクトに対する権利**］の順にクリックします。

3 権利を変更するトラスティ(権利を所有している、またはこれから所有するオブジェクト)の名前やコンテキストを入力します。

4 ［**検索範囲のコンテキスト**］フィールドで、トラスティが権利割り当てを持っているeDirectoryオブジェクトを検索する際の検索範囲となるeDirectoryツリーの部分を指定します。

5 **OK**をクリックします。

検索の進行状況を表す画面が表示されます。検索が終了すると、［他のオブジェクトに対する権利］ページに検索結果が表示されます。

6 必要に応じてトラスティのeDirectory権利割り当てを編集します。

6a 権利割り当てを追加するには、［**オブジェクトの追加**］をクリックし、制御するアクセス権の対象となるオブジェクトを選択して、［**OK**］をクリックします。次に、［**割り当てられた権利**］をクリックし、トラスティの権利を割り当てて、［**完了**］をクリックします。

6b 権利割り当てを変更するには、制御するアクセス権の対象となるオブジェクトを選択し、［**割り当てられた権利**］をクリックし、必要に応じてトラスティの権利の割り当てを変更してから、［**完了**］をクリックします。

権利の割り当てを作成または変更する場合、オブジェクト全体に対しても、オブジェクトのすべてのプロパティまたは個々のプロパティに対しても、アクセスを付与したり拒否したりすることができます。

6c 権利割り当てを削除するには、制御するアクセス権の対象となるオブジェクトを選択して、［**オブジェクトの削除**］をクリックします。

トラスティには、オブジェクトやプロパティに対する明示的な権利はすでにありませんが、継承や同等セキュリティによる有効な権利はまだ存在する可能性があります。

7 **OK**をクリックします。

同等セキュリティを付与する

別のeDirectoryオブジェクトに対して同等セキュリティとなっているユーザは、事実上そのオブジェクトのすべての権利を持っています。ユーザは自動的に、所属するグループや役割に対して同等セキュリティになります。すべてのユーザは、［Public］トラスティ、およびTreeオブジェクトなど、eDirectoryツリーのユーザオブジェクトの上にある個々のコンテナに対して、暗黙で同等セキュリティとなります。また、任意のeDirectoryオブジェクトに対して同等セキュリティを明示的に付与することもできます。

注: このセクションのタスクを実行すると、eDirectory権利を通じて管理権限を委託することができます。ロールベースサービス(RBS)役割を使用する管理アプリケーションがある場合、それらの役割にユーザメンバーシップを割り当てることで管理権限を委託することもできます。

- 77 ページの 「メンバーシップに基づいて同等セキュリティを付与する」
- 77 ページの 「明示的に同等セキュリティを付与する」
- 78 ページの 「オブジェクト固有のeDirectoryプロパティの管理者を設定する」

メンバーシップに基づいて同等セキュリティを付与する

1 同等セキュリティにするユーザのグループオブジェクトか役割オブジェクトを作成します(まだ作成していない場合)。

詳細については、105 ページの 「オブジェクトを作成する」を参照してください。

2 グループや役割に、ユーザに必要なeDirectory権利を与えます。

詳細については、75 ページの 「権利を明示的に割り当てる」を参照してください。

3 グループや役割のメンバーシップを編集して、グループや役割の権利を必要とするユーザを追加します。

- グループオブジェクトの場合、［**グループのメンバーの変更**］ウィンドウを使用します。

  NetIQ iManagerで［**役割およびタスク**］>［**グループ**］>［**グループのメンバーの変更**］をクリックし、グループオブジェクトの名前とコンテキストを指定して、［**OK**］をクリックします。［一般］タブで、グループに追加するメンバーを指定して、［**OK**］をクリックします。

- 役割オブジェクトの場合、［**オブジェクトの変更**］ウィンドウを使用します。

  NetIQ iManagerで［**役割およびタスク**］>［**ディレクトリ管理**］>［**オブジェクトの変更**］をクリックし、職種オブジェクトの名前とコンテキストを指定して、［**OK**］をクリックします。［**その他**］をクリックし、**rbsMember**を選択して［**編集**］をクリックします。［属性の編集］ウィンドウで、役割に追加するメンバーを指定して［**OK**］をクリックします。

4 **OK**をクリックします。

明示的に同等セキュリティを付与する

1 NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。

2 ［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。

3 同等セキュリティにするユーザまたはオブジェクトの名前とコンテキストを入力またはブラウズして、［**OK**］をクリックします。

4 ［**セキュリティ**］タブをクリックし、次のように同等セキュリティを付与します。

- ユーザを選択した場合は、［**同等セキュリティ**］をクリックし、そのユーザとセキュリティを同等にするオブジェクトの名前とコンテキストを選択またはブラウズして、［**OK**］をクリックします。
- ユーザを同等セキュリティにする対象のオブジェクトを選択した場合は、［**同等セキュリティ保有者**］をクリックし、そのオブジェクトとセキュリティの面で同等にするユーザの名前とコンテキストを選択またはブラウズして、［**OK**］をクリックします。

これらの2つのプロパティページのコンテキストは、システムによって同期されます。

5 **OK**をクリックします。

オブジェクト固有のeDirectoryプロパティの管理者を設定する

1 オブジェクト固有のプロパティのトラスティにするユーザ、グループ、役割、またはコンテナのオブジェクトを作成します(まだ作成していない場合)。

トラスティとしてコンテナを作成する場合、コンテナ内またはその下のすべてのオブジェクトに権利が付与されます。プロパティは継承可能なものにする必要があります。そうしないと、コンテナおよびそのメンバーは下位レベルへの権利を持たなくなります。

詳細については、105 ページの 「オブジェクトを作成する」を参照してください。

2 NetIQ iManagerで、［**役割およびタスク**］ボタン をクリックします。

3 ［**権利**］>［**トラスティの変更**］の順にクリックします。

4 管理者に管理してもらう最高レベルのコンテナの名前とコンテキストを指定し、［**OK**］をクリックします。

5 ［トラスティの変更］ページで、［**トラスティの追加**］をクリックし、管理者を表すオブジェクトを選択して［**OK**］をクリックします。

6 追加したトラスティの［**割り当てられた権利**］をクリックし、［**プロパティの追加**］をクリックします。

7 プロパティリストに追加するプロパティを選択して、［**OK**］をクリックします。

8 管理者が管理するそれぞれのプロパティについて、必要な権利を割り当てます。

それぞれの権利割り当ての［**継承可能**］チェックボックスを必ずオンにしてください。

9 ［**完了**］をクリックして、［**OK**］をクリックします。

eDirectoryオブジェクトまたはプロパティへの権利継承をブロックする

eDirectoryでは、コンテナでの権利の割り当てが継承可能である場合も継承不能である場合もあります。のファイルシステムでは、フォルダ上のすべての権利の割り当ては継承可能です。eDirectoryでは、トラスティが誰であるかに関係なく、個別の従属項目で権利が有効にならないように、それらの項目での権利の継承を阻止できます。

1 NetIQ iManagerで、［**役割およびタスク**］ボタン をクリックします。

2 ［**権利**］>［**権利継承フィルタの変更**］の順にクリックします。

3 権利継承フィルタを変更する対象のオブジェクトの名前とコンテキストを指定して、［**OK**］をクリックします。

これで、すでにオブジェクトに設定された権利継承フィルタのリストが表示されます。

4 プロパティページで、必要に応じて権利継承フィルタのリストを編集します。

フィルタのリストを編集するには、オブジェクトのACLプロパティに対するスーパバイザ権またはアクセス制御権を持っている必要があります。オブジェクトの継承された権利を全体的にブロックするフィルタは、オブジェクトのすべてのプロパティおよび個々のプロパティに対して設定できます。

注: このオブジェクトのトラスティに明示的に付与された権利は継承されないため、これらのフィルタでそのような権利を阻止することはできません。

---

5 **OK**をクリックします。

eDirectoryオブジェクトまたはプロパティへの有効な権利を参照する

有効な権利は、ユーザが特定のネットワークリソース上で実行できる実際の権利です。有効な権利は、明示的な権利の割り当て、継承、および同等セキュリティを基に、eDirectoryによって計算されます。システムにクエリを設定すると、リソースへのユーザの有効な権利が決定されます。

1 NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。

2 ［**権利**］>［**有効な権利の表示**］の順にクリックします。

3 参照する有効な権利を持つトラスティの名前とコンテキストを入力し、［**OK**］をクリックします。

4 次のオプションから選択します。

オプション	説明
プロパティ名	トラスティが有効な権利を持っているプロパティを表示します。プロパティはeDirectoryから読み込まれるため、通常英語で表示されます。リスト内の各項目は次のタイプのいずれかです。 ［すべての属性権］-オブジェクトのすべてのプロパティを表します。 ［エントリ権］-オブジェクト全体を表します。スーパバイザの場合を除き、このアイテムへの権利にはプロパティの権利は含まれません。 特定のプロパティ-トラスティが個々に権利を持つ特定のプロパティです。デフォルトでは、このオブジェクトクラスのプロパティのみが表示されます(次を参照)。
有効な権利	eDirectoryで計算されたとおりに、選択されたプロパティへのトラスティの有効な権利を表示します。
スキーマ内のすべてのプロパティを表示する	このチェックボックスをオフにしておくと、このオブジェクトクラスのプロパティのみが表示されます。 eDirectoryスキーマで定義されたすべてのクラスのプロパティを表示するには、このチェックボックスをオンにします。追加のプロパティが有効になるのは、このオブジェクトがコンテナである場合、またはそれが拡張されて補助クラスのプロパティを含む場合のみです。追加のプロパティの横には行頭文字は表示されません。

5 **完了**をクリックします。

2 NetIQ eDirectoryネットワークの設計

NetIQ eDirectoryの設計は、実質的に、ネットワークのすべてのユーザとリソースに影響を与えます。eDirectoryの設計が良ければ、ネットワークの効率性、耐障害性、安全性、拡張性、機能性が高まり、それによってネットワーク全体のパフォーマンスと価値が向上します。この章では、eDirectoryネットワーク設計上のヒントについて説明します。

eDirectory設計の基本

効率のよいeDirectory設計の基盤となるのは、ネットワークのレイアウト、会社の組織構造、および適切な準備です。

eビジネス用にeDirectoryを設計する場合は、93 ページの 「eビジネスに対応するeDirectoryの設計」を参照してください。

ネットワークのレイアウト

ネットワークのレイアウトとは、ネットワークの物理的な設定のことです。効率のよいeDirectoryを設計するには、次の項目について考慮する必要があります。

- WANリンク
- リモートアクセスを必要とするユーザ
- ネットワークリソース(サーバ数など)
- 頻繁な停電など、ネットワークの状態
- 予測されるネットワークレイアウトの変更

組織の構造

組織の構造は、eDirectoryの設計に影響します。効率的なeDirectory設計を作成するには、以下が必要になります。

- 組織図および運営形態についての理解
- eDirectoryの設計および実装を完了するのに必要な技能のある担当者

次の技能を持った担当者を選出する必要があります。

- eDirectory設計の焦点およびスケジュールの管理
- eDirectoryの設計、設計標準、およびセキュリティについての理解
- 物理的なネットワーク構造の理解および管理
- インターネットワークのバックボーン、テレコミュニケーション、WAN設計、およびルータ配置の管理

eDirectory設計の準備をする

eDirectoryの設計に実際に着手する前に、次を実行します。

- スコープおよびスケジュールの現実的な見積もりの設定
- eDirectory実装の設計によって影響があるすべてのユーザへの連絡
- および81 ページの 「組織の構造」の情報の参照81 ページの 「ネットワークのレイアウト」

eDirectoryツリーの設計

ネットワークの設計と実装で最も重要な作業は、eDirectoryツリーの設計です。ツリーの設計には、次の作業が含まれます。

- 82 ページの 「命名標準ドキュメントを作成する」
- 85 ページの 「Treeの上位層を設計する」
- 87 ページの 「ツリーの下位層を設計する」

命名標準ドキュメントを作成する

オブジェクト名などの標準名を規定すると、ユーザと管理者の両方が、ネットワークをより直感的に理解できるようになります。書き出された標準では、管理者による、電話番号や住所などの他のプロパティ値の設定方法も指定できます。

ディレクトリの検索とブラウズでは、名前やプロパティ値の整合性が重要になります。

また、標準的な名前を使用することで、NetIQ Identity ManagerはeDirectoryとその他のアプリケーションの間でデータを容易に移動できます。Identity Managerの詳細については、『*NetIQ Identity Manager Setup Guide (NetIQ Identity Managerセットアップガイド)*』を参照してください。

命名規則

- 82 ページの 「オブジェクト」
- 83 ページの 「サーバオブジェクト」
- 83 ページの 「国オブジェクト」

オブジェクト

- コンテナ内で一意の名前にします。たとえば、同じコンテナ内でDebra JonesとDaniel Jonesの両方に「DJONES」という名前を付けることはできません。

- 特殊文字を使用することもできます。ただし、プラス記号(+)、等号(=)、およびピリオド(.)を使用する場合は、直前に円記号(\)を入力する必要があります。サーバオブジェクトとカントリオブジェクト、およびバインダリサービスと多言語環境には、追加の命名規則が適用されます。
- 大文字と小文字、およびアンダースコアとスペースは、入力時にはそのまま表示されますが、実際には区別されません。 たとえばManager_ProfileとMANAGERPROFILEは同一と見なされます。
- 名前をコマンドラインやログインスクリプトに入力するときにスペースを使用する場合は、名前全体を引用符で囲む必要があります。

サーバオブジェクト

- 新しいサーバをインストールすると、サーバオブジェクトが自動的に作成されます。
- 既存のWindowsサーバ、および他のツリー内のeDirectoryサーバに対して、追加のサーバオブジェクトを作成できますが、それらはすべてバインダリオブジェクトとして扱われます。
- サーバオブジェクトを作成するとき、その名前は物理サーバ名と一致していなければなりません。また、サーバ名には次の規定があります。
  - ネットワーク全体で固有である
  - 2～47文字の長さである
  - A～Zまでの文字、0～9までの数字、ハイフン(-)、ピリオド(.)、およびアンダースコア(_)のみを含む
  - 最初の文字にピリオドを使用しない
- 一度付けたサーバオブジェクト名をNetIQ iManagerで変更することはできません。サーバで名前を変更すると、新しい名前が自動的にiManagerに表示されます。

国オブジェクト

国オブジェクトは、2文字の標準ISOカントリコードに従って命名します。

詳細については、ISO 3166 Code Lists (https://www.iso.org/iso-3166-country-codes.html)を参照してください。

多言語環境の注意事項

複数の言語で稼動しているワークステーションがある場合は、必要に応じて、オブジェクト名に使用する文字を、すべてのワークステーションで表示できる文字のみに制限します。たとえば、ワークステーションを日本語環境で使用している場合には、ヨーロッパの言語で表示できない文字を名前に使用しないよう制限します。

重要: Tree名は必ず英語で指定するようにします。

標準ドキュメントの例

次は、最もよく使用される一部のプロパティに関する標準ドキュメントの例です。使用しないプロパティについては、標準を規定する必要はありません。標準ドキュメントは、オブジェクトの作成または修正を担当するすべての管理者に配布します。

オブジェクトクラス | プロパティ	Standard	例	理由
ユーザ | ログイン名	ファーストネームのイニシャル、ミドルネームのイニシャル(ある場合)、姓の組み合わせ(すべて小文字)。最大8文字です。各共通名はすべて、社内全体で固有のものにします。	msmith、bjohnson	eDirectoryでは会社全体で固有の名前を使用する必要はありませんが、固有にすると、同じコンテキスト(またはバインダリコンテキスト)内での不整合を避けることができます。
ユーザ | 姓	姓(通常の大文字/小文字表記)。	Smith	メールラベルの生成に使用されます。
電話番号およびFax番号	ハイフンで区切られた番号。	米国: 123-456-7890、その他: 44-344-123456	自動ダイヤルソフトウェアで使用されます。
複数のクラス | 地域	2文字の地域コード(大文字)、ハイフン、メール配達地点の組み合わせ。	BA-C23	社内のメール配達で使用されます。
組織 | 名前	すべてのツリーに与える会社名。	YourCo	独立したツリーがある場合、標準の組織名を使用することで、将来ツリーのマージができます。
部門 | 名前(ロケーションに基づく)	2または3文字の地域コードで、すべて大文字。	ATL、CHI、CUP、LA、BAT、BOS、DAL	短く、標準的な名前を使用することで、効率的に検索できます。
部門 | 名前(部署に基づく)	部署名または略語。	Sales、Eng	短く、標準的な名前を使用することで、どの部署で使用しているコンテナか見分けやすくなります。
グループ | 名前	わかりやすい名前。	Project Managers	ユーティリティによってはすべて表示できない場合があるため、極端に長い名前を避けてください。
ディレクトリマップ | 名前	ディレクトリマップが示すディレクトリの内容。	DOSAPPS	短く、標準的な名前を使用することで、どの部署で使用しているコンテナか見分けやすくなります。
プロファイル | 名前	プロファイルの目的。	MobileUser	短く、標準的な名前を使用することで、どの部署で使用しているコンテナか見分けやすくなります。
サーバ | 名前	SERV、ハイフン、部署、ハイフン、固有番号の組み合わせ。	SERV-Eng-1	eDirectoryでは、ツリー内で固有のサーバ名を使用する必要があります。

Treeの上位層を設計する

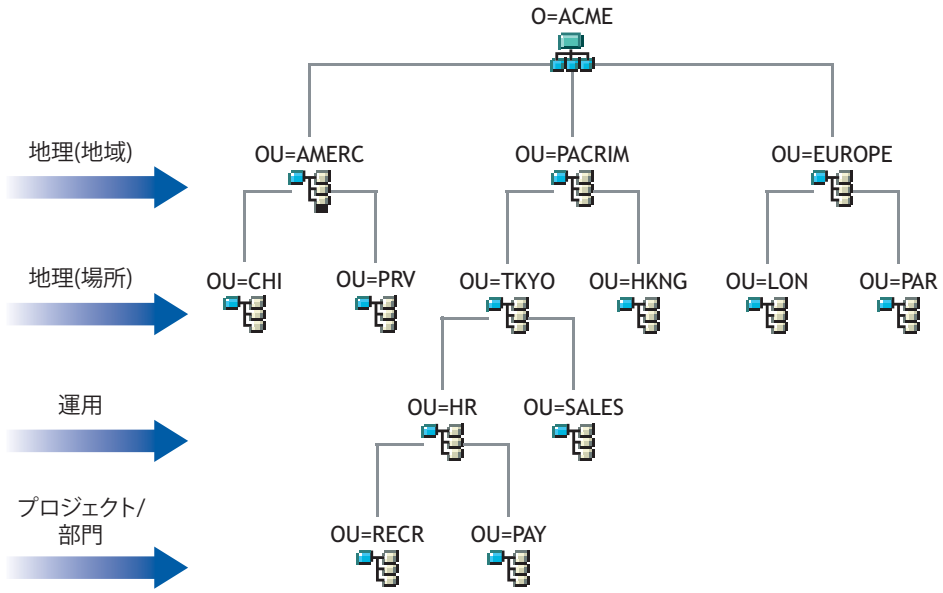
ツリーの上位層を変更するとツリーの残りの部分すべてに影響するため、ツリーの上位層は慎重に設計します。WANリンクがある場合は、特に注意する必要があります。ツリーの最上部は、後からの変更がなるべく必要でないように設計します。

eDirectoryツリーの作成時には、次のeDirectory設計規則に従います。

- ピラミッド型の設計を使用する。
- eDirectoryツリーは1つにし、固有の名前を付ける。
- 組織オブジェクトを1つ作成する。
- 物理的なネットワーク構造を表す第1レベルの部門群を作成する。

図 2-1は、eDirectory設計規則を示しています。

図 2-1 *eDirectory設計規則*



ツリーの上位層を作成するには、105 ページの 「オブジェクトを作成する」および105 ページの 「オブジェクトのプロパティの変更」を参照してください。

ピラミッド型の設計の使用

ピラミッド型のeDirectoryでは、管理や、大きなグループに対する変更、および論理パーティションの作成をより容易に実行できます。

ピラミッド型の代わりに使用できる設計として、フラットツリー型があります。フラットツリー型では、すべてのオブジェクトがツリーの最上部に置かれます。eDirectoryではフラットツリー型の設計もできますが、管理やパーティション化がより難しくなる可能性があります。

固有の名前を持つ単一のeDirectoryツリーの使用

ほとんどの組織では、ツリーを1つにするのが最適です。デフォルトでは、ツリーは1つだけ作成されます。ツリーが1つだけだと、ネットワーク内のユーザの識別を統一でき、セキュリティ管理もより容易になります。また、1箇所で集中管理できます。

業務では単一のツリーの使用を推奨しますが、追加のツリーのテストや開発を否定するわけではありません。

組織によっては、法的または政治的な問題、あるいは社内の事情から、複数のツリーが必要になる場合もあります。たとえば、自立した7つの組織から構成される組織では、7つのツリーが必要になることも考えられます。組織で複数のツリーが必要な場合は、管理を容易にするためにNetIQ Identity Managerを使用することを検討してください。Identity Managerの詳細については、『*NetIQ Identity Manager Setup Guide (NetIQ Identity Managerセットアップガイド)*』を参照してください。

ツリーには、他のツリー名と重複しない、固有の名前を付けます。「EDL-TREE」のように、短くてわかりやすい名前を指定します。

同じネットワーク内に同じ名前のツリーが存在すると、次のような問題が発生する場合があります。

- 更新内容が、対象のツリーとは別のツリーに適用される
- リソースが消失する
- 権利が消失する
- データが破損する

DSMergeユーティリティを使用してツリー名を変更できますが、変更する際には十分に注意する必要があります。ツリー名の変更はネットワーク全体に影響します。ツリー名を変更した場合は、新しいツリー名でクライアントを再設定する必要があります。

単一の組織オブジェクトの作成

通常、1つのeDirectoryツリーには、1つの組織オブジェクトを作成します。デフォルトでは、組織オブジェクトが1つ作成され、それに会社名に基づいた名前が付けられます。これにより、会社全体に適用される変更をツリー内の1個所から設定できます。

たとえば、ZENworks®を使用して、組織オブジェクトの中にワークステーションインポートポリシーオブジェクトを作成できます。このポリシーは、eDirectory内にワークステーションオブジェクトを作成するときの命名方法を定義するもので、組織全体に影響します。

組織コンテナには、次のオブジェクトが作成されます。

- Admin
- サーバ
- ボリューム

  eDirectoryを実行しているWindowsまたはLinuxサーバのみを含むネットワークには、ボリュームオブジェクトがありません。

次のようなケースでは、組織オブジェクトを複数作成することが必要になる場合があります。

- 複数の会社から構成される企業で、それぞれの会社が個別にネットワークを構成している。

- 社内で、独立した業務単位または組織を表す必要がある。
- 各部門が独立した形態をとることを規定する社内ガイドラインやポリシーがある。

物理的なネットワークを表す部門を作成する

第1レベルの部門設計は、eDirectoryの効率性とパーティション化に影響するため重要です。

LANまたはWANを使用して複数のビルや場所などにまたがって構成されているネットワークでは、所在地に基づいて第1レベルの部門オブジェクトを設計します。これにより、1つのパーティション内のすべてのオブジェクトが1箇所に維持されるように、eDirectoryを分割できます。また、各場所でのセキュリティの設定や管理者の割り当ても容易になります。

ツリーの下位層を設計する

ツリーの下位層は、ネットワークリソースの編成に基づいて設計します。eDirectoryツリーの下位層の設計は同じ場所に存在するオブジェクトにのみ影響するため、下位層は上位層よりも自由に設計できます。

ツリーの下位層を作成するには、105 ページの 「オブジェクトを作成する」および105 ページの 「オブジェクトのプロパティの変更」を参照してください。

コンテナ、ツリー、およびデータベースのサイズを決定する

作成する下位層のコンテナオブジェクトの数は、ツリー内のオブジェクトの総数、空きディスク容量、およびディスクの入出力速度制限によって決まります。eDirectoryは、1つのeDirectoryツリー内に10億以上のオブジェクトを格納できることがテストで確認されています。したがって、実際に制約となる項目は、空きディスク容量とディスクの入出力速度、およびパフォーマンスを維持するためのRAMです。大規模なツリーの場合は、レプリカの同期処理が大きく影響することにも注意が必要です。

eDirectory内の一般的なオブジェクトのサイズは3～5KBです。この数値に基づいて、現在保持している、または新たに作成するすべてのオブジェクトの保管に必要な空きディスク容量をすばやく計算できます。オブジェクトのサイズは、データに付属する属性の数や、データの内容に対応して大きくなります。画像やサウンド、または生物統計学などのBLOB(バイナリラージオブジェクト)データを格納するオブジェクトの場合、そのサイズは増加します。

パーティションのサイズが大きくなるほど、レプリケーションのサイクルは遅くなります。ZENworksやDNS/DHCPサービスなど、eDirectoryを使用する必要がある製品を使用する場合、これらの製品によって作成されたeDirectoryオブジェクトにより、格納先のコンテナのサイズが影響を受けます。場合によっては、DNS/DHCPなど、管理目的のみで使用するオブジェクトは固有のパーティションに格納するように検討してください。パーティションを別にすれば、レプリカの同期処理の速度の低下によってユーザのアクセスに支障をきたすことを避けることができます。また、パーティションとレプリカの管理も容易になります。

必要な場合は、eDirectoryデータベースまたはDIB(ディレクトリ情報ベース)セットのサイズを簡単に判別できます。

- Windowsの場合は、\novell\nds\dibfilesにあるDIBセットを確認します。
- Linuxの場合は、インストール時に指定したディレクトリにあるDIBセットを確認します。

作成するコンテナを決定する

通常、同じ必要性からアクセスされるeDirectoryオブジェクトをまとめて格納するコンテナを作成します。それにより、1つのトラスティ割り当てまたはログインスクリプトで多くのユーザにサービスを提供できます。特にログインスクリプトをより効率的にすることを目的としてコンテナを作成できるほか、1つのコンテナに2つの部署を割り当てることによって、ログインスクリプトの管理をより容易にすることもできます。

ネットワーク内のトラフィックを制限するため、ユーザは各自が必要とするリソースの近くに配置するようにします。たとえば、同じ部署で働く社員は、通常、隣り合った位置で作業します。それらの社員は同じファイルシステムにアクセスし、同じプリンタを使用して印刷します。

一般的なワークグループ境界の例外については、容易に対処できます。たとえば、2つのワークグループが共通のプリンタを使用するような場合は、一方のワークグループのプリンタに対して別名オブジェクトを作成します。グループオブジェクトを作成することによって、1つのワークグループ内だけでなく、複数のワークグループに存在する一部のユーザオブジェクトをまとめて管理できます。また、固有のログインスクリプト要件を持つ、一部のユーザ用のプロファイルオブジェクトも作成できます。

ツリーのパーティション化のガイドライン

eDirectoryにパーティションを作成すると、データベースの各部分は複数のサーバに分割して格納されます。パーティション化によって、eDirectoryデータ処理と保管の負荷がネットワーク内の複数のサーバに分散されるため、ネットワークの使用を最適化できます。デフォルトでは、パーティションは1つだけ作成されます。パーティションの詳細については、58 ページの 「パーティション」を参照してください。パーティションの作成については、151ページの第6章「パーティションおよびレプリカの管理」を参照してください。

次のガイドラインは、ほとんどのネットワークに適用できる一般的な規則です。特定の環境設定、ハードウェア、およびトラフィックの処理量など、それぞれのネットワークの運用条件に合わせて若干の調整が必要になる場合もあります。

ツリーの上位層におけるパーティションを決定する

ツリーをピラミッド型に設計するのと同じように、パーティションもピラミッド型に構成します。パーティションの構造は、ツリーの最上位に少数のパーティションがあり、下位になるに従ってパーティションの数が増えていくようにします。このような設計では、下位層より上位層のほうがパーティション数が多いツリー構造に比べて、作成されるサブオーディネートリファレンスの数が少なくなります。

ツリーをピラミッド型に設計するには、常にリーフオブジェクト(特にユーザ)の比較的近くにパーティションを作成するようにします

注: インストール時にツリーのルートに作成されるパーティションについては例外です。

上位層のパーティションを設計する場合は、次の点を考慮します。

- WANインフラストラクチャに基づいて、ツリーの最上部をパーティション化する。ツリーの最上部にはパーティションを少なめに配置し、下位になるに従ってパーティションの数を増やします。

  WANリンクによって区切られている各サイトのコンテナを作成し(各サーバオブジェクトをそのローカルコンテナに格納)、その後、各サイトのパーティションを作成します。

- WANリンクを持つネットワークでは、パーティションが複数の場所にまたがらないようにする。

  パーティションを場所ごとに作成すれば、異なるサイト間のレプリケーショントラフィックによってWAN帯域幅が不必要に消費されることはありません。
- ローカルサーバを中心にしてパーティションを作成する。物理的に離れた場所にあるサーバは別のパーティションに格納します。

ツリーの下位層におけるパーティションを決定する

eDirectoryツリーの下位層のパーティションを設計する場合は、次を考慮します。

- 下位層のパーティションは、事業部、部署、およびワークグループと、それらに関連するリソースに基づいて定義する。
- 各パーティションについて、パーティション内のすべてのオブジェクトが同じ場所にあるようにする。それによって、eDirectoryへの更新がローカルサーバで行われるようになります。

パーティションサイズを決定する

eDirectoryでは、パーティションのサイズについて次の設計制限を推奨しています。

要素	制限容量
パーティションのサイズ	無制限のオブジェクト レプリカDIB(ディレクトリ情報ベース)は1TBに制限
ツリー内のパーティションの総数	無制限
ペアレントパーティションごとのチャイルドパーティション数	150
パーティションごとのレプリカ数	50 レプリカDIBによる制限
レプリカサーバごとのレプリカ数	250

NDS®6および7からのこの設計ガイドラインの変更は、NDS8におけるアーキテクチャの変更によるものです。これらの推奨値は、企業などの分散環境に適用されます。ただし、これらはeビジネスやアプリケーションには適用されない場合があります。

一般的なeビジネスユーザに対しては、すべてのデータが単一のサーバに保管されていることが必要ですが、eDirectoryでは、ツリー内のさまざまなエリアに属するオブジェクトや属性の一部を格納するフィルタ済みレプリカを作成できます。この機能を利用すると、1つのサーバにすべてのデータを保管しなくても、同じようにeビジネスに対応できます。詳細については、65 ページの「フィルタ済みレプリカ」を参照してください。

ネットワーク変数について

パーティションを設計する場合は、次のネットワーク変数について考慮します。

- サーバの数および速度

- ネットワークアダプタ、ハブ、ルータなどのネットワークインフラストラクチャの速度
- ネットワークトラフィックの量

ツリーのレプリカ作成に関するガイドライン

複数のeDirectoryパーティションを作成するだけで、耐障害性やディレクトリのパフォーマンスが向上するわけではありません。複数のレプリカを戦略的に使用することで、これらの点が向上します。レプリカの配置は、アクセス可能性や耐障害性にとってきわめて重要です。eDirectoryのデータには、できるだけすばやくアクセスできるようにする必要があります。また、eDirectoryのデータは障害対策用に複数の場所にコピーする必要があります。レプリカの作成については、151ページの第6章「パーティションおよびレプリカの管理」を参照してください。

レプリカの配置計画では、次のガイドラインを参考にしてください。

- 90 ページの 「ワークグループのニーズ」
- 90 ページの 「障害対策」
- 91 ページの 「レプリカ数を決定する」
- 92 ページの 「Treeパーティションのレプリカを作成する」
- 92 ページの 「管理用にレプリカを作成する」
- 92 ページの 「WANトラフィックを管理する」

ワークグループのニーズ

各パーティションのレプリカを、そのパーティション内の情報を使用するワークグループに物理的に近いサーバ上に作成します。WANリンクの一方の側のユーザが他方の側のサーバに格納されているレプリカに頻繁にアクセスする場合は、WANリンクの両端のサーバ上にそれぞれレプリカを作成します。

レプリカは、ユーザ、グループ、およびサービスによるアクセスが最も多い場所に配置します。2つの独立したコンテナ内の各ユーザグループが別のパーティション境界内の同じオブジェクトにアクセスする必要がある場合は、これらのユーザグループが属する2つのコンテナより1つ上のレベルにあるコンテナ内のサーバ上にレプリカを配置します。

障害対策

ディスクがクラッシュしたり、サーバがダウンした場合、別の場所にあるサーバ上のレプリカによりユーザのネットワークへの認証を行い、使用不能になったサーバに格納されているパーティション内のオブジェクトの情報を取得できます。

いくつかのサーバに同じ情報が配布されていると、ユーザのネットワークへの認証やログインなどのサービスを提供するために、1つのサーバに依存する必要がありません。

耐障害性を確保するには、ディレクトリツリーに十分な数のサーバがあれば、各パーティションについて3つのレプリカを作成します。ローカルパーティションのローカルレプリカは、最低2つは必要です。他の場所にあるデータへのアクセスを確保する場合や、負荷分散および障害対策用にデータのインスタンスを複数維持する必要があるアプリケーションを使用している場合、またeビジネスを展開している場合を除いて、通常は、レプリカの作成は3つまでで十分です。

マスタレプリカは1つだけ保持できます。その他のレプリカは、読み書き可能、読み込み専用、またはフィルタ済みレプリカとして使用します。通常、ほとんどのレプリカは、読み書き可能レプリカとして使用されます。読み書き可能レプリカは、マスタレプリカ同様、オブジェクトの表示、オブジェクトの管理、およびユーザのログインを処理できます。変更が加えられると、読み書き可能レプリカは同期情報を送信します。

読み込み専用レプリカには、書き込みはできません。読み込み専用レプリカは、オブジェクトを検索および表示できます。また、パーティションのレプリカの同期が実行されると、更新されます。

サブオーディネートリファレンスレプリカやフィルタ済みレプリカは、障害対策用にはなりません。サブオーディネートリファレンスはポインタであり、パーティションのルートオブジェクト以外のオブジェクトは格納されません。フィルタ済みレプリカには、パーティション内の特定の一部のオブジェクトのみが格納されます。

eDirectoryでは、パーティションあたりで作成できるレプリカの数に制限はありませんが、レプリカの数が増えるに従って、ネットワークトラフィックの量も増大します。障害対策とネットワークパフォーマンス、それぞれの必要性をバランスよく配慮します。

サーバ上の各パーティションには、レプリカを1つだけ格納できます。1つのサーバには、複数のパーティションのレプリカを格納できます。

組織の障害復旧計画によっては、サーバまたは特定の場所を喪失した場合、ネットワーク再構築のほとんどの作業がパーティションのレプリカを使用して行えます。サーバが1つしかない場所では、eDirectoryを定期的にバックアップします障害対策用のレプリカを作成するための、追加サーバの購入を検討してください。

注

- 一部のバックアップソフトウェアでは、eDirectoryが自動的にバックアップアップされません。
- ウイルス対策またはバックアップソフトウェアのプロセスから、eDirectoryサーバ上のDIBディレクトリを除外することをお勧めします。DIBディレクトリのバックアップは、eDirectoryバックアップツールを使って行えます。eDirectoryのバックアップの詳細については、439 ページの 「NetIQ eDirectoryのバックアップと復元」を参照してください。

レプリカ数を決定する

複数のレプリカの作成を制限する要素となるのは、それぞれのレプリカの同期で必要となる処理時間とトラフィックの量です。オブジェクトが変更されると、変更内容がレプリカリング内のすべてのレプリカに伝達されます。レプリカリング内のレプリカの数が多いほど、変更内容の同期に必要なデータの伝送量も増えます。WANリンク経由でレプリカを同期する必要がある場合、同期にかかる時間のコストが高くなります。

地理上の多くの場所でパーティションを作成した場合、一部のサーバではサブオーディネートリファレンスレプリカが多量に生成されることになります。eDirectoryでは、地域のパーティションを作成することによって、これらのサブオーディネートリファレンスをより多くのサーバに分散させることができます。

Treeパーティションのレプリカを作成する

Treeパーティションはe Directoryツリー内の最も重要なパーティションです。このパーティションの唯一のレプリカが破損した場合、そのパーティションが修復されるか、eDirectoryツリー全体が再構築されるまで、ネットワークの機能が停止します。また、Treeに関連する設計の変更はまったくできなくなります。

Treeパーティションのレプリカの作成時には、サブオーディネートリファレンスの同期にかかるコストを考慮しながら、レプリカ数を決めてください。

管理用にレプリカを作成する

パーティションの変更はマスタレプリカからのみ発生するため、中央サイトのネットワーク管理者のすぐ近くにあるサーバに各マスタレプリカを保管するようにします。一見、リモートサイトにマスタを保管するほうが理に適っているように思えるかもしれませんが、マスタレプリカはパーティション操作が行われる場所に置いてください。

パーティション作成などの重要なeDirectoryの操作は、中央サイトの特定の管理者または管理者グループが担当することを推奨します。担当者を限定することによって、eDirectoryの動作を悪化させるエラーの発生の可能性を制限できるほか、マスタレプリカを中央で一括してバックアップできます。

ネットワーク管理者は、ネットワークトラフィックが少ない時間帯を選んで、レプリカの作成などのコストの高い操作を実行します。

WANトラフィックを管理する

現在、ユーザがWANリンクを使用して特定のディレクトリ情報にアクセスしている場合、必要な情報を格納するレプリカをユーザのローカルサーバに作成することによって、ユーザのアクセス時間とWANトラフィックの量を削減できます。

マスタレプリカをリモートサイトに複製する場合や、アクセスの提供や障害対策用にWAN経由でレプリカを配置する場合には、レプリカの同期処理で使用される帯域幅について考慮します。

ローカルサイト以外の場所におけるレプリカの作成は、推奨する3つのレプリカの作成がローカルサイトで不可能な場合に耐障害性を確保するためと、アクセスを容易にするため、またマスタレプリカを中央で一括して管理および保管するためにのみ行います。

ユーザ環境についてのプランニング

eDirectoryツリーの基本構造を設計し、パーティションとレプリカを設定した後は、管理を単純化し、ネットワークリソースへのアクセスを容易にするためのユーザ環境の設定プランを立てます。ユーザ環境プランを立てるには、ユーザのニーズを確認し、エリアごとにアクセシビリティに関するガイドラインを作成します。

ユーザのニーズを確認する

ユーザのニーズを確認する際には、次の点について考慮します。

- プリンタやファイル保管領域など、物理的なネットワークに関する必要条件

1つのツリー内の複数のユーザグループ、または複数のコンテナに属する複数のユーザグループによってリソースが共有されていないか確認します。また、リモートユーザが必要とする物理的なリソースについても考慮します。

- ユーザのバインダリサービスに関する必要条件

  バインダリサービスに基づくアプリケーションはどれか、またどのユーザによって使用されるか確認します。

- アプリケーションに関する必要条件

  ユーザが必要とするアプリケーションおよびデータファイルはどれか、オペレーティングシステムは何か、またアプリケーションにアクセスする必要があるユーザまたはユーザグループは誰かを確認します。共用アプリケーションを、ZENworksなどのアプリケーションによって自動で起動するのか、または手動で起動するのか確認します。

アクセスに関するガイドラインを作成する

ユーザのニーズについての情報を収集した後、ユーザ環境の作成に使用するeDirectoryオブジェクトを決定します。たとえば、ポリシーパッケージやアプリケーションオブジェクトを作成する場合は、作成数、およびツリー内の保管先について決定します。

また、ユーザのアクセスを制限するセキュリティの実装方法についても決める必要があります。個々のセキュリティ項目に関連する、セキュリティ上の予防措置がないか検討します。たとえば、eDirectoryスーパバイザ権はファイルシステムによって継承されるため、サーバオブジェクトに対してはスーパバイザ権を付与しないよう、ネットワーク管理者に警告する場合があります。

eビジネスに対応するeDirectoryの設計

eDirectoryをeビジネスに利用する場合(サービスのポータルを提供したり、他の企業とデータを共有する場合など)、この章ですでに説明している推奨事項は適用されないことがあります。

その場合は、eビジネスに対応するeDirectoryの設計のガイドラインとして次に示す推奨事項を代わりに使用できます。

- コンテナ数を制限したツリーを作成する。

  このガイドラインは、使用するアプリケーション、およびeDirectoryの実装法に応じて適用します。たとえば、メッセージサーバをグローバルに展開する際には、この章の前半で説明した従来のeDirectory設計ガイドラインを適用したほうがより適切な場合があります。また、ユーザの管理を分散させたい場合は、管理責任のエリアごとに独立したOU(部門)を作成することが必要になる場合があります。

- 最低2つのパーティションを維持する。

  Treeレベルに作成されるデフォルトのパーティションを維持し、その他にツリーの残りの部分のパーティションを作成します。管理目的でOUを個別に作成した場合は、各OUのパーティションを作成します。

  複数のサーバに負荷を分散させるときには、パーティション数の制限を検討しますが、その場合もバックアップや障害回復用に最低2つのパーティションは維持します。

- 障害対策および負荷分散のために、ツリーのレプリカを最低3つ作成する。

  LDAPは負荷の分散を自動では行いません。LDAPの負荷を分散させるには、第4層スイッチの使用を検討します。

- eビジネス用のツリーを別に作成する。サーバやプリンタなど、ツリーに組み込むネットワークリソースを制限する。ユーザオブジェクトのみを格納するツリーの作成を検討する。

  NetIQ Identity Managerを使用すると、このユーザツリーをネットワーク情報を格納する自分の他のツリーにリンクさせることができます。詳細については、『*NetIQ Identity Manager Setup Guide (NetIQ Identity Managerセットアップガイド)*』を参照してください。

- 補助クラスを使用して、スキーマをカスタマイズする。

  カスタマやアプリケーションで標準inetOrgPersonとは異なるユーザオブジェクトが必要となる場合は、補助クラスを使用してスキーマをカスタマイズします。補助クラスを使用すると、アプリケーションの設計時にツリーを再作成しなくても、クラスで使用する属性を変更できます。

- LDIFインポートのパフォーマンスを向上させる。

  NetIQインポート/エクスポート変換ユーティリティを使用すると、eDirectoryは処理中に各オブジェクトに索引を付けます。それによって、LDIFインポートプロセスの処理速度が遅くなることがあります。LDIFインポートのパフォーマンスを向上させるには、作成中のオブジェクトの属性に基づく索引付けをいったん中止し、NetIQインポート/エクスポート変換ユーティリティを使用してから、属性の索引付けを再開します。

- NDS全体で固有の共通名(CN)を実装する。

  eDirectoryでは、異なるコンテナ間で同じ共通名を使用できます。ただし、全体で固有の共通名を使用すれば、共通名の検索で複数の応答を処理するロジックを実装しなくてすみます。

NetIQ Certificate Serverについて

NetIQ Certificate Serverでは、セキュリティコンテナオブジェクトと組織の認証局(CA)オブジェクトを作成することにより、デジタル証明書を作成、発行、および管理できます。組織の認証局オブジェクトにより、セキュリティで保護されたデータ伝送が可能になります。Web関連製品には、組織の認証局オブジェクトが必須です。eDirectory SP4サーバでは、eDirectoryツリー全体のセキュリティコンテナオブジェクトと組織の認証局オブジェクトが自動的に作成され、物理的に格納されます。どちらのオブジェクトもeDirectoryツリーの最上部に作成されます。これらのオブジェクトは、移動せずに作成時の位置にそのまま保管する必要があります。

1つのeDirectoryツリー内に存在できる組織の認証局オブジェクトは1つだけです。最初のサーバ上にすでに作成されている組織の認証局オブジェクトを、別のサーバに移動することはできません。組織の認証局オブジェクトを削除したり、再作成すると、その組織の認証局に関連する証明書はすべて無効になります。

重要: 組織の認証局オブジェクトを永続的に保管しようとするサーバを、最初のeDirectoryサーバにするようにします。組織の認証局オブジェクトの保管先のサーバは、ネットワーク内の継続して稼動する部分であり、アクセス可能で、信頼性が高くなければなりません。

インストール中のサーバがネットワーク内の最初のeDirectoryサーバでない場合、インストールプログラムは組織の認証局オブジェクトが存在するeDirectoryサーバを探し、このサーバを参照します。インストールプログラムは、セキュリティコンテナにアクセスし、サーバ証明書オブジェクトを作成します。

ネットワーク内に組織の認証局オブジェクトがまったく存在しないと、Web関連製品は機能しません。

NetIQ Certificate Serverでタスクを実行するのに必要な権利

NetIQ Certificate Serverの設定に関連するタスクを完了するには、次の表に記載されている権利を管理者が持っている必要があります。

NetIQ Certificate Serverのタスク	必要な権利
1台目のサーバを新しいツリーにインストールするか、まだベースセキュリティをインストールしていないツリーの1台目のサーバをアップグレードするためのベースセキュリティ設定	ツリーのルートのスーパバイザ権 セキュリティコンテナのスーパバイザ権
2台目以降のサーバをインストールするためのベースセキュリティ設定	サーバコンテナのスーパバイザ権 W0オブジェクト(セキュリティコンテナ内)のスーパバイザ権
組織の認証局の作成	セキュリティコンテナのスーパバイザ権
サーバ証明書オブジェクトを作成する	サーバコンテナのスーパバイザ権 組織の認証局オブジェクトのNDSPKI:プライベートキー属性の読み込み権

また、ルート管理者は、サブコンテナの管理者に次の権利を割り当てることによって、組織の認証局を使用する権限を委託することもできます。サブコンテナ管理者がSSLセキュリティを使用してNetIQ eDirectoryをインストールするには、次の権利が必要です。

- セキュリティコンテナにある組織の認証局オブジェクトのNDSPKI:プライベートキー属性の読み込み権
- KAPオブジェクト内のセキュリティコンテナにあるW0オブジェクトのスーパバイザ権

これらの権利はグループや役割に割り当てられ、ここではすべての管理者ユーザが定義されます。NetIQ Certificate Serverに関連する特定のタスクを実行するのに必要な権利の詳細リストについては、695ページの第25章「Certificate Serverについて」を参照してください。

Linuxコンピュータ上のeDirectory操作をセキュリティで保護する

eDirectoryには、PKCS (公開鍵暗号化サービス)が付属しています。PKCSには、PKI (公開鍵インフラストラクチャ)サービスを提供するNetIQ Certificate Server、NICI (Novell International Cryptographic Infrastructure)、およびSAS-SSLサーバが含まれます。

次のセクションでは、eDirectoryの操作におけるセキュリティの確保について説明します。

- 96 ページの 「サーバ上にNICIがインストールおよび初期化されているかどうかを確認する」
- 96 ページの 「サーバ上のNICIモジュールを初期化する」
- 96 ページの 「Certificate Server(PKIサービス)を起動する」
- 97 ページの 「Certificate Server(PKIサービス)を停止する」
- 97 ページの 「組織の認証局オブジェクトを作成する」

- 97 ページの 「サーバ証明書オブジェクトを作成する」
- 98 ページの 「組織の認証局の自己署名証明書のエクスポート」

外部認証局の使用については、695ページの第25章「Certificate Serverについて」を参照してください。

サーバ上にNICIがインストールおよび初期化されているかどうかを確認する

次の条件を満たしているかチェックします。これらの条件は、NICIモジュールが正しくインストールおよび初期化されていることを表します。

- ファイル/etc/nici.cfgが存在する
- ディレクトリ/var/novell/niciが存在する
- ファイル/var/novell/nici/primeniciが存在する

これらの条件を満たしていない場合、次のセクション(96 ページの 「サーバ上のNICIモジュールを初期化する」)の手順に従ってください。

サーバ上のNICIモジュールを初期化する

1 eDirectoryサーバを停止します。

- Linuxシステムでは、次のコマンドを入力します。

  /etc/init.d/ndsd stop

重要: ndsdの開始と停止には、ndsmangaeを使用することをお勧めします。

---

2 NICIパッケージがインストールされているかどうかを確認します。

- Linuxでは、次のコマンドを入力します。

  rpm -qa | grep nici

3 (状況によって実行)NICIパッケージがインストールされていない場合、インストールします。

NICIパッケージがインストールされていないと先に進みません。

4 eDirectoryサーバを開始します。

- Linuxシステムでは、次のように入力します。

  /etc/init.d/ndsd start

重要: ndsdの開始と停止には、ndsmangaeを使用することをお勧めします。

Certificate Server(PKIサービス)を起動する

PKIサービスを開始するには、次のコマンドを入力します。

npki -1

Certificate Server(PKIサービス)を停止する

PKIサービスを停止するには、次のコマンドを入力します。

npki -u

組織の認証局オブジェクトを作成する

1 NetIQ iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、『*NetIQ Certificate Server 3.3 Administration Guide*』の「Creating an Organizational Certificate Authority Object (https://www.netiq.com/documentation/edir88/crtadmin88/data/fbgccghh.html)」を参照してください。

3 ［**役割およびタスク**］ボタン  をクリックします。

4 ［**NetIQ Certificate Server**］>［**Configure Certificate Authority**］をクリックします。

組織の認証局オブジェクトが存在しない場合、［Create an Organizational Certificate Authority Object］ダイアログボックスとオブジェクトを作成するウィザードが開きます。メッセージに従ってオブジェクトを作成します。ダイアログボックスまたはウィザードページの具体的な説明については、［**ヘルプ**］をクリックしてください。

注: eDirectoryツリーは組織の認証局を1つしか格納できません。組織の認証局の作成の詳細については、698 ページの 「組織用の組織認証局を作成する」を参照してください。

サーバ証明書オブジェクトを作成する

サーバ証明書オブジェクトは、eDirectoryサーバオブジェクトを保持するコンテナに作成されます。必要に応じて、サーバ上の個々の暗号化対応アプリケーションに対して、サーバ証明書オブジェクトを個別に作成することができます。あるいは、そのサーバで使用するすべてのアプリケーションに対してサーバ証明書オブジェクトを1つ作成することもできます。

注: サーバ証明書オブジェクトと暗号化キーオブジェクト(KMO)は同じ意味です。eDirectoryオブジェクトのスキーマ名はNDSPKI:暗号化キーです。

---

1 NetIQ iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、709 ページの 「サーバ証明書オブジェクトを作成する」を参照してください。

3 ［**役割およびタスク**］ボタン  をクリックします。

4 ［**NetIQ Certificate Server**］>［**Create Server Certificate (サーバ証明書の作成)**］の順にクリックします。

これによってサーバ証明書の作成ウィザードが開始します。メッセージに従ってオブジェクトを作成します。ウィザードのページに関する具体的な説明については、［**ヘルプ**］をクリックしてください。

組織の認証局の自己署名証明書のエクスポート

自己署名付き証明書は、組織の認証局の識別情報と、組織の認証局によって署名された証明書の有効性を確認するために使用できます。

組織の認証局のプロパティページでは、このオブジェクトに関連付けられた証明書とプロパティを参照できます。［自己署名付き証明書］プロパティページでは、自己署名付き証明書を、暗号化対応のアプリケーションで使用するファイルにエクスポートできます。

組織の認証局に存在する自己署名証明書は、組織の認証局によって署名された証明書を持つサーバ証明書オブジェクトのルート認証局証明書と同じものです。組織の認証局の自己署名付き証明書をルート認証局証明書として認識するサービスでは、組織の認証局によって署名された有効なユーザやサーバが許可されます。

1 NetIQ iManagerで、［**役割およびタスク**］ボタン をクリックします。
2 ［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。
3 組織の認証局オブジェクトの名前とコンテキストを指定して、［**OK**］をクリックします。

   組織の認証局オブジェクトはセキュリティコンテナにあります。
4 ［**証明書**］タブをクリックして、［**自己署名証明書**］をクリックします。
5 **エクスポート**をクリックします。

   証明書のエクスポートウィザードが開始します。メッセージに従って証明書をエクスポートします。ウィザードのページに関する具体的な説明については、［**ヘルプ**］をクリックしてください。
6 ［証明書のエクスポートの概要］ページで、［**Save the Exported Certificate to a File**］をクリックします。

   証明書がファイルに保存され、ルート認証局として暗号化対応アプリケーションにインポートできるようになります。
7 **閉じる**をクリックします。

このファイルを、eDirectoryへのセキュア接続を確立するためのすべてのコマンドライン操作に組み込みます。

ネットワーク時刻の同期

時刻同期は、ネットワーク全体で一貫したサーバ時刻を維持するためのサービスです。時刻同期は、eDirectoryではなく、サーバのオペレーティングシステムによって提供されます。eDirectoryはeDirectory自体の内部時刻に基づいてeDirectoryパケットの正しい順序を維持しますが、その時刻はサーバのオペレーティングシステムから取得されます。

ネットワークでWindowsまたはLinuxを使用する場合は、広く利用されている時刻同期の標準であるNetwork Time Protocol (NTP)を使用してサーバを同期してください。

NTP

NTPは、UDPプロトコルスイートの一部として機能します。UDPプロトコルスイートは、TCP/IPプロトコルスイートの一部として機能します。したがって、NTPを使用するコンピュータには、TCP/IPプロトコルスイートがロードされている必要があります。インターネットへアクセスするネットワーク内のコンピュータは、いずれもインターネット上のNTPサーバから時刻を取得できます。

NTPは、国際時刻標準である協定世界時(UTC)と時刻を同期します。

NTPには、stratum(層)という概念が導入されています。stratum-1サーバには、電波時計または原子時計などの正確な時計が内蔵されています。stratum-2サーバはstratum-1サーバから時刻を取得します。同様に、各層のサーバは1つ前の層のサーバから時刻を取得します。

時刻同期ソフトウェアの詳細については、Network Time Protocol (http://www.ntp.org)のWebサイトを参照してください。

Linuxコンピュータで時刻を同期する

NTP (Network Time Protocol)デーモンxntpdを使用すると、Linuxサーバで時刻を同期できます。xntpdとは、インターネット標準時サーバと同期してシステム時刻を設定および保持するオペレーティングシステムデーモンです。

Linuxシステムでのntpdの実行については、「ntpd - Network Time Protocol (NTP) Daemon (http://www.eecis.udel.edu/~mills/ntp/html/ntpd.html)」を参照してください。

時刻同期を確認する

ツリー内の時刻が同期されているか確認するには、Treeオブジェクトに対して読み書き可能以上の権利を持つ、Tree内のいずれかのサーバから、DSRepairを実行します。

Windows

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 ［**dsrepair.dlm**］>［**開始**］の順にクリックします。
3 ［**修復**］>［**時刻同期**］の順にクリックします。

Linux

1 次のコマンドを実行します。

```
ndsrepair -T
```

3 オブジェクトの管理

NetIQ eDirectoryには、Webベースのネットワーク管理アプリケーションであるNetIQ iManagerが含まれています。これを使用すると、eDirectoryツリーのオブジェクトを管理できます。NetIQ iManagerの特長および利点については、『*NetIQ iManager管理ガイド*』を参照してください。

eDirectoryオブジェクトの管理には、オブジェクトの作成、変更、および操作が含まれます。たとえば、ユーザアカウントの作成や、ユーザの権利の管理などの作業が必要になることがあります。NetIQ iManagerを使用して、以下を行うことができます。

- オブジェクトの参照、作成、編集、および編成などの基本的な管理を行う。
- ユーザのログイン名やeDirectoryで使用されるほかの情報を指定して、ユーザアカウントを作成する。
- 権利の割り当て、同等セキュリティの付与、継承の阻止、および有効な権利の参照を行い、権利を管理する。詳細については、75 ページの 「権利の管理」を参照してください。
- 役割ベースサービスオブジェクトを通じて特定の管理アプリケーションでの管理者の役割を定義し、役割ベースの管理を設定する。

この章では次のトピックについての情報を説明します。

オブジェクトに関連する一般的なタスク

このセクションでは、eDirectoryツリーの管理で使用する基本的なタスクの手順について説明します。

eDirectoryツリーを参照する

iManagerの［**オブジェクトの表示**］ボタン()を使用すると、eDirectoryツリー内のオブジェクトを検索したりブラウズしたりできます。ツリーの構造を表示し、タスクを実行するオブジェクトを右クリックします。実行可能なタスクは、選択するオブジェクトの種類によって異なります。

オブジェクトの検索や参照は、 iManagerの［eDirectoryオブジェクトセレクタ］ページでも行えます。iManagerのほとんどの入力フィールドでは、オブジェクト名とコンテキストを指定したり、［**オブジェクトセレクタ**］ボタン  をクリックして必要なオブジェクトを検索またはブラウズしたりすることができます。［eDirectoryオブジェクトセレクタ］ページでオブジェクトを選択すると、オブジェクトおよびオブジェクトのコンテキストが入力フィールドに挿入されます。

このセクションでは、次のことを説明します。

- 102 ページの 「［オブジェクトの表示］ボタンを使用する」
- 104 ページの 「［オブジェクトセレクタ］ボタンを使用する」

［オブジェクトの表示］ボタンを使用する

次で説明する方法を使用して、管理する特定のオブジェクトを検索します。

- 102 ページの 「［参照］を使用する」
- 103 ページの 「検索の使用」

［参照］を使用する

1. iManagerの［**オブジェクトの表示**］ボタン  をクリックします。
2. ［**参照**］をクリックします。
3. オブジェクトを参照するには、次のオプションを使用します。

オプション	説明
	ツリー内を1レベル下に移動します。
	ツリー内を1レベル上に移動します。
コンテキスト	内容を表示するコンテナの名前を指定します。 このオプションを使用するには、該当するコンテナの名前を指定して［**適用**］をクリックします。
名前	オブジェクトの名前を指定します。 このフィールドには、ワイルドカード文字としてアスタリスク(*)を使用できます。たとえば「g*」と指定すると、gで始まるすべてのオブジェクト(Germany、Gregなど)が検出されます。「*te」と指定すると、teで終わるすべてのオブジェクト(Kate、Corporateなど)が検出されます。 このオプションを使用するには、該当する名前を入力して［**適用**］をクリックします。
タイプ	検索するオブジェクトのタイプを指定します。デフォルト値は、［使用可能なすべてのタイプ］です。 このオプションを使用するには、ドロップダウンリストからオブジェクトタイプを選択して、［**適用**］をクリックします。

4 目的のオブジェクトを見つけたら、オブジェクトを右クリックして、実行可能なタスクのリストから選択します。

検索の使用

1 NetIQ iManagerの［**オブジェクトの表示**］ボタン  をクリックします。

2 **検索**をクリックします。

3 ［**コンテキスト**］フィールドで、検索場所となるコンテナの名前を指定します。

［**サブコンテナを検索**］をクリックすると、現在のコンテナ内にあるすべてのサブコンテナが検索対象に含まれます。

4 ［**名前**］フィールドで、検索するオブジェクトの名前を指定します。

このフィールドには、ワイルドカード文字としてアスタリスク(*)を使用できます。たとえば「g*」と指定すると、gで始まるすべてのオブジェクト(Germany、Gregなど)が検出されます。「*te」と指定すると、teで終わるすべてのオブジェクト(Kate、Corporateなど)が検出されます。

5 ［**タイプ**］ドロップダウンリストで、検索するオブジェクトのタイプを選択します。

6 **検索**をクリックします。

7 目的のオブジェクトを見つけたら、オブジェクトを右クリックして、実行可能なタスクのリストから選択します。

［オブジェクトセレクタ］ボタンを使用する

次で説明する方法を使用して、管理する特定のオブジェクトを検索します。

- 104 ページの 「［参照］を使用する」
- 104 ページの 「検索の使用」

［参照］を使用する

1 iManagerプロパティページの［**オブジェクトセレクタ**］ボタンをクリックします。

2 ［**参照**］をクリックします。

3 オブジェクトを参照するには、次のオプションを使用します。

オプション	説明
	ツリー内を1レベル下に移動します。
	ツリー内を1レベル上に移動します。
検索対象	内容を表示するコンテナの名前を指定して、［**適用**］をクリックします。
次のオブジェクトを検索	オブジェクトの名前を指定します。 このフィールドには、ワイルドカード文字としてアスタリスク(*)を使用できます。たとえば「g*」と指定すると、gで始まるすべてのオブジェクト(Germany、Gregなど)が検出されます。「*te」と指定すると、teで終わるすべてのオブジェクト(Kate、Corporateなど)が検出されます。 このオプションを使用するには、該当する名前を入力して［**適用**］をクリックします。

検索の使用

1 iManagerプロパティページの［**オブジェクトセレクタ**］ボタンをクリックします。

2 **検索**をクリックします。

3 ［**次から検索開始**］フィールドで、検索するコンテナの名前を指定します。

［**サブコンテナを検索**］をクリックすると、現在のコンテナ内にあるすべてのサブコンテナが検索対象に含まれます。

4 ［**次のオブジェクトを検索**］フィールドで、検索するオブジェクトの名前を指定します。

このフィールドには、ワイルドカード文字としてアスタリスク(*)を使用できます。たとえば「g*」と指定すると、gで始まるすべてのオブジェクト(Germany、Gregなど)が検出されます。「*te」と指定すると、teで終わるすべてのオブジェクト(Kate、Corporateなど)が検出されます。

5 **検索**をクリックします。

オブジェクトを作成する

1 iManagerで、［役割およびタスク］ボタン  をクリックします。

2 ［ディレクトリ管理］>［オブジェクトの作成］の順にクリックします。

3 使用可能なオブジェクトクラスのリストからオブジェクトを選択して、［OK］をクリックします。

4 必要な情報を入力して、［OK］をクリックします。

必要な情報は、作成するオブジェクトのタイプによって異なります。詳細情報を表示するには、 をクリックします。

5 OKをクリックします。

オブジェクトのプロパティの変更

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［ディレクトリ管理］>［オブジェクトの変更］の順にクリックします。

3 変更する1つまたは複数のオブジェクトの名前とコンテキストを指定して、［OK］をクリックします。

4 必要に応じてプロパティページを編集します。

特定のプロパティページの詳細情報を表示するには、 をクリックします。

5 OKをクリックします。

オブジェクトをコピーする

このオプションを使用すると、既存のオブジェクトと同じ属性値を持った新しいオブジェクトを作成したり、あるオブジェクトから別のオブジェクトに属性値をコピーしたりできます。

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［ディレクトリ管理］>［オブジェクトのコピー］の順にクリックします。

3 ［コピー元のオブジェクト］フィールドで、コピーするオブジェクトの名前およびコンテキストを指定します。

4 次のいずれかのオプションを選択します。

- Create New Object and Copy Attribute Values
- Copy Attribute Values to an Existing Object

5 アクセス制御リスト(ACL)の権利を、作成/変更しているオブジェクトにコピーする場合、［ACL権利のコピー］をクリックします。

ACL権利をコピーする場合、システムやネットワークの環境によってはさらに処理時間がかかる場合があります。

6 OKをクリックします。

オブジェクトを移動する

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［ディレクトリ管理］>［オブジェクトの移動］の順にクリックします。

3 ［オブジェクト名］フィールドで、移動する1つまたは複数のオブジェクトの名前とコンテキストを指定します。

4 ［移動先］フィールドで、オブジェクトの移動先となるコンテナを指定します。

5 移動する各オブジェクトについて、元の場所に別名を作成するには、［移動したオブジェクトの代わりに別名を作成します］を選択します。

これにより、移動前の場所に依存するあらゆる操作は、操作を更新して移動後の場所を反映できるようになるまで、引き続き実行されます。

6 OKをクリックします。

オブジェクトの削除

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［ディレクトリ管理］>［オブジェクトの削除］の順にクリックします。

3 削除するオブジェクトの名前およびコンテキストを指定します。

4 OKをクリックします。

オブジェクトをリネームする

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［ディレクトリ管理］>［オブジェクトのリネーム］の順にクリックします。

3 ［オブジェクト名］フィールドで、名前変更するオブジェクトの名前およびコンテキストを指定します。

4 ［新規オブジェクト名］フィールドで、オブジェクトの新しい名前を指定します。

［新規オブジェクト名］フィールドには、オブジェクトのコンテキストを含めないでください。

5 名前変更するオブジェクトに別名を作成するには、［リネームしたオブジェクトの代わりに別名を作成］を選択します。

これにより、リネーム前のオブジェクト名に依存するあらゆる操作は、操作を更新してリネーム後のオブジェクト名を反映できるようになるまで、引き続き実行されます。

6 名前変更する前のオブジェクト名を保存するには、［古い名前を保存］をクリックします。

これにより、リネーム前のオブジェクト名が、名前プロパティに未公認の値として追加されます。古い名前を保存すると、この名前に基づいてオブジェクトを検索できます。オブジェクトのリネーム後、そのオブジェクトの［General Identification］タブの［別の名前］フィールドでリネーム前の名前を確認できます。

7 OKをクリックします。

ユーザアカウントの管理

eDirectoryのユーザアカウントの設定には、ユーザオブジェクトの作成、およびログイン制御のプロパティやユーザのネットワークコンピューティング環境の設定があります。テンプレートオブジェクトを使用すると、これらのタスクを簡単に実行できます。

ログインスクリプトを作成すると、ユーザがログインしたときに、自動的にファイルやプリンタなどの必要なネットワークリソースに接続できます。同じリソースを使用するユーザが複数いる場合、コンテナにログインスクリプトコマンドを格納して、ログインスクリプトのプロファイルを作成することができます。

このセクションでは、次のことを説明します。

ユーザアカウントを作成および変更する

ユーザアカウントは、eDirectoryツリー内のユーザオブジェクトです。ユーザオブジェクトは、ユーザのログイン名を指定するほか、eDirectoryがネットワークリソースへのユーザアクセスを制御するために使用するその他の情報を提供します。

このセクションでは、次のことを説明します。

ユーザオブジェクトを作成する

1. iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**ユーザ**］>［**ユーザの作成**］の順にクリックします。
3. ユーザ名とユーザの姓を指定します。
4. ユーザを作成するコンテナを指定します。
5. オプションで追加情報を指定して、［**OK**］をクリックします。

   使用可能なオプションの詳細については、?をクリックしてください。
6. **OK**をクリックします。

ユーザアカウントの変更

1. iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**ユーザ**］>［**ユーザの変更**］の順にクリックします。

3 変更する1人または複数のユーザの名前とコンテキストを指定して、［OK］をクリックします。

4 必要に応じてプロパティページを編集します。

特定のプロパティの詳細情報を表示するには、をクリックします。

5 OKをクリックします。

ユーザアカウントを有効にする

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［ユーザ］>［アカウントの有効化］の順にクリックします。

3 ユーザの名前とコンテキストを指定して、［OK］をクリックします。

ユーザアカウントを無効にする

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［ユーザ］>［アカウントの無効化］の順にクリックします。

3 ユーザの名前とコンテキストを指定して、［OK］をクリックします。

オプションのアカウント機能を設定する

ユーザオブジェクトを作成した後、ユーザのネットワークコンピューティング環境を設定し、追加のログインセキュリティ機能を実装できます。

ユーザのネットワークコンピューティング環境の設定

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［ユーザ］>［ユーザの変更］の順にクリックします。

3 変更する1人または複数のユーザの名前とコンテキストを指定して、［OK］をクリックします。

4 ［全般］タブで、［使用環境］ページをクリックします。

5 プロパティページに入力します。

特定のプロパティの詳細情報を表示するには、をクリックします。

6 OKをクリックします。

ユーザに追加のログインセキュリティを設定する

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［ユーザ］>［ユーザの変更］の順にクリックします。

3 変更する1人または複数のユーザの名前とコンテキストを指定して、［OK］をクリックします。

4 ［制限］タブで、必要なプロパティページに入力します。

ページの詳細情報については、をクリックしてください。

ページ	説明	LDAP属性
パスワード制限	ログインパスワードを設定します。	passwordRequired
ログインの制限	◆ アカウントを有効または無効にします。 ◆ 同時ログインセッション数を制限します。 ◆ ログインの有効期限およびロックアウトする日付を設定します。	loginDisabled loginMaximumSimultaneous loginExpirationTimeまたはloginGraceLimit
ログイン時間制限	ユーザがログインできる時間を制限します。制限を設定し、制限時間になったときにオブジェクトがログインされていると、5分間警告が表示され、5分後にまだオブジェクトがログアウトされていない場合は、そのオブジェクトをログアウトします。リモートからログインする場合は、「113 ページの 「リモートユーザのログイン時間制限」」を参照してください。	loginAllowedTimeMap
アドレス制限	このユーザがログインするネットワークの場所(ワークステーション)を制限します。このページで制限を設定しない場合、ユーザはネットワークのどの場所からでもログインできます。	networkAddressRestriction
アカウントバランス	このユーザのサーバ使用状況のアカウントを設定します。	accountBalance
不正侵入者ロックアウト	不正侵入者が検出されたためにアカウントがロックされた場合、このアカウントを操作します。不正侵入者検出の設定を管理するには、親コンテナの［不正侵入者検出］プロパティページを使用します。	lockedByIntruder

5 OKをクリックします。

コンテナ内のすべてのユーザの不正侵入者検出を設定する

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［ディレクトリ管理］>［オブジェクトの変更］の順にクリックします。

3 コンテナオブジェクトの名前とコンテキストを指定して、［OK］をクリックします。

4 ［全般］タブで、［不正侵入者検出］ページをクリックします。

5 次のオプションを選択します。

オプション	説明
不正侵入者を検出する	コンテナのユーザアカウントの不正侵入者検出システムを有効にします。
不正ログイン試行回数	連続してログインに失敗して不正侵入者検出がアクティブになるまでのログイン試行回数を指定します。ユーザがログインにこのコンテナ内のユーザアカウントを使用し、連続して失敗した回数がこの値を超えると、不正侵入者検出がアクティブになります。この数値は、コンテナの［Login Intruder Limit(不正ログイン制限)］プロパティに格納されます。
不正ログイン回数のリセット間隔	ここで指定した時間間隔以内に連続してログインに失敗すると、不正侵入者検出がアクティブになります。日、時間、および分を入力します。
検出後にアカウントをロックする	このコンテナ内のユーザアカウントに対する不正侵入者検出がアクティブになった場合にログインを無効にするかどうかを指定します。このチェックボックスがオンになっていない場合、不正侵入者検出がアクティブになってもアカウントはロックされません。このチェックボックスをオンにし、不正侵入者の検出によってユーザアカウントがロックされた場合、ユーザオブジェクトの［不正侵入者ロックアウト］プロパティの［ロックされたアカウント］チェックボックスをオフにして、アカウントのロックを解除できます。
日、時間、分	この3つのフィールドでは、不正侵入者検出がこのコンテナ内のユーザアカウントでアクティブになった場合にログインが無効になる時間が指定されます。日、時間、分の値を任意に入力するか、デフォルトの15分をそのまま使用します。指定した時間が経過すると、そのユーザアカウントのログインは再び有効になります。これらのフィールドの内容は、コンテナの［アカウントロックアウト期間］プロパティに格納されます。これら3つのフィールドの値が0と指定されている場合、ユーザアカウントは無期限にロックされます。

6 **OK**をクリックします。

不正侵入者ロックアウト無効期間の設定

この機能を使用すると、現行パスワードの前に使用されていた旧パスワードを使ってユーザがログインしようとしてもアカウントがロックされない期間を指定できます。［*No Intruder Lock Out*］オプションを選択した場合、最後のパスワード変更の時点から指定された期間にわたって、不正侵入者検出が無効になります。

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。

2 ［**NMAS**］>［**NMAS Login Methods**］>［**NDS**］をクリックします。

3 ［NDS］ページで、ユーザアカウントをロックしない期間を指定し、［**OK**］をクリックします。

ログイン時間更新間隔の無効化

ユーザのログイン時間属性の更新を無効にする間隔値を指定することができます。ユーザ、コンテナ、およびログインポリシーに対して間隔値を指定できます。セキュリティオブジェクト(LPO)またはサーバ。この機能を有効にするには、nmas.schファイルを使ってスキーマを拡張する必要があります。

ユーザに対して間隔を指定するには、次の手順を実行します。

1 iManagerで、［**役割およびタスク**］ボタン をクリックします
2 ［**NMAS役割**］>［**NMASユーザ**］をクリックします。
3 間隔を指定するオブジェクトの名前とコンテキストを指定します。
4 ［**全般**］タブで［**その他**］を選択して、［**値がない属性**］から**sasUpdateLoginTimeInterval**を選択します。
5 必要に応じて、矢印ボタンを使って**sasUpdateLoginTimeInterval**を［値がない属性］リストから［**値がある属性**］リストに移動し、［**適用**］をクリックします。

コンテナおよびLPOの更新間隔を指定するには、次の手順を実行します。

1 iManagerで、［**役割およびタスク**］ボタン をクリックします
2 ［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。
3 コンテナまたはログインポリシーオブジェクトの名前とコンテキストを指定して、［**OK**］をクリックします。
4 ［**全般**］タブの［**その他**］を選択して、［**値がない属性**］から**sasUpdateLoginTimeInterval**を選択します。
5 必要に応じて、矢印ボタンを使って**sasUpdateLoginTimeInterval**を［値がない属性］リストから［**値がある属性**］リストに移動し、［**適用**］をクリックします。

ログインスクリプトを設定する

ログインスクリプトは、ユーザがログインしたときに実行される一連のコマンドです。一般的に、ユーザとファイルやプリンタなどのネットワークリソースとの接続に使用されます。ログインスクリプトは、次の順序でユーザのワークステーション上で実行されます。

1. コンテナログインスクリプト
2. プロファイルログインスクリプト
3. ユーザログインスクリプト

ログイン中に、いずれかのログインスクリプトが見つからない場合、それをスキップしてリスト内の次のスクリプトに移ります。何も見つからない場合、デフォルトのスクリプトが実行され、検索ドライブがユーザのデフォルトサーバ上のフォルダにマップされます。デフォルトサーバは、ユーザオブジェクトの［使用環境］プロパティページで設定されます。

ログインスクリプトを作成する

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。
2 ［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。
3 ログインスクリプトを作成するオブジェクトの名前とコンテキストを指定します。

ログインスクリプトの適用先	作成先
1人のユーザのみ	ユーザオブジェクト
まだ作成されていない1人以上のユーザ	テンプレートオブジェクト
1つのコンテナ内のすべてのユーザ	コンテナオブジェクト
1つ以上のコンテナの複数のユーザ	プロファイルオブジェクト

4 **OK**をクリックします。

5 ［**全般**］タブで、［**ログインスクリプト**］ページを選択します。

6 指定するログインスクリプトコマンドを入力します。

詳細については、『*Login Scripts Guide (ログインスクリプトガイド)* (http://www.novell.com/documentation/linux_client/login/data/front.html)』を参照してください。

7 **OK**をクリックします。

ユーザにプロファイルを割り当てる

プロファイルをユーザオブジェクトと関連付けることによって、ユーザのログイン中にそのプロファイルのログインスクリプトが実行されます。ユーザが、プロファイルオブジェクトのブラウズ権、およびプロファイルオブジェクトのログインスクリプトプロパティの読み込み権を持っていることを確認してください。

詳細については、79 ページの 「eDirectoryオブジェクトまたはプロパティへの有効な権利を参照する」を参照してください。

1 iManagerで、［**役割およびタスク**］ボタン  をクリックします。

2 ［**ユーザ**］>［**ユーザの変更**］の順にクリックします。

3 ログインスクリプトを作成するユーザオブジェクトの名前とコンテキストを指定します。

4 **OK**をクリックします。

5 ［**全般**］タブで、［**ログインスクリプト**］ページを選択します。

6 プロファイルオブジェクトをこのオブジェクトに関連付けるには、［**プロファイル**］フィールドにプロファイルオブジェクトの名前とコンテキストを入力します。

7 **OK**をクリックします。

リモートユーザのログイン時間制限

ユーザオブジェクトの［ログイン時間制限］プロパティページで、ユーザがeDirectoryにログインできる時間を制限できます。デフォルトでは、ログイン時間に制限はありません。

ログイン時間制限が設定され、制限時間になったときにユーザがログインしていると、5分以内にログアウトするよう警告が表示されます。ユーザが5分経ってもまだログインしている場合、自動的にログアウトされ、保存していないデータは失われます。

ログイン要求を処理するサーバとは異なるタイムゾーンからリモートでログインする場合、ユーザに設定されたログイン時間制限の時差は調整されます。たとえば、月曜日の午前1時から午前6時までにログインが制限されており、サーバより1時間遅いタイムゾーンからリモートでログインする場合、このユーザの制限は午前2時から午前7時まで有効になります。

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。

2 ［**ユーザ**］>［**ユーザの変更**］の順にクリックします。

3 変更する1人または複数のユーザの名前とコンテキストを指定して、［**OK**］をクリックします。

4 ［**制限**］タブで、［**ログイン時間制限**］をクリックします。

5 次のオプションを選択します。

オプション	説明
タイムグリッド	タイムグリッドのそれぞれのセルは、表示されている週の1日のうちの30分を表します。赤いセルは、このオブジェクトにログインできない制限時間を表します。灰色のセルは制限されていない時間で、このオブジェクトにログインできる時間を表します。時間制限を設定するには、目的の時間をクリックして濃い灰色にします。複数の時間を選択するには、を押しながらセルをクリックし、該当するセルまでドラッグします。設定したログイン時間制限は、このオブジェクトの［Login Allowed Time Map(ログイン許可時間マップ)］プロパティに格納されます。
ログイン時間制限の追加	時間制限を追加するには、灰色のセルをクリックして、このオプションを選択します。
ログイン時間制限の削除	時間制限を削除するには、赤いセルをクリックして、このオプションを選択します。
アップデート	このボタンをクリックすると選択が有効になります。
リセット	このボタンをクリックすると、このプロパティページを開く前の状態にタイムグリッドがリセットされます。

6 **OK**をクリックします。

ユーザアカウントを削除する

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。

2 ［**ユーザ**］>［**ユーザの削除**］の順にクリックします。

3 削除するユーザの名前およびコンテキストを指定します。

4 **OK**をクリックします。

役割ベースサービスを設定する

iManagerを使用すると、管理者は、ユーザに特定の責任を割り当てたり、これらの責任を実行するために必要なツールおよびそれに伴う権利だけを与えたりすることができます。この機能を、役割ベースサービス(RBS)といいます。

役割ベースサービスによって、タスクと呼ばれる機能、および役割と呼ばれるタスクの集まりによって決定されたオブジェクトといった特定の機能だけをユーザが使用できるようにします。ユーザがiManagerにアクセスしたときに表示されるものは、eDirectory内の役割の割り当てが基になっています。表示されるのは、そのユーザに割り当てられたタスクのみです。ユーザは、管理するオブジェクトを見つけるためにツリーをブラウズする必要はありません。そのタスクのiManagerプラグインには、タスクを実行するのに必要なツールとインタフェースが用意されています。

1人のユーザには複数の役割を割り当てることができます。また、複数のユーザに同じ役割を割り当てることもできます。

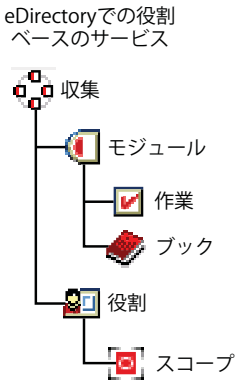
役割ベースサービスは、eDirectory内で定義されたオブジェクトとして表されます。基本のeDirectoryスキーマは、iManagerのインストール中に拡張されます。RBSオブジェクトタイプには、次の表のようなものがあります。

オブジェクト	説明
 rbsCollection	すべてのRBS役割オブジェクトおよびモジュールオブジェクトを格納するコンテナオブジェクト。 RBSコレクションオブジェクトは、すべてのRBSオブジェクトの最上位のコンテナです。ツリーにはRBSコレクションオブジェクトをいくつでも格納できます。これらのオブジェクトには、コレクションを管理する権利を持つユーザとして「所有者」が存在します。 RBSコレクションオブジェクトは次のコンテナのいずれかに作成できます。 ◆ 国 ◆ ドメイン ◆ 地域 ◆ 組織 ◆ 部門
 rbsRole	ユーザ(メンバー)が実行を許可されたタスクを指定するコンテナオブジェクト。役割の定義には、rbsRoleオブジェクトの作成や役割が実行できるタスクの指定が含まれます。 役割メンバーには、ユーザ、グループ、組織、部門があり、ツリーの特定の範囲内の役割に関連付けられています。rbsTaskオブジェクトおよびrbsBookオブジェクトは、rbsRoleオブジェクトに割り当てられます。 rbsRoleオブジェクトは、RBSコレクションコンテナ内にのみ作成できます。

オブジェクト	説明
rbsModule	rbsTaskオブジェクトおよびrbsBookオブジェクトを格納するコンテナオブジェクトです。rbsModuleオブジェクトには、タスクやブックを定義する製品の名前(たとえばeDirectory Maintenance、NMAS、NetIQ Certificate Accessなど)を表すモジュール名の属性があります。 rbsModuleオブジェクトは、RBSコレクションコンテナ内にのみ作成できます。
rbsTask	ログインパスワードのリセットなど、特定の機能を表すリーフオブジェクトです。 rbsTaskオブジェクトは、rbsModuleコンテナ内にのみ格納されます。
rbsBook	ブックに割り当てられる一連のページを含むリーフオブジェクトです。rbsBookは、1つ以上の役割および1つ以上のオブジェクトクラスタイプに割り当てることができます。 rbsBookオブジェクトは、rbsModuleコンテナ内にのみ格納されます。
rbsScope	ユーザオブジェクトごとに割り当てずにACL割り当てを実行するためのリーフオブジェクトです。rbsScopeオブジェクトは、役割が実行されるツリー内のコンテキストを表し、rbsRoleオブジェクトに関連付けられます。このオブジェクトはグループクラスから権利を継承します。ユーザオブジェクトはrbsScopeオブジェクトに割り当てられます。これらのオブジェクトは、関連付けられるツリーのスコープを参照します。 このオブジェクトは、必要な場合は動的に作成され、不要になれば自動的に削除されます。rbsScopeオブジェクトはrbsRoleコンテナ内にのみ格納されます。 **警告:** Scopeオブジェクトの環境設定を変更してはいけません。設定を変更することによって深刻な問題が発生し、システムが故障する可能性があります。

RBSオブジェクトは、次の図に示されているようにeDirectoryツリーに属しています。

図 3-1 eDirectory ツリー内のRBSオブジェクト



RBS役割を定義する

RBS役割は、ユーザが実行を許可されるタスクを指定します。RBS役割の定義には、rbsRoleオブジェクトの作成や、役割が実行できるタスク、およびユーザ、グループ、またはこれらのタスクを実行できるコンテナオブジェクトの指定などがあります。場合によっては、NetIQ iManagerプラグイン(製品パッケージ)に、変更可能な事前定義のRBS役割が備わっていることもあります。

RBS役割が実行できるタスクは、eDirectoryツリー内ではrbsTaskオブジェクトとして公開されます。これらのオブジェクトは、製品パッケージのインストールの際に自動的に追加されます。オブジェクトは1つ以上のrbsModuleに編成され、異なる機能を持つ製品モジュールに対応するコンテナとなります。

役割へのメンバーの割り当てについての詳細は、「117ページの「RBS役割のメンバーシップおよびスコープを割り当てる」」を参照してください。

- 116 ページの 「役割オブジェクトを作成する」
- 116 ページの 「役割に関連付けられたタスクを変更する」
- 117 ページの 「RBS役割のメンバーシップおよびスコープを割り当てる」
- 118 ページの 「役割ベースサービスオブジェクトを削除する」

役割オブジェクトを作成する

Create iManager Roleウィザードを使用して、新しいrbsRoleオブジェクトを作成します。新しいrbsRoleオブジェクトを作成する場合は、他のrbsRoleオブジェクトが属している同じRBSコレクションコンテナ(たとえば、役割ベースサービスコレクションコンテナ)内に作成することをお勧めします。

1. iManagerで、［**設定**］ボタン をクリックします。
2. ［**役割ベースサービス**］>［**RBSの設定**］をクリックします。
3. 新しい役割の作成場所となるコレクションをクリックします。
4. ［**役割**］タブをクリックします。
5. ［**新規**］>［**iManagerの役割**］の順にクリックします。
6. Create iManager Roleウィザードの手順に従って操作します。

役割へのメンバーの追加についての詳細は、「118ページの「カスタムRBSタスクを定義する」」を参照してください。

役割に関連付けられたタスクを変更する

各RBS役割には、それに関連付けられた使用可能なタスクがあります。特定の役割に割り当てるタスクは、必要に応じてタスクを追加したり削除したりすることで選択できます。

1. iManagerで、［**設定**］ボタン をクリックします。
2. ［**役割ベースサービス**］>［**RBSの設定**］をクリックします。
3. 役割の変更場所となるコレクションをクリックします。
4. ［**役割**］タブをクリックします。
5. 変更する役割をクリックします。

6 (オプション)タスクを役割に追加するには、次の手順を行います。

6a **追加**をクリックします。

6b 必要に応じて、矢印ボタンを使って［**すべてのタスク**］リストから［**割り当てられたタスク**］リストにタスクを移動します。

6c ［**OK**］を2回クリックします。

7 (オプション)役割からタスクを削除するには、次の手順を行います。

7a 削除するオブジェクトを選択して、［**削除**］をクリックします。

7b ［**OK**］を2回クリックします。

8 終了したら、［**閉じる**］をクリックします。

RBS役割のメンバーシップおよびスコープを割り当てる

所属する組織に必要なRBS役割を定義すると、それぞれの役割にメンバーを割り当てることができます。その際、それぞれのメンバーが役割の機能を使用できるスコープを指定します。スコープは、この役割を実行できるeDirectoryツリー内の場所またはコンテキストです。

役割へのユーザの割り当ては、次の方法で行うことができます。

- 直接
- グループおよび動的グループの割り当てによる方法役割に割り当てられているグループまたは動的グループのメンバーであれば、ユーザはその役割にアクセスできます。
- 職種の割り当てを使用する。役割に割り当てられている職種に所属する場合は、ユーザはその役割にアクセスできます。
- コンテナの割り当てを使用する。ユーザオブジェクトは、その親コンテナが割り当てられたすべての役割にアクセスできます。さらにツリーのルートまで遡るコンテナの役割にもアクセスできます。

役割との関連付けは、それぞれ異なるスコープで何度も実行できます。また、同じタスクを複数のメンバーに割り当てることもできます。

役割のメンバーシップおよびスコープを割り当てるには、次の操作を実行します。

1 iManagerで、［**設定**］ボタン  をクリックします。

2 ［**役割ベースサービス**］>［**RBSの設定**］をクリックします。

3 役割の変更場所となるコレクションをクリックします。

4 ［**役割**］タブをクリックします。

5 変更する役割を選択します。

6 ［**アクション**］>［**メンバーの関連付け**］をクリックします。

7 (オプション)役割にメンバーを追加するには、次の手順を行います。

7a ［**名前**］フィールドで、追加するオブジェクト(ユーザ、グループ、またはコンテナオブジェクト)の名前とコンテキストを指定します。

7b ［**スコープ**］フィールドで、組織または部門オブジェクトの名前とコンテキストを指定します。

7c **追加**をクリックします。

8 (オプション)役割からメンバーを削除するには、次の手順を行います。

8a 現在の役割メンバーのリストで、削除するメンバーを選択します。

8b **削除**をクリックします。

9 完了したら［**OK**］をクリックし、［**OK**］を再びクリックします。

10 **閉じる**をクリックします。

役割ベースサービスオブジェクトを削除する

1 iManagerで、［**設定**］ボタン  をクリックします。

2 ［**役割ベースサービス**］>［**RBSの設定**］をクリックします。

3 RBS役割の削除場所となるコレクションをクリックします。

4 ［**役割**］タブをクリックします。

5 変更する役割を選択します。

6 **削除**をクリックします。

7 **OK**をクリックします。

8 終了したら、［**OK**］をクリックします。

9 **閉じる**をクリックします。

カスタムRBSタスクを定義する

- 118 ページの 「iManagerタスクを作成する」
- 118 ページの 「役割の割り当てを変更する」
- 119 ページの 「タスクを削除する」

iManagerタスクを作成する

1 iManagerで、［**設定**］ボタン  をクリックします。

2 ［**役割ベースサービス**］>［**RBSの設定**］をクリックします。

3 新しいタスクの作成場所となるコレクションをクリックします。

4 ［**タスク**］タブをクリックします。

5 ［**新規**］>［**iManagerタスク**］の順にクリックします。

6 Task Builderの手順に従ってカスタムタスクを作成します。

役割の割り当てを変更する

1 iManagerで、［**設定**］ボタン  をクリックします。

2 ［**役割ベースサービス**］>［**RBSの設定**］をクリックします。

3 タスクの変更場所となるコレクションをクリックします。

4 ［**タスク**］タブをクリックします。

5 変更するタスクを選択します。

6 ［**アクション**］>［**役割の割り当て**］の順にクリックします。
7 該当する役割を［**使用可能な役割**］から［**割り当て役割**］に移動します。
8 ［**OK**］を2回クリックします。
9 **閉じる**をクリックします。

タスクを削除する

1 iManagerで、［**設定**］ボタン  をクリックします。
2 ［**役割ベースサービス**］>［**RBSの設定**］をクリックします。
3 タスクの削除場所となるコレクションをクリックします。
4 ［**タスク**］タブをクリックします。
5 削除するタスクを選択します。
6 **削除**をクリックします。
7 **OK**をクリックします。
8 終了したら、［**OK**］をクリックします。
9 **閉じる**をクリックします。

4 バックグラウンドプロセスの管理

大規模な動的環境に対応する目的で、eDirectoryには、環境に合わせてシステムを調整するための最適化されたバックグラウンドプロセスと環境設定オプションが備わっています。

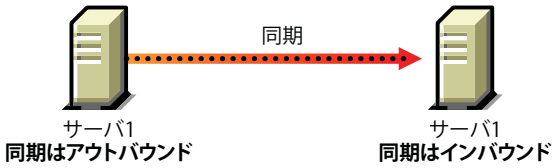
この章には、次のトピックが含まれています。

同期

同期とは、ディレクトリ情報をレプリカ間で転送し、各パーティション内の情報が互いに整合性を保つようにすることです。eDirectoryにより、レプリカリング内のサーバは自動的に同期されます。

同期には、インバウンド同期とアウトバウンド同期があります。たとえば、データに加えられた変更をserver1とserver2の間で同期する必要がある場合、*「アウトバウンド」という用語は、server1からserver2に送信される同期プロセスを意味します。*「インバウンド」という用語は、server2によって受信されたserver1からの同期プロセスを意味します。

図 4-1 *アウトバウンド同期とインバウンド同期*



同期には、次の2つのタイプがあります。

- 通常同期またはレプリカ同期
- 優先度同期

次の表に、通常同期と優先度同期の比較を示します。

表 4-1 *通常同期またはレプリカ同期と優先度同期の比較*

通常同期またはレプリカ同期	優先度同期
レプリカリング内の任意のサーバのデータに変更が加えられた場合にトリガされます。	重要データとして指定しているデータに変更が加えられた場合のみトリガされます。
詳細については、124 ページの 「通常同期またはレプリカ同期」を参照してください。	詳細については、126 ページの 「優先度同期」を参照してください。
データが変更されると、変更内容はバッファに保存されます。通常同期は、変更内容が保存されてから約30秒後に開始されます。	重要データへの変更はバッファに保存されません。優先度同期は、データが変更された直後に開始されます。

通常同期またはレプリカ同期	優先度同期
eDirectoryで最も重要な同期です。変更が優先度同期によって同期されているかどうかにかかわらず実行されます。	通常同期を補完するものです。重要な属性は優先度同期によって同期され、通常同期によって再度同期されます。
eDirectory 8.8サーバ間または以前のバージョンのeDirectoryをホストするサーバ間で実行可能です。	同じパーティションを保持しているeDirectory 8.8以降のサーバ間でのみ実行されます。
機能上、失敗することはありません。 詳細については、122 ページの 「同期の特徴」を参照してください。	優先度同期が失敗した場合、重要なデータへの変更は通常同期によって同期されます。 詳細については、133 ページの 「優先度同期が失敗する場合」を参照してください。

注: 優先度同期情報は、ndstrace、dstrace、またはiMonitorトレース画面内のSYDLまたは同期詳細タグにあります。

同期の特徴

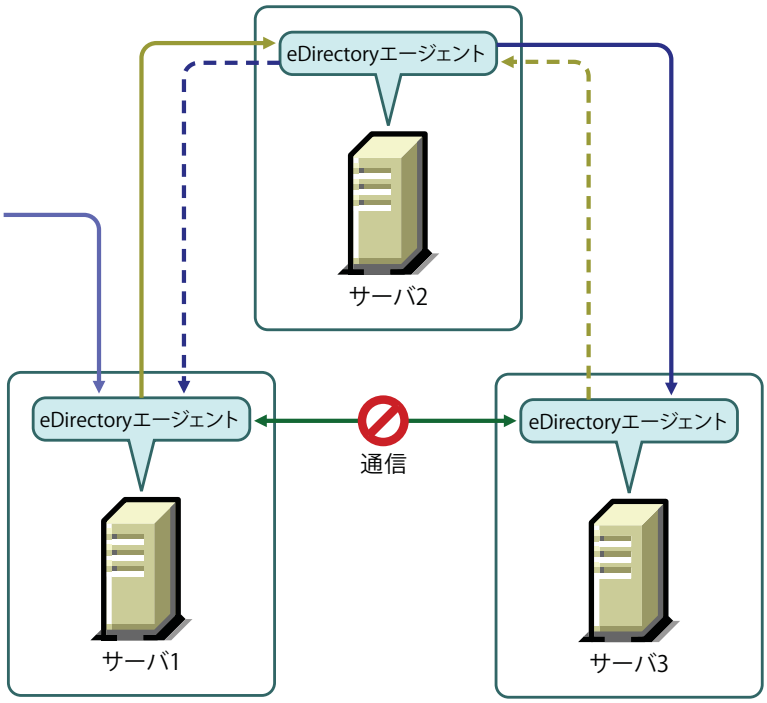
eDirectoryでの同期には、次のような特徴があります。

- 遷移同期です。
- オブジェクトトランザクションモデルを維持します。
- 遷移ベクトル、local received up to、およびremote received up toなどのタイムスタンプがあります。

遷移同期

eDirectoryでの同期は遷移同期です。つまり、eDirectoryでデータへの変更を同期する場合、eDirectoryエージェントがレプリカリング内の他のすべてのエージェントに直接接続して変更を同期する必要はありません。

図4-2 遷移同期



たとえば、Server 1でデータに変更を加えた場合、その変更はServer 1からServer 2、およびServer 2からServer 3に同期されます。通信上の問題のためServer 1がServer 3に直接接続できなかった場合でも、Server 3はServer 2を介してデータへの最新の変更内容を受信します。Server 3は、変更内容を受信したことをServer 2に通知します。次にServer 2は、Server 3とServer 2が同期していることをServer 1に通知します。

オブジェクトトランザクションモデル

eDirectoryでの同期では、LDAPおよびX.500準拠ディレクトリの標準であるオブジェクトトランザクションモデルが維持されます。オブジェクトトランザクションモデルでは、新しいトランザクションを同期する前に、以前のすべてのトランザクションを同期する必要があります。

たとえば、サーバ上でデータにD1、D2、およびD3という変更を加えたとします。ネットワーク障害のため、これらの変更は他のサーバ間で同期されません。サーバ上で別のD4という変更を行った場合、D1、D2、およびD3がレプリカリング内のすべてのサーバ間で同期された後でのみ、D4が同期されます。

遷移ベクトル

遷移ベクトルとは、レプリカのタイムスタンプのことです。レプリカ作成時刻を1970年1月1日からの経過秒数で表したものと、レプリカ番号、および現在のイベント番号を組にして表示されます。例: s3D35F377 r02 e002

詳細については、452 ページの 「遷移ベクトルと復元後の検証処理」を参照してください。

Local Received Up To

Local Received Up To (LRUT)は、ローカルレプリカが変更内容を受信するまでの時間です。

詳細については、257 ページの 「ツリー内のオブジェクトの参照」を参照してください。

Remote Received Up To

Remote Received Up To (RRUT)は、リモートレプリカのLRUTです。

詳細については、257 ページの 「ツリー内のオブジェクトの参照」を参照してください。

通常同期またはレプリカ同期

通常同期またはレプリカ同期は、eDirectoryにおける2つの同期プロセスの1つです。通常同期では、サーバ上のデータへの変更がすべて、レプリカリング内の他のサーバと同期されます。

通常同期は、同じパーティションを持つ任意のバージョンのeDirectoryが実行されているすべてのサーバ間で行われます。

詳細については、155 ページの 「レプリカの管理」を参照してください。

通常同期を有効または無効にするには、NetIQ iMonitorでアウトバウンド同期およびインバウンド同期を有効または無効にします。インバウンド同期およびアウトバウンド同期は両方とも、デフォルトでは有効になっています。通常同期を介して他のサーバ間でデータへの変更を同期するには、iMonitorで同期パラメータを設定する必要があります。詳細については、「252 ページの 「DSエージェントを制御および環境設定する」」を参照してください。

通常同期では、データに変更が加えた場合、変更内容はサーバ間で同期される前に、バッファに保存されます。サーバの同期ステータスは、iMonitorで表示できます。詳細については、「257 ページの 「ツリー内のオブジェクトの参照」」を参照してください。

通常同期は遷移同期であり、オブジェクトトランザクションモデルが維持されます。詳細については、101ページの「遷移同期」および「オブジェクトトランザクションモデル」を参照してください。

通常同期を設定する

通常同期を設定するには、iMonitorの［エージェント同期］にある［エージェント環境設定］を使用します。

この節では、次のトピックについて説明します。

通常同期を有効/無効にする

通常同期を有効または無効にするには、iMonitorでアウトバウンド同期およびインバウンド同期を有効または無効にします。詳細については、「252 ページの 「DSエージェントを制御および環境設定する」」を参照してください。

アウトバウンド同期は、デフォルトで有効になっています。このオプションをサーバで無効にしている場合、このサーバ上のデータへの変更は、他のサーバと同期されません。アウトバウンド同期を無効にする期間(単位は時間)を指定できます。デフォルト(最大時間)は24時間です。指定された期間が過ぎると、そのサーバでデータに加えられた変更が他のサーバと同期されるようになります。

インバウンド同期は、デフォルトで有効になっています。サーバに対してこのオプションを無効にすると、他のサーバでデータに加えられた変更がそのサーバと同期されなくなります。

インラインキャッシュを有効/無効にする

サーバのインラインキャッシュ変更を有効または無効にできます。インラインキャッシュ変更は、アウトバウンド同期が無効になっている場合のみ、無効にできます。アウトバウンド同期を有効にすると、インラインキャッシュ変更も有効になります。

インラインキャッシュ変更を無効にすると、このレプリカの変更キャッシュに無効のマークが付き、［**エージェント環境設定**］>［**パーティション**］に無効フラグが付きます。インラインキャッシュ変更を有効にすると、変更キャッシュの再構築時に、無効な変更キャッシュのフラグが削除されます。

同期スレッド

アウトバウンド同期を行うには、同期スレッドを設定する必要があります。iMonitorで、［**エージェント同期**］の下にある［**エージェント環境設定**］を使用して同期スレッド数を指定できます。有効な値は1～16です。詳細については、252 ページの 「DSエージェントを制御および環境設定する」を参照してください。

同期メソッド

通常、eDirectoryでは、レプリカおよびレプリケーションパートナーの数に基づいてメソッドが自動的に選択されます。同期メソッドは、次のとおりです。

- **パーティションごと:** データへの変更は、他のレプリカと同時に同期されます。変更の同期には複数のスレッドが使用されます。たとえば、レプリカR1のデータにD1、D2、およびD3という変更が加えられ、これらの変更をレプリカR2およびR3の間で同期させる必要がある場合、D1、D2、およびD3はR2およびR3と同時に同期されます。
- **サーバごと:** データへの変更は順次に同期されます。変更の同期には1つのスレッドのみが使用されます。たとえば、レプリカR1のデータにD1、D2、およびD3という変更を加えたとします。これらの変更をレプリカR2およびR3の間で同期させる必要があります。まず、D1がR2およびR3と同期されます。次に、D2がR2およびR3と同期されます。
- **ダイナミック調整:** 割り当てたシステムリソースに基づいて、eDirectoryによって同期メソッドが自動的に選択されます。

iMonitorで、［**エージェント同期**］の下の［**エージェント環境設定**］を使用して同期メソッドを指定できます。詳細については、252 ページの 「DSエージェントを制御および環境設定する」を参照してください。

注: eDirectory9.0以降では、Skulkerはデータトランザクションが正常に完了するとただちに、遅延なく同期を開始します。これは、eDirectoryの操作のパフォーマンスに影響する場合があります。eDirectoryの操作のパフォーマンスを向上させたい場合、NDSD_CC_SKULK_DELAY環境変数をエクスポートすることによって、同期に遅延を導入することができます。この変数の値は、次の例のように秒単位でのみ入力できます。

```
NDSD_CC_SKULK_DELAY=<SECONDS>
NDSD_CC_SKULK_DELAY=5
```

上の例では、eDirectoryサーバ間のデータの同期の遅延は5秒間です。同期がすでに進行中の場合は、即時スカルキングがスケジュールに影響することはありません。

優先度同期

優先度同期は、eDirectoryにおける2つの同期プロセスの1つです。優先度同期を使用すると、通常同期を待たずに重要なデータを同期することができます。

優先度同期はeDirectoryでの通常の同期プロセスを補うものです。通常同期とは異なり、優先度同期では、変更内容はサーバ間で同期される前にバッファに保存されません。そのため、優先度同期は通常同期より高速になります。

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	✓	✓

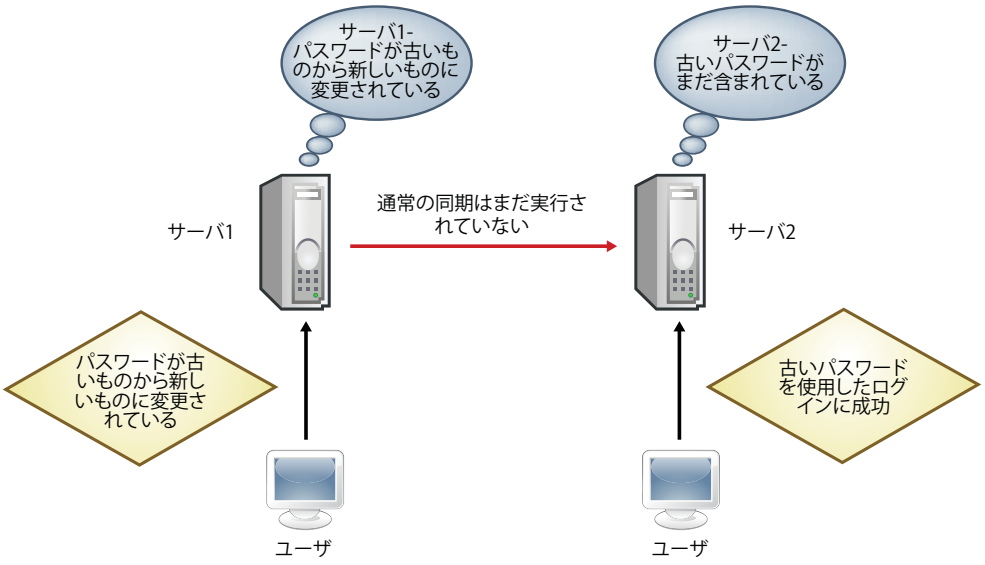
このセクションでは、次の情報を紹介します。

- 126 ページの 「優先度同期の必要性」
- 127 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4-3 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、 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。

優先度同期は、デフォルトで有効になっています。詳細については、「128ページの「インバウンド優先度同期およびアウトバウンド優先度同期を有効/無効にする」」を参照してください。

優先度同期を介して重要なデータへの変更を同期するには、次の手順を実行します。

1 優先度同期のスレッド数を指定します。

詳細については、128 ページの 「優先度同期スレッド」を参照してください。

2 優先度同期キューサイズを指定します。

詳細については、128 ページの 「優先度同期キューサイズ」を参照してください。

3 優先度同期ポリシーを作成して定義するには、優先度同期を介して同期する重要な属性を指定します。

詳細については、131 ページの 「優先度同期ポリシーを作成および定義する」を参照してください。

4 優先度同期ポリシーを1つ以上のパーティションに適用します。

詳細については、132 ページの 「優先度同期ポリシーを適用する」を参照してください。

優先度同期プロセスでは、重要な属性への変更のみが同期されます。優先度同期では、オブジェクトトランザクションモデルが維持されます。したがって、重要ではないデータが変更され、まだ同期されていない場合、および重要なデータが同じエントリで変更された場合には、重要ではないデータが重要なデータとともに同期されます。

たとえば、ユーザがIncome、Employee No、Address、Cube Noという属性を持っているとします。その中のIncomeとAddressが重要な属性です。Employee NoおよびCube Noは変更されていますが、これらの変更はまだ同期されていません。IncomeおよびAddressへの変更が優先度同期を介して同期されると、Employee NoおよびCube Noも(重要データとして指定されていませんが)同期されます。

このセクションでは、次の情報について説明します。

- 128 ページの 「インバウンド優先度同期およびアウトバウンド優先度同期を有効/無効にする」
- 128 ページの 「優先度同期スレッド」
- 128 ページの 「優先度同期キューサイズ」
- 129 ページの 「優先度同期ポリシーを管理する」
- 133 ページの 「優先度同期が失敗する場合」

インバウンド優先度同期およびアウトバウンド優先度同期を有効/無効にする

iMonitorを使って、eDirectoryでのインバウンド/アウトバウンド優先度同期を有効または無効にすることができます。詳細については、「252 ページの 「DSエージェントを制御および環境設定する」」を参照してください。

インバウンド優先度同期は、デフォルトで有効になっています。インバウンド優先度同期をサーバで無効にしている場合、他のサーバ上の重要なデータへの変更は、優先度同期ではこのサーバと同期されません。ただし、変更は通常同期プロセスによって同期されます。

アウトバウンド優先度同期は、デフォルトで有効になっています。このオプションをサーバで無効にしている場合、このサーバ上の重要なデータへの変更は、優先度同期では他のサーバと同期されません。ただし、変更は通常同期プロセスによって同期されます。

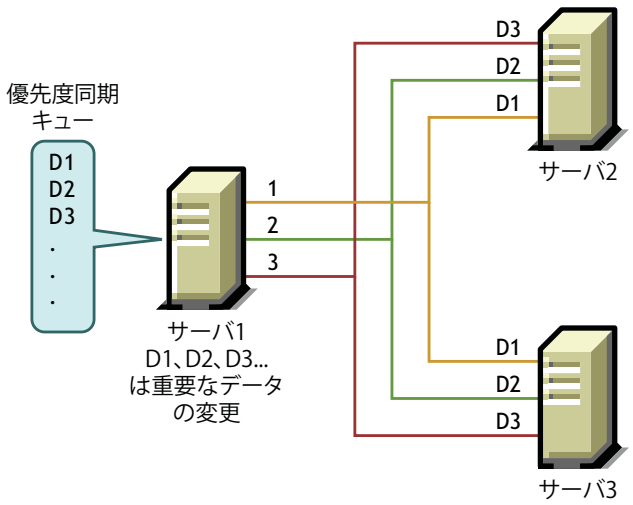
優先度同期スレッド

アウトバウンド優先度同期に使用するスレッド数を設定する必要があります。iMonitorで、［**エージェント同期**］の下にある［**エージェント環境設定**］を使用して、優先度同期スレッド数を指定できます。詳細については、252 ページの 「DSエージェントを制御および環境設定する」を参照してください。有効な値は1～32です。デフォルト値は4です。

優先度同期キューサイズ

これは、同期の前にキューで保持可能な、変更された重要なエントリの最大数です。重要なエントリは、変更されるとすぐに優先度同期キューに入れられ、順次に同期されます。たとえば、server1でD1、D2、およびD3という重要なエントリが変更されており、これらのエントリを、優先度同期を介してserver2およびserver3間で同期させる必要がある場合には、まずD1がserver2およびserver3と同期されます。次にD2がserver2およびserver3と同期され、その後、D3がserver2およびserver3と同期されます。キュー内の以前のエントリがサーバのいずれかと正常に同期していない場合でも、その他のエントリの同期には影響しません。

図4-4 優先度同期キュー



iMonitorで優先度同期キューサイズを指定するには、［**エージェント同期**］の下にある［**エージェント環境設定**］を使用します。詳細については、252 ページの 「DSエージェントを制御および環境設定する」を参照してください。

優先度同期プロセス中、多数の変更が短い間隔で行われ、キューが最大サイズに達した場合には、キューは期限切れになり、新しいキューが形成されます。まだ同期されていない古いキュー内の変更は、通常同期によって同期されます。

優先度同期のキューサイズは、0から2^{32} - 1までの範囲で変更できます。デフォルトでは、この値は2^{32} - 1に設定されています。優先度同期キューサイズが0に設定されている場合、変更は優先度同期では同期されません。これらの変更は通常同期によって同期されます。

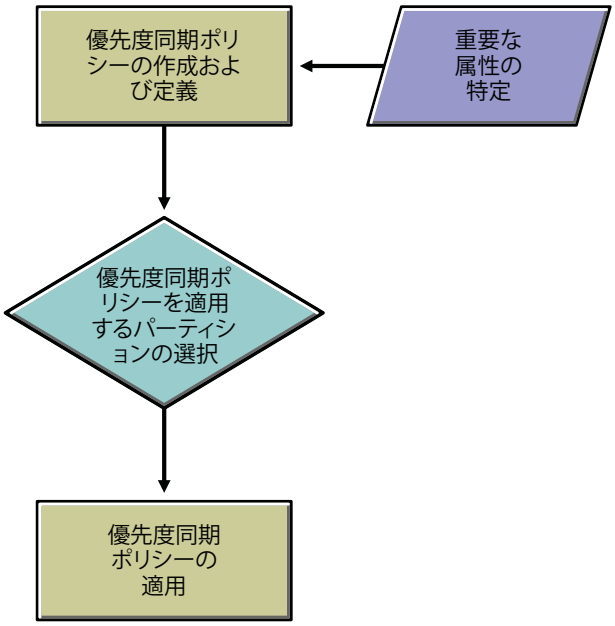
-1を指定すると、キューサイズが無限大になります。-1は2^{32} - 1です。-3などの負の値を指定した場合は、-3 = -1-2になり、2^{32} - 1-2になります。

優先度同期ポリシーを管理する

優先度同期の管理は、iManagerまたはLDAPを使用して、ポリシーを作成および定義し、パーティションに適用することで行えます。優先度同期ポリシーを定義するには、重要な属性を指定します。

注: プラグインは、NetIQ iManager 2.6以降でのみ利用できます。

図4-5 優先度同期プロセス



たとえば、PasswordおよびAccountNumberという属性が重要である場合、これらの属性を含む優先度同期ポリシーPS1を作成できます。その後、ポリシーPS1をパーティションP1に適用できます。サーバ上のエントリのパスワードまたはアカウント番号を変更した場合、その変更は、パーティションP1を持つ他のサーバと直ちに同期されます。

優先度同期が実行されるようにするには、iMonitorでアウトバウンド優先度同期およびインバウンド優先度同期が有効になっていることを確認する必要があります。インバウンド優先度同期およびアウトバウンド優先度同期は、デフォルトで有効になっています。インバウンド優先度同期およびアウトバウンド優先度同期を無効にしている場合、データへの変更は通常同期によって同期されます。

詳細については、252 ページの 「DSエージェントを制御および環境設定する」を参照してください。

この節では、次のトピックについて説明します。

- 131 ページの 「優先度同期ポリシーを作成および定義する」
- 131 ページの 「優先度同期ポリシーを編集する」
- 132 ページの 「優先度同期ポリシーを適用する」
- 133 ページの 「優先度同期ポリシーを削除する」

子パーティションを作成した場合、親に適用されている優先度同期ポリシーが子パーティションに継承されます。パーティションをマージした場合、親の優先度同期ポリシーが保持されます。

優先度同期ポリシーを作成および定義する

優先度同期ポリシーの定義は、属性を直接選択するか、オブジェクトクラスを介して選択することで行えます。オブジェクトクラスを介して属性を選択する場合は、オブジェクトクラスの下にあるすべての属性が優先度同期に選択されます。優先度同期では必須属性またはオプション属性を選択することができます。

優先度同期ポリシーは、iManagerまたはLDAPのいずれかを使用して、eDirectoryツリー内の任意の場所で作成できます。

iManagerの使用:

1. ［**役割およびタスク**］ボタン  をクリックします。
2. ［**パーティションとレプリカの管理**］>［**優先度同期ポリシー**］をクリックします。
3. 優先度同期ポリシー管理ウィザードで、［**ポリシーを作成、編集、適用します**］を選択します。
4. **次へ**をクリックします。
5. ウィザードの指示に従って、ポリシーを作成します。
   ウィザードの各段階で、［ヘルプ］が利用できます。

LDAPを使用する場合:

空の優先度同期ポリシーを作成するには、次のように指定します。

```
dn:cn=policy1,o=policies

changetype:add

objectclass:prsyncpolicy
```

優先度同期ポリシーを定義するには、優先度同期の属性をマークします。

```
dn:cn=policy2,o=policies

changetype:add

objectclass:prsyncpolicy

prsyncattributes:description
```

上の例では、Descriptionが優先度同期としてマークされた属性です。

優先度同期ポリシーを編集する

優先度同期ポリシーオブジェクトの編集は、iManagerまたはLDAPを使用して行えます。

iManagerの使用

1. ［**役割およびタスク**］ボタン  をクリックします。
2. ［**パーティションとレプリカの管理**］>［**優先度同期ポリシー**］をクリックします。
3. 優先度同期ポリシー管理ウィザードで、［**ポリシーを編集します**］を選択します。
4. **次へ**をクリックします。
5. ウィザードの指示に従って、ポリシーを編集します。
   ウィザードの各段階で、［ヘルプ］が利用できます。

LDAPを使用する場合

次の例では、DescriptionではなくSurnameを優先度同期としてマークすることで、優先度同期ポリシーが変更されています。

```
dn:cn=policy2,o=policies

changetype:modify

add:prsyncattributes

prsyncattributes:surname
```

優先度同期としてマークされている属性を優先度同期ポリシーから削除するには、次のように指定します。

```
dn:cn=policy2,o=policies

changetype:modify

add:prsyncattributes

prsyncattributes:description
```

上の例では、属性Descriptionが優先度同期ポリシーから削除されています。

優先度同期ポリシーを適用する

1つの優先度同期ポリシーを多数のパーティションに適用できますが、複数のポリシーを1つのパーティションに適用することはできません。

優先度同期ポリシーをパーティションに適用するには、iManagerまたはLDAPを使用して行えます。

iManagerの使用:

1. ［**役割およびタスク**］ボタン  をクリックします。
2. ［**パーティションとレプリカの管理**］>［**優先度同期ポリシー**］をクリックします。
3. 優先度同期ポリシー管理ウィザードで、［**ポリシーを作成、編集、適用します**］を選択します。
4. ウィザードの指示に従って、ポリシーを適用します。
   ウィザードの各段階で、［ヘルプ］が利用できます。

LDAPを使用する場合:

優先度同期ポリシーをルートパーティションに適用するには、次のように指定します。

```
dn:

changetype:modify

add:prsyncpolicydn

prsyncpolicydn:cn=policy2,o=policies
```

上の例では、policy2がルートパーティションに適用されています。

優先度同期ポリシーを非ルートパーティションに適用するには、次のように指定します。

```
dn:o=org

changetype:modify

add:prsyncpolicydn
```

```
prsyncpolicydn:cn=policy2,o=policies
```

上の例では、policy2が非ルートパーティションに適用されています。

非ルートパーティションの優先度同期ポリシーを置き換えるには、次のように指定します。

```
dn:o=org

changetype:modify

replace:prsyncpolicydn

prsyncpolicydn:cn=policy1,o=policies
```

上の例では、policy2がpolicy1に置き換えられています。

優先度同期ポリシーと非ルートパーティションとの関連付けを解除するには、次のように指定します。

```
dn:o=org

changetype:modify

delete:prsyncpolicydn
```

上の例では、優先度同期ポリシーと非ルートパーティションO=Orgとの関連付けが解除されています。

優先度同期ポリシーを削除する

優先度同期ポリシーの削除は、iManagerまたはLDAPを使用して行えます。

iManagerの使用:

1. ［**役割およびタスク**］ボタン  をクリックします。
2. ［**パーティションとレプリカの管理**］>［**優先度同期ポリシー**］をクリックします。
3. 優先度同期ポリシー管理ウィザードで、［**ポリシーを削除します**］を選択します。
4. ウィザードの指示に従って、ポリシーを削除します。
   ウィザードの各段階で、［ヘルプ］が利用できます。

LDAPを使用する場合:

```
dn:cn=policy1,o=policies

changetype:delete
```

注: 優先度同期ポリシーの作成と管理の詳細については、373 ページの 「LinuxでのLDAPツールの使用」および165 ページの 「NetIQインポート/エクスポート変換ユーティリティ」を参照してください。

優先度同期が失敗する場合

優先度同期は、次のような状況下で失敗する可能性があります。

- ネットワーク障害: ネットワークに障害が発生し、変更内容をリモートサーバに送信できない場合、優先度同期では変更内容が保存されません。

- 優先度同期キュー最大サイズに到達: エントリ数が優先度同期キューサイズを超える場合、優先度同期では、優先度同期キュー内の変更が無視されます。
- スキーマ同期の失敗: スキーマが同期されない場合、優先度同期プロセスが失敗します。
- オブジェクトが他のサーバ上に存在しない:オブジェクトの作成そのものが同期されない場合、優先度同期は失敗します。
- レプリカリング内のサーバの混在: eDirectory 8.8とeDirectory 8.8より前の両方のサーバがある場合、優先度同期が失敗します。

これらの理由のいずれかのために優先度同期が失敗した場合には、重要なデータへの変更は通常同期によって同期されます。

ポリシーベースのレプリケーション

eDirectoryのレプリケーションは、デフォルトでメッシュトポロジに従います。つまり、レプリカリング内のすべてのレプリカが、相互にアウトバウンドおよびインバウンドになることができます。メッシュモデルはすべての環境に適しているとは限りません。*ポリシーベースのレプリケーション*を使用すると、管理者はレプリケーショントポロジを設定し、レプリケーショントラフィックを最適化することができます。

レプリケーショントポロジを設定するには、ポリシーファイルを作成し、1つのファイルですべてのパーティションに対するポリシーを指定して、必要なサーバにそれをコピーします。

Linuxの場合

XML形式のポリシーファイルを作成し、それにselectivesync.xmlという名前を付けて、nds.confファイルと一緒に配置します。

ポリシーのXML定義のサンプルを次に示します。

```
<?xml version="1.0" encoding="utf-8" ?>

<SelectiveSync   xmlns="http://www.novell.com/nds"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.novell.com/nds     file:/opt/novell/eDirectory/
lib64/nds-schema/xsd/selectivesync.xsd" config-version="0.1">

    <Partition DN=".novell.TREE.">

         <SourceServer DN=".server1.novell.TREE.">

                <SyncronizeTo>.server2.novell.TREE.</SyncronizeTo>

         </SourceServer>

         <SourceServer DN=".server2.novell.TREE.">

                <SyncronizeTo>.server3.novell.TREE.</SyncronizeTo>

         </SourceServer>

         <SourceServer DN=".server3.novell.TREE.">

                <SyncronizeTo>.server1.novell.TREE.</SyncronizeTo>

         </SourceServer>

    </Partition>

</SelectiveSync>
```

Windowsの場合

XML形式のポリシーファイルを作成し、それにselectivesync.xmlという名前を付けて、インストール場所(たとえばC:\Novell\NDS)に配置します。

ポリシーのXML定義のサンプルを次に示します。

```
<?xml version="1.0" encoding="utf-8" ?>

<SelectiveSync   xmlns="http://www.novell.com/nds"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.novell.com/nds
C:\Novell\NDS\selectivesync.xsd" config-version="0.1">

    <Partition DN=".novell.TREE.">

         <SourceServer DN=".server1.novell.TREE.">

                <SyncronizeTo>.server2.novell.TREE.</SyncronizeTo>

         </SourceServer>

         <SourceServer DN=".server2.novell.TREE.">

                <SyncronizeTo>.server3.novell.TREE.</SyncronizeTo>

         </SourceServer>

         <SourceServer DN=".server3.novell.TREE.">

                <SyncronizeTo>.server1.novell.TREE.</SyncronizeTo>

         </SourceServer>

    </Partition>

</SelectiveSync>
```

Windowsでは、xsdパスを指定するときにファイルがないことに注意してください。

同期スレッドの手動設定

作成されるスレッドの最大数を設定することで、より多くのサーバに同時に複製されるよう、作成されるスレッド数を手動で増やすことができます。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。

作成されるスレッドの最大数を設定するには、次の手順を実行します。

1. iMonitorにログインします。
2. ［**エージェント環境設定**］>［**エージェント同期**］に移動します。
3. オプションで、［**同期メソッド**］セクションの［**サーバごと**］を選択します。
4. ［**システム計測同期スレッド**］セクションで［**無効**］を選択します。
5. ［**最大手動設定同期スレッド**］セクションで、所要のスレッド数を設定します。

システム計測同期

システム計測同期では、次の2つの式によってSkulkerスレッドの数が計算されます。

- **パーティションモードの場合**: Skulkerスレッドの数=そのサーバ上のパーティションの数
- **サーバモードの場合**: Skulkerスレッドの数=(サーバに認識されているサーバの数+1)/2

ただし［**最大システム計測同期スレッド**］が無効になっている場合は、上記の2つの式は使用されません。代わりに［**最大手動設定同期スレッド**］が使用されます。

たとえば、5つのサーバと3つのパーティションを使って環境がセットアップされているとします。ここで［**最大システム計測同期スレッド**］を有効にした場合、パーティションモードでは、最大で3つのSkulkerスレッドがサーバによって作成される可能性があり、サーバモードでも、最大で3つのSkulkerスレッドが作成される可能性があります。しかし、最大数の3つのSkulkerスレッドが存在しても、1つのサーバがすべてのパーティション上の他の4つのサーバに並列的に更新を送ることはできません。この場合は、［**最大システム計測同期スレッド**］を無効にして、［**最大手動設定同期スレッド**］でSkulkerスレッドの数を増やします。

Skulkerスレッドの最大数

［**最大手動設定同期スレッド**］を12に設定すれば、1つのサーバはすべてのパーティションのすべてのサーバに更新を並行して送ることができます。ただし、このセットアップでは、サーバモードで12個を超えるSkulkerスレッド、パーティションモードで3個を超えるSkulkerスレッドを作成できません。たとえ［**最大手動設定同期スレッド**］を12より高い値に設定したとしてもです。

非同期アウトバウンド同期の設定

旧リリースのeDirectoryでは、1つのサーバから別のサーバへのアウトバウンド同期が単一のスレッドで順次的に実行されたため、変更の複製に長時間かかりました。

eDirectoryに備わっている1つのスレッドは、変更キャッシュを分析し、他のサーバに送るパケットを準備した後、パケットのキューを満たします。別のスレッドがパケットを取得し、それらを他のサーバに1つずつ送ります。これにより同期が最適化され、時間が短縮されます。

1つのサーバから別のサーバへのアウトバウンド同期を設定するには、次の手順を実行します。

1. iMonitorにログインします。
2. ［**エージェント環境設定**］>［**バックグラウンドプロセスの設定**］の順に選択します。
3. ［**非同期アウトバウンド同期設定**］セクションで、［**有効**］を選択します。

注: 非同期アウトバウンド同期を有効にすると、受信側サーバでCPUとI/Oの使用率が増加する可能性があります。これを回避するには、［**非同期ディスパッチャスレッド遅延**］で遅延時間を指定することにより、パケットを送信するときの遅延を設定できます。この遅延時間として0～999ミリ秒の値を設定できます。デフォルト値は0ミリ秒です。

バックグラウンドプロセスの設定

次の設定を使用して、Skulker、パージャ、および破損通知のバックグラウンドプロセスの速度を制御できます。

- CPUは、同じプロセス(Skulker、パージャ、または破損通知)の実行と実行の間の遅延時間とコンピュータリソースの最大使用率を指定します。
- 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を設定する方法については、255 ページの 「バックグラウンドプロセスの設定」を参照してください。

ハード制限ポリシー

ハード制限ポリシーはデフォルトで有効です。バックグラウンドプロセスは、特定数のオブジェクトを処理した後、100ミリ秒(デフォルト値)にわたってスリープ状態になります。遅延(スリープ)時間を短くして、システムのパフォーマンスを向上させることができます。遅延が0ミリ秒に近く、これらのプロセスの1つ以上がバックグラウンドで実行されている場合には、CPU使用率を増やすことができます。これを監視し、必要に応じて調整する必要があります。

CPUベースの動的ポリシー

CPUベースのポリシーにより、システムで次の3つのバックグラウンドプロセスの遅延を動的に調整して、CPU最大使用率を制限できます。

- 変更キャッシュ処理遅延(アウトバウンド同期の一部)
- ObitProc遅延(破損通知処理)
- パージャ遅延(変更キャッシュのプルーニング)

CPU使用率が設定されたレベルに自動的に制限されます。クライアントの負荷が高い場合はバックグラウンドプロセスが遅くなり、クライアントの負荷が減少するとバックグラウンドプロセスの速度が上がります。バックグラウンドプロセスを遅くすべきでない場合は、このポリシーでスリープ時間を短くすることにより、最大遅延限度を設定できます。ただし、スリープ時間を小さく設定すると、CPU制限の違反が発生する可能性があります。

バックグラウンドプロセスの間隔

次のバックグラウンドプロセスの間隔値を設定できます。

- バックリンク/DRL間隔
- クリーン間隔
- アウトバウンド同期間隔
- スキーマ同期間隔
- ジャニタ間隔
- パージャ間隔

バックグラウンドプロセスの間隔を設定するには、次の操作を行います。

1 iMonitorにログインします。

2 ［**エージェント環境設定**］>［**バックグラウンドプロセスの設定**］の順に選択します。

3 ［**バックグラウンドプロセス間隔**］セクションで、間隔の値を指定します。

5 スキーマの管理

NetIQ eDirectoryツリーのスキーマは、このツリーに含めることができるオブジェクト(ユーザ、グループ、プリンタなど)のクラスを定義します。スキーマによって、各オブジェクトタイプを構成する属性(プロパティ)が指定されます。属性には、オブジェクトの作成に不可欠な必須属性と、必要に応じて指定できるオプション属性があります。

eDirectoryオブジェクトはそれぞれオブジェクトクラスに属し、オブジェクトクラスはオブジェクトに関連付けることのできる属性を指定します。すべての属性は一連の属性タイプに基づくもので、属性タイプもまた、一連の標準的な属性構文に基づいています。

eDirectoryスキーマは、各オブジェクトの構造を制御するだけではなく、eDirectoryツリー内でのオブジェクト間の関係も制御します。スキーマルールを設定すると、オブジェクトは他のサブオーディネートオブジェクトを含むことができます。このように、スキーマによってeDirectoryツリーの構造が決まります。

組織が必要とする情報の変化に応じて、スキーマに変更を加える必要が出てくることがあります。たとえば、ユーザオブジェクトに、以前はFAX番号が不要であっても、現在は必要であるとします。この場合、FAX番号を必須属性とした新しいユーザクラスを作成し、ユーザオブジェクトの作成に、この新しいユーザクラスを使用できます。

ツリーに対してスーパバイザ権を持つユーザは、NetIQ iManagerのスキーマ管理の役割により、ツリーのスキーマをカスタマイズして次のようなタスクを実行することができます。

- スキーマ内のすべてのクラスおよび属性の一覧を表示する。
- 既存のスキーマにクラスまたは属性を追加して、スキーマを拡張する。
- クラスを作成する。名前を付けてから、属性、フラグ、追加先コンテナ、および属性の継承元のペアレントクラスを指定することにより行います。
- 名前を付けてから、構文およびフラグを設定して、属性を作成する。
- 既存クラスへ属性を追加する。
- 使用されていない、あるいは古くなったクラスまたは属性を削除する。
- 潜在的な問題を発見および解決する。

この章では次のトピックについての情報を説明します。

- 140 ページの 「スキーマの拡張」
- 144 ページの 「スキーマの表示」
- 145 ページの 「手動でスキーマを拡張する」
- 147 ページの 「eDirectory 8.7以降に追加されたスキーマフラグ」
- 148 ページの 「クライアントを使用してスキーマ操作を実行する」

スキーマ情報の詳細については、『*NetIQ eDirectory Schema Reference (NetIQ eDirectoryスキーマリファレンス)* (http://developer.novell.com/documentation/ndslib/schm_enu/data/h4q1mn1i.html)』を参照してください。

スキーマの拡張

新しいクラスまたは属性を作成することにより、ツリーのスキーマを拡張できます。eDirectoryツリーのスキーマを拡張するには、ツリー全体に対するスーパバイザ権が必要です。

次の作業により、スキーマを拡張できます。

- クラスを作成する
- クラスを削除する
- 属性を作成する
- クラスへオプション属性を追加する
- 属性を削除する

次の作業により、補助属性のスキーマを拡張できます。

- 補助クラスを作成する
- 補助クラスのプロパティでオブジェクトを拡張する
- オブジェクトの補助プロパティを変更する
- オブジェクトから補助プロパティを削除する

クラスを作成する

組織の必要条件の変化に応じて、既存のスキーマに対しクラスを追加できます。

1 NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。

2 ［**スキーマ**］>［**クラスの作成**］の順にクリックします。

3 クラスの作成ウィザードの指示に従って、オブジェクトクラスを定義します。

ウィザードの各段階で、［ヘルプ］が利用できます。

オブジェクトクラスに追加するカスタムプロパティを定義する場合は、ウィザードを終了し、最初にカスタムプロパティを定義します。詳細については、属性を作成するを参照してください。

クラスを削除する

使用されていないクラスは、そのクラスがeDirectoryツリーのベーススキーマの一部でない限り、削除できます。iManagerでは、ローカルにレプリカ作成されたパーティションで現在使用されているクラスだけは削除できません。

次のような場合に、スキーマからクラスを削除できます。

- 2つのツリーをマージし、クラスの違いを解決した場合
- 特定のクラスが不要になった場合

クラスを削除するには、次を実行します。

1 NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。

2 ［**スキーマ**］>［**クラスの削除**］の順にクリックします。

3 削除するクラスを選択します。

削除可能なクラスのみが表示されます。

4 削除をクリックします。

属性を作成する

属性のカスタムタイプを独自に定義し、それをオプション属性として既存のオブジェクトクラスに追加できます。ただし、既存のクラスに必須属性を追加することはできません。

注: eDirectoryでは、レプリケーションの問題のため、ストリーム属性タイプ以外の属性に60KBまたは30,000文字を超える値を含めることができません。ユーザやアプリケーションが、その制限を超える文字列またはバイナリ属性の値を設定すると、eDirectoryは値が長すぎることを示す-649エラーを返します。

新しい属性を作成するには、次の操作を行います。

1 NetIQ iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［スキーマ］>［属性の作成］の順にクリックします。

3 属性の作成ウィザードの指示に従って、新しい属性を定義します。

ウィザードの各段階で、［ヘルプ］が利用できます。

クラスへオプション属性を追加する

既存のクラスにオプションの属性を追加できます。これは、次のような場合に必要になります。

- 組織の必要とする情報が変化した場合
- ツリーのマージを準備している場合

注: 必須属性は、クラスの作成時にのみ定義できます。

オプション属性クラスを追加するには、次を実行します。

1 NetIQ iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［スキーマ］>［属性の追加］の順にクリックします。

3 属性を追加するクラスを選択して、［OK］をクリックします。

4 ［使用可能なオプション属性］リストで、追加する属性を選択して、 をクリックし、［追加するオプション属性］リストにこれらの属性を追加します。

誤って属性を追加した場合、または追加した属性を削除する場合は、［これらのオプション属性を追加］リストで属性を選択して、 をクリックし、追加する属性のリストから削除します。

5 ［OK］をクリックします。

このクラスにオブジェクトを作成すると、ここで追加したプロパティを含むオブジェクトが作成されます。追加したプロパティの値を設定するには、オブジェクトの［その他］一般プロパティページを使用します。

ヒント: 既存のクラスを変更するには、このページを使用して［Current Attributes］リストに追加します。削除できる属性は、［OK］をクリックする前に追加した属性のみです。前に追加した属性や保存した属性は削除できません。

属性を削除する

使用されていない属性は、その属性がeDirectoryツリーのベーススキーマの一部でない限り、削除できます。

次のような場合に、スキーマから属性を削除できます。

- 2つのツリーをマージし、属性の違いを解決した場合
- 特定の属性が不要になった場合

属性を削除するには、次を実行します。

1. NetIQ iManagerで、［役割およびタスク］ボタン  をクリックします。
2. ［スキーマ］>［属性の削除］の順にクリックします。
3. 削除する属性を選択します。

   削除可能な属性のみが表示されます。
4. 削除をクリックします。

補助クラスを作成する

補助クラスとは、あるオブジェクトクラス全体ではなく、特定のeDirectoryオブジェクトインスタンスに追加される一連のプロパティ(属性)です。たとえば、電子メールアプリケーションの場合、電子メールプロパティという補助クラスを含むようにeDirectoryツリーのスキーマを拡張し、必要に応じてこれらのプロパティを使用して個々のオブジェクトを拡張できます。

スキーママネージャを使用すると、独自の補助クラスを定義できます。補助クラスで定義したプロパティを使用して、個別のオブジェクトを拡張できます。

補助クラスを作成するには、次を実行します。

1. NetIQ iManagerで、［役割およびタスク］ボタン  をクリックします。
2. ［スキーマ］>［クラスの作成］の順にクリックします。
3. クラス名と(オプションの)ASN1 IDを指定し、［次へ］をクリックします。
4. クラスフラグを設定する場合は、［補助クラス］を選択して［次へ］をクリックします。
5. クラスの作成ウィザードの指示に従って、新しい補助クラスを定義します。

   ウィザードの各段階で、［ヘルプ］が利用できます。

補助クラスのプロパティでオブジェクトを拡張する

1. NetIQ iManagerで、［役割およびタスク］ボタン  をクリックします。
2. ［スキーマ］>［オブジェクトの拡張］の順にクリックします。
3. 拡張するオブジェクトの名前とコンテキストを指定して、［OK］をクリックします。

4 使用する補助クラスが［現在の補助クラスの拡張］の下にすでに表示されているかどうかに応じて、適切な操作を実行します。

補助クラスがリストに表示されている	アクション
○	この手順を終了します。代わりに実行する手順については、143 ページの 「オブジェクトの補助プロパティを変更する」を参照してください。
いいえ	［追加］をクリックし、補助クラスを選択して［OK］をクリックします。

5 閉じるをクリックします。

オブジェクトの補助プロパティを変更する

1 NetIQ iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［ディレクトリ管理］>［オブジェクトの変更］の順にクリックします。

3 変更するオブジェクトの名前およびコンテキストを指定して、［OK］をクリックします。

4 ［全般］タブで、［その他］ページをクリックします。

5 表示された画面で、必要な属性値を設定します。

- 値のない属性をダブルクリックし、値のある属性のリストに追加します。
- 値のある属性を選択し、［編集］をクリックして属性を編集するか、［削除］をクリックして属性を削除します。
- 正しく設定するためには、各プロパティの構文について理解している必要があります。詳細については、『*NetIQ eDirectory Schema Reference (NetIQ eDirectoryスキーマリファレンス)* (http://developer.novell.com/documentation/ndslib/schm_enu/data/h4q1mn1i.html)』を参照してください。

6 ［適用］をクリックし、［OK］をクリックします。

オブジェクトから補助プロパティを削除する

1 NetIQ iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［スキーマ］>［オブジェクトの拡張］の順にクリックします。

3 拡張するオブジェクトの名前およびコンテキストを指定して、［OK］をクリックします。

4 ［現在の補助クラスの拡張］のリストから、削除するプロパティが定義されている補助クラスを選択します。

5 ［削除］をクリックし、［OK］をクリックします。

これにより、オブジェクトに最初から定義されていたプロパティを除き、補助クラスによって追加されたすべてのプロパティが削除されます。

6 閉じるをクリックします。

スキーマの表示

スキーマが組織の情報のニーズに合ったものかどうかを評価するために、スキーマを表示したり印刷することができます。組織が大きく、また複雑になると、スキーマをカスタマイズする必要も大きくなります。しかし、小規模な組織でも、特別な記録を必要とする場合があるかもしれません。このような場合、スキーマの表示や印刷は、ベーススキーマにどのような拡張が必要かを決めるのに役立ちます。

クラス情報を参照する

iManagerのClass Informationページには、選択されたクラスに関する情報が表示され、そこで属性を追加できます。このページに表示されているほとんどの情報は、クラスが作成されたときに指定されたものです。オプション属性の中には、後で追加されたものもあります。

クラスの作成中に、そのクラスを他のクラスの属性を継承するように指定した場合は、継承された属性はペアレントクラスの中に分類されます。たとえば、オブジェクトクラスがペアレントクラスで必須属性である場合、このページには、選択されたクラスの必須属性として表示されます。

1. NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**スキーマ**］>［**クラスの情報**］の順にクリックします。
3. 情報を表示するクラスを選択し、［**表示**］をクリックします。
   詳細情報を表示するには、? をクリックします。

属性情報を表示する

1. NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**スキーマ**］>［**属性の情報**］の順にクリックします。
3. 情報を表示する属性を選択し、［**表示**］をクリックします。
   詳細情報を表示するには、? をクリックします。

手動でスキーマを拡張する

.sch拡張子の付いたファイルを使用して、手動でeDirectoryスキーマを拡張できます。

このセクションでは、次のことを説明します。

- 145 ページの 「Windowsでスキーマを拡張する」
- 145 ページの 「Linuxでスキーマを拡張する」

Windowsでスキーマを拡張する

Windowsサーバのスキーマを拡張するには、NDSCons.exeを使用します。eDirectoryに付属しているスキーマファイル(*.sch)は、デフォルトでC:\Novell\NDSディレクトリにインストールされています。

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 **install.dlm**をクリックし、［**開始**］をクリックします。
3 ［**追加のスキーマファイルのインストール**］をクリックし、［**次へ**］をクリックします。
4 管理権を持つユーザとしてログインし、［**OK**］をクリックします。
5 スキーマファイルのパスと名前を指定します。
6 **完了**をクリックします。

Linuxでスキーマを拡張する

次のセクションでは、Linuxコンピュータでのスキーマ拡張について説明します。

- 145 ページの 「ndsschユーティリティを使用して、Linuxでスキーマを拡張する」
- 146 ページの 「RFC 2307スキーマを拡張する」

ndsschユーティリティを使用して、Linuxでスキーマを拡張する

NetIQ iManagerのほかにも、eDirectoryスキーマ拡張ユーティリティndsschを使用して、Linuxコンピュータ上のスキーマを拡張することができます。ツリーのスキーマの変更には、スキーマファイル(.sch)に指定された属性とクラスが使用されます。.schファイルで指定した内容に従って、属性とクラスの関連付けが作成されます。

使用する構文は次のとおりです。

```
ndssch [-h hostname[:port]] [-t tree_name] [-F <logfile>] admin-FDN schemafile...
```

```
ndssch [-h hostname[:port]] [-t tree_name] [-d] admin_FDN schemafile
[schema_description]...
```

ndsschのパラメータ	説明
-h *hostname*	スキーマを拡張するサーバの名前またはIPアドレス。指定したサーバが属しているツリーのスキーマが拡張されます。スキーマを拡張するホスト上にツリーがある場合、このパラメータの指定はオプションです。それ以外の場合、このパラメータの指定は必須です。
port	サーバポート。
-t *tree_name*	スキーマを拡張するツリーの名前。このパラメータの指定は任意です。/etc/opt/novell/eDirectory/conf/nds.confファイルに指定された値が、デフォルトのツリー名になります。詳細については、『「NetIQ eDirectoryインストールガイド」』の「*環境設定パラメータ*」を参照してください。
-F *logfile*	ndsschログファイルのパス名を指定します。
admin-FDN	ツリーに対するeDirectory管理権を持つユーザのフルコンテキスト付きの名前。
schemafile	拡張するスキーマについての情報が入力されたファイルの名前。
-d, *schema_description*	このオプションが使用されている場合、各スキーマファイルにはスキーマファイルの説明が付属しています。

RFC 2307スキーマを拡張する

RFC 2307に定義されている属性とオブジェクトクラスは、ユーザまたはグループ関連、およびNIS関連のものです。 (http://www.ietf.org/rfc/rfc2307.txt)ユーザまたはグループ関連の定義は、/opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-usergroup.schファイルにコンパイルされます。NIS関連の定義は、/opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-nis.schファイルにコンパイルされます。それぞれに対応するLDIF形式のファイルもあります(ユーザ/グループ関連は/opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-usergroup.ldif、NIS関連は/opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-nis.ldif)。

RFC 2307スキーマを拡張するには、ndsschユーティリティまたはldapmodifyツールを使用します。

- 146 ページの 「ndsschユーティリティを使用する」
- 147 ページの 「ldapmodifyユーティリティを使用する」

ndsschユーティリティを使用する

次のいずれかのコマンドを入力します。

ndssch -t tree_name admin-FDN /opt/novell/eDirectory/lib/nds-schema/rfc2307-usergroup.sch

または

ndssch -t tree_name admin-FDN /opt/novell/eDirectory/lib/nds-schema/rfc2307-nis.sch

パラメータ	説明
-t	スキーマを拡張するツリーの名前。このパラメータの指定は任意です。このパラメータが指定されていない場合、/etc/opt/novell/eDirectory/conf/nds.confファイルに指定されたツリー名が使用されます。

ldapmodifyユーティリティを使用する

次のいずれかのコマンドを入力します。

ldapmodify -h -D -w -f /opt/novell/eDirectory/lib/nds-schema/rfc2307-usergroup.ldif

または

ldapmodify -h -D -w -f /opt/novell/eDirectory/lib/nds-schema/rfc2307-nis.ldif

パラメータ	説明
-h *ldaphost*	LDAPサーバの実行場所となっている代替ホストを指定します。
-D *binddn*	*binddn*を使用してX.500ディレクトリにバインドします。RFC 1779に定義されている文字列表現のDNを指定します。
-w *passwd*	簡易認証のパスワードとして、*passwd*を使用します。
-f *file*	エントリ変更情報を標準入力ではなくファイルから読み込みます。

eDirectory 8.7以降に追加されたスキーマフラグ

READ_FILTEREDおよびBOTH_MANAGEDスキーマフラグが、eDirectory 8.7以降に追加されました。

READ_FILTEREDは、属性がLDAPオペレーショナル属性であることを示すために使用されます。LDAPがこのフラグを使用するのは、スキーマを読み込んで属性が「オペレーショナル」であることを知らせる必要がある場合です。内部定義のスキーマ属性には、このフラグが設定されたものもあります。LDAP「オペレーショナル」定義には、3つのスキーマフラグがあります。新しいREAD_FILTEREDフラグとは別に、既存のフラグとして「オペレーショナル」を示すものにはREAD_ONLYフラグとHIDDENフラグがあります。これらのフラグのいずれかがスキーマ定義に存在する場合、LDAPは属性を「オペレーショナル」として扱い、特に必要がない場合はその属性を返しません。

BOTH_MANAGEDは、セキュリティ権利を強制する新しいメカニズムです。これは識別名構文の属性にのみ重要なフラグです。この属性に設定された場合、要求している接続には、ターゲットオブジェクトと属性、およびターゲット属性によって参照されているオブジェクトの両方に対する権利が必要になります。これは、現在のWRITE_MANAGEDフラグの機能を拡張したものです。このフラグは、現在ベーススキーマ属性には設定されていません。この新しいセキュリティ動作はeDirectory 8.7.*x*以降のサーバ上でのみ実行されるため、このフラグに関連する動作に矛盾がないようにするには、ツリー全体をeDirectory 8.7以降にアップグレードする必要があります。

eDirectory 8.7.*x*以降のサーバのみがこれらの新しいフラグを認識するため、ルートパーティションのコピーを格納するeDirectory 8.7.*x*以降のサーバによってのみ、これらのフラグをスキーマ定義に設定できます。これは、ルートを持つサーバのみがスキーマを変更できるためです。通常インストールの新規サーバや、ルートパーティションを保持していない既存サーバをアップグレードしたサーバでは、これらの新しいフラグをツリー内のスキーマに追加することはできません。

これらの新しい機能のいずれかをツリーで有効にする場合は、スキーマが正常に拡張されていて、これらの新しいフラグを追加できることを確認する必要があります。確認する方法には次の2つがあります。1つは、ルートパーティションの書き込み可能なコピーを持つサーバを選択して、eDirectory 8.7以降にアップグレードすることです。これにより、自動的にスキーマが正しく拡張され、新しいフラグに対応します。

2つ目の方法はさらに込み入ったものです。次の手順に従って操作します。

1 新しく8.7.*x*以降のサーバをインストールするか、ツリー内の既存のサーバをアップグレードします。このサーバが[Root]のコピーを保持している必要はありません。

2 ルートパーティションのコピーをこの新しいサーバに手動で追加します。

3 次に示す適切なスキーマ拡張ファイルをこのサーバ上で再実行し、スキーマを拡張します。

Platform	指示
Windows	install.dlmをロードし、［**追加のスキーマファイルのインストール**］をクリックします。
Linux	ndsschユーティリティを使用します。詳細については、145 ページの 「ndsschユーティリティを使用して、Linuxでスキーマを拡張する」を参照してください。

4 これらの新しいフラグが設定された新しいスキーマファイルをインストールします。

5 (オプション)スキーマの同期後は、このサーバからルートレプリカを削除できます。

注: これらの新しいスキーマフラグにより、オプションの機能が有効になります。新しい機能を必要としない場合は、スキーマ定義にこれらの新しいフラグが存在しなくても、ツリー内でのeDirectoryの通常操作に問題が起こることはありません。READ_FILTEREDフラグの場合は、属性の定義によっては表示されないことがあります。このため、オブジェクトのすべての属性に対するLDAP読み込み要求によって、フラグが存在すれば受け取らないはずのデータが余分に取得される場合があります。READ_FILTEREDフラグを含む属性の中には、READ_ONLYフラグまたはHIDDENフラグが存在するために、やはりオペレーショナルとして扱われるものもあります。BOTH_MANAGEDフラグは、すべてのサーバがアップグレードされたツリーでのみ有効になります。その環境の中でのみ、この機能を矛盾なく操作することが可能なためです。

クライアントを使用してスキーマ操作を実行する

eMBox (eDirectory Management Toolbox)クライアントはコマンドラインJavaクライアントで、これを使用するとDSSchema操作にリモートでアクセスできます。DSSchema eMToolを使用すると、スキーマの同期、リモートスキーマのインポート、新規スキーマエポックの宣言、ローカルスキーマのリセット、グローバルスキーマの更新などを実行できます(通常、DSRepairを使用して実行する操作です。詳細については、347 ページの 「スキーマの保守」を参照してください)。

emboxclient.jarファイルは、eDirectoryの一部としてサーバにインストールされます。JVMをインストールしていれば、どのコンピュータでも実行できます。クライアントの詳細については、584 ページの 「コマンドラインクライアントの使用」を参照してください。

DSSchema eMToolを使用する

1 コマンドラインで次のように入力して、対話式モードでクライアントを実行します。

```
java -cp path_to_the_file/emboxclient.jar  -i
```

(クラスパスにemboxclient.jarファイルがすでに含まれている場合は、単に「java -i」と入力します。)

クライアントのプロンプトが次のように表示されます。

```
Client>
```

2 修復するサーバにログインするには、次のように入力します。

```
login -sserver_name_or_IP_address -pport_number
-uusername.context -wpassword -n
```

ポート番号は通常80または8028です。ただし、すでにそのポートを使用しているWebサーバが存在する場合は異なります。-nオプションを使用すると、非セキュア接続が開始されます。

クライアントにログインが成功したかどうかが表示されます。

3 次の構文を使用して修復コマンドを入力します。

dsschema.*task options*

次に例を示します。

「dsschema.rst」と入力すると、このサーバのスキーマを同期するようにツリーのルートのマスタレプリカに要求することができます。

「dsschema.irs-n*MyTree*」と入力すると、MyTreeというツリーからリモートスキーマをインポートすることができます。

各スイッチの間にはスペースが必要です。スイッチの順序は重要ではありません。

クライアントは修復が成功したかどうかを表示します。

DSSchemæMToolオプションの詳細については、149ページの 「DSSchemæMToolオプション」を参照してください。

4 クライアントからログアウトするには、次のコマンドを入力します。

```
logout
```

5 クライアントを終了するには、次のコマンドを入力します。

```
exit
```

DSSchema eMToolオプション

次の表に、DSSchema eMToolオプションを示します。クライアントでlist -t dsschemaコマンドを使用して、DSSchemaオプションの詳細を表示することもできます。詳細については、588 ページの「eMToolとそのサービスを表示する」を参照してください。

オプション	説明
rst	ツリーのルートのマスタレプリカのスキーマをこのサーバに同期します。
irs -n*tree_name*	別のツリーからリモートスキーマをインポートします。
dse	ルートのマスタレプリカを持つサーバ上で新規スキーマエポックを宣言します。
rls	ローカルスキーマを、ルートパーティションのマスタレプリカがあるサーバからのコピーでリセットします。
gsu	グローバルスキーマ更新を実行します。
scc	ドメインクラスのスキーマサーキュラ包含ルールを追加します。

6 パーティションおよびレプリカの管理

パーティションは、eDirectoryツリー内の個別のデータユニットを構成するNetIQ eDirectoryデータベースの論理区分です。システム管理者は、パーティションを利用してeDirectory情報を格納したり、複製したりします。各パーティションは、コンテナオブジェクト、コンテナオブジェクトに含まれるすべてのオブジェクト、およびこれらのオブジェクトについての情報で構成されます。パーティションには、ファイルシステムに関する情報、またはパーティションに含まれるディレクトリやファイルに関する情報はありません。

各サーバに eDirectoryデータベース全体のコピーを保存する代わりに、eDirectoryパーティションのコピーを作成してそれをネットワーク内の複数のサーバ上で保存できます。パーティションのコピーは、レプリカと呼ばれています。各eDirectoryパーティションのレプリカは任意の数だけ作成することができ、任意のサーバに保存できます。レプリカのタイプには、マスタ、読み書き可能、読み込み専用、サブオーディネートリファレンス、フィルタ済み読み書き可能、およびフィルタ済み読み込み専用があります。

次の表で、レプリカタイプについて説明します。

レプリカ	説明
マスタ、読み書き可能、および読み込み専用	特定のパーティションのすべてのオブジェクトおよび属性が含まれます。
サブオーディネートリファレンス	ツリーの接続のために使用されます。
フィルタ済みレプリカ	パーティション全体から取得した情報のサブセットが含まれます。このサブセットは、サーバのレプリケーションフィルタによって定義された必要なクラスおよび属性のみで構成されます。レプリケーションフィルタは、インバウンド同期やローカルでの変更時にレプリカに含めることのできるクラスおよび属性を識別するために使用されます。 フィルタ済みレプリカによって、管理者はまばらで断片的なレプリカを作成できます。 ◆ 指定したオブジェクトクラスだけが含まれるスパースレプリカ ◆ 指定した属性だけが含まれる断片レプリカ フィルタ済みレプリカの機能によって、アプリケーションがeDirectoryに格納されているデータを取得するときのレスポンスが迅速になります。また、フィルタ済みレプリカを使用すると、1つのサーバにより多くのレプリカを格納できます。
読み書き可能フィルタ済みレプリカ	サーバのレプリケーションフィルタのサブセットであるクラスおよび属性をローカルで変更できます。ただし、これらのレプリカを作成できるのは、レプリケーションフィルタ内にそのクラスの必須属性がすべて含まれている場合のみです。
読み込み専用フィルタ済みレプリカ	ローカルで変更できません。

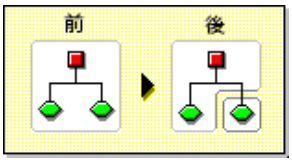
この章では、パーティションおよびレプリカの管理方法を説明します。

パーティションの作成

パーティションを作成すると、ツリーの論理区分が作成されます。これらの論理区分は、ネットワーク内にある別のeDirectoryサーバ間で複製したり配布することができます。

新しいパーティションを作成すると、ペアレントパーティションが分割されて2つのパーティションになります。新しいパーティションは、次の図で示されるように、チャイルドパーティションになります。

図 6-1 パーティションの分割前と分割後



たとえば、1つの部門を選択し、これを新しいパーティションとして作成すると、選択した部門およびそのサブオーディネートオブジェクトすべてがペアレントパーティションから分割されます。

選択した部門は、新しいパーティションのルートになります。新しいパーティションのレプリカは、ペアレントパーティションのレプリカと同じサーバに存在します。また、新しいパーティションのオブジェクトは、そのパーティションのルートオブジェクトに属します。

レプリカすべてを新しいパーティション情報と同期する必要があるため、パーティションの作成には時間がかかる場合があります。パーティションの作成中に別のパーティション操作を実行しようとすると、パーティションが使用中であることを示すメッセージが表示されます。

新しいパーティションのレプリカリストを参照し、リスト内のレプリカがすべてオンの状態であれば、操作が完了していることがわかります。状態は自動的にはリフレッシュされないので、画面を定期的に手動でリフレッシュします。

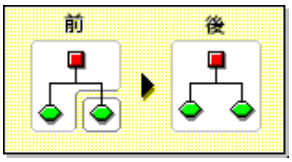
パーティションを作成するには、次の操作を行います。

1. iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**パーティションとレプリカの管理**］>［**パーティションの作成**］をクリックします。
3. 新しいパーティションを作成するコンテナの名前およびコンテキストを指定して、［**OK**］をクリックします。

パーティションのマージ

パーティションをそのペアレントパーティションにマージすると、選択したパーティションおよびそのレプリカがペアレントパーティションに結合されます。パーティションの削除は行いません。次の図のように、パーティションのマージおよび作成のみを実行し、ディレクトリツリーがどのように論理区分に分割されるかを定義します。

図6-2 パーティションのマージ前とマージ後



パーティションとそのペアレントパーティションをマージする理由として、次のようなことが考えられます。

- 2つのパーティションのディレクトリ情報が密接に関連している。
- サブオーディネートパーティションを削除する場合に、その中のオブジェクトを残したい。
- パーティションのオブジェクトを削除する。
- パーティションのすべてのレプリカを削除する。パーティションをその親にマージする操作は、パーティションのマスタレプリカを削除するための唯一の方法です。
- コンテナを移動した後で(パーティションルートに従属パーティションがない場合のみ)、このコンテナをパーティションとする必要がなくなった。
- 会社の組織に変更が生じたため、パーティション構造を変更することでディレクトリツリーを再設計する。

パーティションが大きくて、数百個のオブジェクトが含まれている場合は、ネットワークの応答時間が遅くなるため、パーティションを別々に維持するようにしてください。

ツリーのルートパーティションは最上位のパーティションであり、マージするペアレントパーティションがないため、マージできません。

サーバで処理が完了すると、パーティションがマージされます。パーティションのサイズ、ネットワークトラフィック、サーバの環境設定などによって異なりますが、この操作の完了にはかなり時間がかかる場合があります。

重要: パーティションのマージを行う前に、両パーティションの同期を点検し、続行する前にすべてのエラーを修正します。エラーを修正することにより、ディレクトリでの問題を切り離し、エラーの伝播や新しいエラーの発生を防ぐことができます。

パーティションのマージを行う前に、マージするパーティションのレプリカ(サブオーディネートリファレンスを含む)を持つサーバすべてが稼働していることを確認します。サーバが停止中の場合、eDirectoryはサーバのレプリカを読み込むことができず、操作を完了できません。

パーティションのマージの処理中にエラーが表示された場合は、そのつどエラーを解決します。操作を続けながらエラーを修正すると、さらにエラーが発生するため、必ず操作を中断してからエラーを修正してください。

チャイルドパーティションをペアレントパーティションとマージするには、次の操作を行います。

1 iManagerで、［役割およびタスク］ボタン をクリックします。

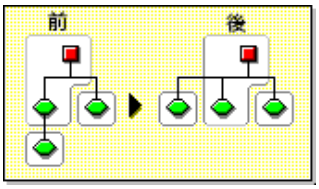
2 ［パーティションとレプリカの管理］>［パーティションのマージ］をクリックします。

3 親パーティションとマージするパーティションの名前およびコンテキストを指定して、［OK］をクリックします。

パーティションの移動

パーティションを移動することで、ディレクトリツリー内のサブツリーを移動できます。ルートパーティションオブジェクト(コンテナオブジェクト)にサブオーディネートパーティションがない場合にのみ、このオブジェクトを移動できます。

図6-3 パーティションの移動前と移動後



パーティションを移動する場合は、eDirectoryの包含ルールに従う必要があります。たとえば、部門は現在のツリーのルートの直下には移動できません。これは、ルートの包含ルールにより移動が許されているのが、地域、国、または組織であるためです。

パーティションを移動する場合、eDirectoryではパーティションのルートオブジェクトへのすべての参照が変更されます。オブジェクトの共通名は変更されませんが、コンテナ(およびそのサブオーディネートコンテナすべて)の完全識別名は変更されます。

パーティションを移動するときに、オプションを選択して、移動するコンテナの代わりに別名オブジェクトを作成することもできます。これにより、ユーザが引き続きネットワークにログインして、元のディレクトリの場所でオブジェクトを検索できます。

作成した別名オブジェクトは、移動したコンテナと同じ共通名を持ち、そのコンテナの新しい完全識別名を参照します。

重要: パーティションを移動したときに、移動したパーティションの代わりとなる別名オブジェクトを作成しないと、パーティションの新しい位置を知らないユーザは元のディレクトリ位置でオブジェクトを見つけようとし、ディレクトリツリーにあるパーティションオブジェクトを見つけることが困難になります。

また、ワークステーションのNAME CONTEXTパラメータがディレクトリツリーコンテナのオリジナルの位置に設定されている場合、これにより、クライアントワークステーションがログインできないという問題が起きるおそれがあります。

オブジェクトを移動すると、オブジェクトのコンテキストが変更されるため、移動したオブジェクトを参照するネームコンテキストを持つユーザのNAME CONTEXTパラメータは、オブジェクトの新しい名前を参照するように更新する必要があります。

コンテナオブジェクトの移動の後に、ユーザのNAME CONTEXTパラメータを自動的に更新するには、NCUPDATEユーティリティを使用します。

移動したパーティションをパーティションとして使用しない場合は、それをペアレントパーティションとマージします。

パーティションを移動する前に、ディレクトリツリーが正しく同期されていることを確認してください。移動元か移動先のいずれかのパーティションで同期エラーが発生している場合は、パーティションの移動操作を実行しないでください。最初に同期エラーを解決します。

パーティションを移動するには、次の手順を実行します。

1 iManagerで、［**役割およびタスク**］ボタン  をクリックします。

2 ［**パーティションとレプリカの管理**］>［**パーティションの移動**］をクリックします。

3 ［**オブジェクト名**］フィールドに移動するパーティションオブジェクトの名前およびコンテキストを指定します。

4 ［**移動先**］フィールドに、パーティションの移動先となるコンテナの名前とコンテキストを指定します。

5 パーティションの移動元の別名を作成する場合は、［**移動したオブジェクトの代わりに別名を作成します**］を選択します。

これにより、移動前の場所に依存するあらゆる操作は、操作を更新して移動後の場所を反映できるようになるまで、引き続き実行されます。

6 ［**OK**］をクリックします。

パーティションの作成操作またはマージ操作のキャンセル

変更を確定する段階まで操作が到達していない場合、パーティションの作成またはマージをキャンセルできます。この機能を使用して、操作を終了できます。また、eDirectoryネットワークが、eDirectoryエラーを返したり、パーティション操作に続く同期に失敗した場合にもこの機能を使用します。

ディレクトリツリーのレプリカで同期エラーが生じていると、操作を中止しても問題が解決しない場合があります。ただし、初期のトラブルシューティングオプションとして、この機能を使用できます。

サーバが停止している、またはその他の理由でサーバが使用できない場合、パーティション操作を完了できるようにサーバがネットワークから見えるようにするか、操作を中止します。データベースが壊れているためにeDirectoryによる同期ができない場合、実行中のパーティション操作すべてを中止する必要があります。

含まれるレプリカの数、サーバの可視性、および既存のワイヤトラフィックの量によりますが、パーティション操作でネットワーク間の完全な同期を行うには、かなりの時間がかかります。

パーティションが使用中であることを示すエラーが表示されても、操作を中止する必要はありません。パーティションのサイズ、接続性の問題などによって異なりますが、通常、パーティション操作は24時間以内に完了します。この時間内で操作が完了しない場合には、実行中の操作を中止します。

レプリカの管理

レプリカの追加、削除、またはレプリカタイプの変更をする前に、ターゲットレプリカの位置を慎重に計画します。詳細については、90 ページの 「ツリーのレプリカ作成に関するガイドライン」を参照してください。

レプリカを追加する

次の機能をディレクトリに提供するために、レプリカをサーバに追加します。

- 障害対策
- データへのより高速なアクセス
- WANリンク上でのより高速なアクセス
- 設定コンテキスト中のオブジェクトへのアクセス(バインダリサービスを使用)

レプリカを追加するには、次の操作を行います。

1 iManagerで、［**役割およびタスク**］ボタン  をクリックします。

2 ［**パーティションとレプリカの管理**］>［**レプリカビュー**］をクリックします。

3 複製したいパーティションまたはサーバの名前とコンテキストを指定して、［**OK**］をクリックします。

4 ［**レプリカの追加**］をクリックします。

5 パーティションまたはサーバの名前およびコンテキストを指定します。

6 次のレプリカタイプのいずれかを選択します。

レプリカタイプ	説明
 読み書き可能	ユーザは、新しいレプリカの内容の読み込みと変更を両方行うことができます。このパーティションのeDirectoryオブジェクトを管理するユーザの近くに変更可能なレプリカがない場合は、このオプションを選択します。
 読み込み専用	ユーザは、新しいレプリカの内容を読み込むことはできますが、変更はできません。このパーティションのeDirectoryオブジェクトを読み込むだけで、変更は行わないユーザの近くにレプリカがない場合は、このオプションを選択します。
 フィルタ済み読み書き可能	ユーザは、新しいレプリカの内容の読み込みと変更を両方行うことができますが、このレプリカの内容は、eDirectoryオブジェクトおよびフィルタで指定されたプロパティのタイプに制限されます。
 フィルタ済み読み込み専用	ユーザは、新しいレプリカの内容を読み込めても変更はできず、このレプリカの内容は、eDirectoryオブジェクトおよびフィルタで指定されたプロパティのタイプに制限されます。

7 ［**OK**］をクリックします。

詳細については、62 ページの 「レプリカのタイプ」を参照してください。

レプリカを削除する

レプリカを削除すると、パーティションのレプリカはサーバから削除されます。

サーバをディレクトリツリーから削除する場合は、その前に、レプリカをサーバから削除します。レプリカを削除することで、サーバを削除するときに起きる問題を減らすことができます。

また、レプリカの削除により、ネットワークの同期トラフィックの量も削減できます。通常、パーティションに7個以上のレプリカは必要ありません。

マスタレプリカまたはサブオーディネートリファレンスは、削除できません。

マスタレプリカを削除するには、次の2つのオプションを利用します。

- マスタレプリカをパーティションの別のレプリカを含むサーバへ移動し、そのレプリカを新しいマスタレプリカにします。

  これにより、元のマスタレプリカは自動的に読み書き可能レプリカに変更され、削除できるようになります。
- パーティションをそのペアレントパーティションとマージします。

  これにより、パーティションのレプリカとペアレントパーティションのレプリカがマージされ、そのサーバからレプリカが削除されます。マージによりパーティションの境界は削除されますが、オブジェクトは削除されません。オブジェクトは、「結合」パーティションのレプリカを持つ各サーバに残ります。

レプリカを削除する場合、次の点に注意します。

- 障害対策として、異なるサーバ上に各パーティションのレプリカを3つ以上保持します。
- レプリカを削除すると、ターゲットサーバ上のディレクトリデータベースのコピーが削除されます。

  データベースは、ネットワークの別のサーバで引き続きアクセスできます。また、レプリカが含まれていたサーバも、eDirectoryで引き続き機能します。

  サブオーディネートリファレンスレプリカは、削除や管理ができません。これは、サーバにパーティション(パーティションの子ではない)のレプリカが含まれる場合に、eDirectoryによって自動的に作成されます。

レプリカを削除するには、次の操作を行います。

1. iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**パーティションとレプリカの管理**］>［**レプリカビュー**］をクリックします。
3. 削除するレプリカを格納するパーティションまたはサーバの名前およびコンテキストを指定して、［**OK**］をクリックします。
4. 削除するレプリカの左にある をクリックします。
5. ［**OK**］をクリックします。

レプリカタイプを変更する

レプリカタイプを変更して、レプリカ情報へのアクセスを制御します。たとえば、既存の読み書き可能レプリカを読み込み専用レプリカに変更して、ユーザがレプリカに書き込んだり、ディレクトリデータを変更できないようにします。

読み書き可能レプリカ、または読み込み専用レプリカのタイプを変更できます。マスタレプリカのタイプは変更できませんが、読み書き可能レプリカまたは読み込み専用レプリカは、マスタレプリカに変更できます。これにより、元のマスタレプリカは、自動的に読み書き可能レプリカに変更されます。

通常、ほとんどのレプリカは、読み書き可能レプリカとして使用されます。読み書き可能レプリカには、クライアント操作による書き込みができます。変更が加えられると、読み書き可能レプリカは同期情報を送信します。読み込み専用レプリカには、クライアント操作による書き込みができません。しかし、レプリカを同期すると、読み込み専用レプリカは更新されます。

サブオーディネートリファレンスのレプリカタイプは、変更できません。サブオーディネートリファレンスがあるサーバに、パーティションのレプリカを配置するには、レプリカの追加操作を行う必要があります。サブオーディネートリファレンスレプリカは、パーティションの完全なコピーではありません。サブオーディネートリファレンスレプリカの配置および管理は、eDirectoryで制御します。サーバがパーティションのレプリカを含む場合、サブオーディネートリファレンスレプリカは、eDirectoryにより自動的にサーバ上に作成されます。ただし、サーバがパーティションのチャイルドレプリカを含む場合には、作成されません。

レプリカタイプを変更するには、次の操作を行います。

1. iManagerで、［役割およびタスク］ボタン  をクリックします。
2. ［パーティションとレプリカの管理］>［レプリカビュー］をクリックします。
3. 変更するレプリカを格納するパーティションまたはサーバの名前およびコンテキストを指定して、［OK］をクリックします。
4. 変更するレプリカのレプリカタイプ(［タイプ］列内)をクリックします。
5. 新しいレプリカタイプをクリックし、［OK］をクリックします。

レプリカタイプ	説明
 マスタ	ユーザは、このレプリカの内容の読み込みと変更を行うことができ、このレプリカは、下位パーティションの作成やマージなど、このパーティションに影響を与える将来のパーティション処理の出発点となります。1つのパーティションに設定できるマスタレプリカは1つだけです。
 読み書き可能	ユーザは新しいレプリカの内容の読み込みと変更を行うことができます。このパーティションのeDirectoryオブジェクトを管理するユーザの近くに変更可能なレプリカがない場合は、このオプションを選択します。
 読み込み専用	ユーザは新しいレプリカの内容を読み込むことができますが、変更はできません。このパーティションのeDirectoryオブジェクトを読み込むだけで、変更は行わないユーザの近くにレプリカがない場合は、このオプションを選択します。
 フィルタ済み読み書き可能	ユーザは新しいレプリカの内容の読み込みと変更を行うことはできますが、内容はフィルタで指定されたeDirectoryオブジェクトとプロパティのタイプに制限されます。
 フィルタ済み読み込み専用	ユーザは新しいレプリカの内容を読み込めても変更はできませんが、内容はフィルタで指定されたeDirectoryオブジェクトとプロパティのタイプに制限されます。

6. ［OK］をクリックします。

詳細については、62 ページの 「レプリカのタイプ」を参照してください。

フィルタ済みレプリカを設定し管理する

フィルタ済みレプリカには、eDirectoryパーティションの情報のフィルタ済みサブセット(オブジェクトまたはオブジェクトクラス、およびこれらのオブジェクトの属性と値のフィルタ済みセット)が保存されます。

管理者は、フィルタ済みレプリカのセットを保持するeDirectoryサーバを作成するためにフィルタ済みレプリカ機能を使用します。フィルタ済みレプリカのセットには、同期するオブジェクトおよび属性のみが含まれます。

このため、iManagerでは、フィルタ済みレプリカのパーティションスコープおよびフィルタを作成できるツールが用意されています。スコープとは、単にパーティションのセットのことで、その範囲でサーバ上にレプリカを置きます。一方、レプリケーションフィルタには、サーバのフィルタ済レプリカのセットでホストするeDirectoryクラスおよび属性のセットが含まれています。この結果、eDirectoryサーバには、ツリー内の多くのパーティションから明確に定義されたデータセットが格納されるようになります。

サーバのパーティションスコープおよびレプリケーションフィルタの記述は、eDirectoryに格納され、iManagerのサーバオブジェクトまたは［パーティションとレプリカ］役割によって管理できます。

- 160 ページの 「フィルタ処理済レプリカウィザードを使用する」
- 160 ページの 「パーティションスコープを定義する」
- 161 ページの 「サーバフィルタを設定する」

フィルタ処理済レプリカウィザードを使用する

フィルタ処理済レプリカウィザードを使用すると、サーバのレプリケーションフィルタおよびパーティションスコープを、表示される手順に従って簡単に設定できます。

1. iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**パーティションとレプリカの管理**］>［**フィルタ処理済レプリカウィザード**］をクリックします。
3. フィルタ済みレプリカを設定するサーバを指定し、［**次へ**］をクリックします。
4. 選択されたサーバに設定されたフィルタのクラスおよび属性を定義するには、［**フィルタセットの定義**］をクリックします。

   レプリケーションフィルタには、サーバのフィルタ済みレプリカセットに保存するeDirectoryクラスと属性のセットが含まれます。フィルタセットの定義の詳細については、161 ページの 「サーバフィルタを設定する」を参照してください。
5. ［**次へ**］をクリックします。
6. このサーバのパーティションスコープを定義するには、［**パーティションスコープの定義**］をクリックします。

   パーティションスコープの詳細については、「160 ページの 「パーティションスコープを定義する」」を参照してください。
7. ［**次へ**］をクリックし、［**終了**］をクリックします。

パーティションスコープを定義する

パーティションスコープは、サーバ上でレプリカを保存するパーティションのセットです。iManagerの［レプリカビュー］ページには、eDirectoryツリーのパーティションの階層が表示されます。個別のパーティション、指定したブランチのパーティションセット、またはツリー内のすべてのパーティションを選択できます。次に、サーバに追加するこれらのパーティションのレプリカタイプを選択するか、既存のレプリカタイプを変更します。

サーバには、完全なレプリカもフィルタ済みレプリカも保存できます。詳細については、65 ページの 「フィルタ済みレプリカ」を参照してください。

eDirectoryサーバのレプリカを表示する

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。

2 ［**パーティションとレプリカの管理**］>［**レプリカビュー**］をクリックします。

3 表示するサーバの名前およびコンテキストを指定して［**OK**］をクリックし、このサーバ上のレプリカのリストを表示します。

eDirectoryサーバにフィルタ済みレプリカを追加する

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。

2 ［**パーティションとレプリカの管理**］>［**レプリカビュー**］をクリックします。

3 フィルタ済みレプリカを追加するサーバの名前およびコンテキストを指定し、［**OK**］をクリックします。

4 ［**レプリカの追加**］をクリックします。

5 パーティションの名前およびコンテキストを指定します。

6 ［**フィルタ済み読み書き可能**］または［**フィルタ済み読み込みのみ**］をクリックし、［**OK**］をクリックします。

完全なレプリカをフィルタ済みレプリカへ変更する

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。

2 ［**パーティションとレプリカの管理**］>［**レプリカビュー**］をクリックします。

3 変更するレプリカを格納するパーティションまたはサーバの名前およびコンテキストを指定して、［**OK**］をクリックします。

4 変更するレプリカのレプリカタイプ(［**タイプ**］列内)をクリックします。

5 ［**フィルタ済み読み書き可能**］または［**フィルタ済み読み込みのみ**］をクリックし、［**OK**］をクリックします。

サーバフィルタを設定する

サーバレプリケーションフィルタには、サーバのフィルタ済みレプリカセットにホストするeDirectoryのクラスと属性のセットが含まれています。どのサーバオブジェクトからでもフィルタを設定できます。フィルタ済みレプリカの場合、サーバごとにフィルタを1つだけ作成できます。つまり、あるeDirectoryサーバ用に定義されているフィルタは、そのサーバ上のすべてのフィルタ済みレプリカに適用されます。ただし、完全なレプリカにはフィルタは適用されません。

サーバのフィルタは必要に応じて変更できますが、変更するとレプリカの再同期が発生するため時間がかかる可能性があります。サーバの機能に関するプラニングは、慎重に行うようにしてください。

次の方法のいずれかで、サーバのフィルタを設定または変更できます。

- 161 ページの 「レプリカビューを使用する」
- 162 ページの 「サーバオブジェクトを使用する」

レプリカビューを使用する

1 iManagerで、［**役割およびタスク**］ボタン  をクリックします。

2 ［**パーティションとレプリカの管理**］>［**レプリカビュー**］をクリックします。

3 変更するレプリカを格納するパーティションまたはサーバの名前およびコンテキストを指定して、［**OK**］をクリックします。

4 変更するサーバまたはパーティションの［Edit in the Filter］列をクリックします。

5 適切なクラスおよび属性を追加し、［**OK**］をクリックします。

6 **完了**をクリックします。

サーバオブジェクトを使用する

1 iManagerで、［**役割およびタスク**］ボタン  をクリックします。

2 ［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。

3 変更するレプリカを格納するサーバの名前およびコンテキストを指定して、［**OK**］をクリックします。

4 ［**レプリカ**］タブをクリックします。

5 このサーバにフィルタが定義されていなかった場合、［**フィルタは空です**］をクリックして［フィルタ編集ダイアログ］ウィンドウを開き、所要のクラスおよび属性を追加します。

または

［**Copy Filter From**］をクリックし、コピーするフィルタを含むオブジェクト(別のサーバなど)をブラウズします。

6 既存のフィルタを編集するには、フィルタ内のハイパーリンク付きアイテムをクリックし、［フィルタの編集］ダイアログボックスを開いて、目的のクラスおよび属性を追加または削除します。

パーティションおよびレプリカを表示する

このセクションでは、次のことを説明します。

サーバのパーティションを表示する

NetIQ iManagerでは、サーバに割り当てられたパーティションを表示できます。サーバオブジェクトをディレクトリツリーから削除しようとする場合、サーバに格納されているパーティションの表示が必要となる場合があります。この場合、オブジェクトを削除する前に、削除するレプリカを表示できます。

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。
2 ［**パーティションとレプリカの管理**］>［**レプリカビュー**］をクリックします。
3 サーバオブジェクトの名前とコンテキストを入力して、［**OK**］をクリックします。

パーティションレプリカを表示する

この操作により、次を識別できます。

- パーティションのレプリカが存在するサーバ
- パーティションのマスタレプリカのホストとなっているサーバ
- 読み書き可能レプリカ、読み込み専用レプリカ、およびサブオーディネートリファレンスレプリカを含むサーバ
- 各パーティションレプリカの状態

パーティションレプリカを表示するには、次の操作を行います。

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。
2 ［**パーティションとレプリカの管理**］>［**レプリカビュー**］をクリックします。
3 パーティションの名前とコンテキストを入力して、［**OK**］をクリックします。

パーティションに関する情報を表示する

パーティションに関する情報(成功した最新の同期や最近試みた同期など)を表示する主な目的は、パーティションの同期情報を確認することです

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。
2 ［**パーティションとレプリカの管理**］>［**パーティションの情報を表示**］をクリックします。
3 パーティションの名前とコンテキストを入力して、［**OK**］をクリックします。

パーティションの階層を表示する

iManagerでは、パーティションの階層を容易に表示できます。コンテナオブジェクトを展開して、ペアレントパーティションやチャイルドパーティションを表示できます。

パーティションのルートである各コンテナには、  が表示されます。

レプリカに関する情報を表示する

レプリカに関する情報を表示する主な目的は、レプリカの状態を確認することですeDirectoryレプリカの状態は、それが実行しているパーティションや複製の操作によってさまざまです。次の表では、iManagerで表示されるレプリカの状態を説明しています。

状態	説明
オン	現在パーティションや複製の操作を実行していない
New (新規)	サーバに新しいレプリカとして追加中
停止中	サーバから削除中
停止	サーバからの削除が完了
マスタ開始	マスタレプリカへ変更中
マスタ完了	マスタレプリカへの変更が完了
タイプの変更	他のレプリカタイプへの変更中
ロック状態	パーティションの移動または修復の操作の準備が滞っている
移動へ移行	パーティションの移動操作を開始中
Move	パーティションの移動操作中
分割へ移行	パーティションの分割操作(チャイルドパーティションの作成)を開始中
分割	パーティションの分割(チャイルドパーティションの作成)操作中
Join	ペアレントパーティションへのマージ中
オンへ移行	オン状態へ戻る直前
不明	iManagerで認識できない状態

レプリカの情報を表示するには、次の操作を行います。

1 iManagerで、［**役割およびタスク**］ボタン  をクリックします。

2 ［**パーティションとレプリカの管理**］>［**レプリカビュー**］をクリックします。

3 パーティションまたはサーバの名前およびコンテキストを入力して、［**OK**］をクリックします。

7 NetIQ eDirectory管理ユーティリティ

この章では、次のNetIQ eDirectoryユーティリティについて説明します。

NetIQインポート/エクスポート変換ユーティリティ

NetIQインポート/エクスポート変換ユーティリティは次の操作に使用できます。

- LDIFファイルからLDAPディレクトリへのデータのインポート
- LDAPディレクトリからLDIFファイルへのデータのエクスポート
- LDAPサーバ間でのデータの移行
- スキーマの比較と更新の実行
- テンプレートを使用したeDirectoryへの情報のロード
- SCHファイルからLDAPディレクトリへのスキーマのインポート

NetIQインポート/エクスポート変換ユーティリティは、形式に応じてデータを読み書きするための一連のハンドラを管理します。データを読み込むハンドラをソースハンドラと呼び、データを書き込むハンドラをターゲットハンドラと呼びます。1つの実行可能モジュールがソースハンドラとターゲットハンドラの両方として機能することもあります。Novellインポート/エクスポート変換エンジンは、ソースハンドラからデータを受け取ってそれを処理し、処理したデータをターゲットハンドラに渡します。

たとえば、LDIFデータをLDAPディレクトリにインポートする場合、NetIQインポート/エクスポート変換エンジンは、LDIFソースハンドラを使用してLDIFファイルを読み込み、読み込んだデータをLDAPターゲットハンドラを使用してLDAPディレクトリサーバに送信します。LDIFファイルの構文、構造、およびデバッグの詳細については、933 ページの付録 J「トラブルシューティング」を参照してください。

NetIQインポート/エクスポート変換クライアントユーティリティは、コマンドラインから、またはNetIQ iManagerの［インポート変換エクスポートウィザード］から実行できます。ただし、コンマ区切りのデータに対応したハンドラは、コマンドラインユーティリティとNetIQ iManagerでのみ使用できます。

NetIQインポート/エクスポート変換ユーティリティは、次のどちらの方法でも使用できます。

NetIQインポート/エクスポート変換エンジンには、ウィザードからもコマンドラインインタフェースからもアクセスできます。ただし、コマンドラインインタフェースの方が、ソースハンドラとターゲットハンドラの組み合わせでより多くの選択肢があります。

NDSおよびeDirectoryの旧バージョンで提供されていたBULKLOADユーティリティとZONEIMPORTユーティリティはどちらも、NetIQインポート/エクスポート変換ユーティリティに置き換わっています。

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

インポート/エクスポート変換ウィザードは次の操作に使用できます。

- 166 ページの 「不足しているスキーマの追加」
- 167 ページの 「データをファイルからインポートする」
- 168 ページの 「データをファイルへエクスポートする」
- 169 ページの 「LDAPサーバ間でデータを移行する」
- 170 ページの 「スキーマをファイルから更新する」
- 171 ページの 「スキーマをサーバから追加する」
- 172 ページの 「スキーマファイルを比較する」
- 172 ページの 「サーバとファイルからスキーマを比較する」
- 173 ページの 「順序ファイルを生成する」

NetIQiManagerの使用方法とアクセス方法の詳細については、『*NetIQiManager管理ガイド*』を参照してください。

不足しているスキーマの追加

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。

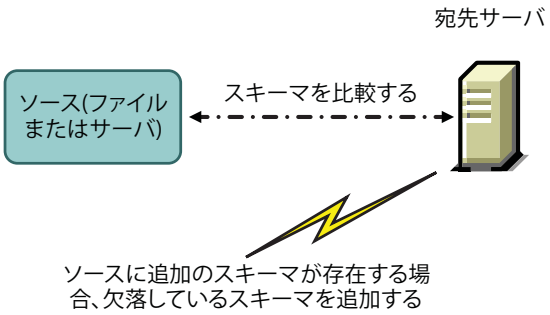
iManagerのICEウィザードからは、不足しているスキーマを次のオプションを使って追加できます。

- 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

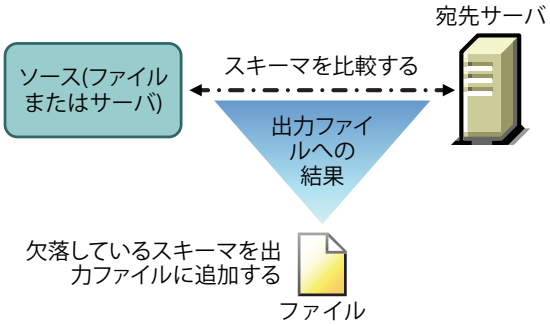
ICEはソースとターゲットのスキーマを比較できます。ソースはファイルまたはLDAPサーバのいずれかで、ターゲットはLDAPサーバです。ソースのスキーマファイルは、LDIF形式またはSCH形式のいずれかになります。

図7-1 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7-2 スキーマを比較して出力ファイルに結果を追加する



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。

データをファイルからインポートする

1. NetIQ iManagerで、［役割およびタスク］をクリックします。
2. ［eDirectoryの保守］>［インポート/エクスポート変換ウィザード］の順にクリックします。
3. ［ディスク上のファイルからデータをインポート］をクリックし、［次へ］をクリックします。
4. インポートするファイルのタイプを選択します。
5. インポートするデータが含まれているファイルの名前を指定し、適切なオプションを指定してから［次へ］をクリックします。

   このページのオプションは、選択したファイルのタイプによって異なります。使用可能なオプションの詳細については、［ヘルプ］をクリックしてください。
6. データのインポート先になるLDAPサーバを指定します。
7. 次の表の説明を参照して、適切なオプションを追加します。

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

8 ［**次へ**］をクリックし、［**終了**］をクリックします。

データをファイルへエクスポートする

1 NetIQ iManagerで、［**役割およびタスク**］をクリックします。

2 ［**eDirectoryの保守**］>［**インポート/エクスポート変換ウィザード**］の順にクリックします。

3 ［**ディスク上のファイルにデータをエクスポート**］>［**次へ**］の順にクリックします。

4 エクスポートするエントリが格納されているLDAPサーバを指定します。

［**詳細設定**］を使用して、LDAPソースハンドラの追加オプションを設定します。使用可能なオプションの詳細については、［**ヘルプ**］をクリックしてください。

5 次の表の説明を参照して、適切なオプションを追加します。

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

6 ［**次へ**］をクリックします。

7 エクスポートするエントリの検索条件を次のように指定します。

オプション	説明
ベースDN	検索要求のベース識別名 このフィールドを指定しなかった場合、デフォルトのベースDNである""(空の文字列)が使用されます。
スコープ	検索要求のスコープ
フィルタ	RFC 1558準拠の検索フィルタ デフォルトは「objectclass=*」です。
属性	検索エントリごとに取得する属性

8 ［**次へ**］をクリックします。

9 エクスポートするファイルのタイプを選択します。

エクスポートされたファイルは、一時的な場所に保存されます。このファイルは、インポート/エクスポート変換ウィザードの最後でダウンロードできます。

10 ［**次へ**］をクリックし、［**終了**］をクリックします。

LDAPサーバ間でデータを移行する

1 NetIQ iManagerで、［**役割およびタスク**］をクリックします。

2 ［**eDirectoryの保守**］>［**インポート/エクスポート変換ウィザード**］の順にクリックします。

3 ［**サーバ間でデータを移行**］>［**次へ**］の順にクリックします。

4 移行するエントリが格納されているLDAPサーバを指定します。

［**詳細設定**］を使用して、LDAPソースハンドラの追加オプションを設定します。使用可能なオプションの詳細については、［**ヘルプ**］をクリックしてください。

5 次の表の説明を参照して、適切なオプションを追加します。

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

6 ［**次へ**］をクリックします。

7 移行するエントリの検索条件を次のように指定します。

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

8 ［**次へ**］をクリックします。

9 データを移行するLDAPサーバを指定します。

10 ［**次へ**］をクリックし、［**終了**］をクリックします。

注: スキーマが各LDAPサービスで整合性を保っていることを確認します。

スキーマをファイルから更新する

1 NetIQ iManagerで、［**役割およびタスク**］をクリックします。

2 ［**eDirectoryの保守**］>［**インポート/エクスポート変換ウィザード**］の順にクリックします。

3 ［**ファイルからスキーマを追加**］>［**次へ**］の順にクリックします。

4 追加するファイルのタイプを選択します。

LDIFおよびスキーマファイルからタイプを選択できます。

5 追加するデータが含まれているスキーマの名前を指定し、適切なオプションを指定してから［**次へ**］をクリックします。

追加先の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**］を選択します。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。

このページのオプションは、選択したファイルのタイプによって異なります。使用可能なオプションの詳細については、［**ヘルプ**］をクリックしてください。

6 スキーマのインポート先になるLDAPサーバを指定します。

7 次の表の説明を参照して、適切なオプションを追加します。

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

8 ［**次へ**］>［**完了**］をクリックします。

スキーマをサーバから追加する

1 NetIQ iManagerで、［**役割およびタスク**］をクリックします。

2 ［**eDirectoryの保守**］>［**インポート/エクスポート変換ウィザード**］の順にクリックします。

3 ［**サーバからスキーマを追加**］>［**次へ**］の順にクリックします。

4 スキーマの追加元になるLDAPサーバを指定します。

5 次の表の説明を参照して、適切なオプションを追加します。

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

追加先の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**］を選択します。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。

6 スキーマの追加先になるLDAPサーバを指定します。

7 次の表の説明を参照して、適切なオプションを追加します。

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

8 ［**次へ**］>［**完了**］をクリックします。

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。

1 NetIQ iManagerで、［**役割およびタスク**］をクリックします。

2 ［**eDirectoryの保守**］>［**インポート/エクスポート変換ウィザード**］の順にクリックします。

3 ［**スキーマファイルの比較**］>［**次へ**］の順にクリックします。

4 比較するファイルのタイプを選択します。

LDIFおよびスキーマファイルから形式を選択できます。

5 比較するデータが含まれているスキーマの名前を指定し、適切なオプションを指定してから［**次へ**］をクリックします。

このページのオプションは、選択したファイルのタイプによって異なります。使用可能なオプションの詳細については、［**ヘルプ**］をクリックしてください。

6 比較するスキーマファイルを指定します。

LDIFファイルのみを選択できます。

7 ［**次へ**］>［**完了**］をクリックします。

2つのスキーマファイルの相違点は、処理の最後に表示されるリンクから確認できます。

サーバとファイルから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。

1 NetIQ iManagerで、［**役割およびタスク**］をクリックします。

2 ［**eDirectoryの保守**］>［**インポート/エクスポート変換ウィザード**］の順にクリックします。

3 ［**サーバとファイル間でスキーマファイルを比較**］>［**次へ**］の順にクリックします。

4 スキーマの比較元になるLDAPサーバを指定します。

5 次の表の説明を参照して、適切なオプションを追加します。

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

6 比較するファイルのタイプを選択します。

7 比較するデータが含まれているファイルの名前を指定し、適切なオプションを指定してから［**次へ**］をクリックします。

このページのオプションは、選択したファイルのタイプによって異なります。使用可能なオプションの詳細については、［**ヘルプ**］をクリックしてください。

8 ［**次へ**］>［**完了**］をクリックします。

サーバのスキーマとスキーマファイルの相違点は、処理の最後に表示されるリンクから確認できます。

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。

1 NetIQ iManagerで、［**役割およびタスク**］をクリックします。

2 ［**eDirectoryの保守**］>［**インポート/エクスポート変換ウィザード**］の順にクリックします。

3 ［**順序ファイルの生成**］、［**次へ**］の順にクリックします。

4 順序ファイルを生成するクラスを選択し、［**表示**］をクリックします。

［**順次属性**］リストに追加する属性を選択します。

補助クラスを選択して、［**Select Auxiliary Classes**］リストに追加します。

［順次属性］リストおよび［補助クラス］リストの詳細については、iMonitorのオンラインヘルプを参照してください。

［次へ］をクリックします。

5 次の表の説明を参照して、適切なオプションを追加します。

オプション	説明
コンテキスト	作成されたオブジェクトを関連付けるコンテキスト
データファイルを選択	データファイルの場所
データファイルでデリミタを選択	データファイル内で使用される区切り記号。デフォルトの区切り記号はコンマ(,)です。
ネーミング属性を選択	選択したクラスで使用できるすべての属性のリストのネーミング属性

［**詳細設定**］を使用して、LDAPソースハンドラの追加オプションを設定します。使用可能なオプションの詳細については、［**ヘルプ**］をクリックしてください。

［**処理するレコード**］を使用して、データファイルで処理するレコードを選択してください。使用可能なオプションの詳細については、［**ヘルプ**］をクリックしてください。

6 次の表の説明を参照して、適切なオプションを追加します。

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

［**詳細設定**］を使用して、LDAPソースハンドラの追加オプションを設定します。使用可能なオプションの詳細については、［**ヘルプ**］をクリックしてください。

7 ［**次へ**］をクリックし、［**終了**］をクリックします。

コマンドラインインタフェースを使用する

NetIQインポート/エクスポート変換ユーティリティのコマンドラインバージョンは、次の操作に使用できます。

- LDIFのインポート
- LDIFのエクスポート
- コンマ区切りデータのインポート
- コンマ区切りデータのエクスポート
- LDAPサーバ間でのデータの移行
- スキーマの比較と更新

- テンプレートを使用したeDirectoryへの情報のロード
- スキーマのインポート

NetIQインポート/エクスポート変換ウィザードは、NetIQ iManagerの一部としてインストールされます。Windowsバージョン(ice.exe)はインストールに組み込まれています。Linuxコンピュータでは、インポート/エクスポートユーティリティはNOVLiceパッケージに組み込まれています。

NetIQインポート/エクスポート変換構文

NetIQインポート/エクスポート変換ユーティリティは、次の構文で起動します。

```
ice general_options
-S[LDIF | LDAP | DELIM | LOAD | SCH] source_options
-D[LDIF | LDAP | DELIM] destination_options
```

またはスキーマキャッシュを使用する場合は、次の構文になります。

```
ice -C schema_options
-S[LDIF | LDAP] source_options
-D[LDIF | LDAP] destination_options
```

スキーマキャッシュを使用して更新を実行する場合、LDIFファイルはターゲットとして有効ではありません。

一般オプションの指定は任意です。ただし、指定する場合はソースハンドラオプションやターゲットハンドラオプションより前に指定します。-S(ソース)ハンドラセクションと-D(ターゲット)ハンドラセクションはどちらを先に指定してもかまいません。

利用できるソースハンドラとターゲットハンドラは次のとおりです。

- 177 ページの 「LDIFソースハンドラのオプション」
- 178 ページの 「LDIFターゲットハンドラのオプション」
- 179 ページの 「LDAPソースハンドラのオプション」
- 182 ページの 「LDAPターゲットハンドラのオプション」
- 183 ページの 「DELIMソースハンドラのオプション」
- 184 ページの 「DELIMターゲットハンドラのオプション」
- 185 ページの 「SCHソースハンドラのオプション」
- 186 ページの 「LOADソースハンドラのオプション」

全般オプション

一般オプションは、NetIQインポート/エクスポート変換エンジンの処理全体に影響のあるオプションです。

オプション	説明
-C	スキーマキャッシュを使用してスキーマの比較および更新を実行する場合に指定します。

オプション	説明
-l *log_file*	出力メッセージ(エラーメッセージなど)を書き込むログファイルの名前を指定します。このオプションを指定しなかった場合、エラーメッセージはice.logに出力されます。 Linuxコンピュータでこのオプションを指定しなかった場合、エラーメッセージはログに記録されません。
-o	既存のログファイルを上書きします。このフラグを設定しなかった場合、メッセージは既存のログファイルの末尾に追加されます。
-e *LDIF_error_log_file*	正常に処理されなかったエントリを書き込むファイルの名前を指定します。エントリはLDIF形式で書き込まれます。このファイルは、内容を調べてエラーを修正したうえで元のディレクトリに再適用できます。
-p *URL*	インポート/エクスポート変換エンジンが使用するXML配置ルールが格納されている場所を指定します。配置ルールはエントリの位置を変更するときに使用します。詳細については、193 ページの 「変換ルール」を参照してください。
-c *URL*	インポート/エクスポート変換エンジンが使用するXML作成ルールが格納されている場所を指定します。作成ルールは、インポート時にエントリを正しく作成するために必要な情報が欠落している場合にそれを補うために使用します。詳細については、193 ページの 「変換ルール」を参照してください。
-s *URL*	インポート/エクスポート変換エンジンが使用するXMLスキーママッピングルールが格納されている場所を指定します。スキーママッピングルールによって、転送元サーバのスキーマエレメントを、転送先サーバ上の同等ではあるが異なるスキーマエレメントにマッピングできます。 詳細については、193 ページの 「変換ルール」を参照してください。
-hまたは-?	コマンドラインのヘルプを表示します。

スキーマオプション

スキーマオプションでは、スキーマキャッシュを使用してスキーマの比較および更新操作を実行できます。

オプション	説明
-C -a	ターゲットスキーマを更新します(足りないスキーマを追加します)。
-C -c *filename*	指定したファイルにターゲットスキーマを出力します。
-C -n	スキーマの事前チェックを無効にします。

ソースハンドラのオプション

ソースハンドラオプション(-S)で、インポートするデータのソースを決定します。コマンドラインには、次のうちの1つだけを指定できます。

オプション	説明
-SLDIF	LDIFファイルをソースとして指定します。 サポートされているLDIFオプションのリストについては、177 ページの 「LDIFソースハンドラのオプション」を参照してください。

オプション	説明
-SLDAP	LDAPサーバをソースとして指定します。 サポートされているLDAPオプションのリストについては、179 ページの「LDAPソースハンドラのオプション」を参照してください。
-SDELIM	コンマ区切りのデータファイルをソースとして指定します。 **注:** パフォーマンスを向上させるには、NetIQインポート/エクスポート変換ユーティリティでDELIMではなくLDIFファイルを指定して、データをインポートします。カスタムPERLスクリプトを使用すると、必要なフォーマットで出力を生成できます。 サポートされているDELIMオプションのリストについては、183 ページの「DELIMソースハンドラのオプション」を参照してください。
-SSCH	スキーマファイルをソースとして指定します。 サポートされているSCHオプションのリストについては、185 ページの「SCHソースハンドラのオプション」を参照してください。
-SLOAD	DirLoadテンプレートをソースとして指定します。 サポートされているLOADオプションのリストについては、186 ページの「LOADソースハンドラのオプション」を参照してください。

ターゲットハンドラのオプション

ターゲットハンドラオプション(-D)で、エクスポートするデータの書き込み先を決定します。コマンドラインには、次のうちの1つだけを指定できます。

オプション	説明
-DLDIF	LDIFファイルを書き込み先として指定します。 サポートされているオプションのリストについては、178 ページの 「LDIFターゲットハンドラのオプション」を参照してください。
-DLDAP	LDAPサーバを書き込み先として指定します。 サポートされているオプションのリストについては、182ページの「LDAPターゲットハンドラのオプション」を参照してください。
-DDELIM	コンマ区切りのデータファイルを書き込み先として指定します。 サポートされているオプションのリストについては、184 ページの「DELIMターゲットハンドラのオプション」を参照してください。

LDIFソースハンドラのオプション

LDIFソースハンドラは、LDIFファイルからデータを読み込んで、それをNetIQインポート/エクスポート変換エンジンに送ります。

オプション	説明
-f *LDIF_file*	LDIFソースハンドラで読み込んだLDIFレコードを格納するファイルの名前を指定します。これらのLDIFレコードはインポート/エクスポート変換エンジンに送信されます。 Linuxコンピュータでは、このオプションを指定しなかった場合、入力データはstdinから読み込まれます。
-a	このオプションを設定した場合、指定したLDIFファイル内のレコードが内容レコード(変更タイプが設定されていないレコード)であれば、これらのレコードの変更タイプは「追加」であるとみなされます。
-c	エラーが発生してもLDIFソースハンドラの処理を続行します。ここでいうエラーとは、LDIF解析エラーや、ターゲットハンドラから返されたエラーなどです。このオプションが設定されている場合にエラーが発生すると、LDIFソースハンドラは、エラーを報告したうえで、LDIFファイルの次のレコードを検出し、処理を続行します。
-n	実際の更新は行わず、更新を行った場合の結果を表示して確認します。このオプションを設定すると、LDIFソースハンドラは、LDIFファイルの解析は行いますが、NetIQインポート/エクスポート変換エンジンやターゲットハンドラへのレコードの送信は行いません。
-m	このオプションを設定した場合、指定したLDIFファイル内のレコードが内容レコード(変更タイプが設定されていないレコード)であれば、これらのレコードの変更タイプは「変更」であるとみなされます。
-x	このオプションを設定した場合、指定したLDIFファイル内のレコードが内容レコード(変更タイプが設定されていないレコード)であれば、これらのレコードの変更タイプは「削除」であるとみなされます。
-R *value*	処理するレコードの範囲を指定します。
-v	ハンドラの冗長モードを有効にします。
-e *value*	LDIFファイル内の属性値を復号化するために使用するスキーム。［des/3des］。
-E *value*	属性の復号化用のパスワード。ADM_E_SRC_PASSWD変数を使用して、LDIFソースハンドラを暗号化できます。

LDIFターゲットハンドラのオプション

LDIFターゲットハンドラは、NetIQインポート/エクスポート変換エンジンからデータを受け取り、そのデータをLDIFファイルに書き込みます。

オプション	説明
-f *LDIF_file*	LDIFレコードの書き込み先になるファイルの名前を指定します。 Linuxコンピュータでは、このオプションを指定しなかった場合、出力データはstdoutに送られます。
-B	バイナリ値も印刷します。
-b	LDIFデータのBase64エンコードを行いません。
-e *value*	LDAPサーバから受け取った属性値を暗号化するために使用するスキーマ。［des/3des］。
-E *value*	属性の暗号化用のパスワード。ADM_E_DEST_PASSWD変数を使用して、LDIFターゲットハンドラを暗号化できます。

LDAPソースハンドラのオプション

LDAPソースハンドラは、検索要求を該当するLDAPサーバに送信することによってそのサーバからデータを読み込みます。LDAPソースハンドラは、検索操作の結果として受け取った検索エントリをNetIQインポート/エクスポート変換エンジンに送ります。

オプション	説明
-s *server_name*	ハンドラが検索要求を送るときの送信先LDAPサーバのDNS名またはIPアドレスを指定します。デフォルトはローカルホストです。 **注:** eDirectory 9.1以降を使用している場合は、このオプションに対してLDAPサーバのFQDNを指定する必要があります。
-p *port*	*server_name*で指定したLDAPサーバのポート番号を整数で指定します。デフォルトは389です。セキュリティで保護された操作の場合、デフォルトポートは636です。 ICEがSSLポート(デフォルトは636)でLDAPサーバと証明書なしで通信している場合は、サーバの証明書を信頼できるものとして許可します。このオプションは、サーバとクライアントの間で暗号化された通信が行われ、サーバの検証を必要としないような制御された環境でのみ使用してください。
-d *DN*	サーバによって指定されたバインド操作に使用するエントリの識別名を指定します。
-w *password*	*DN*で指定したエントリのパスワード属性を指定します。ADM_SRC_PASSWD変数を使用して、LDAPソースハンドラにパスワードを提供できます。
-W	*DN*で指定したエントリのパスワードの入力を求めるプロンプトが表示されます。 このオプションはLinuxでのみ適用できます。
-F *filter*	RFC1558準拠の検索フィルタを指定します。このオプションを指定しなかった場合、デフォルトの検索フィルタである「objectclass=*」が使用されます。
-n	実際の検索は行わず、検索の条件などを表示して確認します。

オプション	説明
-a *attribute_list*	検索対象の属性をカンマ区切りのリスト形式で指定します。属性名を指定するか、次の3つのうちいずれかを指定します。 ◆ 属性を検索しない場合は、(1.1) ◆ すべてのユーザ属性を検索する場合は、(*) ◆ オペレーショナルでない属性をすべて検索する場合は、空のリスト。 このオプションを指定しなかった場合、属性リストは空のリスト(デフォルト)になります。
-o *attribute_list*	LDAPサーバから受け取った検索結果をインポート/エクスポート変換エンジンに送信する前に、その検索結果から削除する属性をカンマ区切りのリスト形式で指定します。このオプションは、-aオプションでワイルドカードを指定してクラスの属性を初めにすべて検索してから、その検索結果をインポート/エクスポート変換エンジンに渡す前に一部の属性を削除したい場合に便利です。 たとえば、「-a* -o telephoneNumber」と指定すると、ユーザレベルの属性がすべて検索された後で、その検索結果から電話番号にフィルタを適用します。
-R	参照結果を自動的に適用しない場合に指定します。デフォルトでは、-dおよび-wオプションで指定された名前とパスワードによる参照結果が自動的に適用されます。
-e *value*	LDAPクライアントSDKで有効にするデバッグフラグを指定します。 詳細については、「「LDAP SDKデバッギングフラグを使用する」」を参照してください。
-b *base_DN*	検索要求のベース識別名を指定します。このオプションを指定しなかった場合、ベースDNはデフォルトの" "(空の文字列)になります。
-c *search_scope*	検索要求のスコープを指定します。有効な値は次のとおりです。 ◆ One: この値を指定すると、ベースオブジェクトの直接の子だけが検索の対象になります。 ◆ Base: この値を指定すると、ベースオブジェクトのエントリだけが検索の対象になります。 ◆ Sub: この値を指定すると、ベースオブジェクトをルートとし、ベースオブジェクトを含むLDAPサブツリーが検索の対象になります。 このオプションを指定しなかった場合は、検索スコープのデフォルトの「Sub」が使用されます。

オプション	説明
-r *deref_aliases*	検索時に別名を逆参照する方法を指定します。指定できる値は次のとおりです。 ◆ Never: この値を指定すると、サーバは別名の逆参照を行いません。 ◆ Always: この値を指定すると、検索のベースオブジェクトを検索するときと検索フィルタに一致するエントリを評価するときの両方で、別名の逆参照が行われます。 ◆ Search: この値を指定すると、ベースオブジェクトを検出した後で検索スコープ内のエントリにフィルタを適用するときには別名の逆参照が行われますが、ベースオブジェクト自体の検索時には別名の逆参照は行われません。 ◆ 検索: この値を指定すると、検索のベースオブジェクトを検索するときには別名の逆参照が行われますが、検索フィルタに一致するエントリを実際に評価するときには別名の逆参照は行われません。 このオプションを指定しなかった場合は、別名逆参照の方式のデフォルトである「Never」が使用されます。
-l *time_limit*	検索の制限時間を秒単位で指定します。
-z *size _limit*	検索結果として取得できるエントリの最大数を指定します。
-V *version*	接続に使用するLDAPプロトコルのバージョンを指定します。この値は2または3にする必要があります。このオプションを指定しなかった場合のデフォルトは3です。
-v	ハンドラの冗長モードを有効にします。
-L *filename*	SSL認証に使用されるサーバキーが格納されているPEM形式のファイルを指定します。デフォルト値は/var/opt/novell/eDirectory/data/SSCert.pemです。 **注:** LDAPサーバでEC証明書を使用している場合は、このオプションとともにSSECCert.pemを渡す必要があります。
-A	属性名のみを取得します。このオプションを指定した場合、出力される検索結果に属性値は含まれません。
-t	エラーが発生してもLDAPハンドラの処理を続行したい場合に指定します。
-m	LDAP操作は「変更」になります。
-x	LDAP操作は「削除」になります。
-k	このオプションはサポートされなくなりました。SSLを使用するには、-Lオプションを使用して有効な証明書を指定します。
-M	Manage DSA ITコントロールを有効にします。
-MM	Manage DSA ITコントロールを有効にし、重要度を高く設定します。

LDAPターゲットハンドラのオプション

LDAPターゲットハンドラは、NetIQインポート/エクスポート変換エンジンからデータを受け取り、それをLDAPサーバに送信します。データは更新操作の形で送信され、送信先サーバによって実行されます。

LDIFファイル内のハッシュ化パスワードについては、「「LDIFファイル内でのハッシュ化パスワードの表記」」を参照してください。

オプション	説明
-s *server_name*	ハンドラが検索要求を送るときの送信先LDAPサーバのDNS名またはIPアドレスを指定します。デフォルトはローカルホストです。
-p *port*	*server_name*で指定したLDAPサーバのポート番号を整数で指定します。デフォルトは389です。セキュリティで保護された操作の場合、デフォルトポートは636です。
-d *DN*	サーバによって指定されたバインド操作に使用するエントリの識別名を指定します。
-w *password*	*DN*で指定したエントリのパスワード属性を指定します。ADM_DEST_PASSWD変数を使用して、LDAPターゲットハンドラにパスワードを提供できます。
-W	*DN*で指定したエントリのパスワードの入力を求めるプロンプトが表示されます。 このオプションはLinuxでのみ適用できます。
-B	サーバへの更新操作の転送に非同期LBURP(LDAP Bulk Update/Replication Protocol)要求を使用しない場合は、このオプションを指定します。代わりに、標準の同期LDAP更新操作要求を使用します。 詳細については、203 ページの 「LBURP (LDAP Bulk Update/Replication Protocol)」を参照してください。
-F	前方向参照を作成できるようにします。作成するエントリの親が存在しない場合、エントリが正常に作成できるよう、そのエントリの親に対応するプレースフォルダが作成されます。このプレースホルダを**前方向参照**といいます。以後の操作で親が作成されると、前方向参照は通常のエントリに変更されます。
-l	パスワード値の格納にNMAS (NetIQモジュラー認証サービス)の簡易パスワードメソッドを使用する場合は、このオプションを指定します。簡易パスワードを使用する場合、パスワードはディレクトリ内の安全な場所に保持されますが、鍵のペアはサーバ間での認証で実際に必要になるまで生成されません。
-e *value*	LDAPクライアントSDKで有効にするデバッグフラグを指定します。 詳細については、「「LDAP SDKデバッギングフラグを使用する」」を参照してください。
-V *version*	接続に使用するLDAPプロトコルのバージョンを指定します。この値は2または3にする必要があります。このオプションを指定しなかった場合のデフォルトは3です。

オプション	説明
-L *filename*	SSL認証に使用されるサーバキーが格納されているPEM形式のファイルを指定します。デフォルト値は/var/opt/novell/eDirectory/data/SSCert.pemです。 **注:** LDAPサーバでEC証明書を使用している場合は、このオプションとともにSSECCert.pemを渡す必要があります。
-k	このオプションはサポートされなくなりました。SSLを使用するには、-Lオプションを使用して有効な証明書を指定します。
-M	Manage DSA ITコントロールを有効にします。
-MM	Manage DSA ITコントロールを有効にし、重要度を高く設定します。
-P	同時LBURP処理を有効にします。このオプションは、LDIF内のすべての処理を追加する場合にだけ有効にします。–Fオプションを使用する場合は、-Pはデフォルトで有効になります。
-Z	非同期要求の数を指定します。この数値は、LDAPサーバから返される結果を待たずに、ICEクライアントからLDAPサーバに非同期に送信できるエントリの数を示します。

DELIMソースハンドラのオプション

DELIMソースハンドラはコンマ区切りのデータファイルからデータを読み込み、それをターゲットハンドラに送信します。

オプション	説明
-f *filename*	DELIMソースハンドラによって読み込まれるコンマ区切りのレコードを含んだファイルの名前を指定します。これらのDELIMレコードはターゲットハンドラに送信されます。
-F *value*	-fで指定したファイルに対する属性のデータオーダを含んだファイルを指定します。 デフォルトでは、区切り文字で区切られたファイル内の属性の列数は、属性値の最大数と一致します。属性が繰り返されている場合、この列数はテンプレート内で属性が繰り返される回数に一致します。このオプションが指定されていない場合、-tを使用してこの情報を直接入力する必要があります。 詳細については、189 ページの 「コンマ区切りのインポートを実行する」を参照してください。
-t *value*	コンマ区切りの属性リストです。このリストによって、-fで指定されたファイルに対する属性のデータオーダを指定します。 デフォルトでは、区切り文字で区切られたファイル内の属性の列数は、属性値の最大数と一致します。属性が繰り返されている場合、この列数はテンプレート内で属性が繰り返される回数に一致します。このオプションまたは-Fのいずれかを指定する必要があります。 詳細については、189 ページの 「コンマ区切りのインポートを実行する」を参照してください。

オプション	説明
-c	エラーが発生してもDELIMソースハンドラの処理を続行したい場合に指定します。ここでいうエラーとは、カンマ区切りデータファイルの解析エラーや、ターゲットハンドラから返されたエラーなどです。このオプションが設定されている場合にエラーが発生すると、DELIMソースハンドラは、エラーを報告したうえで、コンマ区切りデータファイル内の次のレコードを検出し、処理を続行します。
-n *value*	新しいオブジェクトにLDAPネーミング属性を指定します。この属性は、-Fまたは-tを使用して指定する属性データに含まれている必要があります。
-l *value*	RDNの追加先のパスを指定します(o=myCompanyなど)。DNを渡す場合、この値は必要ありません。
-o *value*	オブジェクトクラスのコンマ区切りのリスト(入力ファイルに含まれていない場合)、または補助クラスなどその他のオブジェクトクラスを指定します。デフォルト値は「inetorgperson」です。
-i *value*	スキップする列のコンマ区切りのリストです。この値には、スキップする列の数を整数で指定します。たとえば3列目と5列目をスキップする場合は、「i3,5」と指定します。
-d *value*	区切り記号を指定します。デフォルトの区切り記号はカンマ(,)です。 次に示すのは、特別な場合の区切り記号です。 ◆ [q] =引用符(区切り記号としての単一の") ◆ [t] =タブ たとえば、タブを区切り記号として指定するには、-d[t]を渡します。
-q *value*	2次的区切り記号を指定します。デフォルトのセカンダリ区切り記号は一重引用符(')です。 次に示すのは、特別な場合の区切り記号です。 ◆ [q] =引用符(区切り記号としての単一の") ◆ [t] =タブ たとえば、タブを区切り記号として指定するには、-q[t]を渡します。
-v	冗長モードで実行します。
-k *value*	区切りファイルの最初の行をテンプレートにする場合に指定します。このオプションを-tまたは-Fとともに指定した場合、指定したテンプレートと区切りファイル内のテンプレートの整合性がチェックされます。

DELIMターゲットハンドラのオプション

DELIMターゲットハンドラはソースハンドラからデータを受け取り、そのデータをカンマ区切りのデータファイルに書き込みます。

オプション	説明
-f *filename*	コンマ区切りレコードの書き込み先になるファイルの名前を指定します。

オプション	説明
-F *value*	-fで指定したファイルに対する属性のデータオーダを含んだファイルを指定します。 デフォルトでは、区切り文字で区切られたファイル内の属性の列数は、属性値の最大数と一致します。属性が繰り返されている場合、この列数はテンプレート内で属性が繰り返される回数に一致します。このオプションが指定されていない場合、-tを使用してこの情報を直接入力する必要があります。
-t *value*	コンマ区切りの属性リストです。このリストによって、-fで指定されたファイルに対する属性のデータオーダを指定します。 デフォルトでは、区切り文字で区切られたファイル内の属性の列数は、属性値の最大数と一致します。属性が繰り返されている場合、この列数はテンプレート内で属性が繰り返される回数に一致します。このオプションまたは-Fのいずれかを指定する必要があります。
-I *value*	RDNまたはDNのいずれかになります。ドライバによってデータ内に配置されるのが、DN全体またはRDNのみのどちらになるかを指定します。デフォルト値はRDNです。
-d *value*	区切り記号を指定します。デフォルトの区切り記号はカンマ(,)です。 次に示すのは、特別な場合の区切り記号です。 ◆ [q] =引用符(区切り記号としての単一の") ◆ [t] =タブ たとえば、タブを区切り記号として指定するには、-d[t]を渡します。
-q *value*	2次的区切り記号を指定します。デフォルトのセカンダリ区切り記号は一重引用符(')です。 次に示すのは、特別な場合の区切り記号です。 ◆ [q] =引用符(区切り記号としての単一の") ◆ [t] =タブ たとえば、タブを区切り記号として指定するには、-q[t]を渡します。
-n *value*	インポート処理中に追加されるネーミング属性を指定します。たとえばcnなどです。

SCHソースハンドラのオプション

SCHハンドラは、古いNDSやeDirectoryのスキーマファイル(拡張子*.schがついたファイル)からデータを読み込んで、それをNetIQインポート/エクスポート変換エンジンに送ります。このハンドラを使用すれば、拡張子*.schがついたファイルを入力として、スキーマ関連の操作をLDAPサーバに実装できます。

SCHハンドラは、ソースハンドラだけのハンドラです。スキーマハンドラを使用すると、LDAPサーバに*.schファイルをインポートできますが、*.schファイルをエクスポートすることはできません。

SCHハンドラでサポートされているオプションを次の表に示します。

オプション	説明
-f *filename*	*.schファイルの完全なパス名を指定します。
-v	(オプション)冗長モードで実行します。

LOADソースハンドラのオプション

DirLoadハンドラはテンプレートのコマンドからeDirectory情報を生成します。このテンプレートファイルは-f引数で指定します。このファイルには、属性仕様の情報とプログラム制御の情報が保持されます。

オプション	説明
-f *filename*	すべての属性仕様とプログラムの実行を制御するすべての情報を含んだテンプレートファイルを指定します。
-c	エラーが通知された場合、次のレコードから続行します。
-v	冗長モードで実行します。
-r	データが追加されずに削除されるように、要求を削除要求に変更します。このオプションにより、DirLoadテンプレートを使用して追加されたレコードを削除できます。
-m	テンプレートファイル内に変更要求を作成します。

属性仕様 新しいオブジェクトのコンテキストを決定します。

次の属性仕様ファイルのサンプルを参照してください。

```
givenname: $R(first)
initial: $R(initial)
sn: $R(last)
dn:cn=$A(givenname,%.1s)$A(initial,%.1s)$A(sn),ou=dev,ou=ds,o=novell
objectclass: inetorgperson
telephonenumber: 1-800-$N(1-999,%03d)-$C(%04d)
title: $R(titles)
locality: Our location
```

属性仕様ファイルの形式はLDIFファイルに似ていますが、属性仕様ファイルでは強力な構成体を使用して、詳細な情報と属性間の関係を指定することができます。

固有の数値 指定されたオブジェクトに対する固有の数値を属性値に挿入します。

```
Syntax: $C[(<format)]
```

オプションの<*format*は、値に適用された出力形式を指定します。形式を指定しない場合、カッコは2種類とも必要ありません。

```
$C
$C(%d)
$C(%04d)
```

$Cのみを指定すると、現在の数値が属性値に挿入されます。「%d」は、何も指定されなかった場合にプログラムが使用するデフォルト形式であるため、$Cは$C(%d)と同じです。数値は各オブジェクトの後で増加するため、属性仕様で$Cを複数回使用しても、単一オブジェクト内では数値は変わりません。開始値は、!COUNTER=*value*の構文を使用して、設定ファイル内で指定できます。

任意の数値 次の構文を使用して、属性値に任意の数値を挿入します。

```
$N(<low-<high[,<format])]
```

<*low*と<*high*では、下限値と上限値を指定します。任意の数字が生成される際に各々の値を使用します。オプションの<*format*は、リストの値に適用される出力形式を指定します。

```
$N(1-999)
$N(1-999,%d)
$N(1-999,%03d)
```

リストの任意の文字列 次の構文を使用して、指定したリストから任意に選択された文字列を属性値に挿入します。

```
$R(<filename[,<format])]
```

<*filename*には、値を格納しているファイルを指定します。ファイルへのパスは絶対パスまたは相対パスのどちらでも指定できます。リストを格納しているファイルには、このパッケージに含まれているものがあります。値は改行文字で区切る必要があります。

オプションの<*format*は、値に適用された出力形式を指定します。

```
$A(givenname)
$A(givenname,%s)
$A(givenname,%.1s)
```

前方向参照は使用できませんので注意してください。属性値を使用する場合、その属性は全て、属性仕様ファイル内で現在の属性より前にある必要があります。下記の例では、DNの一部であるcnは、givenname、initial、およびsnから構築されます。したがって設定ファイルでは、これらの属性はDNの前に存在する必要があります。

```
givenname: $R(first)
initial: $R(initial)
sn: $R(last) dn:o=novell,ou=dev,ou=ds,cn=$A(givenname,%.1s)$A(initial,%.1s)$A(sn)
```

DNはLDIFファイル内で特殊処理されます。設定内でのDNの場所に関係なく、DNが最初に(LDIF構文に従って)LDIFファイルに書き込まれます。その他のすべての属性は、表示された順に書き込まれます。

制御設定 オブジェクト作成の際の制御を追加します。すべての制御には、属性設定と区別するために、行頭の文字として感嘆符(!)が付いています。制御はファイル内の任意の場所に置くことができます。

```
!COUNTER=300
!OBJECTCOUNT=2
!CYCLE=title
!UNICYCLE=first,last
!CYCLE=ou,BLOCK=10
```

- カウンタ

  固有のカウンタ値の開始値を提供します。カウンタ値は、$C構文内の任意の属性に挿入されます。

- オブジェクト数

OBJECTCOUNTは、テンプレートから作成されるオブジェクトの数を決定します。

- サイクル

  CYCLEは、ファイル($R構文)から任意の値を抜き出す方法を変更するときに使用できます。この設定には異なる3つの値があります。

  ```
  !CYCLE=title
  ```

  「title」というリスト名が使用される場合は常に、値が任意で選択されるのではなく、リストの順に次の値が抜き出されます。順番に値がすべて使用された場合には、再度リストの最初から開始します。

  ```
  !CYCLE=ou,BLOCK=10
  ```

  リスト「ou」のそれぞれの値が10回ずつ使用され、その後次の値に移動します。

  CYCLE制御設定のうちで最も興味深いバリアントは、UNICYCLEです。UNICYCLEは、一連のソースを左から右の順序で繰り返すように指定します。このため、必要な場合に一意の値が必ず作成されます。UNICYCLE制御を使用する場合、OBJECTCOUNT制御は、オブジェクト数を、リストから作成できる固有のオブジェクトの最大数に制限するためだけに使用します。つまり、UNICYCLEに含まれるリストが15000オブジェクトを作成できる場合、OBJECTCOUNTはその数を減らすことはできますが、増やすことはできません。

  たとえば、givennameファイルに2つの値(「Doug」および「Karl」)があり、かつsnファイルに3つの値(「Hoffman」、「Schultz」、および「Grieger」)があるとします。制御設定が「!UNICYCLE=givenname,sn」であり、属性定義が「cn$R(givenname$R(sn)」である場合、次のcnが作成されます。

  cn: Doug Hoffmancn cn: Karl Hoffmancn cn: Doug Schultzcn cn: Karl Schultzcn cn: Doug Griegercn cn: Karl Grieger

例

ここでは、NetIQインポート/エクスポート変換ユーティリティのコマンドラインユーティリティで次の操作をする場合のコマンドの例を紹介します。

- 188 ページの 「LDIFインポートの実行」
- 189 ページの 「LDIFエクスポートを実行する」
- 189 ページの 「コンマ区切りのインポートを実行する」
- 190 ページの 「コンマ区切りのエクスポートを実行する」
- 190 ページの 「LDAPサーバ間でデータを移行する」
- 190 ページの 「スキーマのインポートを実行する」
- 191 ページの 「LOADファイルのインポートを実行する」
- 193 ページの 「暗号化された属性を含むLDIFエクスポートをLDAPサーバから実行する」
- 193 ページの 「暗号化された属性を含むLDIFインポートを実行する」

LDIFインポートの実行

LDIFのインポートを実行するには、LDIFソースハンドラとLDAPターゲットハンドラを組み合わせて次の例のように指定します。

```
ice -S LDIF -f entries.ldif -D LDAP -s server1.acme.com -p 389 -d cn=admin,c=us -w
secret
```

コマンドラインでこのように指定すると、LDIFデータがentries.ldifから読み込まれ、ポート389にあるLDAPサーバserver1.acme.comに送られます。送信時の識別子は「cn=admin,c=us」、パスワードは「secret」になります。

LDIFエクスポートを実行する

LDIFのエクスポートを実行するには、LDAPソースハンドラとLDIFターゲットハンドラを組み合わせます。次に例を示します。

```
ice -S LDAP -s server1.acme.com -p 389 -d cn=admin,c=us -w password -F
objectClass=* -c sub -D LDIF -f server1.ldif
```

コマンドラインでこのように指定すると、識別子「cn=admin,c=us」およびパスワード「password」を使用してサブツリー検索が実行され、ポート389にあるLDAPサーバserver1.acme.com内のオブジェクトがすべて検出されます。結果のデータはLDIF形式でserver1.ldifに出力されます。

コンマ区切りのインポートを実行する

コンマ区切りのインポートを実行するには、コマンドを次の例のように指定します。

```
ice -S DELIM -f/tmp/in.csv -F /tmp/order.csv -ncn -lo=acme -D LDAP -s
server1.acme.com -p389 -d cn=admin,c=us -w secret
```

コマンドをこのように指定すると、/tmp/in.csvファイルからコンマ区切りの値が読み込まれ、/tmp/order.csvファイルから属性の順序が読み込まれます。in.csv内の各属性エントリに対して、order.csvで属性タイプが指定されます。たとえば、in.csvに次の値があるとします。

```
pat,pat,engineer,john
```

この場合、order.csvに含まれる値は次のようになります。

```
dn,cn,title,sn
```

order.csvの情報は、-tオプションを使用して直接入力することもできます。

次にデータは、識別子「cn=admin,c=us」、およびパスワード「secret」を使用して、ポート389でLDAPサーバserver1.acme.comに送られます。

この例では、-nオプションを使用して、cnがオブジェクトの新しいDNになるように指定し、-lオプションを使用して、このオブジェクトが組織コンテナacmeに追加されるようにします。

NetIQインポート/エクスポート変換ユーティリティを使用して生成されたコンマ区切りファイルは、生成するために使用されたテンプレートを最初の行に含みます。コンマ区切りファイルの最初の行がテンプレートであることを指定するには、-kオプションを使用します。-Fまたは-tを-kとともに使用する場合、指定するテンプレートは、コンマ区切りファイル内のテンプレートと整合していなければなりません。つまり、両方の属性が正確に一致する必要があります。ただし、各属性の出現数や順序は異なっていても構いません。上の例では、in.csvの

最初の行にdn,cn,title,title,title,snが含まれています。以下のテンプレートは整合しており、-kの使用時に-tまたは-Fもともに使用できます。

dn,cn,title,sn (属性titleの反復回数が異なる)

dn,sn,title,cn (属性の順序が異なる)

しかし以下のテンプレートは、in.csv内のテンプレートと整合していないため、-kの使用時に-tまたは-Fを指定することはできません。

dn,cn,title,sn,objectclass (新しい属性objectclassが含まれている)

dn,cn,title (属性snが含まれていない)

コンマ区切りのエクスポートを実行する

コンマ区切りのエクスポートを実行するには、コマンドを次の例のように指定します。

```
ice -S LDAP -s server1.acme.com -p 389 -d cn=admin,c=us -w password -F
objectClass=* -c sub -D DELIM -f /tmp/server1.csv -F order.csv
```

コマンドラインでこのように指定すると、識別子「cn=admin,c=us」およびパスワード「password」を使用してサブツリー検索が実行され、ポート389にあるLDAPサーバserver1.acme.com内のオブジェクトがすべて検出されます。結果のデータはコンマ区切りの形式で/tmp/server1.csvファイルに出力されます。

order.csv内の属性に複数の値が含まれている場合、/tmp/server1.csvでは、この属性の列数が、属性値の最大数と一致します。order.csv内で属性が繰り返されている場合、この属性の列数は、属性が繰り返される回数と一致します。

たとえば、order.csvにdn,sn,objectclassが含まれている場合、エクスポートされたすべてのエントリについて、objectclassの値が4つあるのに対し、dnとsnの値は1つずつしかない場合、dnとsnの列数はそれぞれ1つずつになるのに対し、objectclassの列数は4つになります。objectclassの値を2つだけコンマ区切りファイルに出力するには、order.csvにはdn,sn,objectclass,objectclassが含まれている必要があります。

どちらの場合も、属性が/tmp/server1.csvの最初の行に書き込まれます。最初の例では、/tmp/server1.csvの最初の行にdn,sn,objectclass,objectclass,objectclass,objectclasssが含まれており、2番目の例では、/tmp/server1.csvの最初の行にdn,sn,objectclass,objectclassが含まれています。

2回目以降のインポート時に、最初の行を一連の属性として処理させないようにするには、-kオプションを使用します。詳細については、189 ページの 「コンマ区切りのインポートを実行する」を参照してください。

LDAPサーバ間でデータを移行する

LDAPサーバ間でデータを移行するには、LDAPソースハンドラとLDAPターゲットハンドラを組み合わせます。次に例を示します。

```
ice -S LDAP -s server1.acme.com -p 389 -d cn=admin,c=us -w password -F
objectClass=* -c sub -D LDAP -s server2.acme.com -p 389 -d cn=admin,c=us -w secret
```

このコマンドを実行すると、識別子「cn=admin,c=us」およびパスワード「password」を使用してサブツリー検索が実行され、ポート389にあるLDAPサーバserver1.acme.com内のオブジェクトがすべて検出されます。結果のデータは、識別子「cn=admin,c=us」およびパスワード「secret」で、ポート389にあるLDAPサーバserver2.acme.comに送られます。

スキーマのインポートを実行する

スキーマファイルのインポートを実行するには、コマンドを次の例のように指定します。

```
ice -S SCH -f $HOME/myfile.sch -D LDAP -s myserver -d cn=admin,o=novell -w passwd
```

このコマンドを実行すると、スキーマデータがmyfile.schから読み込まれ、LDAPサーバ「myserver」に送られます。送信時の識別子は「cn=admin,o=novell」、パスワードは「passwd」になります。

LOADファイルのインポートを実行する

LOADファイルのインポートを実行するには、コマンドを次の例のように指定します。

```
ice -S LOAD -f attrs -D LDIF -f new.ldf
```

次に、属性ファイル「attrs」の内容の例を示します。

```
#=====================================================================

#  DirLoad 1.00
#=====================================================================

!COUNTER=300

!OBJECTCOUNT=2
#---------------------------------------------------------------------

#  ATTRIBUTE TEMPLATE
# ---------------------------------------------------------------------

objectclass: inetorgperson

givenname: $R(first)

initials: $R(initial)

sn: $R(last)

dn: cn=$A(givenname,%.1s)$A(initial,%.1s)$A(sn),ou=$R(ou),ou=dev,o=novell,

telephonenumber: 1-800-$N(1-999,%03d)-$C(%04d)

title: $R(titles)
```

コマンドプロンプトから前のコマンドを実行すると、次のLDIFファイルが作成されます。

```
version: 1

dn: cn=JohnBBill,ou=ds,ou=dev,o=novell

changetype: add

objectclass: inetorgperson

givenname: John

initials: B

sn: Bill

telephonenumber: 1-800-290-0300

title: Amigo

dn: cn=BobJAmy,ou=ds,ou=dev,o=novell

changetype: add

objectclass: inetorgperson

givenname: Bob

initials: J

sn: Amy
```

```
telephonenumber: 1-800-486-0301

title: Pomo
```

コマンドプロンプトから次のコマンドを実行すると、データがLDAPハンドラを経由してLDAPサーバに送られます。

```
ice -S LOAD -f attrs -D LDAP -s www.novell.com -d cn=admin,o=novell -w admin
```

次のコマンドを使用する際に前のテンプレートファイルを使用すると、前のコマンドで追加したすべてのレコードが削除されます。

```
ice -S LOAD -f attrs -r -D LDAP -s www.novell.com -d cn=admin,o=novell -w admin
```

-mを使用して変更する場合は、次の例のようにレコードを変更します。

```
# ====================================================================

#  DirLoad 1.00

# ====================================================================
!COUNTER=300

!OBJECTCOUNT=2

#--------------------------------------------------------------------

#  ATTRIBUTE TEMPLATE

# --------------------------------------------------------------------

dn: cn=$R(first),%.1s)($R(initial),%.1s)$R(last),ou=$R(ou),ou=dev,o=novell

delete: givenname

add: givenname

givenname: test1

replace: givenname

givenname: test2

givenname: test3
```

「attrs」ファイルが上のデータを格納しているときに次のコマンドを使用した場合の例を示します。

```
ice -S LOAD -f attrs -m -D LDIF -f new.ldf
```

LDIFデータは次のような結果になります。

```
version: 1

dn: cn=BillTSmith,ou=ds,ou=dev,o=novell

changetype: modify

delete: givenname

-

add: givenname

givenname: test1
```

```
-

replace: givenname

givenname: test2

givenname: test3

-

dn: cn=JohnAWilliams,ou=ldap,ou=dev,o=novell

changetype: modify

delete: givenname

-

add: givenname

givenname: test1

-

replace: givenname

givenname: test2

givenname: test3

-
```

暗号化された属性を含むLDIFエクスポートをLDAPサーバから実行する

暗号化された属性を含むLDIFのエクスポートをLDAPサーバから実行するには、次のように、LDAPソースハンドラおよびLDIFターゲットハンドラを暗号化用のスキームおよびパスワードと組み合わせて使用します。

```
ice -S LDAP -s server1.acme.com -p 636 -L cert-server1.pem -d cn=admin,c=us -w
password -F objectClass=* -c sub -D LDIF -f server1.ldif -e des -E secret
```

暗号化された属性を含むLDIFインポートを実行する

ICEによってあらかじめ暗号化されている属性を持つファイルのLDIFインポートを実行するには、次のように、LDIFソースを、ファイルとLDAPターゲットハンドラをエクスポートするために以前使用したスキームおよびパスワードと組み合わせて使用します。

```
ice -S LDIF -f server1.ldif -e des -E secret -D LDAP -s server2.acme.com -p 636 -L
cert-server2.pem -d cn=admin,c=us -w password
```

変換ルール

NetIQインポート/エクスポート変換エンジンは、ソースハンドラから受け取ったレコードをターゲットハンドラに送る前に、レコードに対して変換処理を行います。この変換処理の内容は一連のルールを使用して指定できます。これらのルールはXMLで記述します(XMLファイルとして作成される場合と、XML用ディレクトリ内に格納されたXMLデータとして作成される場合があります)。このルールにより、LDAPディレクトリ間でのエントリのインポート時に、次の問題が解決されます。

- 不足している情報

- 階層の違い
- スキーマの違い

次の3種類の変換ルールがあります。

ルール	説明
配置	エントリの位置を変更します。 たとえば、あるユーザグループをいったん「l=San Francisco, c=US」というコンテナにインポートし、インポートが終わった後で「l=Los Angeles, c=US」というコンテナに移す場合などに、配置ルールを利用できます。 これらのルールの形式については、199 ページの 「配置ルール」を参照してください。
作成	インポート時にエントリを正しく作成するために必要な情報が欠落している場合にそれを補います。 たとえば、LDIFデータのエクスポート元サーバのスキーマではユーザエントリに必要とされる属性がcn(commonName)属性だけであるのに対し、LDIFデータのインポート先サーバのスキーマではcn属性の他にsn(surname)属性も必要とされる場合が考えられます。このような場合は作成ルールを使用すれば、インポート/エクスポート変換エンジンが各エントリを処理するときに、そのエントリにデフォルトのsn値(" "など)が設定されるようにすることができます。これにより、各エントリはインポート先サーバに送信されるときには必要な属性であるsn属性を持つことになり、エントリの正常な追加が保証されます。 これらのルールの形式については、197 ページの 「作成ルール」を参照してください。
スキーママッピング	サーバ間でデータを転送する場合(直接転送するかLDIFを使用するかに関係なく)で、転送元サーバのスキーマと転送先サーバのスキーマが異なっている場合、次のようにスキーママッピングを使用できます。 ◆ エクスポート元サーバからインポートするエントリのオブジェクトクラスと属性タイプをすべて受け付けることができるように、インポート先サーバ上のスキーマを拡張します。 ◆ 転送元サーバのスキーマエレメントを、転送先サーバ上の同等ではあるが異なるスキーマエレメントにマッピングします。 これらのルールの形式については、196 ページの 「スキーママッピングルール」を参照してください。

これらの変換ルールは、NetIQ eDirectoryインポート/エクスポートウィザードとコマンドラインインタフェースのどちらでも利用できます。XMLルールの詳細については、195ページの 「XMLルールを使用する」を参照してください。

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

1 iManagerで、［**役割およびタスク**］をクリックします。

2 ［**eDirectoryの保守**］>［**インポート/エクスポート変換ウィザード**］の順にクリックします。

3 実行するタスクを選択します。

4 ［**詳細設定**］の下の次のオプションから選択します。

オプション	説明
スキーマルール	インポート/エクスポート変換エンジンが使用するXMLスキーママッピングルールが格納されている場所を指定します。
配置ルール	インポート/エクスポート変換エンジンが使用するXML配置ルールが格納されている場所を指定します。
作成ルール	インポート/エクスポート変換エンジンが使用するXML作成ルールが格納されている場所を指定します。

5 ［次へ］をクリックします。

6 表示される指示に従って、選択したタスクを完了します。

コマンドラインインタフェースを使用する

コマンドラインバージョンで変換ルールを使用するには、NetIQインポート/エクスポート変換ユーティリティの実行ファイルを起動するときに、使用したいルールに対応する一般オプション(-p、-c、または-s)を指定します。詳細については、175 ページの 「全般オプション」を参照してください。

オプション	説明
-p *URL*	インポート/エクスポート変換エンジンが使用するXML配置ルールが格納されている場所です。
-c *URL*	インポート/エクスポート変換エンジンが使用するXML作成ルールが格納されている場所です。
-s *URL*	インポート/エクスポート変換エンジンが使用するXMLスキーママッピングルールが格納されている場所です。

すべての3つのオプションで、*URL*を次のいずれかに指定します。

- 次の形式のURL:

  `file://[path/]filename`

  ファイルは、ローカルファイルシステムに存在する必要があります。
- ベースレベルの検索を指定するRFC2255準拠のLDAPURLと、1つの値の属性タイプに対して1つの属性記述が定義されている属性リスト。

XMLルールを使用する

NetIQインポート/エクスポート変換ルールで使用されるXML形式は、NetIQ Identity Managerの場合と同じです。NetIQ Identity Managerの詳細については、*NetIQ Identity Managerマニュアルサイト*を参照してください。

スキーママッピングルール

スキーママッピングルールの最上位エレメントは、<attr-name-map>です。インポートスキーマとエクスポートスキーマの相互関係は、マッピングルールによって決まります。マッピングルールは、指定されたインポートクラスの定義や属性を、対応するエクスポートスキーマの定義に関連付けます。

マッピングルールは、属性名またはクラス名に対応させて設定します。

- 属性マッピングの場合、マッピングルールでは、それが属性マッピングであること、ネームスペース(nds-nameはソース名のタグ)、eDirectoryネームスペース内での名前、および他のネームスペース(app-nameはターゲット名のタグ)とそのネームスペース内での名前を指定する必要があります。マッピングルールでは、マッピングが特定のクラスに適用されることを指定することも、その属性を持つすべてのクラスに適用されることを指定することもできます。
- クラスマッピングの場合、マッピングルールでは、それがクラスマッピングルールであること、ネームスペース(eDirectoryまたはアプリケーション)とそのネームスペース内での名前、およびその他のネームスペースとそのネームスペース内での名前を指定する必要があります。

スキーママッピングルールの正式なDTD定義を次に示します。

```
<!ELEMENT attr-name-map (attr-name | class-name)*>

<!ELEMENT attr-name (nds-name, app-name)>
<!ATTLIST attr-name
          class-name    CDATA    #IMPLIED>

<!ELEMENT class-name (nds-name, app-name)>

<!ELEMENT nds-name (#PCDATA)>

<!ELEMENT app-name (#PCDATA)>
```

複数のマッピングエレメントをファイルに定義できます。各エレメントは、ファイルに定義されている順番で処理されます。1つのクラスまたは属性を複数回マッピングした場合は、最初のマッピングが優先されます。

スキーママッピングルールの作成例を次に示します。

スキーマルール1: 次のルールでは、ソースのsurname属性をターゲットのinetOrgPersonクラスのsn属性にマッピングします。

```
<attr-name-map>
   <attr-name class-name="inetOrgPperson">
      <nds-name>surname</nds-name>
      <app-name>sn</app-name>
   </attr-name>
</attr-name-map>
```

スキーマルール2: 次のルールでは、ソースのinetOrgPersonクラスの定義をターゲットのUserクラスの定義にマッピングします。

```
<attr-name-map>
   <class-name>
      <nds-name>inetOrgPerson</nds-name>
      <app-name>User</app-name>
   </class-name>
</attr-name-map>
```

スキーマルール3: 次の例では、2種類のルールを定義します。1つ目のルールでは、Surname属性を使用するすべてのクラスについて、ソースのSurname属性をターゲットのsn属性にマッピングします。2つ目のルールでは、ソースのinetOrgPersonクラスの定義をターゲットのUserクラスの定義にマッピングします。

```
<attr-name-map>
   <attr-name>
      <nds-name>surname</nds-name>
      <app-name>sn</app-name>
   </attr-name>
   <class-name>
      <nds-name>inetOrgPerson</nds-name>
      <app-name>User</app-name>
   </class-name>
</attr-name-map>
```

コマンド例: スキーマルールがsr1.xmlファイルに保存されている場合、次のコマンドを指定することにより、1entry.ldfファイルの処理中にそのルールを使用すること、および結果をターゲットファイルoutt1.ldfに送ることがインポート/エクスポート変換ユーティリティに指示されます。

```
ice -o -sfile://sr1.xml -SLDIF -f1entry.ldf -c -DLDIF
-foutt1.ldf
```

作成ルール

作成ルールによって、宛先ディレクトリ内に新規エントリを作成する場合の条件が指定されます。次のエレメントがサポートされます。

- **必須属性** すべての必須属性について、追加レコードに値が必要であること、値がない場合には追加が失敗することを指定します。作成ルールでは、必須属性のデフォルト値を指定できます。レコードに属性値がない場合、そのエントリにはデフォルト値が使用されます。レコードに属性値がある場合は、そのレコード値が使用されます。
- **一致属性** 追加レコードに特定の属性が必要であり、特定の値に一致すること、そうでない場合には追加が失敗することを指定します。
- **テンプレート** eDirectory内のテンプレートオブジェクトの識別名を指定します。現時点では、NetIQインポート/エクスポート変換ユーティリティの作成ルールにテンプレートを指定することはできません。

作成ルールの正式なDTD定義を次に示します。

```
<!ELEMENT create-rules (create-rule)*>

<!ELEMENT create-rule (match-attr*,
                       required-attr*,
                       template?) >
<!ATTLIST create-rule
          class-name    CDATA   #IMPLIED
          description   CDATA   #IMPLIED>

<!ELEMENT match-attr    (value)+ >
<!ATTLIST match-attr
          attr-name      CDATA    #REQUIRED>

<!ELEMENT required-attr (value)*>
<!ATTLIST required-attr
          attr-name     CDATA   #REQUIRED>

<!ELEMENT template EMPTY>
<!ATTLIST template
          template-dn   CDATA   #REQUIRED>
```

複数の作成ルールをファイルに定義できます。各ルールは、ファイルに定義されている順番で処理されます。ルールに適合しないレコードがあると、そのレコードはスキップされますが、レコードのスキップによるエラーは生成されません。

作成ルールの形式例を次に示します。

作成ルール1: 次に紹介するルールでは、inetOrgPersonクラスの追加レコードに次の3つの条件が適用されます。追加レコードには、givenName属性およびSurname属性が必要です。追加レコードにはL属性が必要ですが、この属性値がない場合には、作成ルールによってデフォルト値「Provo」に設定されます。

```
<create-rules>
   <create-rule class-name="inetOrgPerson">
      <required-attr attr-name="givenName"/>
      <required-attr attr-name="surname"/>
      <required-attr attr-name="L">
         <value>Provo</value>
      </required-attr>
   </create-rule>
</create-rules>
```

作成ルール2: 次に紹介する作成ルールでは、ベースクラスの種類に関係なく、すべての追加レコードに次の3つの条件が適用されます。

- 追加レコードには、givenName属性が必要です。この属性が含まれていない場合、追加は失敗します。
- 追加レコードには、Surname属性が必要です。この属性が含まれていない場合、追加は失敗します。
- 追加レコードには、L属性が必要です。この属性が含まれていない場合、L属性はデフォルト値「Provo」に設定されます。

```
<create-rules>
   <create-rule>
      <required-attr attr-name="givenName"/>
      <required-attr attr-name="Surname"/>
      <required-attr attr-name="L">
         <value>Provo</value>
      </required-attr>
   </create-rule>
</create-rules>
```

作成ルール3: 次に紹介する作成ルールでは、ベースクラスの種類に関係なく、すべての追加レコードに次の2つの条件が適用されます。

- 作成ルールは、レコードにuid属性としてratuidが指定されているかチェックします。この属性が含まれていない場合、追加は失敗します。
- 作成ルールは、レコードにL属性が指定されているかチェックします。この属性がない場合、L属性はデフォルト値「Provo」に設定されます。

```
<create-rules>
   <create-rule>
      <match-attr attr-name="uid">
         <value>cn=ratuid</value>
      </match-attr>
      <required-attr attr-name="L">
         <value>Provo</value>
      </required-attr>
   </create-rule>
</create-rules>
```

コマンド例: 作成ルールをcrl.xmlファイルに保存し、次のコマンドを指定することにより、1entry.ldfファイルの処理中にそのルールを使用すること、および結果をターゲットファイルoutt1.ldfに送ることがインポート/エクスポート変換ユーティリティに指示されます。

```
ice -o -cfile://cr1.xml -SLDIF -f1entry.ldf -c -DLDIF
-foutt1.ldf
```

配置ルール

配置ルールによって、ターゲットディレクトリ内でエントリが作成される位置が決まります。配置ルールでは、次の3つの条件を使用して、エントリの配置にそのルールを適用すべきかどうかを決定します。

- **クラス一致:** 配置ルールにmatch classエレメントが定義されている場合、レコードに定義されているobjectClassは、ルールのclass-name属性に一致する必要があります。一致しない場合、そのレコードには配置ルールが使用されません。
- **属性一致:** 配置ルールにmatch attributeエレメントが定義されている場合、レコードでは、match attributeエレメントに定義されている各属性について属性値が必要です。一致しない場合、そのレコードには配置ルールが使用されません。
- **パス一致:** 配置ルールにmatch pathエレメントが定義されている場合、レコードのdn部分は、match pathエレメントに定義されているプリフィックスに一致する必要があります。一致しない場合、そのレコードには配置ルールが使用されません。

ルールの最後のエレメントによって、エントリの配置場所が決まります。配置ルールでは、必要に応じて次のオプションを指定できます。

- **解析済み文字データ** 解析済み文字データを使用して、エントリに使用するコンテナのDNを指定します。
- **名前をコピー** 古いDNのネーミング属性を、エントリの新しいDNで使用することを指定します。
- **属性をコピー** エントリの新しいDNで使用するネーミング属性を指定します。指定されたネーミング属性は、エントリのベースクラスのネーミング属性として有効でなければなりません。
- **パスをコピー** ソースDNをターゲットDNとして使用することを指定します。
- **パスサフィックスをコピー** ソースDNのパスの一部をターゲットDNとして使用することを指定します。match-pathエレメントを指定した場合、古いDNのパスの一部、つまり、match-pathエレメントのプリフィックス属性に一致しない部分だけが、エントリのDNの一部として使用されます。

配置ルールの正式なDTD定義を次に示します。

```
<!ELEMENT placement-rules (placement-rule*)>
<!ATTLIST placement-rules
          src-dn-format    (%dn-format;)   "slash"
          dest-dn-format   (%dn-format;)   "slash"
          src-dn-delims    CDATA           #IMPLIED
          dest-dn-delims   CDATA           #IMPLIED>

<!ELEMENT placement-rule (match-class*,
                          match-path*,
                          match-attr*,
                          placement)>
<!ATTLIST placement-rule
          description      CDATA            #IMPLIED>

<!ELEMENT match-class      EMPTY>
<!ATTLIST match-class
          class-name       CDATA            #REQUIRED>

<!ELEMENT match-path       EMPTY>
<!ATTLIST match-path
          prefix           CDATA            #REQUIRED>

<!ELEMENT match-attr       (value)+ >
<!ATTLIST match-attr
          attr-name        CDATA            #REQUIRED>

<!ELEMENT placement        (#PCDATA |
                            copy-name |
                            copy-attr |
                            copy-path |
                            copy-path-suffix)* >
```

複数の配置ルールエレメントをファイルに定義できます。各ルールは、ファイルに定義されている順番で処理されます。ルールに適合しないレコードがあると、そのレコードはスキップされますが、レコードのスキップによるエラーは生成されません。

配置ルールの形式例を次に示します。scr-dn-format="ldap"属性およびdest-dn-format="ldap"属性によって、ソースDNおよびターゲットDNのネームスペースがLDAP形式として定義されます。

NetIQインポート/エクスポート変換ユーティリティがサポートするソース名およびターゲット名は、LDAP形式のみです。

配置例1: 次の配置ルールでは、レコードはベースクラスinetOrgPersonを持つ必要があります。レコードがこの条件に適合する場合、そのエントリはtestコンテナの直下に置かれ、ソースDNの最上位コンポーネントがエントリのDNの一部として使用されます。

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
    <placement-rule>
       <match-class class-name="inetOrgPerson"></match-class>
       <placement>cn=<copy-name/>,o=test</placement>
    </placement-rule>
 </placement-rules>
```

ベースクラスinetOrgPersonおよび次のDNを持つレコードがあるとします。

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
```

このレコードは、例に示したルールに従って、ターゲットディレクトリ内で次のDNを持ちます。

```
dn: cn=Kim Jones, o=test
```

配置例2: 次の配置ルールでは、レコードはsn属性を持つ必要があります。レコードがこの条件に適合する場合、そのエントリはtestコンテナの直下に置かれ、ソースDNの最上位コンポーネントがエントリのDNの一部として使用されます。

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
    <placement-rule>
       <match-attr attr-name="sn"></match-attr>
       <placement>cn=<copy-name/>,o=test</placement>
    </placement-rule>
 </placement-rules>
```

次のDNおよびsn属性を持つレコードがあるとします。

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
sn: Jones
```

このレコードは、例に示したルールに従って、ターゲットディレクトリ内で次のDNを持ちます。

```
dn: cn=Kim Jones, o=test
```

配置例3: 次の配置ルールでは、レコードはsn属性を持つ必要があります。レコードがこの条件に適合する場合、そのエントリはtestコンテナの直下に置かれ、sn属性がエントリのDNの一部として使用されます。copy-attrエレメントに指定された属性は、エントリのベースクラスのネーミング属性でなければなりません。

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
  <placement-rule>
    <match-attr attr-name="sn"></match-attr>
    <placement>cn=<copy-attr attr-name="sn"/>,o=test</placement>
  </placement-rule>
</placement-rules>
```

次のDNおよびsn属性を持つレコードがあるとします。

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
sn: Jones
```

このレコードは、例に示したルールに従って、ターゲットディレクトリ内で次のDNを持ちます。

```
dn: cn=Jones, o=test
```

配置例4: 次の配置ルールでは、レコードはsn属性を持つ必要があります。レコードがこの条件に適合する場合、ソースDNがターゲットDNとして使用されます。

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
    <placement-rule>
       <match-attr attr-name="sn"></match-attr>
       <placement><copy-path/></placement>
    </placement-rule>
 </placement-rules>
```

配置例5: 次の配置ルールでは、レコードはsn属性を持つ必要があります。レコードがこの条件に適合する場合、エントリのDN全体がtestコンテナにコピーされます。

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
    <placement-rule>
       <match-attr attr-name="sn"></match-attr>
       <placement><copy-path-suffix/>,o=test</placement>
    </placement-rule>
 </placement-rules>
```

次のDNおよびsn属性を持つレコードがあるとします。

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
sn: Jones
```

このレコードは、例に示したルールに従って、ターゲットディレクトリ内で次のDNを持ちます。

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ, o=test
```

配置例6: 次の配置ルールでは、レコードはsn属性を持つ必要があります。レコードがこの条件に適合する場合、エントリのDN全体がneworgコンテナにコピーされます。

```
<placement-rules>
 <placement-rule>
  <match-path prefix="o=engineering"/>
  <placement><copy-path-suffix/>o=neworg</placement>
 </placement-rule>
</placement-rules>
```

次に例を示します。

```
dn: cn=bob,o=engineering
```

は、次のようになります。

```
dn: cn=bob,o=neworg
```

コマンド例: 配置ルールがpr1.xmlファイルに保存されている場合、次のコマンドを指定することにより、1entry.ldfファイルの処理中にそのルールを使用すること、および結果をターゲットファイルfoutt1.ldfに送ることがインポート/エクスポート変換ユーティリティに指示されます。

```
ice -o -pfile://pr1.xml -SLDIF -f1entry.ldf -c -DLDIF
-foutt1.ldf
```

LBURP (LDAP Bulk Update/Replication Protocol)

NetIQインポート/エクスポート変換ユーティリティでは、LDAPサーバへの非同期要求の送信に、LBURPを使用します。これにより、要求は常にプロトコルで指定された順序で処理されます。複数プロセッサ間の相互関係やオペレーティングシステムのスケジューラの設定によって処理順序が変わることはありません。

LBURPにより、NetIQインポート/エクスポート変換ユーティリティは、複数の更新操作を1つの要求として送信したり、これらすべての更新操作に対する応答を1つのレスポンスとして受け取ることができます。これにより、プロトコルのネットワーク処理効率が向上します。

LBURPは次のように機能します。

1. NetIQインポート/エクスポート変換ユーティリティがLDAPサーバにバインドします。
2. サーバからクライアントにバインドレスポンスが送られます。
3. クライアントからサーバに開始LBURP拡張要求が送られます。
4. サーバからクライアントに開始LBURP拡張レスポンスが送られます。
5. 必要に応じてクライアントからサーバにLBURP操作拡張要求が送られます。

   これらの要求は非同期で送信することもできます。要求ごとに通し番号が付けられ、同じクライアントから同じ接続を介して送信された個々の要求の順序はこの通し番号によって特定されます。各要求には、少なくとも1つのLDAP更新操作が設定されます。
6. サーバは、受け取った各LBURP操作拡張要求を通し番号に従って順番に処理し、要求ごとにLBURP操作拡張レスポンスを送信します。
7. サーバへの更新操作の送信がすべて終了すると、クライアントはサーバに終了LBURP拡張要求を送ります。
8. サーバからクライアントに終了LBURP拡張レスポンスが送られます。

LBURPプロトコルにより、NetIQインポート/エクスポート変換機能は、サーバにデータを転送するときに送信元と送信先の間のネットワーク接続の限界まで転送速度を上げることができます。ネットワーク接続が十分に高速であれば、NetIQインポート/エクスポート変換機能から要求が送られてくるのを待つ必要がないため、サーバはすべての処理時間を更新操作の処理だけに費やすことができます。

更新操作の処理効率をさらに上げるため、eDirectoryのLBURPプロセッサは、データベースへの更新操作をグループに分けて行います。LBURPの採用により、従来の同期処理の場合と比べて、LDIFのインポート処理の効率は大幅に改善されています。

LBURPはデフォルトで有効になっていますが、LDIFのインポート中に無効にすることもできます。

LDIFのインポート中にLBURPの有効/無効を切り替えるには、次を実行します。

1 NetIQ iManagerで、［**役割およびタスク**］をクリックします。

2 ［**eDirectoryの保守**］>［**インポート/エクスポート変換ウィザード**］の順にクリックします。

3 ［**ディスク上のファイルからデータをインポート**］をクリックし、［**次へ**］をクリックします。

4 ［**ファイルタイプ**］ドロップダウンリストから**LDIF**を選択し、インポートするデータが格納されているLDIFファイルの名前を指定します。

5 ［**次へ**］をクリックします。

6 データをインポートするLDAPサーバとログインのタイプ(匿名ログインまたは認証ログイン)を指定します。

7 ［詳細設定］の下の［LBURPを使用］を選択します。

8 ［次へ］をクリックし、表示される指示に従ってLDIFインポートウィザードでの残りの作業を完了します。

重要: LBURPは比較的新しいプロトコルであるため、バージョン8.5以前のeDirectoryサーバおよびeDirectory以外のサーバの大部分は、LBURPをサポートしていません。NetIQ eDirectoryインポート/エクスポートウィザードを使用してLBURPをサポートしていないサーバにLDIFファイルをインポートする場合は、LDIFのインポートが正しく行われるよう、LBURPオプションを無効にします。

コマンドラインオプションを使用して、LDIFのインポート中にLBURPの有効/無効を切り替えることができます。詳細については、182 ページの 「-B」を参照してください。

LDIFのインポートを高速化する

1つのLDIFファイルに数千または数百万のレコードがある場合は、次のことを検討してください。

- 204 ページの 「読み書き可能レプリカを持つサーバに直接インポートする」
- 204 ページの 「LBURPを使用する」
- 205 ページの 「データベースキャッシュを設定する」
- 205 ページの 「簡易パスワードを使用する」
- 206 ページの 「インデックスを使用する場合の注意」

読み書き可能レプリカを持つサーバに直接インポートする

実行が可能な場合は、LDIFファイルで示されているすべてのエントリを含む、読み書き可能レプリカを持つサーバをLDIFのインポート先に選択します。これによりネットワーク効率を大幅に高めることができます。

更新時には、インポート先サーバから他のeDirectoryサーバへのチェーン接続は行わないでください。これにより、パフォーマンスはかなり低下します。ただし、一部の更新対象エントリがLDAPを実行していないサーバ上だけに存在する場合には、LDIFファイルをインポートするためにチェーン接続が必要になることもあります。

レプリカとパーティション管理の詳細については、151ページの第6章「パーティションおよびレプリカの管理」を参照してください。

LBURPを使用する

NetIQインポート/エクスポート変換機能では、ネットワークとeDirectoryサーバの処理をできるだけ効率化するために、ウィザードとサーバの間でのデータ転送にLBURPを使用します。LDIFのインポート時にLBURPを使用することにより、LDIFのインポートにかかる時間が大幅に短縮されます。

LBURPの詳細については、203 ページの 「LBURP (LDAP Bulk Update/Replication Protocol)」を参照してください。

データベースキャッシュを設定する

eDirectoryで使用できるデータベースキャッシュの容量は、LDIFインポートの処理速度に大きく影響します。特に、サーバ上のエントリの総数が多いほど影響は大きくなります。LDIFのインポートでは、インポート実行中にはできるだけ多くのメモリをeDirectoryに割り当てると効率的です。インポートが完了してサーバの負荷が通常レベルに戻ったら、メモリの設定を元にもどすことができます。この方法は、eDirectoryサーバで実行する処理がインポートだけの場合に特に効果があります。

eDirectoryデータベースキャッシュの設定の詳細については、551ページの第19章「NetIQ eDirectoryのメンテナンス」を参照してください。

簡易パスワードを使用する

NetIQ eDirectoryでは、公開鍵と秘密鍵のペアを使用して認証を行います。これらの鍵の生成は、CPUに大きな負担のかかる処理です。eDirectory 8.7.3以降では、パスワードの格納に、NMAS (NetIQモジュラー認証サービス)の簡易パスワード機能を使用できます。簡易パスワードを使用する場合、パスワードはディレクトリ内の安全な場所に保持されますが、鍵のペアはサーバ間での認証で実際に必要になるまで生成されません。これにより、パスワード情報を持つオブジェクトをロードする速度を大幅にアップできます。

LDIFのインポート時に簡易パスワードを有効にするには、次を実行します。

1. NetIQ iManagerで、［**役割およびタスク**］をクリックします。
2. ［**eDirectoryの保守**］>［**インポート/エクスポート変換ウィザード**］の順にクリックします。
3. ［**ディスク上のファイルからデータをインポート**］をクリックし、［**次へ**］をクリックします。
4. ［**ファイルタイプ**］ドロップダウンリストから**LDIF**を選択し、インポートするデータが格納されているLDIFファイルの名前を入力します。
5. ［**次へ**］をクリックします。
6. データをインポートするLDAPサーバとログインのタイプ(匿名ログインまたは認証ログイン)を指定します。
7. ［**詳細設定**］の下の［**パスワードをNMASシンプルパスワード/ハッシュ化されたパスワードに格納**］を選択します。
8. ［**次へ**］をクリックし、表示される指示に従ってLDIFインポートウィザードでの残りの作業を完了します。

パスワードの格納に簡易パスワードを使用する場合は、eDirectoryツリーへのログインおよび従来型のファイルサービスやプリントサービスへのアクセスには、NMAS対応のNovell Clientを使用する必要があります。またサーバにはNMASがインストールされている必要があります。名前とパスワードのバインドを行うLDAPアプリケーションは、簡易パスワード機能とスムーズに連携します。

NMASの詳細については、663ページの第24章「eDirectoryの認証フレームワークについて」を参照してください。

インデックスを使用する場合の注意

不要なインデックスがあると、LDIFのインポートにかかる時間が長くなります。これは、定義されているすべてのインデックスで、設定されている属性値を持つエントリごとに追加の処理が実行されるためです。LDIFをインポートする前に、不要なインデックスがないことを確認します。インデックスを作成するときは、あらかじめデータ確認済みのプレディケート統計をロードしてインデックスが本当に必要な箇所を確認すると、不要なインデックスを減らすことができます。

インデックスの調整の詳細については、206 ページの 「インデックスマネージャ」を参照してください。

インデックスマネージャ

インデックスマネージャは、サーバオブジェクトの属性の1つで、データベースインデックスの管理に使用します。eDirectoryでは、データベースインデックスを使用することによって、クエリの処理速度が大幅に向上します。

NetIQ eDirectoryには、基本的なクエリの機能を提供する一連のインデックスが付属しています。これらデフォルトのインデックスの対象となる属性を次に示します。

CN	Aliased Object Name
dc	破損通知
名	Member (メンバー)
Surname (名字)	リファレンス
uniqueID (固有ID)	Equivalent to Me
GUID	NLS: 共通証明書
cn_SS	Revision (改訂数)
uniqueID_SS	extensionInfo
ldapAttributeList	ldapClassList

またカスタマイズされたインデックスを作成して、ユーザの環境におけるeDirectoryのパフォーマンスをさらに向上させることができます。たとえば、デフォルトでインデックス付けされていない属性を検索する新しいLDAPアプリケーションが組織に導入された場合、その属性に対するインデックスを作成すると便利です。

注: インデックスを使用することにより検索の処理速度は上がりますが、インデックスの数が増えるほど更新にかかる時間が長くなります。一般には、パフォーマンスの問題が特定のディレクトリの検索に関係すると思われる場合に、新しいインデックスを作成します。

NetIQ iManagerを使用して、インデックスを作成または削除します。インデックス名、状態、タイプ、ルール、インデックス付き属性など、インデックスのプロパティを表示したり、管理することができます。

インデックスを作成する

1 NetIQ iManagerで、［**役割およびタスク**］をクリックします。

2 ［**eDirectoryの保守**］>［**インデックス管理**］の順にクリックします。

3 利用可能なサーバのリストからサーバを選択します。

4 ［インデックスの変更］ページで［**作成**］をクリックします。

5 インデックス名を入力します。

インデックス名を入力しなかった場合は、選択した属性が自動的にインデックス名として設定されます。

重要: 「$」文字は属性値の区切り記号として使用されます。インデックス名に「$」文字を使用する場合、前に円記号(\)を付けて、LDAPでインデックスを作成するときに「$」文字をエスケープします。

---

6 属性を選択します。

7 インデックスのルールを選択します。

- **値** 属性の値全体または値の最初の部分を照合します。たとえば、値一致は、「Jensen」に一致する「LastName」のあるエントリの検索や、「Jen」で始まる「LastName」があるエントリの検索に使用できます。
- **存在** 特定の属性値ではなく、属性の存在のみを検索します。Login Script属性を持つエントリをすべて検索するクエリは、存在インデックスを使用します。
- **部分文字列** 属性値文字列のサブセットを照合します。たとえば、「der」という値を含む「LastName」を検索するクエリを実行すると、「Derington」、「Anderson」、および「Lauder」が照合の結果として返されます。

  下位文字列インデックスは、作成や維持を行うときに最も多くのリソースが消費されるインデックスです。

8 ［**OK**］をクリックすると、インデックステーブルが更新されます。

9 ［**適用**］をクリックすると、リンバがバックグラウンドプロセスとして再起動され、変更内容が有効になります。

インデックスを削除する

作成したインデックスが不要になる場合があります。必要のない、ユーザ定義または自動で作成したインデックスは、削除できます。

1 NetIQ iManagerで、［**役割およびタスク**］をクリックします。

2 ［**eDirectoryの保守**］>［**インデックス管理**］の順にクリックします。

3 利用可能なサーバのリストからサーバを選択します。

4 ［インデックスの変更］ページで、削除するユーザインデックスまたは自動追加インデックスを選択します。

5 ［**削除**］をクリックすると、インデックステーブルが更新されます。

6 ［**適用**］をクリックすると、リンバがバックグラウンドプロセスとして再起動され、変更内容が有効になります。

インデックスをオフラインにする

一時的にインデックスをオフラインにすることで、処理のピーク時にパフォーマンスを調整できます。たとえば、ユーザ定義のインデックスの使用をすべて中断すると、バルクロードを高速化できます。オブジェクトを追加または変更するときは定義されているインデックスを更新する必要があり、すべてのインデックスをアクティブにするとデータのバルクロードの速度が遅くなるためです。バルクロードが完了すると、再びインデックスをオンラインにできます。

1. NetIQ iManagerで、［**役割およびタスク**］をクリックします。
2. ［**eDirectoryの保守**］>［**インデックス管理**］の順にクリックします。
3. 利用可能なサーバのリストからサーバを選択します。
4. ［インデックスの変更］ページで、オフラインにするインデックスを選択して、［**状態の変更**］をクリックします。

   表示されているテーブルでは、インデックスの状態が［オンライン］から［オフライン］に変わります。インデックスは、次のいずれかの状態になります。

   - **オンライン** : 現在実行中.
   - **オフライン** :［一時停止中］. インデックスを再開するには、［**Bring Online**］をクリックします。
   - **New (新規)** :［オンライン］状態になるのを待機中.
   - **削除済み** : インデックステーブルから削除されるのを待機中.
5. **適用**をクリックします。

他のサーバ上でインデックスを管理する

あるサーバで便利に使用されているインデックスがあり、このインデックスを他のサーバでも使用する場合は、他のサーバにインデックス定義をコピーできます。またプレディケートデータを調べると、これとは逆のケースが発生する場合もあります。つまり、複数のサーバで使用されていたインデックスが、そのいずれかのサーバで不要になるといったケースです。このような場合、インデックスが不要になったサーバからインデックスを削除できます。

インデックスマネージャを使用すると、他のインスタンスに影響を与えずに、インデックスの1つのインスタンスを処理できます。

1. NetIQ iManagerで、［**役割およびタスク**］をクリックします。
2. ［**eDirectoryの保守**］>［**インデックス管理**］の順にクリックします。
3. 利用可能なサーバのリストからサーバを選択します。
4. 同じツリーの別のサーバにインデックス定義をコピーするには、［**インデックス位置の変更**］をクリックします。
5. コピーするインデックス定義を選択します。

   インデックスを1つ選択すると、そのインデックスを提供するツリー内のサーバが一覧表示されます。
6. このカラムを使用して、インデックスのコピーを目的のサーバに移動します。
7. **適用**をクリックします。

eDirectory Service Manager

eDirectory Service Managerでは、使用可能なeDirectoryサービスおよびそのステータスについての情報が提供されます。また、Service Managerからこれらのサービスを開始または停止できます。

Service ManagerはeDirectoryサービスのみを管理します。dsservcfg.xml設定ファイルを使用して管理を行います。このファイルには、各プラットフォームで管理できるサービスを表示します。リストにサービスを追加または削除することもできます。

eDirectory Service Managerには次の方法でアクセスできます。

- 209 ページの 「クライアントのサービスマネージャeMToolを使用する」
- 210 ページの 「NetIQ iManagerでサービスマネージャプラグインを使用する」

クライアントのサービスマネージャeMToolを使用する

eMBox(eDirectory Management Toolbox)クライアントはコマンドラインで実行されるJavaクライアントで、eDirectory Service Manager eMToolにリモートアクセスできます。emboxclient.jarファイルは、eDirectoryの一部としてサーバにインストールされます。JVMをインストールしていれば、どのコンピュータでも実行できます。クライアントの詳細については、584 ページの 「コマンドラインクライアントの使用」を参照してください。

クライアントのサービスマネージャeMToolを使用するには、次の操作を行います。

1 コマンドラインで次のように入力して、対話式モードでクライアントを実行します。

```
java -cp path_to_the_file/emboxclient.jar  -i
```

(クラスパスにemboxclient.jarファイルがすでに含まれている場合は、単に「java -i」と入力します。)

クライアントのプロンプトが次のように表示されます。

```
Client>
```

2 Service Managerを実行するサーバにログインするには、次のコマンドを入力します。

```
login -s server_name_or_IP_address -p port_number
-u username.context -w password -n
```

ポート番号は通常80または8028です。ただし、すでにそのポートを使用しているWebサーバが存在する場合は異なります。-nオプションを使用すると、非セキュア接続が開始されます。

クライアントにログインが成功したかどうかが表示されます。

3 次のいずれかのService Managerコマンドを入力します。

コマンド	説明
service.serviceList	利用できるeDirectoryサービスを表示します。
service.serviceStart -n *Module_name*	指定されたeDirectoryサービスを開始します。
service.serviceStop -n *Module_name*	指定されたeDirectoryサービスを停止します。
service.serviceInfo -n *Module_name*	指定されたサービスに関する情報を表示します。

クライアントでlist -t serviceコマンドを使用して、Service Managerオプションの詳細を表示することもできます。詳細については、588 ページの 「eMToolとそのサービスを表示する」を参照してください。

4 クライアントからログアウトするには、次のコマンドを入力します。

```
logout
```

5 クライアントを終了するには、次のコマンドを入力します。

```
exit
```

NetIQ iManagerでサービスマネージャプラグインを使用する

1 NetIQ iManagerで、［**役割およびタスク**］をクリックします。

2 ［**eDirectoryの保守**］>［**サービスマネージャ**］の順にクリックします。

3 管理するサーバを指定し、［**OK**］をクリックします。

4 選択したサーバの認証を行い、［**OK**］をクリックします。

5 eDirectoryサービスの状態をチェックしたり、サービスを開始または停止するには、次のアイコンを使用します。

アイコン	説明
	サービスは実行中です。
	サービスは停止しています。
	サービスを開始します。
	サービスを停止します。
	サービスは実行中ですが、停止できません。

オフラインのバルクロードユーティリティ

ldif2dibユーティリティでは、eDirectoryサーバがオフラインになったときに、LDIFファイルからNetIQ eDirectoryデータベース(DIB)へのデータのバルクロードを実行できます。eDirectoryは、LinuxとWindowsの両方のプラットフォーム上でこのユーティリティをサポートします。これはオフラインユーティリティであり、他のオンラインツールより高速でバルクロードを実行できます。このユーティリティは、LDIFファイルからDIBにエントリをインポートするときに、既存のディレクトリを使用し、データベースを新規作成しません。

LDIFファイルのエントリを大規模なユーザデータベースに取り込む必要があるときには、ldif2dib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制御チェックなどのオーバーヘッド処理を伴うため、ldif2dibより処理が遅くなります。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。

eDirectoryのパフォーマンスの改善

eDirectoryには、バルクロードのパフォーマンスを向上するための新しいオプションが追加されました。NetIQインポート/エクスポート変換(ICE)ユーティリティを使用したバルクロードのパフォーマンスを向上するために調整できるパラメータは、以下のとおりです。

- 211 ページの 「eDirectoryキャッシュの設定」
- 211 ページの 「LBURPトランザクションサイズの設定」
- 212 ページの 「ICEの非同期要求の数を増やす」
- 213 ページの 「LDAP書き込みスレッド数の増加」
- 213 ページの 「ICEのスキーマ検証を無効にする」
- 213 ページの 「バックリンカ」
- 213 ページの 「ACLテンプレートを無効にする」
- 215 ページの 「インラインキャッシュを有効/無効にする」
- 215 ページの 「LBURPのタイムアウト周期を拡大する」

各オペレーティングシステムの調整可能パラメータも参照してください。

eDirectoryキャッシュの設定

バルクロードのパフォーマンスを最適にするには、eDirectoryキャッシュの割り当てで、ブロックキャッシュにより高い割り当て率を設定します。詳細については、『NetIQ eDirectoryチューニングガイド』の「eDirectoryサブシステムのチューニング」を参照してください。

LBURPトランザクションサイズの設定

LBURPトランザクションサイズによって、1つのトランザクションにおいてICEからLDAPサーバに送信されるレコード数が設定されます。十分なメモリがあり、この値を大きくしてもI/O競合が発生しない場合、この値を大きくすることでバルクロードのパフォーマンスを向上できます。デフォルトのLBURPトランザクションサイズは25です。この値はLDIFファイルが少ない(操作数が100,000より少ない)場合には適切ですが、レコード数が多い場合には不適切です。LBURPトランザクションサイズは、1～350の範囲で設定できます。

トランザクションサイズの変更

トランザクションサイズを変更するには、/etc/opt/novell/eDirectory/conf/nds.confファイルでn4u.ldap.lburp.transizeパラメータの値を変更します。理想的なシナリオでは、トランザクションサイズが大きいほど、パフォーマンスはより高くなります。ただし、次の理由のため、トランザクションサイズには必要以上に大きな値を設定しないようにします。

- トランザクションサイズが大きいほど、サーバはトランザクションを処理するためにより多くのメモリを割り当てる必要があります。システムが少ないメモリで稼働している場合、スワッピングのために処理が遅くなることがあります。
- LDIFファイルにエラーがなく、eDirectoryにある既存のエントリがコメント化されていることが必要です。トランザクションに1つでもエラーがあると(追加しようとしたオブジェクトがすでにディレクトリに存在するという場合も含めて)、eDirectoryはLBURPトランザクション設定を無視し、操作ごとにコミットを実行してデータの整合性を確認します。

  詳細については、『NetIQ eDirectoryトラブルシューティングガイド』の「LDIFファイルのデバッグ」を参照してください。
- LBURPの最適化は、リーフオブジェクトに対してのみ有効です。トランザクションにコンテナオブジェクトとそのサブオーディネートオブジェクトが含まれている場合、eDirectoryはこれをエラーと見なします。これを回避するには、最初に別のLDIFファイルを使用してコンテナオブジェクトをロードするか、前方向参照の使用を有効にします。

  詳細については、『NetIQ eDirectoryトラブルシューティングガイド』の「前方向参照を有効化する」を参照してください。

ICEの非同期要求の数を増やす

この数値は、LDAPサーバから返される結果を待たずに、ICEクライアントからLDAPサーバに非同期に送信できるエントリの数を示します。非同期要求の数は、10～200の範囲内で設定できます。デフォルト値は「100」です。最小値(10)よりも小さい値はデフォルトに戻されます。小さなLDIFファイルには最小値が適切です。理想的なシナリオでは、ウィンドウサイズが大きいほど、パフォーマンスはより高くなります。ただし、ウィンドウサイズが大きくなるほど、クライアントがLDIFファイルのエントリを処理するために割り当てるメモリの量が多くなるため、ウィンドウサイズを必要以上に大きく設定しないでください。システムが少ないメモリで稼働している場合、スワッピングのために処理が遅くなることがあります。ICE内の非同期要求の数を変更するには、ICEコマンドラインオプションまたはiManagerを使用します。

ICEコマンドラインオプションを使用する場合

非同期要求の数は、ICEコマンドラインオプション–Zを使って指定できます。これは、LDAPターゲットハンドラの一部として使用できます。

ICEクライアントによって送信される非同期要求の数を50に設定するには、次のコマンドを入力します。

```
ice -SLDIF -f LDIF_file -a -c -DLDAP -d cn_of_admin -Z50 -w password
```

iManagerのICEウィザードを使用する場合

ICEクライアントによって送信される非同期要求の数をiManagerで設定する方法は次のとおりです。

1. ［**役割およびタスク**］をクリックします。
2. ［**eDirectoryの保守**］>［**インポート/エクスポート変換ウィザード**］の順にクリックします。

3 「データをファイルからインポートする」と「LDAPサーバ間でデータを移行する」の両方のタスクで、LDAPターゲットハンドラ画面で［LBURPウィンドウサイズ］フィールドに値を入力します。

4 ［次へ］をクリックします。

詳細については、ウィザードのヘルプを参照してください。

LDAP書き込みスレッド数の増加

LDAPサーバで複数の書込みスレッドを使えるようになりました。同時処理によって発生するエラーを避けるために前方参照を有効にするには、次のようにICEコマンドラインオプション–Fを使用します。

```
ice -SLDIF -f LDIF_file -a -c -DLDAP -d cn_of_admin -w password  -F
```

ICEのスキーマ検証を無効にする

ICEクライアントのスキーマ検証を無効にするには、次のようにICEコマンドラインオプション–Cと–nを使用します。

```
ice -C -n -SLDIF -f LDIF_file -a -c -DLDAP -d cn_of_admin -w password
```

バックリンカ

バックリンカは、特に参照整合性をチェックするバックグラウンドプロセスであり、eDirectoryサーバが起動してから50分後に実行されます。その後は13時間後に実行されます。バルクロードの処理中にバックリンカが実行されないように注意してください。ロードされるオブジェクトの数やオブジェクトがロードされる回数によっては、バックリンカが実行されると、バルクロードの処理速度が低下することがあります。

ACLテンプレートを無効にする

バルクロードのパフォーマンスを向上させるために、ACL(アクセス制御リスト)テンプレートを無効にすることができます。これによりいくつかのACLが見つからなくなりますが、必要なACLをLDIFファイルに追加するか、それらのACLを後から適用することで、この問題は解決できます。

1 次のコマンドを実行します。

```
ldapsearch -D cn_of_admin -w password -b cn=schema -s base
objectclasses=inetorgperson
```

このコマンドの出力は次のようになります。

```
dn: cn=schema
objectClasses: ( 2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson' SUP
 organizationalPerson STRUCTURAL MAY ( groupMembership $ ndsHomeDirectory
 $ loginAllowedTi meMap $ loginDisabled $ loginExpirationTime $
 loginGraceLimit $ loginGraceRem aining $ loginIntruderAddress $
 loginIntruderAttempts $ loginIntruderResetTim e $
 loginMaximumSimultaneous $ loginScript $ loginTime $
 networkAddressRestri ction $ networkAddress $ passwordsUsed $
 passwordAllowChange $ passwordExpirationInterval $
 passwordExpirationTime $passwordMinimumLength $ passwordRequired $
 passwordUniqueRequired $ printJobConfiguration $ privateKey $ Profile $
 publicKey $ securityEquals $ accountBalance $ allowUnlimitedCredit $
 minimum AccountBalance $ messageServer $ Language $ UID $
 lockedByIntruder $ serverHolds $ lastLoginTime $ typeCreatorMap $
 higherPrivileges $ printerControl $ securityFlags $ profileMembership $
 Timezone $ sASServiceDN $ sASSecretStore $ sASSecretStoreKey $
 sASSecretStoreData $ sASPKIStoreKeys $ userCertificate
 $nDSPKIUserCertificateInfo $ nDSPKIKeystore $ rADIUSActiveConnections $
 rADIUS AttributeLists $ rADIUSConcurrentLimit $ rADIUSConnectionHistory
 $ rADIUSDefa ultProfile $ rADIUSDialAccessGroup $ rADIUSEnableDialAccess
 $ rADIUSPassword $ rADIUSServiceList $ audio $ businessCategory $
 carLicense $ departmentNumbe r $ employeeNumber $ employeeType $
 givenName $ homePhone $ homePostalAddress  $ initials $ jpegPhoto $
 labeledUri $ mail $ manager $ mobile $ pager $ ldap Photo $
 preferredLanguage $ roomNumber $ secretary $ uid $ userSMIMECertifica te
 $ x500UniqueIdentifier $ displayName $ userPKCS12 ) X-NDS_NAME 'User' X
-NDS_NOT_CONTAINER '1' X-NDS_NONREMOVABLE '1' X-NDS_ACL_TEMPLATES (
'2#subtree#[Self]#[All Attributes Rights]' '6#entry#[Self]#loginScript'
'1#subtree#[Root Template]#[Entry Rights]' '2#entry#[Public]#messageServer'
'2#entry#[Root Template]#groupMembership'
'6#entry#[Self]#printJobConfiguration' '2#entry#[Root
Template]#networkAddress') )
```

2 この出力から、太字で示されている情報を削除します。

3 変更を加えた出力をLDIFファイルとして保存します。

4 新しく保存したLDIFファイルに次の情報を追加します。

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: ( 2.16.840.1.113730.3.2.2 )-add:objectclasses
```

これにより、新しいLDIFは次のようになります。

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: ( 2.16.840.1.113730.3.2.2)
-
add:objectclasses
objectClasses: ( 2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson' SUP
 organization alPerson STRUCTURAL MAY ( groupMembership $ ndsHomeDirectory
 $ loginAllowedTimeMap $ loginDisabled $ loginExpirationTime $
 loginGraceLimit $ loginGraceRem aining $ loginIntruderAddress $
 loginIntruderAttempts $ loginIntruderResetTime $
 loginMaximumSimultaneous $ loginScript $ loginTime $
 networkAddressRestri ction $ networkAddress $ passwordsUsed $
 passwordAllowChange $ passwordExpirationInterval $
 passwordExpirationTime $ passwordMinimumLength $ passwordRequired
```

```
$passwordUniqueRequired $ printJobConfiguration $ privateKey $ Profile $
publicKey $ securityEquals $ accountBalance $ allowUnlimitedCredit $
minimum AccountBalance $ messageServer $ Language $ UID $
lockedByIntruder $ serverHolds $ lastLoginTime $ typeCreatorMap $
higherPrivileges $ printerControl $ securityFlags $ profileMembership $
Timezone $ sASServiceDN $ sASSecretStore $ sASSecretStoreKey $
sASSecretStoreData $ sASPKIStoreKeys $ userCertificate $
nDSPKIUserCertificateInfo $ nDSPKIKeystore $ rADIUSActiveConnections $
rADIUSAttributeLists $ rADIUSConcurrentLimit $ rADIUSConnectionHistory $
rADIUSDefa ultProfile $ rADIUSDialAccessGroup $ rADIUSEnableDialAccess
$rADIUSPassword $ rADIUSServiceList $ audio $ businessCategory $
carLicense
$ departmentNumbe r $ employeeNumber $ employeeType $ givenName $
homePhone $ homePostalAddress  $ initials $ jpegPhoto $ labeledUri $ mail
$ manager $ mobile $ pager $ ldap Photo $ preferredLanguage $ roomNumber
$ secretary $ uid $ userSMIMECertifica te $ x500UniqueIdentifier $
displayName $ userPKCS12 ) X-NDS_NAME 'User' X-ND S_NOT_CONTAINER '1' X
-NDS_NONREMOVABLE '1')
```

5 次のコマンドを入力します。

```
ldapmodify -D cn_of_admin -w password -f LDIF_file_name
```

ACLでの作業の詳細については、『NetIQ eDirectoryチューニングガイド』を参照してください。

インラインキャッシュを有効/無効にする

サーバのインラインキャッシュ変更を有効または無効にできます。インラインキャッシュ変更は、アウトバウンド同期が無効になっている場合のみ、無効にできます。［アウトバウンド同期］を有効にすると、［インラインキャッシュ変更］も有効になります。［インラインキャッシュ変更］を無効にすると、このレプリカの変更キャッシュに無効のマークが付けられ、**［エージェント環境設定］>［パーティション］**で無効のフラグが付けられます。インラインキャッシュ変更を有効にすると、変更キャッシュの再構築時に、無効な変更キャッシュのフラグが削除されます。

LBURPのタイムアウト周期を拡大する

デフォルトでは、クライアントのタイムアウト周期は20分(1200秒)です。ただし、バルクロードの処理の際、LBURPトランザクションサイズが250であり、非常に大きな値を持つ多数の属性が対象であり、しかも、サーバで同時LBURP処理が有効になっている場合、サーバはICEクライアントによって送信されるデータを処理するために使用中になり、クライアントへの応答は規定の時間内に行われません。この場合、ICEクライアントはタイムアウトになります。

このため、タイムアウト周期を拡大することをお勧めします。拡大するには、より大きい値(秒単位)を指定して環境変数LBURP_TIMEOUTをエクスポートします。たとえば、1200秒を指定してLBURP_TIMEOUT変数をエクスポートするには、「export LBURP_TIMEOUT=1200」と入力します。

バルクロードにldif2dibを使用する

コマンドラインインタフェースで、インポートするデータが含まれているLDIFファイルと、データをインポートする必要のあるデータベースファイルのパスを指定できます。ldif2dibを使用してデータのバルクロードを実行するには、次の操作を行います。

1 DIBのバックアップを作成します。

バックアップと復元のプロセスの詳細については、439ページの第15章「NetIQ eDirectoryのバックアップと復元」を参照してください。

2 eDirectoryサーバを停止します。

3 LDIFファイルからのバルクロードを開始するには、コマンドプロンプトで次のコマンドを入力します。

```
ldif2dib <LDIF File Name> [Options]
```

各要素の内容は次のとおりです。

- **LDIF File Name:** バルクロードを実行するLDIFファイルの名前を指定します。
- **Options:** これらはオプションです。このユーティリティを調整するために使用できる各種パラメータを指定します。ldif2dibユーティリティでサポートされるオプションは以下のとおりです。

たとえば、バッチモード、キャッシュサイズ、およびブロックキャッシュパーセンテージオプションを指定するためのオプションを設定するには、次のコマンドを入力します。

```
ldif2dib 1MillionUsers.ldif -b/novell/log/logfile.txt -c314572800 -p90
```

ヒント: バルクロード処理を一時的に停止するには、sキーまたはSキーを押します。バルクロード処理を停止するには、エスケープ(Esc)キーを使用します。

複数のインスタンス

ldif2dibを使用して、LDIFファイルからeDirectory (DIB)の特定のインスタンスへのエントリのバルクロードを実行するには、-nオプションでnds.dbファイルの場所を指定します。-nオプションでnds.dbファイルの場所を指定しなかったときに、システムでeDirectoryのインスタンスが1つだけ構成されている場合は、ldif2dibがそのデータベースファイルの場所を自動的に検出します。ただし、インスタンスが複数ある場合は、ldif2dibを実行するとメニューが表示されて構成済みのすべてのインスタンスがリストされ、バルクロードを実行するインスタンスを選択できます。

eDirectoryの複数のインスタンスの詳細については、『NetIQ eDirectoryインストールガイド』の「ndsconfigの使用によるeDirectory 9.2の複数インスタンスの設定」を参照してください。

ldif2dibを調整する

このセクションでは、ldif2dibを調整するために使用できるパラメータについて説明します。

- 217 ページの 「キャッシュを調整する」
- 217 ページの 「トランザクションサイズ」
- 217 ページの 「索引」
- 217 ページの 「ブロックキャッシュの比率」
- 217 ページの 「チェックポイント間隔」

キャッシュを調整する

データベースキャッシュの設定は、eDirectoryのパフォーマンスに影響する重要な設定の1つです。設定値が小さすぎると、より頻繁にディスクから情報を取得する必要があるため、eDirectoryの処理が低速になります。設定値が大きすぎると、他のプロセスの実行に十分なメモリを使用できないため、システム全体が低速になります。キャッシュの詳細については、『NetIQ eDirectoryチューニングガイド』の「FLAIMキャッシュ設定の変更」を参照してください。

キャッシュサイズを大きくすると、一般的に、バルクロードのパフォーマンスは向上します。ただし、キャッシュサイズを、LDIFファイルサイズの3.8倍を超える値に設定しても、パフォーマンスはそれ以上向上しません。

トランザクションサイズ

トランザクションサイズとは、チャンクサイズをトランザクションごとのオブジェクト数で定義したものです。トランザクションサイズが大きい場合は少数の大規模チャンクが結果を書き込み、サイズが小さい場合は多数の小規模チャンクが結果を書き込みます。

トランザクションサイズが大きくなると、バルクロードのパフォーマンスが向上します。トランザクションサイズがゼロの場合は特別なケースで、トランザクションごとのオブジェクト数が無制限になります。トランザクションサイズがゼロの場合は、バルクロードの終了時にコミットが実行されるため、パフォーマンスが高くなります。ただし、LDIFファイルが非常に大規模である場合(オブジェクト数が100万個以上の場合)は、トランザクションサイズを0に設定することはお勧めしません。LDIFファイルが非常に大規模である場合は、トランザクションサイズを最大で4000程に設定できます。

索引

インデックスを使用すると、検索のパフォーマンスは向上しますが、オブジェクトをDIBにロードするたびにインデックスを更新する必要があるため、バルクロードが低速になります。これは、下位文字列インデックスの場合は特に顕著です。そのため、多数のオブジェクトのバルクロードを実行するときには、インデックスを一時停止すると、バルクロードが高速化します。eDirectoryサーバが起動すると、インデックスが自動的に再開されます。-xオプションを使用すると、インデックスを無効にしてからldif2dibを使用してエントリをロードします。

ブロックキャッシュの比率

属性の下位文字列インデックスが有効になっている場合は、ブロックキャッシュの比率を50%に設定することをお勧めします。属性の下位文字列インデックスが無効になっている場合は、ブロックキャッシュの比率を90%に設定できます。

チェックポイント間隔

チェックポイント間隔は、チェックポイントバックグラウンドスレッドが開始されるまでデータベースが待機する時間です。このスレッドが開始されると、オンディスクバージョンのデータベースとインメモリ(キャッシュに保存された)データベースの整合性が保たれます。このチェックポイントスレッドは、ダーティキャッシュをディスクにフラッシュし、その後ロールフォワードログをクリーンアップします。チェックポイントスレッドの実行中にはバルクロードは一時的に停止するため、チェックポイント間隔の値を大きくして、バルクロードを高速にすることをお勧めします。

制限

このセクションでは、ldif2dibユーティリティの制限について説明します。

スキーマ

- LDIFファイルには、エントリが属するすべてのオブジェクトクラスを記述する必要があります。エントリは、継承のために複数のオブジェクトクラスに属すことができます。たとえば、inetOrgPersonタイプのエントリの構文は、LDIFファイルでは次のようになります。

  ```
  objectclass: inetorgperson
  objectclass: organizationalPerson
  objectclass: person
  objectclass: top
  ```

- 現在、以下の構文はサポートされていません。

ACLテンプレート

オブジェクトクラスのACLテンプレートで指定されているACLは、ldif2dibを使用してバルクロードされたオブジェクトには自動的には追加されません。

オプション

Linux上で-bオプションを使用すると、バルクロードの完了後に、統計を表示する画面が表示されなくなります。ただし参照用に、最終統計がログファイルに書き込まれます。

簡易パスワードLDIF

Windowsでは、簡易パスワードを持つLDIFをアップロードするときに、SystemおよびAdministratorフォルダに格納されているNICIキーが同期されていない場合は、ldif2dibが失敗することがあります。この問題に対処するには、次のように、nici/systemフォルダに存在するキーにアクセスします

1. C:\Windows\system32\novell\nici\フォルダに移動します。
2. **Administrator**フォルダに存在するファイルをバックアップします。
3. 次の手順に従って、systemフォルダとそのファイルにアクセスします。
   - **3a** Systemフォルダの［プロパティ］ウィンドウにある［セキュリティ］タブに移動します。
   - **3b** ［**詳細オプション**］を選択し、［**所有者**］タブに移動します。
   - **3c** **Administrator**を選択します。

3d ［セキュリティ］タブに戻り、一覧にAdministratorを追加します。

同じ手順を繰り返し、Systemフォルダに存在するすべてのファイルに対して読み取りアクセスを許可します。

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

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

6 Systemフォルダおよびフォルダ内のファイルに対するAdministratorのアクセス権を元に戻します。

カスタムクラス

ldif2dibを使用して、コンテナオブジェクトが多数含まれているLDIFのバルクロードを実行すると、メモリ内で構築が行われ、結果的に-150エラーが報告されます。

フィルタ済みレプリカ

eDirectoryは、フィルタ適用後のレプリカのバルクロードをサポートしません。

注意事項

以下のシナリオでは、ldif2dibの動作は未定義です。

- 219 ページの 「エントリが重複している」
- 219 ページの 「スキーマチェックが実行されない」
- 219 ページの 「ハードドライブ上のスペースが不足している」
- 220 ページの 「強制終了」
- 220 ページの 「端末のサイズを変更する」

エントリが重複している

重複するエントリまたはDIBにすでに存在するエントリを含むLDIFを、-uオプションを指定せずにアップロードすると、エントリが複数回追加され、DIBの一貫性が失われます。そのため、バルクロードを実行する前に、LDIF内でエントリが繰り返されているかどうか、またはDIBにすでに存在しているかどうかを把握できていない場合は、バルクロード処理中に-uオプションを使用します。

スキーマチェックが実行されない

ldif2dibはスキーマチェックを実行しません。結果として、属性がオブジェクトのスキーマに属していなくても、オブジェクトに属性を追加できます。これにより、DIBの一貫性が失われます。ldif2dibは、スキーマチェックを実行する必要のないLDIFデータに対してのみ使用してください。

ハードドライブ上のスペースが不足している

ハードドライブ上に十分なスペースがないためにすべてのオブジェクトをロードできない場合のldif2dibの動作は未定義です。バルクロード処理を開始する前に、すべてのオブジェクトをロードできるだけの十分なスペースがあることを確認する必要があります。

強制終了

ldif2dibプロセスを強制終了すると、DIBの一貫性が失われます。バルクロード処理を正常終了するには、<Esc>キーを使用します。

端末のサイズを変更する

バルクロード処理中に端末のサイズを変更すると、ユーザインタフェースに表示される統計が乱れる可能性があります。バルクロードの進行中は、端末のサイズ変更を避ける必要があります。

LDIFファイル

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

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

- 220 ページの 「LDIFについて」
- 228 ページの 「LDIFファイルのデバッグ」
- 233 ページの 「LDIFを使用してスキーマを拡張する」
- 237 ページの 「ldif2dibの制限」

LDIFについて

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

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

LDIFファイル形式

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

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

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

LDIF内容レコード

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

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

このLDIFファイルは、次の部分から構成されています。

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

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

LDIF変更レコード

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

LDIF変更レコードでは、LDIF内容レコードと同じ形式の識別名指定子、属性値指定子、およびレコード区切り記号を使用します。(詳細については、221 ページの 「LDIF内容レコード」を参照してください。)LDIF内容レコードとの違いは、LDIF変更レコードにはchangetypeフィールドがあることです。changetypeフィールドは、変更レコードが指定する操作を識別します。

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

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

「追加」変更タイプ

追加変更レコードは、内容変更レコード(「221 ページの 「LDIF内容レコード」」を参照)に、changetype: addフィールドを属性値フィールドの直前に追加したものと同じです。

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

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

「削除」変更タイプ

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

次に、「223ページの「「追加」変更タイプ」」のLDIFファイルで作成した4つのエントリを削除するLDIFファイルの例を示します。

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

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

「変更」変更タイプ

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

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

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

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

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

次のLDIFファイルの例では、複数の変更を組み合わせて指定しています。

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

「DN変更」変更タイプ

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

フィールド	説明
newrdn (必須)	このレコードの処理の実行中にエントリに割り当てられる新しい名前を指定します。新規RDN(newrdn)指定子は、次の2つのどちらかの形式をとる必要があります。 ◆ newrdn: *safe_UTF-8_relative_distinguished_name* ◆ newrdn:: *Base64_encoded_relative_ distinguished_name* 新規RDN指定子は、「DN変更」変更タイプが指定されたすべてのLDIFレコードで指定されている必要があります。
deleteoldrdn (必須)	旧RDN削除(deleteoldrdn)指定子は、古いRDNをnewrdn(新規RDN)に置き換えるか、残しておくかを指定するフラグです。これは、次の2つのどちらかの形式をとります。 ◆ deleteoldrdn: 0 リネーム後も古いRDNの値をエントリ内に残しておくことを指定します。 ◆ deleteoldrdn: 1 エントリのリネーム後に古いRDNの値を削除することを指定します。
newsuperior (オプション)	新規スーペリア(newsuperior)指定子は、このDN変更レコードの処理時にエントリに割り当てる新しいペアレントの名前を指定します。新規スーペリア指定子は、次の2つのどちらかの形式をとります。 ◆ newsuperior: *safe_UTF-8_distinguished_name* ◆ newsuperior:: *Base64_encoded_distinguished_ name* 新規スーペリア指定子は、「DN変更」変更タイプが指定されたLDIFレコードでオプションとして使用できます。これは、エントリのペアレントを変更する場合のみ指定します。

次の「DN変更」変更タイプの例で、エントリの名前を変更する方法を示します。

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

次の「DN変更」変更タイプの例で、エントリを移動する方法を示します。

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

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

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

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

LDIFファイル内での行の折り返し

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

マルチバイトのUTF-8文字の途中では、行を折り返さないでください。

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

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

LDIFファイル内でのハッシュ化パスワードの表記

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

例1

SHAハッシュ化パスワードの場合:

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

例2

SSHAハッシュ化パスワードの場合:

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

例3

Digest MD5ハッシュ化パスワードの場合:

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

LDIFファイルのデバッグ

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

LDIFファイルで問題が発生した場合、次のことを考慮してください。

前方参照を有効化する

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

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

LDIFのインポートが完了した後でも、1つ以上の前方参照が残っている場合があります(たとえば、LDIFファイルでエントリのペアレントが作成されなかった場合など)。この場合、前方向参照はiManagerで不明オブジェクトとして表示されます。前方参照エントリを検索することはできます

が、前方参照エントリには属性も属性値もないため、objectClass以外の属性を読み込むことはできません。ただし、前方参照の下に位置する実オブジェクトエントリ上では、すべてのLDAP操作が正常に機能します。

前方参照エントリを識別する

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

前方参照エントリを通常オブジェクトへ変更する

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

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

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

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

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

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

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

1 NetIQ iManagerで、［**役割およびタスク**］をクリックします。

2 ［**eDirectoryの保守**］>［**インポート/エクスポート変換ウィザード**］の順にクリックします。

3 ［**サーバ間でデータを移行**］>［**次へ**］の順にクリックします。

4 移行するエントリが格納されているLDAPサーバを指定します。

5 次の表の説明を参照して、適切なオプションを追加します。

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

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

7 ［**次へ**］をクリックします。

8 移行するエントリの検索条件を次のように指定します。

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

9 ［**次へ**］をクリックします。

10 データを移行するLDAPサーバを指定します。

11 ［**次へ**］をクリックし、［**終了**］をクリックします。

注: スキーマが各LDAPサービスで整合性を保っていることを確認します。

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

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

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

LDIFファイルの構文をチェックする

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

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

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

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

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

9. ［**次へ**］をクリックし、［**終了**］をクリックします。

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

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

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

LDIFエラーファイルを使用する

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

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

1. NetIQ iManagerで、［**役割およびタスク**］をクリックします。
2. ［**eDirectoryの保守**］>［**インポート/エクスポート変換ウィザード**］の順にクリックします。
3. ［**ディスク上のファイルからデータをインポート**］をクリックし、［**次へ**］をクリックします。
4. ［詳細設定］で、［**失敗したレコードをログに記録**］オプションを選択し、［**次へ**］をクリックします。
5. インポートするファイルのタイプに［**LDIF**］を指定します。
6. インポートするデータが含まれているファイルの名前を指定し、適切なオプションを指定してから［**次へ**］をクリックします。
7. データのインポート先になるLDAPサーバを指定します。
8. 前の表で説明されているように、適切なオプションを追加します。
9. ［**次へ**］をクリックします。ice.logファイルが作成され、そのファイルに出力メッセージ(エラーメッセージを含む)が記録され、失敗したエントリがLDIFフォーマットで出力されます。
10. **完了**をクリックします。

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

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

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

LDAP SDKデバッギングフラグを使用する

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

値	説明
0x0001	LDAPファンクションコールをトレースします。
0x0002	パケットに関する情報を出力します。
0x0004	引数に関する情報を出力します。
0x0008	接続情報を出力します。
0x0010	BERのエンコーディングおよびデコーディング情報を出力します。
0x0020	検索フィルタ情報を出力します。
0x0040	設定情報を出力します。
0x0080	ACL情報を出力します。
0x0100	統計情報を出力します。
0x0200	追加の統計情報を出力します。
0x0400	シェル情報を出力します。
0x0800	解析情報を出力します。
0xFFFF (10進数では、-1)	すべてのデバッギングオプションを有効にします。

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

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

LDIFを使用してスキーマを拡張する

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

新しいオブジェクトクラスを追加する

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

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

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

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

必須属性

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

オプション属性

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

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

包含ルール

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

新しい属性を追加する

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

```
NDSAttributeTypeDescription = "(" whsp
  numericoid whsp  ; AttributeType identifier
  [ "NAME" qdescrs ]  ; name used in AttributeType
  [ "DESC" qdstring ]  ; description
  [ "OBSOLETE" whsp ]
  [ "SUP" woid ]  ; derived from this other AttributeType
  [ "EQUALITY" woid]  ; Matching Rule name
  [ "ORDERING" woid]  ; Matching Rule name
  [ "SUBSTR" woid ]  ; Matching Rule name
  [ "SYNTAX" whsp noidlen whsp ] ;  Syntax OID
  [ "SINGLE-VALUE" whsp ]  ; default multi-valued
  [ "COLLECTIVE" whsp ]  ; default not collective
  [ "NO-USER-MODIFICATION" whsp ] ;  default user modifiable
  [ "USAGE" whsp AttributeUsage ] ;  default userApplications
  [ "X-NDS_PUBLIC_READ" qdstrings ]
                             ; default not public read ('0')
  [ "X-NDS_SERVER_READ" qdstrings ]
                              ; default not server read ('0')
  [ "X-NDS_NEVER_SYNC" qdstrings ]
                               ; default not never sync ('0')
  [ "X-NDS_NOT_SCHED_SYNC_IMMEDIATE" qdstrings ]
                            ;  default sched sync immediate ('0')
  [ "X-NDS_SCHED_SYNC_NEVER" qdstrings ]
                                 ;  default schedule sync ('0')
  [ "X-NDS_LOWER_BOUND" qdstrings ]
                              ;  default no lower bound('0')
                                    ;(upper is specified in SYNTAX)
  [ "X-NDS_NAME_VALUE_ACCESS" qdstrings ]
                         ; default not name value access ('0')
  [ "X-NDS_NAME" qdstrings ]  ; legacy NDS name
  whsp ")"
```

次のLDIFファイルの例では、title属性タイプをスキーマに追加します。

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

単一値と複数値

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

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

既存のオブジェクトクラスへオプション属性を追加する

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

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

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

補助クラスを追加または削除する

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

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

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

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

# now create a user named bobby
dn: cn=bobby,o=bearcave
changetype: add
cn: bobby
sn: bear
givenName: bobby
```

```
bearHair: Short
bearHair: Brown
bearHair: Curly
bearPicture:< file:///c:/tmp/alien.jpg
objectClass: top
objectClass: person
objectClass: inetOrgPerson
objectClass: bearFeatures

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

# now morph john into a bear by adding bearFeatures
dn: cn=john,o=bearcave
changetype: modify
add: objectClass
objectClass: bearFeatures
-
add: bearHair
bearHair: long
bearHair: black
#bearPicture:< file:///c:/tmp/john.jpg>
-

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

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

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

XML解析で発生する既知の問題

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

ldif2dibの制限

- 238 ページの 「簡易パスワードLDIF」
- 238 ページの 「スキーマ」

- 238 ページの 「ACLテンプレート」
- 238 ページの 「シグナルハンドラ」

簡易パスワードLDIF

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

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

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

   または

   C:\Windows\SysWOW64\novell\nici\フォルダに移動します(64ビットNICIの場合)。
2. *Administrator*フォルダのファイルをバックアップします。
3. Systemフォルダの［プロパティ］ウィンドウにある**［セキュリティ］**タブに移動します。
4. **［詳細設定］**を選択し、**［所有者］**タブに移動します。
5. **Administrator**を選択します。
6. **［セキュリティ］**タブに戻り、Administratorを一覧に追加します。
7. 手順ステップ 3～ステップ 6を繰り返し、systemフォルダ内にあるすべてのファイルに対して読み取りアクセス権を取得します。
8. *Administrator*フォルダのファイルをsystemフォルダのファイルで上書きします。
9. アップロードした後に、バックアップファイルを*Administrator*フォルダにコピーします。
10. systemフォルダおよびフォルダ内のファイルへのAdministratorのアクセス権を変更します。

スキーマ

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

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

ACLテンプレート

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

シグナルハンドラ

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

8 eDirectoryを監視する

eDirectoryには、eDirectoryツリー内にあるすべてのサーバに対して、クロスプラットフォーム対応の監視と診断を行う機能があります。この機能を使用すると、各種ツールやプロトコルハンドラから複数のインタフェースを使用して、またはWebブラウザが使えるネットワーク上で、どの場所からでもサーバを監視することができます。ndscheck、iMonitor、LDAP rootdse検索、ndsrepairなどのeDirectoryユーティリティが、監視データの収集に役立ちます。

また、eDirectoryには、eDirectoryサブシステムとバックグラウンドプロセスのリアルタイム統計情報を取得するためのLDAP検索方式があります。この方式では、eDirectoryプロセスおよび処理の状態が、cn=monitorというベースDNを持つエントリとして記録されます。eDirectory管理者は、このインタフェースを使用してeDirectoryのモジュールと操作のステータスを監視できます。eDirectoryは、LDAPプロトコル上でこの機能をサポートするため、データの監視要求を出すことができるのは、LDAPクライアントのみです。

- 239 ページの 「NetIQ iMonitorを使用する?」
- 271 ページの 「cn=monitorを使用した監視」
- 281 ページの 「DSTraceの使用」
- 289 ページの 「DSTraceメッセージ」
- 293 ページの 「iMonitorメッセージのフィルタ」
- 293 ページの 「SALメッセージのフィルタ」

NetIQ iMonitorを使用する?

NetIQ iMonitorには、eDirectoryツリー内にあるすべてのサーバに対して、クロスプラットフォームの監視と診断を行う機能があります。このユーティリティを使用すると、Webブラウザを使用できるネットワーク上の場所ならどこからでもサーバを監視できます。

またiMonitorにより、eDirectory環境に対して、パーティション、レプリカ、またはサーバベースの詳細な管理が可能になります。また、実行しているタスクの種類、タスクの開始時間、結果、および実行時間を検証できます。

iMonitorは、NetIQが従来提供していたサーバベースのeDirectoryツール(DSBrowse、DSトレース、DSDiag、およびDSRepairの診断機能など)の多くに取って代わるものであり、Webベースで使用できます。このため、iMonitorの機能は主にサーバで動作することに重点を置いています。つまりeDirectoryツリー全体ではなく、個々のeDirectoryエージェント(ディレクトリサービスで実行しているインスタンス)の状態が、iMonitorの機能に対して重要な要素となります。

iMonitorには次のような機能があります。

- eDirectoryヘルスサマリ
  - 同期情報
  - 認識されているサーバ
  - エージェントの環境設定

- eDirectoryヘルスチェック
- ハイパーリンク付きのDSトレース
- エージェントの環境設定
- エージェントアクティビティおよびVerb統計
- Reports (レポート)
- エージェント情報
- エラー情報
- オブジェクト/スキーマブラウザ
- NetIQ Identity Manager監視
- 検索
- パーティションリスト
- エージェントプロセスのステータス
- バックグラウンドプロセスのスケジュール
- DSRepair
- 接続監視

iMonitorの情報は、次の要素に基づいて表示されます。

- 確立された識別情報

  iMonitorで実行するすべての要求には、識別情報に基づくeDirectory権が適用されます。たとえば、［DSRepair］ページにアクセスするには、アクセスを行うサーバに対して、サーバの管理者またはコンソールオペレータとしてログインする必要があります。
- 監視しているeDirectoryエージェントのバージョン

  新しいバージョンのNDSおよびeDirectoryには、以前のバージョンにはない機能とオプションがあります。

iMonitorに表示された情報から、ローカルサーバの状態が一目でわかります。

この章では次のトピックについての情報を説明します。

システム要件

iMonitorを使用するには次のものが必要です。

- NetIQ eDirectory 8.7.1以降
- サポートされるWebブラウザ(Microsoft Internet Explorer、Firefoxなど)

プラットフォーム

iMonitorユーティリティは次のプラットフォームで動作します。

- Windows 2000、および2003 Server (SSLなし)
- Linux

Windowsでは、eDirectoryが実行されると、iMonitorは自動的にロードされます。Linuxで iMonitorをロードするには、ndsimonitor -lコマンドを使用します。また、/etc/opt/novell/ eDirectory/conf/ndsimon.confファイルに［ndsimonitor］を追加して、eDirectoryサーバを開始する前にiMonitorを自動的にロードすることもできます。

iMonitorユーティリティは次のWebブラウザで動作します。

- Microsoft IE 10以上
- Firefox* 40以上

監視できるeDirectoryのバージョン

iMonitorを使用して監視できるNDSおよびeDirectoryのバージョンは次のとおりです。

- Windows用のすべてのバージョンのNDSおよびeDirectory
- Linux用のすべてのバージョンのNDSおよびeDirectory

iMonitorへのアクセス

1. iMonitorの実行ファイルがeDirectoryサーバで実行されていることを確認します。
2. Webブラウザを開きます。
3. アドレス(URL)のフィールドに、次の形式で入力します。

   `http://server's_TCPIP_address:httpstack_port/nds`

   たとえば、次のように入力します。

   `http://137.65.135.150:8028/nds`

   DNS名は、iMonitor内でサーバのIP、IPXアドレス、または識別名を使用できる箇所であればどこでも使用できます。たとえば、次のようなDNSが設定されているとします。

   `http://prv-gromit.provo.novell.com/nds?server=prv-igloo.provo.novell.com`

   これは、次の設定と同等です。

   `http://prv-gromit.provo.novell.com/nds?server=IP_or_IPX address`

   または

   ```
   http://prv-gromit.provo.novell.com/nds?server=/cn=prv-
   igloo,ou=ds,ou=dev,o=novell,t=novell_inc
   ```

   eDirectory HTTPSスタックが有効であれば、HTTPSを通してiMonitorを使用できます。
4. ユーザ名、コンテキスト、パスワードを指定します。例: login cn=admin.o=novell

すべての機能にアクセスするには、完全識別名を指定して管理者としてログインするか、管理者と同等のアクセス権でログインします。

5 ［ログイン］をクリックします。

iMonitorのアーキテクチャ

- 242 ページの 「iMonitorページの構成」
- 243 ページの 「動作モード」
- 244 ページの 「すべてのページからアクセス可能なiMonitorの機能」
- 245 ページの 「環境設定ファイル」

iMonitorページの構成

iMonitorの各ページは、ナビゲータフレーム、アシスタントフレーム、データフレーム、およびレプリカフレームの4つのフレームまたはセクションに分かれています。

図 8-1 iMonitorの各フレーム

ナビゲータフレーム: ページの上部にあります。このフレームには、データの読み込み元のサーバ名、ユーザの識別情報、および他の画面(オンラインヘルプ、ログイン、サーバポータルなどのiMonitorページ)にリンクするためのアイコンが表示されます。

アシスタントフレーム: ページの左側にあります。このフレームには、ナビゲーション用の項目(他のページへのリンクなど)、データフレームでのデータの検索に使用する項目、および表示されているページでのデータの取得や解釈に使用する項目が含まれます。

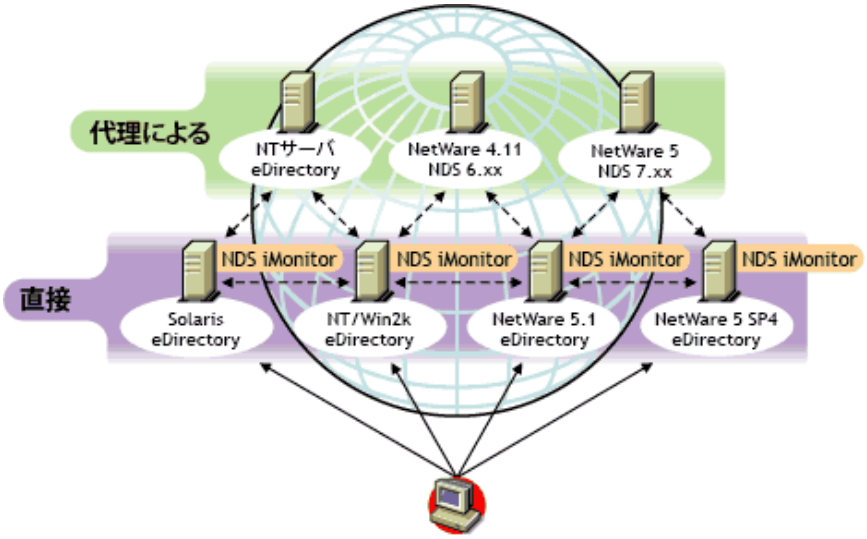
データフレーム: 上部にあるリンクをクリックすると、ローカルサーバに関する詳細情報が表示されます。Webブラウザがフレームをサポートしていない場合には、このページだけが表示されます。

レプリカフレーム: 現在表示されているレプリカを判別できます。またリンクを使用して、現在表示されている情報が、他のサーバやレプリカを基準としたときに、どのような状態になっているかを確認できます。表示したページに、要求したデータの他のレプリカが存在する場合、またはデータフレームに表示されている情報を別の状態で表示するレプリカが存在する可能性がある場合にのみ、レプリカフレームが表示されます。

動作モード

NetIQ iMonitorには、ダイレクトモードと代理人モードという2種類の動作モードがあります。モードを切り替えるために環境設定情報を変更する必要はありません。モードはNetIQ iMonitorが自動的に切り替えますが、eDirectoryツリーのナビゲートを正しく効率的に行うために、これらのモードについて理解しておくことをお勧めします。

図8-2 動作モード



ダイレクトモード: このモードが使用されるのは、WebブラウザがiMonitorの実行ファイルを実行しているマシン上のアドレスまたはDNS名を直接ポイントしていて、そのマシンのローカルeDirectory DIB上の情報だけを読み込んでいる場合です。

iMonitorの一部の機能はサーバ限定です。そのマシン上で動作しているiMonitorでのみ使用できます。サーバ限定の機能では、リモートからアクセスできないローカルAPIのセットを使用します。サーバ限定のiMonitorの機能には、DSトレース、DSRepair、および［バックグラウンドプロセスのスケジュール］ページなどがあります。ダイレクトモードの場合、すべてのiMonitor機能がローカルコンピュータから利用できます。

ダイレクトモードの主な特徴は次のとおりです。

- サーバ限定の機能をすべて使用できます。
- ネットワークの通信量が減少します(高速アクセスが可能)。
- eDirectoryのバージョンに関係なく、プロキシによるアクセスも可能です。

代理人モード: このモードが使用されるのは、Webブラウザが、あるマシンで実行されているiMonitorをポイントしていて、同時に別のマシンから情報を集めている場合です。iMonitorでは、サーバ限定でない機能に対してはサーバ限定でない従来のeDirectoryプロトコルを使用するため、NDS 6.*x*以降の従来のバージョンのeDirectoryでも監視や診断の対象にできます。ただし、サーバ限定の機能では、リモートからアクセスできないAPIが使用されます。

プロキシモードが有効なときに、他のサーバの動作モードをダイレクトモードに切り替えることもできます。ただし、そのサーバのeDirectoryのバージョンでiMonitorがサポートされていることが条件です。プロキシによる情報収集対象のサーバ上でiMonitorが実行されている場合は、ナビゲータフレームに追加のアイコンボタンが表示されます。カーソルをこのアイコン上に移動すると、そのリモートサーバ上で実行されているリモートiMonitorへのリンクが表示されます。ただし、情報収集対象のリモートサーバで以前のバージョンのeDirectoryが実行されている場合は、このアイコンは表示されません。そのリモートサーバがiMonitorをサポートしているバージョンのeDirectoryにアップグレードされるまでは、そのサーバからの情報収集には常にプロキシを使用する必要があります。

プロキシモードの主な特徴は次のとおりです。

- ツリー内のすべてのサーバでiMonitorを実行しなくても、iMonitorの機能の大部分を利用できます
- 1つのサーバをアップグレードするだけで済みます
- 1つのアクセスポイントでダイヤルインが可能です
- iMonitor自体へのアクセスには低速なリンクを使用し、iMonitorからeDirectory情報へのアクセスには高速なリンクを使用できます
- 以前のバージョンのNDSの情報にアクセスできます
- サーバ限定の機能は、iMonitorがインストールされているコンピュータ以外では使用できません

すべてのページからアクセス可能なiMonitorの機能

エージェントの要約、エージェント情報、エージェントの環境設定、トレースの環境設定、DSRepair、レポート、および検索の各ページには、ナビゲータフレームを使用することによってどのiMonitorページからでもリンクできます。その他、どのiMonitorページからでも、ログインしたり、NetIQサポートのWebページにリンクしたりできます。

ログイン/ログアウト: ログインしていない状態では、［**ログイン**］ボタンが有効になります。ログインしている間は［**ログアウト**］ボタンが表示され、ログアウトするとブラウザウィンドウが閉じます。ブラウザウィンドウがすべて閉じられるまではiMonitorセッションは開いたままになるため、再びログインする必要はありません。自分のログインステータスは、ナビゲータフレームに表示された識別情報を調べることによって、どのページからでも確認できます。

サポート接続リンク: ページ右上に表示されるNetIQのロゴは、NetIQサポート接続Webページへのリンクになっています。ここからNetIQのWebサイトに直接リンクして、最新のサーバパッチキット、更新データ、各製品に固有なサポート情報などを取得できます。

環境設定ファイル

iMonitorに含まれる環境設定ファイルを使用すると、ユーティリティのデフォルトの動作や値を変更したり、設定することができます。

環境設定ファイルはテキストファイルで、必要な値が指定された環境設定パラメータタグが含まれています。このファイルは、Windows上ではiMonitorの実行可能ファイルと同じディレクトリ(通常NetIQ eDirectoryの実行可能ファイルと同じ場所)にあり、Linux上では/etcディレクトリにあります。

- 245 ページの 「ndsimon」
- 246 ページの 「ndsimonhealth」

ndsimon

ndsimonの環境設定ファイルでは、トレースファイルの設定の変更、サーバへのアクセス制御、コンテナのリスト表示または検索結果を表示する際のオブジェクトの最大表示数の設定、およびアイドル状態が何分続くと接続がログアウトするかを指定できます。

サーバ	設定ファイル
Windows	*install directory*\novell\NDS\ndsimon.ini
Linux	/etc/opt/novell/eDirectory/conf/ndsimon.conf

ndsimonの環境設定ファイルに設定するパラメータには、次のような2種類のグループがあります。

- iMonitorの実行可能ファイル自体の実行方法に適用されるパラメータ

  iMonitorの実行可能ファイルはロードされると、従来のHTTPポート80でリスンしようとします。このポートが使用中の場合、待機するポートを8028に切り替えます。ポート8008が使用中の場合は、iMonitorはさらにポートを切り替え、番号を2ずつ増やしながら(8010、8012など)8078に達するまで使用可能なポート番号を検索します。

  SSLが設定され使用可能になっている場合も、同様のパターンでバインドが実行されます。この場合、最初にポート81がバインドされ、次に8009、8011、8013と続きます。

  これにより、iMonitorと、同じサーバで実行しているWebサーバとの共存が可能になります。プラットフォームによっては、インストールされたWebサーバをロードする前にiMonitorをロードできます。また、iMonitorをバインドするポートを選択することもできます。通常のポートおよびSSLポートは、HttpPortパラメータおよびHttpsPortパラメータをそれぞれに使用して設定できます。
- 特定の機能またはページに適用されるパラメータ

  iMonitorに付属する環境設定ファイルには、変更可能なパラメータのサンプルが含まれています。これらのパラメータの先頭にはシャープ記号(#)が付いています。これは、パラメータがコメントアウトされていることを示していて、iMonitorが環境設定ファイルを解析するときには、これらのパラメータは無視されます。付属する環境設定ファイルでは、これらのパラメータにはすべて、内部でバインドされたデフォルト値が使用されます。これらのパラメータを使用可能にする、またはパラメータを追加するには、行の先頭の「#」を削除します。

ndsimonhealth

ndsimonhealthの環境設定ファイルでは、［エージェントヘルス］ページのデフォルト設定を変更できます。［エージェントヘルス］オプションを有効または無効にしたり、オプションのレポートレベルおよび範囲を設定したり、サーバのレポートレベルを設定できます。

サーバ	設定ファイル
Windows	*install directory*\novell\NDS\ndsimonhealth.ini
Linux	/etc/opt/novell/eDirectory/conf/ndsimonhealth.conf

ndsimonhealthの環境設定ファイルに設定するオプションには、次のような3種類のオプションがあります。

- オプションのみを有効または無効にする

  オプションを無効にするには、オプションの前のシャープ記号(#)を削除し、コロン(:)の後ろにリスト表示されるすべてのレベルを「OFF」に置き換えます。これらのオプションのレポートレベルを設定するには、オプションの前の「#」文字を削除し、コロンの後ろにレポートレベルを追加します。有効なレベルは、WARN、MARGINAL、およびSUSPECTです。これらのオプションに入力できるレポートレベルは1つだけです。

- 設定の範囲を指定する一般オプション

  これらのオプションでは、レポートレベルの設定を有効または無効にしたり、レポートレベルを設定したりできます。またレポートレベルの範囲の設定もできます。

  これらのすべてのオプションのレポートレベルを設定するには、オプション名の後に-activeと記述し、その後ろに設定するレポートレベルを記述します。たとえば、time_deltaをアクティブに設定するには、環境設定ファイルに次の行を追加します。

  ```
  time_delta-active: WARN
  ```

  time_deltaを非アクティブに設定するには、環境設定ファイルに次の行を追加します。

  ```
  time_delta-active: OFF
  ```

  範囲を入力する場合、指定する範囲はこのレポートレベルを表示しない範囲です。

  3つすべてのレポートレベルをアクティブにするオプションの設定方法、および範囲の設定方法については、次のtime_deltaの例を参照してください。この例では、-2〜2の範囲外では少なくともmarginalのレベルが表示され、-5〜5の範囲外では少なくともsuspectのレベルが表示され、-10〜10の範囲外ではwarningのレベルが表示されます。

  ```
  time_delta-active: WARN | SUSPECT | MARGINAL
  time_delta-Min_Warn:      -10
  time_delta-Min_Suspect:    -5
  time_delta-Min_Marginal:   -2
  time_delta-Max_Marginal:    2
  time_delta-Max_Suspect:     5
  time_delta-Max_Warn:        10
  ```

  これらのオプションのヘルプを表示するには、iMonitorで次のURLを入力します。

  ```
  http://XXX.XXX.XXX.XXX:PORT/nds/help?hbase=/nds/health/OPTION_NAME
  ```

  XXX.XXX.XXX.XXX:*PORT*にはiMonitorがアクセスできるIPアドレスとポート、*OPTION_NAME*にはヘルプ表示するオプション名(time_deltaなど)を入力します。

現在の設定レベルと範囲を表示するには、ブラウザを使用して表示するオプションを含むヘルスページへ進み、ブラウザのURL行の最後に次を追加します。

```
&op=setup
```

- カスタム設定または複合設定が必要なオプション

  設定できるレポートレベルには次の3種類があります。

  - WARNは、すぐにアップグレードする必要があるバージョンのeDirectoryを実行しているサーバを検出します。
  - SUSPECTは、アップグレードが望まれるバージョンのeDirectoryを実行しているサーバを検出します。
  - MARGINALは、最新バージョンではないeDirectoryを実行しているサーバを検出します。

  これらのオプションは、サーバのバージョンが指定された許容範囲にあるかどうかのレポートレベルを設定します。

iMonitorの機能

このセクションではiMonitorの機能について簡単に説明します。

iMonitorが持つ各機能の詳細については、オンラインヘルプの該当するセクションを参照してください。

- 248 ページの 「eDirectoryサーバのヘルス情報の表示」
- 248 ページの 「パーティション同期ステータスの表示」
- 249 ページの 「破損通知プロセスステータスおよびキャッシュの変更回数を表示する」
- 250 ページの 「サーバ接続情報の表示」
- 251 ページの 「認識されているサーバの表示」
- 251 ページの 「レプリカ情報の表示」
- 252 ページの 「DSエージェントを制御および環境設定する」
- 253 ページの 「トレースを環境設定する」
- 254 ページの 「プロセスステータス情報の表示」
- 254 ページの 「エージェントアクティビティの表示」
- 255 ページの 「トラフィックパターンの表示」
- 255 ページの 「バックグラウンドプロセスの表示」
- 255 ページの 「バックグラウンドプロセスの設定」
- 256 ページの 「eDirectoryサーバエラーの表示」
- 256 ページの 「DSRepair情報の表示」
- 257 ページの 「エージェントのヘルス情報を表示する」
- 257 ページの 「ツリー内のオブジェクトの参照」
- 257 ページの 「同期またはパージのためのエントリの表示」
- 258 ページの 「NetIQ Identity Managerの詳細の表示」
- 258 ページの 「レプリカの同期ステータスの表示」
- 258 ページの 「レポートの設定と表示」

- 260 ページの 「スキーマ、クラス、および属性定義の表示」
- 261 ページの 「オブジェクトの検索」
- 261 ページの 「ストリームビューアの使用」
- 262 ページの 「DIBセットのクローン」

eDirectoryサーバのヘルス情報の表示

［エージェントの要約］ページでは、同期設定、エージェントプロセスのステータス、データベースで認識されているサーバの総数など、eDirectoryサーバのヘルス情報を表示できます。

1 iMonitorで、［**エージェントの概要**］  をクリックします。

2 次のオプションから選択します。

［**エージェント同期の概要**］では、レプリカの数とタイプ、およびこれらレプリカが正常に同期されてから経過した時間を表示できます。その他、レプリカのタイプ別にエラーの数を表示することもできます。表示できるレプリカまたはパーティションが1つだけの場合、見出しは「**パーティション同期ステータス**」になります。

［エージェント同期の概要］が表示されない場合、ユーザの識別情報に基づいて見れるレプリカがないということです。

［**データベースで認識されているサーバ合計**］では、ローカルデータベースが認識しているサーバのタイプと数、および各サーバが実行中であるかどうかを表示できます。

［**エージェントプロセスステータス合計**］では、エージェント上で実行されているプロセスのステータスを、管理者に依頼せずに自分で調べることができます。ステータス情報は問題や重要な情報が発生したときに記録されます。表示される表のサイズは、記録されているステータスの数によって異なります。

パーティション同期ステータスの表示

［エージェント同期］ページでは、パーティションの同期状態を表示できます。ページの左側のアシスタントフレームに一覧表示されているオプションから選択して、表示する情報を絞り込むこともできます。

1 iMonitorで、アシスタントフレームの［**エージェント同期**］をクリックします。

2 次のオプションから選択します。

［**パーティション同期ステータス**］では、パーティション、エラーの数、最終同期時刻、最大リングデルタを表示できます。

［**パーティション**］では、各パーティションの［レプリカ同期］ページへのリンクを表示できます。

［**最終同期日時**］では、サーバから個々のパーティションのレプリカをすべて同期できたときから経過した時間を表示できます。

［**最大リングデルタ**］では、リング内にあるすべてのレプリカに対して同期できない可能性があるデータ量を表示します。たとえば、ユーザが自分のログインスクリプトを変更してから30分が経過していない場合、最大リングデルタへの割り当てが45分であれば、このユーザのログインは正常に同期されないおそれがあります。その場合、このユーザがログインしようと

すると以前のログインスクリプトを受け取ることになります。ユーザが45分以上前にログインスクリプトを変更している場合は、このユーザはすべてのレプリカから常に新しいログインスクリプトを受け取ることになります。

［**最大リングデルタ**］に［**不明**］が表示されている場合は、遷移同期ベクトルに不整合があり、レプリカ/パーティション操作が実行中などの理由で最大リングデルタを計算できないことを意味します。

破損通知プロセスステータスおよびキャッシュの変更回数を表示する

特定のパーティションの破損通知プロセスステータスおよびキャッシュの変更回数を表示するには、そのパーティションのパーティションルートオブジェクトに移動します。次の3種類の破損通知のデータが表示されます。

- OBIT_DEAD: オブジェクトが削除されるときに作成されます。
- OBIT_NEWRDN: オブジェクトの名前が変更されるときに作成されます。
- OBIT_MOVED: オブジェクトがある場所から別の場所に移されると作成されます。

オブジェクトが処理される過程で、4つの状態を経ます。オブジェクトはISSUED状態からPURGEABLE状態に移り、最終的にパージされます。4つの状態は次のとおりです。

- ISSUED
- NOTIFIED
- OK_TO_PURGE
- PURGEABLE

特定のオブジェクトに12種類の組み合わせがあります。これらの組み合わせは次のとおりです。

- OBIT_DEAD_ISSUED
- OBIT_DEAD_NOTIFIED
- OBIT_DEAD_OK_TO_PURGE
- OBIT_DEAD_PURGEABLE
- OBIT_NEWRDN_ISSUED
- OBIT_NEWRDN_NOTIFIED
- OBIT_NEWRDN_OK_TO_PURGE
- OBIT_NEWRDN_PURGEABLE
- OBIT_MOVED_ISSUED
- OBIT_MOVED_NOTIFIED
- OBIT_MOVED_OK_TO_PURGE
- OBIT_MOVED_PURGEABLE

これらの組み合わせのそれぞれに対して番号が表示されます。番号は、最後の破損通知処理サイクルが終了した時点で、その特定の状態にあるオブジェクトの合計数を示します。

変更キャッシュカウントは、現行サーバのパーティションの変更キャッシュに入っているオブジェクトの数を表します。以下の図に、そのパーティションの特定のパーティションルートオブジェクトについての破損通知カウントと変更キャッシュカウントを示します。

図8-3 破損通知および変更キャッシュカウントの情報

Obit and Change Cache Count Information	
OBIT_DEAD_ISSUED	8318
OBIT_DEAD_NOTIFIED	0
OBIT_DEAD_OK_TO_PURGE	1682
OBIT_DEAD_PURGEABLE	0
OBIT_NEWRDN_ISSUED	0
OBIT_NEWRDN_NOTIFIED	0
OBIT_NEWRDN_OK_TO_PURGE	0
OBIT_NEWRDN_PURGEABLE	0
OBIT_MOVED_ISSUED	0
OBIT_MOVED_NOTIFIED	0
OBIT_MOVED_OK_TO_PURGE	0
OBIT_MOVED_PURGEABLE	0
Obit Count from database index	10000
Change Cache Count	10002

サーバ接続情報の表示

［エージェント情報］ページでは、ローカルサーバの接続情報を表示できます。

1 iMonitorで、アシスタントフレームの［**エージェント情報**］をクリックします。

2 次のオプションから選択します。

［**Ping情報**］サーバからの通知先アドレスのセットに対して、iMonitorがIP Pingを送信したことを表示します。表示されるのは、応答があった場合です。

［**DNS名**］iMonitorがサーバによってサポートされているIPアドレスに対してアドレスの反転を試みたことを表示します。対応するDNS名が表示されます。

使用しているトランスポート、環境設定、およびプラットフォームによっては、この情報が表示されない場合もあります。

［**接続情報**］サーバの参照、タイムデルタ、一番ルート側のマスタレプリカ、およびレプリカ深さなどのサーバの情報を表示できます。

使用しているトランスポート、環境設定、およびプラットフォームによっては、この情報が表示されない場合もあります。

［**サーバ照会**］ローカルサーバへのアクセスに使用できるアドレスを一括して表示できます。

時刻同期は、最後に発行されたレプリカのタイムスタンプが現在の時刻より遅れない限り、合成時刻や未来の時刻を使用しないことを示します。

eDirectoryは、サーバの現在時刻に基づいてタイムスタンプを発行できる程度に時刻が同期されていることを想定しています。ただし、時刻同期プロトコルが同期状態にあることは保証されていません。

［**タイムデルタ**］iMonitorとリモートサーバの時刻の差を秒単位で表示できます。負の整数はiMonitorの時刻がサーバの時刻より進んでいることを意味します。正の整数はiMonitorの時刻がサーバの時刻より遅れていることを意味します。

［最もルートに近いマスタレプリカ］が表示されている場合、最上位のレプリカつまりネーミングツリーのルートに最も近いレプリカがマスタレプリカであることを意味します。

［レプリカ深さ］最上位レプリカの深さ(最上位レプリカとツリーのルートの間のレベル数)を表示します。

認識されているサーバの表示

［認識サーバ］のリストには、ソースサーバのデータベースが認識しているすべてのサーバがリストされます。フィルタ条件を指定して、データベースで認識されているすべてのサーバまたはレプリカリング内のすべてのサーバのリストを表示できます。サーバの横にアイコンが表示された場合、そのサーバはレプリカリングのメンバーです。

1 iMonitorで、アシスタントフレームの［認識サーバ］をクリックします。

2 次のオプションから選択します。

［エントリID］ローカルサーバのオブジェクト識別子を表示します。エントリIDは、複数のサーバ間で共用することはできません。

［NDSリビジョン］通信相手のサーバにキャッシュまたは保存されているeDirectoryビルド番号またはNDSバージョンを表示します。

［ステータス］サーバのステータス(稼動中、停止中、不明)を表示します。通信相手のサーバのステータスが不明となっている場合、過去にこのサーバと通信する必要がなかったことを表します。

［最終更新時刻］該当するサーバが相手サーバと最後に通信を試みて、その相手サーバが停止中であることを検出したときの時刻を表示します。このカラムが表示されない場合は、すべてのサーバが稼働中であることを意味しています。

レプリカ情報の表示

［パーティション］ページでは、通信相手のサーバ上にあるレプリカに関する情報を表示できます。ページの左側のアシスタントフレームに一覧表示されているオプションから選択して、表示するページの情報を絞り込むことができます。

［Server Partition Information］では、該当するサーバのパーティションについての情報(エントリID、レプリカステータス、パージ時間、最終変更時刻など)を表示できます。

［パーティション］サーバのパーティションのTreeオブジェクトに関する情報を表示できます。

［パージ時間］ すべてのレプリカが削除を認識しているためにすでに削除されたデータを、データベースから削除できる時間を示します。

［最終変更時刻］このレプリカのデータベースに書き込まれたデータの、最後に発行されたタイムスタンプを表示できます。これにより、将来の時刻が設定されていないかどうか、および合成時刻が使用されていないかどうかを確認できます。

［レプリカ同期］パーティションに対応する［レプリカ同期サマリ］ページを表示できます。［レプリカ同期］ページには、パーティション同期ステータスとレプリカステータスについての情報が表示されます。また、パーティションとレプリカのリストを表示することもできます。

DSエージェントを制御および環境設定する

［エージェント環境設定］ページでは、DSエージェントの制御および環境設定ができます。このページで利用できる機能は、現在の識別情報に基づく権利および使用しているeDirectoryのバージョンによって異なります。

1 iMonitorで、［**エージェント環境設定**  をクリックします。

2 次のオプションから選択します。

- ［**エージェント情報**］ローカルサーバの接続情報を表示できます。
- ［**パーティション**］通信しているサーバ上にあるレプリカを表示できます。
- ［**レプリケーションフィルタ**］指定したeDirectoryエージェントに対して設定されたレプリケーションフィルタを表示できます。NDS eDirectory 8.5 (ビルドバージョン85.*xx*)は、「フィルタ済みレプリカ」と呼ばれる機能を初めて実装したeDirectoryバージョンです。フィルタ済みレプリカの使用と設定方法の詳細については、「65 ページの「フィルタ済みレプリカ」」を参照してください。
- ［**エージェントトリガ**］バックグラウンドプロセスを開始します。エージェントトリガは、機能的にはSET DSTRACE=**option*コマンドと同じです。
- ［**バックグラウンドプロセス処理設定**］特定のバックグラウンドプロセスを実行する時間間隔を変更します。バックグラウンドプロセスの設定は、機能的にはSETDSTRACE=!*option*コマンドと同じです。
- ［**エージェント同期**］インバウンド同期やアウトバウンド同期を無効または有効にします。同期を無効にする期間(単位は時間)を指定できます。
- ［**データベースキャッシュ**］DSデータベースエンジンが使用するデータベースキャッシュのサイズを設定します。提供されるさまざまなキャッシュ統計情報により、適切な量のキャッシュが利用可能であるかを判断できます。十分なキャッシュがないと、システムのパフォーマンスが悪化する原因となります。
- ［**ログイン設定**］では、ユーザのログイン時にeDirectoryがログイン属性を更新するかどうかを指定できます。次のオプションは、ユーザがログインする時のeDirectoryの応答方法を制御します。
  - ［**ログイン更新の遅延**］は、更新の時間間隔(秒)を指定します。例えば、1人または複数のユーザが遅延の間にログインした場合、eDirectoryはすべての変更をキューに追加します。遅延が終了すると、eDirectoryはキューにあるすべての変更を適用します。
  - ［**ログイン更新無効間隔**］は、特定のユーザのログイン属性が更新されない時間間隔(秒)を指定します。標準的な間隔は3600秒(1時間)です。例えば、ユーザが午前8時に初めてログインした場合、eDirectoryは属性を更新し、そこから間隔が開始します。ユーザが午前9時前に再びログインした場合、eDirectoryは属性を更新しません。デフォルトは0です。無効間隔は設定されていません。

トレースを環境設定する

［トレースの環境設定］ページの情報にアクセスするには、サーバの管理者と同等の権利またはコンソールオペレータの権利が必要です。このページの情報にアクセスするには、その前に、資格情報を検証できるよう、ユーザ名とパスワードを入力する必要があります。

［トレースの環境設定］ページでは、トレースを設定できます。NetIQ iMonitorのDSTraceは、サーバ限定機能です。つまり、この機能はiMonitorが動作しているサーバ以外からは起動できません。他のサーバで実行されているこの機能にアクセスするには、そのサーバで実行されているiMonitorに切り替える必要があります。

1 iMonitorで、［**トレースの環境設定**  ］をクリックします。

2 次のオプションから選択します。

- **［更新］** トレースオプションおよびトレース行プリフィックスに変更を送信できます。DSトレースがオフになっている場合は、［**オン**］をクリックしてDSトレースをオンにします。DSTraceがすでにオンになっている場合は、［**更新**］をクリックして現在のトレースに変更内容を送信します。
- **［オン］/［オフ］** DSトレースをオンまたはオフにします。ボタン上に表示される文字列は、DSトレースが現在オンかオフかによって異なります。DSTraceがオンになっている場合、ボタンには［**オフ**］というテキストが表示されます。DSトレースのオンとオフを切り替えるには、このボタンをクリックします。DSTraceがオフになっているときに［**オン**］をクリックした場合の動作は、［**更新**］をクリックした場合と同じです。
- **［トレース行プレフィックス］** このオプションを使用すると、トレース行の先頭に追加するデータを選択することができます。
- **［DSトレースオプション］** トレースを開始したローカルDSエージェント上のイベントに対して適用されます。［DSトレースオプショ］ンを使用すると、エラーと潜在的な問題、およびローカルサーバ上のeDirectoryに関する情報を表示できます。［DSトレースオプション］をオンにすると、CPUの負荷が増え、システムのパフォーマンスが低下します。このため、DSトレースオプションは診断のみに使用して、通常はオフにします。DSトレースオプションは、SETDSTRACE=+*option*コマンドと機能的には同じですが、使いやすさの点では優れています。
- **［イベント環境設定］** DSTraceで監視のために有効または無効にするeDirectoryとNMASのイベントオプションをリスト表示します。イベントシステムは、オブジェクトの追加、削除、属性値の変更など、ローカルな操作に対してイベントを生成します。個々のイベントタイプ対して、そのイベントタイプに固有の情報が含まれた構造が返されます。
- **［トレース履歴］** 以前に実行したトレースのリストを表示できます。各トレースログは、トレースデータの収集期間によって識別されます。
- **［トレーストリガ］** DSトレース内で、指定したDSエージェント情報を表示するために設定する必要があるフラグを表示できます。トレーストリガを有効にした場合、トレースに書き込まれる情報の量が多くなります。NetIQサポート部門からの指示があった場合にのみ、トレーストリガを有効にすることをお勧めします。

3 ［**オン**］をクリックしてDSTraceをオンにし、変更内容を送信します。

4  または［**トレースライブ**］をクリックして、iMonitorでDSトレースを表示します。

プロセスステータス情報の表示

［エージェントプロセスのステータス］ページでは、バックグラウンドプロセスのステータスに関するエラーと発生した各エラーの詳細情報を表示できます。ページの左側のアシスタントフレームに一覧表示されているオプションから選択して、このページに表示する情報を絞り込むことができます。

iMonitorで、アシスタントフレームの［**エージェントプロセスのステータス**］をクリックします。現在、バックグラウンドプロセスのステータスで報告される情報には、次のものが含まれます。

- スキーマの同期
- 破損通知処理
- 外部参照/DRL
- リンバ
- ［Repair］

エージェントアクティビティの表示

［エージェントアクティビティ］ページでは、トラフィックパターンや考えられるシステムボトルネックを調べることができます。このページでは、現在eDirectoryで処理されているバーブおよび要求が表示されます。また、これらのうち、データベースへの書き込みのためにDIBロックを取得しようとしている要求がどれかを特定したり、DIBロックの取得待機中の要求数を調べることもできます。

NetIQ eDirectory 8.6以降のバージョンを実行しているサーバを表示すると、パーティションのリスト、およびナビゲータフレームで指定したサーバが含まれるレプリカリングに参加しているサーバも表示されます。NetIQ eDirectory 8.6を導入すると、同期処理はシングルスレッドではなくなります。eDirectory 8.6以降のバージョンのサーバは、1つ以上のレプリケーションパートナーに複数のパーティションを同時に発信する可能性があります。このため、このような並行同期処理の監視がさらに容易になるよう、［同期アクティビティ］ページが作成されています。

1. iMonitorで、アシスタントフレームの［**エージェントアクティビティ**］をクリックします。
2. 次のオプションから選択します。
   - ［**Verb Activity and Statistics(バーブアクティビティおよび統計情報)**］eDirectoryの最後の初期化以降に呼び出されたバーブの総数や発行された要求の数をリアルタイムで表示できます。また、現在アクティブになっている要求の数と、これらの要求を処理するための最小、最大、および平均時間(ミリ秒単位)も表示されます。
   - ［**SynchronizationCurrentandSchedule(現在同期およびスケジュール)**］インバウンド同期およびアウトバウンド同期が発生したさまざまな時刻のリストを表示します。インバウンド同期またはアウトバウンド同期が現在実行中の場合、プロセスが実行中であること、そのサイクルが開始された時刻、およびそのプロセスを実行しているサーバを示すアイコンも表示されます。

     インバウンド同期およびアウトバウンド同期が無効になっている場合は、現在同期が無効であることおよび再び有効になる予定の時刻を示すアイコンが表示されます。アウトバウンド同期では、次に再び有効になる予定時刻も表示されます。
   - **イベント**現在アクティブな状態にあるイベント、イベントハンドラの統計情報、イベント統計情報の概要、および呼び出された現在のイベント権利機能のリストを表示できます。
   - ［**バックグラウンド処理スケジュール**］スケジュールされているバックグラウンド処理、その現在の状態、および再実行のスケジュールを表示できます。

トラフィックパターンの表示

［Verb統計］ページでは、トラフィックパターンや考えられるシステムボトルネックを調べることができます。このページでは、eDirectoryの最後に初期化されてから呼び出されたバーブの総数や発行された要求の数がリアルタイムで表示されます。その他、これら要求のうち現在アクティブなものの数や、これら要求の処理にかかる時間の最大値、平均値、最小値(それぞれミリ秒単位)も表示できます。バックグラウンドプロセス、バインダリ、および標準eDirectory要求が追跡されます。

このページを以前のバージョンのeDirectoryで表示すると、eDirectory 8.5以降で表示する場合より情報量が少なくなります。

バックグラウンドプロセスの表示

［バックグラウンド処理スケジュール］ページでは、スケジュールされているバックグラウンドプロセスを、現在の状態と次回の実行予定時刻とともに表示できます。NetIQ iMonitorのバックグラウンド処理スケジュールは、サーバ中心の機能です。つまり、この機能はiMonitorが動作しているサーバ以外からは表示できません。他のサーバで実行されているバックグラウンド処理スケジュール機能にアクセスするには、そのサーバで実行されているiMonitorに切り替える必要があります。eDirectory 8.5以降のバージョンにアップグレードしたサーバの数が増えれば、iMonitorのサーバ中心の機能がさらに使えるようになります。その他のサーバ限定機能には、［DSトレース］ページおよび［DSRepair］ページなどがあります。

［バックグラウンド処理スケジュール］ページの情報にアクセスするには、サーバの管理者と同等の権利またはコンソールオペレータの権利が必要です。このページの情報にアクセスするには、資格情報の確認のためにログインする必要があります。

バックグラウンドプロセスの設定

管理者はiMonitorの［バックグラウンドプロセスの設定］ウィンドウで次のいずれかのバックグラウンドプロセス遅延設定ポリシーを設定することで、バックグラウンドプロセスサイクルの実行時間を短縮することができます。

- CPU
- ハードメモリ制限
- パージャ処理遅延

バックグラウンドプロセスを設定するには、次の手順に従います。

1. iMonitorにログインします。
2. ［**エージェント環境設定**］>［**バックグラウンドプロセスの設定**］の順に選択します。
3. ［**バックグラウンドプロセス遅延設定(ミリ秒)**］セクションまでスクロールダウンし、遅延間隔を0秒から100ミリ秒までの任意の値に設定します。

   デフォルトでは、3つすべてのプロセスのスリープ時間を100秒に設定した［**ハード制限**］ポリシーが有効になっています。

   または

   ［**CPU Policy**］を選択し、必要に応じて適切に設定します。

   デフォルトでは、［最大CPU使用率］パラメータが80%に設定され、［遅延上限］が100ミリ秒に設定されています。

4 ［**パージャ間隔**］フィールドに、遅延間隔を入力します。

デフォルトでは、30分に設定されています。この値は、要件に合わせて変更できます。

eDirectoryサーバエラーの表示

［エラー索引］ページでは、eDirectoryサーバ上で検出されたエラーについての情報を表示できます。検出されたエラーは、eDirectory固有のエラー、および関連のあるその他のエラーの2つのフィールドに分けて表示されます。表示されるエラーのそれぞれに説明がハイパーリンクされていて、エラーの内容、考えられる原因、回復手段などがわかります。

1 iMonitorで、アシスタントフレームの［**エラー索引**］をクリックします。

［エラー索引］ページからは、エラーや技術情報に関してNetIQが提供している最新のドキュメントやホワイトペーパーにリンクできます。

DSRepair情報の表示

［DSRepair］ページでは、検出された問題を表示したり、DIBセットのバックアップやクリーンアップを実行できます。NetIQ iMonitorのDSRepairは、サーバ中心の機能です。つまり、この機能はiMonitorが動作しているサーバ以外からは起動できません。他のサーバで実行されているDSRepair情報にアクセスするには、そのサーバで実行されているiMonitorに切り替える必要があります。eDirectoryの新しいバージョンにアップグレードしたサーバの数が増えれば、iMonitorのサーバ中心の機能がさらに使えるようになります。この機能以外には、［DSトレース］ページや［バックグラウンド処理スケジュール］ページなどがサーバ限定の機能です。

［DSRepair］ページの情報にアクセスするには、サーバの管理者と同等の権利またはコンソールオペレータの権利が必要です。このページの情報にアクセスするには、資格情報の確認のためにログインする必要があります。

1 iMonitorで、［**DSRepair**  ］をクリックします。

2 次のオプションから選択します。

- ［**ダウンロード**］ファイルサーバから修復関連のファイルを取得できます。DSRepairユーティリティが実行中の場合や、iMonitorの［DSRepair］ページから修復を開始した場合には、操作が完了するまではdsrepair.logにアクセスできません。
- ［**古いDIBセットを削除**］では、赤い［**X**］をクリックすることで古いDIBセットを削除できます。

  警告: この操作は元に戻すことができません。このオプションを選択すると、古いDIBセットがファイルシステムからパージされます。

- ［**DSRepair拡張スイッチ**］問題の修正、問題のチェック、データベースのバックアップ作成などを実行できます。NetIQサポート部門から指示がない限り、［**サポートオプション**］フィールドに情報を入力する必要はありません。

3 ［**修復の開始**］をクリックして、サーバ上でDS Repairを実行します。

エージェントのヘルス情報を表示する

［エージェントヘルス］ページでは、指定したeDirectoryエージェントのヘルス情報およびそのエージェントに関連するパーティションおよびレプリカリングを表示できます。

1 iMonitorで、アシスタントフレームの［**エージェントヘルス**］をクリックします。

2 リンクをクリックすると、詳細な情報が表示されます。

ツリー内のオブジェクトの参照

［参照］ページでは、ユーザのツリー内にある任意のオブジェクトを参照できます。ページ最上部のナビゲーションバーには、表示中のオブジェクトが存在するサーバ、およびオブジェクトへのパスが表示されます。ページの左側にある［レプリカ］フレームでは、実パーティション上にある同じオブジェクトを表示またはアクセスできます。ページ内の下線付きオブジェクトをクリックすると、オブジェクトに関する詳しい情報が表示されます。また、ナビゲータフレーム内にある名前の任意の一部分をクリックすると、ツリーの上の階層を参照できます。

このページに表示される情報は、ログイン時のeDirectory権、参照するオブジェクトのタイプ、および実行しているNDSまたはeDirectoryのバージョンによって異なります。スーパーバイザ権でログインした場合、このページにはXRefオブジェクトが表示されます。レプリカリストを使用して、レプリカの実コピーへジャンプできます。ダイナミックグループのオブジェクトを参照している場合、ダイナミックメンバーに対してタイムスタンプは表示されません。

［レプリカ同期］このオブジェクトを含むレプリカの同期ステータスを表示します。

［エントリ同期］サーバ側から見て同期が必要である属性を表示します。

［接続情報］iMonitorがこのオブジェクトの情報をどこで取得したかが表示されます。

［エントリ情報］オブジェクトの名前、フラグ、ベースクラス、変更タイムスタンプ、および接続情報のサマリを表示します。

［すべてのレプリカにエントリを送信］このエントリの属性を他のすべてのレプリカに再送信します。オブジェクトに多数の属性値がある場合、この処理には時間がかかることがあります。この処理では、そのオブジェクトの、他のすべてのコピーが同一になるわけではありません。他のレプリカが各属性を再考慮できるようにするだけです。

［すべて送信］(参照しているオブジェクトがパーティションルートの場合および［カスタムモード］オプションが有効になっている場合のみ表示されます)。このパーティション内のすべてのエントリを、パーティションのレプリカを保持しているすべてのサーバに再送信します。この処理では、そのオブジェクトの、送信されたすべてのコピーが同一になるわけではありません。他のレプリカが各オブジェクトとその属性を再検討できるようにするだけです。

同期またはパージのためのエントリの表示

［変更キャッシュ］ページでは、同期またはパージにおいてこのサーバが検討する必要のあるエンティティのリストを表示できます。このオプションを使用できるのは、ユーザがアクセスしているサーバがeDirectory 8.6以降を実行しており、また、表示中のオブジェクトがパーティションルートである場合だけです。このページを表示するには、eDirectoryサーバに対するスーパバイザ権が必要です。

［エントリ同期］エントリが同期を必要とする理由を判別できます。

注: iMonitorの［キャッシュの変更］ページには、限られた数のオブジェクトだけが表示されます。サーバ上の特定のパーティションまたはすべてのパーティションの、変更キャッシュに入っているすべてのオブジェクトを表示するには、［レポート］ページで［変更キャッシュのダンプ］レポートを実行します。iMonitorのレポートの設定および実行方法の詳細については、258 ページの 「レポートの設定と表示」を参照してください。

NetIQ Identity Managerの詳細の表示

［DirXMLの概要］ページでは、ユーザのサーバで実行中のすべてのDirXMLドライバ、各ドライバのステータス、保留中の関連付け、およびドライバの詳細のリストを表示できます。

1 iMonitorで、［**DirXMLの概要**  ］をクリックします。

2 次のオプションから選択します。

［**ステータス**］指定したドライバの現在の状態を表示します。表示されるステータスは、［停止］、［開始します］、［稼働中］、［シャットダウン保留中］、および［スキーマ取得中］です。

［**起動オプション**］選択したドライバの現在の起動オプションを表示します。

［**保留中**］まだ作成されていない関連付けの数を表示します。

［ドライバ詳細］アイコンは、ユーザのサーバで実行中のDirXMLドライバに関する、加入者および発行者の詳細、XMLルール、フィルタ、および保留中の関連付けリストを表示します。このページには、最初の50個の保留中オブジェクトに関する詳細も表示されます。このページに表示されるXMLルールを使用すると、指定したDirXMLドライバに対するオブジェクトの作成を続行するために必要な、保留中のオブジェクト内で検索すべき情報を判断できます。

レプリカの同期ステータスの表示

［レプリカ同期］ページでは、レプリカの同期ステータスを表示できます。

1 iMonitorで、アシスタントフレームの［**エージェント同期**］をクリックします。

2 表示するパーティションの［**レプリカ同期**］をクリックします。

3 このページにあるリンク、および左側のナビゲーションバーにあるリンクを使用すると、他のパーティションにアクセスしたり、レプリカリング内でジャンプすることができます。

レポートの設定と表示

［レポート］ページでは、このサーバで直接実行されているレポートを表示および削除できます。一部のレポートでは、実行に長時間を要し、多くのリソースを消費する場合があります。

スケジュールされたレポートは、［パブリック］識別情報を使用して、ユーザ認証なしで実行されます。ユーザが実行するレポートはすべて、ユーザの権利で直接実行されます。すべてのレポートデータは、レポートを実行したサーバに保管されます。デフォルトでは、iMonitorはオペレーティングシステムに応じて次のディレクトリにレポートデータを格納します。

プラットフォーム	ディレクトリ
Windows	C:\Novell\NDS\ndsimon\dsreports\
Linux	/var/opt/novell/eDirectory/data/dsreports

［レポートの環境設定］ページでは、事前に設定されたレポート、カスタムレポート、およびスケジュール設定されたレポートのリストを表示できます。このページを使用して、レポートを変更および実行できます。また、iMonitorページ用のカスタムレポートの作成もできます。次の表に、iMonitorに含まれている事前設定のレポートを示します。

レポート	説明
サーバ情報	ツリー全体を調べて、検索可能な各NCPサーバと通信し、検知したすべてのエラーをレポートします。このレポートを使用して、時刻同期およびLimberの問題を診断できます。また、現在のサーバ自体が他のすべてのサーバと通信可能であるかどうかも知ることができます。環境設定ページで選択されている場合、このサーバはツリー内にある各サーバのNDSエージェントヘルス情報を生成することもできます。
破損通知リスティング	このサーバ上のすべての破損通知を表示します。
オブジェクト統計情報	オブジェクトを指定したスコープで調べて、要求される条件に一致したオブジェクトのリストを生成します。この条件には、将来の時刻、不明なオブジェクト、名前が変更されたオブジェクト、ベースクラス数、コンテナ、別名、外部参照などがあります。
変更キャッシュのダンプ	サーバ上の選択されたパーティションまたはすべてのパーティションの変更キャッシュにあるすべてのオブジェクトをリストします。このレポートは、サーバ間で同期する必要がある属性や値と共に、変更キャッシュにあるオブジェクトのXMLダンプも生成します。レポートには、変更キャッシュに含まれている、すべてのオブジェクトの分析に関する情報が示されます。 **注:** iMonitorが変更キャッシュダンプを格納する場所は、上記の表にリストされている実際の変更キャッシュダンプレポートを格納するディレクトリと同じです。
サービスアドバタイジング	SLPまたはSAPを使用して現在のサーバに認識されている、すべてのディレクトリとサーバを表示します。
エージェントヘルス	現在のサーバのヘルス情報を収集します。
値数	指定した値より値数が多い属性を持つオブジェクトのリストを生成します。

レポートの表示と削除

1 iMonitorで、［**レポート**］をクリックします。

2 レポートを削除するには、をクリックし、レポートを表示するには をクリックします。

レポートの実行

1 iMonitorで、［**レポート**］>［**レポート設定**］の順にクリックします。

2 をクリックしてレポートを実行します。

レポートの設定またはスケジュールを行う

1 iMonitorで、［**レポート**］>［**レポート設定**］の順にクリックします。

2 をクリックし、レポートを設定およびスケジュールします。

3 目的のオプションを選択し、［**デフォルトの保存**］をクリックして選択したオプションを保存します。

4 (オプション)レポートが定期的に、または後で実行されるように設定します。

4a レポートの頻度、開始時刻、および開始日を指定します。

4b ［**スケジュール**］をクリックします。

5 ［**レポートの実行**］をクリックしてレポートを開始します。

カスタムレポートの作成

カスタムレポートを作成すると、iMonitorの任意のページをレポートとして起動できます。

1 iMonitorで、［**レポート**］>［**レポート設定**］の順にクリックします。

2 ［**実行可能レポート**］リストで、  ［**カスタムレポート**］をクリックします。

3 レポートの名前を入力し、レポートとして起動するiMonitorページのURLを入力します。

カスタムレポートを実行する場合は、次のURLを入力します。

/nds/*required page*

4 ［**保存されるレポート**］フィールドに、保持または保存するレポートのバージョンの数を指定します。

5 (オプション)［**保存**］をクリックしてレポートを保存します。

6 (オプション)レポートが定期的に、または後で実行されるように設定します。

6a レポートの頻度、開始時刻、および開始日を指定します。

6b ［**スケジュール**］をクリックします。

7 ［**レポートの実行**］をクリックしてレポートを開始します。

スキーマ、クラス、および属性定義の表示

［スキーマ］ページでは、ユーザのスキーマ、クラス、および属性の定義を表示できます。すでに作成されている拡張や特定のスキーマに固有の情報(スキーマに行った変更や拡張など)を添付して、ツリー上にロードされているスキーマを表示できます。

1 iMonitorで、アシスタントフレームの［**スキーマ**］をクリックします。

2 次のオプションから選択します。

［**同期リスト**］このサーバと同期する相手のサーバを表示します。このオプションは、NDS eDirectory8.5以降を実行しているサーバに対してのみ使用できます。この情報を表示するには、サーバに対するスーパーバイザ権が必要です。

［**スキーマルート**］ツリーのルートに最も近いスキーマレプリカに関する情報を表示します。

各eDirectoryサーバには、エントリ内のスキーマのレプリカが保存されています。スキーマレプリカは、ディレクトリオブジェクトを格納しているパーティションから分割されて保存されます。任意のスキーマレプリカへの変更内容は、すべてのレプリカに伝えられます。スキーマの変更は、ルートパーティションの書き込み可能なレプリカを保存するサーバを通してのみ実行できます。ルートパーティションの読み込み可能なレプリカを保存しているサーバは、スキーマ情報を読み込むことはできますが、変更はできません。

属性定義各属性の名前、属性値が含まれる構文、および属性が受ける制約がリストされます。左側のナビゲーションフレームを使用すると、個々の属性をブラウズしたり、それらにアクセスしたりすることができます。

［クラス定義］各クラスの名前、ルール、および属性を表示します。左側のナビゲーションフレームを使用すると、個々の属性を参照したり、それらにアクセスすることができます。

オブジェクトの検索

［検索］ページでは、さまざまなクエリオプションおよびフィルタに基づいて、オブジェクトを検索できます。検索クエリオプションおよびフィルタは、基本フォームとカスタムフォームという2つのレベルの検索要求フォームに分けられます。基本検索要求フォームは、eDirectoryの一般ユーザ向けであり、基本的な検索に使用します。カスタム検索要求フォームは、熟練ユーザ向けであり、複雑な検索に使用します。現在はサーバレベルの検索のみがサポートされています。

4つのセクション内の検索オプションおよび検索フィルタは、すべて結合可能です。空白フィールド(相対識別名を除く)は無視されます。<Ctrl>キーを使用して、マルチリスト上でアイテムを選択解除したり、複数のアイテムを選択することができます。選択解除したマルチリストも無視されます。

1. NetIQ iMonitorで、［**検索**  をクリックします。
2. 次のオプションから選択します。
   - **［スコープオプション］**検索のスコープを指定できます。
   - **［エントリフィルタ］**エントリ情報に関連する検索クエリフィルタを指定できます。
   - **［属性と値のフィルタ］**属性および値に関連する検索クエリフィルタを指定できます。
   - **［表示オプション］**検索結果の表示形式を制御するオプションを指定できます。

   注: ［**表示オプション**］設定を使用できるのは、［**詳細**］をクリックしてすべての［高度な検索］オプションを表示している場合のみです。
3. 検索要求フォームの一番下にある［**ヘルプ**］ボタンをクリックすると、そのフォームに関連する簡潔なヘルプ情報が表示されます。

   ヘルプ情報をクリアするには、［**再ロード**］または［**リフレッシュ**］をクリックします。

ストリームビューアの使用

［ストリームビューア］ページでは、次の形式で現在のストリームを表示できます。

- プレーンテキスト
- HTML
- GIF
- JPEG
- BMP
- WAV
- 16進ダンプ
- その他

特定の形式で常に表示したいストリーム属性がある場合、［ストリームビューア］を使用してデフォルトの表示設定を選択します。

［NDSストリーム属性セットアップ］ブラウザでストリームを表示するためのデフォルトの形式を変更します。ストリームが正しく表示されるかどうかはブラウザに依存します。ブラウザによっては、ユーザが選択した設定が適用されない場合があります。

デフォルト設定に加えた変更を適用するには、ユーザがサーバに認証される必要があります。変更内容はstreams.ini (Windowsサーバの場合)またはstreams.conf (Linuxサーバの場合)に保存されます。デフォルトの設定を手動で編集することもできます。

DIBセットのクローン

このオプションでは、1つのサーバ(ソースサーバ)に保存されているeDirectoryデータベースのDIBファイルセットを完全に複製できます。DIBクローンは、ツリー内のすべてのマスタレプリカが保持されているソースサーバから複製する必要があります。クローンは別のサーバ(ターゲットサーバ)に配置することができます。ターゲットサーバがeDirectoryを開始すると、サーバはDIBファイルセットをロードし、サーバオブジェクトのマスタレプリカに接続し、名前を解決し、クローン作成後に行われたDIBファイルセットのすべての変更を同期します。

eDirectory DIBセットのクローンは、クローンを作成したサーバのオペレーティングシステムと同じオペレーティングシステムが稼働するサーバ上にだけ配置する必要があります。たとえば、DIBファイルセットのクローンをLinuxサーバに復元する場合は、Windowsサーバではなく Linuxサーバでクローンを作成します。

この機能のバックエンドはeDirectory 8.7に搭載されていましたが、eDirectory 8.7.1でiMonitor 2.4以降が稼働するようになるまでサポートされていませんでした。このオプションは、バージョンが8.7以前のNetIQ eDirectoryやNDSでは使用できません。

図 8-4 iMonitorの［DIBセットのクローン］ページ

このセクションでは、次の情報を紹介します。

- 263 ページの 「DIBセットのクローンの使用事例」
- 264 ページの 「クローンを作成する」

DIBセットのクローンの使用事例

DIBセットのクローンは次のような場合に使用します。

- すでに「オン」の状態になっているパーティションで新しいサーバを作成します。

  次の利点があります。

  - レプリカリングに新しいサーバを追加する際に、リング内のすべてのサーバが稼動中または実行中である必要がありません。
  - 新しいサーバは自動的にすべてのパーティションを保持しますが、同期する必要はありません。
  - すばやく処理できます。
- 障害回復

長所	短所
◆ パーティションを1度コピーするだけで成功します。 ◆ 複数のパーティションをもつ大きなサーバを停止させる時間が少なくてすみます。	◆ 対象のパーティションを少なくとも1度は正しくコピーする必要があります。 ◆ SSLやセキュリティバックアップに対応しません。 ◆ ファイルシステムを処理しません。

- バックアップおよび復元

長所	短所
◆ 大規模のデータベースでは特に、処理に時間がかかりません。	◆ eDirectoryのコアを追加するだけです。LDAP、SNMP、SSLなどはインストールされません。また設定も行われません。 ◆ 最新の変更は取得されません。スナップショットのみが取得されます。ロールフォワードログは実行されません。

このような欠点があるため、バックアップ処理および復元処理のためにDIBセットのクローンを使用することはお勧めできません。

クローンを作成する

DIBファイルセットのクローンは、元のサーバでオンラインまたはオフラインのいずれでも作成できます。オフラインで行う場合は、eDirectoryを停止させておく必要があります。オンラインモードで、eDirectoryは稼働状態になり、ロックされません。

- 264 ページの 「オンラインによる方法」
- 266 ページの 「オフラインによる方法」

警告: 別のサーバのクローンを作るために、識別情報管理サーバでDibcloneユーティリティを使用しないでください。これを行うと、クローンのサーバに不要なTAOファイルが生成されてしまいます。

オンラインによる方法

1 ndscloneモジュールをソースサーバにロードします。

プラットフォーム	スキーマを拡張するには、次の操作を行います。
Windows	NDSCons.exeで**dsclone.dll**を選択し、［**開始**］をクリックします。
Linux	ndsmodules.confファイルに「ndsclone」エントリを追加し、http://IP address:port/dhostページを使用してDirectory Clone Agentをロードします。 **注:** ndscloneモジュールは、ndstrace -c "load ndsclone"コマンドでロードすることもできます。

2 DIBクローンプロセスをソースサーバで開始する前に、iMonitorの［エージェント環境設定］ページで、インバウンド同期を無効にします。

3 DIBファイルセットのクローンを作成します。

3a iMonitorで、DIB環境設定のクローンを実行します。

［**エージェント環境設定**］>［**DIBセットのクローン**］>［**新しいクローンの作成**］の順にクリックします。

3b ターゲットサーバの完全修飾名と、DIBファイルのクローンが配置される場所のファイルパスを指定してから、［**クローンオブジェクトの作成**］チェックボックスと［**DIBをオンラインでクローン**］チェックボックスをオンにします。

ターゲットサーバのNCPサーバ名(クローンオブジェクト)は、ターゲットサーバの名前と一致させる必要があります。

3c **送信**をクリックします。

NDSクローンオブジェクトが作成され、DIBファイルセットが指定された配置先にコピーされます。

4 ターゲットサーバでeDirectoryのインストールと構成を行い、サーバを停止します。

5 クローンのDIBファイルセットが格納されているDIBディレクトリをターゲットサーバにコピーします。

さらに、Linuxシステムの場合は、/etc/opt/novell/eDirectory/conf/nds.confファイルをソースサーバからターゲットサーバにコピーし、ターゲットサーバへの次の参照を更新します。

- 次のパラメータに関するIPアドレスの変更
  - n4u.server.interfaces
  - http.server.interfaces
  - https.server.interfaces
- 手順3bで作成されたNCPサーバ名をn4u.nds.server-nameパラメータに指定します。
- 優先サーバ名をn4u.nds.preferred-serverパラメータに指定します。通常、ターゲットサーバのホスト名が優先サーバ名と見なされます。

6 ターゲットサーバの/var/opt/novell/nici/0と/var/opt/novell/nici/0/backupからnicisdi.keyを削除します。

7 次に、ターゲットサーバを起動し、ndsconfig upgradeコマンドを実行します。

注: Windowsでは、サイレントインストーラを使用してeDirectoryサーバをアップグレードするために、EConfig.ps1コマンドを実行する必要があります。アップグレードのときには、upgrade.niレスポンスファイルで、クローンされたDIBのツリー名、サーバ名、およびADMIN資格情報を指定しなければなりません。また、ツリーの他のサーバのIPが含まれる既存のサーバIPも指定する必要があります。詳細については、『*NetIQ eDirectoryインストールガイド*』の「WindowsでのeDirectoryの無人アップグレード」を参照してください。

---

8 ターゲットサーバオブジェクトのマスタレプリカがeDirectoryを実行していて、使用可能になっていることを確認します。ターゲットサーバ上でeDirectoryが初期化されると、eDirectoryはターゲットサーバの最終的な名前が解決できるマスタレプリカと通信を行います。

9 ターゲットサーバのレプリカ属性値が、すべてのサーバと同期されていることを確認します。すべてのサーバで属性の変更が適用されたら、ソースサーバのインバウンド同期を再び有効にします。インバウンド同期は、iMonitorの［エージェント環境設定］ページまたはDSTraceで有効にできます。

10 eDirectoryの環境設定を完了するには、267 ページの 「eDirectoryの設定を完了する」を参照してください。

オフラインによる方法

1 DIBファイルセットのクローンを作成します。

1a iMonitorで、DIB環境設定のクローンを実行します。

［**エージェント環境設定**］>［**DIBセットのクローン**］>［**新しいクローンの作成**］の順にクリックします。

1b ターゲットサーバの完全修飾名を指定し、［**クローンオブジェクトの作成**］チェックボックスをオンにして、［**DIBをオンラインでクローン**］チェックボックスをオフにします。

ターゲットサーバのNCPサーバ名は、ターゲットサーバの名前と一致させる必要があります。

1c **送信**をクリックします。

NDSクローンオブジェクトが作成されます。ソースサーバ上のDIBはロックされているため、eDirectoryがロックされているというエラーが報告されます。

2 ターゲットサーバでeDirectoryのインストールと構成を行い、サーバを停止します。

3 ソースサーバのDIBディレクトリにある*.nds、nds*、およびnds.rfl/*.*ファイルを、ターゲットサーバ上のコピー先またはメディアに手動でコピーします。セットをターゲットサーバのDIBディレクトリに移動するのに都合のよい場所にします。さらに、Linuxシステムの場合は、/etc/opt/novell/eDirectory/conf/nds.confファイルをターゲットサーバに転送し、ターゲットサーバに対する次の参照を更新します。

- 次のパラメータに関するIPアドレスの変更
  - n4u.server.interfaces
  - http.server.interfaces
  - https.server.interfaces
- 手順1bで作成されたNCPサーバ名をn4u.nds.server-nameパラメータに指定します。
- 優先サーバ名をn4u.nds.preferred-serverパラメータに指定します。通常、ターゲットサーバのホスト名が優先サーバ名と見なされます。

4 ターゲットサーバの/var/opt/novell/nici/0と/var/opt/novell/nici/0/backupからnicisdi.keyを削除します。

5 NDSD_DISABLE_INBOUND=Y環境変数をエクスポートしてから、ndsdを起動してソースサーバ上のインバウンド同期を無効にします。

6 ソースサーバ上でeDirectoryを再起動します。

ファイルがコピーされる前にソースサーバ上でeDirectoryが再起動された場合、このクローンは無効とみなされます。その場合は、新しいNCPサーバオブジェクトを削除してクローンを再作成する必要があります。

7 次に、ターゲットサーバを起動し、ndsconfig upgradeコマンドを実行します。

注: Windowsの場合、eDirectoryセットアップファイルを実行する必要があります。また、セットアップファイルを実行してeDirectoryサーバをアップグレードするときに、eDirectoryツリーを選択してログインすることも必要です。

8 ターゲットサーバのレプリカ属性値が、すべてのサーバと同期されていることを確認します。すべてのサーバで属性の変更が適用されたら、ソースサーバのインバウンド同期を再び有効にします。インバウンド同期は、iMonitorの［エージェント環境設定］ページまたはDSTraceで有効にできます。

9 DIBディレクトリにクローンのDIBファイルセットが格納されているターゲットサーバに、eDirectoryをインストールし、サーバを起動します。

新しいターゲットサーバオブジェクトのマスタレプリカがeDirectoryを実行していて、使用可能になっていることを確認します。ターゲットサーバ上でeDirectoryが初期化されると、eDirectoryはターゲットサーバの最終的な名前が解決できるマスタレプリカと通信を行います。

10 eDirectoryの環境設定を完了するには、267 ページの 「eDirectoryの設定を完了する」を参照してください。

eDirectoryの設定を完了する

- 「SIDKEY」(237ページ)
- 「SAS、LDAP、およびSNMPサービスを設定する」(237ページ)

SDIKEY

1 ターゲットサーバ上で、eDirectoryを停止します。

2 ターゲットサーバのファイルシステムで、/var/opt/novell/nici/0/nicisdi.keyファイルと/var/opt/novell/nici/0/backup/nicisdi.keyファイルを移動または名前変更します。

プラットフォーム	ディレクトリ
Windows	C:\Windows\SysWOW64\novell\nici\nicisdi.key
Linux	/var/opt/novell/nici/0/nicisdi.key
	/var/opt/novell/nici/0/backup/nicisdi.key

3 ターゲットサーバ上でeDirectoryを開始します。

SAS、LDAP、HTTP、およびSNMPサービスを設定する

Linux: コマンドラインで次のコマンドを入力することで、1つの操作でSAS、LDAP、SNMP、およびHTTPサービスを設定できます。

ndsconfig upgrade [-a admin FDN]

Windows: eDirectoryインストーラを実行し、SAS、LDAP、SNMP、およびHTTPサービスの設定を完了します。

設定の完了後、デフォルトではHTTPがポート80および443でリスンします。eDirectoryは、HTTPのポート設定をHTTPサーバオブジェクトに格納します。必要に応じて、管理者ユーザとしてポート設定を変更できます。

サービスを個別に設定する場合は、次の表を参照してください。

SAS

プラットフォーム	コマンドまたはツール
Windows	iManagerを使用してSASサービスオブジェクトおよび証明書を作成します。

LDAP

プラットフォーム	コマンドまたはツール
Windows	iManagerを使用してLDAPサーバおよびグループオブジェクトを作成します。

［SNMP］

プラットフォーム	コマンドまたはツール
Windows	rundll32 snmpinst, snmpinst **-c オブジェクトの作成 -a ユーザFDN -p パスワード -h ホスト名またはIPアドレス**

セキュリティ保護されたiMonitor操作の実現

iMonitor環境へのアクセスをセキュリティ保護するには、次の保護手順を実行します。

1. ファイアウォールを使用してVPNアクセスを準備します。これは、NetIQ iManagerおよび、アクセス制限が必要な他のすべてのWebベースのサービスの場合も同様です。
2. ファイアウォールが設置されているかどうかに関係なく、アクセスの種類を制限することによって、iMonitorはさらにDoS(Denial of Service)攻撃から保護されます。

   iMonitorはURL要求を経由して受け取るデータを十分に確認しますが、あらゆる不正な入力を拒否できるとは保証できません。無効なURLを通じたDoS攻撃の危険を減らすため、iMonitorの環境設定ファイルのLockMask: オプションを使用して3つのレベルのアクセスが制御されます。

アクセスレベル	説明
0	iMonitorのURL処理において事前の認証は不要です。この場合、［パブリック］識別子のeDirectory権利がすべての要求に適用され、iMonitorが表示する情報は［パブリック］ユーザの権利で表示できるものに限定されます。ただし、iMonitorにURLを送る際に認証が不要であるため、iMonitorは、不正なURLの送信によるDoS攻撃を受けやすくなる可能性があります。

アクセスレベル	説明
1(デフォルト)	iMonitorがURLを処理する前に、eDirectory識別子としての認証が必要です。この場合、その識別子のeDirectory権利はすべての要求に適用されるため、eDirectory権利によって制限を受けます。DoS攻撃を受ける危険性はレベル0と同様ですが、DoS攻撃は実際にサーバに認証を受けたものでないと行うことができないことが異なります。認証が正常に実行されるまでは、すべてのiMonitorのURL要求への返答は［ログイン］ダイアログボックスで行われます。したがってこの段階では、設定された正当性を持たないユーザによる攻撃を通さないようにする必要があります。
2	iMonitorがURLを処理する前に、iMonitorが認証しているサーバ上のスーパバイザに相当するeDirectory識別子としての認証が必要です。DoS攻撃を受ける危険性はレベル1と同様ですが、DoS攻撃を行うには実際にサーバのスーパバイザとして認証される必要があります。認証が正常に実行されるまでは、すべてのiMonitorのURL要求への返答は［ログイン］ダイアログボックスで行われます。したがってこの状態に設定されているときには、iMonitorは認証されていないユーザおよびスーパバイザとして認証されていないユーザからの攻撃を通さないようにする必要があります。

レベル1はデフォルトです。多くの管理者はツリー内のすべてのサーバにアクセスできるスーパバイザ権を持っていませんが、管理しているサーバと通信するサーバ上のiMonitorサービスを使用する必要が生じる可能性があるためです。

注: iMonitorにはRepair、トレースなど複数の機能があり、これらの機能にアクセスするには、LockMaskの設定に関係なくスーパバイザに相当する権利が必要です。

HTTPサーバオブジェクトの設定

eDirectoryをインストールすると、HTTPサーバオブジェクトが作成されます。このオブジェクトのディレクトリに、HTTPサーバのデフォルトの設定があります。ただし、このデフォルト設定は、NetIQ iManagerを使用して変更することができます。HTTPサーバオブジェクトとは、サーバ固有の環境設定データのことです。

HTTPサーバオブジェクトには、次の属性があります。

- **httpDefaultTLSPort:** HTTPサーバがリスンするセキュアポートを指定します。
- **httpDefaultClearPort:** HTTPサーバがリスンするクリアテキストポートを指定します。
- **httpAuthRequiresTLS:** クリアテキストポート経由の要求をセキュアポートにリダイレクトするかどうかを指定します。
- **httpTraceLevel:** DSTraceでのHTTPサーバのデバッグレベルを指定します。
- **httpKeyMaterialObject:** HTTPサーバがセキュア接続を処理するときに使用する必要がある証明書オブジェクトのDNが格納されます。SuiteBモードでiMonitorインタフェースを設定するには、httpBindRestrictionsの値をSuiteBモードに設定して目的のSuiteBモードを有効にしてから、httpKeyMaterialObjectに適切なECDSAサーバ証明書を関連付けます。デフォルトでは、httpKeyMaterialObjectはRSA証明書を使用するように設定されています。
- **httpSessionTimeout:** HTTPセッションのタイムアウトを指定します。デフォルト値は900秒です。
- **httpKeepAliveRequestTimeout:** 各HTTP要求のキープアライブタイムアウトを指定します。デフォルト値は15秒です。

- **httpRequestTimeout:** 各HTTP要求のタイムアウトを指定します。デフォルト値は300秒です。
- **httpIOBufferSize:** HTTPサーバの入力および出力バッファサイズを指定します。デフォルトは8192バイトです。
- **httpThreadsPerCPU:** CPUごとに生成するHTTPスレッドの数を指定します。デフォルト値は2スレッドです。
- **httpHostServerDN:** 関連付けられているNCPサーバオブジェクトのDNが格納されます。
- **httpBindRestrictions:** サイファの暗号化レベルを設定するために使用できます。
  - **RSA:** 次の値を使用して、サイファの使用を制限できます。
    - 0 - HIGH、MEDIUM、LOW、およびEXPORTサイファを許容
    - 1 - HIGH、MEDIUM、およびLOWサイファだけを許容
    - 2 - HIGHおよびMEDIUMサイファだけを許容
    - 3 - HIGHサイファだけを許容

    デフォルト値は3です。
  - **ECDSA 256:** 次の値を使用して、サイファの使用を制限できます。
    - 4 - 128ビットのサイファまたは256ビットのサイファを許可
  - **ECDSA 384:** 次の値を使用して、サイファの使用を制限できます。
    - 5 - 128ビットのサイファまたは256ビットのサイファを許可
    - 6 - 256ビットのサイファを許可

  ECDSA証明書の場合、eDirectoryはSuite B Cipherのみを許可します。

  SuiteBモードでLDAPおよびhttpstkインタフェースを設定するには、管理者の権利でiManagerにログインし、SuiteBモードのいずれかを有効にしてから、これらのインタフェースに適切なECDSAサーバ証明書を関連付けます。この作業は、ldapServerやhttpServerなどのサーバのLDAPおよびhttpstk環境設定オブジェクトを使用するすべてのeDirectoryサーバに対して実行する必要があります。SuiteBモードをオンにする前に、eDirectory環境内のLDAPクライアント、LDAPブラウザ、およびWebブラウザのすべてが、TLS 1.2証明書とEC証明書をサポートしていることを確認してください。

ndsconfigを使用するHTTPスタックパラメータの設定

ndsconfigを使用するHTTPスタックパラメータは次のとおりです。

- **http.server.interfaces:** HTTPサーバがリスンするクリアテキストインタフェースが格納されます。これは、ndsconfigによる新しいインスタンスの設定中に設定されます。
- **http.server.request-io-buffer-size:** HTTPサーバの入力および出力バッファサイズを指定します。デフォルト値は8192バイトです。
- **http.server.request_timeout-seconds:** 各HTTP要求のタイムアウトを指定します。デフォルト値は300秒です。
- **http.server.keep-timeout-seconds:** 各HTTP要求のキープアライブタイムアウトを指定します。デフォルト値は15秒です。
- **http.server.threads-per-processor:** CPUごとに生成するHTTPスレッドの数を指定します。デフォルト値は2スレッドです。
- **http.server.session-exp-seconds:** HTTPセッションのタイムアウトを指定します。デフォルト値は900秒です。

- **http.server.trace-level:** DSTraceでのHTTPスタックのデバッグ レベルを指定します。デフォルトレベルは2です。
- **http.server.clear-port:** HTTPサーバがリスンするクリアテキストポートを指定します。
- **http.server.tls-port:** HTTPサーバがリスンするセキュアポートを指定します。
- **http.server.auth-req-tls:** クリアテキストポート経由の要求をセキュアポートにリダイレクトするかどうかを指定します。
- **https.server.interfaces:** HTTPサーバがリスンするセキュアインタフェースが格納されます。これは、ndsconfigによる新しいインスタンスの設定中に設定されます。
- **https.server.cached-cert-dn:** HTTPサーバがセキュア接続を処理するときに使用する必要がある証明書オブジェクトのDNが格納されます。

cn=monitorを使用した監視

eDirectoryには、eDirectoryサーバの現在の状態を監視するためのLDAP検索メソッドが用意されています。eDirectoryは、eDirectoryサブシステムとバックグラウンドプロセス(スレッドプール、接続テーブル、DClient、DSエージェント、バックグラウンドプロセス、LDAPサーバなど)に関する有用なパフォーマンスメトリックおよびサーバ状態の情報を、cn=monitorのベースDNを持つエントリとして記録します。これらの統計情報をサーバから取得するには、cn=monitorの検索ベースを使用して検索要求を発行します。取得したこの統計情報を使用して、eDirectory環境を監視することができます。

重要: cn=monitorは仮想オブジェクトであり、eDirectoryツリーに実際に存在するわけではありません。このメソッドは、LDAPインタフェースを通してeDirectoryを監視する場合に使用できます。

---

eDirectoryサブシステムは、監視フレームワーク内のデータ生成元として登録されています。eDirectoryの登録済みデータ生成元を、表 8-1に示します。このフレームワークは、登録済みのすべてのデータ生成元からリアルタイムのデータを収集し、このデータの要求側(このデータのコンシューマ)と共有します。監視フレームワークは、検索要求に応じて動的にオブジェクトを収集して、cn=monitorのサブツリーに返します。各オブジェクトには、サーバの特定の側面についての情報が含まれています。一部のオブジェクトは他のオブジェクトのコンテナとして機能し、cn=monitorを最上位のオブジェクトとするオブジェクト階層を構築するために使用されます。監視フレームワーク、アクセス対象、およびその他のコントロールが提供する情報(LDAPサーバ固有の情報や接続固有の情報など)には、LDAPクライアントを使用してアクセスできます。eDirectoryでは、この検索要求を、NCPサーバオブジェクトのNDSRightsToMonitor属性に対する書き込み権を持つユーザに制限しています。

すべての登録済みデータ生成元からのデータには、ldapsearchまたは汎用のLDAPブラウザを使用してアクセスできます。

すべての登録済みデータ生成元の監視データを表示するには、ldapsearchコマンドを使用します。

```
ldapsearch -h <SrvIP> -p <port> -D <user dn> -w <password> -s sub -b cn=monitor
```

注: eDirectoryでは、cn=monitor検索でのデータフィルタリングをサポートしていません。再帰的に実行するようスケジュールされた一部のバックグラウンドプロセスについては、eDirectoryはcn=monitor検索の応答で、スケジュールされた回数分のプロセスを表示します。そのようなプロセスの一例は、SkulkerWorkerProcです。

監視統計情報の表示

ldapsearchは、すべての登録済みデータ生成元からのデータを、LDAP形式で、cn=monitorをベースとして使用して返します。LDAPサーバは、LDAPオブジェクト形式のデータコンシューマとしても機能します。

表 8-1には、データ生成元と、それに対応する、監視統計情報を格納しているパラメータがリストされます。eDirectoryと一緒に他の製品が設定されている場合は、データ生成元がこれ以外にも存在する可能性があります。

表 8-1　データ生成元と監視統計情報パラメータ

データ生成元	監視統計情報パラメータ
エージェント	◆ バックグラウンドプロセス ◆ パーティション ◆ システムの状態
DHOST	次のDHOSTプロセスおよび接続情報が監視されます。 ◆ インバウンド接続 ◆ スレッドプール情報 ◆ ThreadsSpawned ◆ ThreadsDied ◆ ThreadsIdle ◆ ThreadsWorkers ◆ ThreadPeakWorkers ◆ ThreadPoolReadyQueueItems ◆ ThreadPoolReadyQueueMaxWaitTime ◆ ThreadMinWaitTime ◆ ThreadMaxWaitTime
DClient	◆ アウトバウンドのコンテキスト ◆ アウトバウンド接続
LDAP	◆ バインディング ◆ 着信操作 ◆ 発信操作 ◆ トラフィック量

データ生成元	監視統計情報パラメータ
レコードマネージャ	◆ キャッシュ失敗表示 ◆ キャッシュ障害 ◆ 現在のサイズ、ヒット数 ◆ ヒット表示 ◆ キャッシュに保存された項目 ◆ 最大サイズ ◆ OldVersionCachedCount ◆ OldVersionCachedSize ◆ DIbサイズ ◆ チェックポイントスレッド

cn=monitorの検索ベースを使用して検索要求を発行すると、表 8-2に示されているように、監視フレームワークは検索要求の応答で、cn=monitorサブツリーのオブジェクトを動的に生成して返します。

表 8-2 *cn=monitor検索で監視されるオブジェクト*

オブジェクト名	説明
cn=Monitor	データを監視するルートレベルオブジェクト。
cn=Agent,cn=Monitor	ディレクトリサービスエージェントに関する情報を提供します。
cn=BackGroundProcInterval,cn=Agent,cn=Monitor	バックグラウンドプロセスに関する情報を提供します。(特定のプロセス、または通常はすべてのバックグラウンドプロセス)
cn=ARC resolve timer thread,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	詳細参照コストのバックグラウンドプロセスに関する情報を提供します。
cn=BacklinkProc,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	バックリンカのバックグラウンドプロセスに関する情報を提供します。
cn=CPU Usage monitor,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	CPU使用率のバックグラウンドプロセスに関する情報を提供します。
cn=CheckBacklinks,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	バックリンカのチェックのバックグラウンドプロセスに関する情報を提供します。
cn=CheckExtRefProc,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	外部参照のチェックのバックグラウンドプロセスに関する情報を提供します。
cn=ExtRefRefreshProc,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	外部参照の更新のバックグラウンドプロセスに関する情報を提供します。
cn=Janitor,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	ジャニタのバックグラウンドプロセスに関する情報を提供します。
cn=RunLimberUp,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	スケジュールリンバのバックグラウンドプロセスに関する情報を提供します。

オブジェクト名	説明
cn=Limber,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	リンバ(コネクティビティチェック)のバックグラウンドプロセスに関する情報を提供します。
cn=HiConvergenceHeartBeat,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Skulkerのスケジュールのバックグラウンドプロセスに関する情報を提供します。
cn=ObitProc,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	破損通知のバックグラウンドプロセスに関する情報を提供します。
cn=PartitionPurgeProcess,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	パーティションパージャのバックグラウンドプロセスに関する情報を提供します。
cn=Predicate Statistics Update,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	予測統計情報更新のバックグラウンドプロセスに関する情報を提供します。
cn=RNRAdvertise,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	アドバタイズサービスアドレスのバックグラウンドプロセスに関する情報を提供します。
cn=RefreshBinderyContext,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	バインダリ更新のバックグラウンドプロセスに関する情報を提供します。
cn=Repair Inactive Replicas,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	非アクティブレプリカの修復のバックグラウンドプロセスに関する情報を提供します。
cn=SchemaProc,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	スキーマ同期のバックグラウンドプロセスに関する情報を提供します。
cn=SkulkerProc,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	同期のバックグラウンドプロセスに関する情報を提供します。
cn=SkulkerWorkerProc,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	同期のバックグラウンドプロセスに関する情報を提供します。
cn=Partition,cn=Agent,cn=Monitor	サーバ上のすべてのユーザパーティションに関する情報を提供します。同じ属性の値が複数ある場合、それは複数のパーティションがあることを意味します
cn=Status,cn=Agent,cn=Monitor	サーバのステータスに関する情報を提供します。
cn=DHOST,cn=Monitor	DHOSTサブシステムに関する情報を提供します。
cn=InBoundConnection,cn=DHOST,cn=Monitor	インバウンド接続テーブルの情報に関する情報を提供します。
cn=ThreadPool,cn=DHOST,cn=Monitor	DHOSTスレッドプール統計に関する情報を提供します。
cn=Dclient,cn=Monitor	サーバ側DClientに関する情報を提供します。
cn=OutBoundConnection,cn=Dclient,cn=Monitor	アウトバウンド接続テーブルの情報に関する情報を提供します。
cn=OutBoundContext,cn=Dclient,cn=Monitor	アウトバウンドコンテキストテーブルの情報に関する情報を提供します。
cn=LDAP,cn=Monitor	LDAPサーバの情報を提供します。
cn=LDAPStatistics,cn=LDAP,cn=Monitor	LDAPサーバの統計に関する情報を提供します。

オブジェクト名	説明
cn=Bindings,cn=LDAPStatistics,cn=LDAP,cn=Monitor	LDAPサーバ上のバインディング統計に関する情報を提供します。
cn=IncomingOperations,cn=LDAPStatistics,cn=LDAP,cn=Monitor	LDAPサーバ上の着信操作統計に関する情報を提供します。
cn=OutgoingOperations,cn=LDAPStatistics,cn=LDAP,cn=Monitor	LDAPサーバ上の発信操作統計に関する情報を提供します。
cn=TrafficVolume,cn=LDAPStatistics,cn=LDAP,cn=Monitor	LDAPサーバのトラフィック量統計に関する情報を提供します。
cn=RecordManager,cn=Monitor	FLAIMデータベースに関する情報を提供します。
cn=Size,cn=RecordManager,cn=Monitor	FLAIMデータベースのサイズに関する情報を提供します。
cn=CheckPointThreadData,cn=RecordManager,cn=Monitor	チェックポイントスレッドに関する情報を提供します。
cn=CacheStatistics,cn=RecordManager,cn=Monitor	FLAIMデータベースのキャッシュ統計に関する情報を提供します。
cn=CacheFaultLooks,cn=CacheStatistics,cn=RecordManager,cn=Monitor	キャッシュ失敗表示の情報を提供します。
cn=CacheFaults,cn=CacheStatistics,cn=RecordManager,cn=Monitor	キャッシュ失敗の情報を提供します。
cn=HitLooks,cn=CacheStatistics,cn=RecordManager,cn=Monitor	キャッシュヒット表示の情報を提供します。
cn=Hits,cn=CacheStatistics,cn=RecordManager,cn=Monitor	キャッシュヒットの情報を提供します。
cn=ItemsCached,cn=CacheStatistics,cn=RecordManager,cn=Monitor	キャッシュに保存された項目数の情報を提供します。
cn=OldVersionCachedCount,cn=CacheStatistics,cn=RecordManager,cn=Monitor	古いバージョンのキャッシュに保存された項目数の情報を提供します。
cn=MaximumSize,cn=CacheStatistics,cn=RecordManager,cn=Monitor	最大キャッシュサイズの情報を提供します。
cn=CurrentSize,cn=CacheStatistics,cn=RecordManager,cn=Monitor	現在のキャッシュサイズの情報を提供します。
cn=OldVersionCachedSize,cn=CacheStatistics,cn=RecordManager,cn=Monitor	古いバージョンのキャッシュサイズの情報を提供します。

各オブジェクトには、サーバの特定の側面(接続やスレッドなど)についての情報が格納されます。監視統計情報が格納される属性を、表 8-3に示します。

表 8-3 統計情報を監視するための属性

属性	説明
BackgroundProcScheduled	バックグラウンドプロセスが次にスケジュールされている時刻。複数の値は、バックグラウンドプロセスが複数回スケジュールされていることを意味します。
BackgroundProcStartTime	次のバックグラウンドプロセスの開始時刻。複数の値は、バックグラウンドプロセスが複数回実行されることを意味します。
PerishableData	他のサーバと同期されていない状態のデータの量(秒単位で示されます)。
OBIT_NEWRDN_PURGEABLE	PURGEABLE状態のNEWRDN破損通知の数。
OBIT_NEWRDN_OK_TO_PURGE	パージ可能状態のNEWRDN破損通知の数。
OBIT_NEWRDN_NOTIFIED	NOTIFIED状態のNEWRDN破損通知の数。
OBIT_NEWRDN_ISSUED	ISSUED状態のNEWRDN破損通知の数。
OBIT_MOVED_PURGEABLE	PURGEABLE状態に移された破損通知の数。
OBIT_MOVED_OK_TO_PURGE	パージ可能状態に移された破損通知の数。
OBIT_MOVED_NOTIFIED	NOTIFIED状態に移された破損通知の数。
OBIT_MOVED_ISSUED	ISSUED状態に移された破損通知の数。
OBIT_DEAD_PURGEABLE	PURGEABLE状態で停止している破損通知の数。
OBIT_DEAD_OK_TO_PURGE	パージ可能状態で停止している破損通知の数。
OBIT_DEAD_NOTIFIED	NOTIFIED状態で停止している破損通知の数。
OBIT_DEAD_ISSUED	ISSUED状態で停止している破損通知の数。
OBIT_COUNT_FROM_DATABASE_INDEX	破損通知の合計数。
MaxRingDelta	レプリカリングの任意の2つのサーバ間で同期されていない状態のデータの最大量(秒単位で示されます)。
ChangeCacheCount	パーティション上の現在の変更キャッシュカウント。
eDirectoryUpTime	サーバ起動後の経過時間(秒数)。
eDirectorySystemCurrTime	サーバの現在のシステム時刻。
eDirectoryAgentVersion	カレントディレクトリサーバエージェントのバージョン。
MaxInBoundConnection	最大インバウンド接続。
InBoundConnectionCount	現在のインバウンド接続数。
ThreadsWorkers	スレッドプール内のワーカスレッド数。
ThreadsSpawned	生成されたスレッド数。
ThreadsIdle	アイドルスレッド数。
ThreadsDied	停止スレッド数。
ThreadWaitingQueuePeakItems	待機キュー内のスレッドの最大数。

属性	説明
ThreadWaitingQueueItems	待機キュー内の現在のスレッド数。
ThreadPoolReadyQueueMaxWaitTime	ReadyQueue内のスレッドの最大待機時間。
ThreadPoolReadyQueueItems	ReadyQueue内の現在のスレッド数。
ThreadPeakWorkers	プールワーカの最大数。
ThreadMinWaitTime	スケジュールされるまでのスレッドの最小待機時間。
ThreadMaxWaitTime	スケジュールされるまでのスレッドの最大待機時間。
TotalOpenOutBoundConnection	現在のオープンアウトバウンド接続数。
RefusedOutBoundConnection	拒否されたアウトバウンド接続数。
MaxOutBoundConnection	最大アウトバウンド接続数。
TotalOutBoundContextCount	最大アウトバウンドコンテキスト数。
ActiveOutBoundContextCount	現在のアウトバウンドコンテキスト数。
unAuthBinds	認証を省略した匿名バインド要求を受け取った回数。
strongAuthBinds	バインド要求のうち、強度の高い認証手続きであるSASLおよびX.500の認証に成功したものの回数。外部認証手続きによるものも数に含みます。
simpleAuthBinds	バインド要求のうち、簡易認証手続きにより認証に成功したものの回数。簡易認証手続きとは、パスワードを暗号化して、またはクリアテキストのまま送ることにより行うものです。
bindSecurityErrors	バインド要求のうち、認証手続きが適切でない、あるいは資格情報が無効であるために拒否したものの回数。
wholeSubtreeSearchOps	受け取ったサブツリー全体の検索要求の数。
searchOps	受け取った検索要求(ベースオブジェクト検索、1レベル検索、サブツリー全体の検索)の数。
removeEntryOps	受け取ったエントリ削除要求の数。
readOps	受け取った読み出し要求の数。
oneLevelSearchOps	受け取った1レベル検索要求の数。
modifyRDNOps	受け取ったRDN(相対識別名)変更要求の数。
modifyEntryOps	受け取ったエントリ変更要求の数。
listOps	受け取ったリスト要求の数。
inOps	クライアントから受け取った要求の数。
extendedOps	拡張処理の回数。
compareOps	受け取った比較要求の数。
addEntryOps	受け取ったエントリ追加要求の数。
abandonOps	LDAPが破棄した要求の数。
referrals	処理要求に応じて返した参照の個数。

属性	説明
chainings	このeDirectoryサーバから他のeDirectoryサーバに転送した処理の数。
outBytes	インタフェース上の送信トラフィック(バイト単位)。クライアントやeDirectoryサーバへの応答と、他のeDirectoryサーバへの要求がこれに含まれます。
inBytes	インタフェース上の受信トラフィック(バイト単位)。クライアントからの要求と、他のeDirectoryサーバからの応答がこれに含まれます。
合計	FLAIMキャッシュに含まれる項目の合計数。
EntryCache	エントリキャッシュに含まれる項目の合計数。
BlockCache	ブロックキャッシュに含まれる項目の合計数。
TotalSize	FLAIMキャッシュに含まれる項目の合計サイズ。
EntryCacheSize	エントリキャッシュに含まれる項目の合計サイズ。
BlockCacheSize	ブロックキャッシュに含まれる項目の合計サイズ。
CheckPointThreadWritingDataBlocks	0は、そのチェックポイントがダーティブロックに書き込んでいないことを意味します。1は、そのチェックポイントがダーティブロックに書き込んでいることを意味します。
CheckPointThreadStartTime	チェックポイントスレッドの開始時刻。この値を確認する必要があるのは、チェックポイントスレッドが実行されている場合のみです。
CheckPointThreadLogBlocksWritten	書き込まれたログブロックの数。
CheckPointThreadIsRunning	0は、チェックポイントが実行されていないことを意味します。1は、チェックポイントスレッドが実行されていることを意味します。
CheckPointThreadIsForced	チェックポイントが強制されているかどうかを示します。
CheckPointThreadForceStartTime	チェックポイントの強制開始時刻。この値を確認する必要があるのは、チェックポイントが強制的に開始される場合のみです。
CheckPointThreadDirtyCacheBlocks	ダーティキャッシュブロックの数。
CheckPointThreadDataBlocksWritten	書き込まれたダーティブロックの数。
CheckPointThreadBlockSize	現在のブロックサイズ。
TotalDIBSize	FLAIMデータベースの合計サイズ。
DIBStreamFileSize	ストリームファイルの合計サイズ。
DIBRollBackFileSize	ロールバックファイルの合計サイズ。
DIBRflmFileSize	ロールフォワードログファイルの合計サイズ。
DIBFileSize	DIBファイルの合計サイズ。

以下に、LDAP検索の出力例を示します。

```
# LDAPv3
# base <cn=monitor> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
# BackGroundProcInterval, Agent, Monitor
dn: cn=BackGroundProcInterval,cn=Agent,cn=Monitor
slowSyncInterval: 1800
fastSyncInterval: 5
ServerStateUpThreshold: 1800
JanitorInterval: 120
HeartBeatSkulkInterval: 3600
FlatCleaningInterval: 43200
DRLInterval: 60
BacklinkInterval: 46800
objectclass: Top
objectclass: extensibleObject
# .GOOD-ONE., Partition, Agent, Monitor
dn: cn=.GOOD-ONE.,cn=Partition,cn=Agent,cn=Monitor
ChangeCacheCount: 0
objectclass: Top
objectclass: extensibleObject
# InBoundConnection, DHOST, Monitor
dn: cn=InBoundConnection,cn=DHOST,cn=Monitor
MaxInBoundConnection: 256
InBoundConnectionCount: 20
objectclass: Top
objectclass: extensibleObject
# ThreadPool, DHOST, Monitor
dn: cn=ThreadPool,cn=DHOST,cn=Monitor
ThreadsWorkers: 37
Monitoring
ThreadsSpawned: 3572
ThreadsIdle: 7
ThreadsDied: 3535
ThreadWaitingQueuePeakItems: 24
ThreadWaitingQueueItems: 20
ThreadPoolReadyQueueMaxWaitTime: 574529
ThreadPoolReadyQueueItems: 0
ThreadPeakWorkers: 90
ThreadMinWaitTime: 2
ThreadMaxWaitTime: 16394616
objectclass: Top
objectclass: extensibleObject
# OutBoundConnection, Dclient, Monitor
dn: cn=OutBoundConnection,cn=Dclient,cn=Monitor
TotalOpenOutBoundConnection: 17
RefusedOutBoundConnection: 0
MaxOutBoundConnection: 4294967295
objectclass: Top
objectclass: extensibleObject
# OutBoundContext, Dclient, Monitor
dn: cn=OutBoundContext,cn=Dclient,cn=Monitor
TotalOutBoundContextCount: 256
objectclass: Top
objectclass: extensibleObject
# Bindings, LDAPStatistics, LDAP, Monitor
dn: cn=Bindings,cn=LDAPStatistics,cn=LDAP,cn=Monitor
unAuthBinds: 6908
strongAuthBinds: 0
simpleAuthBinds: 4433475
```

```
bindSecurityErrors: 0
objectclass: Top
objectclass: extensibleObject
# IncomingOperations, LDAPStatistics, LDAP, Monitor
dn: cn=IncomingOperations,cn=LDAPStatistics,cn=LDAP,cn=Monitor
wholeSubtreeSearchOps: 4426462
searchOps: 4426462
removeEntryOps: 0
readOps: 0
oneLevelSearchOps: 0
modifyRDNOps: 0
modifyEntryOps: 4
listOps: 0
inOps: 8901739
extendedOps: 0
compareOps: 0
addEntryOps: 5
abandonOps: 0
objectclass: Top
objectclass: extensibleObject
# OutgoingOperations, LDAPStatistics, LDAP, Monitor
dn: cn=OutgoingOperations,cn=LDAPStatistics,cn=LDAP,cn=Monitor
referrals: 0
chainings: 0
objectclass: Top
objectclass: extensibleObject
# TrafficVolume, LDAPStatistics, LDAP, Monitor
dn: cn=TrafficVolume,cn=LDAPStatistics,cn=LDAP,cn=Monitor
outBytes: 326809576
inBytes: 380249498
objectclass: Top
objectclass: extensibleObject
Monitoring
# CacheFaultLooks, RecordManager, Monitor
dn: cn=CacheFaultLooks,cn=RecordManager,cn=Monitor
TotalSize: 2699
EntryCacheSize: 2539
BlockCacheSize: 160
objectclass: Top
objectclass: extensibleObject
# CacheFaults, RecordManager, Monitor
dn: cn=CacheFaults,cn=RecordManager,cn=Monitor
TotalSize: 1948
EntryCacheSize: 1788
BlockCacheSize: 160
objectclass: Top
objectclass: extensibleObject
# CurrentSize, RecordManager, Monitor
dn: cn=CurrentSize,cn=RecordManager,cn=Monitor
TotalSize: 4849664
EntryCacheSize: 3866624
BlockCacheSize: 983040
objectclass: Top
objectclass: extensibleObject
# HitLooks, RecordManager, Monitor
dn: cn=HitLooks,cn=RecordManager,cn=Monitor
TotalSize: 656418775
EntryCacheSize: 489811630
BlockCacheSize: 166607145
objectclass: Top
```

```
objectclass: extensibleObject
# Hits, RecordManager, Monitor
dn: cn=Hits,cn=RecordManager,cn=Monitor
TotalSize: 449815580
EntryCacheSize: 283226835
BlockCacheSize: 166588745
objectclass: Top
objectclass: extensibleObject
# ItemsCached, RecordManager, Monitor
dn: cn=ItemsCached,cn=RecordManager,cn=Monitor
TotalSize: 1865
EntryCacheSize: 1691
BlockCacheSize: 174
objectclass: Top
objectclass: extensibleObject
# MaximumSize, RecordManager, Monitor
dn: cn=MaximumSize,cn=RecordManager,cn=Monitor
TotalSize: 200015872
EntryCacheSize: 100007972
BlockCacheSize: 100007900
objectclass: Top
objectclass: extensibleObject
# OldVersionCachedCount, RecordManager, Monitor
dn: cn=OldVersionCachedCount,cn=RecordManager,cn=Monitor
TotalSize: 7
EntryCacheSize: 3
BlockCacheSize: 4
objectclass: Top
objectclass: extensibleObject
# OldVersionCachedSize, RecordManager, Monitor
dn: cn=OldVersionCachedSize,cn=RecordManager,cn=Monitor
Monitoring
TotalSize: 21376
EntryCacheSize: 4448
BlockCacheSize: 16928
objectclass: Top
objectclass: extensibleObject
# search result
search: 2
result: 0 Success
# numResponses: 20
# numEntries: 19
```

DSTraceの使用

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

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

ndstraceコマンドの完全な構文は次のとおりです。

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

DSTraceユーティリティは、次の3つの主要部分で構成されています。

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

基本機能

DSTraceの基本機能は次のとおりです。

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

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

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

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

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

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

```
ndstrace command_option
```

次の表では、入力可能なコマンドオプションのリストを示します。

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

デバッギングメッセージ

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

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

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

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

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

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

トレースフラグ	説明
ABUF	eDirectory要求との連携、またはeDirectory要求への応答として受信されたデータを含む、インバウンドおよびアウトバウンドパケットバッファに関するメッセージと情報です。
ALOC	メモリ割り当ての詳細について示すメッセージです。
AREQ	他のサーバまたはクライアントからのインバウンド要求に関するメッセージです。
AUTH	認証に関するメッセージとエラーレポートです。
BASE	最小限のデバッギングレベルでのデバッグエラーメッセージ。
BLNK	バックリンクとインバウンドの破損通知メッセージおよびエラーレポートです。
CBUF	アウトバウンドDSクライアント要求に関するメッセージです。
CHNG	キャッシュ変更メッセージです。
COLL	以前に更新内容を受信したときのオブジェクトの更新情報に関するステータスおよびエラーレポートです。
CONN	ローカルサーバが接続を試みている相手のサーバ、およびローカルサーバが接続できない原因となっている可能性のあるエラーとタイムアウトについての情報を示すメッセージです。
DNS	eDirectory統合DNSサーバプロセスに関するメッセージです。

トレースフラグ	説明
DRLK	分散リファレンスリンクメッセージです。
DVRS	eDirectoryが機能している可能性のあるDirXML®ドライバ固有のエリアを示すメッセージ。
DXML	DirXMLイベントの詳細について示すメッセージです。
FRAG	eDirectoryメッセージをNCPサイズのメッセージに分解する、NCP™ Fraggerからのメッセージ。
IN	インバウンドの要求およびプロセスに関するメッセージです。
INIT	eDirectoryの初期化に関するメッセージです。
INSP	ソースサーバのローカルデータベース内のオブジェクトの整合性に関するメッセージです。このフラグを使用すると、ソースサーバのディスクストレージシステム、メモリ、プロセッサの要求量が増加します。オブジェクトが破損しない限り、このフラグは有効に設定しないでください。
JNTR	janitor、レプリカの同期、フラットクリーナなどのバックグラウンド処理に関するメッセージです。
LDAP	LDAPサーバに関するメッセージです。
LMBR	limber処理に関するメッセージです。
LOCK	ソースサーバのローカルデータベースロックの使用および操作に関するメッセージです。
LOST	消失エントリに関するメッセージです。
MISC	eDirectory内の異なるソースからのメッセージです。
MOVE	パーティションの移動操作、またはサブツリーの移動操作からのメッセージです。
NCPE	NCPレベルの要求を受信したサーバを示すメッセージです。
NMON	iMonitorに関するメッセージです。
OBIT	破損通知処理からのメッセージです。
PART	バックグラウンド処理および要求処理からのパーティション操作に関するメッセージです。
PURG	パージ処理に関するメッセージです。
RECM	ソースサーバのデータベースの操作に関するメッセージです。
RSLV	名前解決要求の処理に関するメッセージです。
SADV	SLP (Service Location Protocol)のツリー名とパーティションの登録に関するメッセージです。
SCMA	スキーマの同期処理に関するメッセージです。
SCMD	スキーマ関連の操作の詳細について示すメッセージです。インバウンド同期とアウトバウンド同期の両方についての詳細を示します。
SKLK	レプリカの同期処理に関するメッセージです。
SPKT	eDirectory NCPサーバレベルの情報に関するメッセージです。

トレースフラグ	説明
STRM	ストリーム構文の属性の処理に関するメッセージです。
SYDL	レプリケーション処理時の詳細について示すメッセージです。
SYNC	インバウンド同期トラフィック(サーバ側で受信される内容)についてのメッセージです。
TAGS	トレースオプションを識別するタグ文字列が表示されます。このトレースオプションでは、トレース処理で表示される各行のイベントが生成されます。
THRD	バックグラウンド処理(スレッド)の開始時と終了時を示すメッセージです。
TIME	同期処理時に使用される遷移ベクトルに関するメッセージです。
TVEC	Synchronize Up To、レプリカ、および遷移ベクトルなどの属性に関するメッセージです。
VCLN	他のサーバへの接続の確立または切断に関するメッセージです。

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

```
set ndstrace = A81164B91
```

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

バックグラウンド処理

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

```
set ndstrace = *H
```

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

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

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

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

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

トレースフラグ	パラメータ	説明
*A	なし	ソースサーバのアドレスキャッシュをリセットします。
*AD	なし	ソースサーバのアドレスキャッシュを無効にします。
*AE	なし	ソースサーバのアドレスキャッシュを有効にします。

トレースフラグ	パラメータ	説明
*B	なし	ソースサーバ上で1秒後にバックリンク処理の実行を開始するようにスケジュールします。
!B	時刻	バックリンク処理の実行間隔を分単位で設定します。 デフォルト=1500分(25時間)。範囲=2～10080分(168時間)
*CT	なし	ソースサーバのアウトバウンド接続テーブルと、テーブルの現在の統計情報を表示します。これらの統計情報には、他のサーバやクライアントからソースサーバへのインバウンド接続に関する情報は含まれていません。
*CTD	なし	コンマ区切りの形式で、ソースサーバのアウトバウンド接続テーブルと、テーブルの現在の統計情報を表示します。これらの統計情報には、他のサーバやクライアントからソースサーバへのインバウンド接続に関する情報は含まれていません。
*D	レプリカrootEntry ID	指定したローカルエントリIDをソースサーバの［すべてのオブジェクトを送信］リストから削除します。エントリIDでは、サーバのローカルデータベースで固有のパーティションルートオブジェクトを指定する必要があります。通常、このコマンドは、サーバのアクセス不能が原因でSend All Updates処理が何度試みられても失敗する場合にのみ使用します。
!D	時刻	インバウンド同期およびアウトバウンド同期の間隔を分単位で指定された値に設定します。 デフォルト=24分。範囲=2～10080分(168時間)
!DI	時刻	インバウンド同期の間隔を分単位で指定された値に設定します。 デフォルト=24分。範囲=2～10080分(168時間)
!DO	時刻	アウトバウンド同期の間隔を分単位で指定された値に設定します。 デフォルト=24分。範囲=2～10080分(168時間)
*E	なし	ソースサーバのエントリキャッシュを再初期化します。
!E	なし	インバウンド同期およびアウトバウンド同期処理の実行を開始するようにスケジュールします。
!EI	なし	インバウンド同期処理の実行を開始するようにスケジュールします。
!EO	なし	アウトバウンド同期処理の実行を開始するようにスケジュールします。
*F	なし	janitor処理の一部として、フラットクリーナ処理の実行がソースサーバ上で5秒後に開始されるようにスケジュールします。

トレースフラグ	パラメータ	説明
!F	時刻	フラットクリーナ処理の実行間隔を分単位で設定します。 デフォルト=240分(4時間)。範囲=2～10080分(168時間)
*FL	1-10	DSTraceが使用するローリングログファイルの数を設定します。このパラメータを1より大きい値に設定した場合、ソースサーバのndstrace.logファイルが設定されている最大ファイルサイズに達すると、DSTraceはログファイルの名前をndstrace1.logに変更して、新しいndstrace.logファイルを作成します。このファイルが最大ファイルサイズに達すると、先ほどのndstrace1.logファイルがndstrace2.logに名前を変更され、それより新しいndstrace.logファイルがndstrace1.logに名前を変更されます。 この処理は、DSTraceがこのオプションによって設定されたローリングログファイルの最大数に達するまで継続します。指定された制限に達すると、一番古いログファイルが削除されて、指定された最大数のローリングログファイルのみが保持されます。 最大10個のローリングログファイルを設定できます。デフォルトでは、DSTraceはローリングログファイルを少なくとも1個使用する必要があります。このパラメータを0に設定すると、DSTraceはパラメータ値として1を使用します。
*G	レプリカrootEntry ID	指定したルートパーティションIDの変更キャッシュを再構築します。
*H	なし	ソースサーバ上で直ちににレプリカ同期処理の実行を開始するようにスケジュールします。
!H	時刻	Heatbeat同期処理の実行間隔を分単位で設定します。 デフォルト=30分。範囲=2～1440分(24時間)
*HR	なし	メモリ内で最後に送信されたベクトルを消去します。
*I	レプリカrootEntry ID	指定したローカルエントリIDをソースサーバの［すべてのオブジェクトを送信］リストに追加します。エントリIDでは、サーバのローカルデータベースで固有のパーティションルートオブジェクトを指定する必要があります。レプリカの同期処理では、［すべてのオブジェクトを送信］リストがチェックされます。パーティションのルートオブジェクトのエントリIDがリスト内に存在する場合、Synchronized Up To属性の値に関係なく、eDirectoryによってパーティション内のすべてのオブジェクトと属性が同期されます。
!I	時刻	Heatbeat同期処理の実行間隔を分単位で設定します。 デフォルト=30分。範囲=2～1440分(24時間)
*J	なし	レプリカの同期処理の一部として、ソースサーバ上でパージ処理の実行を開始するようにスケジュールします。

トレースフラグ	パラメータ	説明
!J	時刻	janitor処理の実行間隔を分単位で設定します。 デフォルト=2分。範囲=1～10080分(168時間)
*L	なし	ソースサーバ上で5秒後にlimber処理の実行を開始するようにスケジュールします。
*M	［Bytes］	ソースサーバのndstrace.logファイルで使用する最大ファイルサイズを変更します。このコマンドは、デバッグファイルの状態に関係なく使用できます。bytesの値は10000バイトと100MBの間で10進の値を指定する必要があります。この範囲外の値が指定された場合、変更は行われません。
!M	なし	eDirectoryで使用されるメモリの最大量をレポートします。
!N	0 | 1	名前の形式を設定します。 0=16進数のみ。1=full dot形式
*P	なし	調整可能なパラメータとそのデフォルトの設定を表示します。
*R	なし	ndstrace.logファイルのサイズをゼロバイトに再設定します。このコマンドは、SETパラメータのNDS Trace File Length Set to Zeroと同じ働きをします。
*S	なし	サーバ上のレプリカを同期する必要があるかどうかをチェックするスカルク処理をスケジュールします。
!SI	時刻	インバウンドスキーマ同期処理の実行間隔を分単位で設定します。 デフォルト=24分。範囲=2～10080分(168時間)
!SO	時刻	アウトバウンドスキーマ同期処理の実行間隔を分単位で設定します。 デフォルト=24分。範囲=2～10080分(168時間)
!SIO	時刻	時間を分単位で指定し、その間のインバウンドスキーマ同期処理を無効にします。 デフォルト=24分。範囲=2～10080分(168時間)
!SO0	時刻	時間を分単位で指定し、その間のインバウンドスキーマ同期処理を無効にします。 デフォルト=24分。範囲=2～10080分(168時間)
*SS	なし	強制的に即時スキーマの同期を実行します。
*SSA	なし	スキーマの同期処理の実行を即時に開始するようにスケジュールします。過去24時間以内に同期が行われていた場合でも、すべてのターゲットサーバでスキーマの同期が強制的に実行されます。

トレースフラグ	パラメータ	説明
*SSD	なし	ソースサーバの［ターゲットスキーマ同期］リストをリセットします。このリストでは、スキーマの同期処理の実行中にソースサーバと同期する必要のあるサーバが識別されます。レプリカを保持していないサーバは、サーバオブジェクトとレプリカを保持しているサーバのターゲットリストに包含されるように要求を送信します。
*［SSL］	なし	ターゲットサーバのスキーマ同期リストを印刷します。
*ST	なし	ソースサーバ上のバックグラウンド処理のステータス情報を表示します。
*STX	なし	ソースサーバ上のバックリンク処理(外部参照)のステータス情報を表示します。
*STS	なし	ソースサーバ上のスキーマ同期処理のステータス情報を表示します。
*STO	なし	ソースサーバ上のバックリンク処理(破損通知)のステータス情報を表示します。
*STL	なし	ソースサーバ上のlimber処理のステータス情報を表示します。
!T	時刻	サーバの稼動状態のチェックの実行間隔を分単位で設定します。 デフォルト=30分。範囲=1～720分(12時間)
*U	サーバのオプションのID	コマンドにエントリIDが含まれていない場合は、以前に「**down**」から「**up**」にラベルが付加された任意のサーバのステータスを変更します。コマンドにローカルエントリIDが含まれている場合は、指定されたサーバのステータスを「**down**」から「**up**」に変更します。エントリIDは、ソースサーバのデータベースで固有であり、サーバを表すオブジェクトを参照する必要があります。
!V	リスト	制限のあるeDirectoryバージョンのリストを表示します。バージョンが表示されない場合は、制限がないことを示します。各バージョンはコンマで区切られます。
*Z	なし	現在、スケジュールされているタスクを表示します。

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、「293 ページの 「iMonitorメッセージのフィルタ」」を参照してください。

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
  ```

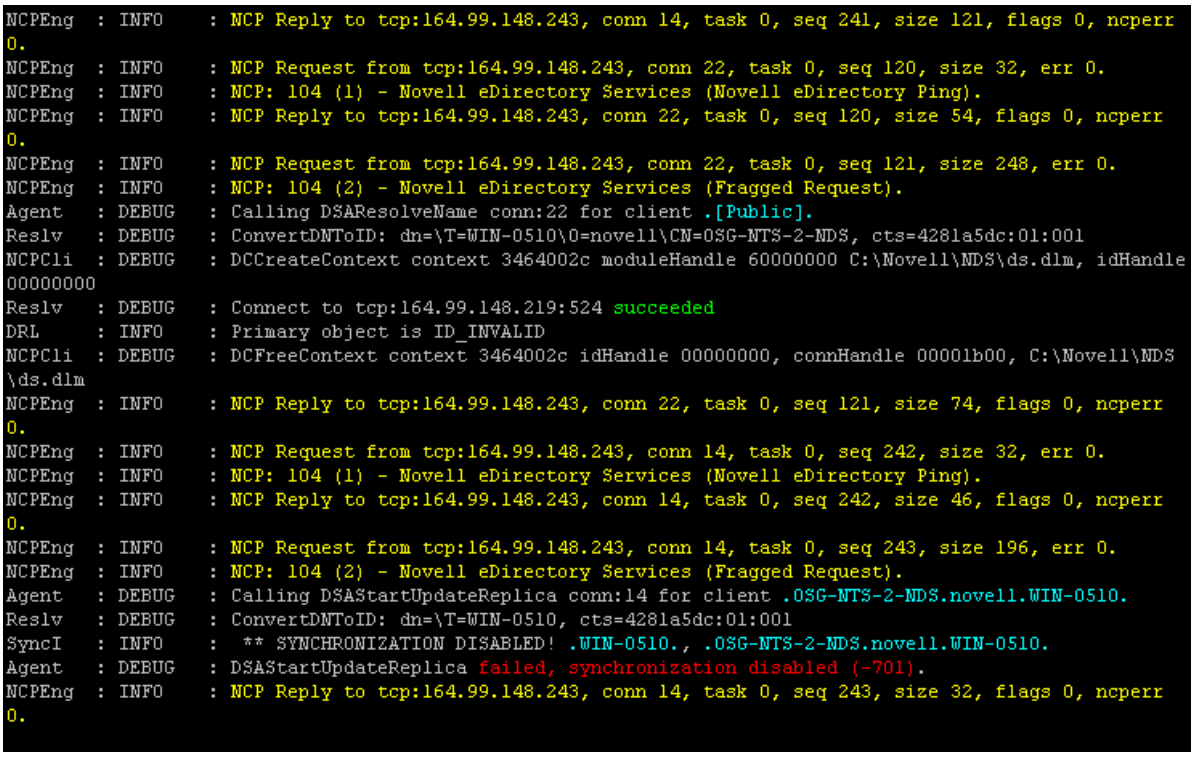
- 接続IDに基づいてフィルタを無効にするには、次のように入力します。

  ```
  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 8-5 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



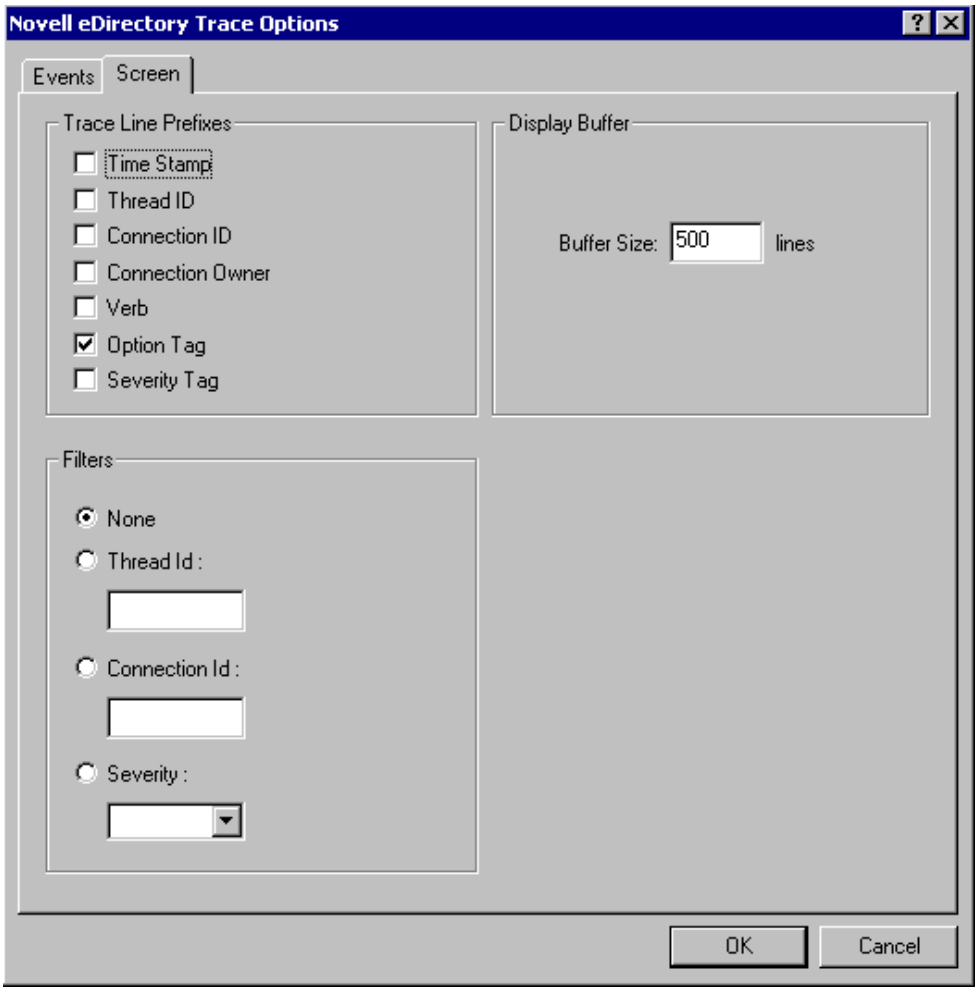
Windows

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8-6 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。
- Windowsでは、トレースレベルの重大度は動作しません。

---

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。

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 8-4 *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。

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。

9 eDirectoryサーバのSecretStore環境設定

eDirectoryをインストールすると、デフォルトでSecretStoreの実行可能ファイルとライブラリがインストールされます。ただし、eDirectoryの新しいインストールに対するSecretStoreの設定はオプションです。eDirectoryサーバをアップグレードする場合は、既存の設定が変更されることなくそのまま維持されます。LinuxおよびWindowsプラットフォームで次のコマンドを使用して、SecretStoreの機能に対応するようにeDirectoryスキーマを拡張してください。

```
ice -S SCH -f /var/opt/novell/eDirectory/lib/nds-schema/sssv3.sch -D LDAP -s
<serverIP> -d <adminDN>
```

例: ice -S SCH -f /var/opt/novell/eDirectory/lib/nds-schema/sssv3.sch -D LDAP -s 1.2.3.4 -d cn=admin,o=administrators

SecretStoreの設定および設定解除は、以降のセクションで説明する手順で行うことができます。

- 295 ページの 「Linux」
- 295 ページの 「Windows」

Linux

SecretStoreの設定

SecretStoreを設定するには、次の手順に従います。

1. 設定する場合は、ssscfg-cを実行します。
2. エントリ「ssncp」を/etc/opt/novell/eDirectory/conf/ndsmodules.confに追加し、eDirectoryの起動中にデフォルトでSecretStoreモジュールがロードされるようにします。後からnssユーティリティを使用して、SecretStoreモジュールをロードまたはアンロードすることもできます。

SecretStoreの設定解除

設定解除する場合は、ssscfg-dコマンドを実行します。エントリ「ssncp」が/etc/opt/novell/eDirectory/conf/ndsmodules.conf内にある場合は、このエントリを削除します。

Windows

次の手順でSecretStoreを設定および設定解除します。

1. 設定する場合は、ssscfg.exe-cを実行します。
2. 設定解除する場合は、ssscfg.exe-dを実行します。

ssscfg.exeユーティリティは、eDirectoryInstallDrive:>\Novell\NDS\ディレクトリにあります。eDirectoryサーバの起動中にSecretStoreモジュールを自動ロードするには、NDSCons.exeのGUIインタフェースで、ssncp.dlmモジュールをautoに設定します。

10 NetIQ eDirectoryツリーのマージ

NetIQ eDirectoryのマージユーティリティを使用すると、2つのNetIQ eDirectoryツリーをマージして、単一のeDirectoryツリーを作成できます。マージされるのはTreeオブジェクトだけです。コンテナオブジェクトとそのリーフオブジェクトは、マージ後のツリー上でもそれぞれ異なるオブジェクトとして存在します。

ヒント: リーフオブジェクトを移動する場合や、パーティションをマージする場合には、NetIQ iManagerを使用します。

マージする2つのツリーをそれぞれソースツリーおよびターゲットツリーといいます。1つのツリーを別のツリーにマージする前に、ターゲットツリーにあるルートパーティションのレプリカを１つだけ残し、その他のすべてのレプリカを削除する必要があります。ターゲットツリーにルートパーティションのレプリカが1つしかない場合には、マージ処理を続行できます。マージ後は、ルートパーティションのレプリカが2つになります。1つはターゲットツリー上にあったレプリカで、もう1つはマージ操作を実行したソースツリーのサーバ上にあったレプリカです。ルートパーティションのレプリカを追加する必要がある場合は、マージが完了した後に保存することができます。

マージ時にターゲットツリーサーバにルートパーティションのレプリカが複数ある場合、マスタレプリカを保持していないサーバで、外部参照オブジェクトの位置に関する問題が発生する可能性があります。外部参照オブジェクトは、サブオーディネートリファレンスのパーティションルートに含まれています。これは、パーティションの境界を表すルートパーティションのレプリカを持つ別のサーバに配置する必要があります。ソースツリーにあるルートパーティションの下位パーティションごとに、ターゲットツリーにあるサブオーディネートリファレンスのパーティションルートを持つ必要があります。エラーが生じた場合、同期ステータスに関するeDirectoryエラーコード-605が報告されます。この場合、DSRepairを使用して、エラーが発生したサーバのローカルデータベースを修復します。詳細については、338 ページの 「ローカルデータベースの修復の実行」を参照してください。

DSMergeを実行しても、コンテナ内のeDirectory名またはコンテキストは変わりません。オブジェクト権とプロパティ権はマージ後のツリーでも保持されます。

この章では、次のトピックについて説明します。

eDirectoryツリーの統合

eDirectoryツリーをマージするには、iManagerのツリーのマージウィザードを使用します。このウィザードでは、2つのeDirectoryツリーのルートをマージできます。マージされるのはTreeオブジェクトだけです。コンテナオブジェクトとそのリーフオブジェクトは、マージ後のツリー上でもそれぞれ異なるオブジェクトとして存在します。

マージする2つのツリーはそれぞれソースツリーおよびターゲットツリーといいます。ソースツリーのマージ先ツリーがターゲットツリーです。

DSMergeを実行しても、コンテナ内のオブジェクトの名前は変わりません。オブジェクト権とプロパティ権はマージ後のツリーでも保持されます。

前提条件

- ❒ ソースツリーの［ルート］パーティションのマスタレプリカが格納されているサーバに、eDirectoryがインストールされている必要があります。
- ❒ 正しい機能を維持するには、ソースツリーの他のサーバをeDirectory 8.8以降にアップグレードする必要があります。

注: 許可されたログインメソッドを削除するには、ldapdeleteツールまたはiManagerを使用します。

ターゲットツリーの要件

- ❒ ターゲットツリーの［ルート］パーティションのマスタレプリカが格納されているサーバに、NetIQ eDirectoryがインストールされている必要があります。このサーバで他のバージョンのNDS®またはeDirectoryが実行されている場合は、マージ操作が正常に完了しません。
- ❒ 正しい機能を維持するには、ターゲットツリーの他のサーバをeDirectory 8.8以降にアップグレードする必要があります。
- ❒ ソースツリーとターゲットツリーの両方で、Treeのサブオーディネートコンテナを同じ名前で維持することはできません。2つのツリーをマージする前に、一方のコンテナをリネームする必要があります。
- ❒ ソースツリーとターゲットツリーの両方にセキュリティオブジェクトがある場合は、ツリーをマージする前にどちらかを削除する必要があります。

スキーマの要件

マージ操作を実行する前に、2つのツリーのスキーマが正確に一致している必要があります。ツリーごとに[Root]パーティションのマスタレプリカを含むサーバでDSRepairを実行する必要があります。［リモートスキーマのインポート］オプションを使用して、各ツリーで他のツリーのスキーマがすべて認識されていることを確認します。

1 NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。

2 ［**eDirectoryの保守**］>［**スキーマの保守**］の順にクリックします。

3 スキーマの保守操作を実行するサーバを指定し、［**次へ**］をクリックします。

4 指定したサーバに対する認証を行ってから、［**次へ**］をクリックします。

5 ［**リモートスキーマのインポート**］>［**次へ**］の順にクリックします。

6 スキーマのインポート元のツリー名を指定します。

7 ［**Start**］をクリックします。

このオプションは、スキーマの相違点が報告されなくなるまで、ソースツリーとターゲットツリーの両方で実行することが必要な場合があります。そうしないとマージ操作は成功しません。

8 スキーマの保守操作によって返された情報とともに「完了」メッセージが表示されたら、［**閉じる**］をクリックして終了します。

ソースツリーをターゲットツリーへマージする

ツリーをマージすると、ソースツリー内のサーバがターゲットツリーに組み込まれます。

ターゲットツリーのTreeオブジェクトがソースツリーのオブジェクトの新しいTreeオブジェクトになり、ソースツリーにあるすべてのサーバのツリー名がターゲットツリーのツリー名に変わります。

ターゲットツリー内のサーバのツリー名はマージ後も変わりません。

ソースツリーのTreeオブジェクトの下位オブジェクトは、ターゲットツリーのTreeオブジェクトの下位オブジェクトになります。

パーティションの変化

マージ実行時には、ソースツリーのTreeオブジェクトの下にあるオブジェクトがDSMergeによって複数のパーティションに分けられます。

続いて、ソースツリー内のサーバから、Treeパーティションのレプリカがマスタレプリカを除いてすべて削除されます。ソースツリーのマスタレプリカを保持していたサーバには、ターゲットツリーのツリーパーティションのレプリカが作成されます。

図 10-1および図 10-2は、2つのツリーをマージした場合のパーティションの変化を示します。

図 10-1　マージ前のeDirectoryツリー

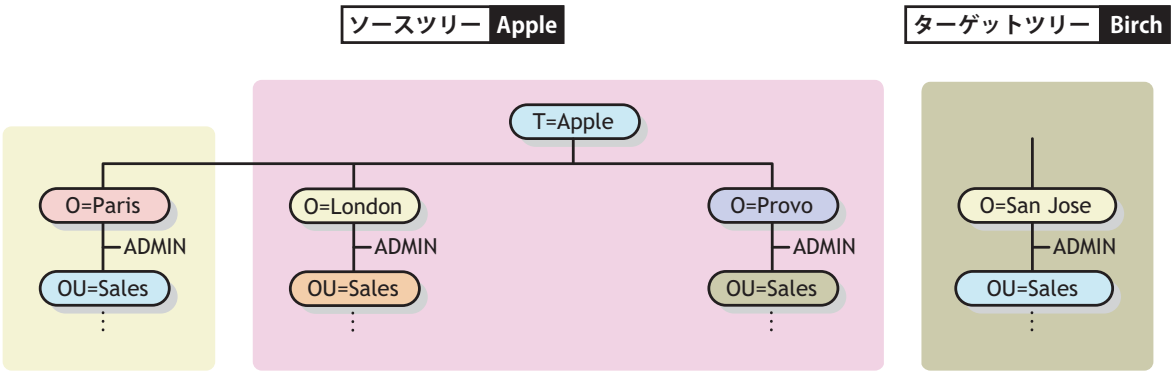
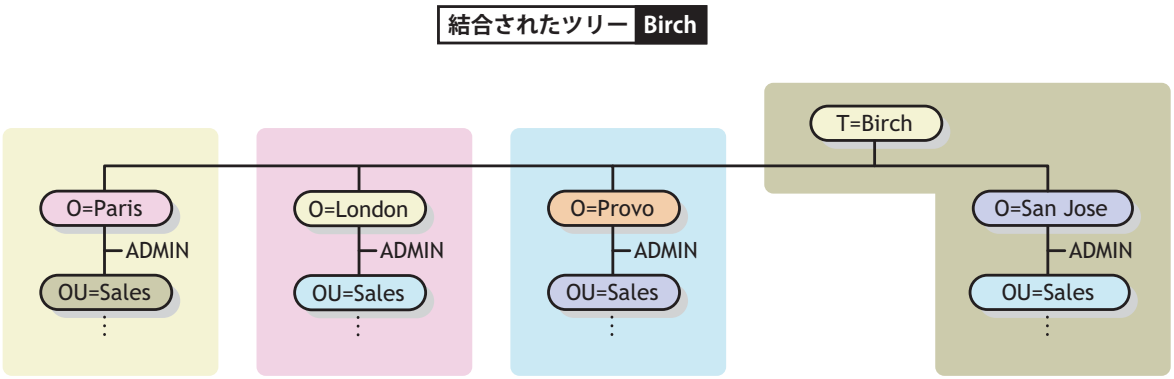


図 10-2　マージ後のeDirectoryツリー



ソースツリーとターゲットツリーを準備する

マージ操作を開始する前に、そのマージ操作の影響を受けるすべてのサーバが安定した状態で同期していることを確認する必要があります。次の表で、マージ対象のソースツリーとターゲットツリーの準備に関する前提条件について説明します。

必要条件	必要な措置
ソースツリーまたはターゲットツリーのツリーパーティションのレプリカを保持しているすべてのサーバ上でWANMANがオフになっている。	WANMANポリシーを調べて、WAN通信の制約によるマージ操作への支障がないことを確認します。必要があれば、マージ操作を開始する前にWANMANをオフにします。
ソースツリーのTreeオブジェクトに別名またはリーフオブジェクトが存在しない。	ソースツリーのTreeオブジェクトに存在する別名またはリーフオブジェクトを削除します。

必要条件	必要な措置
ソースツリーおよびターゲットツリーに同じ名前がない。	同じ名前がある場合には、ソースツリーまたはターゲットツリーのオブジェクト名を変更します。コンテナオブジェクト名を変更したくない場合は、コンテナの1つから同じツリー内の別のコンテナにオブジェクトを移動し、空になったコンテナをDSMerge実行前に削除します。詳細については、101ページの第3章「オブジェクトの管理」を参照してください。 Treeオブジェクトの直下でないコンテナオブジェクトの場合は、両ツリーに同じコンテナオブジェクトがあってもかまいません。
ソースツリー上にログイン接続が存在しない。	ソースツリーのすべての接続を終了します。
ソースツリーのeDirectoryおよびターゲットツリーのeDirectoryのバージョンが同じである。	ルートパーティションのレプリカを持つ、eDirectory でないすべてのサーバをアップグレードします。
ターゲットツリー内のルートレプリカのコピーが1つである。	ターゲットツリー上の、マスタレプリカを除いたすべてのレプリカを削除します。
ソースツリーおよびターゲットツリーのスキーマが同じである。	DSMergeを実行します。出力されるレポートを見てスキーマに問題があることがわかった場合は、DSRepairを使用してスキーマを一致させます詳細については、348 ページの「リモートスキーマをインポートする」を参照してください。DSMergeを再実行します。
単一のツリーだけが、ツリーのルートの下位にセキュリティコンテナを保持できる。	ソースツリーおよびターゲットツリーの両方がセキュリティコンテナを保持している場合は、「837 ページの付録 A「NMASの注意事項」」で説明されている手順に従って、一方のコンテナを削除します。

マージ操作は単独のトランザクションなので、実行中に停電やハードウェアエラーが発生しても重大な障害にはつながりません。ただし、DSMergeを実行する前に、あらかじめeDirectoryデータベースの通常のバックアップをとっておくことをお勧めします。詳細については、439ページの第15章「NetIQ eDirectoryのバックアップと復元」を参照してください。

マージする前の時刻の同期

重要: 時刻同期の正確な環境設定は複雑な作業です。ツリーをマージする前に、両ツリーを同期させるのに十分な時間があることを確認します。

時刻の異なる複数のタイムソースが使用されていたり、ツリー内のサーバの中に時刻が同期されていないものがあると、eDirectoryは正しく機能しません。

マージを実行する前に、両ツリーにあるすべてのサーバの時刻が同期されていること、およびこれらのサーバがタイムソースとして同じタイムサーバを使用していることを確認します。ただし、ターゲットツリーの時刻は5分以内であればソースツリーの時刻より進んでいてもかまいません。

一般に、1つのツリー上に存在できるタイムサーバは、リファレンスタイムサーバまたはシングルタイムサーバのどちらか1つだけです。同様に、マージ後のツリー上に存在できるタイムサーバも、リファレンスタイムサーバまたはシングルタイムサーバのどちらか1つだけです。

マージする両ツリーのそれぞれにリファンレスタイムサーバまたはシングルタイムサーバがある場合は、どちらかのツリーの設定をもう一方のツリーにあるリファンレスタイムサーバまたはシングルタイムサーバに変更して、マージ後のツリー上でリファレンスタイムサーバまたはシングルタイムサーバが1つだけになるようにします。

タイムサーバのタイプの詳細については、『*OESPlanningandImplementationGuide(OES プラニングおよび実装ガイド)* (http://www.novell.com/documentation/oes11/oes_implement_lx/data/time.html)』の「Time Services (時刻サービス)」を参照してください。

2つのツリーのマージ

すべてのメニューオプションの機能を使用できるようにするには、Treeパーティションのマスタレプリカが格納されているサーバ上でDSMergeを実行します。

マスタレプリカが格納されている場所が不明な場合は、マスタレプリカを必要とする操作を実行すると、正確なサーバ名がプロンプトに表示されます。

マージ操作を実行するには、次のどちらかの方法を使用します。

- iManager
- コマンドラインクライアント

  詳細については、311 ページの 「クライアントを使用したツリーのマージ」を参照してください。

大きなツリーをマージするときは、Treeオブジェクト直下にあるオブジェクトの数が少ないほうのツリーをソースツリーとして指定したほうが、処理速度が大幅に速くなります。Treeオブジェクトの直下にあるオブジェクトすべてに対して新しいパーティションが作成されるため、この方法をとると、マージ実行時に分割されるパーティションの数が少なくてすむためです。

ソースツリーの名前はマージ後には存在しなくなります。したがって、場合によっては、クライアントワークステーションの環境設定を変更する必要があります。Novell Client for DOS/Windowsの場合は、net.cfgファイルの優先ツリーステートメントおよび優先サーバステートメントを確認します。Novell Client for Windowsの場合は、クライアントのプロパティページにある優先ツリーステートメントおよび優先サーバステートメントを確認します。

優先サーバが使用されている場合は、ツリーのマージやツリー名の変更を行っても、そのクライアントは名前によってサーバにログインした状態のままなので操作による影響はクライアント側にはありません。優先ツリーが使用されている場合は、ツリーのマージやツリー名の変更を行うと、元のツリー名はなくなります。マージを行った後にはターゲットツリーの名前だけが残ります。優先ツリーの名前を新しいツリー名に変更します。

ヒント: ターゲットツリーの名前はマージの結果作成されるツリーの名前としてそのまま残るので、アップデートする必要のあるクライアントワークステーションの数を少なくするには、クライアントワークステーションの数が多い方のツリーをターゲットツリーとして指定します。または、マージ操作の後でツリー名を変更して、最終的なツリー名が接続されているクライアントワークステーションの数が多い方のツリーに一致するようにします。詳細については、310 ページの 「ツリー名の変更」を参照してください。

次の前提条件の一覧を使用して、マージ操作の準備ができているか確認します。

- ❒ iManagerによるソースツリーのサーバへのアクセス権があること
- ❒ マージする両ツリーのTreeオブジェクトに対するスーパバイザオブジェクト権を持つ管理者オブジェクトの名前とパスワードがわかっていること

- ❒ 2つのツリーのeDirectoryデータベースがバックアップされていること
- ❒ 両ツリー内のすべてのサーバが同期されていて、同じタイムソースを使用していること
- ❒ (オプション)ツリー内のサーバがすべて動作可能であること(動作不能状態のサーバは動作可能になった時点で自動的に更新されます)。
- ❒ 「300 ページの 「ソースツリーとターゲットツリーを準備する」」に表示された前提条件を確認すること

マージプロセス自体には2、3分しかかかりませんが、次のような場合は、付随的な作業が必要になるため、マージ操作が完了するまでに要する時間が長くなります。

- Treeオブジェクトの下に多数のオブジェクトがあり、パーティションに分ける必要がある
- ソースツリーに多数のサーバがあり、ソースツリーのツリー名を変更する必要がある

2つのツリーをマージするには、次を実行します。

1. NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**eDirectoryの保守**］>［**ツリーのマージ**］の順にクリックします。
3. マージを実行するサーバ(これがソースツリーになります)を指定し、［**次へ**］をクリックします。
4. そのサーバに対する認証を行ってから、［**次へ**］をクリックします。
5. ソースツリーの管理者ユーザ名とパスワードを指定します。
6. ターゲットツリー名、管理者ユーザ名、およびパスワードを指定してから、［**開始**］をクリックします。

   ツリーのマージウィザードのステータスウィンドウが表示され、マージの進行状況が表示されます。
7. マージプロセスから返された情報とともに「完了」メッセージが表示されたら、［**閉じる**］をクリックして終了します。

注: 親パーティションが非EBA対応で、子パーティションがEBA対応の場合は、この2つのパーティションをマージしないでください。これを行うと、EBA機能が停止する可能性があります。

マージ後の作業

2つのツリーをマージした後は、状況に応じて次の手順を行ってください。

1. すべてのツリー名が正しく変更されたことを確認します。
2. マージ操作によって作成された新しいパーティションを確認します。

   新しいツリーに小さいパーティションが多数存在する場合や、関連する情報が格納されたパーティションが複数存在する場合は、これらのパーティションをマージすることもできます。詳細については、153 ページの 「パーティションのマージ」を参照してください。
3. DSMerge実行前にリーフオブジェクトや別名をツリーから削除した場合は、ツリーにそれらのリーフオブジェクトや別名を再作成します。
4. eDirectoryツリーのパーティション構成を調べます。

   マージ後のツリー内でのレプリカの位置はソースツリー内での位置と異なる場合があります。パーティション構成の変更や検査は慎重に行ってください。
5. クライアントワークステーションの環境設定を更新します。

Novell Client for Windowsの場合は、クライアントのプロパティページの優先ツリーステートメントおよび優先サーバステートメントを確認するか、またはターゲットツリーの名前を変更します。

優先サーバが使用されている場合は、ツリーのマージやツリー名の変更を行っても、そのクライアントは名前によってサーバにログインした状態のままなので操作による影響はクライアント側にはありません。優先ツリーが使用されている場合は、ツリーのマージやツリー名の変更を行うと、元のツリー名はなくなります。マージを行った後にはターゲットツリーの名前だけが残ります。優先ツリーの名前を新しいツリー名に変更します。

ソースツリーのTreeオブジェクトのACL(アクセス制御リスト)は保持されます。したがって、このTreeオブジェクトに対してソースツリーのユーザが持つ管理者権限は、引き続き有効です。

マージ後も、両ツリーの管理者ユーザは存在したままで、それぞれのコンテナオブジェクトによって固有のものとして識別されます。

セキュリティ上必要であれば、2つの管理者ユーザオブジェクトの一方を削除するか、両オブジェクトの権利を制限することもできます。

サーバツリーの結合

［**ツリーの結合**］オプションを使用すると、単一サーバソースツリーのTreeオブジェクトを、ターゲットツリーにある指定のコンテナに結合できます。結合が完了すると、ソースツリーのツリー名は、ターゲットツリーのツリー名になります。

結合操作中に、DSMergeによってソースツリーのTreeオブジェクトのオブジェクトクラスがドメインに変更され、新しいパーティションが作成されます。新しいドメインオブジェクトは、新しいパーティションのパーティションルートになります。ソースツリーのツリーオブジェクトの下にあるすべてのオブジェクトはドメインオブジェクトに属すことになります。

ターゲットツリーの管理者には、作成されたツリーのルートコンテナに対する権利があるため、結合後のソースツリーのルートに対する権利もあります。

注: 権利継承が再計算されて有効になるには、数時間かかる可能性があります。この時間は、ツリーの複雑さ、サイズ、パーティション数によって異なります。

ソースツリーの管理者は、新しく作成されたドメインオブジェクト内でのみ権利を所有します。

図 10-3と図 10-4に、ツリーを特定のコンテナに結合した場合の変化を示します。

図 10-3　結合前のeDirectory ツリー

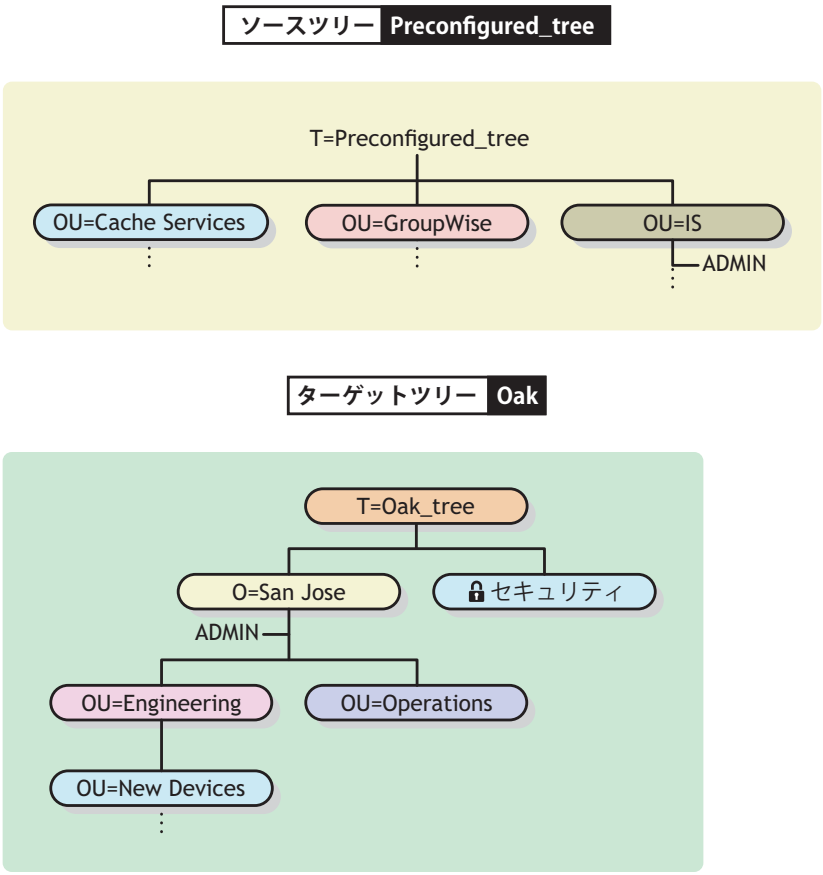
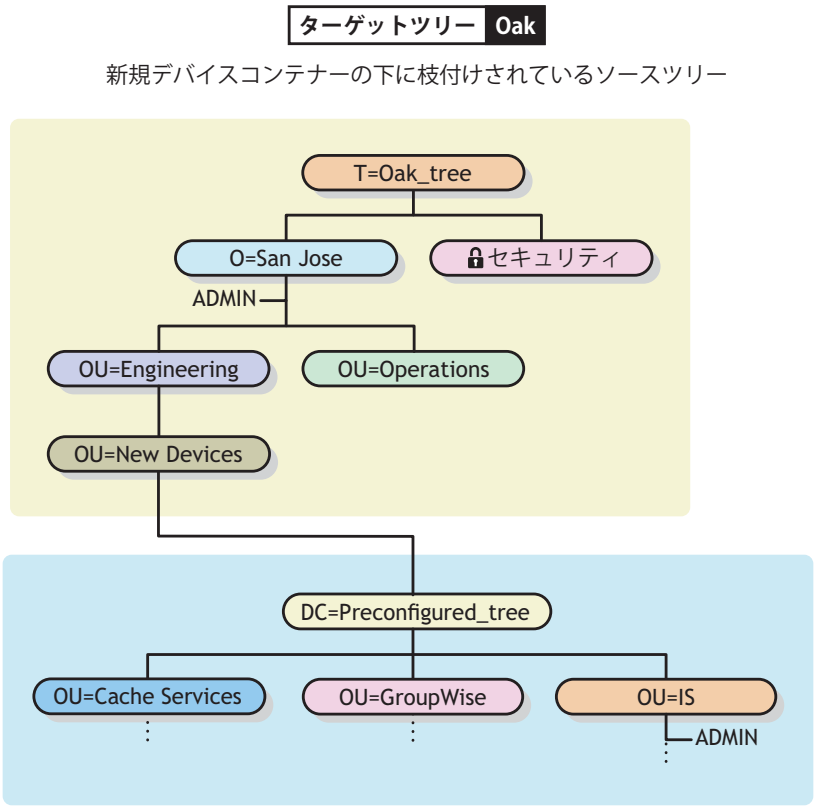


図 10-4 結合後のeDirectoryツリー



このセクションでは、次の情報について説明します。

- 306 ページの 「コンテキスト名の変更について」
- 307 ページの 「ソースツリーとターゲットツリーを準備する」
- 308 ページの 「結合操作における包含要件」
- 309 ページの 「ソースツリーとターゲットツリーを結合する」

コンテキスト名の変更について

ソースツリーをターゲットツリーのコンテナに結合すると、ソースツリー内にあるオブジェクトの識別名の後ろに、ソースツリー名、続いてソースツリーをマージしたターゲットツリーコンテナの識別名が追加されます。相対識別名は変わりません。

たとえば、区切り文字としてドットを使用している場合、ソースツリーPreconfigured_tree内にあるオブジェクトAdminのタイプ付きの名前は次のようになります。

```
CN=Admin.OU=IS.T=Preconfigured_tree
```

Preconfigured_treeをOak_treeのNew Devicesコンテナにマージした後は、Adminのタイプ付きの名前は次のようになります。

```
CN=Admin.OU=IS.DC=Preconfigured_tree.OU=Newdevices.
OU=Engineering.O=Sanjose.T=Oak_tree.
```

注: コンテナDNを含め、どのタイプのDNでも、使用できる最大文字数は、255文字です。この制限は、1つのツリーのルートをターゲットツリーの下端近くにあるコンテナに結合する場合に特に重要です。

Oak_treeの後にある最後のドット(Oak_tree.)は、この識別名を構成する最後の要素がツリー名であることを示しています。このドットを省略する場合は、ツリー名も省略します。

ソースツリーとターゲットツリーを準備する

結合操作を開始する前に、その結合操作の影響を受けるすべてのサーバが安定した状態であることを確認する必要があります。次の表では、結合前のソースツリーとターゲットツリーの準備に関する前提条件について説明します。

必要条件	必要な措置
ソースツリー内のサーバが1つである。	ソースツリーから、1つだけ残してすべてのサーバを削除します。
ソースツリーのTreeオブジェクトに別名またはリーフオブジェクトが存在しない。	ソースツリーのTreeオブジェクトに存在する別名またはリーフオブジェクトを削除します。
結合コンテナ内に同じ名前がない。	同じ名前がある場合は、ターゲットツリーの結合コンテナ内のオブジェクトまたはソースツリー内のオブジェクト名を変更します。 オブジェクト名を変更したくない場合は、コンテナの1つから同じツリー内の別のコンテナにオブジェクトを移動し、空になったコンテナをDSMerge実行前に削除します。詳細については、101ページの第3章「オブジェクトの管理」を参照してください。 同じペアレントオブジェクトの直下でないコンテナオブジェクトの場合は、両ツリーに同じコンテナオブジェクトがあってもかまいません。オブジェクトは、直接のコンテナオブジェクトによって識別されます。
ソースツリーおよびターゲットツリーのeDirectoryバージョンが8.51 SP2a以降である。	DSMergeは、eDirectoryの適切なバージョンを検索します。使用できるバージョンが見つからない場合、DSMergeはエラーを返します。eDirectoryの最新バージョンは、NetIQダウンロードページ (https://www.netiq.com/products)から入手できます。
ターゲットツリーを結合するコンテナがレプリカを持たないパーティション（単一サーバパーティション）にある。	ターゲットコンテナに複数のレプリカがある場合は、次のうち1つを実行します。 ◆ このコンテナに関連付けられたパーティションをマスタレプリカにし、その他のレプリカを削除します。 ◆ または、ターゲットツリーの結合コンテナを別のパーティションとして切り離し、レプリカを削除します。 結合が完了した後は、パーティションの関連付けを再構築できます。

必要条件	必要な措置
ターゲットコンテナを保持するサーバがルートパーティションのレプリカも保持している。	サーバがルートのレプリカを保持していない場合、ディレクトリはターゲットツリーの管理権を確認できないので、結合は失敗し、エラー「-672 アクセスできません」が表示されます。 iManagerを使用してルートのレプリカを追加します。詳細については、156 ページの 「レプリカを追加する」を参照してください。
ソースツリーおよびターゲットツリーのスキーマが同じである。	DSMergeで［結合］オプションを実行します。出力されるレポートからスキーマに問題があることがわかった場合は、ターゲットツリー上でDSRepairを実行してソースツリーからスキーマをインポートします。 結合操作によって、自動的にスキーマがターゲットツリーからソースツリーにインポートされます。 DSMergeを再実行します。
単一のツリーだけが、ツリーのルートの下位にセキュリティコンテナを保持できる。	ソースツリーおよびターゲットツリーの両方がセキュリティコンテナを保持している場合、837ページの付録 A「NMASの注意事項」で説明されている手順に従って、一方のコンテナを削除します。
ソースツリーの時刻基準は、再設定する必要があります。	ソースツリーは、ターゲットツリーのサーバからタイムソースを取得するように、セカンダリサーバとして設定される必要があります。 Timesyncを再設定する場合は、『*OES Planning and Implementation Guide*』の「Configuring and Administering Time Synchronization (http://www.novell.com/documentation/oes11/oes_implement_lx/data/time.html#time-cfgnadmin)」を参照してください。

結合操作における包含要件

ソースツリーをターゲットツリーのコンテナに結合するには、ターゲットツリーのコンテナでソースツリーの受け入れ準備を整えておく必要があります。ターゲットツリーのコンテナは、クラスドメインのオブジェクトを包含できなければなりません。包含に問題があると、結合操作中に「-611 不正な包含ルールです」というエラーが発生します。

次の表の情報を使用して、DSRepairを実行して包含リストを変更する必要があるかどうかを判断します。

ターゲットツリーのコンテナ要件	ターゲットツリーのコンテナオブジェクトが、包含リスト内のドメインオブジェクトを包含していること。 これを確認するには、［**iMonitor**］>［**スキーマ**］を使用します。包含リストにドメインが包含されていない場合、DSRepairを実行してスキーマを拡張します。
ソースツリーの要件	結合操作によって、ソースツリーのルートがクラスツリールートからクラスドメインに変更されます。Treeの下位オブジェクトはすべて、スキーマルールに従い、クラスドメインに適切に包含されている必要があります。 これを確認するには、［**iMonitor**］>［**スキーマ**］を使用します。包含リストにドメインが包含されていない場合、DSRepairを実行してスキーマを拡張します。

包含要件が満たされていない場合は、DSRepairを実行してスキーマを修正します。

1. NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**eDirectoryの保守**］>［**スキーマの保守**］の順にクリックします。
3. 操作を実行するサーバを指定し、［**次へ**］をクリックします。
4. ユーザ名、パスワード、および操作を実行するサーバのコンテキストを指定し、［**次へ**］をクリックします。
5. ［**オプションスキーマ拡張機能**］をクリックし、［**開始**］をクリックします。
6. 表示される指示に従って、操作を完了します。

ソースツリーとターゲットツリーを結合する

前提条件を満たしていることを確認し、DSMergeを使用して結合を実行します。

1. NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**eDirectoryの保守**］>［**ツリーの結合**］の順にクリックします。
3. 結合を実行するサーバ(これがソースツリーになります)を指定し、［**次へ**］をクリックします。
4. そのサーバに対する認証を行ってから、［**次へ**］をクリックします。
5. ソースツリーの管理者名とパスワード、ターゲットツリー名、およびターゲットツリーの管理者名とパスワードを指定します。
6. ［**Start**］をクリックします。

   ツリーの結合ウィザードのステータスウィンドウが表示され、結合の進行状況が表示されます。結合処理から戻された情報とともに、最後に「完了」メッセージが最後に表示されます。
7. ［**閉じる**］をクリックして終了します。

ツリー名の変更

マージする2つのツリーの名前が同じ場合は、どちらかの名前を変更する必要があります。

ここで名前を変更できるのはソースツリーだけです。ターゲットツリーの名前を変更するには、ターゲットツリー上のいずれかのサーバに対してNetIQ iManagerのツリー名の変更ウィザードを実行する必要があります。

ツリー名を変更しても、バインダリコンテキストは自動的には変更されません。autoexec.ncfファイルで設定されたバインダリコンテキストセットにもツリー名(例: SET Bindery Context = O=n.*test_tree_name*)が含まれるため、ツリー名が最近変更されたサーバでは、ツリー名が変更される前のコンテキストは使用されません。

したがって、ツリー名を変更した場合、クライアントワークステーションの環境設定の変更が必要になる可能性があります。Novell Client for DOS/Windowsの場合は、net.cfgファイルの優先ツリーステートメントおよび優先サーバステートメントを確認します。Novell Client for Windowsの場合は、クライアントのプロパティページにある優先ツリーステートメントおよび優先サーバステートメントを確認します。

優先サーバが使用されている場合は、ツリーのマージやツリー名の変更を行っても、そのクライアントは名前によってサーバにログインした状態のままなので操作による影響はクライアント側にはありません。優先ツリーが使用されている場合は、ツリーのマージやツリー名の変更を行うと、元のツリー名はなくなります。マージを行った後にはターゲットツリーの名前だけが残ります。優先ツリーの名前を新しいツリー名に変更します。

2つのツリーをマージする場合、ターゲットツリーの名前はマージの結果作成されるツリーの名前としてそのまま残るので、アップデートする必要のあるクライアントワークステーションの数を少なくするには、クライアントワークステーションの数が多い方のツリーをターゲットツリーとして指定します。

または、マージの後でツリー名を変更して、最終的なツリー名がクライアントワークステーションの数が多い方のツリーに一致するようにすることもできます。

マージ後のツリーの名前は、元のソースツリーの名前に変更することもできます。このオプションを選択する場合は、ターゲットツリーにあるクライアントワークステーションのnet.cfgファイルを更新する必要があります。

次の前提条件の一覧を使用して、リネーム操作の準備ができているか確認します。

- ❒ ソースツリー上のサーバコンソールへのアクセス権があること、またはこのサーバとのRCONSOLEセッションが確立済みであること
- ❒ ソースツリーのTreeオブジェクトに対するスーパバイザオブジェクト権があること
- ❒ (オプション)ツリー内のサーバがすべて動作可能であること(動作不能状態のサーバは動作可能になった時点で自動的に更新されます)。

ツリー名を変更するには、次を実行します。

1. NetIQ iManagerで、［**役割およびタスク**］オプションをクリックします。
2. ［**eDirectoryの保守**］>［**ツリー名の変更**］の順にクリックします。
3. ツリー名の変更ウィザードを実行するサーバ(ターゲットツリー内のサーバ)を指定し、［**次へ**］をクリックします。
4. そのサーバに対する認証を行ってから、［**次へ**］をクリックします。
5. 新しいツリー名、管理者ユーザ名、およびパスワードを指定します。

6 ［Start］をクリックします。

ツリー名の変更ウィザードのステータスウィンドウが表示され、リネーム処理の進行状況が表示されます。

7 名前変更プロセスから返された情報とともに「完了」メッセージが表示されたら、［閉じる］をクリックして終了します。

注: EBA対応のeDirectoryツリーの名前を変更した後、ebaclientinitユーティリティを使用して、.eba.p12ファイルをダウンロードします。詳細については、509 ページの 「ebaclientinitユーティリティの実行」を参照してください。

クライアントを使用したツリーのマージ

eMBox(eDirectory Management Toolbox)クライアントはコマンドラインJavaクライアントで、これを使用するとDSMergeにリモートアクセスできます。emboxclient.jarファイルは、eDirectoryの一部としてサーバにインストールされます。JVMをインストールしていれば、どのコンピュータでも実行できます。クライアントの詳細については、「584ページの「コマンドラインクライアントの使用」」を参照してください。

DSMerge eMToolを使用する

1 コマンドラインで次のように入力して、対話式モードでクライアントを実行します。

```
java -cp path_to_the_file/emboxclient.jar  -i
```

(クラスパスにすでにemboxclient.jarファイルが設定されている場合は、「java -i」とだけ入力します)。

クライアントのプロンプトが次のように表示されます。

```
Client>
```

2 DSMergeを実行する(ソースツリーになる)サーバにログインするには、次のコマンドを入力します。

```
login -sserver_name_or_IP_address -pport_number
-uusername.context -wpassword -n
```

ポート番号は通常80または8028です。ただし、すでにそのポートを使用しているWebサーバが存在する場合は異なります。-nオプションを使用すると、非セキュア接続が開始されます。

クライアントはログインが成功したかどうかを表示します。

3 次の構文を使用してマージコマンドを入力します。

dsmerge.*task options*

たとえば、「dsmerge.m -uadmin -ptest -TApple -Uadmin -Ptest」と入力すると、ターゲットツリーApple (ターゲットツリーのユーザ名はAdmin、ユーザパスワードはtest)が、現在ログインしているソースツリー(ソースツリーのユーザ名はAdmin、ユーザパスワードはtest)にマージされます。

「dsmerge.g -uadmin -ptest -TOrange -Uadmin -Ptest -CFruit」と入力すると、現在ログインしているソースツリー(ソースツリーのユーザ名はAdmin、ユーザパスワードはtest)が、ターゲットツリーOrange(ターゲットツリーのユーザ名はAdmin、ユーザパスワードはtest)に含まれるコンテナFruitに結合されます。

各スイッチの間にはスペースが必要です。スイッチの順序は重要ではありません。

クライアントはDSMerge操作が成功したかどうかを表示します。

DSMergeeMToolオプションの詳細については、「312ページの 「DSMergeeMToolオプション」」を参照してください。

4 クライアントからログアウトするには、次のコマンドを入力します。

```
logout
```

5 クライアントを終了するには、次のコマンドを入力します。

```
exit
```

DSMerge eMToolオプション

次の表に、DSMerge eMToolオプションを示します。クライアントでlist -t dsmergeコマンドを使用して、DSMergeオプションの詳細を表示することもできます。詳細については、588 ページの「eMToolとそのサービスを表示する」を参照してください。

マージ操作	クライアントのコマンド
ツリーの名前が変更できるかどうかチェックする	dsmerge.pr -u*User* -p*User_password* -n*New_tree_name*
ツリー名を変更する	dsmerge.r -u*User* -p*User_password* -n*New_tree_name*
2つのツリーがマージできるかチェックする	dsmerge.pm -u*Source_tree_user*-p*Source_tree_user_password* -T*Target_tree_name* -U*Target_tree_user* -P*Target_tree_password*
2つのツリーのマージ	dsmerge.m -u*Source_tree_user*-p*Source_tree_user_password* -T*Target_tree_name*-U*Target_tree_user* -P*Target_tree_password*
ソースツリーがターゲットツリーのコンテナに結合できるかチェックする	dsmerge.pg -u*Source_tree_user* -p*Source_tree_user_password* -T*Target_tree_name* -U*Target_tree_user* -P*Target_tree_password* -C*Target_tree_container*
ソースツリーをターゲットツリーのコンテナに結合する	dsmerge.g -u*Source_tree_user* -p*Source_tree_user_password* -T*Target_tree_name* -U*Target_tree_user* -P*Target_tree_password* -C*Target_tree_container*
実行中のDSMerge操作をキャンセルする	キャンセル

11 eDirectoryのデータを暗号化する

NetIQ eDirectoryでは、次の状態にある特定のデータを暗号化できます。

- ディスクに保存されている。
- 2つ以上のeDirectoryサーバ間で転送される。そのため、機密データのセキュリティを強化できます。

次のものを暗号化することによって、データを保護できます。

- 属性: ディスクに格納されている機密データを保護する場合。

  詳細については、313 ページの 「暗号化属性」を参照してください。
- レプリケーション: eDirectoryサーバ間のレプリケーション中に機密データを保護する場合。

  詳細については、323 ページの 「暗号化レプリケーション」を参照してください。

重要: EBA (Enhanced Background Authentication)を導入すると、EBA対応のeDirectoryサーバ間でデータレプリケーションが行われる際に、自動的にデータが暗号化されます。サーバの一方がEBA対応でない場合は、暗号化複製ポリシーを設定してデータを暗号化することができます。

暗号化属性

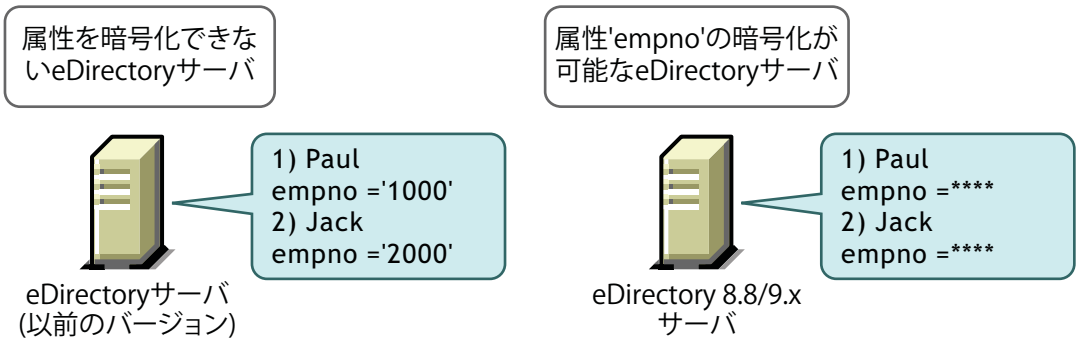
データがディスクに格納されている間は属性を暗号化してデータを保護できます。暗号化属性はサーバ固有の機能です。この機能は、銀行顧客のクレジットカード番号のような機密データを保護する必要がある場合に使用できます。

属性を暗号化すると、属性値がエンコードされます。たとえば、DIBに格納されている属性empnoを暗号化するとします。empno=1000である場合、属性値(1000)はクリアテキスト形式ではディスクに保存されません。この暗号化された値は、セキュリティ保護されたチャネルからディレクトリにアクセスした場合にのみ読み取ることができます。

方式内のすべての属性に対して暗号化を有効にすることができます。ただし、共通名(CN)属性に対してではなく、重要なデータに対してのみ暗号化を有効にすることをお勧めします。暗号化する属性の決定については、「330 ページの 「データを暗号化するときにデータの完全な安全性を確保する」」を参照してください。

Publicおよびサーバが読み込める暗号化属性へのアクセスに制限はありません。つまり、クライアントはクリアテキストを使用してこれらの属性にアクセスすることができ、ユーザはこれらの暗号化用の属性にDIBレベルでマークすることができます。スキーマで「パブリック読込み」フラグが設定されている属性に対して暗号を有効にしても、セキュアではない手段によるその属性へのアクセスは防止されません。

図 11-1 暗号化属性



eDirectory内のデータは次の方法で保存できます。

- DIB(Data Information Base)またはデータベースに保存
- バックアップデータとして保存
- LDIFファイル

属性を暗号化するには、暗号化属性ポリシーを作成してサーバに適用します。

属性を暗号化するには、iManagerで次の操作を実行します。

1 暗号化属性ポリシーを作成して定義します。

1a 暗号化する属性を選択します。

1b 属性の暗号化スキームを選択します。

詳細については、「317ページの 「暗号化属性ポリシーを作成して定義する」」を参照してください。

2 サーバに暗号化属性ポリシーを適用します。

詳細については、「317 ページの 「暗号化属性ポリシーを適用する」」を参照してください。

LDAPを使用して属性を暗号化することもできます。

詳細については、「317ページの 「LDAPを使用して暗号化属性ポリシーを管理する」」を参照してください。

注: 暗号化属性ポリシーの割り当ては、リンバの実行時に有効になります。

ベストプラクティスとして、次の推奨事項に従うことをお勧めします。

- 暗号化する属性のうち、重要な属性のみをマークします。暗号化する属性すべて(パブリックやサーバが読み込める属性など)にマークはしないでください。
- 暗号化する属性をマークする場合は、強力な暗号化アルゴリズムであるAESを使用してください。

このセクションでは、次の情報について説明します。

- 321 ページの 「暗号化属性を表示する」
- 322 ページの 「バックアップデータを暗号化/復号化する」
- 322 ページの 「暗号化属性を含むDIBファイルセットのクローンを作成する」
- 322 ページの 「レプリカリングにeDirectory サーバを追加する」
- 322 ページの 「下位互換性」
- 323 ページの 「暗号化属性に移行する」
- 323 ページの 「暗号化属性のレプリカを作成する」

暗号化方式を使用する

eDirectory では、属性のセキュリティを確保するために、次の暗号化方式がサポートされています。

- AED(Advanced Encryption Standard)
- トリプルDES
- DES(Data Encryption Standard)

1つの暗号化属性ポリシーに含まれる各属性に対して、個別に暗号化方式を選択することもできます。たとえば、EP1という暗号化属性ポリシーに含まれる属性cubenoに対しては暗号化方式としてAESを選択し、属性empnoに対してはトリプルDESを選択することができます。詳細については、「317 ページの 「暗号化属性ポリシーを作成して定義する」」を参照してください。

属性の暗号化方式を変更するには、暗号化属性ポリシーを編集します。暗号化されている属性を復号化することもできます。詳細については、「317ページの「暗号化属性ポリシーを編集する」」を参照してください。

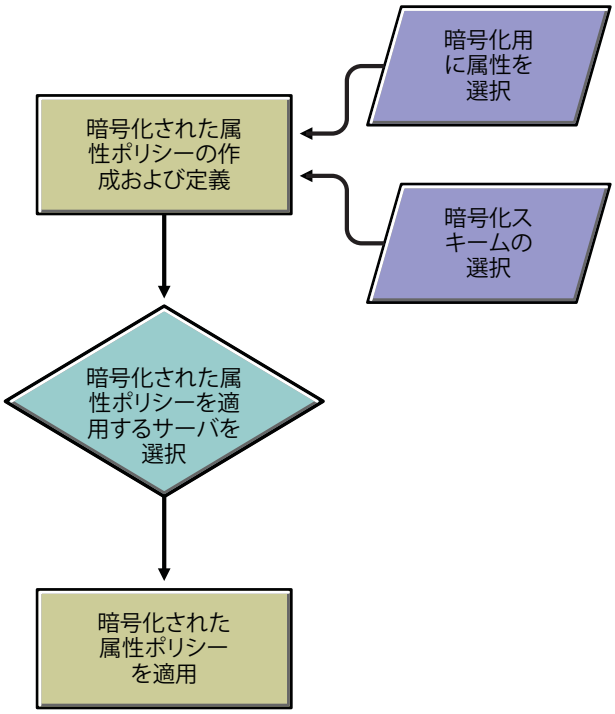
レプリカリング内の各サーバに対して、個別に暗号化方式を選択することもできます。たとえば、属性を暗号化する際に、Server1ではAESを使用し、Server2ではトリプルDESを使用し、Server3では暗号化方式を使用しないというような設定が可能です。

暗号化属性ポリシーを管理する

ポリシーを作成して定義し、サーバに適用することで、属性の暗号化を管理できます。

暗号化属性ポリシーを定義するには、暗号化する属性と暗号化方式を選択します。

図 11-2 属性を暗号化する



暗号化属性ポリシーの管理には、iManagerを使用できます。この節では、次のトピックについて説明します。

- 316 ページの 「iManagerを使用して暗号化属性ポリシーを管理する」
- 317 ページの 「LDAPを使用して暗号化属性ポリシーを管理する」
- 319 ページの 「暗号化属性ポリシーをコピーする」
- 319 ページの 「パーティション操作」

iManagerを使用して暗号化属性ポリシーを管理する

このセクションでは、次の手順について説明します。

- 317 ページの 「暗号化属性ポリシーを作成して定義する」
- 317 ページの 「暗号化属性ポリシーを編集する」
- 317 ページの 「暗号化属性ポリシーを適用する」
- 317 ページの 「暗号化属性ポリシーを削除する」

暗号化属性がeDirectoryサーバに存在する場合、iManagerは次の方法で動作します。

1. クリアテキストまたはセキュリティで保護されたチャネルを介して、暗号化属性の読み込み、表示、修正を行うことはできません。
2. クリアテキストまたはセキュリティで保護されたチャネルでiManagerを介して、暗号化属性以外の属性を持つエントリの属性の読み込み、表示、修正を行うことはできません。これは、エントリ全体がブロックされていることを意味します。

暗号化属性ポリシーを作成して定義する

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［eDirectoryの暗号化］>［Encryption Attributes］の順にクリックします。

3 暗号化属性ポリシー管理ウィザードで、［ポリシーの作成、編集、および割り当てを行います］を選択します。

4 暗号化属性ポリシー管理ウィザードの指示に従って、ポリシーを作成し定義します。

ウィザードの各段階で、［ヘルプ］が利用できます。

暗号化属性ポリシーを編集する

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［eDirectoryの暗号化］>［Encryption Attributes］の順にクリックします。

3 暗号化属性ポリシー管理ウィザードで、［ポリシーの編集］を選択します。

4 暗号化属性ポリシー管理ウィザードの指示に従って、ポリシーを編集します。

ウィザードの各段階で、［ヘルプ］が利用できます。

暗号化属性ポリシーを適用する

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［eDirectoryの暗号化］>［Encryption Attributes］の順にクリックします。

3 暗号化属性ポリシー管理ウィザードで、［ポリシーの作成、編集、および割り当てを行います］を選択します。

4 暗号化属性ポリシー管理ウィザードの指示に従って、ポリシーを適用します。

ウィザードの各段階で、［ヘルプ］が利用できます。

暗号化属性ポリシーを削除する

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［eDirectoryの暗号化］>［Encryption Attributes］の順にクリックします。

3 暗号化属性ポリシー管理ウィザードで、［ポリシーの削除］を選択します。

4 暗号化属性ポリシー管理ウィザードの指示に従って、ポリシーを削除します。

ウィザードの各段階で、［ヘルプ］が利用できます。

LDAPを使用して暗号化属性ポリシーを管理する

重要: 暗号化属性を管理するには、LDAPではなくiManagerを使用することを強くお勧めします。

このセクションでは、次の手順について説明します。

- 318 ページの 「暗号化属性ポリシーを作成して定義する」
- 318 ページの 「暗号化属性ポリシーを編集する」
- 319 ページの 「暗号化属性ポリシーを適用する」
- 319 ページの 「暗号化属性ポリシーを削除する」

注: LDIFで暗号化する属性をマーキングする場合は、属性と方式のリストではなく、属性と方式のペアを指定する必要があります。これは暗号化属性に付随する現行の制約です。

暗号化属性ポリシーを作成して定義する

1 暗号化属性ポリシーを作成します。

たとえば、AE Policy- test-serverという暗号化属性ポリシーの場合は次のようになります。

```
dn: cn=AE Policy - test-server, o=novell
changetype: add
objectClass: encryptionPolicy
```

2 作成したポリシーオブジェクトにattrEncryptionDefinition属性を追加して、暗号化する属性をマーキングします。

たとえば、暗号化する属性の名前がCRIDの場合は、次のように暗号化方式と属性名を指定します。

```
dn: cn=AE Policy - test-server, o=novell
changetype: modify
add: attrEncryptionDefinition
attrEncryptionDefinition: aes$CRID
```

注: 属性名の指定には、その属性のNDS名を使用します。eDirectoryでは多くの属性がLDAP名とNDS名の両方を持っています。ここでは、NDS名を必要とする属性名を指定してください。

3 attrEncryptionRequiresSecure属性をポリシーに追加します。

この属性の値によって、暗号化属性にアクセスする際にセキュリティ保護されたチャネルの使用を常に要求するかどうかが指定されます。この値が0の場合、常には要求しないことを示します。この値が1の場合は、常に要求することを示します。

次に例を示します。

```
dn: cn=AE Policy - test-server, o=novell
changetype: modify
add: attrEncryptionRequiresSecure
attrEncryptionRequiresSecure: 0
```

4 NCPサーバにポリシーを関連付けます。

test-serverというNCPサーバの場合は次のようになります。

```
dn: cn=test-server, o=novell
changetype: modify
add: encryptionPolicyDN
encryptionPolicyDN: cn=AE Policy - test-server, o=novell
```

暗号化属性ポリシーを編集する

次のLDIFファイルは、attrEncryptionRequireSecure属性の値を変更することで暗号化属性ポリシーを編集する方法を示しています。

```
dn: cn=AE Policy - test-server, o=novell
changetype: modify
replace: attrEncryptionRequiresSecure
attrEncrytionRequiresSecure: 1
```

暗号化属性ポリシーを適用する

次のLDIFファイルは、AE Policy-test-serverという暗号化属性ポリシーをtest-serverというサーバに適用する方法を示しています。

```
dn: cn=test-server, o=novell
changetype: modify
add: encryptionPolicyDN
encryptionPolicyDN: cn=AE Policy - test-server, o=novell
```

暗号化属性ポリシーを削除する

次のLDIFファイルは、暗号化属性ポリシーを削除する方法を示しています。

```
dn: cn=AE Policy - test-server, o=novell
changetype: delete
```

注: LDAPを使用して暗号化属性を管理する方法の詳細については、373 ページの 「LinuxでのLDAPツールの使用」および165 ページの 「NetIQインポート/エクスポート変換ユーティリティ」を参照してください。

暗号化属性ポリシーをコピーする

暗号化属性ポリシーをコピーして多数のサーバにまったく同じ設定内容を反映させることができます。ポリシーは、オブジェクトとしてeDirectoryに保存されます。

iManagerを使用してポリシーオブジェクトをコピーする手順については、105 ページの 「オブジェクトをコピーする」を参照してください。

パーティション操作

2つのパーティションをマージすると、ペアレントのポリシーがマージ後のパーティションで保持されます。パーティションを分割すると、ペアレントのポリシーがチャイルドパーティションに継承されます。

推奨: eDirectoryは、暗号化のマークが付いているべきでない、いくつかの属性を内部操作用に保管しています。これらの属性に暗号化のマークが付けられると、eDirectoryの一部の機能が壊れるか、期待通りの動作をしなくなる可能性があります。

暗号化のマークを付けてはならない属性は次のとおりです。

- federationBoundaryType
- ボリューム
- ACL
- federationBoundary
- member
- federationControl
- federationSearchPath
- encryptionPolicyDN
- indexDefinition
- dgIdentity

- dgAllowUnknown
- agTimeout
- Host Server
- hostResourcePath
- ndsPredicateState
- ndsStatusExternalReference
- ndsStausLimber
- ndsStatusSchema

上記のリストはすべてを網羅しているわけではありませんが、ここにリストされた属性と同様の属性には、暗号化のマークを付けないでください。

暗号化属性にアクセスする

属性を暗号化すると、暗号化属性へのアクセスも保護されます。これは、eDirectoryが、暗号化された属性へのアクセスを、セキュアチャネル(LDAPセキュアチャネル、NCPセキュアチャネルなど)経由のみに制限できるからです。ただし、セキュアNCP接続を作成するために使用するDClientアプリケーションは一般利用者向けには提供されていないので、NCP接続を設定して使用できるのは、NetIQの内部顧客に限られます。

また、バックアップ(ndsbackup)ユーティリティを使用して、暗号化属性をバックアップすることもできます。

デフォルトでは、セキュリティ保護されたチャネルからしか暗号化属性にアクセスできません。

ただし、クライアントがクリアテキストで暗号化属性にアクセスできるようにするには、［常にセキュアチャネルが必要］オプションを無効にする必要があります。詳細については、320 ページの「クリアテキストチャネルから暗号化属性へのアクセスを有効/無効にする」を参照してください。

クリアテキストチャネルから暗号化属性へのアクセスを有効/無効にする

iManagerまたはLDAPのいずれかを使用して、［常にセキュアチャネルが必要］オプション(つまり、attrEncryptionRequireSecure属性)を有効または無効にすることで、クリアテキストチャネルから暗号化属性へのアクセスを有効または無効にすることができます。

このセクションでは、次のことを説明します。

- 321 ページの 「iManagerを使用してクリアテキストチャネルから暗号化属性へのアクセスを有効/無効にする」
- 321 ページの 「LDAPを使用してクリアテキストチャネルから暗号化属性へのアクセスを有効/無効にする」

iManagerを使用してクリアテキストチャネルから暗号化属性へのアクセスを有効/無効にする

iManagerを使用してクリアテキストチャネルから暗号化属性へのアクセスを有効または無効にするには、次の作業を行う際に、暗号化属性ポリシー管理ウィザードで［常にセキュアチャネルが必要］を有効または無効にします。

- 暗号化属性ポリシーを作成して定義する。
- 暗号化属性ポリシーを編集する。

LDAPを使用してクリアテキストチャネルから暗号化属性へのアクセスを有効/無効にする

LDAPを使用してクリアテキストチャネルから暗号化属性へのアクセスを有効にするには、次の属性を暗号化属性ポリシーに追加します。

attrEncryptionRequiresSecure

この属性を0に設定すると、セキュリティ保護されたチャネルを必ずしも使用する必要はなくなります。つまり、クリアテキストチャネルから暗号化属性にアクセスできます。この属性を1に設定すると、セキュリティ保護されたチャネルの使用が常に要求されるようになります。つまり、セキュリティ保護されたチャネルからのみ暗号化属性にアクセスできます。

詳細については、「318 ページのステップ 3」を参照してください。

暗号化属性を表示する

暗号化されている属性が表示されるかどうかは、［常にセキュアチャネルが必要］オプションが有効になっているかどうかによって決定されます。つまり、暗号化属性にアクセスする際にセキュリティ保護されたチャネルを使用するかどうかによって決まります。

- 321 ページの 「iManagerを使用して暗号化属性を表示する」
- 321 ページの 「DSBrowseを使用して暗号化属性を表示する」
- 322 ページの 「SNMPトラップ」

iManagerを使用して暗号化属性を表示する

［常にセキュアチャネルが必要］が有効になっている場合は、暗号化属性を表示できません。エラー「–6089」が返されます。これは、暗号化属性にアクセスする際にセキュリティ保護されたチャネルを使用する必要があることを示しています。

［常にセキュアチャネルが必要］が無効になっている場合は、iManagerで暗号化属性値を表示できます。

詳細については、257 ページの 「ツリー内のオブジェクトの参照」を参照してください。

DSBrowseを使用して暗号化属性を表示する

［常にセキュアチャネルが必要］オプションが有効になっている場合、つまり、暗号化属性にアクセスする際にセキュリティ保護されたチャネルの使用が常に要求される場合は、暗号化されたエントリの属性を表示することはできません。ただし、暗号化されていないエントリの属性は表示できます。

SNMPトラップ

暗号化属性にアクセスする際にセキュリティ保護されたチャネルの使用を常に要求するように指定している場合は、NDS®値イベントがブロックされます。値イベントに関連するトラップの値データはNULLになり、結果は-6089に設定されます。これは、暗号化属性の値を取得するために、セキュリティ保護されたチャネルを使用する必要があることを示します。次のトラップの値データはNULLになります。

- ndsAddValue
- ndsDeleteValue
- ndsDeleteAttribute

バックアップデータを暗号化/復号化する

暗号化属性を含むサーバ上のデータをバックアップする際には、バックアップデータを暗号化または復号化するためのパスワードを入力するよう求められます。これには、バックアップユーティリティの-Eオプションを使用して簡単に対応できます。詳細については、ndsbackupのマニュアルページを参照してください。

データのバックアップの詳細については、「439ページの第15章「NetIQ eDirectoryのバックアップと復元」」を参照してください。

暗号化属性を含むDIBファイルセットのクローンを作成する

暗号化属性を含むeDirectoryデータベースのクローンを作成すると、DIBファイルセットのクローンにも暗号化属性値が含まれます。DIBファイルセットのクローンに含まれる値を暗号化するには、eDirectoryで使用されるキーを保護するためのパスワードを設定する必要があります。DIBファイルセットのクローンを他のサーバに配置する際には、このパスワードの入力を求められます。

詳細については、263 ページの 「DIBセットのクローンの使用事例」を参照してください。

レプリカリングにeDirectory サーバを追加する

eDirectory サーバは、レプリカが格納されたいずれかのサーバまたはすべてのサーバ上で属性が暗号化されているかどうか、あるいは［常にセキュアチャネルが必要］が有効になっているかどうかに関わらず、レプリカリングに追加できます。

eDirectory サーバをレプリカリングに追加する際の詳細については、「156 ページの 「レプリカを追加する」」を参照してください。

下位互換性

暗号化属性にアクセスするには、iManager、SNMP、DirXML®、NSureAuditなどのすべてのeDirectoryユーティリティを、セキュリティ保護されたNCP™に変更する必要があります。変更しない場合は、暗号化属性にアクセスする際にセキュリティ保護されたチャネルの使用を要求しないように指定する必要があります。詳細については、「320ページの「クリアテキストチャネルから暗号化属性へのアクセスを有効/無効にする」」を参照してください。

暗号化属性に移行する

eDirectoryをアップグレードする際は、暗号化属性ポリシーを作成して定義することで、既存の属性を暗号化できます。詳細については、315 ページの 「暗号化属性ポリシーを管理する」を参照してください。

暗号化属性のレプリカを作成する

デフォルトでは、サーバに暗号化属性が存在している場合でも、暗号化複製は無効になっています。暗号化属性を安全に複製するには、暗号化複製を有効にする必要があります。暗号化複製の設定については、「323 ページの 「暗号化レプリケーション」」を参照してください。

暗号化レプリケーション

eDirectoryでは、eDirectoryサーバ間で転送されるデータを暗号化できます。データがクリアテキスト形式で転送されなくなるため、複製時のセキュリティを強化できます。

図 11-3 *暗号化レプリケーション*

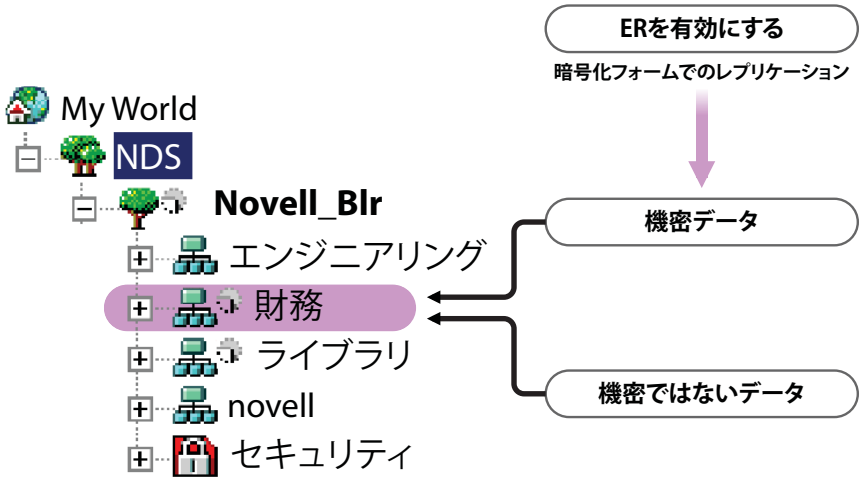


図 11-3では、「finance」と「library」がツリー内のパーティションに相当します。「finance」には、レプリケーションの際に暗号化しなければならない機密データが含まれる可能性があります。その場合は、パーティション「finance」に対して暗号化複製を有効にすることができます。「library」のように重要データが含まれていないパーティションについては、暗号化複製を有効にする必要はありません。

重要: パーティションに対して暗号化複製を有効にすると、複製処理の速度が低下する可能性があります。暗号化複製を有効または無効にするには、iManagerを使用します。

この節では、次のトピックについて説明します。

- 324 ページの 「暗号化複製の必要性」
- 324 ページの 「暗号化複製を有効にする」
- 328 ページの 「新しいレプリカをレプリカリングに追加する」

- 329 ページの 「同期と暗号化複製」
- 330 ページの 「暗号化複製ステータスを表示する」

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。

暗号化複製を有効にする

暗号化複製を有効にするには、暗号化複製を有効にするようにパーティションを設定する必要があります。設定はパーティションのルートオブジェクトに保存されます。

暗号化複製は、パーティションレベルでもレプリカレベルでも有効にすることができます。

レプリカレベルの設定は、パーティションレベルの設定よりも優先されます。つまり、次のようになります。

- 暗号化複製がパーティションレベルで有効になっていて、特定のレプリカで無効になっている場合、それらのレプリカの間の複製はクリアテキスト形式で行われます。
- パーティションレベルで暗号化複製が無効になっていて、特定のレプリカで有効になっている場合、それらのレプリカの間の複製は暗号化された形式で行われます。

表 11-1 *パーティションレベルの暗号化複製の設定を上書きする*

パーティションレベル	レプリカレベル	複製
有効	無効	暗号化されない
無効	有効	暗号化される

このセクションでは、次の手順について説明します。

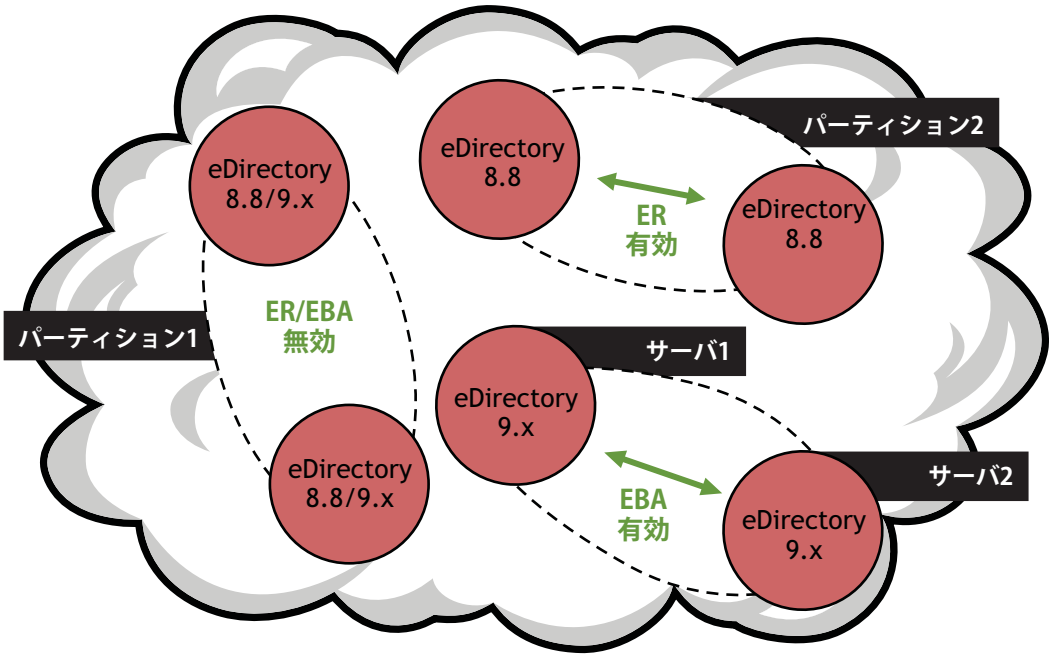
- 325 ページの 「パーティションレベルで暗号化複製を有効にする」
- 327 ページの 「レプリカレベルで暗号化複製を有効にする」

パーティションレベルで暗号化複製を有効にする

パーティションレベルで暗号化複製を有効にすると、そのパーティションをホストしているすべてのレプリカの間で行われる複製が暗号化されます。たとえば、パーティションP1のレプリカとして、R1、R2、R3、およびR4があるとします。その場合は、これらのレプリカの間のすべての複製(インバウンドとアウトバウンドの両方)を暗号化できます。

パーティションレベルで暗号化複製を有効にするには、そのパーティションをホストしているすべてのサーバでeDirectory 8.8以降が実行されている必要があります。

図 11-4　暗号化レプリケーション



レプリカレベルで暗号化複製が設定されている場合は、レプリカレベルの設定がパーティションレベルの設定よりも優先されます。「324 ページの 表 11-1」を参照してください。

下位互換性は、暗号化複製がパーティションレベルで有効になっているかどうかに依存します。詳細については、「328ページの「新しいレプリカをレプリカリングに追加する」」を参照してください。

パーティションレベルで暗号化複製を有効にするには、次のセクションで説明するように、iManagerまたはLDAPを使用します。

- 325 ページの 「iManagerを使用してパーティションレベルで暗号化複製を有効にする」
- 326 ページの 「LDAPを使用してパーティションレベルで暗号化複製を有効にする」
- 328 ページの 「パーティション操作」

iManagerを使用してパーティションレベルで暗号化複製を有効にする

1 ［**役割およびタスク**］ボタン をクリックします。

2 ［**eDirectoryの暗号化**］>［**暗号化複製**］の順にクリックします。

3 暗号化複製を有効にするパーティションを入力またはブラウズします。

4 次へをクリックします。

5 暗号化複製ウィザードで、［すべてのレプリカ同期を暗号化する］を選択します。

ウィザードの各段階で、［ヘルプ］が利用できます。

注: パーティションレベルで暗号化複製を無効にする場合は、［すべてのレプリカ同期を暗号化する］の選択を解除します。

6 完了をクリックします。

暗号化複製ウィザードでパーティション全体に対して暗号化複製を有効にした場合でも、特定のレプリカに対して暗号化複製を無効にできます。暗号化複製が無効になっているレプリカは、暗号化された形式のデータを送受信しません。［すべてのレプリカ同期を暗号化する］の選択を解除することで、パーティション全体に対して暗号化を無効にするすることもできます。

LDAPを使用してパーティションレベルで暗号化複製を有効にする

重要: iManagerを使用して暗号化複製を有効にすることを強くお勧めします。

複製を暗号化するには、属性dsEncryptedReplicationConfigを使用します。構文は次のとおりです。

```
enable/disable flag#destination replica number#source replica number
```

次のいずれかのフラグに置き換えます。

- 0: 暗号化複製が無効になります。
- 1: 暗号化複製が有効になります。

ソースレプリカ番号とターゲットレプリカ番号は、パーティションのソースレプリカ番号とターゲットレプリカ番号です。ソースレプリカ番号とターゲットレプリカ番号はどちらを先に指定しても構いません。レプリカAからBへの複製が暗号化されている場合は、BからAへの複製も暗号化されます。

注: パーティションレベルのソースレプリカ番号とターゲットレプリカ番号を0にして、フラグを1に設定した場合は、すべてのレプリカで暗号化複製が有効になります。

パーティションレベルで暗号化複製を有効にするには、dsEncryptedReplicationConfig属性の値を1#0#0に設定します。

次に、パーティションレベルで暗号化複製を有効にするためのLDIFファイルの例を示します。

```
dn: o=ou
changetype:modify
replace: dsEncryptedReplicationConfig
dsEncryptedReplicationConfig:1#0#0
```

レプリカレベルの設定は、パーティションレベルの設定よりも優先されます。詳細については、「328 ページの「LDAPを使用してレプリカレベルで暗号化複製を有効にする」」を参照してください。

レプリカレベルで暗号化複製を有効にする

レプリカレベルで暗号化複製を有効にすると、特定のレプリカの間の複製が暗号化されます。指定したレプリカの間で行われるアウトバウンドおよびインバウンドの複製が暗号化されます。

たとえば、パーティションP1のレプリカとして、R1、R2、R3、およびR4があるとします。この場合、レプリカR1とR2の間、またはR2とR4の間の複製を暗号化できます。

パーティションのレプリカの間で暗号化複製を有効にするには、レプリカの間の暗号化リンクを定義する必要があります。詳細については、「327 ページの 「iManagerを使用してレプリカレベルで暗号化複製を有効にする」」を参照してください。

1つのレプリカで暗号化複製を有効にした場合は、次のような複製が行われます。

- サーバからこのレプリカへのインバウンド同期が暗号化されます。
- このレプリカから別のサーバへのアウトバウンド同期が暗号化されます。

暗号化複製が有効になっているレプリカは、eDirectory 8.8以降のサーバ上に配置されている必要があります。レプリカリング内にあるレプリカのうち、暗号化複製が有効になっていない残りのレプリカは、eDirectory 8.8より古いバージョンのeDirectoryサーバ上に配置しても構いません。

レプリカレベルで暗号化複製を無効にするには、iManagerの暗号化複製の環境設定のウィザードで、該当するレプリカに対し［**リンクを暗号化する**］を無効にします。

レプリカレベルで暗号化複製を有効にするには、次のセクションで説明するように、iManagerまたはLDAPを使用します。

- 327 ページの 「iManagerを使用してレプリカレベルで暗号化複製を有効にする」
- 328 ページの 「LDAPを使用してレプリカレベルで暗号化複製を有効にする」

iManagerを使用してレプリカレベルで暗号化複製を有効にする

iManagerを使用してレプリカレベルで暗号化複製を有効にするには、暗号化リンクを作成します。暗号化リンクで接続されたレプリカの間では、複製が暗号化されます。暗号化リンクを作成するには、レプリカレベルで暗号化複製を設定する際に、ソースレプリカと1つまたは複数のターゲットレプリカを選択します。

たとえば、パーティションP1のレプリカとして、R1、R2、R3、およびR4があるとします。R1とR2の間の複製を暗号化するには、いずれかのレプリカをソースレプリカに指定し、他方のレプリカをターゲットレプリカに指定して暗号化リンクを作成します。

暗号化リンクを作成した後は、iManagerの暗号化複製の環境設定のウィザードで［**リンクを暗号化する**］を選択または選択解除することにより、特定のレプリカに対してこれらのリンクを暗号化することができます。詳細については、「327 ページの 「iManagerを使用してレプリカレベルで暗号化複製を有効にする」」を参照してください。

レプリカレベルで暗号化複製を有効にする

1. ［**役割およびタスク**］ボタン  をクリックします。
2. ［**eDirectoryの暗号化**］>［**暗号化複製**］の順にクリックします。
3. 暗号化複製を有効にするパーティションを入力またはブラウズします。
4. **次へ**をクリックします。

5 暗号化複製ウィザードの［暗号化同期］テーブルで、［新規］を選択して暗号化リンクを定義します。

5a ［ソースレプリカの選択］フィールドで、ソースとして使用するレプリカを指定またはブラウズします。

5b ［対象先レプリカ］フィールドで、複製先として使用する1つ以上のレプリカを指定またはブラウズします。

5c ［リンクを暗号化する］を選択します。

5d OKをクリックします。

6 完了をクリックします。

LDAPを使用してレプリカレベルで暗号化複製を有効にする

重要: iManagerを使用して暗号化複製を有効にすることを強くお勧めします。

複製を暗号化するには、属性dsEncryptedReplicationConfigを使用する必要があります。構文は次のとおりです。

```
enable/disable flag#destination replica number#source replica number
```

この構文の詳細については、326 ページの「LDAPを使用してパーティションレベルで暗号化複製を有効にする」を参照してください。

この構文でレプリカ番号を指定すると、指定したレプリカの間の複製が暗号化されます。次に、この構文の例を示します。

- 1#0#1: レプリカ番号1と、パーティション内の他のすべてのレプリカの間で、暗号化複製が有効になります。
- 0#3#1: レプリカ番号3と#1の間で暗号化複製が無効になります。
- 0#1#1:レプリカ番号1で暗号化複製が無効になります。

次に、レプリカ番号1と3の間で暗号化複製を無効にするためのLDIFファイルの例を示します。

```
dn: o=ou
changetype: modify
replace: dsEncryptedReplicationConfig
dsEncryptedReplicationConfig: 0#3#1
```

パーティション操作

パーティションを分割すると、ペアレントパーティションの暗号化複製の設定がチャイルドパーティションに継承されます。パーティションをマージすると、ペアレントパーティションの暗号化複製の設定がマージ後のパーティションで保持されます。

新しいレプリカをレプリカリングに追加する

レプリカリングに新しいレプリカを追加する場合は、パーティションレベルおよびレプリカレベルで暗号化複製が有効になっているかどうかによって、それぞれ異なる影響を受けます。

レプリカをレプリカリングに追加する場合の詳細については、「155ページの「レプリカの管理」」を参照してください。

次のセクションで説明するように、どちらレベルでも、レプリカリングに追加するeDirectoryサーバのバージョンによって、複数のシナリオが考えられます。

- 329 ページの 「パーティションレベルで暗号化複製を有効にする」
- 329 ページの 「レプリカレベルで暗号化複製を有効にする」
- 329 ページの 「追加するサーバで暗号化複製を有効にする」

パーティションレベルで暗号化複製を有効にする

追加しようとしているeDirectoryサーバのバージョンによって、シナリオは異なります。

場面	データの暗号化
EBAなし、暗号化複製が無効の、eDirectory 9.1以降のサーバを追加する	データは平文で受け渡されます。
暗号化複製あり、EBAなしの、eDirectory 9.1以降のサーバを追加する	eDirectoryは、暗号化複製ポリシーに基づいてデータを暗号化します。
EBAありのeDirectory 9.1以降のサーバを追加する	EBAベースの暗号化が、暗号化複製より優先されます。

レプリカレベルで暗号化複製を有効にする

ソースレプリカと特定のターゲットレプリカの間で暗号化複製が有効になっている場合は、eDirectory 8.8以降のサーバをレプリカリングに追加できます。

ソースレプリカと、レプリカリング内の他のすべてのレプリカの間で暗号化複製が有効になっている場合、このシナリオは当てはまりません。その場合は、パーティションレベルで暗号化複製が有効または無効になっているレプリカリングにレプリカを追加することと同じになります。詳細については、「329ページの 「パーティションレベルで暗号化複製を有効にする」」を参照してください。

追加するサーバで暗号化複製を有効にする

追加しようとしているサーバのプラットフォームがLinuxの場合は、ndsconfig -Eオプションを使用してそのサーバでの暗号化複製を有効にできます。詳細については、ndsconfigのマニュアルページを参照してください。

追加するサーバのプラットフォームがWindowsの場合は、インストールウィザードで［暗号化複製を有効にします］オプションを選択します。

追加しようとしているサーバのプラットフォームがLinux以外の場合は、iManagerまたはLDAPを使用して暗号化複製を有効にできます。詳細については、「324 ページの 「暗号化複製を有効にする」」を参照してください。

同期と暗号化複製

特定のレプリカで暗号化複製を有効にして、設定の変更を他のサーバと同期しない場合、レプリカ間の複製は暗号化された形式で行われます。暗号化複製の設定変更が同期されていないレプリカでは、引き続きクリアテキスト形式で複製が行われます。

それまで暗号化複製の設定がレプリカ間で同期されていなかった場合でも、レプリカ間の複製は暗号化された形式で行われます。

暗号化複製ステータスを表示する

次の手順に従って、iMonitorを介して暗号化複製ステータスを表示できます。

1 iMonitorで、アシスタントフレームの［**エージェント同期**］をクリックします。

2 表示するパーティションの［**レプリカ同期**］をクリックします。

レプリカステータス情報が表示されます。現在接続されているレプリカからのリンクが暗号化されているかどうかが［**Encryption Status**］フィールドに表示されます。

基本的に、暗号化複製(ER)には次の3つのシナリオがあります。

- **パーティションレベルでERが有効:** 接続先のレプリカの［**暗号化状態**］は［使用可能］として示されます。

  どのレプリカに接続しているかを確認するには、レプリカフレームでハイパーリンクが付いていないレプリカを探します。そのレプリカが、現在接続しているレプリカです。他のレプリカをブラウズすると、そのレプリカの［**暗号化状態**］も［使用可能］として示されます。

- **レプリカレベルでERが有効:** 特定のレプリカからすべてのレプリカへの(つまり1つからすべてへの)ERが有効になっている場合です。この場合は、そのレプリカに接続すると、レプリカの［**暗号化状態**］が［使用可能］として示されます。

- **一部のレプリカでERが有効/無効:** 一部のレプリカでERが有効/無効 – パーティション全体ではERが有効になっているが、一部のサーバでは無効になっている場合、またはその逆の場合です。

  たとえば、3つのレプリカを含むパーティションAでERが有効に設定されていて、レプリカ1とレプリカ3の間のERが無効に設定されている場合、レプリカ1に接続すると、［**暗号化状態**］は次のように表示されます。

  Server 1使用可能

  Server 2

  Server 3使用不可

  これは、Server 1からレプリカリング内のすべてのサーバへのERは有効であるが、Server 1からServer 3へのERは管理者によって無効にされていることを意味します。

データを暗号化するときにデータの完全な安全性を確保する

データを暗号化するときには、まず、次の基本的な規則を守ることが重要です。

最終的に暗号化される情報をハードディスク(またはその他の媒体)にクリアテキストの形式で書き込まないこと。

既存のクリアテキストデータを暗号化対象としてマークすれば、そのデータは暗号化されますが、既存のクリアテキストデータは、DIBが存在するハードディスクのどこかに残る可能性があります。

次の操作を実行しようとすると、データベース内のどこかのブロックにデータのクリアテキスト部分が残ります。

- 既存のクリアテキストデータを暗号化対象としてマークする
- 暗号化属性の暗号化方式を変更する

以下のセクションでは、データを暗号化するときのシナリオを想定し、暗号化データの完全な安全性を確保する手順を説明します。

- 331 ページの 「完全に新しい設定でデータを暗号化する」
- 331 ページの 「既存の設定でデータを暗号化する」
- 333 ページの 「結論」

完全に新しい設定でデータを暗号化する

新しい設定では、オペレーティングシステムをインストールしただけの状態でeDirectoryをインストールします。したがって、DIBが存在するハードディスク上にクリアテキストデータが存在しないことが保証されます。

eDirectory内の暗号化データの完全な安全性を確保するには、次の手順を実行します。

1 どの属性をどの方式で暗号化するかをあらかじめ決めておきます。

つまり、データをクリアテキスト形式でeDirectoryにアップロードする前に、暗号化する属性を決めておく必要があります。

警告: いったんデータをクリアテキスト形式でeDirectoryにロードしたら、属性を暗号化対象としてマークしないでください。そうすることもできますが、その場合はセキュリティの問題が発生します。

---

2 eDirectoryを設定し、属性に適用する暗号化スキームを設定します。

3 既存のデータを新しいサーバにロードします。

LDIFファイルからバルクロードすることと他のサーバから複製するという2つがよくあるシナリオです。バルクロードするときは、クリアテキストのLDIFファイルをDIBが存在するハードディスクにコピーしないでください。

注: クリアテキストデータをディスクに書き込んではいけないという規則を思い出してください。

---

4 既存のすべてのクリアテキストデータを破壊します。

クリアテキストデータが格納されているディスク(またはその他の媒体)を完全に消去してください。消去する対象には、サーバのバルクロードに使われたクリアテキストのLDIFファイル、複製に使われた他のサーバ、古いバックアップが残っているテープなどが含まれます。

既存の設定でデータを暗号化する

このシナリオには次のような状況があります。

- 331 ページの 「既存のクリアテキストデータを暗号化データに変換する」
- 333 ページの 「データの暗号化方式を変更する」

既存のクリアテキストデータを暗号化データに変換する

クリアテキストデータを暗号化対象としてマークし、以下の方法でデータの安全性を確保できます。

- 332 ページの 「複製を利用する方法」
- 332 ページの 「バックアップおよび復元を利用する方法」

複製を利用する方法

1 新しいサーバで次のように暗号化を設定します。

1a どの属性をどの方式で暗号化するかをあらかじめ決めておきます。

つまり、データをクリアテキスト形式でeDirectoryにアップロードする前に、暗号化する属性を決めておく必要があります。

警告: いったんデータをクリアテキスト形式でeDirectoryにロードしたら、属性を暗号化対象としてマークしないでください。そうすることもできますが、その場合はセキュリティの問題が発生します。

1b 新たにフォーマットされ、パーティションが作成されたディスクで、クリアインストール(場合によってはOSも含めて)を行います。

これは、ディスクにクリアテキストデータが存在する可能性を排除するためです。つまり、以前クリアテキストデータが保存されていた既存のコンピュータにeDirectoryを再インストールすることはできません。ディスクからデータのすべての痕跡を完全に消去する必要があります。eDirectoryをインストールする前に、ディスクで安全な消去用ソフトウェアを使用する、磁気バルクイレーサーを使用するなど、データを徹底的に破壊する操作を行います。

1c eDirectoryを設定し、属性に適用する暗号化スキームを設定します。

2 暗号化する既存のデータが存在するレプリカリングにそのサーバを移動し、複製を実行した後、古いサーバをオフラインにします。

3 既存のすべてのクリアテキストデータを破壊します。

クリアテキストデータが格納されているディスク(またはその他の媒体)を完全に消去してください。消去する対象には、サーバのバルクロードに使われたクリアテキストのLDIFファイル、複製に使われた他のサーバ、古いバックアップが残っているテープなどが含まれます。

バックアップおよび復元を利用する方法

1 新しいサーバで次のように暗号化を設定します。

1a どの属性をどの方式で暗号化するかをあらかじめ決めておきます。

つまり、データをクリアテキスト形式でeDirectoryにアップロードする前に、暗号化する属性を決めておく必要があります。

警告: いったんデータをクリアテキスト形式でeDirectoryにロードしたら、属性を暗号化対象としてマークしないでください。そうすることもできますが、その場合はNote Aで説明しているセキュリティの問題が発生します。

1b 新たにフォーマットされ、パーティション化されたディスクで、クリアインストール(場合によってはオペレーティングシステムも含む)を行います。

これは、ディスクにクリアテキストデータが存在する可能性を排除するためです。つまり、以前クリアテキストデータが保存されていた既存のコンピュータにeDirectoryを再インストールすることはできません。ディスクからデータのすべての痕跡を完全に消去する必要があります。eDirectoryをインストールする前に、ディスクで安全な消去用ソフトウェアを使用する、磁気バルクイレーサーを使用するなど、データを徹底的に破壊する操作を行います。

1c eDirectoryを設定し、属性に適用する暗号化スキームを設定します。

2 新しいサーバで、バックアップされたDIB(既存のクリアテキストデータが格納されている)を復元します。DIBをバックアップするには、DIBセットのクローンまたはホットバックアップを使用できます。

3 既存のすべてのクリアテキストデータを破壊します。

クリアテキストデータが格納されているディスク(またはその他の媒体)を完全に消去してください。消去する対象には、サーバのバルクロードに使われたクリアテキストのLDIFファイル、複製に使われた他のサーバ、古いバックアップが残っているテープなどが含まれます。

データの暗号化方式を変更する

バックアップと復元を利用してこの操作を行うには、次の手順を実行します。

1 属性の暗号化アルゴリズムを変更します。

2 DIBのバックアップをとります。DIBをバックアップするには、DIBセットのクローンまたはホットバックアップを使用できます。

3 バックアップされたDIBを新しいサーバ上で復元し、古いサーバを削除します。

4 古いサーバ上にあるすべての既存のクリアテキストデータを破壊します。そうすることで、古い暗号化方式で暗号化されたデータの断片がハードディスクから一掃されます。

クリアテキストデータが格納されているディスク(またはその他の媒体)を完全に消去してください。消去する対象には、サーバのバルクロードに使われたクリアテキストのLDIFファイル、複製に使われた他のサーバ、古いバックアップが残っているテープなどが含まれます。

結論

ここで説明したシナリオ以外にも、この問題が発生する状況はあり得ます。「最終的に暗号化される情報をハードディスク(またはその他の媒体)にクリアテキストの形式で書き込まない」という規則を守っている限り、暗号化データの完全な安全性が確保されます。

12 NetIQ eDirectoryデータベースの修復

DSRepairユーティリティを使用して、eDirectoryツリーのデータベースを保守および修復することができます。このユーティリティでは、次の操作を実行できます。

- 不正なレコード、スキーマの不一致、不正なサーバアドレス、外部参照など、eDirectoryの問題の修正
- eDirectoryスキーマへの詳細な変更
- データベースの終了やユーザの介入を伴わない、自動的なデータベースの構造チェック
- データベースのオペレーショナルインデックスの確認
- 空のレコードを破棄することによる空き領域の増量。
- ローカルデータベースを修復します。
- レプリカ、レプリカリングおよびサーバオブジェクトの修復
- 同期エラーに対する、各ローカルパーティションの各サーバの分析
- ローカルデータベース内のオブジェクトの検出と同期

すべてのeDirectoryデータベースの問題が致命的であるというわけではなく、eDirectoryによって処理を続行できる問題もあります。ただしデータベースが破損すると、ローカルデータベースを開くことができないことを知らせるメッセージがコンソールに表示されます。この場合、修復を実行するかNetIQサポート部門に連絡します。

eDirectoryに問題が発生したか、NetIQサポート部門から指示されたのでない限り、修復操作を実行することはお勧めできません。ただし、修復ユーティリティや他のNetIQユーティリティ(iMonitorなど)の診断機能を使用することはお勧めします。詳細については、239ページの第8章「eDirectoryを監視する」を参照してください。

iManagerには次の修復ウィザードが含まれています。

ウィザード	説明
基本修復ウィザード	標準修復、ローカルデータベースの修復、または単一オブジェクトの修復を実行できます。また、外部参照をチェックして不明なリーフオブジェクトを削除できます。
ログファイルウィザード	修復ログファイルを開いて、ログファイルオプションを設定できます。
iMonitorによる修復	iMonitorを開いて、このプログラムの修復オプションを使用できます。
レプリカ修復ウィザード	すべてまたは選択したレプリカの修復、タイムスタンプの修復と新しいエポックの宣言、現在のサーバを新しいマスタレプリカに設定、および必要に応じて選択したレプリカの削除などを実行できます。
レプリカリングの修復ウィザード	すべてまたは選択したレプリカリングの修復、リング内のすべてのサーバにすべてのオブジェクトを送信、選択したレプリカでマスタレプリカのすべてのオブジェクトを受信、および必要に応じてレプリカリングから現在のサーバの削除などを実行できます。

ウィザード	説明
スキーマの保守ウィザード	ツリーからスキーマを要求、ローカルスキーマのリセット、新規スキーマエポックの宣言、オプションスキーマ拡張機能の実行、リモートスキーマのインポート、およびスキーマの更新などを実行できます。
サーバの修復ウィザード	すべてのネットワークアドレスを修復するか、サーバのネットワークアドレスのみを修復することができます。
同期修復ウィザード	現在のサーバで選択したレプリカの同期、現在のサーバの同期ステータスのレポート、すべてのサーバの同期ステータスのレポート、時刻同期の実行、および即時同期のスケジュールが実行できます。

ウィザードは、次のような操作のときに役立ちます。

- 336 ページの 「基本修復操作の実行」
- 340 ページの 「修復ログファイルの表示と設定」
- 341 ページの 「NetIQ iMonitorでの修復の実行」
- 342 ページの 「レプリカの修復」
- 345 ページの 「レプリカリングを修復する」
- 347 ページの 「スキーマの保守」
- 350 ページの 「サーバのネットワークアドレスの修復」
- 351 ページの 「同期化操作の実行」
- 354 ページの 「DSRepairオプション」
- 359 ページの 「クライアントを使用したデータベースの修復」
- 361 ページの 「グラフィカルなDS修復ユーティリティ」

基本修復操作の実行

基本修復ウィザードでは、標準修復、ローカルデータベースの修復、または単一オブジェクトの修復を実行できます。また、外部参照をチェックして不明なリーフオブジェクトを削除できます。

- 336 ページの 「標準修復を実行する」
- 338 ページの 「ローカルデータベースの修復の実行」
- 339 ページの 「外部参照のチェック」
- 339 ページの 「単一オブジェクトの修復」
- 339 ページの 「不明なリーフオブジェクトの削除」

標準修復を実行する

標準修復では、指定されたサーバのeDirectoryデータベースファイルに致命的なeDirectoryエラーがないかチェックし、修復します。このオプションは、実行されるたびに8つの主要な操作を実行します。これらの操作には、管理者が関与する必要はありません。これらの操作の中には、実

行中にデータベースをロックするものがあります。標準修復では、ローカルデータベースファイルのセットが一時的に作成され、修復操作はこれらのファイルに対して実行されます。つまり、重大な問題が発生したとしても、オリジナルのファイルは無事です。

特定の問題をトラブルシューティングし、それを解決することは標準修復を実行することよりはるかに優れています。標準修復を実行すると、データベースファイルが現在使用している2倍の容量の空きディスクが必要になる場合があります。詳細については、338 ページの 「ローカルデータベースの修復の実行」を参照してください。

eDirectoryが使用するオペレーショナルインデックスの再構築は、ローカルデータベースがロックされているときのみ可能です。

次の表に、標準修復の実行中に行われる操作について示します。

操作	データベースのロック	説明
データベース構造およびインデックスのチェック	○	データベースレコードとインデックスの構造および形式を調べます。eDirectory環境のデータベースレベルで構造的な破損が組み込まれていないことを確認します。
データベース全体を再構築する	○	構造チェックおよびインデックスチェック中に見つかったエラーを解決します。正しいデータ構造を復元し、eDirectoryデータベースおよびインデックスファイルを再作成します。
ツリー構造のチェックを実行	○	データベースレコード間のリンクを検証し、各チャイルドレコードに対して有効なペアレントレコードがあることを確認します。これは、データベースの整合性を確認するのに役立ちます。無効なレコードにはマークがつけられ、eDirectoryレプリカ同期処理の実行中に別のパーティションレプリカから復元できます。
すべてのローカルレプリカを修復	○	各オブジェクトと属性をスキーマ定義でチェックし、eDirectoryデータベースの不整合を解決します。ここでは、内部データ構造の形式もすべてチェックします。 この操作では、データベースから無効なレコードを削除することにより、ツリー構造のチェック中に見つかった不整合も解決します。この結果、無効なレコードにリンクされているすべてのチャイルドレコードは、すべてオーファンとしてマークされます。これらのオーファンレコードは失われませんが、この処理によって、データベースの再構築中に多数のエラーが発生する可能性があります。これは正常な反応で、孤立したオブジェクトはレプリカ同期の過程で自動的に再編成されます。
ネットワークアドレスの修復	いいえ	eDirectory内で保存しているサーバのネットワークアドレスを、ローカルSAP、SLP、またはDNSテーブルで維持されている値でチェックし、eDirectoryが現在も正確な情報を保持していることを確認します。矛盾が見つかった場合、eDirectoryは正しい情報で更新されます。
ストリームシンタックスファイルを確認する	○	ログインスクリプトなどのストリームシンタックスファイルは、eDirectoryデータベースの特殊領域に保存されます。この操作では、各ストリームシンタックスファイルが有効なeDirectoryオブジェクトに関連付けられているかどうかをチェックします。関連付けられていないストリームシンタックスファイルは削除され、そのファイルを参照している属性はパージされます。

標準修復を実行するには、次の操作を行います。

1 iManagerで、［役割およびタスク］ボタン をクリックします。
2 ［eDirectoryの保守］>［eDirectoryの修復］の順にクリックします。
3 操作を実行するサーバを指定し、［次へ］をクリックします。
4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［次へ］をクリックします。
5 ［標準修復］をクリックし、［開始］をクリックします。
6 表示される指示に従って、操作を完了します。

ローカルデータベースの修復の実行

eDirectoryでオープンおよびアクセスできるように、この修復操作を使用してローカルデータベースの矛盾を解決します。

ローカルデータベースの修復は、一時ファイルセットに対して実行するように指定することもできます。一時ファイルセットを指定しなかった場合、修復操作はアクティブなデータベースに対して実行されます。

一時データベースファイルセットに対して修復操作を実行する場合は、この操作中はデータベースを閉じておく必要があります。操作対象を一時ファイルセットにした場合、修復結果を反映する前に、その確認を求めるメッセージが表示されます。それ以外の場合、修復結果は即座に反映されます。

修復操作が終了すると、その修復操作のログを表示して、修復を完了させるのにさらに必要な操作があるかどうかを確認できます。詳細については、340ページの「修復ログファイルの表示と設定」を参照してください。

1 iManagerで、［役割およびタスク］ボタン をクリックします。
2 ［eDirectoryの保守］>［eDirectoryの修復］の順にクリックします。
3 操作を実行するサーバを指定し、［次へ］をクリックします。
4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［次へ］をクリックします。
5 ［ローカルデータベースの修復］をクリックし、［次へ］をクリックします。
6 ローカル修復の実行オプションを指定し、［開始］をクリックします。
7 表示される指示に従って、操作を完了します。

外部参照のチェック

この修復操作は、各外部参照オブジェクトをチェックして、そのオブジェクトを含むレプリカがあるかどうかを調べます。オブジェクトのあるパーティションのレプリカが含まれているすべてのサーバにアクセスできない場合、オブジェクトは見つけられません。オブジェクトが見つからない場合、警告が表示されます。

この操作では破損情報も表示されます。

1 iManagerで、［役割およびタスク］ボタン をクリックします。
2 ［eDirectoryの保守］>［eDirectoryの修復］の順にクリックします。
3 操作を実行するサーバを指定し、［次へ］をクリックします。

4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［次へ］をクリックします。

5 ［外部参照のチェック］をクリックし、［開始］をクリックします。

6 表示される指示に従って、操作を完了します。

単一オブジェクトの修復

この修復操作は、eDirectoryがデータへアクセスするのを妨げるような、eDirectoryオブジェクトの不整合を解決します。この操作は、ユーザ作成のパーティションおよび外部参照パーティションでのみ有効です。

この操作は、アクティブなデータベースファイルに対して実行されます。破損が物理的なレベルの場合は、まず物理チェックおよび構造チェックを実行してから単一オブジェクトの修復を行います。

修復操作時点のeDirectoryデータベースのバックアップコピーを保持していることを確認します。

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［eDirectoryの保守］>［eDirectoryの修復］の順にクリックします。

3 操作を実行するサーバを指定し、［次へ］をクリックします。

4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［次へ］をクリックします。

5 ［単一オブジェクトの修復］をクリックし、［開始］をクリックします。

6 修復するオブジェクトを指定し、［次へ］をクリックします。

7 表示される指示に従って、操作を完了します。

不明なリーフオブジェクトの削除

オブジェクトに必須プロパティがない場合、あるいはその他に無効な点がある場合(プロパティがオブジェクトタイプの最低要件を満たしていない場合)、修復によって一貫性のないオブジェクトが不明なオブジェクトに変更されます。不明なオブジェクトは実際のオブジェクトであり、eDirectory側では既知のオブジェクトです。不明なオブジェクトになっているのは、オブジェクトクラスの検証が不完全なためです。疑問符アイコンで表示される不明なオブジェクトは削除できますが、簡単に元のオブジェクトタイプに戻すことはできません。

この修復操作では、ローカルeDirectoryデータベースのオブジェクトのうち、オブジェクトクラスが不明で、従属オブジェクトを維持していないオブジェクトをすべて削除します。削除はeDirectoryツリーの他のレプリカと同時に後で行われます。

重要: この操作の意味を完全に理解しているかNetIQサポート部門から実行の指示がない限り、この操作は実行しないでください。

---

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［eDirectoryの保守］>［eDirectoryの修復］の順にクリックします。

3 操作を実行するサーバを指定し、［次へ］をクリックします。

4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［次へ］をクリックします。

5 ［不明リーフオブジェクトの削除］をクリックし、［開始］をクリックします。

6 表示される指示に従って、操作を完了します。

修復ログファイルの表示と設定

修復ログファイルには、ローカルパーティションとサーバに関する詳細情報が含まれます。この情報はデータベースの破損を診断するのに役立ちます。ログファイルウィザードでは、修復ログファイルを開いてログファイルオプションを設定できます。

このセクションでは、次の操作について説明します。

- 340 ページの 「ログファイルを開く」
- 341 ページの 「ログファイルオプションを設定する」

ログファイルを開く

この操作を行って、修復ログファイルを表示します。ログファイルのデフォルト名はdsrepair.logです。修復操作の結果は、このログファイルに書き込まれます。

ログファイル操作のオン/オフ切り替え、名前の変更、およびログファイルの削除またはリセットなどができます。詳細については、341 ページの 「ログファイルオプションを設定する」を参照してください。

1 iManagerで、［役割およびタスク］ボタン  をクリックします。

2 ［eDirectoryの保守］>［ログファイル］の順にクリックします。

3 操作を実行するサーバを指定し、［次へ］をクリックします。

4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［次へ］をクリックします。

5 ［ログファイルを開く］をクリックし、［開始］をクリックします。

6 表示される指示に従って、操作を完了します。

ログファイルオプションを設定する

この操作を行って、修復ログファイルを管理します。ログファイルのオン/オフ切り替え、ログファイルの削除、追加、ファイル名の変更などが行えます。

1 iManagerで、［役割およびタスク］ボタン  をクリックします。

2 ［eDirectoryの保守］>［ログファイル］の順にクリックします。

3 操作を実行するサーバを指定し、［次へ］をクリックします。

4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［次へ］をクリックします。

5 ［ログファイルオプション］をクリックし、［次へ］をクリックします。

6 表示される指示に従って、操作を完了します。

NetIQ iMonitorでの修復の実行

NetIQl iManagerの［**iMonitorによる修復**］オプションを使用して、修復機能にアクセスできます。iMonitorの［修復］ページでは、問題を表示したり、eDirectoryデータベースのバックアップやクリーンアップを実行できます。

iMonitorでは、DSRepair機能はサーバ限定の機能です。つまり、この機能はiMonitorが実行されているローカルサーバでのみ使用できます。他のサーバで実行されているこの機能にアクセスするには、そのサーバで実行されているiMonitorに切り替える必要があります。

［DS Repair］ページにアクセスするには、アクセスしようとするサーバの管理者またはコンソールオペレータと同等の権利が必要です。つまり、このページの情報にアクセスするには、まずログインして資格情報のチェックを受ける必要があります。

1. iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**eDirectoryの保守**］>［**iMonitorによる修復**］の順にクリックします。
3. 操作を実行するサーバを指定し、［**OK**］をクリックします。

   手動でiMonitorを開いて修復オプションを実行するには、［**iMonitorを実行 > してiMonitorから修復にアクセスする**］をクリックした後で［**OK**］をクリックします。
4. アクセスしようとしているサーバのユーザ名、コンテキスト、およびパスワードを指定してから［**OK**］をクリックし、［iMonitor Repair］ページを開きます。
5. 修復オプションを指定し、［**修復の開始**］をクリックします。

iMonitorで利用可能な修復機能の詳細については、「256ページの「DSRepair情報の表示」」を参照してください。

レプリカの修復

レプリカの修復操作では、レプリカの各オブジェクトとスキーマとの整合性が保たれているかどうか、オブジェクトの各属性とスキーマとの整合性が保たれているかどうかをチェックし、属性の構文に従ってデータをチェックします。レプリカに関連する他の内部データ構造もチェックされます。

レプリカの修復ウィザードを使用して、次の操作を実行します。

- 342 ページの 「すべてのレプリカを修復する」
- 342 ページの 「選択したレプリカを修復する」
- 343 ページの 「タイムスタンプを修復する」
- 344 ページの 「このサーバを新しいマスタレプリカに設定する」
- 344 ページの 「選択したレプリカを削除する」

すべてのレプリカを修復する

この操作では、レプリカテーブルに表示されたすべてのレプリカを修復します。

30分前までにローカルeDirectoryデータベースの修復操作を行っていない場合、この操作を実行する前にローカルデータベースを修復してください。詳細については、338 ページの 「ローカルデータベースの修復の実行」を参照してください。

1 iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2 ［**eDirectoryの保守**］>［**レプリカの修復**］の順にクリックします。
3 操作を実行するサーバを指定し、［**次へ**］をクリックします。
4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［**次へ**］をクリックします。
5 ［**すべてのレプリカの修復**］をクリックし、［**開始**］をクリックします。
6 表示される指示に従って、操作を完了します。

選択したレプリカを修復する

この操作では、レプリカビューに表示されているレプリカのうち、選択したレプリカのみ修復します。

30分前までにローカルeDirectoryデータベースの修復操作を行っていない場合、この操作を実行する前にローカルデータベースを修復してください。詳細については、338 ページの 「ローカルデータベースの修復の実行」を参照してください。

1 iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2 ［**eDirectoryの保守**］>［**レプリカの修復**］の順にクリックします。
3 操作を実行するサーバを指定し、［**次へ**］をクリックします。
4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［**次へ**］をクリックします。
5 ［**選択したレプリカを修復する**］をクリックし、［**次へ**］をクリックします。
6 修復するレプリカを指定し、［**開始**］をクリックします。
7 表示される指示に従って、操作を完了します。

タイムスタンプを修復する

注: この操作を行う前に、同期修復ウィザードを使用して、レプリカリング内のすべてのサーバが正しく通信していることを確認します。詳細については、351 ページの 「同期化操作の実行」を参照してください。

この操作では、選択したパーティションのレプリカをすべて最新版に更新するために、マスタレプリカの新しい参照ポイントを指定します。

この操作は、常にパーティションのマスタレプリカ上で実行されます。マスタレプリカは、このサーバのローカルレプリカである必要はありません。

オブジェクトが作成または変更されるとタイムスタンプが設定されますが、これは一意でなければなりません。マスタレプリカのタイムスタンプはすべて検査されます。タイムスタンプが現在のネットワーク時間より遅れている場合、新しいタイムスタンプに置き換えられます。タイムスタンプが最新であれば、新しいタイムスタンプは発行されません。すべてのタイムスタンプの時刻が一致すると、新規エポックが宣言されます。

この操作は、レプリカのオブジェクト間、またはオブジェクトのプロパティ間で矛盾が生じている場合に使用します。たとえば、ログインスクリプトを更新したのにログイン時に古いログインスクリプトが表示される場合は、レプリカ間で正しく同期が取られているかどうかを確認してください。将来のタイムスタンプと現在の時刻の時間差が1分以内であれば、最終的にeDirectory自体がその状況を修正します。新規エポックの宣言は非常に費用のかかる操作であり、定期的な使用はお勧めしていません。

eDirectoryはデータベースとして厳密な整合性はとられていません。したがってそのレプリカ同期の確認には5～10分かかることがあります。この操作を行うと、次の状態になります。

- 新規エポックがマスタレプリカで宣言され、その影響がマスタレプリカのすべてのオブジェクトに及ぶ可能性があります。
- すべてのタイムスタンプが調べられ、必要に応じて修復されます。
- レプリカ間の同期が取られるまで、日付の古いタイムスタンプ(エポック)を保持するレプリカからの更新内容は受け付けられません。
- レプリカは、マスタレプリカまたは新規エポックを受信済みの他のレプリカのすべてのオブジェクトのコピーを受け取ります。
- このレプリカは、マスタレプリカと同じエポックになります。
- 以前のエポックからの変更内容は失われます。
- マスタレプリカが現在のサーバに存在する必要はありませんが、この修復操作を実行するにはマスタレプリカに対するスーパバイザ権が必要です。
- そのほかのレプリカは新しい状態になります。

タイムスタンプを修復して新規エポックを宣言するには、次の操作を行います。

1. iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**eDirectoryの保守**］>［**レプリカの修復**］の順にクリックします。
3. 操作を実行するサーバを指定し、［**次へ**］をクリックします。
4. 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［**次へ**］をクリックします。
5. ［**タイムスタンプを修復して新しいエポックを宣言する**］をクリックし、［**次へ**］をクリックします。
6. 表示される指示に従って、操作を完了します。

このサーバを新しいマスタレプリカに設定する

この操作では、選択したパーティションのローカルレプリカをマスタレプリカとして設定します。元のマスタレプリカを損失した場合には、この操作で新しいマスタレプリカを設定できます。マスタレプリカがあるサーバでハードディスク障害が発生すると、そのマスタレプリカが失われることがあります。その場合は、マスタレプリカを変更する必要があります。

NetIQ iManagerで使用可能な通常のパーティション操作を実行する場合は、このオプションを使用しないでください。詳細については、151ページの第6章「パーティションおよびレプリカの管理」を参照してください。

1. iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**eDirectoryの保守**］>［**レプリカの修復**］の順にクリックします。
3. 新しいマスタレプリカに指定するサーバを指定し、［**次へ**］をクリックします。
4. ユーザ名、パスワード、およびコンテキストを指定してサーバに対する認証を行い、［**次へ**］をクリックします。
5. ［**このサーバを新しいマスタレプリカに設定**］をクリックし、［**次へ**］をクリックします。
6. 表示される指示に従って、操作を完了します。

選択したレプリカを削除する

この操作では、選択したレプリカをこのサーバから削除します。レプリカは削除されるか、サブオーディネートリファレンスに変更されます。

NetIQ iManagerで使用可能な通常のパーティション操作を実行する場合は、このオプションを使用しないでください。詳細については、151ページの第6章「パーティションおよびレプリカの管理」を参照してください。

1. iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**eDirectoryの保守**］>［**レプリカの修復**］の順にクリックします。
3. 削除するレプリカを含むサーバを指定し、［**次へ**］をクリックします。
4. ユーザ名、パスワード、およびコンテキストを指定してサーバに対する認証を行い、［**次へ**］をクリックします。
5. ［**選択したレプリカを破棄する**］をクリックし、［**次へ**］をクリックします。
6. 削除するレプリカを指定し、［**次へ**］をクリックします。
7. 表示される指示に従って、操作を完了します。

レプリカリングを修復する

レプリカリングの修復操作では、レプリカを保持する各サーバのレプリカリング情報をチェックし、リモートID情報を検証します。

レプリカリング修復ウィザードを使用して、次の操作を実行します。

- 345 ページの 「すべてのレプリカリングを修復する」
- 345 ページの 「選択したレプリカリングを修復する」
- 346 ページの 「リング内のすべてのサーバにすべてのオブジェクトを送信する」

- 346 ページの 「マスタから選択したレプリカへすべてのオブジェクトを受信する」
- 347 ページの 「レプリカリングからこのサーバを削除する」

すべてのレプリカリングを修復する

この操作では、レプリカビューに表示されたすべてのレプリカのレプリカリングを修復します。

30分前までにローカルeDirectoryデータベースの修復操作を行っていない場合、この操作を実行する前にローカルデータベースを修復してください。詳細については、338 ページの 「ローカルデータベースの修復の実行」を参照してください。

1 iManagerで、［役割およびタスク］ボタン をクリックします。
2 ［eDirectoryの保守］>［レプリカリングの修復］の順にクリックします。
3 操作を実行するサーバを指定し、［次へ］をクリックします。
4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［次へ］をクリックします。
5 ［Repair All Replica Rings］をクリックし、［次へ］をクリックします。
6 表示される指示に従って、操作を完了します。

選択したレプリカリングを修復する

この操作では、レプリカテーブルで選択したレプリカのレプリカリングを修復します。

30分前までにローカルeDirectoryデータベースの修復操作を行っていない場合、この操作を実行する前にローカルデータベースを修復してください。詳細については、338 ページの 「ローカルデータベースの修復の実行」を参照してください。

1 iManagerで、［役割およびタスク］ボタン をクリックします。
2 ［eDirectoryの保守］>［レプリカリングの修復］の順にクリックします。
3 操作を実行するサーバを指定し、［次へ］をクリックします。
4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［次へ］をクリックします。
5 ［Repair the Selected Replica Ring］をクリックし、［次へ］をクリックします。
6 修復するレプリカを指定し、［次へ］をクリックします。
7 表示される指示に従って、操作を完了します。

リング内のすべてのサーバにすべてのオブジェクトを送信する

この操作では、レプリカリング内で選択したサーバから、選択したパーティションのレプリカを含む他のすべてのサーバに、すべてのオブジェクトを送信します。

レプリカリング内で選択したサーバ上の選択したパーティションのレプリカが、レプリカリング内の他のすべてのサーバと同期していることを確かめるには、この操作を行います。該当するパーティションのサブオーディネートリファレンス(レプリカ)のみを含むサーバでは、この操作は実行できません。

選択したサーバに保持されているレプリカとまだ同期していない他のレプリカに加えた変更は失われます。この操作を実行する前に、同期ステータスを確認してください。

重要: この操作はレプリカ内のオブジェクトを再作成するため、ネットワークトラフィックの量が大幅に増加する可能性があります。これは診断操作ではありません。

1 iManagerで、［役割およびタスク］ボタン をクリックします。
2 ［eDirectoryの保守］>［レプリカリングの修復］の順にクリックします。
3 操作を実行するサーバを指定し、［次へ］をクリックします。
4 サーバのユーザ名、パスワード、およびコンテキストを指定して、［次へ］をクリックします。
5 ［リング内の各サーバにすべてのオブジェクトを送信する］をクリックし、［次へ］をクリックします。
6 表示される指示に従って、操作を完了します。

マスタから選択したレプリカへすべてのオブジェクトを受信する

この操作では、選択したサーバ上のレプリカで、マスタレプリカのすべてのオブジェクトを受信します。

レプリカリング内で選択したサーバ上の選択したパーティションのレプリカが、マスタレプリカと同期していることを確かめるには、この操作を行います。この操作は、マスタレプリカがあるサーバでは実行できません。

重要: この操作を行うと、ネットワークトラフィックの量が大幅に増加します。この操作を要求することにより、現在のレプリカは、サーバに新しいレプリカがあるかのように動作します。さらに、レプリカの状態は新規になります。

1 iManagerで、［役割およびタスク］ボタン をクリックします。
2 ［eDirectoryの保守］>［レプリカリングの修復］の順にクリックします。
3 操作を実行するサーバを指定し、［次へ］をクリックします。
4 サーバのユーザ名、パスワード、およびコンテキストを指定して、［次へ］をクリックします。
5 ［マスタから選択したレプリカにすべてのオブジェクトを受信する］をクリックし、［次へ］をクリックします。
6 表示される指示に従って、操作を完了します。

レプリカリングからこのサーバを削除する

この操作では、現在のサーバに保存されているレプリカのうち、選択したレプリカから特定のサーバを削除します。

警告: この操作を誤用すると、eDirectoryデータベースで致命的な破損が生じることがあります。NetIQサポート部門の担当者からの指示がない限り、この操作は実行しないでください。

1 iManagerで、［役割およびタスク］ボタン をクリックします。
2 ［eDirectoryの保守］>［レプリカリングの修復］の順にクリックします。
3 操作を実行するサーバを指定し、［次へ］をクリックします。
4 サーバのユーザ名、パスワード、およびコンテキストを指定して、［次へ］をクリックします。

5 ［レプリカリングからのサーバの削除］をクリックし、［次へ］をクリックします。

6 表示される指示に従って、操作を完了します。

スキーマの保守

スキーマとはオブジェクト属性のルールおよび定義を体系化したもので、これにより、各オブジェクトの内容と形式が構築され、データベース内でのオブジェクト間の関係が確立されます。

スキーマの保守ウィザードには、eDirectoryサーバのスキーマを［Root］のマスタに合わせるために必要なスキーマ操作がいくつか用意されています。ただし、これらの操作は必要な場合にのみ使用してください。スキーマは、ローカル修復操作および標準修復操作によってすでに検査されています。

eDirectoryスキーマの詳細については、「139ページの第5章「スキーマの管理」」を参照してください。

スキーマの保守ウィザードを使用して、次の操作を実行します。

- 347 ページの 「ツリーからスキーマを要求する」
- 348 ページの 「ローカルスキーマをリセットする」
- 348 ページの 「オプションスキーマ拡張機能を実行する」
- 349 ページの 「リモートスキーマをインポートする」
- 349 ページの 「新規スキーマエポックを宣言する」

ツリーからスキーマを要求する

この操作を実行すると、ツリーのルートのマスタレプリカが自身のスキーマをこのサーバのスキーマに同期させます。スキーマに対する変更の内容は、24時間以内に[Root]のマスタレプリカからこのサーバに伝達されます。

重要: すべてのサーバがマスタレプリカのスキーマを要求すると、ネットワークトラフィックが増加します。そのため、このオプションの使用には細心の注意を払うようにしてください。

---

1 iManagerで、［役割およびタスク］ボタン  をクリックします。

2 ［eDirectoryの保守］>［スキーマの保守］の順にクリックします。

3 操作を実行するサーバを指定し、［次へ］をクリックします。

4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［次へ］をクリックします。

5 ［ツリーからスキーマを要求］をクリックし、［次へ］をクリックします。

6 表示される指示に従って、操作を完了します。

ローカルスキーマをリセットする

この操作は、ローカルスキーマのタイムスタンプをクリアし、着信スキーマの同期を要求するスキーマリセット機能を呼び出します。

［Root］パーティションのマスタレプリカから実行した場合、この操作はできません。ツリー内のすべてのサーバが同時にリセットされるわけではありません。

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。
2 ［**eDirectoryの保守**］>［**スキーマの保守**］の順にクリックします。
3 操作を実行するサーバを指定し、［**次へ**］をクリックします。
4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［**次へ**］をクリックします。
5 ［**ローカルスキーマをリセット**］をクリックし、［**次へ**］をクリックします。
6 表示される指示に従って、操作を完了します。

オプションスキーマ拡張機能を実行する

この操作では、包含など拡張機能のためにスキーマを拡張および変更します。

この操作では、このサーバに［Root］パーティションのレプリカが含まれ、そのレプリカが使用可能な状態であることが必要になります。

以前のバージョンのeDirectoryでは、このオプションで加えた変更の同期ができません。

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。
2 ［**eDirectoryの保守**］>［**スキーマの保守**］の順にクリックします。
3 操作を実行するサーバを指定し、［**次へ**］をクリックします。
4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［**次へ**］をクリックします。
5 ［**オプションスキーマ拡張機能**］をクリックし、［**次へ**］をクリックします。
6 表示される指示に従って、操作を完了します。

リモートスキーマをインポートする

この操作では、現在のツリーのスキーマに追加したいスキーマが含まれているeDirectoryツリーを選択します。

ツリーを選択すると、［Root］パーティションのマスタレプリカを保持するサーバに接続されます。現在のツリー上にあるスキーマの拡張には、そのサーバのスキーマが使用されます。

2つのツリーをマージするには、一方のツリーからもう一方のツリーへ繰り返しスキーマをインポートする必要があります。詳細については、297ページの第10章「NetIQ eDirectoryツリーのマージ」を参照してください。

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。
2 ［**eDirectoryの保守**］>［**スキーマの保守**］の順にクリックします。
3 操作を実行するサーバを指定し、［**次へ**］をクリックします。

4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［次へ］をクリックします。

5 ［リモートスキーマのインポート］をクリックし、［次へ］をクリックします。

6 表示される指示に従って、操作を完了します。

新規スキーマエポックを宣言する

エポックとは、基準点として任意に選択される瞬間のことです。時代や新規バージョンと同義です。エポックは、レプリカの同期を制御します。新規エポックに宣言されると、マスタレプリカで機能します。他のレプリカは、新規エポックを持つレプリカに更新情報を送ることはできませんが、そのレプリカと完全に同期するまでは更新情報を受け取ります。

指定したパーティションの他のレプリカが更新済みレプリカと同期された場合、つまり各レプリカのエポックが同じになると、双方向の同期が再び許可されます。

新規スキーマエポッククを宣言すると、［Root］パーティションのマスタレプリカを保持するサーバに接続され、スキーマレコード上の不正なタイムスタンプが修復されます。次にスキーマの新規エポックがそのサーバで宣言され、ツリー全体に影響を与えます。

他のすべてのサーバは、修復されたタイムスタンプを保持する新しいスキーマのコピーを受け取ります。

受け取る側のサーバが新規エポック内に存在しなかったスキーマを含む場合は、古いスキーマを使用するオブジェクトおよび属性が「不明」オブジェクトクラスまたは属性に変更されます。

重要: NetIQサポート部門からの指示がない限り、この操作は実行しないでください。

---

1 iManagerで、［役割およびタスク］ボタン  をクリックします。

2 ［eDirectoryの保守］>［スキーマの保守］の順にクリックします。

3 操作を実行するサーバを指定し、［次へ］をクリックします。

4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［次へ］をクリックします。

5 ［新規エポックの宣言］をクリックし、［次へ］をクリックします。

6 表示される指示に従って、操作を完了します。

サーバのネットワークアドレスの修復

サーバの修復ウィザードでは、レプリカリングのすべてのサーバのネットワークアドレスとローカルデータベースのサーバオブジェクトを修復します。さらに、レプリカリングの選択したサーバのネットワークアドレスとローカルデータベースのサーバオブジェクトも修復できます。

サーバの修復ウィザードを使用して、次の操作を実行します。

- 350 ページの 「すべてのネットワークアドレスを修復する」
- 350 ページの 「サーバのネットワークアドレスの修復」

すべてのネットワークアドレスを修復する

この操作では、ローカルeDirectoryデータベース内で、すべてのサーバのネットワークアドレスをチェックします。使用できるトランスポートプロトコルに応じて、SAPテーブル、SLPディレクトリエージェント、およびDNSローカルまたはリモート情報でサーバ名を検索します。

その後、eDirectoryサーバオブジェクトのネットワークアドレス属性、およびすべてのパーティション［Root］オブジェクトの各レプリカ属性のアドレスレコードと、各アドレスが比較されます。アドレスが異なる場合は、同じになるように更新されます。

SAPテーブル、ローカル/リモートDNS情報、またはSLPディレクトリエージェントにサーバのネットワークアドレスが見つからなければ、修復は行われません。

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。
2 ［**eDirectoryの保守**］>［**サーバの修復**］の順にクリックします。
3 操作を実行するサーバを指定し、［**次へ**］をクリックします。
4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［**次へ**］をクリックします。
5 ［**すべてのネットワークアドレスを修復**］をクリックし、［**次へ**］をクリックします。
6 表示される指示に従って、操作を完了します。

サーバのネットワークアドレスの修復

この操作では、ローカルeDirectorデータベース内で、選択したサーバのネットワークアドレスをチェックします。現在バインドされているトランスポートプロトコルに応じて、ローカルSAPテーブル、SLPディレクトリエージェント、およびローカルまたはリモートのDNS情報でサーバ名を検索します。ネットワークアドレスが見つかれば、そのアドレスをeDirectoryサーバオブジェクトのネットワークアドレス属性の値、およびすべてのパーティション［Root］オブジェクトのレプリカ属性のアドレスレコードと照合します。アドレスが異なる場合は、同じになるように更新されます。

SAPテーブル、SLPディレクトリエージェント、またはローカル/リモートDNS情報にサーバのネットワークアドレスが見つからなければ、修復は行われません。

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。
2 ［**eDirectoryの保守**］>［**サーバの修復**］の順にクリックします。
3 操作を実行するサーバを指定し、［**次へ**］をクリックします。
4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［**次へ**］をクリックします。
5 ［**このサーバのネットワークアドレスの修復**］をクリックし、［**次へ**］をクリックします。
6 表示される指示に従って、操作を完了します。

問題

NetIQ SLPはオプションのパッケージです。認証機能は、NetIQ SLPパッケージの一部としては実装されません。

eDirectoryは現在OpenSLPとの互換性を持つようになり、OpenSLPの認証機能が使用されます。

注: Linuxでは、eDirectoryはすべてのインタフェースをリスンするわけではありませんが、nds.confファイルで指定された特定のIPは例外です。新しいIPV6アドレスを追加する場合は、リスナを開始する新しいアドレスと、対応する追加対象の参照を反映するようnds.confファイルが変更されていることを確認します。

同期化操作の実行

同期修復ウィザードでは、現在のサーバで選択したレプリカの同期、現在のサーバの同期ステータスのレポート、すべてのサーバの同期ステータスのレポート、時刻同期の実行、および即時同期のスケジュールができます。

同期修復ウィザードを使用して、次の操作を実行します。

- 352 ページの 「選択したレプリカをこのサーバで同期する」
- 352 ページの 「このサーバの同期ステータスをレポートする」
- 352 ページの 「すべてのサーバの同期ステータスをレポートする」
- 353 ページの 「時刻同期を実行する」
- 354 ページの 「即時同期をスケジュールする」

選択したレプリカをこのサーバで同期する

この操作では、選択したパーティションのレプリカを持つすべてのサーバ上で、完全な同期ステータスを確保します。

このオプションにより、パーティションの状態を確認できます。そのパーティションのレプリカを持つサーバがすべて正常に同期していれば、そのパーティションは異常なしと見なされます。レプリカリング内の各サーバが接続されると、次に、接続された各サーバは、レプリカリング内の他のすべてのサーバに対して、即時に同期を実行します。

サーバは、そのサーバ自身とは同期されません。そのため、現在のサーバのレプリカのステータスは［ホスト］として示されます。

1 iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2 ［**eDirectoryの保守**］>［**同期の修復**］の順にクリックします。
3 操作を実行するサーバを指定し、［**次へ**］をクリックします。
4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［**次へ**］をクリックします。
5 ［**このサーバ上で選択したレプリカを同期する**］をクリックし、［**次へ**］をクリックします。
6 表示される指示に従って、操作を完了します。

このサーバの同期ステータスをレポートする

この操作では、現在のサーバ上にレプリカを持つすべてのパーティションのレプリカ同期ステータスをレポートします。

この操作では、パーティションのレプリカを保持する各サーバのレプリカの［Root］オブジェクトから同期ステータス属性を読み込みます。レポートには、すべてのサーバに対して正常に同期が行われた最終時刻と、最終同期以降発生したエラーが表示されます。

12時間以内に同期が完了していない場合は、警告メッセージが表示されます。

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。
2 ［**eDirectoryの保守**］>［**同期の修復**］の順にクリックします。
3 操作を実行するサーバを指定し、［**次へ**］をクリックします。
4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［**次へ**］をクリックします。
5 ［**Report the Sync Status on This Server**］をクリックし、［**次へ**］をクリックします。
6 表示される指示に従って、操作を完了します。

すべてのサーバの同期ステータスをレポートする

この操作では、現在のサーバ上にレプリカを持つすべてのパーティションのレプリカ同期ステータスを確保します。

この操作では、パーティションのレプリカを保持する各サーバのレプリカの［Root］オブジェクトから同期ステータス属性を読み込みます。レポートには、すべてのサーバに対して正常に同期が行われた最終時刻と、最終同期以降発生したエラーが表示されます。

12時間以内に同期が完了していない場合は、警告メッセージが表示されます。

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。
2 ［**eDirectoryの保守**］>［**同期の修復**］の順にクリックします。
3 操作を実行するサーバを指定し、［**次へ**］をクリックします。
4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［**次へ**］をクリックします。
5 ［**すべてのサーバの同期ステータスのレポート**］をクリックし、［**次へ**］をクリックします。
6 表示される指示に従って、操作を完了します。

時刻同期を実行する

この操作では、ローカルeDirectoryデータベースに登録されているすべてのサーバに接続し、各サーバのeDirectoryと時刻同期ステータスに関する情報を要求します。

各サーバ上で実行しているeDirectoryのバージョンが［**DSバージョン**］フィールドに表示されます。

サーバに何のレプリカも含まれていない場合は、［**レプリカの深さ**］フィールドに「-1」と表示されます。［Root］パーティションのレプリカが含まれている場合は、「0」と表示されます。指定したサーバ上にレプリカがある場合は、［Root］に最も近いレプリカが［Root］からオブジェクト何個分離れているかを示す正の整数が表示されます。

eDirectoryツリー内のすべてのサーバは、同じタイムソースと同期している必要があります。そうしなければ、矛盾が発生したときに、レプリカ間でのオブジェクトの同期が正確に管理されなくなります。

同期修復ウィザードでは、各サーバのタイムソースはレポートできません。ただし、タイムサーバのタイプは報告します。この情報を参照すれば、時刻同期が正確に設定されているかどうかを確認できます。

重要: 「同期(誤差0.5秒弱)」の時刻同期ステータスを監視するには、DSRepairではなくNetIQ iMonitorを使用してください。詳細については、239ページの第8章「eDirectoryを監視する」を参照してください。

詳細については、98 ページの 「ネットワーク時刻の同期」を参照してください。

1 iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2 ［**eDirectoryの保守**］>［**同期の修復**］の順にクリックします。
3 操作を実行するサーバを指定し、［**次へ**］をクリックします。
4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［**次へ**］をクリックします。
5 ［**時刻の同期**］をクリックし、［**次へ**］をクリックします。
6 表示される指示に従って、操作を完了します。

即時同期をスケジュールする

この操作では、すべてのレプリカの同期を即座に行うようスケジュールします。この操作は、同期プロセスが通常のスケジュールどおりに実行されるのを待つことなく、同期情報を確認したい場合に使用します。

1 iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2 ［**eDirectoryの保守**］>［**同期の修復**］の順にクリックします。
3 操作を実行するサーバを指定し、［**次へ**］をクリックします。
4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、［**次へ**］をクリックします。
5 ［**即時同期をスケジュールする**］をクリックし、［**次へ**］をクリックします。
6 表示される指示に従って、操作を完了します。

DSRepairオプション

各eDirectoryプラットフォームのDSRepairユーティリティには、NetIQ iManagerで利用可能な修復機能のほかにも、通常の操作では非表示になっている拡張機能がいくつかあります。これらの拡張機能は、さまざまなプラットフォームでDSRepairユーティリティをロードする際にスイッチを使用して利用可能にできます。

- 354 ページの 「eDirectoryサーバ上でDSRepairを実行する」
- 356 ページの 「DSRepairコマンドラインオプション」
- 358 ページの 「DSRepair詳細設定スイッチの使用」

eDirectoryサーバ上でDSRepairを実行する

- 354 ページの 「Windows」
- 354 ページの 「Linux」

Windows

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 ［dsrepair.dlm］をクリックして、［開始］をクリックします。

DSRepairの詳細オプションを開くには、NetIQ eDirectory Servicesコンソールの［起動パラメータ］フィールドに「–a」と入力し、dsrepair.dlmを開始します。

Linux

DSRepairを実行するには、サーバコンソールに次の構文を使用して「ndsrepair」と入力します。

```
ndsrepair {-U |-E |-C |-P [-Ad] |-S [-Ad]|-N |-T |-J <entry_id> [-Ad -AM <attribute name>]} [-A <yes/no>] [-O <yes/no>][-F filename] [-h <local_interface:port>] [--config-file <configuration_file_path>]
```

または

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

重要: 詳細設定スイッチ［-Ad］は最後の引数として指定する必要があります。-Ad詳細設定スイッチオプションは、NetIQサポート技術者から指示があった場合にのみ有効にすることをお勧めします。config-fileを引数として指定する場合は、詳細設定スイッチ［-Ad］の前に指定する必要があります。

例

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

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

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

```
ndsrepair -S -Ad
```

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

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

オブジェクトのエントリIDが分かっている場合に1つのオブジェクトを修復するには、次のコマンドを入力します。

```
ndsrepair -J <entry ID in hex>
```

特定のパーティションまたはレプリカを修復するには、次のコマンドを入力します。

```
ndsrepair -P
```

このコマンドは、サーバに存在するすべてのパーティションのリストを返します。いずれかのパーティションを選択して実行可能な操作のリストを取得できます。

使用するために解放可能なデータベースの空き領域に関する情報を表示するには、次のコマンドを入力します。

```
ndsrepair -I
```

ネットワークアドレスを修復するには、次のコマンドを入力します。

```
ndsrepair -N
```

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

DSRepairコマンドラインオプション

オプション	説明
-U	［標準修復］オプションです。ユーザの操作なしにDSRepairを実行して終了します。修復が完了したらログファイルをチェックして、DSRepairで実行された処理を確認できます。 このオプションの指定時に実行される修復は、デフォルトの推奨されている通常の修復ではありません。特定の問題をトラブルシューティングし、それを解決することは標準修復を実行することよりはるかに優れています。
-P	［レプリカ操作とパーティション操作］オプションです。現在のサーバのeDirectoryデータベースファイルにレプリカが保存されているパーティションが表示されます。［レプリカオプション］メニューには、「レプリカの修復」、「パーティション操作のキャンセル」、「同期のスケジュール」、および「ローカルレプリカをマスタレプリカとして指定」を実行するオプションがあります。
-S	［グローバルスキーマの操作］オプションです。このサーバのスキーマをTreeオブジェクトのマスタに準拠させるのに必要なスキーマ操作がいくつか含まれています。ただし、これらの操作は必要な場合にのみ使用してください。スキーマは、ローカル修復操作および標準修復操作によってすでに検査されています。
-C	［外部参照オブジェクトのチェック］オプションです。各外部参照オブジェクトをチェックして、そのオブジェクトを含むレプリカがあるかどうかを調べます。オブジェクトのあるパーティションレプリカを含むすべてのサーバがアクセス不能の場合、オブジェクトは見つかりません。オブジェクトが見つからない場合、警告が表示されます。
-E	［レプリカ同期のレポート］オプションです。現在のサーバ上にレプリカを持つすべてのパーティションのレプリカ同期ステータスをレポートします。この操作により、パーティションのレプリカを保持する各サーバ上にあるレプリカのツリーオブジェクトから、同期ステータス属性が読み込まれます。レポートには、すべてのサーバに対して正常に同期が行われた最終時刻と、最終同期以降発生したエラーが表示されます。12時間以内に同期が完了していない場合は、警告メッセージが表示されます。

オプション	説明
-N	［このデータベースに認識されているサーバ］オプションです。ローカルeDirectoryデータベースに認識されているすべてのサーバが表示されます。現在のサーバにTreeパーティションのレプリカがある場合、このサーバにはeDirectoryツリー内のすべてのサーバのリストが表示されます。サーバオプションを実行するサーバを1つ選択します。
-J	ローカルサーバ上の1つのオブジェクトを修復します。修復するオブジェクトのエントリID(16進形式で)を指定する必要があります。破損している1つの特定のオブジェクトを修復する場合、標準修復(-U)オプションの代わりに、このオプションを使用できます。データベースのサイズによっては、［標準修復］オプションの完了に何時間もかかる場合があります。このオプションを使用して、時間を節約することができます。
-T	［時刻同期］オプションです。ローカルeDirectoryデータベースに登録されているすべてのサーバにアクセスして、各サーバの時刻同期ステータスの情報を要求します。このサーバにTreeパーティションのレプリカがある場合は、eDirectoryツリー内のすべてのサーバがポーリングされます。各サーバで実行されているeDirectoryのバージョンもレポートされます。
-A	既存のログファイルに付加します。情報は既存のログファイルに追加されます。デフォルトでは、このオプションは有効です。
-O	出力をファイルに記録します。デフォルトでは、このオプションは有効です。
-F *filename*	出力を指定したファイルに記録します。
-R	［ローカルデータベースの修復］オプションです。ローカルeDirectoryデータベースを修復します。eDirectoryでオープンおよびアクセスできるように、修復操作を使用してローカルデータベースの矛盾を解決します。このオプションには、データベースの修復操作を容易にするサブオプションがあります。このオプションにはファンクション修飾子があります。ファンクション修飾子については、次の表で説明します。
-I	使用するために解放可能なデータベース内の空き領域に関する情報を表示します。eDirectoryを使用すると、空のレコードを取得し、ndsrepairコマンドの再利用オプションを使用して、空き領域を再利用することができます。

-Rオプションで使用するファンクション修飾子を次に示します。

オプション	説明
-l	修復操作中にeDirectoryデータベースをロックします。
-u	修復操作中に一時eDirectoryデータベースを使用します。変更の保存または破棄するためのプロンプト、およびログファイルの表示のプロンプトが表示されます。
-m	修復されていない元のデータベースを維持します。
-i	eDirectoryデータベース構造とインデックスをチェックします。
-f	データベースの空き領域を増やします。

オプション	説明
-d	データベース全体を再構築します。
-t	ツリー構造のチェックを実行します。データベース内での接続状況が正しいかどうかを調べるため、ツリー構造のリンクをすべてチェックするには、「はい」を設定します。チェックを省略するには、「いいえ」を設定します。デフォルト値は「はい」です。
-o	オペレーショナルスキーマを再構築します。
-r	すべてのローカルレプリカを修復します。
-v	ストリームファイルを確認します。
-c	ローカル参照をチェックします。

DSRepair詳細設定スイッチの使用

警告: このセクションで説明する機能は、正しく使用しないとeDirectoryツリーが破損して元に戻せないことがあります。NetIQサポート担当者からの指示がない限り、この機能は使用しないでください。

生産環境でこれらのうちのいずれかの機能を使用する前に、あらかじめサーバ上のeDirectoryのフルバックアップをとっておくことをお勧めします。詳細については、439ページの第15章「NetIQ eDirectoryのバックアップと復元」を参照してください。

Linuxでは、「ndsrepair -R -Ad -XK2」と入力します。

Windowsでは、dsrepair.dlmを開始する前に、NDSコンソールの［**起動パラメータ**］フィールドにこれらのオプションを入力します。詳細については、354 ページの 「eDirectoryサーバ上でDSRepairを実行する」を参照してください。

スイッチ	説明
-P	タイプが不明なeDirectoryオブジェクトをすべて、参照済みとしてマークします。参照されたオブジェクトは、eDirectoryレプリカ同期処理の対象にはなりません。
-WM	多くの場合、ZENworks ® 2.0を使用していると、WM: Registered Workstations属性が非常に高くなります。DSRepairを-WMオプションを指定して実行すると、こうした高い値がクリアされます。
-XK2	このサーバのeDirectoryデータベース内のすべてのeDirectoryオブジェクトを削除します。この操作では、破損したレプリカがどんな方法を使っても削除できない場合に、破損レプリカを削除できます。
-XK3	このサーバのeDirectoryデータベース内のすべての外部参照を削除します。この操作では、機能していないレプリカ内の外部参照をすべて削除できます。参照が原因で問題が発生している場合、レプリカが再度機能するために、eDirectoryは参照を再作成できます。
-RC	DIBをバックアップします。このオプションは、Windowsでのみ使用できます。
-OT	ローカルデータベース修復の実行中、破損通知にタイムスタンプを含めます。INHIBIT MOVEを除くすべての破損通知にタイムスタンプを含めます。

スイッチ	説明
-NLD	NLS:ライセンス許可証オブジェクトとNLS:製品コンテナオブジェクトからIRFを削除します。
-AM	特定の条件に一致する属性をFLAIMデータベース内の別のコンテナに移動します。どのeDirectory属性が別のコンテナへの移動に適しているかについて詳しくは、『NetIQ eDirectoryチューニングガイド』の「FLAIM属性コンテナリゼーション」を参照してください。
-AH	DIBサイズが1GBよりも小さく、古いNDOファイルが72時間よりも古い場合、NDOファイルは作成されません。

クライアントを使用したデータベースの修復

eMBox(eDirectory Management Toolbox)クライアントはコマンドラインJavaクライアントで、これを使用するとDSRepairにリモートアクセスできます。クライアントはバッチモードで実行できるため、これを使用してeDirectory DSRepair eMToolで標準修復を行うことができます。

emboxclient.jarファイルは、eDirectoryの一部としてサーバにインストールされます。JVMをインストールしていれば、どのコンピュータでも実行できます。クライアントの詳細については、「584ページの 「コマンドラインクライアントの使用」」を参照してください。

DSRepair eMToolを使用する

1 コマンドラインで次のように入力して、対話式モードでクライアントを実行します。

```
java -cp path_to_the_file/emboxclient.jar -i
```

(クラスパスにemboxclient.jarファイルがすでに含まれている場合は、単に「java -i」と入力します。)

クライアントのプロンプトが次のように表示されます。

```
Client>
```

2 修復するサーバにログインするには、次のように入力します。

```
login -s server_name_or_IP_address -p port_number
-u username.context -w password -n
```

ポート番号は通常80または8028です。ただし、すでにそのポートを使用しているWebサーバが存在する場合は異なります。-nオプションを使用すると、非セキュア接続が開始されます。

クライアントはログインが成功したかどうかを表示します。

3 次の構文を使用して修復コマンドを入力します。

dsrepair.*task options*

たとえば、dsrepair.ufrは標準修復を実行します。

dsrepair.rld -a –vは、［すべてのローカルレプリカを修復］オプションおよび［ローカル参照をチェックする］オプションを使用して、ローカルデータベースを修復します。

各スイッチの間にはスペースが必要です。スイッチの順序は重要ではありません。

クライアントは修復が成功したかどうかを表示します。

DSRepair eMToolオプションの詳細については、「360 ページの 「DSRepair eMToolのオプション」」を参照してください。

4 クライアントからログアウトするには、次のコマンドを入力します。

```
logout
```

5 クライアントを終了するには、次のコマンドを入力します。

```
exit
```

DSRepair eMToolのオプション

次の表にDSRepair eMToolのオプションを示します。クライアントでlist -t dsrepairコマンドを使用してDSRepairオプションの詳細を表示することもできます。詳細については、588 ページの「eMToolとそのサービスを表示する」を参照してください。

オプション	説明
rso -o -d	単一オブジェクトの修復(16進数のオブジェクトID、オブジェクトDN)
rts	時刻同期
rss	すべてのパーティションの同期ステータスのレポート
rld -l -t -d -p -i -f -c -o -a -m -v	◆ ローカルデータベースを修復する ◆ 全体の修復中にeDirectoryデータベースをロックする ◆ 修復中に一時的なeDirectoryデータベースを使用する ◆ 修復されていない元のデータベースを維持する ◆ データベース構造のチェックを実行する ◆ データベース構造とインデックスのチェックを実行する ◆ データベースの空き領域を増やす ◆ ツリー構造のチェックを実行する ◆ オペレーショナルスキーマを再構築する ◆ すべてのローカルレプリカを修復する ◆ メールディレクトリとストリームファイルを検証する ◆ ローカル参照をチェックする
ufr	標準修復
rsn -o -d	選択したサーバのネットワークアドレスを修復する(16進数のオブジェクトID、オブジェクトDN)
ran	すべてのネットワークアドレスの修復
rsr -p -d	選択したレプリカの修復(パーティションID、パーティションDN)
rer	すべてのレプリカの修復
ror -p -d	選択したレプリカリングの修復(パーティションID、パーティションDN)
rar	すべてのレプリカのレプリカリングの修復

オプション	説明
ssa -p -d	すべてのサーバのレプリカ同期ステータスのレポート(パーティションID、パーティションDN)
cer	外部参照のチェック
rao -p -d -s -d	このレプリカのすべてのオブジェクトの受信(パーティションID、パーティションDN、サーバID、サーバDN)
sao -p -d -s -d	リング内のすべてのレプリカに対するすべてのオブジェクトの送信(パーティションID、パーティションDN、サーバID、サーバDN)
dne -p -d	タイムスタンプの修復と新しいエポックの宣言(パーティションID、パーティションDN)
sri -p -d	即時同期のスケジュール(パーティションID、パーティションDN、サーバID、サーバDN)
sks -p -d -s -d	選択したサーバでのレプリカの同期(パーティションID、パーティションDN、サーバID、サーバDN)
ske -p -d	すべてのサーバでのレプリカの同期(パーティションID、パーティションDN)
dsr -p -d	このサーバで選択したレプリカの削除(パーティションID、パーティションDN)
xsr -p -d -s -d	レプリカリングからのサーバの削除(パーティションID、パーティションDN、サーバID、サーバDN)
dnm -p -d	このサーバを新しいマスタレプリカとして設定(パーティションID、パーティションDN)
dul	不明リーフオブジェクトの削除

グラフィカルなDS修復ユーティリティ

グラフィカルなDS修復ユーティリティがOES11SP1に追加されました。このツールは新しいOES11 SP1のインストール時に自動的にインストールされます。

ユーザインタフェースを起動するには、サーバコンソールでndsgrepairコマンドを実行します。コンソールを使用して実行可能な修復操作のほとんどは、このグラフィカルインタフェースを使用して実行できます。すべてのヘルプトピック(メニューオプションなど)を参照するには、F1キーを押すか、またはUIメインメニューで、［**ヘルプ**］>［**ヘルプコンテンツ**］の順にクリックします。

OES 11 SP1にアップグレードする場合は、次の手順を実行して、eDirectoryパターンの下でnovell-ndsgrepairを手動で選択します。

1. YaSTを開き、［**OES Install and Configuration**］を選択しします。
2. ［詳細］をクリックし、左側の［**Novell eDirectory Pattern**］を選択して、右側の［パッケージ］の一番下までスクロールします。
3. ［**novell-ndsgrepair**］を選択し、［**受諾**］、［次へ］、［**終了**］の順にクリックします。

13 LDAP Services for NetIQ eDirectoryについて

LDAP (Lightweight Directory Access Protocol)は、クライアントアプリケーションでディレクトリ情報にアクセスするためのインターネット通信プロトコルです。LDAPは、X.500 DAP (Directory Access Protocol)に基づいていますが、従来のクライアントほど複雑ではなく、X.500標準に基づくその他のディレクトリサービスと同時に使用することができます。

一般に、LDAPは最も単純なディレクトリアクセスプロトコルとして使用されます。

NetIQ eDirectory用のLDAP (Lightweight Directory Access Protocol)サービスは、LDAPクライアントからeDirectoryに保存されている情報にアクセスするためのサーバアプリケーションです。

LDAPサービスには、LDAPを通じて利用できる次のようなeDirectory機能が含まれます。

- プロビジョニング
- アカウント管理
- 認証
- 権限付与
- 識別情報管理
- 通知
- レポーティング
- 認定
- セグメンテーション

クライアントごとに異なるディレクトリアクセスレベルを設定して、ディレクトリにアクセスするための安全な接続を確立できます。このセキュリティメカニズムを利用すると、一般に公開するディレクトリ情報、組織内で利用する情報、および特定のグループまたは個人だけが利用できる情報を区別して管理できます。

各LDAPクライアントで利用できるディレクトリ機能は、LDAPクライアントおよびLDAPサーバに組み込まれた機能により異なります。たとえば、LDAP Services for eDirectoryを利用すると、LDAPクライアントはeDirectoryデータベース内のデータを読み書きできます。ただし、これにはLDAPクライアントに必要な許可が与えられている必要があります。クライアントは、ディレクトリデータの読み書きが許可される場合と、読み込みしか許可されない場合があります。

一般的なクライアント機能を利用すると、クライアントから次のような処理を実行できます。

- 電子メールアドレスや電話番号など、特定の個人についての情報を検索する。
- 特定の姓または特定の文字で始まる姓を持つすべての個人の情報を検索する。
- 任意のeDirectoryオブジェクトまたはエントリについての情報を検索する。
- 氏名、電子メールアドレス、勤務先電話番号、および自宅電話番号を取得する。
- 会社名および市町村名を取得する。

以降のセクションで、LDAP Services for eDirectoryについて説明します。

- 362 ページの 「LDAPサービスの主な用語」
- 364 ページの 「LDAPとeDirectoryの連携について」
- 374 ページの 「LinuxでのLDAPツールの使用」
- 385 ページの 「拡張可能一致検索フィルタ」
- 387 ページの 「LDAPトランザクション」

LDAPの詳細については、次のWebサイトを参照してください。

- OpenLDAP (http://www.openldap.org/)
- LDAP Roadmap & FAQ (http://www.kingsmountain.com/ldapRoadmap.shtml)

LDAPサービスの主な用語

- 362 ページの 「クライアントとサーバ」
- 362 ページの 「オブジェクト」
- 363 ページの 「参照」

クライアントとサーバ

LDAPクライアント— Internet Explorer、NetIQインポート/エクスポート変換ユーティリティなどのような、1つのアプリケーションです。

LDAPサーバ— nldap.dlm (Windows用)またはlibnldap.so (Linux用)が動作しているサーバです。

オブジェクト

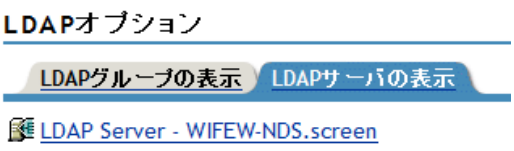
LDAPグループオブジェクト— LDAPサーバでNetIQ LDAPプロパティの設定と管理を行います。

このオブジェクトはeDirectoryのインストール時に作成されます。LDAPグループオブジェクトには、複数のLDAPサーバ間で共有できる便利な設定情報が含まれています。

LDAPサーバオブジェクト— LDAPクライアントによるNetIQ LDAPサーバ上の情報へのアクセスおよび使用方法の設定と管理を行います。

このオブジェクトはeDirectoryのインストール時に作成されます。LDAPサーバオブジェクトとは、サーバ固有の設定データのことです。

次の図は、NetIQ iManagerのLDAPサーバオブジェクトを表したものです。



参照

参照— LDAPサーバがLDAPクライアントに送信するメッセージです。このサーバからは結果がすべて提供されず、他のLDAPサーバにまだデータがある可能性をクライアントに通知します。

参照には、操作を続行するのに必要な情報がすべて含まれます。

シナリオ:LDAPクライアントがLDAPサーバに要求を送信しますが、サーバは操作のターゲットエントリをローカルで見つけることができません。その場合、LDAPサーバはパーティションおよび他のサーバに関して所有する知識参照を使用して、そのエントリについてより多くの知識を持つ別のサーバを特定します。LDAPサーバは参照情報をクライアントに送信します。

クライアントは識別されたサーバに対する新しいLDAP接続を確立し、操作を再試行します。

参照には次の利点があります。

- LDAPクライアントが操作を制御し続けます。

  常に状況を把握することにより、クライアントはより的確な判断ができ、ユーザにフィードバックを返すことができます。また、参照を検索しない選択をしたり、検索の前にユーザに確認メッセージを表示することもできます。
- 多くの場合、参照の方がチェーンよりもリソースを効果的に使用できます。

  チェーンでは、エントリの多い検索操作が要求されると、ネットワーク全体に2度送信される場合があります。1度目はデータのあるサーバからチェーンを実行するサーバへの送信です。2度目はチェーンを実行するサーバからクライアントへの送信です。

  参照では、クライアントはデータのあるサーバから、1回の送信で直接データを受け取ることができます。
- エントリの格納場所がわかっていれば、クライアントは直接データのあるサーバにアクセスすることができます。

  チェーンでは、クライアントは詳細を見ることができません。データの出所がわからない場合、そのデータを保持しているサーバにクライアントが直接アクセスすることはありません。

参照には次の欠点があります。

- クライアントが参照とその検索方法を認識できる能力が必要です。
- LDAPv2クライアントでは結果が認識されないか、認識に古い非標準の方法が使用されます。
- すべてのeDirectoryパーティションにLDAPサーバのサービスが適用されていなくてはなりません。

  適用されていない場合、参照結果をパーティションのデータに送信できません。

上方参照— 通信中のサーバのデータよりもツリーの高い位置にあるデータを持つサーバを参照することです。詳細については、425 ページの 「上方参照を設定する」を参照してください。

上方参照では、マルチベンダツリーで、上方または隣接した非eDirectoryパーティションにあるオブジェクトに関する要求が処理されます。

eDirectoryサーバがこのタイプのツリーに含まれるようにするには、eDirectoryは非信頼とマークされたパーティション内で、階層データを上方に保持するようにします。非信頼領域のオブジェクトは、正しいDN階層を構築するのに必要なエントリのみから構成されます。これらのエントリは、X.500の“Glue”エントリに類似しています。

eDirectoryでは、知識情報をLDAP参照データの形式で非信頼領域に配置できます。この情報は、LDAPクライアントに参照を返すのに使用します。

LDAP操作をeDirectoryツリーの信頼されていない領域で実行すると、LDAPサーバは正しい参照データを検索し、クライアントに参照を返します。

チェーン— サーバベースのネームレゾリューションプロトコル。

LDAPクライアントがLDAPサーバに要求を送信しますが、サーバは操作のターゲットエントリをローカルで見つけることができません。LDAPサーバ(サーバA)はeDirectoryツリーのパーティションおよび他のサーバに関して所有する知識参照を使用して、DNについてより多くの知識を持つ、別のLDAPサーバ(サーバB)を特定します。LDAPサーバAは、特定されたLDAPサーバBと通信します。

必要に応じ、サーバAがエントリのレプリカを持つサーバに接続するまでこの処理が続けられます。その後、eDirectoryは詳細をすべて処理し、操作を完了します。サーバ間の処理はクライアントには表示されないため、クライアントは最初のサーバAが要求を処理したものと判断します。

LDAPサーバにチェーンを使用した場合、次の利点があります。

- ネームレゾリューションの詳細をすべてクライアントから見えなくします。
- 自動で再認証を行います。
- クライアントのプロキシの役割を果たします。
- eDirectoryツリーにLDAPサービスをサポートしないサーバがあっても、シームレスに実行されます。

一方、チェーンには次の欠点があります。

- チェーンを使用して名前解決中には、サーバからのフィードバックがなくクライアントが待機する必要がある場合があります。
- LDAPサーバが、WANリンク経由で多くのエントリを送信するよう要求された場合、処理に長時間かかることがあります。
- ほぼ同じ処理能力を持つサーバがいくつかある場合、別々のサーバが2つの要求を同じエントリ上で処理してしまうことがあります。

  eDirectoryは、サーバを接続コスト順にソートしようとします。負荷分散のため、eDirectoryは一番コストの低いサーバの中からランダムに選択を行います。

LDAPとeDirectoryの連携について

このセクションでは次について説明します。

- 365 ページの 「LDAPからeDirectoryに接続する」
- 368 ページの 「クラスと属性のマッピング」
- 371 ページの 「非標準スキーマ出力を有効にする」
- 372 ページの 「構文の相違」
- 373 ページの 「サポートされるNetIQ LDAPコントロールと拡張」

LDAPからeDirectoryに接続する

すべてのLDAPクライアントが、次のいずれかのユーザタイプでNetIQ eDirectoryにバインド(接続)されます。

- ［Public］ユーザ(匿名バインド)
- プロキシユーザ(プロキシユーザ匿名バインド)
- NDSまたはeDirectoryユーザ(NDSユーザバインド)

ユーザの認証に使用されるバインドタイプにより、LDAPクライアントがアクセスできる内容が決定されます。LDAPクライアントは、作成した要求をディレクトリに送信することにより、ディレクトリにアクセスします。LDAPクライアントがLDAP Services for eDirectoryを通じて要求を送信した場合、eDirectoryは、その中からLDAPクライアントが適切なアクセス権を持つ属性の要求だけを処理します。

たとえばLDAPクライアントが、読み込み権が必要なある属性値を要求したものの、その属性についてユーザに許可されているのが比較権だけである場合、この要求は拒否されます。

標準ログイン制限とパスワード制限は引き続き適用されます。ただし、制限はすべてLDAPの実行場所と関係します。時刻およびアドレス制限も適用されますが、アドレス制限はeDirectoryログインが実行された場所(この場合はLDAPサーバ)を基準に決定されます。

［Public］ユーザとして接続する

匿名バインドは、ユーザ名またはパスワードを使用しない接続です。サービスでプロキシユーザの使用が設定されていない場合、名前とパスワードが定義されていないLDAPクライアントでLDAP Services for eDirectoryにバインドすると、ユーザはeDirectoryに[Public]ユーザとして認証されます。

[Public]ユーザとは、非認証のeDirectoryユーザのことです。デフォルトでは、[Public]ユーザにはeDirectoryツリー内のオブジェクトのブラウズ権が割り当てられます。［パブリック］ユーザ用のデフォルトブラウズ権では、eDirectoryオブジェクトをブラウズすることはできますが、ほとんどのオブジェクト属性にアクセスすることはできません。

多くの場合、LDAPクライアントは、デフォルトの［Public］権だけでは不十分です。［Public］の権利は変更できますが、変更した権利はすべてのユーザに対して許可されることになります。この問題を解決するために、プロキシユーザ匿名バインドを使用することをお勧めします。詳細については、365 ページの 「プロキシユーザとして接続する」を参照してください。

［Public］ユーザによるオブジェクト属性へのアクセスを許可するには、[Public]ユーザを該当する(1つまたは複数の)コンテナのトラスティに設定し、適切なオブジェクト権および属性権を割り当てる必要があります。

プロキシユーザとして接続する

代理ユーザ匿名バインドは、eDirectoryユーザ名にリンクされた匿名接続です。プロトコルでプロキシユーザの使用が設定されている場合、LDAPクライアントがLDAP for eDirectoryに匿名でバインドすると、ユーザはeDirectoryによりプロキシユーザとして認証されます。LDAP Services for eDirectoryとeDirectoryの両方でユーザ名が設定されます。

通常、匿名バインドにはLDAPのポート389が使用されます。ただし、ポートはインストール時に手動で変更することができます。

次に、プロキシユーザ匿名バインドの概念について説明します。

- 匿名バインドを経由するLDAPクライアントアクセスは、すべてプロキシユーザオブジェクトを通して割り当てられます。
- 匿名バインドではLDAPクライアントからパスワードが提供されないので、プロキシユーザにnullパスワードを適用し、パスワード変更間隔などのパスワード制限を設定しないようにします。パスワードを強制的に有効期限切れにしたり、プロキシユーザにパスワードの変更を許可したりしないでください。
- プロキシユーザオブジェクトのアドレス制限を設定すると、ユーザがログインできるロケーションを制限できます。
- eDirectory内にプロキシユーザオブジェクトを作成し、公開するeDirectoryオブジェクトに対する権利を割り当てる必要があります。デフォルトのユーザ権では、特定のオブジェクトと属性だけに対する読み込みアクセス権が許可されます。アクセスする必要がある各サブツリー内のすべてのオブジェクトと属性に対するプロキシユーザ読み込み権および検索権を割り当てます。
- LDAP Services for eDirectoryを設定するLDAPグループオブジェクトの［全般］ページで、プロキシオブジェクトを有効化する必要があります。このため、1つのLDAPグループ内のすべてのサーバに対し、プロキシユーザオブジェクトは1つしか作成できません。詳細については、393 ページの 「LDAPオブジェクトを環境設定する」を参照してください。
- プロキシユーザオブジェクトに対し、すべてのプロパティ(デフォルト)か、選択したプロパティの権利を許可できます。

プロキシユーザに対して選択したプロパティの権利だけを許可するには、次を実行します。

1. NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**権利**］>［**トラスティの変更**］の順にクリックします。
3. 代理ユーザが権利を持つ最上位コンテナの名前とコンテキストを指定するか、  をクリックし、問題のコンテナをブラウズして［**OK**］をクリックします。
4. ［トラスティの変更］画面で［**トラスティの追加**］をクリックします。
5. 代理ユーザのオブジェクトをブラウズしてクリックし、［**OK**］をクリックします。
6. 追加した代理ユーザの左側にある［**割り当てられた権利**］をクリックします。
7. ［すべての属性権］および［エントリ権］チェックボックスをオンにし、［プロパティの削除］をクリックします。 **> >**
8. ［**プロパティの追加**］をクリックし、［**スキーマ内のすべてのプロパティを表示する**］チェックボックスをオンにします。
9. mailstop(リストの小文字のセクション)や役職など、代理ユーザが継承可能な権利を選択し、［**OK**］をクリックします。

   その他の継承可能な権利を追加する場合は、手順ステップ 8～ステップ 9を繰り返します。
10. ［**完了**］をクリックして、［**OK**］をクリックします。

プロキシユーザ匿名バインドを実装するには、eDirectory内にプロキシユーザオブジェクトを作成し、そのユーザに適切な権利を割り当てる必要があります。アクセスする必要がある各サブツリー内のすべてのオブジェクトと属性に対するプロキシユーザ読み込み権および検索権を割り当てます。同じ代理ユーザ名を指定して、LDAP Services for eDirectory内でプロキシユーザ名を有効化する必要もあります。

1 NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2 ［**LDAP**］ > ［**LDAPオプション**］をクリックする。
3 ［**LDAPグループの表示**］をクリックします。
4 設定するLDAPグループオブジェクトの名前をクリックします。
5 ［**プロキシユーザ**］フィールドにeDirectoryユーザオブジェクトの名前とコンテキストを指定します。
6 **適用**をクリックし、**OK**をクリックします。

LinuxでIdapconfigユーティリティを使用する

たとえば、LDAP Search Referral UsageでLDAPサーバによるLDAP参照の処理方法を指定します。

1 システムプロンプトで、次のコマンドを入力します。

```
ldapconfig -s "LDAP:otherReferralUsage=1"
```

2 ユーザFDN(完全識別eDirectoryユーザ名)とパスワードを入力します。

NDSまたはeDirectoryユーザとして接続する

eDirectoryユーザバインドは、LDAPクライアントが完全なeDirectoryユーザ名とパスワードを使用して確立する接続です。eDirectoryユーザバインドはeDirectoryにより認証されます。LDAPクライアントは、そのeDirectoryユーザにアクセスが許可されているすべての情報にアクセスできます。

次に、eDirectoryユーザバインドに関する重要な概念について説明します。

- eDirectoryユーザバインドは、LDAPクライアントに入力されたユーザ名とパスワードを使用してeDirectoryへの認証が行われます。
- LDAPクライアントアクセスに使用するeDirectoryユーザ名とパスワードは、Novell Clientがeディレクトリにアクセスする場合も使用できます。
- 非TLS接続では、eDirectoryパスワードはLDAPクライアントとLDAP Services for eDirectoryの間の経路をクリアテキストデータとして転送されます。
- クリアテキストパスワードが無効にされている場合は、非TLS接続上で転送されたユーザ名またはパスワードを含むeDirectoryバインド要求は、すべて拒否されます。
- eDirectoryユーザパスワードの有効期限が切れた場合、そのユーザのeDirectoryバインド要求は拒否されます。

LDAPクライアントにeDirectory権を割り当てる

1 LDAPクライアントがeDirectoryにアクセスするときに使用するユーザ名のタイプを決定します。
   - ［Public］ユーザ(匿名バインド)

- プロキシユーザ(プロキシユーザ匿名バインド)
- NDSユーザ(NDSユーザバインド)

詳細については、365 ページの 「LDAPからeDirectoryに接続する」を参照してください。

2 ユーザが1つの代理ユーザまたは複数のeDirectoryユーザ名でLDAPにアクセスする場合、iManagerを使用して、eDirectory内またはLDAPでこれらのユーザ名を作成します。

3 LDAPクライアントが使用するユーザ名に、適切なeDirectory権を割り当てます。

ほとんどのユーザに割り当てられるデフォルトの権利では、ユーザ自身が持つオブジェクト以外にはアクセスできません。別のオブジェクトやその属性にアクセスするには、eDirectoryで割り当てられた権利を変更する必要があります。

LDAPクライアントからeDirectoryオブジェクトおよび属性へのアクセスが要求されると、eDirectoryは、LDAPクライアントのeDirectory識別情報に基づいて要求を受諾または拒否します。識別情報はバインド時に設定されます。

クラスと属性のマッピング

クラスとは、ディレクトリ内のオブジェクトのタイプ(ユーザ、サーバ、グループなど)です。属性とは、特定のオブジェクトについての追加情報を定義するディレクトリ要素です。たとえば、ユーザオブジェクト属性にはユーザの姓、電話番号などがあります。

スキーマとは、ディレクトリで使用できるクラスと属性、およびディレクトリ構造(クラス間の相互関係)を定義する一連の規則です。LDAPディレクトリとeDirectoryディレクトリのスキーマが異なる場合は、LDAPクラスと属性を、適切なeDirectoryオブジェクトと属性へマッピングしなければならない場合があります。これらのマッピングで、LDAPスキーマからeDirectoryスキーマへの名前の変換を定義します。

LDAP Services for eDirectoryにはデフォルトマッピングがあります。LDAPクラスおよび属性と、eDirectoryオブジェクトタイプおよびプロパティとの対応関係は多くの場合論理的で、直観的に理解できます。ただし、実装時の条件によっては、クラスと属性のマッピングを再設定する必要が生じることもあります。

ほとんどの場合、LDAPクラスとeDirectoryオブジェクトタイプとの間のマッピングは、一対一の対応関係です。ただし、LDAPスキーマでは、同じ属性を意味するCNおよび共通名のような別名もサポートされています。

LDAPグループ属性をマッピングする

デフォルトのLDAP Services for eDirectory環境設定には、事前定義されたクラスと属性のマッピングがあります。これは、LDAP属性のサブセットからeDirectory属性のサブセットへのマッピングです。デフォルト環境設定でマッピングされていない属性には、自動生成されたマッピングが割り当てられます。スキーマ名がスペースまたはコロンを含まない有効なLDAP名である場合は、マッピングは必要ありません。クラスおよび属性のマッピングを調べて、必要に応じて再設定します。

1 NetIQ iManagerで、［**役割およびタスク**］ボタン をクリックします。

2 ［**LDAP**］>［**LDAPオプション**］>［**LDAPグループの表示**］の順にクリックします。

3 LDAPグループオブジェクトをクリックし、［**属性マップ**］をクリックします。

4 必要に応じて属性を追加、削除、または変更します。

LDAP属性の種類によっては別名(CNおよび共通名など)が存在する場合があるため、複数のLDAP属性を対応する1つのeDirectory属性名にマッピングする必要が生じることがあります。LDAP Services for eDirectoryがLDAP属性情報を返す場合、リスト内で検出された最初の一致する属性の値が返されます。

複数のLDAP属性を1つのeDirectory属性にマッピングする場合は、属性の順序に意味があります。リスト内の順序を変更することにより、属性の優先度を変更できます。

5 **適用**をクリックし、**OK**をクリックします。

LDAPグループのクラスマッピング

LDAPクライアントがLDAPサーバにLDAPクラス情報を要求すると、サーバは対応するeDirectoryクラス情報を返します。デフォルトのLDAP Services for eDirectory環境設定には、事前定義されたクラスと属性のマッピングがあります。

注: eDirectoryでは、LDAPグループオブジェクトのクラスマッピングはLDAPサーバ間では伝搬しません。複数のサーバ上で同じクラスマッピングを使用するには、環境内のすべてのLDAPグループオブジェクトに、マッピングを手動で追加します。

---

1 NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。

2 ［**LDAP**］ > ［**LDAPオプション**］をクリックする。

3 LDAPグループオブジェクトをクリックし、［**クラスマップ**］をクリックします。

4 必要に応じてクラスを追加、削除、または変更します。

デフォルトのLDAP Services for eDirectory環境設定には、事前定義されたクラスと属性のマッピングがあります。これは、LDAPクラスと属性のサブセットからeDirectoryクラスと属性のサブセットへのマッピングです。デフォルト環境設定でマッピングされていない属性またはクラスには、自動生成されたマッピングが割り当てられます。

スキーマ名がスペースまたはコロンを含まない有効なLDAP名である場合は、マッピングは必要ありません。クラスおよび属性のマッピングを調べて、必要に応じて再設定します。

5 **適用**をクリックし、**OK**をクリックします。

LDAPクラスと属性をマッピングする

LDAPディレクトリとeDirectoryディレクトリのスキーマは異なるため、LDAPクラスと属性を、適切なeDirectoryオブジェクトと属性へマッピングする必要があります。これらのマッピングで、LDAPスキーマからeDirectoryスキーマへの名前の変換を定義します。

有効なLDAPスキーマ名であれば、スキーマエントリに対するLDAPスキーママッピングは必要ありません。LDAPでは、スキーマ名で使用できる文字は英数字とハイフン記号(-)だけです。LDAPスキーマ名ではスペースは使用できません。

スキーマをLDAPの外部に拡張する場合、.schファイルなどLDAPの外部にスキーマを拡張した後でオブジェクトIDによる検索を確実に実行するには、LDAPサーバ環境設定をリフレッシュする必要があります。

多対一マッピング

eDirectoryからLDAPをサポートするために、LDAP Servicesは、(ディレクトリサービスレベルではなく)プロトコルレベルのマッピングを使用して、LDAPとeDirectoryの間で属性とクラスを変換します。したがって、2つのLDAPクラスまたは属性を同じeDirectoryクラスまたは属性にマッピングできます。

たとえば、LDAPを使用してCnを作成し、CommonName=Valueを検索すると、Cnと属性値が同じ可能性のあるcommonNameが返されます。

すべての属性を要求すると、そのクラスのマッピングリストの最初にある属性が返されます。名前で属性を要求すると、正しい名前が返されます。

多対一クラスマッピング

LDAPクラス名	eDirectoryクラス名
alias aliasObject	別名
groupOfNames groupOfUniqueNames group	グループ
mailGroup rfc822mailgroup	NSCP:mailGroup1

多対一属性マッピング

LDAP属性名	eDirectory属性名
c countryName	C
cn commonName	CN
uid userId	uniqueID (固有ID)
description multiLineDescription	説明
l localityname	L
member uniqueMember	Member (メンバー)
o organizationname	O
ou organizationalUnitName	OU
sn surname	Surname (名字)
st stateOrProvinceName	S
certificateRevocationList;binary certificateRevocationList	ndspkiCertificateRevocationList
authorityRevocationList;binary authorityRevocationList	authorityRevocationList
deltaRevocationList;binary deltaRevocationList	deltaRevocationList
cACertificate;binary cACertificate	cACertificate
crossCertificatePair;binary crossCertificatePair	crossCertificatePair

LDAP属性名	eDirectory属性名
userCertificate;binary userCertificate	userCertificate

注: ;binaryの付いた属性はセキュリティに関連しています。これらは、アプリケーションが;binaryを付けて取得された名前を必要とする場合のために、マッピングテーブル内に存在します。;binaryを付けずに取得した名前が必要な場合は、マッピングの順序を変更できます。

非標準スキーマ出力を有効にする

eDirectoryには、互換モードスイッチがあります。この機能により、非標準スキーマ出力が使用できるため、現行のADSIクライアントおよび従来のNetscape*クライアントでスキーマを読み込むことができます。このスイッチは、LDAPサーバオブジェクト内の属性を設定することにより実装されます。属性名はnonStdClientSchemaCompatModeです。通常の場合、LDAPサーバオブジェクトはサーバオブジェクトと同じコンテナ内にあります。

非標準出力は、LDAP用の現行IETF規格には適合しませんが、現行バージョンのADSIクライアントおよび従来のクライアントでは正常に処理できます。

非標準出力の出力形式は次のとおりです。

- SYNTAX OIDは一重引用符で囲まれます。
- 上限は出力されません。
- X-オプションは出力されません。
- 複数の名前が存在する場合は、最初に検出された名前だけが出力されます。
- OIDが定義されていない属性やクラスは、それぞれ小文字で「attributename-oid」、「classname-oid」と出力されます。
- 名前にハイフンが含まれていてOIDが定義されていない属性またはクラスは出力されません。

OIDまたはオブジェクト識別子は、自身の属性またはobjectclassをLDAPサーバに追加するのに必要なオクテット数値の文字列です。

非標準スキーマ出力を有効化するには、次を実行します。

1. NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**LDAP**］ > ［**LDAPオプション**］をクリックする。
3. ［**LDAPサーバの表示**］をクリックし、LDAPサーバオブジェクトをクリックします。
4. ［**検索**］をクリックし、［**古いADSIおよびNetscapeスキーマ出力を有効にする**］をクリックします。

   非標準の出力は、現在IETFがLDAPについて定義している規格に準拠していませんが、現在のADSIクライアントおよび以前のNetscapeクライアントでは動作します。
5. ［**適用**］、［**情報**］の順にクリックし、［**リフレッシュ**］をクリックします。

構文の相違

LDAPとeDirectoryでは使用される構文が異なります。次のような重要な相違点があります。

- 372 ページの 「コンマ」

- 372 ページの 「タイプ付きの名前」
- 372 ページの 「エスケープ文字」
- 373 ページの 「複数のネーミング属性」

コンマ

LDAPでは、区切り記号としてピリオドではなくコンマを使用します。たとえば、eDirectoryの識別名(完全名)は次のように記述します。

CN=JANEB.OU=MKTG.O=EMA

LDAP構文を使用すると、同じ識別名は次のようになります。

CN=JANEB,OU=MKTG,O=EMA

また、次は別のLDAP識別名の例です。

CN=Bill Williams,OU=PR,O=Bella Notte Corp
CN=Susan Jones,OU=Humanities,O=University College London,C=GB

タイプ付きの名前

eDirectoryでは、タイプなしの名前(.JOHN.MARKETING.ABCCORP)とタイプ付きの名前(CN=JOHN.OU=MARKETING.O=ABCCORP)の両方を使用します。LDAPでは、区切り記号としてコンマを使用したタイプ付きの名前(CN=JOHN,OU=MARKETING,O=ABCCORP)だけを使用します。

エスケープ文字

LDAP識別名では、エスケープ文字として円記号(\)を使用します。1つの円記号とプラス記号(+)またはコンマ(,)を指定すると、識別名を拡張できます。

次に例を示します。

CN=Pralines\+Cream,OU=Flavors,O=MFG (CN is Pralines+Cream)

CN=D. Cardinal,O=Lionel\,Turner and Kaye,C=US (OはLionel、Turner、およびKaye)

詳細については、Internet Engineering Task ForceのRFC 2253 (http://www.ietf.org/rfc/rfc2253.txt?number=2253)を参照してください。

複数のネーミング属性

オブジェクトは、スキーマ内の複数のネーミング属性を使用して定義できます。LDAPとeDirectoryのユーザオブジェクトには、いずれもCNとUIDの2つのネーミング属性があります。識別名の中のネーミング属性は、プラス記号(+)で区切ります。属性に明示的なラベルが付いていない場合は、スキーマによりそれぞれの文字列に対応する属性が決定されます(eDirectoryとLDAPの両方で、最初の文字列はCN、次の文字列はUIDになります)。識別名の中の各部分に手動でラベルを付けると、ネーミング属性の順序を変更できます。

2つの相対識別名の例を次に示します。

Smith (CNはSmith CN=Smith)

Smith+Lisa (CNはSmith、UIDはLisa CN=Smith UID=Lisa)

2つの相対識別名(SmithとSmith+Lisa)は、2つの異なる相対識別名によって参照されるため、同じコンテキスト内に共存することができます。

サポートされるNetIQ LDAPコントロールと拡張

LDAPクライアントとLDAPサーバは、LDAP 3プロトコルを使用することにより、コントロールと拡張を適用してLDAP操作を拡張できます。コントロールと拡張を使用することによって、要求や応答の一部として追加情報を指定できます。拡張された各操作は、自身の属性またはobjectclassをLDAPサーバに追加するのに必要な、オクテット数値の文字列であるオブジェクト識別子(OID)により識別されます。LDAPクライアントは、実行するべき拡張操作のOID、およびその拡張操作に固有なデータを指定して、拡張操作要求を送信できます。LDAPサーバはこの要求を受信すると、拡張操作を実行し、OIDと追加データが設定された応答をクライアントに送信します。

たとえば、クライアントがサーバに検索要求を送信するとき、ソートを指定するコントロールをこの要求に入れることができます。サーバはこの検索要求を受け取ると、検索結果をソートしてから、その結果をクライアントに戻します。コントロールはサーバからクライアントに送ることもできます。たとえば、サーバは、クライアントにパスワード期限切れを通知する認証要求のコントロールを送ることができます。

デフォルトでは、起動直後のeDirectory LDAPサーバは、すべてのシステム拡張ならびに選択されたオプション拡張およびコントロールをロードできる状態にあります。オプション拡張に対応するLDAPサーバオブジェクトのextensionInfo属性により、システム管理者は、オプション拡張およびコントロールの選択と選択解除ができます。

拡張操作を有効にするため、LDAP 3プロトコルはルートDSE内のsupportedControl属性およびsupportedExtension属性に含まれる、サポートされているコントロールと拡張のリストをサーバに要求します。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、432ページの 「LDAPサーバの情報を取得する」を参照してください。

サポートされているLDAPコントロールと拡張のリストについては、『LDAP and eDirectory Integration NDK』の「LDAP Controls (http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/cchbehhc.html)」と「LDAP Extensions (http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/a6ik7oi.html)」を参照してください。

LinuxでのLDAPツールの使用

eDirectoryには、/opt/novell/eDirectory/binに格納されている、LDAPツールがあり、これらはLDAPディレクトリサーバを管理するのに役立ちます。

注: eDirectory 9.0以降、PEM証明書は特定のTLS変数経由で渡されます。これらの変数は/etc/opt/novell/eDirectory/conf/openldap/ldap.confファイルで定義するか、個別にエクスポートできます。詳細については、OpenLdapマニュアルのWebサイトおよびマニュアルページを参照してください。

ツール	説明
ice	エントリをファイルからLDAPディレクトリにインポートし、ファイルのディレクトリ内のエントリを変更し、エントリをファイルにエクスポートし、ファイルの属性とクラス定義を追加します。
ldapadd	LDAPディレクトリに新しいエントリを追加します。
ldapdelete	LDAPディレクトリサーバからエントリを削除します。ldapdeleteツールは、LDAPサーバとの接続を開始し、エントリのバインドと削除を行います。
ldapmodify	LDAPサーバとの接続を開始し、エントリのバインド、変更、追加を行います。
ldapmodrdn	LDAPディレクトリサーバ内のエントリの相対識別名(RDN)を変更します。LDAPサーバとの接続を開始し、エントリのRDNのバインドと変更を行います。
ldapsearch	LDAPディレクトリサーバでエントリを検索します。LDAPサーバとの接続を開始し、バインドを行い、指定されたフィルタを使用して検索を実行します。フィルタは、RFC 2254 (http://www.ietf.org/rfc/rfc2254.txt)で定義されたLDAPフィルタの文字列表現に準拠している必要があります。
ndsindex	インデックスの作成、一覧表示、一時停止、再開、削除を行います。

詳細については、『*LDAP Libraries for C Doc*』の「LDAP Tools (http://developer.novell.com/ndk/doc/cldap/ltoolenu/data/hevgtl7k.html)」を参照してください。

LDAPツールを安全に実行するには、「Linuxコンピュータ上のeDirectory操作をセキュリティで保護する」を参照し、安全にeDirectoryとLDAPを接続するためのコマンドラインによるLDAP操作にPEMファイルを指定します。

LDAPツール

LDAPユーティリティは、エントリの削除、変更、追加、スキーマの拡張、相対識別名の変更、エントリの新規コンテナへの異動、検索インデックスの作成、検索の実行に使用できます。

注: RFC 2256に準拠するため、eDirectoryのLDAPインタフェースでは、パスワードの長さが128文字以下の場合にのみ、バインドが許可されます。また、パスワードをLDAPから設定する場合、最大128文字のパスワードのみ設定できます。

ldapadd

ldapaddユーティリティを使用して、新しいエントリを追加します。構文は次のとおりです。

```
ldapadd [-c] [-C] [-l] [-M] [-P] [-r] [-n] [-v] [-F] [-l limit] [-M[M]] [-d
debuglevel] [-D  binddn] [[-W]| [-w passwd]] [-h  ldaphost] [-p ldapport] [-P
version] [-Z[Z]] [-f file]
```

-fオプションが指定されていると、ldpaddは変更をファイルから読み出します。-fオプションが指定されていないと、ldpaddは変更をstdinから読み出します。

ヒント: LDAPユーティリティからの出力はstdoutに送られます。出力を見る前にユーティリティが終了する場合は、出力をファイルにリダイレクトしてください。例: ldapadd [options] > out.txt

オプション	説明
-a	新しいエントリを追加します。ldapmodifyのデフォルトは、既存エントリの変更です。ldapaddとして呼び出されると、このフラグは常にオンになります。
-r	デフォルトでは既存の値を置換します。
-c	連続操作モード。エラーが通知されても、ldapmodifyは変更動作を継続します。デフォルトでは、エラーが通知されると終了します。
-f *file*	エントリ情報を標準入力ではなくLDIFファイルから読み出します。レコードの最大長は4096行です。
-F	replica:で始まる入力行の内容に関わりなく、すべての変更を強制的に適用します。デフォルトでは、replica:行が使用中のLDAPサーバホストおよびポートと照らして比較され、replogレコードを実際に適用するべきかどうかが判断されます。

すべてのLDAPツールの共通オプション

すべてのLDAPツールに共通するオプションがいくつかあります。次の表は、これらのオプションを表示したものです。

オプション	説明
-C	後に続く参照(匿名バインド)を有効にします。
-d *debuglevel*	LDAPデバッグレベルをdebuglevelに設定します。このオプションを有効にするには、ldapmodifyをコンパイルするときにLDAP_DEBUGの定義が必要です。
-D *binddn*	binddnを使用してLDAPディレクトリにバインドします。*binddn*には、RFC 1779に定義されている文字列表現のDNを指定します。
-f *file*	ファイルから行を読み取り、1行ごとにLDAP検索を実行します。この場合、コマンドラインで指定したフィルタは、%sが最初に出現した個所がファイルの行に置換されるというパターンとして機能します。1つのハイフン(-)文字がファイルとして指定された場合には、標準入力から行が読み取られます。
-h *ldaphost*	LDAPサーバの実行場所となっている代替ホストを指定します。
-l *limit*	接続タイムアウト(秒)を指定します。
-M	Manage DSA ITコントロール(非クリティカル)を有効にします。
-MM	Manage DSA ITコントロール(クリティカル)を有効にします。
-n	完了した場合の結果を表示しますが、実際にはエントリを変更しません。-vと組み合わせて使用すると、デバッグ時に便利です。
-p *ldapport*	LDAPサーバがリスンする代替TCP™ポートを指定します。
-P *version*	LDAPのバージョン(2または3)を指定します。

オプション	説明
-v	冗長モードが設定され、多くの診断メッセージが標準出力に書き込まれます。
-w *passwd*	簡易認証のパスワードとして、*passwd*を使用します。
-W	簡易認証のプロンプトです。コマンドラインにパスワードを指定するかわりに、このオプションが使用されます。
-Z	操作をバインドして実行する前に、TLSを開始します。TLSを開始する操作の途中でエラーが発生すると、エラーは無視され操作は続行されます。エラーが発生した場合に操作を中止するには、このオプションではなく-ZZオプションの使用をお勧めします。 このオプションでポートが指定されている場合、そのポートはクリアテキスト接続を受信する必要があります。 サーバの識別情報を確認するには、このオプションを-eオプションと組み合わせて使用し、サーバ証明書ファイルを指定する必要があります。TLSを開始すると、これによりサーバのルート認証局証明書が確認されます。-eオプションが指定されていない場合、サーバからのすべての証明書が許可されます。
-ZZ	操作をバインドして実行する前に、TLSを開始します。TLSを開始する操作の途中でエラーが発生すると、操作は中止されます。 このオプションでポートが指定されている場合、そのポートはクリアテキスト接続を受信する必要があります。 サーバの識別情報を確認するには、このオプションを-eオプションと組み合わせて使用し、サーバ証明書ファイルを指定する必要があります。TLSを開始すると、これによりサーバのルート認証局証明書が確認されます。-eオプションが指定されていない場合、サーバからのすべての証明書が許可されます。

例

/tmp/entrymodsファイルが存在し、その内容が次のようであると仮定します。

```
dn: cn=Modify Me, o=University of Michigan, c=US

changetype: modify

replace: mail

mail: modme@terminator.rs.itd.umich.edu

-

add: title

title: Manager

-

add: jpegPhoto

jpegPhoto: /tmp/modme.jpeg

-

delete: description
```

-

この場合、コマンドldapmodify -b -r -f /tmp/entrymodsは、Modify Meエントリのmail属性の中身をmodme@terminator.rs.itd.umich.eduの値に置き換え、Managerというタイトルを追加し、/tmp/modme.jpegファイルの内容をjpegPhotoとして追加し、description属性を完全に削除します。

このような変更は、以下のようにldapmodifyの古い入力規則を使用して実行することもできます。

```
cn=Modify Me, o=University of Michigan, c=US

mail=modme@terminator.rs.itd.umich.edu

+title=Manager

+jpegPhoto=/tmp/modme.jpeg

-description
```

コマンドは次のようになります。

```
ldapmodify -b -r -f /tmp/entrymods
```

/tmp/newentryファイルが存在し、その内容が次のようであると仮定します。

```
dn: cn=Barbara Jensen, o=University of Michigan, c=US

objectClass: person

cn: Barbara Jensen

cn: B Jensen

sn: Jensen

title: Manager

mail: bjensen@terminator.rs.itd.umich.edu

uid: bjensen
```

この場合、/tmp/newentryファイルの値を使用して、コマンドldapadd -f /tmp/entrymodsはB Jensenの新しいエントリを追加します。

/tmp/newentryファイルが存在し、その内容が次のようであると仮定します。

```
dn: cn=Barbara Jensen, o=University of Michigan, c=US

changetype: delete
```

この場合、コマンドldapmodify -f /tmp/entrymodsはB Jensenのエントリを削除します。

ldapdelete

ldapdeleteユーティリティは、指定したインデックスを削除します。LDAPサーバとの接続を開始し、バインドしてから削除します。構文は次のとおりです。

```
ldapdelete [-n] [-v] [-c] [-r] [-l] [-C] [-M] [-d debuglevel] [-f file] [-D binddn]
[[-W]| [-w passwd]] [-h ldaphost] [-p ldapport] [-Z[Z]] [dn]...
```

dnパラメータは、削除するエントリの識別名のリストです。

これは、-fオプションと次の方法でやり取りします。

- コマンドラインに-fオプションがなく、コマンドラインでDNが指定されている場合、ユーティリティにより指定したエントリが削除されます。
- コマンドラインにdnと-fの両方がある場合、ユーティリティは削除するDNをファイルから読み込んで、コマンドラインのDNは無視します。
- コマンドラインにdnと-fオプションがない場合、ユーティリティはstdinからdnを読み込みます。

ヒント: LDAPユーティリティからの出力はstdoutに送られます。出力を見る前にユーティリティが終了する場合は、出力をファイルにリダイレクトしてください。例: ldapdelete [options] > out.txt

オプション	説明
-c	連続操作モード。エラーが通知されても、ldapdeleteは削除動作を継続します。デフォルトでは、エラーが通知されると終了します。
-f *file*	ファイルから行を読み取り、1行ごとにLDAP検索を実行します。この場合、コマンドラインで指定したフィルタは、%sが最初に出現した個所がファイルの行に置換されるというパターンとして機能します。
-r	再起的に削除します。

注: 共通オプションについての詳細は、375 ページの 「すべてのLDAPツールの共通オプション」を参照してください。

例

ldapdeleteのコマンド「cn=Delete Me, o=University of Michigan, c=US」では、「University of Michigan」組織のエントリの真下にあるcommonName「Delete Me」で指定されたエントリを削除します。この場合、削除が許可されるためにはbinddnおよびpasswdを指定する必要があります(-Dオプションおよび-wオプションを参照)。

ldapmodify

ldapmodifyユーティリティを使用すると、既存エントリの属性を変更したり、新規エントリを追加することができます。構文は次のとおりです。

```
ldapmodify [-a] [-c] [-C] [-M] [-P] [-r] [-n] [-v] [-F] [-l limit] [-M[M]] [-d
debuglevel] [-D binddn] [[-W]|[-w passwd]] [-h ldaphost] [-p ldap-port] [-P
version] [-Z[Z]] [-f file]
```

-fオプションを指定すると、ldapmodifyにより変更がファイルから読み出されます。-fオプションを指定しない場合、変更はstdinから読み出されます。

ヒント: LDAPユーティリティからの出力はstdoutに送られます。出力を見る前にユーティリティが終了する場合は、出力をファイルにリダイレクトしてください。例: ldapmodify [options] > out.txt

オプション	説明
-a	新しいエントリを追加します。ldapmodifyのデフォルトは、既存エントリの変更です。ldapaddとして呼び出されると、このフラグは常にオンになります。
-r	デフォルトでは既存の値を置換します。
-c	連続操作モード。エラーが通知されても、ldapmodifyは変更動作を継続します。デフォルトでは、エラーが通知されると終了します。
-f *file*	エントリ情報を標準入力ではなくLDIFファイルから読み出します。レコードの最大長は4096行です。
-F	replica:で始まる入力行の内容に関わりなく、すべての変更を強制的に適用します。デフォルトでは、replica:行が使用中のLDAPサーバホストおよびポートと照らして比較され、replogレコードを実際に適用するべきかどうかが判断されます。

注: 共通オプションについての詳細は、「375ページの 「すべてのLDAPツールの共通オプション」」を参照してください。

ldapmodrdn

ldapmodrdnを使用すると、エントリの相対識別名を変更できます。また、エントリを新しいコンテナに移動することもできます。構文は次のとおりです。

```
ldapmodrdn [-r] [-n] [-v] [-c] [-C] [-l] [-M] [-s newsuperior] [-d debuglevel] [-D
binddn] [[-W]|[-w  passwd]]  [-h ldaphost] [-p ldapport] [-Z[Z]] [-f file] [dn
newrdn]
```

注: LDAPユーティリティからの出力はstdoutに送られます。出力を見る前にユーティリティが終了する場合は、出力をファイルにリダイレクトしてください。例: ldapmodrdn [options] > out.txt

オプション	説明
-c	連続操作モード。エラーが通知されても、ldapmodifyは変更動作を継続します。デフォルトでは、エラーが通知されると終了します。
-f *file*	エントリ変更情報を標準入力やコマンドラインではなくファイルから読み出します。古いRDNと新規RDNの間に空白行がないことを確認します。空白行があると、-fオプションは失敗します。
-r	エントリから旧RDN値を削除します。デフォルトでは、以前の値が保持されます。
-s *newsuperior*	エントリの移動先のコンテナの識別名を指定します。

注: 共通オプションについての詳細は、すべてのLDAPツールの共通オプションを参照してください。

例

/tmp/entrymodsファイルが存在すると仮定すると、次のような内容になります。

```
cn=Modify Me, o=University of Michigan, c=US

cn=The New Me
```

ldapsearch

ldapsearchユーティリティは、指定された属性とオブジェクトクラスのディレクトリを検索します。構文は次のとおりです。

```
ldapsearch [-n] [-u] [-v] [-t] [-A] [-T] [-C] [-V] [-M] [-P] [-L] [-d debuglevel]
[-f file] [-D binddn] [[-W]| [-w bindpasswd]] [-h ldaphost] [-p ldapport] [-b
searchbase] [-s scope] [-a deref] [-l time limit] [-z size limit] [-Z[Z]] filter
[attrs....]
```

ldapsearchツールはLDAPサーバとの接続を開始し、バインドを行い、フィルタを使用して検索を実行します。フィルタは、RFC 2254 (http://www.ietf.org/rfc/rfc2254.txt)で定義されたLDAPフィルタの文字列表現に準拠している必要があります。

ldapsearchが1つ以上のエントリを検出すると、attrsで指定された属性が取得され、エントリと値が標準出力に書き込まれます。属性がリストされない場合、すべての属性が戻ります。

ヒント: LDAPユーティリティからの出力はstdoutに送られます。出力を見る前にユーティリティが終了する場合は、出力をファイルにリダイレクトしてください。例: ldapsearch [options] filter [attribute list] > out.txt

---

オプション	説明
-a *deref*	別名の逆参照の処理方法を指定します。次の値を使用します。 ◆ ［Never］:ベースオブジェクトを探すときと検索するときの両方で、別名の逆参照は行われません。 ◆ ［Always］: ベースオブジェクトを探すときと検索するときの両方で、別名の逆参照を常に行います。 ◆ ［Search］:ベースオブジェクトの従属を検索するときは別名の逆参照を行いますが、ベースオブジェクトを探すときには行いません。 ◆ ［Find］: ベースオブジェクトを探すときは別名の逆参照を行いますが、ベースオブジェクトのサブオーディネートを従属するときには行いません。
-A	値ではなく、属性のみ取り込まれます。エントリに属性が存在するかどうかを確認して、具体的な属性値を知る必要がない場合に便利です。
-CC	後に続く参照(同じバインドDNとパスワードで認証されたバインド)を有効にします。
-b *searchbase*	*searchbase*を検索の開始ポイントとして使用します。
-L	エントリをLDIF形式で出力します。
-LL	エントリをLDIF形式で出力します。コメントは出力されません。

オプション	説明
-LLL	エントリをLDIF形式で出力します。コメントおよびバージョンは出力されません。
-s *scope*	検索のスコープを指定します。スコープとして、ベースオブジェクトを示す「base」、1レベルを示す「one」、またはサブツリー検索を示す「sub」を指定します。デフォルトは「sub」です。
-S *attribute*	戻されたエントリを属性に基づいてソートします。デフォルトでは、戻ったエントリのソートを行いません。属性が長さ0の文字列("")の場合、エントリはその識別名のコンポーネントによりソートされます。詳細については、ldap_sortを参照してください。通常は、ldapsearchはエントリを受け取った順に出力します。-Sオプションを指定するとデフォルトが無効になり、すべてのエントリが取得され、ソートされてから出力されます。
-t	検索されたバイナリ値が一時ファイルに書き込まれます。これは、jpegの写真やオーディオなどASCII以外の値を扱うときに便利です。
-tt	すべての値が一時ファイルに書き込まれます。
-T *path*	ファイルをパス(デフォルト: /tmp)で指定されたディレクトリに書き出します。
-u	識別名(DN)をユーザにわかりやすい形式で出力します。
-V	ファイルのURLプリフィックスです。
-V *prefix*	ファイルのURLプレフィックスを指定します(デフォルト: file://tmp/)。
-z *sizelimit*	検索が終了するまで最大*sizelimit*エントリだけ待機します。

注: 共通オプションについての詳細は、「375ページの 「すべてのLDAPツールの共通オプション」」を参照してください。

例

次のコマンドを実行します。

```
ldapsearch "cn=mark smith" cn telephoneNumber
```

commonName「mark smith」のエントリのサブツリー検索(デフォルトの検索ベースを使用)を実行します。commonNameの値およびtelephoneNumberの値が取得され、標準出力に表示されます。2つのエントリが検出された場合、次のように出力されます。

```
cn=Mark D Smith, ou="College of Literature, Science, and the Arts", ou=Students,
ou=People, o=University of Michigan, c=US

cn=Mark Smith

cn=Mark David Smith

cn=Mark D Smith 1

cn=Mark D Smith

telephoneNumber=+1 313 930-9489
```

```
cn=Mark C Smith, ou=Information Technology Division, ou=Faculty and Staff,
ou=People,o=University of Michigan, c=US

cn=Mark Smith

cn=Mark C Smith 1

cn=Mark C Smith

telephoneNumber=+1 313 764-2277
```

コマンド:

```
ldapsearch -u -t "uid=mcs" jpegPhoto audio
```

デフォルトの検索ベースを使用して、ユーザID「mcs」のエントリのサブツリー検索を実行します。エントリのDNは、DN自体を含む行の後にわかりやすい形式で出力されます。また、Jpegの写真の値およびオーディオの値が取得され、一時ファイルに書き込まれます。要求された属性がそれぞれ1つの値をもつエントリが１つ検出された場合、次のように出力されます。

```
cn=Mark C Smith, ou=Information Technology Division, ou=Faculty and Staff,
ou=People, o=University of Michigan, c=US

Mark C Smith, Information Technology Division, Faculty and Staff, People,
University of Michigan, US

audio=/tmp/ldapsearch-audio-a19924

jpegPhoto=/tmp/ldapsearch-jpegPhoto-a19924
```

次のコマンドは、organizationNameが「university」で始まるすべての組織のc=USレベルで、1レベルの検索を実行します。

```
ldapsearch -L -s one -b "c=US" "o=university*" o description
```

検索結果はLDIF形式で表示されます。organizationNameの値および記述属性の値が取得され、標準出力に書き込まれます。出力結果の例は次のようになります。

```
dn: o=University of Alaska Fairbanks, c=US

o: University of Alaska Fairbanks

description: Preparing Alaska for a brave new yesterday.

description: leaf node only

dn: o=University of Colorado at Boulder, c=US

o: University of Colorado at Boulder

description: No personnel information

description: Institution of education and research

dn: o=University of Colorado at Denver, c=US

o: University of Colorado at D
```

ndsindex

ndsindexユーティリティは、インデックスと複合インデックスを作成、一覧表示、一時停止、再開、または削除します。複合インデックスについては、ndsindexユーティリティで$の符号で区切られた複数の属性を指定できます。構文は次のとおりです。

注

- 複合インデックスの場合は複数の属性を指定できます。NetIQでは、パフォーマンス向上のために最大3つまでの属性を入力することをお勧めします。値タイプの複合インデックスの場合、最大5つの属性を追加できます。
- ndsindexユーティリティの接続先は、インデックスを追加したのと同じサーバにするようお勧めします。

```
ndsindex list [-h <hostname>] [-p <port>] -D <bind DN> -W|[-w <password>] [-l
limit] -s <eDirectory Server DN> [-Z[Z]] [<indexName1>, <indexName2>.....]
```

```
ndsindex add -a [-h <hostname>] [-p <port>] -D <bind DN> -W|[-w <password>] [-l
limit] -s <eDirectory Server DN> [-Z[Z]] <indexDefinintion1>
[<indexDefinintion2>.....]
```

注

- 先祖IDを持つインデックスはvalueインデックスタイプでのみ作成できます。PresenceおよびSubstringのインデックスタイプで先祖IDを使用することはできません。
- 先祖IDを持つインデックスを作成すると、データベースサイズが大きくなります。

```
ndsindex delete [-h <hostname>] [-p <port>] -D <bind DN> -W|[-w <password>] [-l
limit] -s <eDirectory Server DN> [-Z[Z]] <indexName1> [<indexName2>.....]
```

```
ndsindex resume [-h <hostname>] [-p <port>] -D <bind DN> -W|[-w <password>] [-l
limit] -s <eDirectory Server DN> [-Z[Z]] <indexName1> [<indexName2>.....]
```

```
ndsindex suspend [-h <hostname>] [-p <port>] -D <bind DN> -W|[-w <password>] [-l
limit] -s <eDirectory Server DN> [-Z[Z]] <indexName1> [<indexName2>.....]
```

オプション	説明
リスト	指定したインデックスを表示します。インデックスが指定されていない場合、ndsindexはサーバ上のすべての既存のインデックスを表示します。
add	新しいインデックスを作成します。
削除	指定したインデックスを削除します。
再開	指定したインデックスをオフラインの状態から再開します。
一時停止	指定したインデックスを一時停止してオフラインの状態にします。
-s *eDirectory Server DN*	eDirectoryサーバのDNを指定します。

注: 共通オプションについての詳細は、「375ページの 「すべてのLDAPツールの共通オプション」」を参照してください。

例

サーバMyHost上のインデックスを表示するには、次のコマンドを入力します。

```
ndsindex list -h MyHost -D cn=admin,o=mycompany -w password -s cn=MyHost,o=novell
```

電子メールの属性にMyIndexという名前の下位文字列インデックスを作成するには、次のコマンドを入力します。

```
ndsindex add -h myhost -D cn=admin, o=mycompany -w password -s cn=myhost, o=novell
"MyIndex;email address;substring"
```

市町村の属性にMyIndexという名前の値インデックスを作成するには、次のコマンドを入力します。

```
ndsindex add -h myhost -D cn=admin,o=mycompany -w password -s cn=myhost,o=novell
"MyIndex;city;value"
```

自宅電話番号の属性にMyIndexという名前の存在インデックスを作成するには、次のコマンドを入力します。

```
ndsindex add -h myhost -D cn=admin,o=mycompany -w password -s cn=myhost,o=novell
"MyIndex;homephone;presence"
```

MyIndexという名前のインデックスを削除するには、次のコマンドを入力します。

```
ndsindex delete -h myhost -D cn=admin,o=mycompany -w password -s cn=myhost,o=novell
MyIndex
```

MyIndexという名前のインデックスを一時停止するには、次のコマンドを入力します。

```
ndsindex suspend -h myhost -D cn=admin,o=mycompany -w password -s
cn=myhost,o=novell MyIndex
```

MyIndexという名前のインデックスを再開するには、次のコマンドを入力します。

```
ndsindex resume -h myhost -D cn=admin,o=mycompany -w password -s cn=myhost,o=novell
MyIndex
```

複合インデックスの例

email addressとsurnameの属性にMyIndexという名前の値インデックスを作成するには、次のコマンドを入力します。

```
ndsindex add –h myhost –D cn=admin, o=mycompany –w password –s cn=myhost, o=netiq
'MyIndex;email address$surname;value'
```

注: タイプがPresenceおよびSubstringの複合インデックスを作成することはできません。

拡張可能一致検索フィルタ

RFC 2251 (http://www.ietf.org/rfc/rfc2251.txt)で定義されるLDAP 3のコアプロトコルを指定するには、LDAPサーバが拡張可能一致検索フィルタ機能を認識できなくてはなりません。拡張可能一致検索では、LDAPクライアントは検索フィルタに次の項目を指定することができます。

- オプションの属性名
- オプションの一致ルール
- DN属性がエントリの一部として考慮されるべきかを示すフラグ
- 一致検索に使用される値

拡張可能一致検索フィルタの文字列を次に示します。

```
extensible = attr [":dn"] [":" matchingrule] ":=" value /
             [:dn"] ":" matchingrule ":=" value
```

次の表は、拡張可能検索フィルタパラメータを表示したものです。

パラメータ	説明
attr	適合する属性を指定します。
[":*dn*"]	一致ルールが比較一致に含まれるていることを示します。
[":" *matchingrule*]	使用する一致ルールを指定します。
":="	一致ルールを指定しないと、完全一致とみなされます。
value	比較値

extensibleMatchは、LDAP 3から導入された新しいフィルタです。matchingRuleフィールドがない場合は、属性フィールドが必ず必要です。完全一致検索はその属性に対して実行されます。attributeフィールドがなく、matchingRuleが存在する場合、そのmatchingRuleをサポートするエントリ内のすべての属性がmatchValueと比較され、matchingRuleによりアサーション値の構文が決定されます。

フィルタ項目は次のように評価されます。

- TRUE:エントリに1件以上の一致があることを表します。
- FALSE:エントリに一致する属性がないことを表します。
- matchingRuleを認識できなかったり、assertionValueを解析できない場合は「未定義」とされます。

matchingRuleの他にtypeフィールドがある場合、matchingRuleはそのtypeで使用できるものでなくてはなりません。使用できない場合、フィルタ項目は定義されません。検索フィルタに:dnが指定されている場合、エントリの識別名に含まれるすべての属性に対して一致検索が適用されます。また、フィルタ項目の評価がTRUEの識別名が1つ以上属性を持っている場合も、評価はTRUEになります。dnAttributesフィールドがあるので、単語の一致検索などで、1つのルールをエントリに適用し、別のルールをエントリとDN属性に適用するというように、一般的な一致ルールを複数設定する必要がなくなります。

拡張可能一致検索フィルタにより、LDAPクライアントでは次の2つのことが可能になります。

- 同じタイプのデータに対し、複数の一致ルールをサポートできます。
- 検索条件にDN要素を含めることができます。

  DN指定により、DNの特定要素の一致検索を実行できます。

eDirectory 8.7.3以降のバージョンは、DN属性の照合用に拡張可能な一致フィルタをサポートします。拡張可能一致検索フィルタのもう一つの要素である一致ルールは未定義とみなされ、無視されます。DN一致検索を使用すると、LDAPクライアントでeDirectoryツリーからオブジェクトを簡単に検索できます。たとえば、

```
(&(ou:dn:=sales)(objectclass=user))
```

のような複雑なLDAP検索フィルタにより、セールスコンテナの下のセールスファンクションにあるすべてのユーザオブジェクトをリストすることができます。

使用例

次は、eDirectory 8.7.3以降でサポートされている、拡張可能な一致検索フィルタの文字列の例です。

```
(o:dn:=Ace Industry)
```

これは:dnの使用例です。一致を評価するとき、エントリの識別名の属性はエントリの一部とみなされることを表しています。これは、完全一致であることを意味します。

```
(:dn:2.4.8.10:=Dino)
```

これはエントリの属性に適用するフィルタの例です。一致ルールが2.4.8.10のDNの属性も考慮されます。

次は、eDirectory 8.7.3以降でサポートされて*いない*拡張可能一致検索検索フィルタの文字列の例です。

```
(cn:1.2.3.4.5:=John Smith)
```

この例は、属性タイプcnと値John Smithを指定するフィルタを表しています。一致ルールoid 1.2.3.4.5により、ディレクトリサーバにより一致検索が実行されます。

```
(sn:dn:2.4.6.8.10:=Barbara Jones)
```

これは:dnの使用例です。比較するときは一致ルール2.4.6.8.10を使用する必要があることと、一致を評価するときにはエントリの識別名の属性をエントリの一部とみなす必要があることを示します。

LDAPトランザクション

eDirectory LDAPサーバは、複数の更新操作を1つのアトミックな操作(トランザクションともいう)にまとめることをサポートします。eDirectoryのLDAPによるトランザクションのサポートは“LDAP Transactions” (http://www.watersprings.org/pub/id/draft-zeilenga-ldap-txn-05.txt)および“LDAP: Grouping of Related Operations” (http://www.watersprings.org/pub/id/draft-zeilenga-ldap-grouping-05.txt)という2つのインターネット仕様に基づいています。

LDAPトランザクションを使用することで、LDAPアプリケーションは複数のLDAP更新操作(追加、変更、削除、名前変更)をグループとして送信し、この操作のグループ全体をコミットまたは中止することができます。

次のように、LDAPトランザクションのコンテキストで出現するエンティティがいくつかあります。

- CreateGroupingRequest (2.16.840.1.113719.1.27.103.1) – これは関連する操作をグループ化するLDAP拡張操作です。拡張操作は要求されたグループ化のタイプを識別するcreateGroupTypeという値を保持します。LDAPトランザクションの場合、グループ化タイプはtransactionGroupingTypeです。(2.16.840.1.113719.1.27.103.8)
- CreateGroupingResponse (2.16.840.1.113719.1.27.103.1) – これはcreateGroupingRequestへのLDAPサーバの応答であり、groupCookieとオプションのcreateGroupValueという2つの応答フィールドが含まれています。
- GroupingControl (2.16.840.1.113719.1.27.103.7) - これは、このコントロールによって保持される値であるgroupCookieにより、グループ化に対する操作の関連付けを示すために使用されます。

- EndGroupingRequest (2.16.840.1.113719.1.27.103.2) – これは、グループ化要求の終了を示すために使用する、もう1つのLDAP拡張操作です。LDAPトランザクションの場合、これはトランザクションの終了を示し、最終的にトランザクションのコミットまたは中止になります。
- EndGroupingResponse (2.16.840.1.113719.1.27.103.2) – これは、endGroupingResponseに対するLDAPサーバの応答であり、成功または失敗をLDAPクライアントに示します。

LDAPトランザクションで、LDAPサーバとLDAPクライアントがやり取りする要求と応答のシーケンスは次のとおりです。

- サーバでアトミックな操作(つまりトランザクション)として処理する複数のLDAP操作をクライアントが送信する場合、最初にcreateGroupingRequestを送信する必要があります。その際、createGroupTypeはtransactionGroupingTypeとし、createGroupValueは付けません。
- eDirectoryサーバがトランザクションを処理できる場合、クライアントから要求されたグループ化を固有に識別するgroupingCookieとともに、成功の結果コードを返します。処理できない場合、サーバは失敗の理由を示す非成功の結果コードをクライアントに返します。
- クライアントがサーバから成功の結果コードを受け取ると、サーバから返されるgroupingCookieを含むGroupingControlをその後の更新操作に添付し、1つのトランザクションの一部として処理することを示します。サーバがトランザクションの一部として更新操作を処理できる場合、サーバは成功を返し、この要求をキューに入れます。サーバがトランザクションの一部として更新操作を処理できない場合、サーバは失敗の理由を示す非成功の結果コードをクライアントに返します。
- クライアントがグループ化コントロールを添付してすべての更新操作をサーバに送信した後、クライアントはgroupingCookieとともにendGroupingRequestをサーバに送信し、トランザクションを終了することを通知します。endGroupValueがない場合はコミット要求を示し、一方、空のendGroupValueは中止要求を示します。
- サーバは、1つのトランザクション内の保留中のすべての操作を適用します。成功すると、成功を返します。成功しなかった場合、非成功の結果コードを返します。
- クライアントとサーバ間の上記のやり取りの間のいずれかの時点で、サーバがトランザクションの指定の処理を続行できない場合、サーバはendGroupingNotice (2.16.840.1.113719.1.27.103.4)を発行します。その後、クライアントがcookieを使用し続けると、非成功の結果コードを含む応答を受け取ります。

rootDSEエントリのsupportedGroupingTypes属性にtransactionGroupingTypeが存在すれば、LDAPトランザクションがサポートされます。

eDirectoryのLDAPトランザクションの実装は、LDAPトランザクション仕様の古いバージョンに基づいています。本書の執筆時点で、LDAPトランザクションの最新リビジョンのドラフトは Lightweight Directory Access Protocol (LDAP) Transactions (http://tools.ietf.org/html/rfc5805)で参照できます。

制限

LDAPトランザクションの機能には、次の制限があります。

- トランザクションとしてグループ化された操作の影響を受けるすべてのオブジェクトは、サーバにローカルにホストされている必要があります。これらの操作のいずれにおいても、LDAPサーバが別のサーバにチェーンする必要はありません。
- スキーマの変更およびDN変更の操作(サブツリーの移動?)は、LDAPトランザクション内にグループ化できません。

- ストリーム構文のパスワードおよび属性は、LDAPトランザクションの一部として追加できません。
- 1つのトランザクションを別のトランザクションにネストすることはサポートされていません。

14 LDAP Services for NetIQ eDirectoryの環境設定

eDirectoryインストールプログラムにより、LDAP Services for NetIQ eDirectoryが自動的にインストールされます。eDirectoryのインストールについては、『*NetIQ eDirectoryインストールガイド*』を参照してください。

この章では、以下の説明を行います。

LDAPツールについては、「LDAPツールNDK (http://developer.novell.com/documentation/cldap/ltoolenu/data/hevgtl7k.html)」を参照してください。

LDAP Services for eDirectoryをロードおよびアンロードする

LDAP Services for eDirectoryをロードするには、次のコマンドを入力します。

サーバ	コマンド
Windows	［NDSCONS］画面で［nldap.dlm］を選択し、［開始］をクリックします。

サーバ	コマンド
Linux	Linuxコマンドプロンプトで、次のように入力します。 /opt/novell/eDirectory/sbin/nldap -l

LDAP Services for eDirectoryをアンロードするには、次のコマンドを入力します。

サーバ	コマンド
Windows	［DHOSTCONS)］画面で［nldap.dlm］を選択し、［停止］をクリックします。
Linux	LDAPをアンロードするには、［DHostemotemanagement］ページで［*LDAPv3 for NetIQ eDirectory*］アクションアイコンをクリックして停止します。 または Linuxコマンドプロンプトで、次のように入力します。 /opt/novell/eDirectory/sbin/nldap -u

LDAPサーバがロードされているか確認する

LDAPオブジェクトの設定を行う前に、LDAPサーバがロードされ、動作していることを確認します。この画面では、LDAPサーバがロードされているか確認する方法を説明します。サーバが動作しているか確認するには、「391ページの 「LDAPサーバが実行されているか確認する」」を参照してください。

Windowsの場合

1 Windowsサーバで、ndscons.exeを開きます。

［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、［nldap.dlm］までスクロールし、［ステータス］カラムを表示します。

カラムに［稼働中］と表示されます。

NetIQ iManagerを使用することもできます。

1 ［役割およびタスク］オプションをクリックします。

2 ［eDirectoryの保守］>［サービスマネージャ］の順にクリックします。

3 接続、サーバ、DNS名、またはIPアドレスを選択し、［OK］をクリックします。

4 パスワードを入力し、［OK］をクリックします。

5 ［LDAP Agent for NetIQ eDirectory 9.2］をクリックします。

［モジュール情報］セクションの［ファイル名］フィールドにnldap.nlmと表示されます。

Linuxの場合

LDAPサーバが実行されていることを確認するには、次のコマンドを実行します。

```
ndstrace -c modules | grep nldap
```

LDAPサーバがロードされていないか、実行されていない場合、nldapモジュールがロードされていないことを示すエラーが表示されます。

次のオプションを使用することもできます。

- LDAPサーバが実行されておりSSLポートをリスンしているかどうかを確認するには、nldap-sコマンドを実行します。
- LDAPサーバが実行されておりTCLポートをリスンしているかどうかを確認するには、nldap-cコマンドを実行します。

これらはエラーなしで実行されている、eDirectoryのすべてのインスタンスを表示します。
LDAPサーバがロードされておらず、いずれのポートもリスンしていない場合、上記のコマンドはエラー-255(LDAPサーバが実行されていることを確認する)を表示します。

LDAPサーバが実行されているか確認する

LDAPサーバをロードした後で、それが実行されているか確認します。その後、デバイスが監視しているか確認します。

- 391 ページの 「シナリオ」
- 392 ページの 「LDAPサーバが実行されているか確認する」
- 392 ページの 「デバイスが受信待機していることを確認する」

シナリオ

通常、LDAPサーバはロードされるとすぐに実行されます。ただし、次の2つのシナリオでは、サーバが正しく実行されないことがあります。

シナリオ:サーバがゾンビ状態にある。 LDAPサーバはDHostローダが外部依存関係を解決できる限り、ロードを続けます。ただし、LDAPサーバは有効な設定を2つの設定オブジェクト(LDAPサーバオブジェクトとLDAPグループオブジェクト)から取得するまで、正しく動作しません。

LDAPサーバが、「ロードはされても、実行されない(ゾンビ)状態」の場合、LDAPサーバは定期的に設定オブジェクトを探そうとします。オブジェクトの設定が正しくなかったり、オブジェクトが破損したりしている場合、LDAPサーバ(nldap.nlm、nldap.dlm、libnldap.so、またはlibnldap.sl)は、アンロードされるかダウンするまで、ゾンビ状態になります。

ローダはLDAPサーバがロードされていると示しているのに、nldap.nlm(またはnldap.dlm、libnldap.so、libnldap.sl)によりLDAPポート(389、636)が開かれていません。また、LDAPクライアントの要求はどれも実行されていません。

定期的な試行の記録と、サーバが稼動状態にならない原因を示すDSＴｒａｃｅメッセージが表示されます。

シナリオ:サービス拒否 。Digital Airlines社のサーバは現在、長時間(20分以上)かかる検索を処理しています。この処理では、膨大なデータの中から検索が行われています。

この検索の実行中に、あるユーザが次のいずれかを実行します。

- 環境設定パラメータを変更し、設定オブジェクトを更新する。
- ［**Refresh Server Now**］をクリックする。

- LDAPサーバ(nldap.nlm、nldap.dlm、libnldap.so、libnldap.slのいずれか)をアンロードする。
- サーバ全体を終了しようとする。

LDAPサーバは、現在の処理が完了してから更新を適用します。この更新が完了するまで、新しい操作は実行されません。この遅れにより、サーバの検索が完了し、更新が適用されるまでの間、サーバが新しい要求に応答しなくなったように見えることがあります。アンロードの実行中にサーバが停止したように見えることもあります。

検索要求が長く、多くの一致項目がある場合、LDAPサーバをアンロードしようとすると検索は中止され、次の一致項目がクライアントに返される時にアンロードが実行されます。ただし、検索要求の結果、20分間に1件以下しか一致する項目が見つからなかった場合、LDAPサーバは実行中のNDS®またはeDirectory要求を中止できません。

リフレッシュまたは更新の場合、クライアントに返される多くの一致レコードがあっても検索は中止されません。

LDAPサーバが実行されているか確認する

LDAPサービスが実行されていることを確認するには、NetIQインポート/エクスポート変換ユーティリティ(ICE)を使用します。ワークステーションでice.exeを実行するか、またはNetIQ iManagerを使用します。

NetIQ iManagerの使用

NetIQ iManagerでLDAPサーバが動作していることを確認するには、168 ページの「データをファイルへエクスポートする」の手順に従います。

IPアドレスとポート番号を入力して接続が確立された場合は、サーバは機能しています。その他の場合は、エラーメッセージが表示されます。ログファイルまたはエクスポートファイルをダウンロード(表示)してください。

デバイスが受信待機していることを確認する

デバイスがポート389で受信待機していることを確認します。

1. コマンドラインで次を入力します。

   netstat -a

2. ローカルアドレスが*servername*:389で、状態がLISTENINGの行を探します。

次のいずれかの状況が発生した場合は、NetIQ iMonitorを実行します。

- ICEユーティリティから情報を取得できない
- LDAPサーバがLDAP要求をハンドルしているか確認できない

NetIQ iMonitorの詳細については、245 ページの 「環境設定ファイル」および253 ページの 「トレースを環境設定する」を参照してください。

LDAP要求の詳細については、『「NetIQ eDirectoryインストールガイド」.』の「*LDAPを介したeDirectoryとの通信*」を参照してください。

SSLv3無効化によるPOODLE攻撃の防止

セキュアな通信のためにeDirectoryがLDAPSプロトコルをSSLv3で使用する場合、CVE-2014-3566のとおり、SSLv3がPOODLE攻撃に対して脆弱であることに注意してください。

デフォルトでは、eDirectoryはFIPSモードで実行され、SSLv3経由で通信を許可しません。詳細については、「FIPSモードでeDirectoryを設定する」を参照してください。eDirectoryサーバでTLSのFIPSモードを無効にする場合は、次の手順を使用して、LDAPのSSLv3を無効にすることをお勧めします。

解決策:

1. NetIQダウンロードWebサイト (https://dl.netiq.com/index.jsp)から、最新のeDirectory用iManagerプラグインをダウンロードしてインストールします。
2. iManagerを起動し、［**役割およびタスク**］をクリックします。
3. ［**LDAP**］>［**LDAPオプション**］>［**LDAPサーバの表示**］の順にクリックし、［**LDAPサーバ**］を選択します。
4. **[接続]**タブをクリックします。
5. ［**SSLv3の無効化**］を有効にし、［**適用**］をクリックします。

   注: 非英語環境では［**SSLv3の無効化**］を使用できません。このオプションを使用するには、優先する表示言語を英語に変更します。
6. LDAP Services for eDirectoryをアンロードして、ロードします。

   詳細については、「LDAP Services for eDirectoryのロードとアンロード」を参照してください。

LDAPオブジェクトを環境設定する

eDirectoryのインストール時に、LDAPサーバオブジェクトとLDAPグループオブジェクトが作成されます。LDAPサービスのデフォルト設定は、これらの2つのオブジェクト上のディレクトリにあります。NetIQ iManagerでLDAP管理タスクを使用することで、デフォルトの設定を変更できます。

LDAPサーバオブジェクトとは、サーバ固有の設定データのことです。

LDAPグループオブジェクトには、複数のLDAPサーバ間で共有できる便利な設定情報が含まれています。このオブジェクトは、共通の設定データとLDAPサーバグループを提供します。サーバは共通データを持っています。

複数のLDAPサーバオブジェクトを、1つのLDAPグループオブジェクトと関連させることができます。関連するすべてのLDAPサーバは、サーバ固有の設定をそれぞれのLDAPサーバオブジェクトから取得しますが、共通する情報や共有情報はLDAPグループオブジェクトから取得します。

デフォルトでは、LDAPグループオブジェクトおよびLDAPサーバオブジェクトが、eDirectoryインストールプログラムによってnldap.nlmまたはnldap.dlmに対して1つずつインストールされます。
その後、複数のLDAPサーバオブジェクトを、1つのLDAPグループオブジェクトに関連付けることができます。

重要: 新しいバージョンのLDAPサーバオブジェクトを古いバージョンのLDAPグループオブジェクトに関連付けることもできますが、異なるバージョン間での関連付けはお勧めしていません。たとえば、eDirectory 8.7.3 SP9のLDAPグループオブジェクトとeDirectory·9.0以降のLDAPサーバオブジェクトとの関連付けは避けるようにしてください。

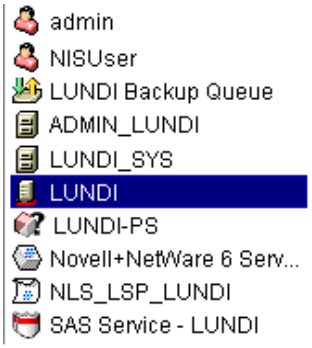
LDAPグループオブジェクトが保持する、共通情報の量は制限されています。属性に含まれるデータはほとんど共通しているため、LDAPは多くの属性を読み込む必要がありません。多くのLDAPサーバは同じデータを使用する必要があります。共通の、または共有グループオブジェクトがない場合は、各LDAPサーバにそのデータを複製する必要があります。

LDAPサーバオブジェクトでは、LDAPグループオブジェクトよりも多くのサーバ固有の設定オプションとデータが許可されています。

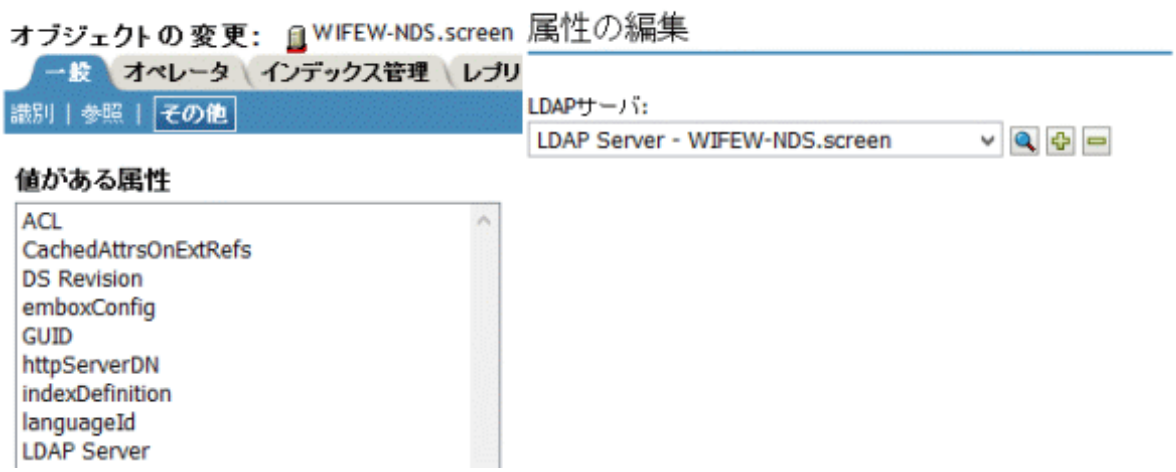
どちらのオブジェクトも、相互にポイントされたDN構文属性を持っています。

LDAPサーバがその設定データを探せるようにするには、関連付けを追加する必要があります。関連付けは、通常のeDirectory設定データを保持するNCP™サーバを通じて行われます。この関連付けは、eDirectoryインストールプログラムにより自動で行われます。

各eDirectoryサーバは、NCPサーバオブジェクトを持っています。次の図の「Lundi」というサーバには、このオブジェクトがiManager上と同じように表示されています。



このオブジェクトは、特定のホストeDirectoryサーバのLDAPサーバオブジェクトを指すLDAPサーバ属性を持っています。次の図は、この属性を示しています。



通常、LDAPサーバオブジェクト、LDAPグループオブジェクト、NCPサーバオブジェクトは同じコンテナ内にあります。eDirectoryのインストールで、サーバおよび管理者コンテキストを指定するときに、このコンテナを指定します。

LDAPサーバオブジェクトを移動するときは、それを書き込み可能なレプリカに置く必要があります。

Linux上でLDAPサーバオブジェクトおよびLDAPグループオブジェクトを環境設定する

LDAP環境設定ユーティリティはldapconfigです。LinuxシステムでLDAPサーバオブジェクトおよびLDAPグループオブジェクトの属性を変更、表示、リフレッシュするには、ldapconfigを使用します。

Linuxシステム上でLDAP属性値を表示するときには次の構文を使用します。

```
ldapconfig get [...] | set attribute-value-list  [-t treename | -p hostname[:port]] [-w password] [-a user FDN] [-f]
```

```
ldapconfig [-t tree_name | -p host_name[:port]] [-w password] [-a user FDN] [-V] [-R] [-H] [-f] -v attribute,attribute2...
```

Linuxシステム上でLDAP属性値を変更するときには次の構文を使用します。

```
ldapconfig [-t tree_name | -p host_name[:port]] [-w password] [-a admin_FDN] -s attribute=value,...
```

パラメータ	説明
-t *treename*	コンポーネントのインストール先となるeDirectoryツリーの名前。
-p *hostname*	ホストの名前です。DNS名またはIPアドレスを指定することもできます。
-w	管理権を持つユーザのパスワード。
-a	管理権を持つユーザの完全識別名。次に例を示します。 cn=user.o=org1
get | -V	すべてのLDAPサーバとLDAPグループの属性を表示します。
get | -v *attribute list*	属性リストにある属性の現在の値を表示します。
set | -s *attribute-value pairs*	属性を指定した値で設定します。
-v	LDAP属性値を表示します。
-s	インストールされたコンポーネントの属性値を設定します。
-R	LDAPサーバをリフレッシュします。
-V	現在のLDAP環境設定を表示します。
-H	使用方法とヘルプを表示します。
-f	フィルタ済みレプリカ上での操作を許可します。

パラメータ	説明
attribute	設定可能なLDAPサーバ属性名またはグループ属性名。詳細については、396 ページの 「LDAPサーバオブジェクトの属性」および404 ページの 「LDAPグループオブジェクトの属性」を参照してください。

例

属性リストの属性の値を表示するには、次のコマンドを入力します。

```
ldapconfig [-t tree_name | -p host_name[:port]]
[-w password] [-a user_FDN] -v "Require TLS for simple binds with
password","searchTimeLimit"
```

LDAP TCPポート番号と検索サイズの制限を1000に設定するには、次のコマンドを入力します。

```
ldapconfig [-t tree_name | -p host_name[:port]]
[-w password] [-a admin_FDN] -s "LDAP TCP Port=389","searchSizeLimit=1000”
```

LDAPサーバオブジェクトの属性

NetIQ LDAPサーバプロパティを設定および管理するために、LDAPサーバオブジェクトを使用します。

次の表に、LDAPサーバ属性の説明を示します。

属性	説明
LDAPサーバ	eDirectoryのLDAPサーバオブジェクトの完全識別名。
LDAP Host Server	LDAPサーバの実行場所となるホストeDirectoryサーバの完全識別名。
LDAPグループ	eDirectoryの中で、このLDAPサーバがメンバーとして属するLDAPグループオブジェクト。
LDAP Server Bind Limit	LDAPサーバに同時にバインドできるクライアントの数。0を指定すると、無制限になります。
LDAP Server Idle Timeout	あるクライアントとLDAPサーバの間で、ここで指定した期間無活動状態が継続すると、このクライアントとLDAPサーバの接続が切断されます。0を指定すると、無制限になります。
LDAP Enable TCP	このオプションは廃止される予定です。ldapInterfacesから使用可能です。 詳細については、400 ページの 「ldapInterfaces」を参照してください。
LDAP Enable TLS	このオプションは廃止されました。ただし、ldapInterfacesから使用可能です。 詳細については、400 ページの 「ldapInterfaces」を参照してください。
LDAP TCP Port	このオプションは廃止されました。ただし、ldapInterfacesから使用可能です。 詳細については、400 ページの 「ldapInterfaces」を参照してください。

属性	説明
LDAP TLSポート	このオプションは廃止されました。ただし、ldapInterfacesから使用可能です。 詳細については、400 ページの 「ldapInterfaces」 を参照してください。
keyMaterialName	このLDAPサーバに関連付けられた、SSL LDAP接続に使用するeDirectoryの証明書オブジェクトの名前。
searchSizeLimit	LDAPサーバが検索要求への応答としてLDAPクライアントに返すエントリの最大数。0を指定すると、無制限になります。 ユーザがLDAPサーバオブジェクト上で管理者権限を持っている場合、searchSizeLimit値は考慮されません。管理権はキャッシュに保存されるので、ユーザの管理権に対する変更は直ちに有効にはなりません。管理権に対する変更は、次回のLDAPサーバ更新で有効になります。デフォルトでは、LDAPサーバは30分ごとに更新されます。
searchTimeLimit	LDAPサーバによるLDAP検索がタイムアウトになるまでの最大秒数。0を指定すると、無制限になります。 ユーザがLDAPサーバオブジェクト上で管理者権限を持っている場合、searchTimeLimit値は考慮されません。管理権はキャッシュに保存されるので、ユーザの管理権に対する変更は直ちに有効にはなりません。管理権に対する変更は、次回のLDAPサーバ更新で有効になります。デフォルトでは、LDAPサーバは30分ごとに更新されます。
filteredReplicaUsage	LDAPサーバがLDAP検索のために、フィルタ処理されたレプリカを使用するかどうかを指定します。 値は1(フィルタ済みレプリカを使用)か0(フィルタ済みレプリカ不使用)です。
sslEnableMutualAuthentication	LDAPサーバにおいて、SSLベースの相互認証(証明書に基づくクライアント認証)を有効にするかどうかを指定します。
ldapTLSVerifyClientCertificate	LDAPによるTLS操作のクライアント認証の確認を有効または無効にします。
ldapNonStdAllUserAttrsMode	非標準のすべてのユーザとオペレーショナル属性を有効または無効にします。

属性	説明
ldapBindRestrictions	LDAPクライアント接続でLDAPバインド制限とサイファレベルを有効にします。この属性はクライアント接続の制御に使用できます。iManagerを使用して、次の7つのLDAPバインド制限のいずれかを設定できます。 ◆ **なし:** デフォルトでは、このオプションは有効になっています。このオプションは匿名単純認証と非匿名単純認証の両方を有効にします。このオプションの値は、0です。 ◆ **匿名単純バインドを不許可にする:** 匿名単純認証を無効にするには、値を1に設定します。非匿名単純認証が有効になります。 ◆ **非匿名単純認証を不許可にする:** 非匿名単純認証を無効にするには、値を2に設定します。 ◆ **匿名単純認証と非匿名単純認証を許可しない:** 匿名単純認証と非匿名単純認証の両方を無効にするには、値を3に設定します。 **注:** 非匿名単純認証を無効にすると、適切な猶予ログインの制限が強制的に適用されます。 ◆ **非認証バインドを許可しない:** パスワードを使用しない単純認証を無効にするには、値を4に設定します。 ◆ **匿名の非認証バインドを許可しない:** 匿名単純認証と非認証バインドを無効にするには、値を5に設定します。 ◆ **非匿名単純認証と非認証バインドを許可しない:** 非匿名単純認証と非認証バインドを無効にするには、値を6に設定します。このシナリオでは、匿名単純認証が有効になります。 ◆ **匿名単純認証、非匿名単純認証、および非認証バインドを許可しない:** 匿名単純認証、非匿名単純認証、および非認証バインドを無効にするには、値を7に設定します。 **注:** 4から7までの値は、ldapconfigユーティリティで設定できます。iManagerでは、この値を設定できません。詳細については、表 14-1を参照してください。 RSAと楕円曲線デジタル署名(ECDSA)アルゴリズムでは、eDirectoryは次の値を使用してサイファの使用を制限できます。 ◆ **RSA:** 次の値を使用します。 ◆ **高度暗号化(128ビットを超える):** 128ビット暗号化よりも上位の暗号レベルと128ビットキーの一部の暗号スイートの使用を指定する場合には、値を48に設定します。 ◆ **中度暗号化:** 128ビット暗号化の暗号レベルの使用を指定するには、値を32に設定します。 ◆ **低度暗号化:** エクスポート暗号スイートを除く、64または56ビット暗号化の使用を指定する場合、値を16に設定します。 ◆ **エクスポート:** 40ビットおよび56ビット暗号化を含むサイファレベルの使用を指定します。値0。 デフォルトは［高］で、128ビット暗号化よりも大きいサイファレベルとなります。この値が［0］に設定されている場合、eDirectory 9.1 SP4にアップグレードされた後、値が自動的に［高］に変更されます。 **注:** TLSのFIPSモードを有効にすると、eDirectoryは暗号化設定を無視し、［高］暗号化のみを許可します。

属性	説明
	Suite Bモード: 次の値を使用します。 ◆ **Suite B Cipher(128ビット):** 128ビットレベルのセキュリティを使用して、Suite Bモードの操作を有効にするには、値を64に設定します。このオプションを選択すると、eDirectoryは、ピア(任意のLDAPクライアント)による128ビットレベルと192ビットレベルの両方のセキュリティの使用を許可します。このオプションではECDSA 256またはECDSA 384のいずれかの証明書を使用できます。 ◆ **Suite B Cipher(128ビットのみ)を使用する:** 128ビットレベルのセキュリティを使用して、Suite Bモードの操作を有効にするには、値を80に設定します。このオプションを選択すると、eDirectoryは、ピア(任意のLDAPクライアント)による192ビットレベルのセキュリティの使用を許可しなくなります。このオプションではECDSA256証明書のみを使用できます。 ◆ **Suite B Cipher(192ビット)を使用する:** 192ビットレベルのセキュリティを使用して、Suite Bモードの操作を有効にするには、値を96に設定します。このオプションを選択すると、eDirectoryは、ピア(任意のLDAPクライアント)による192ビットレベルのセキュリティの使用のみを許可します。このオプションではECDSA 384証明書のみを使用できます。 eDirectoryでは、ldapbindrestrictionsと暗号レベルの値を組み合わせて使用できます。詳細については、表 14-1を参照してください。
ldapChainSecureRequired	これはブール属性です。有効な場合、他のeDirectoryへのチェーンはセキュアなNCPで行われます。デフォルトでは、ldapChainSecureRequiredは無効です。

属性	説明

ldapInterfaces	LDAPサーバが(クリアテキストおよびセキュアなポートの両方を)リスンするLDAP URLを保存するために使用される複数値のSYN_CI_STRING属性。この属性は、eDirectoryサーバでそれぞれのインスタンスが特定のインタフェースについてリスンすることが必要な、複数のインスタンスを構成する際に役立ちます。これは、LDAP URL形式のIPアドレスとポート番号を使用して設定できます。LDAPサーバはこれらのIPアドレスとポートをリスンします。
	
	IPv4とIPv6リスナの例を次に示します。
	
	`ldap://192.168.1.1:389 - To specify for IPv4 specific address on clear text port`
	
	`ldaps://192.168.2.1:636 - To specify for IPv4 specific address on secure port`
	
	`ldap://[2015::3]:389 - To specify for IPv6 specific address on clear text port`
	
	`ldaps://[2015::3]:636 - To specify for IPv6 specific address on secure port`
	
	`ldap://[::]:389 - To specify for IPv6 unspecified address on clear text port`
	
	`ldaps://[::]:636 - To specify for IPv6 unspecified address on secure port`
	
	新しいサーバがeDirectory 9.1以降で設定されている場合は、LDAP Enable TCP、LDAPEnableTLS、LDAPTCPPort、およびLDAPTLSPortの属性は自動入力されません。設定中にldapおよびldapsに対して選択されたポートに対応するldapInterface属性値は自動入力されます。例: ldap://:389、ldaps://:636デフォルトでは、IPv4インタフェース値のみがldapInterfaces属性に追加されます。
	
	アップグレード中に、eDirectoryは、LDAPEnableTCP、LDAPEnableTLS、LDAPTCPPort、LDAPTLSPort属性を削除するためにトリガされます。これらの属性に対応する値がldapInterfaceに入力されます。ldapconfig setコマンドは、コンマ区切りの値を取得して、既存のすべての値を新しい値に置き換えます。

ldapStdCompliance	eDirectory LDAPサーバはデフォルトでは、1つのレベルの検索でサブオーディネート参照を返しません。これを有効にするには、ldapStdComplianceを値1にしてオンにする必要があります。この値を設定すると、LDAPサーバは1つのレベルの検索でサブオーディネート参照を返すようになります。
ldapChainSecureRequired	これはブール属性です。有効な場合、他のeDirectoryへのチェーンはセキュアなNCPで行われます。デフォルトでは、この属性は無効です。
ldapEnablePSearch	LDAPサーバで持続的検索機能を有効にするかどうかを指定します。 Values= yes, no
ldapMaximumPSearchOperations	同時に実行できる持続的検索操作の数を制限するための整数値です。0を指定すると、検索操作は無制限になります。

属性	説明
ldapIgnorePSearchLimitsForEvents	持続的検索要求によって最初の結果が返された後で、サイズと時間の制限を無視するかどうかを指定します。 Values= yes, no この属性がFALSEに設定されている場合、すべての持続的検索操作は検索制限の制約を受けます。サイズと時間のいずれかの制限に達した場合、検索操作は失敗し、該当するエラーメッセージが返されます。
ldapGeneralizedTime	時刻を*YYYYMMDDHHmmSS.0Z*形式で表示するために汎用タイムを有効にします。 Values= yes, no
ldapPermissiveModify	LDAP変更操作を拡張するためにPermissive Modify Controlを有効にします。存在しない属性を削除したり、属性にすでにある属性値を追加しようとすると、エラーメッセージが表示されることなく操作が完了します。 Values= yes, no
ldapSSLConfig	この属性では、LDAPサーバオブジェクトでTLSプロトコルおよび暗号を定義することができます。デフォルトの設定では、この属性は無効です。この環境設定属性は、次の優先順位に従います。 ◆ LDAPサーバオブジェクトのldapSSLConfig属性値 ◆ LDAPグループオブジェクトのldapSSLConfig属性値 この属性でプロトコルと暗号が定義されていない場合、ldapBindRestrictionsで指定されているデフォルトの構成に従います。詳細については、404 ページの 「ldapSSLConfig属性を使用してプロトコルと暗号を構成する」を参照してください。 **注:** ldapSSLConfig属性は、eDirectory 9.0 SP2以降で使用できます。
ldapGroupSSLConfig	この属性では、LDAPグループオブジェクトでTLSプロトコルおよび暗号を定義することができます。デフォルトの設定では、この属性は無効です。この環境設定属性は、次の優先順位に従います。 ◆ LDAPサーバオブジェクトのldapSSLConfig属性値 ◆ LDAPグループオブジェクトのldapSSLConfig属性値 この属性でプロトコルと暗号が定義されていない場合、ldapBindRestrictionsで指定されているデフォルトの構成に従います。詳細については、404 ページの 「ldapSSLConfig属性を使用してプロトコルと暗号を構成する」を参照してください。 **注:** この属性をldapconfig get/set コマンドで設定する場合、ldapGroupSSLConfigを使用します。ldifファイルで設定する場合には、ldapSSLConfigにLDAPグループオブジェクトDNを指定して使用します。

表 14-1 ldapbindrestrictionsとサイファレベルの組み合わせ値

ldapbindrestriction	証明書	サイファレベル	組み合わせ値
なし	RSA	エクスポート	0
	RSA	高	48
	RSA	中	32
	RSA	低い	16
	ECDSA 256/384	SUITEB128	64
	ECDSA 256	SUITEB128ONLY	80
	ECDSA 384	SUITEB192	96
匿名単純認証を許可しない	RSA	エクスポート	1
	RSA	高	49
	RSA	中	33
	RSA	低い	17
	ECDSA 256/384	SUITEB128	65
	ECDSA 256	SUITEB128ONLY	81
	ECDSA 384	SUITEB192	97
ローカルバインドを許可しない	RSA	エクスポート	2
	RSA	高	50
	RSA	中	34
	RSA	低い	18
	ECDSA 256/384	SUITEB128	66
	ECDSA 256	SUITEB128ONLY	82
	ECDSA 384	SUITEB192	98
匿名単純認証とバインド解除を許可しない	RSA	エクスポート	3
	RSA	高	51
	RSA	中	35
	RSA	低い	19
	ECDSA 256/384	SUITEB128	67
	ECDSA 256	SUITEB128ONLY	83
	ECDSA 384	SUITEB192	99

ldapbindrestriction	証明書	サイファレベル	組み合わせ値
非認証バインドを許可しない	RSA	エクスポート	4
	RSA	高	52
	RSA	中	36
	RSA	低い	20
	ECDSA 256/384	SUITEB128	68
	ECDSA 256	SUITEB128ONLY	84
	ECDSA 384	SUITEB192	100
匿名の非認証バインドを許可しない	RSA	エクスポート	5
	RSA	高	53
	RSA	中	37
	RSA	低い	21
	ECDSA 256/384	SUITEB128	69
	ECDSA 256	SUITEB128ONLY	85
	ECDSA 384	SUITEB192	101
非匿名単純認証と非認証バインドを許可しない	RSA	エクスポート	6
	RSA	高	54
	RSA	中	38
	RSA	低い	22
	ECDSA 256/384	SUITEB128	70
	ECDSA 256	SUITEB128ONLY	86
	ECDSA 384	SUITEB192	102
匿名単純認証、非匿名単純認証、および非認証バインドを許可しない	RSA	エクスポート	7
	RSA	高	55
	RSA	中	39
	RSA	低い	23
	ECDSA 256/384	SUITEB128	71
	ECDSA 256	SUITEB128ONLY	87
	ECDSA 384	SUITEB192	103

LDAPグループオブジェクトの属性

LDAPクライアントのNetIQ LDAPサーバに対するアクセス方法と、サーバ上の情報の使用方法を設定および管理するには、LDAPグループオブジェクトを使用します。

単純認証にTLSが必要な場合は、「407ページの 「パスワードとの単純バインドにTLSを要求する」」を参照してください。この属性は、LDAPサーバがLDAPクライアントからパスワードをクリアテキストで送信することを許可するかどうかを指定します。値は1(はい)または1(いいえ)です。

デフォルトの参照、referralIncludeFilter、referralExludeFilter、およびLDAPサーバによるLDAP参照の処理方法を指定するには、「417 ページの 「参照を使用する」」を参照してください。

TLSプロトコルと暗号を指定するには、ldapSSLConfig属性を使用できます。詳細については、404 ページの 「ldapSSLConfig属性を使用してプロトコルと暗号を構成する」を参照してください。

ldapSSLConfig属性を使用してプロトコルと暗号を構成する

eDirectoryを使用すると、LDAPサーバのTLS通信に必要な各種TLSパラメータと暗号を定義できます。

LDAPサーバオブジェクトとグループオブジェクトの両方に関して、ldapSSLConfig属性でプロトコルと暗号をJSON形式で指定できます。たとえば、以下に示されているようにJSON形式でプロトコルと暗号を定義できます。

```
{
    "Version": 1,
    "Info": {
        "Protocol": "+ALL-SSLv3",
        "Ciphers": "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384"
    }
}
```

注: ldapSSLConfig属性で間違った情報を指定すると、ldapBindRestrictionsで指定されているデフォルト構成が使用されます。

暗号を設定する

OpenSSL暗号リスト形式を使用して、独自の暗号リストを構成できます。次の例では、LDAPサーバのTLS通信時に使用される暗号リスト形式を示します。

- RSA証明書: !CAMELLIA:!DH:!SRP:!MD5:HIGH + aRSA
- ECDSA証明書: HIGH+aECDSA
- Suite B 128ビット準拠の暗号スイート(ECDSA証明書使用): ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256
- Suite B 192ビット準拠の暗号スイート(ECDSA証明書使用): ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES-GCM-SHA

暗号リスト形式について詳しくは、OpenSSL ciphers (https://www.openssl.org/docs/man1.0.2/apps/ciphers.html)マニュアルを参照してください。

プロトコルを設定する

eDirectoryでは、TLS通信中に必要なプロトコルのリストを柔軟に設定できます。プロトコルのリストを制御するには、ldapSSLConfig属性で必要なプロトコルをJSON形式で定義します。次のプロトコル文字列を設定できます。

- SSLv3
- TLSv1.0
- TLSv1.1
- TLSv1.2
- ALL

各プロトコル文字列の前に「+」または「-」記号を入力する必要があります。「+」記号はプロトコル文字列がeDirectoryで許可されていることを、「-」記号はプロトコル文字列が許可されていないことを示します。次の表に、TLSプロトコル構成のいくつかを示します。

プロトコル構成	説明
+TLSv1.2	TLSv1.2のみを許可します
+ALL-TLSv1.0	TLSv1.0以外のすべてを許可します
+ALL-TLSv1.2-TLSv1.1	SSLv3とTLSv1.0を許可します
+ALL	SSLv3、TLSv1.0、TLSv1.1、TLSv1.2を許可します

注: +ALLを指定する場合、プロトコルの前に付けることができるのは「-」記号だけです。

例:

Suite B準拠モードでプロトコルと暗号を構成する

```
{
    "Version": 1,
    "Info": {
        "Protocol": "+TLSv1.2",
        "Ciphers": "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384"
    }
}
```

上の例では、プロトコルがJSON形式で+ TLSv1.2として定義されています。Suite B準拠モードでは、TLSv1.2のみがサポート対象プロトコルです。

非Suite B準拠モードでプロトコルおよび暗号を設定する

```
{
    "Version": 1,
    "Info": {
        "Protocol": "+ALL-SSLv3",
        "Ciphers": "HIGH+aECDSA"
    }
}
```

上の例では、プロトコルがJSON形式で+ALL-SSLv3と定義されています。つまり、TLS通信時にはSSLv3以外のすべてのサポート対象プロトコルが許可されます。

LDAPサーバをリフレッシュする

LDAPサーバの環境設定オプションやLDAPサーバの設定を変更した場合、変更を有効にするにはサーバをリフレッシュする必要があります。

ただし、LDAP要求のサービスの実行中はサーバをリフレッシュできません。たとえば、eDirectoryツリーの処理に15分かかる場合には、この処理が完了するまでリフレッシュは実行されません。

同様に、LDAPサーバスレッドの実行中は、LDAPサーバを終了することはできません。

リフレッシュの実行が予定されている場合は、LDAPサーバはリフレッシュが実行されるまで新しいLDAP要求の開始を遅らせます。

デフォルトでは、LDAPサーバは30分間隔でLDAPサーバオブジェクトとLDAPグループオブジェクトのタイムスタンプをチェックし、設定に変更がなかったか確認します。設定が変更されている場合、サーバはその変更を適用します。

設定のタイムスタンプが前回と変わらない場合には、リフレッシュは実行されません。強制的にリフレッシュを実行すると、サーバはタイムスタンプを無視して変更を適用します。

LDAPサーバをリフレッシュするには、次のいずれかを実行します。

- iManagerを使用する

  1. ［**役割およびタスク**］ページで、［**LDAP**］>［**LDAPオプション**］>［**LDAPサーバの表示**］の順にクリックします。
  2. LDAPサーバをクリックし、［**リフレッシュ**］をクリックします。

- サーバが次のリフレッシュ間隔で再設定されるまで待つ。
- nldap.nlmをアンロードしてから再ロードする。

  nldap.nlmをアンロードする前に前提条件のNLMプログラムをアンロードする必要はありません。

  nldap.nlmがアンロードされると、従属するNLMプログラムが再ロードされます。

- コマンドラインで、リフレッシュ間隔を変更する。

  このオプションは、WANリンクが継続して実行されていない場合に便利です。必要に応じ、一時的にサーバのハートビート処理の長さを変更できます。

  この変更は持続しません。nldap.nlmをロードするたびに、コマンドを再入力する必要があります。

  サーバコンソールで次を入力します。

  ldap refresh [=] [*date*][*time*][*interval*]

  - 日付変数の形式は、mm:dd:yyyyです。すべての日付フィールドに0と入力すると、現在の日付が使用されます。

- 時間変数の形式は、hh:mm:ssです。すべての時刻フィールドに0と入力すると、現在の時刻が使用されます。
- 間隔変数の形式は0または1～2147483647分の間です。0と入力すると、デフォルトの30分が使用されます。

このコマンドは、sys:\systemディレクトリのautoexec.ncfファイルに追加できます。nldap.nlmをロードした行の後に、このコマンドを配置します。

認証とセキュリティ

このセクションでは、次の情報について説明します。

パスワードとの単純バインドにTLSを要求する

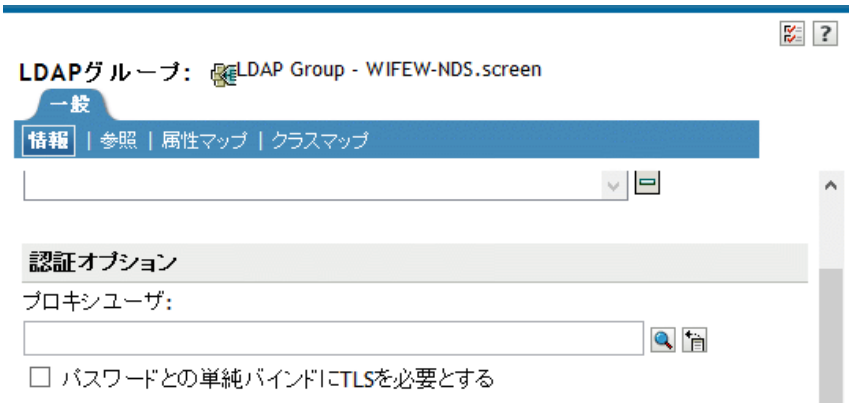
SSL(Secure Socket Layer) 3.1はNetscapeでリリースされました。IETFは、TLS (Transport Layer Security) 1.0を実装することで、その標準の所有権を持ちます。TLS 1.0はSSLv2およびv3と後方互換性があります。

TLSを使用すると、接続をセッション層で暗号化することができます。TLS接続のために、暗号化されたポートを使用する必要はありません。方法はもう1つあります。ポート636は暗黙的なTLSポートであり、クライアントがセキュアポートに接続すると、LDAPサーバは自動的にTLSセッションを開始します。

クライアントは、まずクリアテキストポートに接続し、後でTLSを使用して暗号化された接続にアップグレードすることもできます。

パスワードとの単純バインドにTLSを要求するには、次を実行します。

1. NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**LDAP**］>［**LDAPオプション**］>［**LDAPグループの表示**］の順にクリックします。
3. LDAPグループオブジェクトをクリックしてから、［**全般**］タブの［**情報**］をクリックします。
4. ［**パスワードとの単純バインドにTLSを必要とする**］チェックボックスをオンにします。



5 **適用**をクリックし、**OK**をクリックします。

TLSを開始/停止する

LDAP拡張オペレーションSTARTTLSにより、クリア接続から暗号化された接続にアップグレードすることができます。このアップグレードは、eDirectory8.7の新機能です。

暗号化された接続を使用すると、パケット全体が暗号化されます。このため、ネットワーク経由で送信されたデータが第三者によって診断されることはありません。

シナリオ:STARTTLSを使用する— ポート389にクリア接続し、匿名検索を行います。ただし、セキュリティ保護されたデータを扱う場合にはTLSセッションに切り換えます。拡張オペレーションSTARTTLSを実行し、クリア接続から暗号化された接続にアップグレードします。これでデータの安全が確保されます。

暗号化されたセッションをクリア接続に切り替えるには、TLSを停止します。クリア接続では、クライアントが送受信するデータは暗号化および解読されないので、負荷は少なくなります。そのため、クリア接続の使用時の方が、データの通信速度が速くなります。この時点で、接続は匿名にダウングレードされています。

認証を受けるにはLDAPバインド操作を使用します。バインドは、ユーザの資格情報に基づいてIDを確立します。TLSを停止するときに、LDAPサービスは以前に確立された認証をすべて削除します。認証ステータスが匿名に変わります。匿名以外の状態に切り替える場合は、再認証を受ける必要があります。

シナリオ:再認証— あるユーザがSTOPTLSを実行します。すると、そのユーザの状態が匿名に変わります。このユーザのファイルにネット上でアクセスするには、Bindコマンドを実行し、ログイン認証情報を入力します。ユーザが認証され、インターネット上でクリアテキストで作業を続行できます。

TLSのサーバを環境設定する

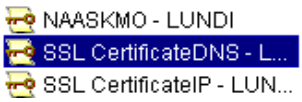
TLSセッションがインスタンス化されると、ハンドシェークが行われます。サーバとクライアントがデータを交換します。ハンドシェークの方法はサーバが決定します。サーバの正当性を証明するため、サーバは常にサーバの証明書をクライアントに送信します。このハンドシェークにより、そのサーバがクライアントに指定されたサーバであることが証明されます。

クライアントにも正当性の証明を要求するには、サーバに値を設定します。これはldapTLSVerifyClientCertificateという属性です。

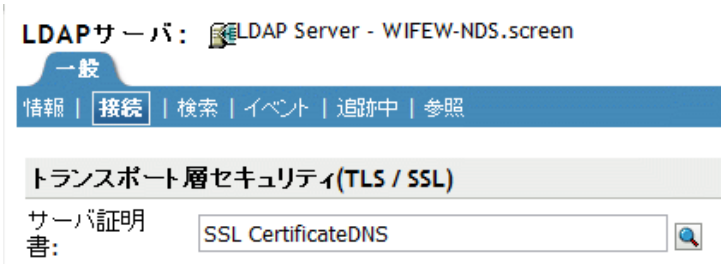
値	説明
0	オフ. ハンドシェーク時に、サーバがクライアントに証明書を提供します。サーバがクライアントに証明書の送信を要求することはありません。クライアントは証明書を使用することも、無視することもできます。セキュリティ保護されたセッションが確立されます。
1	ハンドシェークの間、サーバは証明書をクライアントに送信し、クライアントからも証明書を要求します。クライアントはサーバに証明書を送信できます。クライアントの証明書が検証されます。サーバがクライアントの証明書を確認できない場合、接続は終了します。 クライアントが証明書を送信しない場合、サーバは接続を維持します。
2	ハンドシェークの間、サーバはクライアントから証明書を要求します。クライアントが証明書を提供しない、または証明書が確認できない場合には、接続は終了します。

サーバがTLSをサポートするよりも前に、サーバにその正当性の証明に使用するX.509証明書を提供する必要があります。

この証明書は、eDirectoryのインストール時に自動的に提供されます。インストール時に、PKI (公開鍵インフラストラクチャ)とNMAS (NetIQモジュラー認証サービス)の一部として、キーマテリアルオブジェクトが作成されます。次の図は、iManagerにおけるこれらのオブジェクトを示しています。



インストール中、これらの証明書の1つがLDAPサーバと自動的に関連付けられます。NetIQ iManagerのLDAPサーバオブジェクトの［接続］タブにDNが表示されます。このDNは、X.509認定を表しています。次の図のサーバ証明書フィールドは、このDNを示しています。



NetIQ iManagerで、暗号化キーオブジェクト(KMO)証明書をブラウズできます。また、ドロップダウンリストから、別の証明書に変更することもできます。DNSまたはIP証明書のいずれかを使用します。

検証の際には、サーバは証明書にある名前(ハードIPアドレスまたはDN)を確認します。

TLS接続を確立するには、次の条件を確認します。

- LDAPサーバは、サーバのKMOを知る必要があります。
- クリアポートに接続してから、セキュアポートに接続するかTLSを開始します。

LDAPサーバを再設定し、サーバをリフレッシュします。406ページの「LDAPサーバをリフレッシュする」を参照してください。iManagerはサーバを自動的に更新します。

TLSのクライアントを環境設定する

LDAPクライアントとは、たとえば、Internet Explorer、ICEのようなアプリケーションのことです。クライアントは、LDAPサーバが使用する認証局を認知している必要があります。

重要: eDirectory 9.1以降、ndsindexおよびiceを含むすべてのLDAPユーティリティで受け入れられるのは.PEM形式の証明書のみになりました。.PEM証明書をLDAP操作で使用する方法について詳しくは、373 ページの 「LinuxでのLDAPツールの使用」 を参照してください。

---

eDirectoryツリーが構成されている場合、デフォルトでは構成によって次のものが作成されます。

- ツリーの認証局(ツリーCA)
- ツリーCAからのKMO

LDAPサーバはこの認証プロバイダを使用します。

クライアントは、LDAPサーバが使用していると主張するツリー認証局を確認できるよう、信頼する証明書をインポートする必要があります。この証明書をサーバからインポートしておくと、サーバがその証明書を送信してきたときに、クライアントはそれを確認し正当なサーバであるかどうか確かめることができます。

クライアントが安全に接続できるよう、接続前にクライアントの環境設定をしておく必要があります。

クライアントによる証明書のインポート方法は、使用しているアプリケーションの種類によって異なります。各アプリケーションには、何らかの証明書をインポートする方法があります。IEとICEでは、方法が異なります。これらは異なるLDAPクライアントです。各クライアントは、それぞれの方法で信頼する証明書を探します。

ルート認証局をエクスポートする

ルート認証局は、証明書サーバを受け入れるときに自動的にエクスポートできます。

ルート認証局を手動でエクスポートするには、「725ページの「ルート認証局または公開鍵証明書のエクスポート」」を参照してください。

エクスポート機能により、指定したファイルが作成されます。ファイル名は変更できますが、マテリアルオブジェクトのタイプを認識できるよう、ファイル名に「DNS」または「IP」を残しておくことをお勧めします。また、サーバ名も残しておきます。

eDirectoryとの安全なLDAP接続を確立するブラウザに、自己割り当て認証局をインストールします。

InternetExplorerなど、Microsoft社の製品で証明書を使用する場合は、.der拡張子を残しておくようにします。

アプリケーションまたはSDKが証明書を要求する場合は、証明書をデータベースにインポートします。

Internet Explorer 5の場合は、ルート証明書が自動的にエクスポートされ、レジストリが更新されます。これには、Microsoftが通常使用している.x509拡張子が必要です。

クライアント証明書で認証を受ける

相互認証には、TLSセッションとクライアント証明書が必要です。サーバとクライアントの両方が、それぞれが自分の主張するオブジェクトであることを証明する必要があります。クライアントの証明書がトランスポート層で確認されます。しかし、LDAPプロトコル層では、LDAPバインド要求を出すまでクライアントは匿名になります。

この時点で、クライアントはその正当性をサーバに証明しましたが、LDAPにはまだ証明されていません。クライアント証明書に含まれたIDで認証を受けたい場合は、クライアントはSASL EXTERNALメカニズムを使ってバインドされます。

1 NetIQ iManagerで、［**役割およびタスク**］ボタン をクリックします。
2 ［**LDAP**］ > ［**LDAPオプション**］をクリックする。
3 ［**LDAPサーバの表示**］をクリックし、LDAPサーバオブジェクトの名前をクリックします。
4 ［**接続**］をクリックします。
5 Transport Layer Securityセクションのドロップダウンメニューから［**クライアント証明書**］、［**必須**］の順に選択します。

   これにより、相互認証が可能になります。
6 **適用**をクリックし、**OK**をクリックします。

サードパーティプロバイダの証明書を使用する

eDirectoryのインストール時に、LDAPサーバにツリー認証局(CA)が提供されます。LDAPキーオブジェクトは、その認証局に基づいています。クライアントがLDAPサーバに送信する証明書は、このツリー認証局から検証できます。

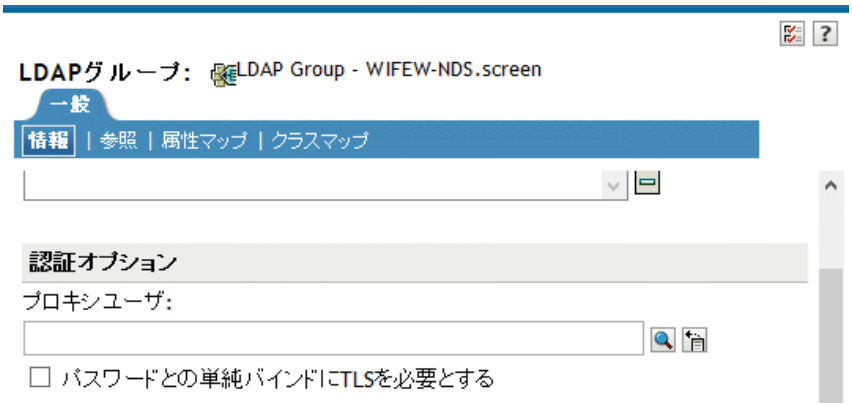
LDAP Services for eDirectoryは、複数の認証局をサポートしています。NetIQのツリー認証局は1つの認証局にすぎません。LDAPサーバが、他のCAを持っている場合があります(例:外部団体のVeriSign*など)この追加CAもルート認証局です。

LDAPサーバが複数の認証局を使用するように設定するには、LDAPサーバオブジェクトでldapTLSTrustedRootContainer属性を設定します。LDAPサーバが複数の認証局を参照することにより、クライアントは外部の認証局を使用できます。

LDAPプロキシユーザを作成および使用する

NetIQ eDirectoryは、認証されていないユーザに［パブリック］識別子を割り当てます。LDAPプロトコルでは、認証されていないユーザは匿名ユーザになります。デフォルトでは、LDAPサーバは匿名ユーザに[Public]識別子の権利を与えます。この権利により、非承認のeDirectoryおよび匿名LDAPユーザは、[Public]権を使用してeDirectoryを参照することができます。

また、LDAPサーバは匿名ユーザによる別のプロキシユーザの権利の使用を許可します。この値はLDAPグループオブジェクトにあります。NetIQ iManagerでは、この値は、［プロキシユーザ］フィールドで指定します。次の図は、NetIQ iManagerの［プロキシユーザ］フィールドを示しています。



プロキシユーザは識別名です。このプロキシIDに、Public識別子とは別の権利を与えることができます。プロキシユーザを使用すると、eDirectoryツリー内の特定コンテナへのLDAP匿名アクセスを制御できます。

注: 代理ユーザのログイン制限は、すべての匿名LDAPユーザに適用する場合以外は設定しないでください。

シナリオ: NLDAP代理ユーザを設定する— Digital Airlines社はリサーチ会社のDataSure社と契約を締結しています。DataSure社はLDAPを使用して、Digital Airlines社のLinuxサーバであるDigitalAir43にアクセスし、リサーチの内容を保存します。あなたはDataSure社にDigitalAir43のディレクトリに対するパブリック権利を与えたくありません。

そのために、LDAPプロキシユーザを作成し、そのユーザにDataSureディレクトリに対する特定の権利を割り当てます。LDAPグループオブジェクトにプロキシ識別名を作成し、サーバをリフレッシュします。サーバは自動的に、すべての新規または既存の匿名ユーザについて、プロキシユーザの権利の使用を開始します。

1. NetIQ iManagerで、［**役割およびタスク**］ボタン をクリックします。
2. ［**ディレクトリ管理**］>［**オブジェクトの作成**］の順にクリックし、代理ユーザを作成します(例 : LDAPProxy)。
3. ユーザにNULLパスワードを割り当てます。
4. (オプション)指定したディレクトリにプロキシユーザの権利を割り当てます。
5. ［**LDAP**］>［**LDAPオプション**］>［**LDAPグループの表示**］>［LDAPグループオブジェクト］の順にクリックします。
6. ［**プロキシユーザ**］フィールドで［**参照**］ボタンをクリックし、LDAPProxyユーザを選択して［**OK**］をクリックします。

SASLを使用する

SASL (Simple Authentication and Security Layer)は、異なるメカニズムを介して、接続ベースのプロトコルに認証のサポートやデータのセキュリティサービスを追加するためのメカニズムです。プロトコルとメカニズム間の整形式のインタフェースを提供します。さらに、データ整合性、データ機密性、その他のサービスとともに、データセキュリティ層内での後続のプロトコル交換のセキュリティを保護するためのプロトコルを提供します。

SASLは、メカニズムを再設計せずに新しいプロトコルが既存のメカニズムを再使用できるように設計されており、既存のプロトコルもプロトコルの設計を変更せずに新しいメカニズムを使用できるようにします。SASLを使用するために、各プロトコルは、どのメカニズムが使用されるかを識別する方法、メカニズム固有のサーバチャレンジとクライアント応答を交換する方法、および認証交換の結果を通信する方法を提供します。

SASLメカニズムには、大文字、数字、ハイフン、およびアンダースコアで構成される、文字列によって名前が付けられます。SASLメカニズム名は、IANA (Internet Assigned Numbers Authority)に登録する必要があります。

サーバが要求されたメカニズムをサポートする場合、認証プロトコル交換を開始します。これは要求されたメカニズムに固有の一連のサーバチャレンジとクライアント応答で構成されます。認証プロトコル交換時に、メカニズムは認証を実行し、クライアントからサーバへ承認IDを送信して、メカニズム固有のセキュリティ層の使用をネゴシエートします。セキュリティ層の使用について合意すると、メカニズムは、それぞれの側で受信可能な最大の暗号テキストバッファサイズの定義つまりネゴシエートする必要もあります。

LDAPサーバでは次のメカニズムがサポートされます。

- DIGEST-MD5
- EXTERNAL
- NMAS_LOGIN
- GSSAPI

これらのメカニズムは、eDirectoryのインストールまたはアップグレード時に、サーバにインストールされます。ただし、Linuxでは、nmasinstユーティリティを使用して、NMASメソッドをインストールする必要があります。

前述したとおり、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。これらは登録されているメカニズムなので、利用には正しい命名規則を使用する必要があります。

LDAPバインドプロトコルでは、クライアントは認証に様々なSASLメカニズムを使用することができます。アプリケーションがLDAPバインドAPIを使用している場合は、単純認証を選択し、DNとパスワードを入力するか、SASLバインドを選択し、SASLメカニズム名と、そのメカニズムが要求する、関連するSASL資格情報を提供する必要があります。

DIGEST-MD5

LDAPはバインド要求でDIGEST-MD5メカニズムをサポートします。LDAP単純認証(DNおよびクリアテキストパスワード)を要求する代わりに、DNとMD5資格情報を提供することで、LDAP SASLバインドを要求します。DIGEST-MD5メカニズムにはTLSは必要ありません。LDAPサーバは、クリア接続およびセキュア接続の両方でDIGEST-MD5をサポートします。

MD5は、暗号化されたパスワードのハッシュを提供します。パスワードは、クリア接続でも暗号化されます。そのためLDAPサーバは、ポートがクリアテキストポートか暗号化されたポートかに関係なく、MD5を使ったパスワードを受け入れます。他のユーザがこの接続を傍受しようとしても、パスワードは検出できません。ただし、接続全体に対してなりすましやハイジャックがなされる可能性はあります。

このメカニズムはLDAP SASLバインドです(単純認証ではありません)。そのため、インストール時に［**パスワードとの単純バインドにTLSを必要とする**］チェックボックスがオンになっていても、LDAPサーバはこの要求を受け入れます。

EXTERNAL

EXTERNALメカニズムにより、ユーザDNおよび資格情報がサーバに提供されたことがLDAPサーバに通知されます。そのため、バインド要求時にはDNと資格情報は必要ありません。

LDAPバインド要求は、SASL EXTERNALメカニズムを使用して、サーバに次を実行するよう指示します。

- EXTERNAL層に資格情報を問い合わせる
- ユーザをその資格情報とユーザで認証する

その後、セキュアなハンドシェークが実行されます。LDAPサーバはクライアントから資格情報を要求しクライアントがサーバに資格情報を渡すと、サーバはクライアントから渡された証明書を受信し、その証明書をNMASモジュールに渡して、証明書の中にどんなDNが指定されていてもユーザを認証します。

使用できるDNの証明書を使用するには、クライアントを設定する必要があります。証明書の設定に関する詳細は、「NMASオンラインヘルプ (https://www.netiq.com/documentation/edir88/nmas88/data/bookinfo.html)」を参照してください。

クライアントがEXTERNALメカニズムを送信する場合でも、LDAPサーバが要求の処理に失敗する場合があります。失敗の原因として可能性があるものを次に示します。

- 接続がセキュア接続ではない。
- 接続はセキュア接続だが、クライアントがハンドシェーク時に要求された証明書を提供しなかった。
- SASLモジュールを使用できない。

NMAS_LOGIN

NMAS (NetIQモジュラー認証サービス)は、さまざまなログインと認証方法を使用してネットワークに認証されるアプリケーションを作成することができる開発フレームワークです。NMASフレームワークでは、Novell International Cryptographic Infrastructure (NICI)とNetIQ Directory Services (eDirectory)を活用する、モジュール式のプラグイン方法を使用して、柔軟かつ拡張可能なログインと認証システムを設計することができます。

NMAS_LOGINメカニズムにより、LDAPサーバにNMASのバイオメトリック機能が提供されます。詳細については、「NetIQモジュラー式認証サービスNDK (http://www.novell.com/documentation/developer/nmas/)」を参照してください。

GSSAPI

GSSAPIメカニズムにより、Kerberosユーザがチケットを使用してeDirectoryサーバへの認証を受けられるようになります。その際に、個別のLDAPユーザパスワードの入力は不要です。この機能は、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向けのものです。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、Kerberosサーバで発行されたチケットを使用してLDAPサーバへの認証を行うことができます。

GSSAPIの設定については、859ページの付録E「eDirectoryでのGSSAPIの設定」を参照してください。

NMASベースのログインを使用したLDAP認証

eDirectoryでは、NMASログインがデフォルトで有効になっています。NMASログインを無効にするには、NDSD_TRY_NMASLOGIN_FIRSTをfalseに設定します。

注: eDirectoryサービスをRHEL 7.xおよびSLES 12.xプラットフォーム上のpre_ndsd_start_customスクリプトで実行するために必要なすべての環境変数を追加する必要があります。

LDAPサーバを使ってディレクトリを検索する

このセクションでは、次の情報について説明します。

- 415 ページの 「検索制限を設定する」
- 417 ページの 「参照を使用する」
- 424 ページの 「フィルタ済みレプリカを検索する」

検索制限を設定する

LDAPサーバオブジェクトの次の属性により、LDAPサーバのディレクトリ検索方法を制御することができます。

- 検索エントリの制限

検索のサイズを制限します。デフォルトは0で、サイズの制限はありません。LDAPサーバの負荷が大きくなりすぎないように、検索要求に対してLDAPサーバが返すエントリ数を制限できます。

シナリオ:検索のサイズを制限する— ユーザは、検索結果が何千件にもなりそうな、あるオブジェクトの検索を要求します。ただし、検索結果は10件に制限してあります。LDAPサーバは10件の検索結果を返すと検索を中止します。一致するデータがまだ存在しているが、検索が終了されたことを告げるシステムメッセージが表示されます。

- 結果送信時間

  サーバが検索を行う時間を制限します。デフォルトは0秒です。これは時間制限がないことを表します。

次の図は、NetIQ iManagerにおけるこれらの属性を示します。

1. iManagerで、［**役割およびタスク**］ボタン をクリックします。
2. ［**LDAP**］>［**LDAPオプション**］>［**LDAPサーバの表示**］の順にクリックします。
3. ［LDAPサーバオブジェクト］>［**検索**］の順にクリックします。
4. 制限セクションをスクロールして値を入力し、［**OK**］をクリックします。

クライアントも、検索要求に制限を設定することもできます(たとえば検索を2秒に制限するなど)。クライアントの制限がサーバの制限と競合する場合、LDAPサーバは値が小さい方の要求を採用します。

検索は、アクセス制御リスト(ACL)に基づいて実行されます。このため、匿名検索の場合は、ディレクトリに何千というエントリが存在していても、Public権で見ることのできるごく一部のエントリしか返されないことがあります。

参照を使用する

参照は、名前を解決するためのクライアント中心の方法です。LDAPクライアントがLDAPサーバに要求を送信すると、LDAPサーバは要求操作のターゲットエントリをローカルに見つけようとします。LDAPサーバはターゲットエントリを見つけられないと、所有する知識参照を使用して、そのエントリについてのより多くの知識を持つ第2のLDAPサーバへの参照を生成します。第1のサーバは、参照情報をLDAPクライアントに送信します。

次に、LDAPクライアントは第2のLDAPサーバへ接続し、操作を再実行します。第2のLDAPサーバが操作のターゲットエントリを保持している場合は、そのサーバが操作を実行します。エントリを保持していない場合は、第2のLDAPサーバもまた参照をクライアントに送信します。この操作は、次のいずれかの状況になるまで続けられます。

- クライアントがターゲットエントリを保持するサーバと接続し、要求する操作が実行できる。
- LDAPサーバが、エントリは存在しないとのエラーを返す。
- LDAPサーバがこれ以上参照先がないことを通知する。

LDAP for eDirectory 8.7で導入された機能により、参照の動作が以前のバージョンのeDirectoryおよびNDSから少し変更されました。これにより、LDAPサービスの環境設定方法も変更されました。

デフォルトの参照

通常、デフォルトの参照URLには、ツリーのルートを保持するサーバを指すLDAPURLが含まれています。LDAP URLの形式はldap://*ホスト*:*ポート*です。

［デフォルト参照URL］フィールドに、デフォルトの参照先を入力します。

これまで、eDirectory LDAPサーバは、多くのフェイルオーバー時にデフォルトの参照先を送信していました。これが、この動作を予期しないユーザを混乱させる結果になっています。そこで、LDAP Services for eDirectoryでは、サブオーディネート参照で、どんな場合にデフォルトの参照先が送信されるかを指定できるようになりました。

この新しいオプションは、LDAPサーバオブジェクトとLDAPグループオブジェクトのldapDefaultReferralBehavior属性の値(設定)で指定します。値は次のビットのビットマスクである整数です。

ビット	値
0x00000001	ベースDNが見つかりません
0x00000002	ベースDNは、利用できないeDirectoryサーバ上にあります
0x00000004	検索スコープのエントリは、利用できないeDirectoryサーバ上にあります

LDAPサーバがその操作に対して「常に参照する」に設定されており、リストされたいずれかの条件と一致し、対応する値が設定されている場合、デフォルトの参照先が返されます。

検索操作の参照先を設定する

LDAP for eDirectory 8.7で導入された機能により、参照の動作が以前のバージョンのeDirectoryおよびNDSから少し変更されました。これにより、LDAPサービスの環境設定方法も変更されました。

eDirectoryツリー内の他のeDirectoryサーバに参照先を返すようにeDirectory LDAPサーバを設定することができます。デフォルトでは、LDAPサーバはユーザに代わってすべての操作を他のeDirectoryサーバにチェーンし、参照先は返しません。

eDirectory 8.7より以前は、参照先オプションの設定はLDAPグループオブジェクトでだけしか使用できませんでした。eDirectory 9.0以降では、LDAPサーバオブジェクトにもこれらのオプションを設定できるようになりました。LDAPサーバオブジェクトの設定により、LDAPグループオブジェクトの設定は上書きされます。

dapSearchReferralOption属性を操作することにより、照会先オプションを設定することができます。LDAP Services for eDirectory 8.7より以前は、この属性を次のオプションに設定することができました。

- 420 ページの 「チェーンを優先する」 (デフォルトオプション)
- 420 ページの 「参照を優先する」
- 421 ページの 「常に参照する」

これらの参照オプションは、eDirectoryツリー内の他のeDirectoryサーバの参照およびチェーンでだけ使用できます。この設定は、信頼されていないパーティションからの参照は制御しません。そのため、［照会先オプション］ドロップダウンリストでオプション(［常にチェーンする］など)を選択しても、他のサーバの信頼されていないパーティションからは参照先が送信されます。

LDAP Services for eDirectory 8.7.aでは［常にチェーンする］オプションにより、eDirectory DSA以外の上方参照がサポートされています。詳細については、419ページの「常にチェーンする」を参照してください。

次の図は、検索およびその他の操作に使用する［LDAP参照］ドロップダウンリストを示しています。

eDirectory操作にはこの他に、「追加」、「削除」、「編集」、「バインド」の各操作の参照があります。

常にチェーンする

［常にチェーンする］オプションは、「まったく参照しない」ように設定するオプションです。このオプションを選択すると、eDirectory LDAPサーバは、eDirectoryツリー内にある他のeDirectoryサーバに参照先を返しません。LDAPサーバは、要求を出したクライアントに代わって他のLDAPサーバをチェックし、クライアントに参照先を返します。

［常にチェーンする］オプションは、eDirectoryをグローバル連結ツリーのサブオーディネートサーバとして使用している場合に適しています。

この参照先オプションは、eDirectoryツリー内の参照先の処理設定にのみ使用します。このオプションがeDirectoryサーバ以外のサーバの参照の動作に影響することはありません。

他のディレクトリサーバへの参照をブロックすることにあまり意味はありませんが、これが重要になる場合もあります。eDirectory 8.7以降のサーバ上の信頼されていないデータを古いバージョンのeDirectoryサーバ上で複製すると、古いサーバを参照したときにクライアントアプリケーションのグローバルツリーが歪んで表示されることがあります。

たとえば、LDAPクライアントはLDAPサーバの参照をキャッシュし、最後に通信したサーバに要求を送信するとします。クライアントが上方参照をサポートするeDirectoryサーバに要求を送信するよう設定されている場合、クライアントのグローバルツリーは正常に表示されます。

しかし、eDirectory 8.7以前のLDAPサーバは、信頼されていない領域と上方参照を認識しません。このため、クライアントがeDirectoryツリー内の以前のバージョンのeDirectoryサーバの参照に従い、要求をそのサーバに送信し続けると、以前のバージョンのLDAPサーバにより、信頼されていないデータが実際のディレクトリツリーデータであるかのように表示されてしまいます。

ただし、クライアントによっては、RootDSEのsupportedFeatures属性を取得し、サーバが上方参照をサポートしているか確認するものもあります。

チェーンを優先する

［チェーンを優先する］オプションを選択すると、通常、検索操作で参照先は返されません。LDAPサーバはその代わり、すべてのeDirectory DSAに対する検索操作を実行します。

ただし、持続的検索制御を設定して検索を実行する場合は例外となります。NetIQが実装する持続的検索ではチェーンがサポートされていないため、検索スコープがローカルに限られていなければ参照が送信されます。

LDAPサーバが検索操作を受信します。ツリーのエントリがローカルに格納されていない場合、サーバは自動的に他のサーバにチェーンします。エントリの検出後、LDAPサーバはLDAPクライアントのプロキシとして機能します。LDAPサーバはLDAPクライアントがバインドされたものと同じ識別情報を使用してリモートサーバの認証を受け、そこで検索操作を続行します。

最初に要求を受信したLDAPサーバが、LDAPクライアントにすべての検索エントリと検索結果を送信します。このLDAPサーバが要求をすべて処理するため、LDAPクライアントからは他のサーバが関与していることはわかりません。

eDirectoryでチェーンを使用すると、あるLDAPサーバに多くのデータがない場合でも、そのサーバがツリー全体のデータを保持しているかのように見えます。

［チェーンを優先する］は、パーティションに深くかかわるオプションです。

シナリオ:他のパーティションで情報を探す— Digital Airlines社で、ユーザがLDAPサーバDAir43に［チェーンを優先する］オプションを選択しました。DAir43はパーティションAにあります。パーティションBはAのサブパーティションで、LDAPサーバDAir44はこのパーティションにあります。

あるLDAPクライアントが検索を要求します。DAir43は、エントリをローカルで検索しますが、データが一部しか見つかりません。DAir43は、要求されたエントリを持つDigitalAir44に自動的にチェーンします。DAir44は、DAir43にデータを送信し、DAir43は、LDAPクライアントにエントリを送信します。

［チェーンを優先する］オプションを使用すると、操作が持続的検索である場合を除き、LDAPサーバは必要に応じて検索を他のサーバにチェーンします。持続的検索の詳細については、「430ページの 「持続的検索: eDirectoryイベントの設定」」を参照してください。

参照を優先する

［参照を優先する］オプションを選択すると、必要に応じ、参照の検索結果がeDirectoryツリー内の他のeDirectoryサーバに返されます。この参照は、データを持つサーバが動作可能であり、LDAPサービスが稼動していることをローカルサーバが確認した場合のみ送信されます。それ以外の場合、操作は他のサーバにチェーンされるか、他のサーバが動作していない場合は処理に失敗します。

パーティションが2つあり、サブツリー検索を実行するとします。ローカルサーバから検索エントリがすべて検出されるまで検索が実行されます。そこで、今度は他のサーバの検索を実行します。データのレプリカ(そのパーティション)を持つサーバがnldap.nlmも実行している場合、LDAPサーバはLDAP参照を確立し、それをLDAPクライアントに返します。

レプリカのあるサーバがnldap.nlmを実行していない場合、LDAPサーバは要求を他のサーバにチェーンし、そこで検索を完了します。

nldap.nlmが起動されると、LDAPサーバはそのLDAPサーバが参照先となっているeDirectoryと通信します。クライアントが参照を受信したのに、その参照が停止した場合は、LDAPサーバが実行されていません。

常に参照する

［参照を優先する］オプションは、デフォルト参照がさまざまなフェイルオーバー(たとえば、オブジェクトが見つからなかったり、サーバがダウンしているなど)の状況で送信される場合を除き、［参照を優先する］と同じロジックに従います。

残りのデータのある他のサーバでLDAPサービスが実行されていない場合、最初のLDAPサーバは要求を第2のサーバへチェーンしません。

［常に参照する］オプションを設定している場合には、デフォルト参照を指定することができます。［デフォルトの照会先］フィールドで2つの異なるベンダのLDAPサーバを結合し、独自のディレクトリツリーを構築することができます。

シナリオ:デフォルトのサーバを使用する— 1つのLDAPツリーがあるとします。ツリーの一部にはeDirectoryのサービスが適用されています。サブオーディネイトパーティションにはiPlanetのサービスが実行されています。［デフォルトの照会先］フィールドに、iPlanetサーバのURLを入力します。あるLDAPクライアントが検索を要求します。

ベースDNを解決できないため、LDAPサーバは［デフォルトの照会先］フィールドに入力された文字列をクライントに送ります。LDAPクライアントはこの参照のURLで指定された場所を参照してiPlanetサーバに接続し、ここで検索は完了します。

デフォルト参照が設定されており、サーバが探しているベースDNを見つけられない場合、クライアントはデフォルト参照を受け取ります。

参照の形式は、LDAP URLです。例: LDAP://123.23.45.6:389

LDAPサーバがデフォルト参照をクライアントに送信するとき(ベースDNが利用できない場合)は、サーバはこれにスラッシュ(/)とクライアントが検索中のDNを追加します。デフォルト参照と追加された情報がクライアントに送信されます。クライアントはデフォルト参照で指定したサーバに検索要求を送信します。

LDAPグループオブジェクトには、デフォルト参照の文字列フィールドがあります。LDAPサーバは、そのデータを文字列として扱います。このとき、確認は行われません。入力された文字列が、参照の先頭に追加されます。また、なんらかのデータが参照に追加されます。LDAPサーバが受け入れる文字列の形式は、URLのような形式になります。

LDAPが実行されている他のeDirectoryサーバの参照がクライアントに返されるとき、クライアントは1つのサーバにつき2つの参照を受信します。

- クライアントをクリアテキストポートに導く参照
- クライアントをセキュアポートに導く参照

2つの参照を区別するために、クリアテキスト参照にはldap://、セキュアポートの表示にはldaps://が付きます。

サーバからの参照の場合は、ポート番号を追加します。

他の操作の参照を設定する

履歴参照オプション設定は通常、検索操作にのみ使用します。他の処理に比較オプションを適用する場合は、ldapOtherReferralOption属性が使用されます。この属性により、同じ値を使って検索以外の操作の動作を制御できます(参照を送信しないバインドは除きます)。

参照フィルタリング

ツリーで実行されている複数のレプリカサーバがあり［参照を優先する/常に照会］オプションを使用して参照を返すようにLDAPサーバを設定してある場合、要求された操作内のDNによって識別されるオブジェクトがローカルに存在しないと、LDAPサーバは参照を返します。そのような場合、LDAPクライアントはサーバに要求を送信し、サーバはそのオブジェクトを保持しているすべてのLDAPサーバの参照リストを返します。この参照リストを使用して、LDAPクライアントはこれらの参照のいずれかに従って操作を実行します。クライアントがリソース不足のサーバまたは低速リンクを経由するサーバへの参照に従うことを選択した場合、クライアントはサーバから応答が遅いと認識する場合があります。この場合、LDAPクライアントのパフォーマンスが影響を受けます。LDAPアプリケーション開発者はサーバとネットワークの構成に関する完全な知識を持っていないため、この問題の解決策は、LDAPサーバに参照フィルタリングメカニズムを提供し、特定のサーバの参照を返すことです。管理者は、ネットワークおけるLDAPサーバの性質やネットワークリンクの速度など、必要な知識を持ち、参照フィルタリングの適切な設定を行うことができる場合があります。

属性「referralIncludeFilter」と「referralExcludeFilter」を使用して、LDAPグループオブジェクトに参照フィルタを設定します。これらの属性でこれらのフィルタを設定すると、このLDAPグループオブジェクトに属するすべてのLDAPサーバにこの設定が適用されます。LDAPサーバは、referralIncludeListフィルタに一致するすべてのLDAP参照を返し、referralExcludeFilterフィルタに一致するものをドロップします。

referralIncludeFilterのみを指定した場合、referralIncludeFilter値に一致するLDAP参照がLDAPクライアントに返され、それ以外のすべての参照は参照リストから除外されます。同様に、referralExcludeFilterのみを指定した場合、referralExcludeFilter値に一致しないLDAP参照がLDAPクライアントに返されます。両方のフィルタが存在し、参照がこれらのフィルタのどちらにも一致しない場合、参照は除外されます。

使用可能なすべての参照がフィルタによって許可されていない場合、サーバは使用可能な参照がないかのように動作し、LDAP_OTHER(80)を返します。一部のクライアントツールはこれを「不明なエラー」としてレポートします。これらのフィルタ属性を追加または変更した後、LDAPサーバがリフレッシュされなかった場合、変更内容は次の自動リフレッシュ後に有効になります。

現時点では、これらのフィルタ属性の追加または変更は、iManagerのタブでのみ実行できます。

LDAP参照フィルタリングを指定する形式 —LDAP参照フィルタの形式は、次の単純なIPアドレス形式です。

[ldap://] | [ldaps://] *IPAdress*[:port]

ここで、クリアテキストポートまたはTLSポートを指定することは、先頭にldap://またはldaps://文字列を付加することと同じです。ldapまたはldapsのどちらも指定しない場合、一致検索フィルタはクリアテキスト参照とTLS参照の両方に適用されます。

例:

例	説明
1.2.3.4	# 任意のポートでLDAPとLDAPSの両方の参照に一致
1.2.	# 1.2.X.Yというすべてのipアドレスに一致
1.2.3.	# 1.2.3.Yというすべてのipアドレスに一致
ldap://またはldap://*	# すべてのクリアテキストポートLDAP参照に一致
ldaps://またはldaps://*	# すべてのSSLポートLDAP参照に一致
*	# すべてに一致
ldaps://5.6.7.8:636	# 5.6.7.8というipアドレスのSSLポート636に一致

これらのフィルタ属性(referralIncludeFilterおよびreferralExcludeFilter)は複数値です。必要な数の一致フィルタを選択できます。

サンプルシナリオ

- LDAPサーバが1.2.X.YというIPアドレス(X = {0〜255}およびY = {0〜255})の参照のみを返し、他のすべてを除外するには、次のように入力します。

  referralIncludeFilter = { 1.2 }

- LDAPサーバが164.99.X.YというIPアドレス(Xは100以外)に一致するすべての参照を除外し、164.99.100.Yに一致する参照を返すには、次のように入力します。

  referralIncludeFilter = { 164.99.100., "*"}

  referralExcludeFilter = { 164.99. }

  ここで、IPアドレス164.99.100.YはreferralExcludeFilterに一致しますが、これらのIPアドレスはreferralIncludeFilterとより多くのフィールドで一致するため、これらの参照はLDAPクライアントに返されます。

  注: 部分的なIPアドレスを指定する際、末尾の「.」は省略できます。

- LDAPサーバがクリアテキストポート参照のみを返し、SSLポート参照をドロップするには、次のように入力します。

  referralIncludeFilter = { "ldap://" }

  または

  referralExcludeFilter = { "ldaps://" }

- LDAPサーバがIPアドレスのセットから返し、それ以外のすべてのIPアドレス参照をドロップするには、次のように入力します。

  referralIncludeFilter = { 1.2.3.4, 2.3.4.5:389, 3.4.5.6:636, ldaps://4.5.6.7 }

  referralExcludeFilter = { "*" }

  注: ここで、referralExcludeFilterは必要ありません。いずれかの入力されたreferralIncludeFilterは他のすべてを除外することを意味します。

- 次のように2つのフィルタがあるとします。

referralIncludeFilter = { 1.2.3.4 }

referralExcludeFilter = { 2.3.4.5 }

IPアドレス3.4.5.6の参照は、referralExcludeFilterに一致しないとしても、referralIncludeフィルタとも一致しないので除外されます。

無効なフィルタ —次のフィルタはサポートされていません。

「.2.3.4」または「*.2.3.4」は、IPアドレス*X*.2.3.4に一致しません。

「2.3.4*」は2.3.41または2.3.42のようなIPアドレスに一致しません。

sever1.mydomain.comまたは*.mydomain.comのようなDNS名はサポートされていません。最初のポートから最後のポートまでを指定した参照IPアドレスの許可など、フィルタにポート範囲を追加することはできません。これらの属性にこれらのフィルタの値を追加する前に、検証チェックは行われません。ただし、無効なフィルタの場合、LDAPサーバはそれらのフィルタを無視し、ログをndsd.logファイルに記録します。

既知の問題 —LDAProotDSE検索では、LDAPURL形式のレプリカサーバがある場合、altServersが返されます。これらのURLは、このメカニズムを使用してフィルタ処理されません。

ManageDsaITの非サポート

LDAP Services for eDirectoryでは、eDirectoryツリー内のeDirectoryサーバの分散関係は、ManageDsaIT制御以外の方法で管理されます。ManageDsaIT制御によって、LDAPクライアントがeDirectoryサブオーディネートまたは相互参照の問い合わせや更新を実行することはできません。

サポートされていない機能

LDAP Services for eDirectoryは、サブオーディネートリファレンスをサポートしていません。信頼されたパーティションのサブオーディネートパーティションとして信頼されていないパーティションを作成したり、そのパーティションから参照を送信させると失敗する場合があります。これを行う場合、参照は操作のベースDNを解決するときのみ送信されます。SearchResultReferencesは送信されません。

信頼されていない領域のデータの分散更新はサポートされていません。ルートサーバで名前の変更があった場合、名前の変更を信頼されていない領域で同じデータを持ったeDirectoryサーバにコピーするような組み込みのメカニズムはありません。

フィルタ済みレプリカを検索する

フィルタはレプリカが持つデータ量を制限します。そのため、フィルタ済みのレプリカには、ディレクトリが保持する実データが完全には表示されません。次はレプリカに適用されたフィルタの例です。

- レプリカに含まれるのはユーザオブジェクトだけです。
- レプリカにはすべてのユーザオブジェクトが含まれますが、オブジェクトには電話番号と住所しか含まれません。

フィルタ済みレプリカのデータは不完全なため、LDAP検索の結果も制限されます。そのため、デフォルトでは、LDAP検索要求はフィルタ済みレプリカを調べません。

次のような場合は、フィルタ済みレプリカ検索を実行しても、レプリカフィルタから何も検索結果が返されないことがあります。

- 検索フィルタに一致するオブジェクトがローカルのフィルタ済みレプリカサーバに存在しない場合、結果が完全なレプリカサーバから取得されるため、ローカルのレプリカフィルタの結果と一致しないことがあります。
- 検索ベースがフィルタ済みレプリカサーバのローカルにない場合、検索フィルタに一致するオブジェクトが完全なレプリカサーバから取得され、これがローカルレプリカのフィルタの結果と一致しないことがあります。

ただし、フィルタ済みレプリカに必要なデータがあることがわかっている場合は、LDAPサーバがフィルタ済みレプリカを検索するように設定することができます。

1 NetIQ iManagerで、［**役割およびタスク**］ボタン をクリックします。
2 ［**LDAP**］ > ［**LDAPオプション**］をクリックする。
3 ［**LDAPサーバの表示**］をクリックし、LDAPサーバの名前をクリックします。
4 ［**検索**］をクリックします。
5 ［**検索にフィルタ済みレプリカを含める**］を選択し、［**適用**］をクリックします。

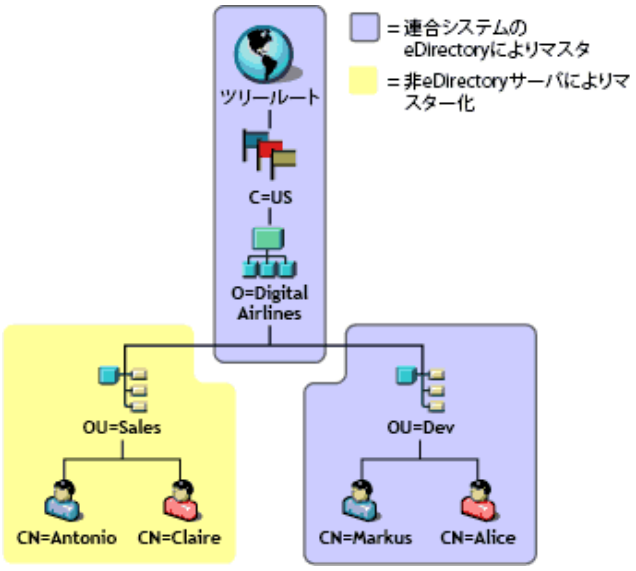
上方参照を設定する

組織の規模が大きくなると、さまざまなベンダのLDAPサーバソフトウェアを使用したディレクトリツリーが必要になります。このようなツリーを、グローバル連結ツリーといいます。LDAPServices for eDirectoryには、参照を連結ツリーの上方のDSAに返す機能があります。

シナリオ:連結ツリーでの上方参照

Digital Airlines社には、あるネットワーク担当者がいます。Digital Airlines社のディレクトリツリーのルート(ツリーのルートからO=Digital Airlinesまで)のマスタは、OpenLDAPサーバ上にあります。組織(OU=Sales)のマスタはeDirectoryサーバにあり、その他の組織(OU=Dev)はiPlanetサーバ上にあります。

次の図は、このツリーを示します。



eDirectoryにマスタがあるのは、OU=Salesのパーティション内のデータだけです。他の領域のデータのマスタはeDirectory以外のDSA上にあります。ネットワーク担当者は、操作の対象がO=Digital Airlinesより上の領域、またはOU=Sales階層に属さないO=Digital Airlinesより下の領域である場合、上方参照を返すようにLDAPサービスを設定します。

ベースDNがOU=Dev,O=Digital Airlines,C=USのeDirectory LDAPサーバに操作が送信されます。そのエントリを保持するサーバ、またはそのエントリを保持するサーバを認知しているサーバを指す参照が返されます。

同様に、O=Digital Airlines,C=USが対象のサブツリー検索でも、ルートDSAの参照が返されます。するとルートDSAが、OU=SalesおよびOU=Devのマスタであるの照会を返します。

LDAPサービスにより、eDirectoryサーバがこのツリーに参加するのにデータ階層データを信頼されていないパーティションに持つことができます。信頼されていない領域のオブジェクトに含まれるのは、正しいDN階層を構築するのに必要なエントリだけです。これらのエントリは、X.500の“Glue”エントリに類似しています。

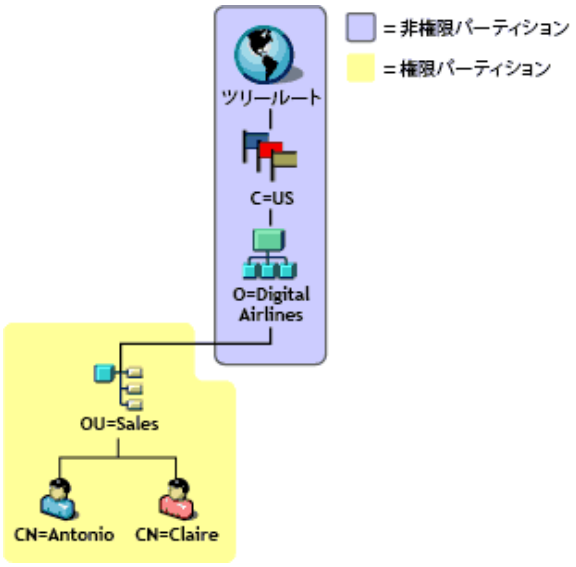
このシナリオでは、ルート、C=US、O=Digital AirlinesオブジェクトはeDirectoryサーバの信頼されていない領域にあります。

eDirectoryでは、知識情報(参照データ)を信頼されていない領域に置くことができます。この情報は、LDAPクライアントに参照を返すのに使用します。

LDAP操作をeDirectoryツリーの信頼されていない領域で実行すると、LDAPサーバは正しい参照データを検索し、クライアントに参照を返します。

信頼されていない領域を作成する

次の図は、「425 ページの 「シナリオ:連結ツリーでの上方参照」」で示した、eDirectoryサーバの連結ツリーが保持する実際のデータを示しています。



エントリは、マスタが他のDSA上にあっても、OU=Sale s 上に配置されます。これは、eDirectoryサーバが持つエントリに適切なDNを提供できるようにするためです。

信頼されていない領域を作成するには、次を実行します。

1 信頼されていないデータは信頼されたデータとは切り離します。

信頼された領域の最上部に、パーティション境界を作成します。他に指定がない場合、eDirectoryサーバはすべてのデータに対して信頼されたサーバであるとみなされます。

2 ルートパーティションに信頼されていないパーティションとマークします。

2a 信頼属性を、パーティションの最もルートに近い属性に追加します。

2b 値が0の信頼属性を作成します。

3 信頼されていない領域の最下部に境界線をひきます。

このサーバの信頼されたサブツリー領域にパーティションルートを作成します。たとえば上の図の場合は、パーティションルートはOU=Saleエントリにあります。新しいパーティションには、0に設定された信頼された属性はありません。そのため、サーバはパーティションに対し信頼されたサーバであることになります。

4 LDAPサーバをリフレッシュします。

LDAPサーバは、その設定がリフレッシュされるたび、信頼された領域および信頼されていない領域の境界をキャッシュします。手動でサーバの設定をリフレッシュしない場合、サーバは30分ごとのバックグラウンドタスクで自動的にリフレッシュします。

複数のパーティションがある場合は、信頼された領域のチェーンに重ねることができます。ただし、LDAP Services for eDirectoryでは、すべての信頼されていないパーティションは連続していなければならず、ローカルレプリカがそれを保持している必要があります

参照データを指定する

操作が信頼されていない領域で実行されていることが検出されると、LDAPサーバは参照をクライアントに返すのに使用する情報を探します。この参照情報は、次のいずれかになります。

- 信頼されていない領域のいずれか、またはすべてのエントリにある情報
- サーバの環境設定データを持つLDAPサーバまたはLDAPグループオブジェクト上の、デフォルト参照として指定された情報

信頼されていない領域のエントリが持つ参照情報は、即時上方参照です。このような参照情報は、複数の値をとるref属性から構成されています。この属性の詳細については、RFC 3296 (http://www.ietf.org/rfc/rfc3296.txt)を参照してください。

デフォルト参照設定が持つ参照情報は上方参照で、値を1つとります。X.501のimmSuperおよびsuprDSEタイプを参照してください。

参照データはLDAP URLの形式で保持されますが、これにはホストと(オプションで)参照先のDSAのポートだけしか指定されていません。この参照データの例は次のようになります。

```
ldap://ldap.digital_airlines.com:389
```

LDAPサーバは操作のベースDN(見つからない場合は一致したDN)を参照します。ベースDNに参照情報が含まれる場合、LDAPサーバはその情報を参照先として返します。

参照情報が見つからない場合、LDAPサーバはツリーの上方向に向かって参照情報を探します。すべてのエントリを検索しても参照情報が見つからない場合、LDAPサーバは上方参照を返します。この参照先は、LDAPグループまたはLDAPサーバオブジェクト上のデフォルト参照設定にあります。

即時上方参照の追加

immediateSuperiorReferenceと呼ばれる補助オブジェクトクラスを信頼されていない領域のエントリに追加することができます。この補助クラスは、1つ以上のLDAP URLとともに作成されるref属性を追加します。それぞれのURLはDSAのホスト名と(オプションで)ポートを指します。

上方参照を追加する

これまで、LDAPグループオブジェクトはldapReferral属性を持っていました。この属性は、eDirectoryツリーの他のeDirectoryサーバに参照を返すときに発生する、さまざまなフェイルオーバーの状況で使用されるデフォルトの参照先を保持していました。LDAP Services for eDirectoryでは、この属性は、連結ツリーの上方DSAのデフォルト参照を1つ指定するために使用します。

また、ldapReferral属性がLDAPサーバオブジェクトに追加されました。ldapReferral属性にLDAPサーバオブジェクトの値が含まれる場合、この設定によりLDAPグループオブジェクトの同じ属性の値は上書きされます。この動作により、グループに属するすべてのLDAPサーバに特定のデフォルト参照を設定し、1つか2つのサーバのデフォルト参照を別のデフォルトで上書きすることができます。

ldapReferral属性の値は、LDAP URLです。URLには、ホストと参照先のDSAのポート(オプション)が含まれます。

LDAPで参照情報を更新する

上記のステップに従い、LDAPを使ってこのタスクを実行しても、即時上方参照を追加することはできないことが多くありました。これは、ルートパーティションがすでに信頼されていないとマークされており、LDAPはパーティション内のデータに対するどの操作についても参照を送信していたためです。

信頼されていない領域の情報の更新または問い合わせを行うには、LDAP要求にManageDsaIT制御を設定する必要があります。この制御の詳細については、RFC 3296 (http://www.ietf.org/rfc/rfc3296.txt)を参照してください。この制御により、LDAPサーバは信頼されていない領域全体を信頼された領域であるかのように扱うことができます。

注: 上方参照機能は、LDAPでのみ利用できます。他のプロトコル(NDAPなど)には、信頼属性が存在することによる影響はありません。そのため、NetIQ iManagerを使用した信頼されていない領域のデータの参照や更新が妨害されることはありません。

影響を受ける操作

信頼されていない領域と上方参照は、次のLDAP操作に影響します。

- 検索と比較
- 編集と追加

  DN構文属性値はチェックされません。そのため、グループメンバー属性は、信頼されていない領域のエントリを指すDNを含むことができます。
- 削除
- ﾘﾈｰﾑ (moddn)
- 移動(moddn)

  親DNが信頼されていない領域にある場合、affectsMultipleDSAsエラーが返されます。
- 拡張

上方参照のサポートの有無を確認する

上方参照は、Novell LDAP Services for eDirectory 8.7以降でのみサポートされています。ルートDSEのsupportedFeatures属性により、eDirectoryサーバがこの機能をサポートしているかどうかを確認できます。supportedFeatures属性の値がOID 2.16.840.1.113719.1.27.99.1である場合は、この機能はサポートされています。その他のルートDSEオブジェクトに対する確認方法では、次が変更されています。

- namingContexts

  この属性は、サーバが信頼されているローカルDSAに保持されるパーティションルートだけを表示します。信頼されていないパーティションルートは表示されません。
- altServer

  この属性は、ローカルサーバと信頼されていないパーティションだけを共有する他のeDirectoryサーバをリストしません。

- superiorReference

  この属性は、DSAの上方参照を通知します。この値は、LDAPサーバまたはLDAPグループオブジェクト上のldapReferral属性を更新することにより管理されます。

持続的検索: eDirectoryイベントの設定

NetIQ eDirectoryでは、ディレクトリ内で重大なイベントが発生したときにアプリケーションに通知するためのイベントサービスが用意されています。これには、ディレクトリサービスに関する一般イベントも含まれます。それ以外はeDirectoryとその機能に固有のイベントです。

eDirectoryイベントは、LDAPプロトコルに対して、次の2つの異なる拡張を通してアプリケーションに通知されます。

- 持続的検索制御の実装

  NetIQ eDirectoryの持続的検索機能は、最初の一致するエントリが返された後も続行される検索操作です。持続的検索はLDAP ｖ3の検索操作が拡張されたもので、クライアントからサーバへの検索結果内で更新をチェックする作業が不要になります。持続的検索制御により、クライアントは、ベースDN、検索スコープ、検索フィルタなどを指定する通常のLDAP検索操作を実行することができます。その後、サーバは最後にSearchResultDoneメッセージを返すのではなく、操作による接続が維持されます。このため、クライアントは検索結果に含まれるのエントリが変更されるたびに、最新のエントリを受け取ることができます。これにより、更新が発生するたびにクライアントは目的のエントリのキャッシュを維持したり、何らかのロジックをトリガすることができます。

  記事「Persistent Search: A Simple LDAP Change Notification Mechanism (http://www.ietf.org/proceedings/01mar/I-D/ldapext-psearch-03.txt)」では、この拡張についてさらに詳しく説明しています。

- イベントの監視(eDirectory独自の拡張LDAP操作)

eDirectoryイベントサービスを使用するアプリケーションは、ディレクトリに対する大きな計算負荷となることがあります。そこで、さまざまな属性パラメータを使用して、個々のeDirectoryサーバにおけるイベントサービスの使用を制御することができます。これらのパラメータはLDAPサーバオブジェクト上に格納されます。NetIQ iManagerを使用して、これらのパラメータを設定します。

イベントサービスを使用する特定のアプリケーションにより、これらのパラメータを特定の値に指定するよう要求される場合があります。特定のアプリケーション独自の要求は、そのアプリケーションのマニュアルに示されています。

詳細については、「Understanding and Using Persistent Search in eDirectory (http://support.novell.com/techcenter/articles/dnd20030204.html)」を参照してください。

持続的検索の管理

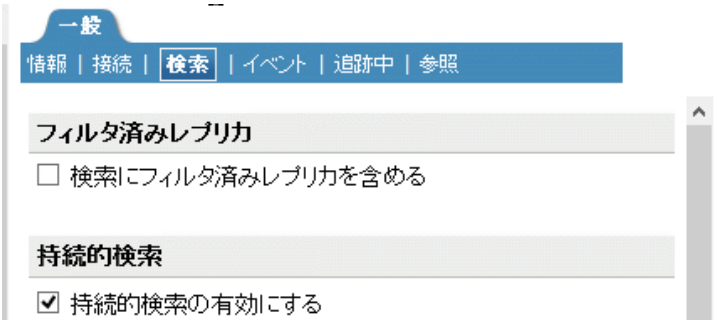
iManagerを使用すると、持続的検索を表示または編集することができます。

1 iManagerで、［**役割およびタスク**］ボタン  をクリックします。

2 ［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。

3 変更するLDAPサーバオブジェクトの名前とコンテキストを入力するか、をクリックし、LDAPサーバオブジェクトをブラウズまたは検索します。

4 ［OK］をクリックし、［全般］タブの［検索］をクリックします。



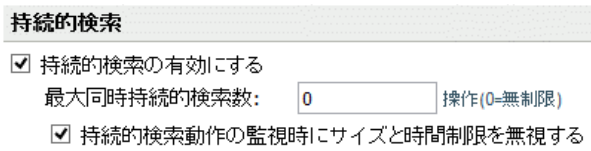
5 持続的検索を有効にします。

［持続的検索を有効にする］チェックボックスはデフォルトでオンになっています。このサーバの持続的検索を無効にして禁止するには、チェックボックスをオフにします。

注: 以前に確立された持続的検索操作を無効にすると、このオプションを無効にしてサーバをリフレッシュした後も操作が継続する場合があります。

6 このサーバ上の同時持続的検索の数を制御します。

［最大同時持続的検索数］フィールドの値を指定します。0を指定すると、同時持続的検索数は無制限になります。



7 サイズおよび時間の制限を無視するかどうかを制御します。

持続的検索要求が最初の検索結果を送信した後で、サイズおよび時間制限を無視するかどうかを指定するには、［持続的検索動作の監視時にサイズと時間制限を無視する］チェックボックスをオンにします。

このオプションを選択しない場合、すべての持続的検索操作は検索制限の制約を受けます。サイズと時間のいずれかの制限に達した場合、検索操作は失敗し、該当するエラーメッセージが返されます。

8 適用をクリックし、OKをクリックします。

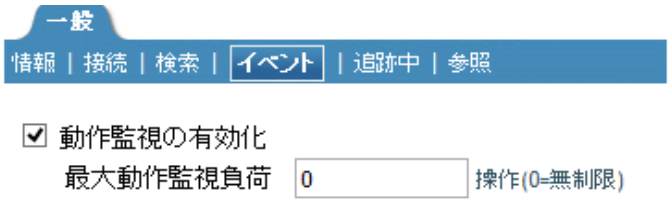
イベントの監視拡張操作の使用を制御する

1 iManagerで、［役割およびタスク］ボタン をクリックします。

2 ［LDAP］ > ［LDAPオプション］をクリックする。

3 ［LDAPサーバの表示］をクリックし、LDAPサーバの名前をクリックします。

4 ［イベント］をクリックします。



5 クライアントアプリケーションがこのLDAPサーバ上でイベントを監視できるかどうかを制御します。

クライアントアプリケーションがこのLDAPサーバ上でイベントを監視できるようにするには、［**動作監視の有効化**］チェックボックスをオンにします。

イベントの監視を無効にするには、チェックボックスをオフにします。

6 イベント監視アプリケーションがサーバ上に置くことのできる最大負荷を制御します。

［**最大動作監視負荷**］フィールドに値を入力します。

イベントデータの処理と、監視対象アプリケーションへのイベント通知の送信は、LDAPサーバに対して計算負荷となります。あるイベントによるサーバへの正確な負荷は、監視されるイベントの頻度、イベントに関係したデータ、およびそのイベントを監視しているクライアントアプリケーションの数によって決まります。

［最大動作監視負荷］は、イベント監視拡張がサーバにかけることができる負荷の大きさを示す相対値です。0を指定すると、無制限になります。この属性の適切な値を見つけるには、実際にいろいろな値を試してみてください。

7 **適用**をクリックし、**OK**をクリックします。

LDAPサーバの情報を取得する

LDAPサーバについての情報を取得するには、ICEかLDAP検索を使用します。これらのユーティリティはrootDSE(ディレクトリサービスエージェント、固有エントリ)から情報を要求します。

rootDSEは、ディレクトリツリーの擬似オブジェクトです。このオブジェクトは、ツリーのルートにある名前のないエントリです。rootDSEは接続しているサーバに固有の情報を持っています。たとえば、rootDSEはスキーマと、スキーマがサポートする拡張およびコントロールの場所の情報を持っています。

rootDSEはツリー内の名前のないエントリであるため、通常、LDAPサーバは検索操作でrootDSEをクライアントに返しません。

次の表は、rootDSEから得られる情報を表示したものです。

情報と説明	引用
スキーマの場所: LDAPサーバまたはツリーのスキーマの場所は、subschemaSubentryを読み込むことによって検索できます。eDirectoryでは、cn=schemaが検索のベースになります。	subschemaSubentry: cn=schema

情報と説明	引用
サポートされている拡張:拡張により、コンテキストの作成、マージ、新しいレプリカの追加、LDAPサーバのリフレッシュ、レプリカの削除、レプリカタイプのマスタから読み込み/書き込みまたは読み込み専用への変更などのサーバの管理、および識別情報の管理ができます。 拡張の形式はASN.1OIDです。拡張の詳細については、「LDAP Extensions (http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/a6ik7oi.html)」を参照してください。	supportedExtension: 2.16.840.1.113719.1.27.100.12 supportedExtension: 2.16.840.1.113719.1.27.100.7 supportedExtension: 2.16.840.1.113719.1.27.100.8
LDAPサーバを提供しているベンダ	vendorName: NetIQ Corporation.
LDAPサーバがサポートしているディレクトリバージョン	vendorVersion: eDirectory v8.7.0 (10410.29)
eDirectoryが実行しているバージョン	vendorVersion: eDirectory v8.7.0 (10410.29)
ディレクトリサーバ名とディレクトリツリー名	dsaName: cn=WestWindNDS,o=westwind directoryTreeName: t=WESTWINDTREE
サポートされているSASLメカニズム	supported SASLMechanisms: EXTERNAL supported SASLMechanisms: DIGEST-MD5 supported SASLMechanisms: NMAS LOGIN
サポートされているLDAPサーバのバージョン。	supportedLDAPVersion: 2 supportedLDAPVersion: 3
サーバ統計情報: rootDSEはLDAPサーバに関するさまざまな統計情報を提供します(強力な認証バインド数など)。	errors: 0 securityErrors: 0 chainings: 3 referralsReturned: 6 extendedOps: 0 abandonOps: 0 wholeSubtreeSearchOps: 1

rootDSEの情報は、アプリケーション開発に活用することができます。

シナリオ:アプリケーションの開発— あるユーザが新しいレプリカを作成するアプリケーションを作成しています。rootDSEを読み込むと、リストにsupportedExtension: 2.16.840.1.113719.1.27.100.7と記述されています。これにより、サーバが新しいレプリカを作成するコールをサポートすることがわかります。

また、NetIQ iManagerはrootDSEで利用できる機能をチェックし、その情報に従って動作します。

rootDSEを検索するには、ワークステーションで次を入力します。

ldapsearch -h *hostname* -p 389 -b "" -s base "objectclass=*"

この検索は、ldap_search APIを使用したどのアプリケーションでも実行することができます。

検索の鍵はスコープがベース(-s base)であることです。また、ベースはnullであり、フィルタがobjectclass = *に設定されていることにも注意してください。このクライアントの場合、ベースは-bです。

rootDSEの読み取り方法の詳細については、次のいずれかを参照してください。

- LDAP Libraries for C (http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html)
- LDAP Classes for Java (http://developer.novell.com/documentation/jldap/jldapenu/data/bktitle.html)

LDAP検索フィルタの詳細については、LDAP Search Filters (http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/a3saoeg.html)を参照してください。このセクションは、NDKマニュアルの「LDAP and NDS Integration」にあります。

汎用タイムサポートの設定

汎用タイムサポートのオプションによって、時間をYYYYMMDDHHmmSS.0Z形式で表示できます。ldapconfigユーティリティまたはLDAP iManagerプラグインを使用して、LDAP汎用タイムサポートを有効または無効にすることができます。

汎用タイムサポートは、次のいずれかの方法を使用して有効にすることができます。

LDAP iMangerプラグイン

1. NetIQ iManagerで、［**役割およびタスク**］ボタンをクリックします。
2. ［**LDAP**］>［**LDAPオプション**］>［**LDAPサーバの表示**］の順にクリックします。
3. ［LDAPサーバオブジェクト］>［**検索**］の順にクリックします。
4. ［非標準の動作］セクションにスクロールして、［**時刻を一般的な形式で表示します**］をクリックし、［**OK**］をクリックします。

ldapconfigユーティリティ

```
ldapconfig set "ldapGeneralizedTime=yes/no" -a <admin-FDN> -w <admin-password">
```

許容変更制御の設定

ldapPermissiveModifyオプションをTRUEに設定することで、現在のLDAP変更操作を拡張できます。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。

LDAP iMangerプラグイン

1. NetIQ iManagerで、［**役割およびタスク**］ボタンをクリックします。
2. ［**LDAP**］>［**LDAPオプション**］>［**LDAPサーバの表示**］の順にクリックします。
3. ［LDAPサーバオブジェクト］>［**検索**］の順にクリックします。
4. ［非標準の動作］セクションにスクロールして、［**PermissiveModifyControlを有効にする**］をクリックし、［**OK**］をクリックします。

ldapconfigユーティリティ

```
ldapconfig set "ldapPermissiveModify=yes/no" -a <admin-FDN> -w <admin-password">
```

プロキシ承認コントロール

eDirectoryには、RFC4370で規定されているように、LDAPプロトコルを使用してプロキシ承認を制御する柔軟性があります。プロキシ承認コントロールにより、クライアントは、接続に関連付けられている現在の承認IDの代わりに、指定された承認IDを使用して操作を処理することを要求できます。この機能は、各操作の承認IDを指定するためのメカニズムを提供し、複数のユーザの代わりにいくつかの操作を実行する必要があるクライアントで役に立ちます。

eDirectoryサーバで認証するには、管理者がクライアント要求でプロキシ承認コントロールOID、2.16.840.1.113730.3.4.18を指定する必要があります。プロキシ承認コントロールを使用するには、認証済みユーザが偽装ユーザに対してスーパバイザ権を持っている必要があります。

1. eDirectoryツリーを作成し、そこにユーザオブジェクトを追加します。
2. ログインして、［iManager］>［役割およびタスク］>［権利］>［トラスティの変更］の順に選択して、ユーザを選択します。
3. OKをクリックします。
4. ［トラスティの追加］をクリックして、リストから別のユーザを選択します。
5. ユーザの［割り当てられた権利］をクリックします。
6. ［All Attribute Rights］には［スーパバイザ］を選択し、ユーザには［エントリ権］を選択します。
7. ［完了］をクリックし、［適用］をクリックします。

ldapsearchのプロキシ承認を実行するには、次のコマンドを使用します。

```
ldapsearch -x -h <SrvIP> -p <Port> -D <Admin DN> -w <Password> -e
'!authzid=dn:<Impersonate user> -b o=novell -s one
```

プロキシ承認コントロールを使用して他のLDAP操作を実行するには、LDAP要求に2.16.840.1.113730.3.4.18 OIDを指定します。

プロキシ承認操作の監査

プロキシ承認操作を監査するために、eDirectoryは、DSE_IMPERSONATEという新しいイベントを提供します。

LDAP拡張DNコントロール

eDirectoryにはLDAP拡張DNコントロールが備わっています。このコントロールは、識別名オブジェクトの拡張フォームを要求するために、拡張LDAP検索で使用しｊます。この拡張フォームには、オブジェクトGUIDの文字列表現と、オブジェクトの識別名が含まれます。

eDirectoryサーバでLDAP拡張DNコントロール機能を使用するには、管理者は拡張LDAP検索要求でLDAP拡張DNコントロールのOID1.2.840.113556.1.4.529を指定する必要があります。

拡張DNコントロールによって、クライアントは、このコントロールを使用するLDAP検索によって返される結果に、オブジェクトのGUIDデータと、distinguishedNameオブジェクトが含まれるように要求できます。次のように返されます。

```
<GUID=xxxxxxxx>;distinguishedName
```

xxxxxxxxはGUIDが含まれる文字列、distinguishedNameはDN(例: cn=users,dc=fabrikam,dc=com)です。

LDAP拡張DNコントロールは、整数のフラグ値も渡すことができます。渡されるフラグ値によって、返されるGUID値の文字列形式が決まり、次のBERエンコードシーケンスに設定されます。

```
Sequence {
  Flag    INTEGER
}
```

フラグ値0の場合、GUID値は16進数文字列形式で返されます。例:
<GUID=3BC72D2DEC5A704BBDC21F4EF97B7870>

フラグ値1の場合、標準文字列形式でGUID値が返されます。例: <GUID=098f2470-bae0-11cd-b579-08002b30bfeb>

一部としてDNが含まれるeDirectoryのデータタイプには複雑なものもいくつかあります。eDirectoryがLDAP拡張DNコントロールで処理する複雑なデータタイプは以下のみです。

- SYN_PATH (volumeDNのGUIDが返されます)
- SYN_DN
- SYN_TYPED_NAME

注: 前述の複雑なデータタイプが含まれる拡張DNコントロールを使用する場合、LDAP検索のパフォーマンスが影響を受けます。

例:

次のC++コード例は、シーケンスデータを手動でフォーマットする方法を示しています。ber_printf関数を使用してシーケンスデータを作成します。フラグ部分には、GUID文字列の書式指定子が含まれます。

```
LDAPControl *FormatExtDNFlags(int iFlagValue)
{
  BerElement *pber = NULL;
  LDAPControl *pLControl = NULL;
  berval *pldctrl_value = NULL;
  int success = -1;

  // Ensure that iFlagValue is either 0 or 1. Convert TRUE (-1) to a legal value.
  if(iFlagValue != 0)
         iFlagValue = 1;

  // Format and encode the SEQUENCE data in a BerElement.
  pber = ber_alloc_t(LBER_USE_DER);
  if(pber==NULL) return NULL;
  pLControl = new LDAPControl;
  if(pLControl==NULL) { ber_free(pber,1); return NULL; }
  ber_printf(pber,"{i}",iFlagValue);

  // Transfer encoded data into a BERVAL.
  success = ber_flatten(pber,&pldctrl_value);
  ber_free(pber,1);
  if(success != 0) {return NULL;}
```

```
  // Copy the BERVAL data to the LDAPControl structure.
  pLControl->ldctl_oid = LDAP_SERVER_EXTENDED_DN_OID;
  pLControl->ldctl_iscritical = true;
  pLControl->ldctl_value.bv_val = new char[pldctrl_value->bv_len];
  memcpy(pLControl->ldctl_value.bv_val,
         pldctrl_value->bv_val, pldctrl_value->bv_len);
  pLControl->ldctl_value.bv_len = pldctrl_value->bv_len;

  // Cleanup temporary berval.
  ber_bvfree(pldctrl_value);

  // Return formatted LDAPControl data.
  return pLControl;
}
```

次のC++コード例は、拡張DNコントロールとldap_search_ext_s関数を併用する方法について示しています。

```
        int err;
        LDAP *ldapConnection = NULL;
        LDAPControl *pExtDNControl;
        LDAPControl *controlArray[2];
        LDAPMessage *results = NULL;
        LDAPMessage *message = NULL;
        char *dn = NULL;

        // Connect to the default LDAP server.
        ldapConnection = ldap_open( NULL, 0 );
        if ( ldapConnection == NULL ) goto FatalExit0;

        // Bind to the server using default credentials.
        err = ldap_simple_bind_s( ldapConnection, NULL, NULL);
        if (LDAP_SUCCESS != err) goto FatalExit0;

        // Setup the extended DN control, requesting 'standard string' format.
        pExtDNControl = FormatExtDNFlags(1);
        if (pExtDNControl == NULL) goto FatalExit0;
        controlArray[0] = pExtDNControl;
        controlArray[1] = NULL;

        // Perform a synchronous search.
        err   = ldap_search_ext_s( ldapConnection,
                        "cn=users,dc=Fabrikam,dc=com",
                        LDAP_SCOPE_SUBTREE,
                        "objectClass=*",
                        NULL,          // Retrieve all attributes.
                        0,             // Retrieve attributes and values.
                        (LDAPControl **) &controlArray,
                        NULL,          // Client controls.
                        0,             // Timeout.
                        0,             // Sizelimit.
                        &results       // Receives identifier for results.
                        );
        if (LDAP_SUCCESS != err) goto FatalExit0;

        // Process the search results.
        message = ldap_first_entry( ldapConnection, results );
        while (message != NULL)
        {
```

```
                // Print the distinguished name of the object.
                dn = ldap_get_dn( ldapConnection, message );
                if (!dn) goto FatalExit0;
                printf( "  Distinguished Name is : %s\n", dn );
                ldap_memfree(dn);
                message = ldap_next_entry( ldapConnection, message );
        }

FatalExit0:
        if (ldapConnection)
                ldap_unbind( ldapConnection );
        if (results)
                ldap_msgfree( results );
}
```

LDAPイベントの監査

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処理が発生する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サーバからフェッチします。

LDAPイベントの監査の詳細については、LDAP Event Services (http://developer.novell.com/documentation/ldapover/ldap_enu/data/ag7bleo.html)を参照してください。

15 NetIQ eDirectoryのバックアップと復元

NetIQ eDirectoryは、レプリケーションにより耐障害性が保たれるようになっています。eDirectoryツリーに属するサーバに障害があっても、別のサーバがサービスを続行できます。この意味でレプリカ作成機能は、最も重要な保護機能と位置づけられています。

ただし1台だけのサーバで運用している環境では、レプリカ作成は不可能です。また、レプリカを作成していても、完全に復元するのは困難な場合もあります。ハードウェア障害など、機器が破損したときや、火事や水害で何台ものサーバが動かなくなってしまった場合などです。各サーバのeDirectoryをバックアップしておけば、ネットワークの耐障害性を高めることになります。

eDirectoryバックアップツールでは、サーバ単位でeDirectoryデータベースをバックアップすることができます。これには次のような利点があります。

- **どのプラットフォームでも同じツールで操作可能。**
- **稼動中でもバックアップ可能。** eDirectoryデータベースを停止することなく、そのままで完全なバックアップを取ることできます。
- **個々のサーバ単位に、迅速な復元処理が可能。** ハードウェア障害からの復元には特に有用です。
- **高い拡張性。** 数千万から数億単位のオブジェクトを保持したeDirectoryデータベースを持つサーバでもバックアップ可能です。バックアップの処理速度は主としてI/Oチャネルの帯域幅で決まります。
- **レプリカ作成機能とDSMASTERサーバを組み合わせて運用していれば、ツリー全体の復元も容易。** DSMASTERサーバを設定していない場合でも、かなりの程度まで復元できます。詳細については、451 ページの 「DSMASTERサーバによる災害対策」を参照してください。
- **関連ファイルもバックアップ可能。** サーバにある、データベース以外の関連ファイルもバックアップできます。NICIセキュリティファイル、ストリームファイル、インクルードファイルで指定したファイル(autoexec.ncfなど)が対象になります。
- **サーバの停止直前の状態にeDirectoryを復元可能。** ただしロールフォワードログを継続的に保存していることが条件です。詳細については、453 ページの 「ロールフォワードログを使用する」を参照してください。
- **ハードウェアのアップグレードを単純化。** サーバの識別情報を新しいマシンに移行する簡単な方法は、eDirectoryデータベースのコールドバックアップを取り、それを復元するやり方です。RAMのアップグレードなど、変更を加える際の安全措置としても有効です。詳細については、563 ページの 「ハードウェアのアップグレードやサーバの交換」を参照してください。
- **分散環境での運用を考慮。** ロールフォワードログがあれば、ツリー内の他のサーバと完全に同期した状態にまで復元できます。
- **無人でのバックアップが可能。** バッチファイルを作成し、DSBK Clientを使用して無人でバックアップを実行できます。

eDirectoryバックアップツールには、個々のサーバ単位でデータベースおよび関連ファイルのバックアップを取り、復元するために必要な機能がすべて揃っています。個々のオブジェクトやツリーの一部を単位としてバックアップ/復元することはできません。

システムバックアップ機能と組み合わせれば、eDirectoryバックアップファイルをテープに保存して安全を期すことができます。

OES 2 Linuxの場合、NetIQ Storage Management Servicesを使用してeDirectoryをバックアップすることができます。SMSには、eDirectoryのバックアップと復元のためのターゲットサービスエージェント(TSA)が用意されています。TSANDSサービスは、ディレクトリツリーのSMSAPIの実装を提供します。アプリケーションはこの機能を使用してeDirectoryオブジェクトのバックアップと復元を行います。

TSANDSは、バックアップアプリケーションを最大限活用するために、次の機能をサポートします。

- eDirectoryオブジェクトに適用できるフィルタ。
- バックアップデータからeDirectoryオブジェクトを選択的に復元。
- 特定のリソースセットをリネームする機能。
- eDirectory変更日に基づく、インクリメンタルバックアップと差分バックアップのサポート。
- SIDF準拠のソフトウェアによるデータ解釈を可能とするSIDFフォーマットのデータ。

TSANDSの使用法に関する詳細については、TSANDSマニュアルページを参照してください。

この章では、次のトピックについて説明します。

eDirectoryのバックアップ処理に関する確認事項

複数サーバ構成のツリーで、サーバが停止していてもオブジェクトにアクセスできるようにする

❒ 複数サーバ構成のツリーでは、耐障害性を得るため、すべてのeDirectoryパーティションについて、複数台のサーバにレプリカが作成されていることを確認します。

レプリカの作成については、「156 ページの 「レプリカを追加する」」を参照してください。

個々のサーバについて、ハードウェア障害などの場合に、迅速に完全復元できるようにするための準備

❒ 定期的に(週1回など)eDirectoryデータベースのフルバックアップを取ってください。

❒ 定期的に(毎晩など)インクリメンタルバックアップを取ってください。

- ❒ EBA対応サーバのフルバックアップを取得する間はNICIおよびストリーム属性を必ず選択してください。そうでない場合、バックアップ操作が失敗します。
- ❒ eDirectoryのフル/インクリメンタルバックアップ終了後、すぐにファイルシステムをテープにフル/インクリメンタルバックアップしてください。

  バックアップツールは、サーバ上の指定したディレクトリにバックアップファイルを作成しますが、これを直接テープに保存する機能はありません。したがって、eDirectoryのバックアップ処理後すぐにファイルシステムのバックアップを行い、安全な記録媒体であるテープに保存する必要があります。
- ❒ 必要に応じて、ロールフォワードログ記録を残すよう設定してください。

  レプリカリングに属するサーバは、ロールフォワードログ機能を有効にしておく必要があります。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないことになります。他のサーバとレプリカを共有するデータベースは、停止直前の状態にまで復元しない限りデフォルトではオープンされません。

  単一サーバ環境では、ロールフォワードログがなくても復元後の検証に失敗することはありませんが、最後にバックアップを取った時の状態にしか戻りません。ロールフォワードログがあれば、システム停止直前の状態まで復元できます。

  ロールフォワードログ機能を使う際の主な注意点は次のとおりです。詳細については、453 ページの 「ロールフォワードログを使用する」を参照してください。

  - ロールフォワードログの新しい場所を指定してください(デフォルトの使用はお勧めしません)。

    ログはサーバ上のローカルファイルとして保存する必要があります。障害対策上、eDirectoryと同じディスクパーティション/ボリューム、同じ記憶デバイスは避けてください。ロールフォワードログ専用の、独立したパーティション/ボリュームを用意するとよいでしょう。
  - ロールフォワードログの保存先を文書に記録しておき、障害時にはすぐにわかるようにしてください。

    サーバが正常に機能するときにこの場所を見つけるには、455 ページの 「ロールフォワードログの保存先」を参照してください。ただしハードウェア障害などeDirectoryに影響する障害がサーバで発生すると、ロールフォワードログの場所を見ることができなくなります。
  - ロールフォワードログを保存しているディスクパーティション/ボリュームの空き容量を監視し、容量不足にならないようにしてください。

    容量不足のためロールフォワードログが作成できなくなると、eDirectoryは応答しなくなります。
  - ロールフォワードログの保存先にアクセスできるユーザを制限し、権利のないユーザがログを参照できないようにしてください。
  - 復元が必要となったときは、復元処理の終了後、そのサーバのロールフォワードログ設定をやり直してください。復元処理の過程で、設定が初期状態に戻るためです。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。
- ❒ NICIを使用する場合、eDirectoryがDIBを開き、暗号化されたデータを読み込むのに同じNICIファイルが必要となるため、eDirectoryのバックアップにNICIセキュリティファイルが含まれていることを確認します。

  詳細については、『NICI Administration Guide』の「Backing Up and Restoring NICI」を参照してください。

- ❒ 複数サーバ構成のツリーの場合、バックアップ処理にバックアップツールを使うためには、レプリカを共有するサーバすべてをeDirectory 8.5以降にアップグレードする必要があります。

  8.5より前のeDirectoryとは、復元後の検証処理の互換性がないためです。復元検証処理の詳細については、445 ページの 「バックアップツールによる復元作業の概要」を参照してください。

- ❒ 定期的にバックアップログを調べて、無人でのバックアップが正常に実行されていることを確認してください。

- ❒ ロールフォワードログディレクトリから古いログファイルを削除します。

- ❒ サーバをアップグレードする際は、「563 ページの 「ハードウェアのアップグレードやサーバの交換」」を参照してコールドバックアップを取ってください。

- ❒ 複数サーバ構成のツリーでは、障害対策のため、すべてのeDirectoryパーティションについて、複数台のサーバにレプリカが作成されていることを確認します。

  パーティションのレプリカを作成しておけば、保守作業などのためサーバを停止している間もオブジェクトにアクセスできるばかりでなく、ハードウェア障害などでサーバが使えなくなった場合に備える障害対策としても役立ちます。逆に複数サーバ構成のツリーで複製されていないパーティションを保持するサーバがあると、障害時にそのパーティションを復元できない恐れがあります。一番良いのは、すべてのパーティションが複製されることを確認することです。複数サーバ構成のツリー内にレプリカを作成していないパーティションがある場合の問題点の詳細については、「バックアップツールによる復元作業の概要, ロールフォワードログを使用する」および「復元後の検証処理に失敗した場合の対処方法」を参照してください。

  レプリカの作成については、「61 ページの 「レプリカ」」および「151ページの第6章「パーティションおよびレプリカの管理」」を参照してください。

- ❒ eDirectoryおよび関連ファイルのバックアップを収めたテープは、安全な場所に保管するようにしてください。

- ❒ バックアップ計画が適切であるか、定期的に検証するようにしてください。

- ❒ (オプション)コールドバックアップ(データベースをクローズしてフルバックアップを取る作業)や高度なバックアップ/復元操作をリモート操作で実行する場合は、リモート側マシンにDSBKをインストールしてください。また、VPNを使用するなど、ファイアウォール越しにアクセスできるように設定する必要があります。

  iManagerを使用すればファイアウォールの外側からでも作業が可能ですが、コールドバックアップや高度な操作はサポートされていません。

  DSBKは、eDirectoryをインストールする際、同時にインストールされます。Sun JVM 1.3.1が動作するワークステーション上でも使えます。DSBKのインストールや設定の手順については、「460 ページの 「DSBKの使用」」を参照してください。

- ❒ (オプション)コールドバックアップ(データベースをクローズしてフルバックアップを取る作業)や高度なバックアップ/復元操作をリモート操作で実行する場合は、リモート側マシンにeMBoxをインストールしてください。また、ファイアウォールの背後に(VPNアクセスなど)アクセスを配置します。iManagerは、ファイアウォール外で、バックアップと復元タスクをリモートで実行しますが、コールドバックアップや高度なタスクはサポートしていません。

  iManagerを使用すればファイアウォールの外側からでも作業が可能ですが、コールドバックアップや高度な操作はサポートされていません。

  eMBoxは、eDirectoryをインストールする際、同時にインストールされます。Sun JVM 1.3.1が動作するワークステーション上でも使えます。eMBoxのインストールや設定の手順については、「594ページの 「eMBoxクライアントを使ったバックアップ/復元作業」」を参照してください。

災害により何台ものサーバが被害を受けた場合に備える準備

- ❒ 上述の対策はすべて実施してください。
- ❒ 複数サーバ構成のツリーであれば、障害対策のためにDSMASTERサーバを用意するようお勧めします。

  詳細については、451 ページの 「DSMASTERサーバによる災害対策」を参照してください。
- ❒ 災害からの復旧計画が適切であるか、定期的に検証するようにしてください。

バックアップサービスおよび復元サービスについて

eDirectoryバックアップツールについて

バックアップツールには、個々のサーバ単位で、稼動したままの状態で継続的にeDirectoryデータベースのバックアップを取る機能があります。データベースを停止することなく、処理を始めた時点のバックアップを取ることができます。つまり、バックアップ作業はいつでも可能であり、その間もeDirectoryを使い続けることができます

注: 特に指示しなければこの「ホット」バックアップになりますが、必要であればデータベースを停止して「コールド」バックアップを取ることもできます。

また、ロールフォワードログを有効にすれば、最後にバックアップを取った時点以降のトランザクションをすべて記録しておけます。これを使えば、サーバが停止する直前の状態に復元することもできます。さらに、レプリカリングに属するサーバすべてについてロールフォワードログを取る必要があります。これにより、他のサーバとの同期状態も復元できます。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないことになります。ロールフォワードログの機能は、デフォルトでは無効になっています。詳細については、453 ページの 「ロールフォワードログを使用する」を参照してください。

バックアップツールはeDirectoryのオブジェクトをすべて一度にバックアップできるわけではありません。各サーバのパーティションをバックアップするだけです。この方式は、特定のサーバのみを復元する場合に優れているばかりでなく、TSA for NDS®バックアップを使う旧式の方法に比べて高速です。ただし、eDirectory 8.6のマニュアルにも記載されているように、TSA for NDSは今でも使用できます。必要に応じてTSA for NDSと新しいバックアップを使い分けられます。動作の違いについては、「444ページの「DSBKのバックアップおよび復元とTSAforNDSバックアップの違い」」を参照してください。

eDirectoryバックアップツールは、ファイルシステムバックアップ機能と組み合わせて使用して、eDirectoryバックアップファイルをテープに安全に保存する必要があります。NetIQはバックアップ用製品を開発している主要企業と提携しています。詳細については、NetIQ eDirectory Partner Products (http://www.novell.com/partnerguide/section/466.html)を参照してください。

バックアップツールで作成されるバックアップファイルやログファイルの形式については、「450 ページの 「バックアップログファイルの書式」」および「446 ページの 「バックアップファイルのヘッダ書式」」を参照してください。

DSBKのバックアップおよび復元とTSAforNDSバックアップの違い

eDirectoryの以前のバージョンでは、バックアップ/復元ツールは、ツリーをオブジェクト単位でバックアップする方式を使用していました。

eDirectory 8.7で組み込まれたバックアップツールは、方式やアーキテクチャが一新されています。ツリーではなくサーバを基準とし、個々のサーバのeDirectoryデータベースをバックアップします。この変更により、以前のTSA for NDSバックアップよりも大幅に速くなりました。

TSAforNDSは今でも使用できますが、今後は新しいバックアップツールを使うようお勧めします。

新旧バックアップツールの違いを次の表に示します。

項目	TSA for NDSによる以前のバックアップ	バックアップツールによる「ホットバックアップ」
バックアップの対象	ツリー全体をオブジェクト単位でバックアップ。	サーバ単位でeDirectoryデータベースをバックアップ。 ツリー全体の耐障害性は主としてレプリカ作成機能で確保していますが、サーバ単位のバックアップ機能によりさらに強固になります。 災害などで何台ものサーバが停止した場合でもツリーを復元できるようにするためには、DSMASTERサーバを導入し、それに応じたレプリカ作成方針を立てる必要があります。「45ページの 「DSMASTERサーバによる災害対策」」を参照してください。
Speed	N/A	大幅に改善されています。新しいバックアップの機能では処理性能を最重視しました。
バックアップファイルの保存先	直接テープに書き出し可。	ファイルシステム上のバックアップファイルとして書き出し。 別途ファイルシステムのバックアップツールを使って、テープに書き出す必要があります。
プラットフォーム間の違い	プラットフォームによって使い方が別々。	どのプラットフォームでも同じ使い方。

項目	TSA for NDSによる以前のバックアップ	バックアップツールによる「ホットバックアップ」
個々のサーバ単位での復元	考慮されていません。	ハードディスクが障害した後にサーバ単位で復元することができます。サーバを別のマシンに移行する際にもバックアップを利用できます。 ロールフォワードログを使えば、停止直前の状態に復元することも可能です。これにより、レプリカリングに属する他のサーバと同期状態を揃えることができます。 eDirectoryの関連ファイルもバックアップの対象とすることができます。たとえばNICIファイルのバックアップと復元ができます。独自の関連ファイルリストを作成して、対象ファイルをバックアップに追加することもできます。
NICIファイルのバックアップ/復元	考慮されていません。	NICIファイルのバックアップ/復元も可能です。これにより、復元後、暗号化データにアクセスできます。復元作業の時間を大幅に短縮できるでしょう。
個々のサーバのロールフォワードログ	考慮されていません。	最後にバックアップを取った時点以降のトランザクションを、ロールフォワードログとしてすべて記録しておけます。これを使うと、停止直前の状態にまで復元することができます。複数サーバ環境では、これを使用して他のサーバと同期状態を揃えることができます。ロールフォワードログの機能は、デフォルトでは無効になっています。詳細については、453 ページの 「ロールフォワードログを使用する」を参照してください。

バックアップツールによる復元作業の概要

復元作業に先立ち、バックアップファイルをすべて揃えておく必要があります。その手順については「457 ページの 「復元処理の準備」」を参照してください。iManagerやDSBKからバックアップツールの復元機能を呼び出すと、バックアップツールで次のような処理が行われます。

1. DSエージェントをクローズします。
2. アクティブなDIB(Data Information Base)セットを、NDSからRSTに切り替えます。

   注: 既存のNDSデータベースはそのままサーバに残り、復元後の検証に失敗した場合は、再びこれがアクティブなDIBセットになります。
3. 復元処理が始まります。新たにRSTというDIBセットを作り、そこに復元します。
4. DIBセットをいったん無効にします。

   擬似サーバのログイン無効属性をオンにします。これは、このDIBセットを使ってDSエージェントがオープンされるのを避けるための措置です。
5. ロールフォワードログに関する設定をデフォルトに戻します。これを防ぐには、-sスイッチを使用します。

したがって、復元後はロールフォワードログを書き出さない設定になります。書き出し先ファイル名の設定もデフォルトに戻ります。

注: このサーバでロールフォワードログ記録を使うためには、復元後に改めて有効に切り替え、障害対策のための書き出し先も設定し直して、ロールフォワードログ記録の環境設定を再作成する必要があります。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

---

6. 復元されたRSTデータベースの検証処理を行います。

   復元されたデータの整合性を確認します。この確認は、レプリカを共有しているすべてのサーバにアクセスし、遷移ベクトルを比較して実行されます。

   検証結果はログファイルに出力されます。

   リモートサーバの遷移ベクトルの方がローカルベクトルより後の時間に作成されたものである場合は、復元されなかったデータがあるということなので、検証処理は失敗します。

   いずれかのレプリカが検証に失敗した場合、ログファイルに記録される情報の例を示します。比較された遷移ベクトルがわかります。

   ```
   Server: \T=LONE_RANGER\O=novell\CN=CHIP
      Replica: \T=LONE_RANGER\O=novell
         Status: ERROR = -6034
            Local TV             Remote TV
            s3D35F377 r02 e002   s3D35F3C4 r02 e002
            s3D35F370 r01 e001   s3D35F370 r01 e001
            s3D35F363 r03 e001   s3D35F363 r03 e001
            s3D35F31E r04 e004   s3D35F372 r04 e002
            s3D35F2EE r05 e001   s3D35F2EE r05 e001
            s3D35F365 r06 e003   s3D35F365 r06 e003
   ```

   詳細については、452 ページの 「遷移ベクトルと復元後の検証処理」を参照してください。

7. 検証に成功した場合は、RSTをNDSと改名し、ログイン無効属性をオフにします。したがってこれがサーバでアクティブなeDirectoryデータベースになります。失敗した場合は改名しないので、元のNDSが再びアクティブなDIBセットになります。

   検証に失敗した場合の復旧方法については、「478 ページの 「復元後の検証処理に失敗した場合の対処方法」」を参照してください。

注: 「高度な復元オプション」を使えば、強制的にRSTデータベースをアクティブにし、ロックを解除することもできますが、NetIQサポート部門の指示がない場合はお勧めできません。

バックアップファイルのヘッダ書式

バックアップファイルのヘッダには、次のような重要な情報が記録されています。

- バックアップファイルが作成された時点のファイル名。

  バックアップ作成後にファイル名を変更した場合にはこの情報が有用になります。

- バックアップ時点のロールフォワードログ名。

  1回分のフルバックアップと3回分のインクリメンタルバックアップがあって、最後のインクリメンタルバックアップから復元しているような場合に役立ちます。完全に復元するために必要な最初のロールフォワードログを知ることができます。

- このサーバが保持しているレプリカのリスト。

各レプリカをどのサーバに配置しているか記録していない場合に役立ちます。災害で何台ものサーバが停止した場合、バックアップファイルのヘッダに表示されたこの情報を見れば、最初にどのサーバを復元するべきか判断できます。

- 同時にバックアップするようユーザのインクルードファイルに指定された関連ファイル名。
- 複数のファイルに分割してバックアップする場合のファイル数。

各バックアップファイルのヘッダはXML形式で記述されます。ヘッダ部に続き、データベース内のデータを、バイナリ形式で記録します

注: ファイルの末尾にバイナリデータがあると構文解析でエラーが発生しますが、XMLヘッダはXML標準に適合しています。

バックアップが複数のファイルに分かれる場合、各ファイルに同じヘッダ情報を記録します。

警告: バックアップファイルを開くときは、ヘッダを確認するだけにしてください。ファイルを保存または変更しようとすると、ファイルの一部が切り捨てられる場合があります。ほとんどのアプリケーションがバイナリデータを正しく保存することができません。

XMLヘッダのDTDを次に示しますこのDTDは参照のため、バックアップファイルのヘッダの一部として書き込まれます。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<!DOCTYPE backup [
<!ELEMENT backup (file|replica)*>
<!ELEMENT file (#PCDATA)>
<!ELEMENT replica EMPTY>
<!ATTLIST backup version CDATA #REQUIRED
    backup_type (full|incremental) #REQUIRED
    idtag CDATA #REQUIRED
    time CDATA #REQUIRED
    srvname CDATA #REQUIRED
    dsversion CDATA #REQUIRED
    compression CDATA "none"
    os CDATA #REQUIRED
    current_log CDATA #REQUIRED
    number_of_files CDATA #IMPLIED
    backup_file CDATA #REQUIRED
    incremental_file_ID CDATA #IMPLIED
    next_inc_file_ID CDATA #IMPLIED>
<!ATTLIST file size CDATA #REQUIRED
    name CDATA #REQUIRED
    encoding CDATA "base64"
    type (user|nici) #REQUIRED>
<!ATTLIST replica partition_DN CDATA #REQUIRED
    modification_time CDATA #REQUIRED
    replica_type (MASTER|SECONDARY|READONLY|SUBREF|
    SPARSE_WRITE|SPARSE_READ|Unknown) #REQUIRED
    replica_state (ON|NEW_REPLICA|DYING_REPLICA|LOCKED|
    CRT_0|CRT_1|TRANSITION_ON|DEAD_REPLICA|
    BEGIN_ADD|MASTER_START|MASTER_DONE|
    FEDERATED|SS_0|SS_1|JS_0|JS_1|MS_0|MS_1|
    Unknown) #REQUIRED>
]>
```

DTDに含まれる属性について次の表で説明します。

属性	説明
backup version	バックアップツールのバージョン。
backup backup_type	フルバックアップかインクリメンタルバックアップかの別コールドバックアップはフルバックアップとして扱います。
backup idtag	バックアップ時刻に基づいて生成されたGUID。バックアップファイル名が変わっていても、これを使えばバックアップを識別できます。
backup time	バックアップ処理の開始日時。
backup srvname	バックアップ対象サーバの識別名。
backup dsversion	サーバ上で稼動しているeDirectoryのバージョン。
backup compression	バックアップツールがバックアップデータを圧縮したかどうか。これはバックアップデータのみに適用されます。ヘッダ自体が圧縮されることはありません。
backup os	バックアップ処理を実行したオペレーティングシステム。復元はこれと同じオペレーティングシステムのみで行うようお勧めします。
backup current_log	復元に必要な最初のロールフォワードログ。これは復元用の複数の正しいファイルを収集するのに役立ちます。
backup number_of_files	分割してバックアップする場合のファイル数。ひとつ目のバックアップファイルにのみ記録されます。
backup backup_file	このバックアップファイル名。 複数のファイルに分けてバックアップする場合、各ファイル名には順序番号がつきますが、それも含むファイル名が記録されます。複数のバックアップファイルのファイル名の例は、「-s *file_size*」を参照してください。
backup incremental_file_ID	インクリメンタルバックアップの場合、そのファイルのID。
backup next_inc_file_ID	これに続くインクリメンタルバックアップに与えるID。正しく復元するために必要な情報です。
ファイルサイズ	このファイルの<file>タグ間にあるデータ長。
file name	バックアップファイル名およびその保存先。
file encoding	ファイルのエンコードに使ったアルゴリズム。
file type	これがNICIファイルか、それ以外にユーザが指定したファイルかの別。
password	NICIバックアップのパスワードを指定します。NICIファイルを復元するためには同じパスワードを指定する必要があります。
replica partition_DN	パーティションの識別名。 各レプリカをどのサーバに配置しているか記録していない場合に役立ちます。災害で何台ものサーバが停止した場合、バックアップファイルのヘッダに表示されたこの情報を見れば、最初にどのサーバを復元するべきか判断できます。
replica modification_time	バックアップ時点の、このレプリカの遷移ベクトル。
replica replica_type	レプリカの種別。マスタ、読み込み専用など。

属性	説明
replica_state	バックアップ時点でのレプリカの状態。「On」、「New Replica」など。

バックアップファイルのヘッダ例を次に示します。これはWindowsサーバで作成したもので、NICIセキュリティファイルもバックアップ対象になっています。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<!DOCTYPE backup [
<!ELEMENT backup (file|replica)*>
<!ELEMENT file (#PCDATA)>
<!ELEMENT replica EMPTY>
<!ATTLIST backup version CDATA #REQUIRED
    backup_type (full|incremental) #REQUIRED
    idtag CDATA #REQUIRED
    time CDATA #REQUIRED
    srvname CDATA #REQUIRED
    dsversion CDATA #REQUIRED
    compression CDATA "none"
    os CDATA #REQUIRED
    current_log CDATA #REQUIRED
    number_of_files CDATA #IMPLIED
    backup_file CDATA #REQUIRED
    incremental_file_ID CDATA #IMPLIED
    next_inc_file_ID CDATA #IMPLIED>
<!ATTLIST file size CDATA #REQUIRED
    name CDATA #REQUIRED
    encoding CDATA "base64"
    type (user|nici) #REQUIRED>
<!ATTLIST replica partition_DN CDATA #REQUIRED
    modification_time CDATA #REQUIRED
    replica_type (MASTER|SECONDARY|READONLY|SUBREF|
    SPARSE_WRITE|SPARSE_READ|Unknown) #REQUIRED
    replica_state (ON|NEW_REPLICA|DYING_REPLICA|LOCKED|
    CRT_0|CRT_1|TRANSITION_ON|DEAD_REPLICA|
    BEGIN_ADD|MASTER_START|MASTER_DONE|
    FEDERATED|SS_0|SS_1|JS_0|JS_1|MS_0|MS_1|
    Unknown) #REQUIRED>
]>

<backup version="2" backup_type="full" idtag="3D611DA2" time="2002-8-19'T10:32:35"
srvname="\T=MY_TREE\O=novell\CN=DSUTIL-DELL-NDS" dsversion="1041081"
compression="none" os="windows" current_log="00000003.log" next_inc_file_ID="2"
number_of_files="0000001" backup_file="c:\backup\header.bak"><replica
partition_DN="\T=MY_TREE" modification_time="s3D611D95_r1_e2"
replica_type="MASTER" replica_state="ON" /><replica
partition_DN="\T=MY_TREE\O=part1" modification_time="s3D611D95_r1_e2"
replica_type="MASTER" replica_state="ON" /><replica
partition_DN="\T=MY_TREE\O=part2" modification_time="s3D611D95_r1_e2"
replica_type="MASTER" replica_state="ON" /><replica
partition_DN="\T=MY_TREE\O=part3" modification_time="s3D611D96_r1_e2"
replica_type="MASTER" replica_state="ON" /><file size="190"
name="C:\WINDOWS\system32\novell\nici\bhawkins\XARCHIVE.001" encoding="base64"
type="nici">the data is included here</file>

<file size="4228" name="C:\WINDOWS\system32\novell\nici\bhawkins\XMGRCFG.KS2"
encoding="base64" type="nici">the data is included here</file>

<file size="168" name="C:\WINDOWS\system32\novell\nici\bhawkins\XMGRCFG.KS3"
```

```
encoding="base64" type="nici">the data is included here</file>

<file size="aaac" name="C:\WINDOWS\system32\novell\nici\nicintacl.exe"
encoding="base64" type="nici">the data is included here</file>

<file size="150" name="C:\WINDOWS\system32\novell\nici\NICISDI.KEY"
encoding="base64" type="nici">the data is included here
</file>

<file size="4228" name="C:\WINDOWS\system32\novell\nici\system\Xmgrcfg.ks2"
encoding="base64" type="nici">the data is included here
</file>

<file size="168" name="C:\WINDOWS\system32\novell\nici\system\Xmgrcfg.ks3"
encoding="base64" type="nici">the data is included here
</file>

<file size="1414" name="C:\WINDOWS\system32\novell\nici\xmgrcfg.wks"
encoding="base64" type="nici">the data is included here
</file>

</backup>
```

ヘッダ部に続き、データベースのバックアップデータをバイナリ形式で格納します。

バックアップログファイルの書式

eDirectoryバックアップツールは、前回までのバックアップを含め、処理内容を細かく記録したログを残すようになっています。このログファイルにはすべてのバックアップ履歴、バックアップの開始および終了時刻、およびバックアッププロセス中に発生した考えられるエラーについての情報が含まれます。前回までのログに追記する形で記録します。書き出し先を別途指定することもできます。

無人バックアップが正常に実行されているか確認するためにも、このログは重要です。最終行を見ると、成功か失敗かの区別およびエラーコードがわかります。

バックアップツールのログファイルには、過去のバックアップ処理のIDも記録されています。これは復元に必要なフルバックアップ、インクリメンタルバックアップのファイルを間違いなく揃えるために役立ちます。先頭の4行は、バックアップファイルのヘッダ情報をそのまま複写したものです。

また、同時にバックアップしたファイル名も記録します。NICIファイルや、インクルードファイルでユーザが指定したファイルがこれに当たります。

復元処理の際は、実際に復元されたファイルを記録します。

ログファイルの出力例を次に2つ示します。

```
|==================DSBackup Log: Backup================|
Backup type: Full
Log file name: sys:/backup/backup.log
Backup started: 2002-6-21'T19:53:5GMT
Backup file name: sys:/backup/backup.bak
Server name: \T=VIRTUALNW_TREE\O=novell\CN=VIRTUALNW
Current Roll Forward Log: 00000001.log
DS Version: 1041072
Backup ID: 3D138421
Backing up security file: sys:/system/nici/INITNICI.LOG
Backing up security file: sys:/system/nici/NICISDI.KEY
Backing up security file: sys:/system/nici/XARCHIVE.000
Backing up security file: sys:/system/nici/XARCHIVE.001
Backing up security file: sys:/system/nici/XMGRCFG.KS2
Backing up security file: sys:/system/nici/XMGRCFG.KS3
Backing up security file: sys:/system/nici/XMGRCFG.NIF
Starting database backup...
Database backup finished
Completion time 00:00:03
Backup completed successfully

|==================DSBackup Log: Restore================|
Log file name: sys:/save/doc.log
Restore started: 2002-7-19'T19:1:34GMT
Restore file name: sys:/backup/backup.bak
Starting database restore...
Restoring file sys:/backup/backup.bak
Restoring file sys:/system/nici/INITNICI.LOG
Restoring file sys:/system/nici/NICISDI.KEY
Restoring file sys:/system/nici/XARCHIVE.000
Restoring file sys:/system/nici/XARCHIVE.001
Restoring file sys:/system/nici/XMGRCFG.KS2
Restoring file sys:/system/nici/XMGRCFG.KS3
Restoring file sys:/system/nici/XMGRCFG.NIF
Database restore finished
Completion time 00:00:15
Restore completed successfully
```

DSMASTERサーバによる災害対策

複数サーバ環境で、サーバがすべて失われてしまうような災害にも備えるためには、ツリーの一部としてDSMASTERサーバを導入することを検討してください。

バックアップツールは、各サーバを個別にバックアップするために使用されます。これはツリーではなくサーバを単位とします。ただし、DSMASTERサーバを作成しておけば、バックアップツールでも、ツリー構造全体をバックアップできるようになります。運用例の概要については、「486ページの 「シナリオ: 複数サーバ構成のネットワークで、すべてのサーバが使えなくなった場合」」を参照してください。

災害からの復旧で問題となるのは、同じパーティションのレプリカが複数あって、互いに整合性が取れていない場合の対処方法です。災害によってロールフォワードログも失われている場合、すべてのサーバを同じ時点の状態に復元することはできません。バックアップされたレプリカはサーバごとに異なる時点のものなので、ロールフォワードログを使わずに単純に復元しただけでは、全体をツリーとしてまとめる際に問題が起こるためです。

注: 復元検証処理はこのような問題を防ぐためのものです。デフォルトでは、他のレプリカとの不整合が見つかると、eDirectoryデータベースが復元後にオープンになりません。

DSMASTERサーバを導入すればこのような事態に備えることができます。ツリー全体のマスタコピーを作成しておき、これを復元の基準点として使用します。

DSMASTERサーバを導入する手順を次に示します。

- ある1台のサーバに、ツリーに属するパーティションすべてのレプリカを保持するよう設定してください。これにより、ツリー全体のコピーが、特定のサーバのeDirectoryデータベース中に作られるようになります。ただし、ツリーの容量が大きい場合は、複数台のキーサーバに分けても構いません。これをDSMASTERサーバと呼びます。DSMASTERサーバに作るレプリカは、マスタまたは読み書き用と設定してください。

  注: 複数台のキーDSMASTERサーバに分割する場合は、同じパーティションのレプリカが2台以上に作られることのないようにしてください。重複のない構成にしておけば、災害後の復元作業において、レプリカ間に不整合が生じることはありません。

  災害から復旧する際に、最新のロールフォワードログは使えません。このログは各サーバのローカルファイルとして保存されるためです。したがって、複数台のDSMASTERサーバを、すべて同じ時点の状態に戻すことはできない場合があります。2台のDSMASTERサーバに同じレプリカがあれば、これが一致せず、ツリーに不整合が生じる恐れがあります。そのため、障害復旧としては、同じパーティションのレプリカを複数のDSMASTERサーバに作成することは避ける必要があります。

  レプリカ全般については、「61 ページの 「レプリカ」」を参照してください。

- DSMASTERサーバを定期的にバックアップして、ツリー全体のバックアップコピーを作成してください。災害対策としては、DSMASTERサーバのバックアップ以外にも、充分な予防措置を講じておくとよいでしょう。

以上のようにツリーを設計しておくと、災害が起こっても、迅速にツリー構造を再構築し、稼動させることができます。1台だけのサーバ(あるいは少数のキーサーバ)のみを復元し、これをマスタレプリカとして扱うようにすればよいのです。

このツリーが稼動し始めてから、フル/インクリメンタルバックアップファイルを使用して、DSMASTER以外のサーバも順次復元していきます。ロールフォワードログがないため、これらの他のサーバで復元処理の検証が失敗します。そこで、レプリカリングからいったん外し、DSRepairを使って、すべてのレプリカ情報を外部参照に変更します。その後、DSMASTERサーバ上のコピーからレプリカを作成して、改めてサーバにレプリカを追加します。この手順については、「478ページの「復元後の検証処理に失敗した場合の対処方法」」に記載されています。

災害により一部のサーバが失われた場合、操作手順はやや複雑になりますので、NetIQサポート部門に連絡してください。

遷移ベクトルと復元後の検証処理

遷移ベクトルとは、レプリカのタイムスタンプのことです。レプリカ作成時刻を1970年1月1日からの経過秒数で表したものと、レプリカ番号、および現在のイベント番号を組にして表示されます。ここで例を示します。

```
s3D35F377 r02 e002
```

バックアップと復元のコンテキストでは、復元されたサーバが参加しているレプリカリング内で正しく同期していることを確認するために遷移ベクトルが使用されます。

同じパーティションのレプリカを保持するサーバは、レプリカの同期を取るため、互いにデータをやり取りしています。サーバはレプリカリング内の他のサーバと通信するたびに、他のサーバの遷移ベクトルを記録しています。遷移ベクトルを使用すると、レプリカリング内の各レプリカが同期を保つためには、どのデータを送ればよいか、サーバが常に把握できます。サーバが停止するとこの通信が止まり、再び通信できるようになるまでの間、他のサーバはそのサーバに関して遷移ベクトルの更新や変更を記録しますが、送信しません。

あるサーバのeDirectoryを復元した後、検証処理として、復元された遷移ベクトルをレプリカリングに属する他のサーバと比較します。これは、復元されたレプリカが他のサーバと同期の取れた状態であるかどうか確認するために実行されます。

リモートサーバの遷移ベクトルの方がローカルベクトルより後の時間に作成されたものである場合は、復元されなかったデータがあるということなので、検証処理は失敗します。これは、前回のフルバックアップまたはインクリメンタルバックアップの前に継続的なロールフォワードログ記録を有効にしていなかった、ロールフォワードログを復元に含めなかった、または復元で指定したロールフォワードログがすべて揃っていなかった、などの理由でデータが不足していることが考えられます。

デフォルトでは、復元したeDirectoryデータベースが他のレプリカと整合が取れていない場合、そのままではオープンできません。

遷移ベクトルに不整合があるログファイルエントリの例については、「445ページの「バックアップツールによる復元作業の概要」」を参照してください。

検証に失敗した場合の対処方法については、「478ページの「復元後の検証処理に失敗した場合の対処方法」」を参照してください。

ロールフォワードログを使用する

ロールフォワードログとは、他のデータベース製品でいう「ジャーナル」に相当する機能です。ロールフォワードログ(RFL)は、データベースの変更をすべて記録したものです。

ロールフォワードログを使用する利点は、最後のフル/インクリメンタルバックアップ以降の変更履歴が得られるため、障害で停止する直前の状態にまでeDirectoryを復元できることです。ロールフォワードログを使用しないと、最後のフル/インクリメンタルバックアップを取った時点までしかeDirectoryを復元できません。

eDirectoryは、トランザクションをデータベースに反映する前に、その操作内容をログファイルに記録するようになっています。デフォルトでは、ログファイルはディスク容量の節約のために次々に重ね書きされるようになっているため、eDirectoryの変更履歴は残りません。

継続的にロールフォワードログを取る設定にすると、変更履歴が連続したロールフォワードログファイルに保存されます。ロールフォワードログ記録はサーバの性能には影響がありません。eDirectoryがすでに作成しているログファイルのエントリを単に保存するだけです。

レプリカリングに属するサーバは、ロールフォワードログ機能を有効にしておく必要があります。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないことになります。他のサーバとレプリカを共有するデータベースは、停止直前の状態にまで復元しない限りデフォルトではオープンされません。ロールフォワードログがない場合は、「478ページの「復元後の検証処理に失敗した場合の対処方法」」で説明されている別の手順で復旧してください。

ロールフォワードログの機能は、デフォルトでは無効になっています。サーバで必要に応じて有効に切り替えてください。ロールフォワードログは、サーバの復元作業を実行すると再び無効になり、設定がデフォルトに戻ります。このため復元後に再び有効にし、設定を再作成した上で、改めてフルバックアップを取ってください。

注: フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

単一サーバ環境ではロールフォワードログがなくても構いません。しかしロールフォワードログがあれば、最後のバックアップ時ではなくシステム停止直前の状態に復元できます。

ロールフォワードログをオンにする場合、ディスクの空き容量は常に監視している必要があります。詳細については、456 ページの 「ロールフォワードログのバックアップと削除」を参照してください。

この節では、次の項目について説明します。

ロールフォワードログ記録の切り替えや設定には、iManagerまたはDSBKを使います。604ページの「iManagerによるロールフォワードログの設定」または465ページの「DSBKによるロールフォワードログの設定」を参照してください。

ロールフォワードログ機能を使用する上での注意事項

継続的にロールフォワードログ機能を使用する場合、次のような点に注意してください。

- **バックアップ処理の実行前にロールフォワードログ機能を有効にしておかないと、** データベースの復元に利用することはできません。
- **障害に備えるため、eDirectoryとは別の記憶デバイスにロールフォワードログを保存するようにしてください。** セキュリティを考慮すれば、ログへのアクセス権も制限する必要があります。詳細については、455 ページの 「ロールフォワードログの保存先」を参照してください。
- **ロールフォワードログの保存先を文書に記録しておいてください。** 詳細については、455 ページの 「ロールフォワードログの保存先」を参照してください。
- **ログの保存先のディスクの空き容量を常に監視している必要があります。** 詳細については、456 ページの 「ロールフォワードログのバックアップと削除」を参照してください。
- **ロールフォワードログ機能が無効になっていたり、ログファイルを損失した場合は、有効に切り替えた後、改めてフルバックアップを取ってください。** そうしなければ完全に復元できなくなる恐れがあります。次のような状況の場合に必要です。
  - 復元処理の直後。復元処理の過程で、ロールフォワードログ機能は無効になり、設定もデフォルト値に戻ってしまいます。
  - デバイス障害などにより、ロールフォワードログを保存しているディレクトリを損失した場合。
  - 意図せずにロールフォワードログ機能を無効にしてしまった場合。

- **ストリームファイルのログ機能を有効にすると、ディスクの空き容量が急速に減少します。**

  ストリームファイル(ログインスクリプトなど)のログ出力を有効にすると、変更があるたびに、ストリームファイル全体がロールフォワードログに複写されるためです。ストリームファイルのログ出力を無効にし、フル/インクリメンタルバックアップの際にのみストリームファイルをバックアップすると、ログファイルが大きくなるのを遅らせられます。

- **データベースの復元で最も時間を要するのは、ロールフォワードログを参照する処理です。**

  ロールフォワードログの容量は、ツリー構造に対して施された更新の回数に応じて増え、ストリームファイル(ログインスクリプトなど)のログ出力を有効にするとさらに増えます。

  データベースが頻繁に更新されるようであれば、バックアップの頻度を上げることも検討するとよいでしょう。こうすると、復元処理の過程でロールフォワードログを参照する処理が少なくなります。

- **ロールフォワードログファイルの名前を変更しないでください。** ログが作成されたときとファイル名が異なる場合、そのログファイルを復元に使用することはできません。
- **eDirectoryを削除するとロールフォワードログもすべて消えてしまいます。** いったんデータベースを削除した後、ログファイルを使って復元するのであれば、eDirectoryを削除する前に、別の場所にコピーしておいてください。
- **復元が必要な場合は、復元処理の終了後にそのサーバのロールフォワードログ設定を再作成してください。** この機能を有効にし、ログの保存先を安全な場所に設定します。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

  この手順が必要となるのは、復元処理の過程で、ロールフォワードログに関する設定はデフォルトに戻るためです。つまり、ロールフォワードログ機能は無効となり、保存先もデフォルトの場所になるからです。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

ロールフォワードログの保存先

ロールフォワードログ機能を有効にした場合、その保存先を、eDirectoryとは別の記憶デバイスに変更します。

保存先を設定する上で、次の点に注意してください。

- **デフォルトの場所のままにせず、必ずeDirectoryとは別のストレージデバイス上に配置してください。** こうしておけば、デバイス障害のためにeDirectoryが失われても、復元のためにロールフォワードログにアクセスできます。

  サーバにストレージデバイスが1つしかない場合、デバイス障害が起こると、ロールフォワードログではeDirectoryの耐障害性は保たれません。この機能はロールフォワードログを使用しないでおく方法もあります。

  ロールフォワードログの保存先を変更するには、iManagerのバックアップ環境設定画面、またはDSBKのsetconfigコマンドを使用してください。ロールフォワードログはサーバ上のローカルファイルとして保存する必要があります。

- **保存先を記録してください。** ロールフォワードログの保存先を記録して、サーバのデータベースの復元が必要なときに見つけられるようにしてください。これはサーバが正常で障害が発生する前に実行することが重要です。

  サーバが正常に動作していれば、iManagerのバックアップ環境設定画面、またはDSBKのbackup getconfigオプションで調べることができます。ただし、ハードウェア障害などでeDirectoryが使えない状態になると、この方法でロールフォワードログの場所を調べることはできません。

サーバに障害が発生し、それを復元する場合は、eDirectoryを新たにインストールすると、ロールフォワードログの保存先設定はデフォルトの場所に戻ります。このため、復元作業のためにeDirectoryを再インストールしたとしても、サーバの停止前にロールフォワードログをどこに保存していたか、eDirectoryで調べることはできません。その場合は記録を参照して位置を調べる必要があります。

ロールフォワードログの保存先設定は、_ndsdb.iniファイルにも記録されています。ただし、eDirectoryと同じディスクパーティション/ボリュームにあるため、eDirectoryがあるストレージデバイスに障害が起これば、ログの保存先を調べるために_ndsdb.iniファイルを使用することはできません。

- **ロールフォワードログの保存先へのアクセス権を制限してください。** これはセキュリティ上の問題です。見ただけで中身がわかるような形式にはなっていませんが、デコードは可能なため、重要なデータが漏洩する恐れがあります。
- **ディスクの空き容量が充分かどうか、常に監視している必要があります。** 詳細については、456 ページの 「ロールフォワードログのバックアップと削除」を参照してください。
- **ロールフォワードログ専用のディスクパーティション/ボリュームを用意するのが最善です。**

  こうしておけば、ディスク容量やアクセス権を監視しやすくなります。
- **ログの保存先パスのうち、一番深い階層のディレクトリ名はeDirectoryによって作成されます。** この名前は現在のeDirectoryデータベース名に基づいて決まります。

  たとえばログの保存先を「d\Novell\NDS\DIBFiles」と指定した場合、eDirectoryデータベース名が「NDS」であれば、実際の保存先ファイルは「d:\Novell\NDS\DIBFiles\nds.rfl」となります。データベースの名前をNDSからND1に変更した場合、ロールフォワードログのディレクトリはd:\Novell\NDS\DIBFiles\nd1.rflに変更されます。

  保存先の設定を変えるとその時点で新しいディレクトリができますが、ロールフォワードログはデータベースでトランザクションが発生するまで作成されません。
- **復元の際は、必要なロールフォワードログをすべて同じディレクトリに集めます。** 詳細については、457 ページの 「復元処理の準備」を参照してください。

ロールフォワードログのバックアップと削除

放置しておけばロールフォワードログは次々に蓄積され、ディスクパーティション/ボリュームがいっぱいになります。ディスク容量が不足してロールフォワードログを作成できない場合は、eDirectoryはそのサーバに対して応答しなくなります。定期的にログファイルをバックアップし、サーバからは削除するようにして、常に充分なディスク容量を確保するようお勧めします。

削除しても構わないロールフォワードログを判別し、バックアップを取った上で削除するには、次の手順に従います。

1 「最後に使用済みになった」ロールフォワードログ名を調べてください。

  最後の使用済みロールフォワードログの名前は、次のような方法で調べることができます。

  - iManagerで［**eDirectoryの保守**］>［**バックアップ環境設定**］の順にクリックし、表示されるファイル名を調べます。
  - DSBKでgetconfigbackupコマンドを実行します。手順については、465 ページの 「DSBKによるロールフォワードログの設定」を参照してください。

  「最後に使用済みになった」ロールフォワードログとは、トランザクション履歴の記録が終わり、今は書き出しをしていないログファイルのうち、最新のものを表します。データベースはこのファイルに対する書き込みを終えて、今は新しいログファイルで始めているため、オープ

ンしておく必要はもうありません。そのため、「最後に使用済みになった」ロールフォワードログと呼ばれます。一方、データベースがトランザクションを記録している現在のロールフォワードログは「使用中」で、データベースに必要なものです。

2 ファイルシステムのバックアップ機能を使って、ロールフォワードログをテープに保存してください。

3 「最後に使用済みになった」ものよりも古いロールフォワードログを削除してください。

警告: ロールフォワードログを削除する際にはより注意を払い、削除しようとするファイルが確実にバックアップされているか、繰り返し確認してください。

「最後に使用済みになった」ロールフォワードログとは、データベースが記録を完了しクローズにしたファイルを指します。サーバからこのファイルを削除しても構わないという意味ではありません。まだテープにバックアップしていないファイルは削除しないようにしてください。

テープに保存してあるロールフォワードログを復元のために使う場合は、次の点に注意してください。

- 復元に使用する他のロールフォワードログと同様に、ファイルシステムをバックアップしたテープから取得したログファイルは、他のログと合わせてひとつのフォルダに集めてください。このフォルダは、サーバからローカルにアクセスできる必要があります。
- テープおよびサーバに複製されたファイルのタイムスタンプを比較する必要があります。タイムスタンプに違いがある場合は、最新のサーバ上のファイルを使います。たとえば、ファイルシステムのバックアップ中にデータベースで使用されていたロールフォワードログファイルは、テープでは不完全になります。最新の完全なファイルはサーバに格納されています。

注意: eDirectoryを削除するとロールフォワードログも削除される問題

サーバからeDirectoryを削除すると、ロールフォワードログのディレクトリおよびその中身もすべて削除されます。いったんデータベースを削除した後、ログファイルを使って復元するのであれば、eDirectoryを削除する前に、別の場所にコピーしておいてください。

復元処理の準備

eDirectoryデータベースの復元作業で最も大切なのは、復元が完全に行われたかどうか確認することです。作業に先立ち、「457ページの「復元作業の前提条件」」の説明に従って、必要な準備を行います。必要なバックアップファイルを揃える手順については、「458ページの「復元に必要なバックアップファイルの収集」」を参照してください。

復元作業の前提条件

❒ 復元するサーバとレプリカを共有しているサーバはすべて、稼動状態で、通信できるようにしておかなければなりません。これは、復元後の検証処理で、同じレプリカリングに属するサーバ間の整合性を確認するために必要です。

❒ 必要な次のバックアップファイルをすべて収集してください。

- フルバックアップおよびそれ以降のインクリメンタルバックアップのファイルを、復元するサーバの、1つのディレクトリ内に集めます。

- 最後にバックアップを取って以降のロールフォワードログをすべて、同じサーバ上のもう1つのディレクトリにまとめておきます。

  このサーバがレプリカリングに属している場合、最後にバックアップを取った時点以降のロールフォワードログをすべて、ひとつのディレクトリ内に集めておきます。ファイル名はログ生成時と同じにしておかなければなりません。

詳細については、458 ページの 「復元に必要なバックアップファイルの収集」を参照してください。

注: サーバのバックアップファイルがない場合は、Xbrowseを使用して、サーバ情報の回復に役立つ情報をeDirectoryに問い合わせてください。この作業は、サーバオブジェクトやその関連オブジェクトをツリーから削除する前に実行する必要があります。

Xbrowseの詳細については、NetIQサポートのWebサイト (http://support.novell.com/docs/Readmes/InfoDocument//2960653.html)を参照してください。

❒ eDirectoryを再インストールし、仮のツリーで稼動させておきます。

障害が起きる前と同じ名前のサーバを作成するので、まずサーバを新しいツリーで稼動させます。復元でサーバーの完全な識別情報を再作成する前に元のツリーに新しくインストールしたサーバを置くことで混乱が生じないようにするためです。データベースの復元処理が完了してから、本来のツリーにサーバを組み入れることになります。

❒ (状況によって実行)このサーバでロールフォワードログ機能を使うためには、復元後に改めて有効に切り替え、障害対策のための書き出し先も設定し直して、ロールフォワードログの環境設定を再作成する必要があります。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

復元処理の過程で、ロールフォワードログの機能は無効になり、ログ保存先の設定もデフォルトに戻ってしまいます。

フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

❒ (状況によって実行)IPアドレスを指定してこのサーバにアクセスするアプリケーションやオブジェクトがある場合は、元と同じIPアドレスを設定してください。

復元の過程で、eDirectoryバックアップツールはまず、フルバックアップファイルからの復元を試みます。それが済むと、バックアップツールでインクリメンタルバックアップファイルの名前を入力するよう求められます。その際、次に適用するべきファイルのIDが提示されます。インクリメンタルバックアップファイルからの復元が終わると、今度はロールフォワードログを参照しての復元処理が始まります。445 ページの 「バックアップツールによる復元作業の概要」も参照してください。

必要なファイルをすべて揃えた後、iManagerやDSBK Clientから復元処理を起動します。466 ページの 「DSBKによるバックアップファイルの復元作業」または606 ページの 「iManagerによるバックアップファイルの復元作業」を参照してください。

復元に必要なバックアップファイルの収集

1 ファイルシステムをバックアップしたテープから、eDirectoryフルバックアップファイルを、サーバ上の適当なディレクトリにコピーしてください。

最後に取ったフルバックアップのIDは、バックアップツールのログファイルで確認できます。

2 同様に、一連のインクリメンタルバックアップファイルを、サーバ上の適当なディレクトリにコピーしてください。

必要なインクリメンタルバックアップファイルは、フルバックアップファイルのヘッダ部で確認できます。「next_inc_file_ID」属性として、次のインクリメンタルバックアップファイルのIDが記述されています。next_inc_file_IDは、インクリメンタルバックアップファイルのヘッダ部にある「incremental_file_number」属性のIDと同じです。ヘッダの説明は、「446 ページの「バックアップファイルのヘッダ書式」」を参照してください。

警告: バックアップファイルを開くときは、ヘッダを確認するだけにしてください。ファイルを保存または変更しようとすると、ファイルの一部が切り捨てられる場合があります。ほとんどのアプリケーションがバイナリデータを正しく保存することができません。

インクリメンタルバックアップファイルにはそれぞれ、次のインクリメンタルバックアップファイルのIDが記載されています。

このIDもバックアップツールのログファイルで確認できます。

同じ名前のファイルがいくつもあって、ひとつのディレクトリにまとめるためにファイル名を変更しているような場合、IDはその識別に不可欠です。たとえば無人でのバックアップにいつも同じバッチファイルを使っていて、バックアップファイル名が常に同じであるような場合です。ヘッダ部のIDを見れば、ファイル名が変わっていても適切なファイルを判別できます。

3 (状況によって実行)ロールフォワードログ機能を有効にしていた場合は、最後のバックアップ以降のロールフォワードログを、生成時のファイル名のまま、サーバ上の適当なディレクトリに集めてください。

このサーバがレプリカリングに属している場合は、ロールフォワードログを使った復元処理が必須です。ロールフォワードログがすべて揃っていない場合、復元検証は失敗してしまいます。リング内の他のレプリカと比較して遷移ベクトルが一致しないからです。デフォルトでは、復元したeDirectoryデータベースが他のレプリカと整合が取れていない場合、そのままではオープンできません。

テキストエディタで最新のバックアップファイルを開き、ヘッダの「current_log」属性を読んで、最初に必要なロールフォワードログを特定します。この作業を繰り返して、続くすべてのロールフォワードログを集めます。

警告: バックアップファイルを開くときは、ヘッダを確認するだけにしてください。ファイルを保存または変更しようとすると、ファイルの一部が切り捨てられる場合があります。ほとんどのアプリケーションがバイナリデータを正しく保存することができません。

必要なロールフォワードログがすべて1ヶ所にまとまっているとは限りません。よく確認して、すべて同じディレクトリに揃えてください。ロールフォワードログは、次の理由から複数の場所に格納されている場合があります。

- 最後にeDirectoryのフル/インクリメンタルバックアップを実行してから、ロールフォワードログの保存先を変更した場合。
- ファイルシステムのバックアップを使用して、ロールフォワードログをテープにバックアップした後で、空きディスク容量を確保するためにそれらのファイルを削除した場合。

  テープにバックアップされたロールフォワードログを取得する場合は、データが最新のセットであることを確認してください。テープおよびサーバに複製されたファイルのタイムスタンプを比較する必要があります。ファイルシステムのバックアップ中にデータベースで使用されていたロールフォワードログファイルは、テープでは不完全になります。最新の完全なファイルはサーバに格納されています。

- 最後にバックアップを実行してからeDirectoryデータベースの名前を変更した(NDSからND1に変更した場合など)。この変更により、ロールフォワードログのパスの最後のディレクトリ名が変更されます。

  たとえばログの保存先を「D:\novell\nds\dibfiles\」と指定した場合、eDirectoryデータベース名が「NDS」であれば、実際の保存先ファイルはディレクトリ「D:\novell\nds\dibfiles\nds.rfl\」となります。データベースの名前をNDSからND1に変更した場合、ロールフォワードログのディレクトリはD:\Novell\nds\dibfiles\nd1.rfl\に変更されます。

重要: 必要なロールフォワードログがすべてそろっていることを確認してください。バックアップツールでは、ロールフォワードログがすべてそろっているかどうか確認できません。ロールフォワードログは順番に開かれて使用されます。指定したディレクトリ内に次のロールフォワードログが見つからない場合は、復元プロセスが中止されます。必要なロールフォワードログがすべてそろっていなければ復元は完了しません。

DSBKの使用

DSBKは、eDirectoryバックアップを実行する簡易なコマンドラインパーサです。ただし、DSBKでは最初にログインしたり役割ベースサービスを設定することなく、サーバコンソールからバックアップを実行できます。これは、Linuxではスクリプトとして実行され、Windowsではコンソールユーティリティとして実行されます。

DSBK操作が完了すると、操作の結果がファイル(Linuxではdsbk.err)に書き込まれ、プログラムを使用して開き、その内容を表示することができます。操作時にエラーが発生した場合は、このファイルの最初の4バイトにエラーコードが記録されます。エラーが発生しなかった場合、このファイルの最初の4バイトには0が記録されます。

注: バックアップまたは復元の設定を完了する前に、NetIQによって指定されたすべてのガイドラインを済ませていることを確認します。

eDirectoryのバックアップ/復元作業に先立ち、「eDirectoryのバックアップ処理に関する確認事項」を参照して問題点を確認し、効率的に作業できるようにしてください。

このセクションでは、次の点を説明します。

前提条件

- ロールフォワードログを作成するのであれば、バックアップを行う前にこの機能を有効にしてください。

  レプリカリングに属するサーバは、ロールフォワードログ機能を有効にしておく必要があります。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないことになります。

  ロールフォワードログの詳細については、「ロールフォワードログを使用する」を参照してください。また、この機能を有効にする手順については、DSBKによるロールフォワードログの設定を参照してください。

- eDirectory以外にも追加でバックアップしたいファイルがあれば、それを列挙したインクルードファイルを作っておいてください。

  スイッチを使用して、ストリームファイルをバックアップすることができます。NICIファイルは常にバックアップするようお勧めします。NICIのバックアップ方法の詳細については「NICIのバックアップと復元」を参照してください。

  それ以外にautoexec.ncfファイルなどをバックアップしたい場合は、そのパスとファイル名をインクルードファイルに列挙します。複数のファイルがある場合はセミコロンで区切ります。改行(ハードリターン)や空白を含めないようにしてください。例:
  sys:\system\autoexec.ncf;sys:\etc\hosts;

- eDirectoryのバックアップ後すぐに、ファイルシステムのバックアップ作業を行い、テープに保存できるよう準備してください。バックアップツールによる処理では、サーバ上にバックアップファイルができるだけです。

ヒント: コピー先ストレージデバイスに容量の制約がある場合は、あらかじめeDirectoryバックアップファイルの最大サイズを設定すると便利です。その場合、backupコマンドの「-s」オプションを使い、バイト単位で指定します。また、バックアップファイルの作成後、サードパーティ製ファイル圧縮ツールを使う方法もあります。80%程度は圧縮できます。

- コマンドラインオプションについては、「バックアップ/復元のコマンドラインオプション」を参照してください。

さまざまなプラットフォームでDSBKを使用する

- 461 ページの 「Linux上でDSBKを使用する」
- 463 ページの 「WindowsでDSBKを使用する」

Linux上でDSBKを使用する

DSBKコマンドは、eDirectoryがインストールされているLinuxサーバのシェルで直接実行できます。

コマンドの出力はeDirectoryインスタンス固有のログファイルに書き込まれます(デフォルトのインスタンス: /var/opt/novell/eDirectory/log/ndsd.log)。

```
DSBK HELP
To get help on a specific function type "help <function name>"
 Current functions:
  backup
  restore
  restadv
  getconfig
  setconfig
  cancel
```

DSBKコマンドをcrontabに入力して、dsbk getconfigおよびdsbk backupコマンドを定期的に実行し、週1回フルバックアップを行い他の日にインクリメンタルバックアップを行ったり、必要に応じて任意の組み合わせを行ったりすることができます。

DSBKでRFLを使用する

- 次のコマンドを使用してRFLをオンにします。

  ```
  dsbk setconfig -L
  ```

  -Lオプションにより、新しいロールフォワードログ記録セッションを開始します。
- 次のコマンドを使用して、作成されるロールフォワードログの場所を設定します。

  ```
  dsbk setconfig -L -r <roll forward log directory>
  ```
- 次のコマンドを使用して、作成されるロールフォワードログの場所を取得します。

  ```
  dsbk getconfig
  ```
- -aオプションを使用して、バックアップ時に、ロールフォワードログのディレクトリから古いログファイルを削除します。

  ```
  backup -f <file name> -l <file name> [-s <size>] [-u <file name>] [-e
  <password>] [-t] [-w] [-a]
  [-b|-i|-c] [-o] [-d] [--config-file <configuration file>]
  ```

ヒント: DSBKユーティリティを対話形式で使用する場合は、2つ目の端末ウィンドウを開いて、tail -f <instance specific ndsd.log>を実行します。これにより、入力されたコマンドに対する出力をすぐに読み込むことができます。

バックアップが完了したら、標準のファイルシステムバックアップユーティリティを使用してバックアップします。

注: DSBKコマンドラインオプションに関する詳細については、「バックアップ/復元のコマンドラインオプション」を参照してください。

WindowsでDSBKを使用する

このセクションでは、WindowsプラットフォームでのDSBKユーティリティの基本的な操作について説明します。

eDirectoryをホストするWindowsサーバ上でDSBKを使用する場合、次の手順を実行します。

1. **NetIQ eDirectoryサービス**コンソールからユーティリティを起動します。**dsbk.dlm**は［サービス］タブのサービスリストで使用可能なオプションの1つです。**dsbk**サブコマンドとそのサブコマンドのパラメータは［**起動パラメータ**］フィールドで指定します。
2. getconfigスイッチを使用して、バックアップの現在の設定を表示します。すべてのDSBKコマンドの出力は、WindowsのeDirectoryインストールフォルダにあるbackup.outファイルに追加されます。
3. 次のコマンドを使用して、作成されるロールフォワードログの場所を設定します。

   ```
   setconfig -r <roll forward log directory> -L
   ```

   -Lオプションにより、新しいロールフォワードログ記録セッションを開始します。
4. 次のコマンドで、ツリー上のバックアップを開始します。

   ```
   backup -f <backup file> -l <logfile> -t -w -b -e <password>
   ```

   次のオプションを使用します。

   - -t: ストリームファイルのバックアップを取ります。
   - -w: 同じ名前の既存のバックアップファイルを上書きします。
   - -b: フルバックアップを実行します。
   - -e <*password*>: 指定したパスワードを使用してNICIバックアップを実行します。
   - -a: 「ホット」バックアップ中にロールフォワードログのディレクトリから古いログファイルを削除します。

   たとえば、次のようにバックアップを起動します。

   ```
   backup -f c:\dsbk.bak -l c:\backup.log -t -w -b -e novell
   ```

   完了したバックアップのステータスはbackup.outファイルで確認できます。

   注: DSBKコマンドラインオプションに関する詳細については、「バックアップ/復元のコマンドラインオプション」を参照してください。

次のコマンドを使用してRFLをオンにすることができます。

```
setconfig -r <roll forward log directory> -L
```

DSBKによる手動バックアップ

DSBKを使って、eDirectoryデータベースの中身を、指定したファイルにバックアップすることができます。バックアップファイルには、eDirectoryをその時点の状態に復元するために必要な情報がすべて含まれています。また、処理結果は所定のログファイルに記録されます。

DSBKを使うと次のような作業ができます。

- データベースを開いたままで、フル/インクリメンタルバックアップ(ホットバックアップ)。

「ホット」バックアップの場合、処理中もeDirectoryデータベースは開いたままでありながら、バックアップ開始時点のスナップショットである完全なバックアップを作成できます。

- コールドバックアップ(データベースをいったん停止してフルバックアップ)。

  この機能は、ハードウェアをアップグレードする、あるいはサーバを新規マシン(同じオペレーティングシステムが動作するもの)に移行する場合に有用です。詳しくは、ハードウェアのアップグレードやサーバの交換 を参照してください。

- バックアップ後、データベースを閉じたままにしてロックする設定。
- バックアップファイルの最大サイズの設定。

手順

DSBKを使ってeDirectoryデータベースをバックアップする手順を次に示します。

1 次の一般的な形式に従って、dsbk backupコマンドを入力します。

  dsbk backup -b *-f backup_filepath_and_backup_filename* -l *backup_log_filename_and_path* -u *include_file_filename_and_path* -t -w

  各スイッチの間にはスペースが必要です。スイッチの順序は重要ではありません。

  たとえば、Windowsでは、次のコマンドを入力します。

  dsbk backup -b -f c:\backups\8_20_2001.bak -l c:\backups\backup.log -u c:\backups\myincludefile.txt -t -w

  この例では、フルバックアップを取ること(-b)、バックアップファイルをc:\backups\8_20_2001.bakとすること、処理結果をc:\backups\backup.logに出力すること、さらに、データベースとともに、次に示す他のファイルもバックアップすることを指定しています。

  - 管理者があらかじめ作成したインクルードファイル(-u c:\backups\myincludefile.txt)に列挙されたファイル。
  - ストリームファイル(-t)。

  さらにこの例では「-w」オプションが指定されているため、同じ名前のバックアップファイルがあれば上書きされます。

  出力はdsbackup.outファイルに書き込まれ、バックアップが成功したかどうかを示します。

  eDirectoryのバックアップ処理が終了したら、すぐにファイルシステムのバックアップ作業を行い、テープに保存しますバックアップツールによる処理では、サーバ上にバックアップファイルができるだけです。

eDirectoryのバックアップの自動化

eDirectoryのバックアップを自動化するには、次のコマンドをバッチに記述します。

```
dhostcon.exe 192.168.1.1 load dsbk backup -b -f <Backup File> -l <Log File> -t -w
```

次に例を示します。

```
c:\novell\nds\dhostcon.exe 192.168.1.1 load dsbk backup -b -f edirbackup.bak -l
c:\novell\edir-backup.log -t -w
```

このファイルをeDirectoryがインストールされている場所に保存します。

DSBKによるロールフォワードログの設定

DSBKを使用して、ロールフォワードログの設定を変更します。次のような設定ができます。

- 現在の設定の確認
- ロールフォワードログ機能の有効/無効の切り替え

  レプリカリングに属するサーバは、ロールフォワードログ機能を有効にしておく必要があります。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないことになります。
- ロールフォワードログの保存先ディレクトリの変更
- ロールフォワードログのファイルサイズの最小値、最大値の設定
- 現在使用中のログ、既に書き出しを終えた最新のログの判別
- ストリームファイルをロールフォワードログに含めるかどうかの切り替え

ロールフォワードログの詳細については、「453ページの「ロールフォワードログを使用する」」を参照してください。

手順

1 次のように入力して、現在の設定を確認します。

dsbk getconfig

オプション指定は必要ありません。

たとえば次のように表示されます。

```
Roll forward log status OFF
Stream file logging status OFF
Current roll forward log directory C:\rfl\nds.rfl
Minimum roll forward log size (bytes) 104857600
Maximum roll forward log size (bytes) 4294705152
Last roll forward log not used 00000000.log
Current roll forward log 00000001.log
*** END ***
```

2 setconfigコマンドで設定を変更します。次のような形式で入力してください。

dsbk setconfig [-L|-l] [-T|-t] -r *path_to_roll-forward_logs* -n *minimum_file_size* -m *maximum_file_size*

各スイッチの間にはスペースが必要です。スイッチの順序は重要ではありません。

ロールフォワードログ専用のディスクパーティション/ボリュームを用意するのが最善です。こうしておけば、ディスク容量やアクセス権を監視しやすくなります。

警告: ロールフォワードログ記録を有効にしたら、デフォルトの保存先は使用しないでください。障害対策のためには、eDirectoryとは別のディスクパーティション/ボリューム、別の記憶デバイスを指定してください。ロールフォワードログディレクトリは、バックアップ環境設定を変更するサーバ上である必要があります。

重要: ロールフォワードログ機能を有効にする場合、ログを保存するボリュームのディスク容量を常に監視してください。これを怠ると、ログの容量は増える一方なので、ディスクパーティション/ボリュームがあふれてしまう恐れがあります。ディスク容量が不足してロールフォワードログを作成できない場合は、eDirectoryはそのサーバに対して応答しなくなりま

す。書き出しが終わったロールフォワードログは、定期的にバックアップし、サーバから削除するようお勧めします。詳細については、456 ページの 「ロールフォワードログのバックアップと削除」を参照してください。

DSBKによるバックアップファイルの復元作業

DSBKを使用して、手動で作成したバックアップファイルに保存されたデータから、eDirectoryデータベースを復元します。処理結果は所定のログファイルに記録されます。

DSBKを使えば、iManagerにはない高度な復元オプションも使用することができます。これらは、「467 ページの 「バックアップ/復元のコマンドラインオプション」」のrestoreおよびrestadvの項に記載されています。

追加の前提条件

- ❒ 復元対象サーバにeDirectoryをインストールし、稼動させておいてください。

  たとえば記憶デバイスの障害の場合、デバイスを交換し、改めてeDirectoryをインストールすることになります。故障したサーバごと交換する、あるいは単に新しいサーバに移行する場合は、新しいサーバにオペレーティングシステムをインストールした上で、eDirectoryも準備します。
- ❒ コマンドラインオプションについては、「467 ページの 「バックアップ/復元のコマンドラインオプション」」を参照してください。
- ❒ 復元処理の詳細については、「445 ページの 「バックアップツールによる復元作業の概要」」を参照してください。

手順

DSBKを使ってeDirectoryデータベースを復元する手順を次に示します。

1. 必要なバックアップファイルを集めておきます。詳しくは「457 ページの 「復元処理の準備」」を参照してください。
2. 次の一般的な形式に従って、dsbk restoreコマンドを入力します。

   dsbk restore -r -a -o -f *full_backup_path_and_filename* -d *roll-forward_log_location* -l *restore_log_path_and_filename*

   各スイッチの間にはスペースが必要です。スイッチの順序は重要ではありません。-rスイッチを使用してeDirectoryデータベースそのものを復元します。このスイッチを指定しないと、その他の種類のファイルのみが復元の対象となります。復元処理の終了後にデータベースをアクティブにして開くには、-aおよび-oを指定してください。

   ロールフォワードログを使って復元する場合は、ログのフルパスを指定しなければなりません。フルパスは、eDirectoryにより自動的に作成されたディレクトリ(通常は\nds.rfl)を含みます。このディレクトリについて詳しくは455 ページの 「ロールフォワードログの保存先」を参照してください。

   次に例を示します。

   dsbk restore -r -a -o -f $HOME/backup/nds.bak -d $HOME/backup/rfldir/nds.rfl -l $HOME/backup/backup.log

この例では、データベースそのものを復元し(-r)、復元の検証が正常終了してから、そのデータベースをアクティブにして(-a)、開く(-o)よう指定しています。-fスイッチでフルバックアップファイルの場所を、-dでロールフォワードログの場所を指定しています。また、復元処理の結果を記録するログファイルを、-lで指定しています。

DSBKはフルバックアップを復元します。復元が正常に終了したかどうかを示す出力がndsd.logに書き込まれます。

3 (状況によって実行)復元処理に失敗した場合は、ログファイルでエラーの原因を確認してください。

復元後の検証に失敗した場合の対処については、「478 ページの 「復元後の検証処理に失敗した場合の対処方法」」を参照してください。

注: レプリカリング中にeDirectory 8.5より前のバージョンが稼動しているサーバがある場合、復元処理は失敗します。エラーコードは-666、すなわち「DSバージョンの不整合」となります。

---

4 (状況によって実行)NICIセキュリティファイルを復元した場合は、復元の完了後、サーバを再起動してNICIを再初期化し、その後でDIBを復元します。

5 ここでサーバが通常どおり要求に応答することを確認しておきます。

6 (状況によって実行)このサーバでロールフォワードログ機能を使うためには、改めて有効に切り替え、障害対策のための書き出し先も設定し直して、ロールフォワードログの環境設定を再作成する必要があります。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

この手順が必要となるのは、復元処理の過程で、ロールフォワードログに関する設定はデフォルトに戻るためです。つまり、ロールフォワードログ機能は無効となり、保存先もデフォルトの場所になるからです。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

ロールフォワードログの詳細については、「453 ページの 「ロールフォワードログを使用する」」を参照してください。

以上で復元作業が終了しました。NICIの再初期化も済んでいるので、暗号化された情報にもアクセスできます。ロールフォワードログ機能を使用する場合は、今後の障害に備えるため、再びこの機能を有効にし、フルバックアップを取っておいてください。

バックアップ/復元のコマンドラインオプション

eDirectory バックアップツールのコマンドラインオプションは、backup、restore、restadv、getconfig、setconfig、およびcancelの6つの関数に分類されます。

オプションはどのような順序で指定しても構いません。各オプション間は空白で区切ってください。

オプション	説明
backup	データベースおよび関連ファイルのバックアップ
-f *file_name*	(必須)バックアップファイルの名前とパス。 バックアップツールで作成するバックアップファイルのファイル名と場所を指定します。バックアップ対象サーバ上のローカルファイルを指定してください。たとえば、backup -f C:\backup\ndsbak.bakと指定すると、データベースがC:\backup\ndsbak.bakにバックアップされます。

オプション	説明
-l *file_name*	(必須)ログファイルの名前とパス バックアップ処理の結果を出力するログファイルを指定します。
-b	(オプション)フルバックアップを実行. eDirectoryデータベースのフルバックアップを取ります。これがデフォルトの動作で、「-i」も「-c」も指定しなければフルバックアップになります。■分節拡張■-iと-cのどちらも指定しなかった場合は、フルバックアップが実行されます。
-i	(オプション)インクリメンタルバックアップを実行. eDirectoryデータベースのインクリメンタルバックアップを取ります。最後に実施したフル/インクリメンタルバックアップ以降、変化した部分のみをバックアップします。
-t	(オプション)ストリームファイルもバックアップ. eDirectoryデータベースをバックアップする際、ストリームファイルも含める指定です。
-u *file_name*	(オプション)インクルードファイル名およびパス. バックアップ対象に追加するファイル名を列挙した、インクルードファイルを指定します。この環境設定ファイルは、サーバのeDirectoryデータベースを復元する際に必要な他のファイルをバックアップに含めるように作成できます。 インクルードファイルには各ファイルのフルパスを記述し、末尾にセミコロン(;)を置いてください。 ファイルのリストにスペースやハードリターンを含めないでください。 指定どおりバックアップされたことは、ログファイルを見るか、バックアップファイルのヘッダを見れば確認できます。450 ページの 「バックアップログファイルの書式」および446 ページの 「バックアップファイルのヘッダ書式」を参照してください。 **警告:** バックアップファイルを開くときは、ヘッダを確認するだけにしてください。ファイルを保存または変更しようとすると、ファイルの一部が切り捨てられる場合があります。ほとんどのアプリケーションがバイナリデータを正しく保存することができません。

オプション	説明
-s *file_size*	(オプション)バックアップファイルの最大容量(MB単位)。 バックアップファイルの最大容量(MB)を指定します。バックアップファイルを保存する記憶媒体に容量制限がある場合、このオプションで最大容量を指定するとよいでしょう。 最大容量に達すると新しいバックアップファイルが生成されます。ファイル名の末尾に、5桁の16進数値を追加した名前になります。この拡張の数字は、新規ファイルが作成されるたびに1ずつ増加します。 たとえば、コマンドの一部として「backup -f 10:/backup/mydib.bak -s 10」というスイッチを使用した場合は、バックアップファイルの最大容量を10MBに設定できます。データベースが35MBあったとすれば、最終的に以下のバックアップファイルができます。 C:\backup\mydib.bak、サイズは9.6MB C:\backup\mydib.bak.00001、サイズは9.6MB C:\backup\mydib.bak.00002、サイズは9.6MB C:\backup\mydib.bak.00003、サイズは5.6MB 最小可能サイズは約1MBです。バックアップで作成されるファイル数によって、最初のファイルが大きくなる場合があります。 最初のファイルには、number_of_filesというバックアップタグの下に属性が含まれています。これはバックアップファイルの総数を表します。上記の例では4となります。また、各バックアップファイルのヘッダに、backup_fileという属性が含まれています。これは本来のバックアップファイル名を表します。詳細については、446 ページの 「バックアップファイルのヘッダ書式」を参照してください。 上記の4つのバックアップファイルを使って復元する場合、コマンドは次のようになります。 restore -f C:\backup\mydib.bak -l *log_file_path_and_filename* ファイルが複数に分かれていることはバックアップツールによって自動的に認識され、同じディレクトリ内にある、上記の名前のファイルが検索されます。 **ヒント:** サードパーティ製のファイル圧縮ツールを使えば、バックアップファイルの容量を小さくすることができます。80%程度は圧縮できます。

オプション	説明
-w	(オプション)同名のバックアップファイルがあれば上書き -fスイッチで指定されたものと同じ名前のバックアップファイルがあれば、上書きします。この指定がない場合で同名のファイルが存在すると、対話式モードであれば、バックアップツールは上書きしてよいかどうか確認を求めます。バッチモードでは、同じ名前のファイルが存在する場合に-wが指定されていないと、デフォルトの動作として、ファイルは上書きされず、バックアップは作成されません。 eDirectoryのフル/インクリメンタルバックアップの都度、すぐにファイルシステムのバックアップを取っているのであれば、前回のバックアップファイルはテープに保存されているはずです。したがって上書きしても問題ありません。 **重要:** バッチファイルを使って無人バックアップを行う場合、このオプションを指定してください。同じバッチファイルを繰り返し使用するなど、同じ名前のバックアップファイルが存在する場合、バックアップが正常に行われるように、-wオプションを使用して、既存のバックアップファイルが上書きされるようにしてください。 バッチモードでは、同じ名前のファイルが存在する場合に-wが指定されていないと、デフォルトの動作として、ファイルは上書きされず、バックアップは作成されません。なお、対話式モードの場合は、-wが指定されていないと、ファイルを上書きしてよいかどうか問い合わせます。
-c	(オプション)コールドバックアップを実行 フルバックアップと同様ですが、いったんデータベースを停止してから実行します。-oまたは-o -dが指定されている場合を除き、バックアップ終了後、データベースは再びオープンされます。
-o	(オプション)コールドバックアップ後、データベースを停止したままにする -cスイッチを使用した場合にのみ使用できます。コールドバックアップの終了後、データベースを停止したままにします。この機能は、ハードウェアをアップグレードする、あるいは新規サーバ(同じオペレーティングシステムが動作するもの)に移行する場合に有用です。詳しくは「563 ページの「ハードウェアのアップグレードやサーバの交換」」を参照してください。
-d	(オプション)コールドバックアップ後、DSエージェントを無効にする -cスイッチと-oスイッチの両方を指定した場合にのみ使用できます。コールドバックアップ後、DSエージェントを無効にします。この機能は、ハードウェアをアップグレードする、あるいは新規サーバ(同じオペレーティングシステムが動作するもの)に移行する場合に有用です。詳しくは「563 ページの 「ハードウェアのアップグレードやサーバの交換」」を参照してください。 擬似サーバの「login disabled」属性を設定することにより、DSエージェントを無効にします。その結果、eDirectoryを起動しようとすると「-663」エラーが発生します。
-e *password*	NICIバックアップの実行 *password*は、NICIバックアップパスワードを指定します。この同じパスワードをNICIファイルの復元でも指定する必要があります。

オプション	説明
--config-file *configuration file*	(オプション)バックアップするeDirectoryのインスタンスを指定できます。 *configuration file*は、バックアップするeDirectoryインスタンスの環境設定ファイルへの絶対パスを指定します。次に例を示します。 --config-file /etc/opt/novell/eDirectory/conf/nds.conf このスイッチは、Linux環境にのみ適用されます。
restore	データベースおよび関連ファイルの復元
-f *file_name*	(必須)バックアップファイルの名前とパス。 復元に使うフルバックアップファイルを指定します。このファイルは復元対象サーバ上に置いておかなければなりません。たとえば、restore -f :/backup/ndsbak.bakを指定すると、ファイルC:/backup/ndsbak.bakから復元されます。 複数のファイルに分かれている場合は、すべて同じディレクトリ内に集めておいてください。
-l *file_name*	(必須)ログファイルの名前とパス 復元処理の結果を出力するログファイルを指定します。
-r	(オプション)DIBセットも復元。 eDirectoryデータベースを復元する旨の指定です。 **警告:** このオプションを指定しなかった場合、eDirectoryデータベース自身は復元されません。指定した種類以外のファイルのみが復元の対象になります。
-d *dir_name*	(オプション)ロールフォワードログのあるディレクトリ ロールフォワードログを集めたディレクトリを指定します。復元対象サーバ上のフルパスで指定してください。必要なロールフォワードログをすべて、作成時と同じファイル名にして、ひとつのディレクトリに集めておかなければなりません。 バックアップファイルからの復元後、ロールフォワードログを使って、バックアップ時点以降の変更を反映させます。-dスイッチが使用されない場合、バックアップ時にロールフォワードログ記録を有効にしていても、バックアップツールはログファイルを参照しません。 最初に適用するべきロールフォワードログは、最新のバックアップファイルをテキストエディタで開き、backupタグのcurrent_log属性を見れば確認できます。ここでいう最新のバックアップファイルとは、-fオプションで指定するフルバックアップファイルか、または復元処理で適用することになる最後のインクリメンタルバックアップファイルです。ヘッダに記述される属性について詳しくは、「446ページの「バックアップファイルのヘッダ書式」」を参照してください。 **警告:** バックアップファイルを開くときは、ヘッダを確認するだけにしてください。ファイルを保存または変更しようとすると、ファイルの一部が切り捨てられる場合があります。ほとんどのアプリケーションがバイナリデータを正しく保存することができません。

オプション	説明
-u	(オプション)インクルードファイルに列挙されたファイルも復元 データベースに追加する形でバックアップしていたファイルも復元します。 バックアップの過程で、データベース以外にもバックアップが必要なファイルを列挙したファイルを作成し、インクルードファイルとして指定することもできます。しかしその場合でも、「-u」オプションで指定しなければ復元されません。
-a	(オプション)検証後、DIBをアクティブにする指定。 復元後の検証処理が正常終了したら、データベース名をRSTからNDSに変更します。この処理の概要については、「445 ページの 「バックアップツールによる復元作業の概要」」を参照してください。
-o	(オプション)処理終了後、データベースをオープンする 処理の終了後にデータベースをオープンするようにバックアップツールに指示します。検証処理が正常終了すれば、データベースが自動的に開きます。失敗した場合は、復元前のデータベースが開きます。この処理の概要については、「445ページの「バックアップツールによる復元作業の概要」」を参照してください。
-s	復元処理後にロールフォワードログをリセットしないようにバックアップツールに指示します。主に、デフォルトのRFLの場所のインスタンスで使用されます。
-n	(オプション)復元後にデータベースを検証しない 検証せずにデータベースを復元するようにバックアップツールに指示します。このサーバの遷移ベクトルをレプリカリングに属する他のサーバと比較する、という検証処理を行いません。遷移ベクトルの詳細については、「452 ページの 「遷移ベクトルと復元後の検証処理」」を参照してください。他のオプションで明示的に指定されていない限り、RSTからNDSへの改名もしません。 **重要:** NetIQサポートから提案されない限り、このオプションの使用はお勧めできません。
-v	(オプション)上書きして復元 検証処理を行うことなく、データベース名をRSTからNDSに変更します。 **重要:** NetIQサポートから提案されない限り、このオプションの使用はお勧めできません。
-k	(オプション)データベースのロックを解除 NDSデータベースのロックを解除します。
-i	順番になったインクリメンタルファイルのカンマ区切りリスト。
-e *password*	バックアップしたNICIファイルの復元 *password*は、NICIファイルのバックアップで使用されたNICIバックアップパスワードを指定します。NICIファイルの復元時に誤ったパスワードが指定された場合は、エラーメッセージが表示されます。

オプション	説明
--config-file *configuration file*	(オプション)復元するeDirectoryのインスタンスを指定できます。 *configuration file*は、復元するeDirectoryインスタンスの環境設定ファイルへの絶対パスを指定します。次に例を示します。 --config-file /etc/opt/novell/eDirectory/conf/nds.conf このスイッチは、Linux環境にのみ適用されます。
restadv	高度な復元機能。 **注:** すべての高度な復元オプションで、DSエージェントがクローズされます。
-l *file_name*	(必須)ログファイルの名前とパス 復元処理の結果を出力するログファイルを指定します。
-o	(オプション)処理終了後、データベースをオープンする 処理の終了後にデータベースをオープンするようにバックアップツールに指示します。検証処理が正常終了すれば、データベースが自動的に開きます。失敗した場合は、復元前のデータベースが開きます。 この処理の概要については、「445 ページの 「バックアップツールによる復元作業の概要」」を参照してください。
-n	(オプション)前に失敗した復元の検証処理を起動 前に復元して検証に失敗したRSTデータベースを再度検証します。
-m	(オプション)復元されたDIBファイルの削除 RSTデータベースが存在すれば削除します。
-v	(オプション)上書きして復元 検証処理を行うことなく、データベース名をRSTからNDSに変更します。 **重要:** NetIQサポートから提案されない限り、このオプションの使用はお勧めできません。
-k	(オプション)データベースのロックを解除 NDSデータベースのロックを解除します。
-i	順番になったインクリメンタルファイルのカンマ区切りリスト。 **重要:** このオプションは、DSBKにのみ適用されます。
getconfig	ロールフォワードログに関する現在の設定を表示。

オプション	説明

	指定できるオプションはありません。
	
	現在の設定を表示します。たとえば、ロールフォワードログ記録が無効になっている場合、getconfigコマンドでは次のような情報が表示されます。
	
	`  Roll forward log status OFF`
	`Stream file logging status OFF`
	`Current roll forward log directory C:\rfl\nds.rfl`
	`Minimum roll forward log size (bytes) 104857600`
	`Maximum roll forward log size (bytes) 4294705152`
	`Last roll forward log not used 00000000.log`
	`Current roll forward log 00000001.log`
	`*** END ***`

setconfig	ロールフォワードログに関する設定の変更。
-L	(オプション)ロールフォワードログ記録の有効化。 ロールフォワードログ機能を有効にします。(デフォルトでは無効)。この記録を有効にしておけば、停止する直前の状態にまでサーバを復元できるようになります。無効のままであれば、最後のフル/インクリメンタルバックアップ時点までしか復元できません。 レプリカリングに属するサーバについては、ロールフォワードログ記録を有効にして、他のサーバとの同期状態も復元できるようにしてください。 ただし管理者にとっては、監視しなければならない対象が増えます。これを怠ると、ログの容量は増える一方なので、ディスクパーティション/ボリュームがあふれてしまう恐れがあります。ディスク容量が不足してロールフォワードログを作成できない場合は、eDirectoryはそのサーバに対して応答しなくなります。定期的にバックアップを取り、使わなくなったログは削除する必要があります。詳細については、456 ページの 「ロールフォワードログのバックアップと削除」を参照してください。 詳細については、453 ページの 「ロールフォワードログを使用する」を参照してください。
-I	(オプション)ロールフォワードログ機能の無効化。 ロールフォワードログ機能を無効にします(デフォルトでは無効)データベースでは連続したログを保存していくのをやめ、現在のロールフォワードログに上書きしていくようになります。ロールフォワードログ作成がオフの場合、最後にフル/インクリメンタルバックアップを実行した時点までしかデータベースを復元できません。 誤って無効にしてしまった場合、ただちに有効にすると同時に、今障害が起こっても復元できるよう、改めてデータベースのバックアップを取ってください。 詳細については、453 ページの 「ロールフォワードログを使用する」を参照してください。

オプション	説明
-T	(オプション)ストリームファイルのログ出力開始 (ロールフォワードログ機能が有効な場合のみ)ストリームファイルが更新された場合、その全体をロールフォワードログにコピーするようになります。ストリームファイルとは、ログインスクリプトなど、データベースに関係する追加の情報ファイルのことです。 ただしストリームファイルを記録すると、ディスクの空き容量が急速に減少します。ログの出力先ディスクパーティション/ボリュームの空き容量を、常に監視するようにしてください。ディスク容量が不足してロールフォワードログを作成できない場合は、eDirectoryはそのサーバに対して応答しなくなります。
-t	(オプション)ストリームファイルのログ出力停止 ストリームファイルが更新されても、その全体をロールフォワードログにコピーしないようになります。この場合でも、フル/インクリメンタルバックアップの際には、ストリームファイルもバックアップできます。ストリームファイルを頻繁に更新しないのであれば、この方法で充分でしょう。 ストリームファイルを記録しないと、ログファイルの容量が急速に増えるのを抑えることにもなります。
-r *dir_name*	(オプション)ロールフォワードログの出力先ディレクトリの設定。 ロールフォワードログの出力先ディレクトリを指定します。たとえば、setconfig -r vol2:\rflというコマンドを実行すると、vol2:\rfl以下にディレクトリが作成され、その下にログファイルができるようになります。 このディレクトリ名は現在のeDirectoryデータベース名に基づいて決まります。通常のインストールでは「NDS」なので、最終ディレクトリ名はvol2:\rfl\nds.rfl\となります。ここでeDirectoryデータベース名を「ND1」に変更すると、保存先もこれに合わせてvol2:\rfl\nd1.rfl\に変わります。 現在の保存先設定はgetconfigコマンドで確認できます。 保存先の設定を変えるとその時点で新しいディレクトリができますが、ログファイルは実際にトランザクションが発生するまで作成されません。 **重要:** バックアップツールでは、ロールフォワードログの保存先ディレクトリが変わったことを認識できません。データベースを復元する際には、最後のバックアップ以降のロールフォワードログをすべて、ひとつのディレクトリに集めておく必要があります。 詳細については、453 ページの 「ロールフォワードログを使用する」を参照してください。
-n *file_size*	(オプション)ロールフォワードログの最小容量の設定 ロールフォワードログの最小容量をバイト単位で指定します。この容量に達した後、実行中のトランザクションが終了すると、ログ出力先が新しいファイルに切り替わります。
-m *file_size*	(オプション)ロールフォワードログの最大容量の設定 ロールフォワードログの最大容量をバイト単位で指定します。この上限に達してもトランザクションが進行中の場合は、トランザクションは次のファイルに続けて記録されます。この設定は最小サイズの設定より常に大きくする必要があります。

オプション	説明
-s	(オプション)ログ出力先ファイルの強制切り替え 実行中のトランザクションが終了した時点で、ログ出力先を新しいファイルに切り替えます。次のトランザクション開始時に新しいファイルが作成されます。
キャンセル	バックアップ/復元処理を取り消します。指定できるオプションはありません。 **注:** このオプションは、DSBKに適用されません。
--config-file *configuration file*	(オプション)ロールフォワードログ設定を構成するeDirectoryのインスタンスを指定できるようにします。 *configuration file*は、ロールフォワードログ設定を構成するeDirectoryインスタンスの環境設定ファイルへの絶対パスを指定します。次に例を示します。 --config-file /etc/opt/novell/eDirectory/conf/nds.conf このスイッチは、Linux環境にのみ適用されます。

cronジョブとしてのDSBKの実行

dsbkスクリプトには、DSTraceバイナリへのフルパスが含まれていません。そのため、デフォルト設定を使用してcronジョブとしてスクリプトを実行すると、スクリプトが失敗します。ただし、パスを追加するように/opt/novell/eDirectory/bin/dsbkスクリプトを変更しないでください。これは、今後のeDirectoryパッチによって、このファイルが上書きされ、スクリプトに対して行われたすべてのカスタマイズが元に戻される可能性があるためです。

代わりに、dsbkをcronジョブとして実行する前に、crontabファイル内のPATH環境変数にndstraceが配置されているディレクトリを追加します。そうすれば、cronジョブがndstraceアプリケーションを探して実行します。

NICIの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。NICIのバックアップと復元は、ルートユーザに対してのみサポートされ、非ルートユーザに対してはサポートされません。

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。eDirectoryのバックアップソリューション(DSBKとeMBox Backup)では、以下を可能にするスイッチ(-e)が使用されます。

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。

eDirectoryのバックアップソリューションの詳細については、「460ページの 「DSBKの使用」」を参照してください。

NICIのバックアップ

NICIバックアップは、フルeDirectoryバックアップまたはインクリメンタルeDirectoryバックアップと一緒に実行できます。

NICIバックアップを実行するコマンドは次のとおりです。

dsbk backup -f file_name -l log_file_name -e password

-fと-lは、backupコマンドと一緒に使用すべき必須オプションです。

-eは、NICIファイルをバックアップするためのスイッチです。

file_nameは、バックアップツールで作成するバックアップファイルのファイル名と場所を指定します。

log_file_nameは、バックアップ操作の結果を記録するために作成されるログファイルのファイル名と場所を指定します。

passwordは、NICIバックアップパスワードを指定します。パスワードは平文として指定できます。Linuxでは、パスワードをファイルとして渡すこともできます。この同じパスワードをNICIファイルの復元でも指定する必要があります。

注: NICIバックアップパスワードを-eスイッチと一緒に指定しなかった場合は、次のエラーメッセージが表示されます。

DSBKでは:

```
Enter password along with the (-e) option!
DSBK error! 4
```

NICIの復元

1 NICIファイルだけを復元します(DIBは復元しません)。

dsbk restore -f file_name -l log_file_name -e password

-fと-lは、restoreコマンドと一緒に使用すべき必須オプションです。

-eは、NICIファイルを復元するためのスイッチです。

file_nameは、復元する情報を含むバックアップファイルのファイル名と場所を指定します。log_file_nameは、復元操作の結果を記録するために作成されるログファイルのファイル名と場所を指定します。passwordは、NICIファイルのバックアップで使用されたNICIバックアップパスワードを指定します。NICIファイルの復元時に誤ったパスワードが指定された場合は、エラーメッセージが表示されます。

2 ndsdサーバを再起動します。

3 DIBを復元します。

dsbk restore -f file_name -l log_file_name -a -r -o

-fと-lは、restoreコマンドと一緒に使用すべき必須オプションです。

-aは検証後にDIBをアクティブにし、-rはDIBセットを復元し、-oは終了後にデータベースを開きます。

NICIバックアップがフルバックアップ中とインクリメンタルバックアップ中に実行され、フルバックアップとインクリメンタルバックアップで別々のNICIバックアップパスワードが使用された場合は、NICIファイルを復元するときに、フルバックアップで使用されたパスワードを使用してNICIファイルを復元する必要があります。

注: パスワードを-eスイッチと一緒に指定しなかった場合は、次のエラーメッセージが表示されます。

DSBKでは:

```
Enter password along with the (-e) option!
DSBK error! 4
```

NICIの復元中に誤ったパスワードが指定された場合は、次のエラーが表示されます。

```
NICI RESTORE: "NICI Files has not been restored(Check your parameters)" Error!: -32
```

復元後の検証処理に失敗した場合の対処方法

復元処理の一環として検証を行います。復元されたeDirectoryデータベースと、レプリカリングに属する他のサーバとの間で、遷移ベクトルを比較するというものです。復元プロセスの詳細については、「445ページの「バックアップツールによる復元作業の概要」」と「452ページの「遷移ベクトルと復元後の検証処理」」を参照してください。

遷移ベクトルが合致しなければ、検証に失敗したことになります。これは一般に、復元処理に使ったファイルのデータが不足していたことを表します。たとえば次のような状況が考えられます。

- 最後にバックアップを実施した後、ロールフォワードログ機能を有効にしていなかった場合。
- ロールフォワードログを取っていたのに、復元の際これを使わなかった場合。
- ロールフォワードログが不足していた場合。

復元したeDirectoryデータベースが他のレプリカと整合が取れていない場合、デフォルトでは、そのデータベースはオープンできません。

バックアップファイルやロールフォワードログの指定を単に忘れただけであれば、正しく指定してもう一度復元処理を実行すればよいはずです。次回に復元が成功すれば、検証に成功し、データベースがオープンされるでしょう。

必要なバックアップファイルやロールフォワードログが揃っていない場合は、以下の手順でサーバを復旧してください。検証に失敗したときの復旧手順の概要を説明します。

- サーバの識別情報やファイルシステム権利は、バックアップファイルなどが不足していても復旧できるはずです。
- バックアップからレプリカを復元できない場合でも、サーバとしては動作します。新しいレプリカが追加されたものとして扱われ、他のサーバにも影響を及ぼしてしまうのです。したがって、レプリカリングからいったんサーバを外し、高度な復元機能やDSRepairツールを使って元の状態に復旧してから、改めてレプリカリングに追加してください。
- このサーバにしかデータがない、すなわち他のサーバにレプリカが作られていないパーティションについては、残念ながら復元できません。

検証に失敗した後、このセクションの説明に従ってサーバの識別情報やファイルシステム権利を復旧し、レプリカリングからいったん外し、再び追加します。ｋこの手順でレプリケーションが終了すれば、サーバは元どおりに機能するようになるはずです。ただしレプリカを作っていなかったために復元できなかったパーティションを除きます。

まず、「479ページの「レプリカリングをクリーンアップする」」に従って作業してください。それが終了したら480 ページの 「サーバの復旧とレプリカの再追加」に進みます。

レプリカリングをクリーンアップする

この手順では、次の方法について説明します。

- **マスタレプリカの再割り当て。** 障害が発生したサーバが、あるパーティションのマスタレプリカを保持していた場合は、DSRepairを使って、レプリカリストに属する他のサーバ上のレプリカを、マスタとして扱うよう指定します。
- **障害が発生したサーバに対するレプリカリストの参照の削除。** 障害が発生したサーバを含むレプリカリングのメンバーである各サーバに対して、障害が発生したサーバが利用できなくなったことを通知する必要があります。

前提条件

- ❒ eDirectoryそのものは、当該サーバに正常にインストールされているものとします。
- ❒ 復元を試み、検証処理で失敗したことが前提です。
- ❒ eDirectoryデータベースは稼動しており、(復元処理により作成された)RSTデータベースもマシンに残っているものとします。
- ❒ どのパーティションのレプリカがこのサーバに保持されていたか、は分かっているものとします。このサーバのレプリカはバックアップファイルのヘッダ部に記録されています。

手順

レプリカリングをクリーンアップするには、次の操作を行います。

1 DSRepairを起動します。復元対象サーバとレプリカを共有しているサーバのコンソールから、次のオプションを指定して起動してください。

- **Windows:** -aスイッチを使用します。
- **Linux:** -Adスイッチを使用します。

-aまたは-Adスイッチを使用した詳細オプションでDSRepairを実行する方法については、「353 ページの 「DSRepairオプション」」を参照してください。

警告: -aまたは-Adを指定してDSRepairを使用する場合は、詳細オプションによってはツリーが破損することがあります。

2 ［**レプリカ操作とパーティション操作**］を選択します。

3 編集したいパーティションを選択します。このパーティションが属するレプリカリングから、障害の起こったサーバを外すことになります。

4 ［**レプリカリングの表示**］を選択して、このパーティションに関するレプリカを持つサーバのリストを表示します。

5 (状況によって実行)当該サーバにマスタレプリカがあった場合、［**このサーバを新しいマスタレプリカに設定**］コマンドで、他のサーバにマスタを切り替えます。

この時点で、対象のレプリカリングは新しいマスタレプリカを保持しています。リングを構成するすべてのレプリカに対して、新しいマスタが存在することが通知されます。

6 そのまましばらく待ちます。上記のレプリカがマスタになったことが他のサーバに認識されるまで、しばらく待ちます。

7 ［**レプリカリングの表示**］に戻ります。障害が発生したサーバの名前を選択して、［**レプリカリングからのサーバの削除**］を選択してください。

DSRepairを起動する際に詳細オプションで-aまたは-Ad(プラットフォームにより選択)を指定していなかった場合、このコマンドは表示されません。

警告: 障害の起こったサーバをマスタレプリカに設定したままで、このコマンドを実行しないでください。リング内のサーバリストを見れば確認できます。マスタレプリカであれば、「ステップ 5」を参照して、他のサーバにマスタを切り替えてから、当該サーバをレプリカリングから外します。

8 管理者としてログインします。

9 説明メッセージを読み、それに対する同意を入力して処理を続行します。

10 DSRepairを終了します。

レプリカリングを構成するすべてのサーバに通知が行われます。

11 障害が発生したサーバを含んでいる各レプリカリングごとに、1つのサーバ上で、この手順を繰り返します。

続いて、障害が生じたサーバ上に、新たにレプリカを構築します。「480ページの「サーバの復旧とレプリカの再追加」」に進んでください。

サーバの復旧とレプリカの再追加

レプリカ設定を「外部参照」側に書き替え、自分自身はレプリカリングに属していないものとして動作するようにします。その上でサーバからレプリカを削除すると、データベースのロックを解除できるようになります。

レプリカを削除すれば、レプリカをサーバに再追加する作業は終わりです。あとは自動的に、他のサーバから各レプリカの最新版を参照し、再追加していきます。各レプリカが再追加されたら、サーバは元と同じように機能するはずです。

DSRepairを使用してレプリカを削除し、レプリケーション機能により再追加する手順を次に示します。

1 479 ページの 「レプリカリングをクリーンアップする」が完了していることを確認します。

2 上書き復元コマンドを、次のように実行します。併せてログファイル名も指定してください。

dsbk restadv -v -l *logfilename*

この詳細復元オプションにより、RSTデータベース(復元したが検証に失敗したもの)の名前をNDSに変更します。ただしロックは解除しません。

3 サーバコンソールで、DSRepairの高度な復元機能により、レプリカ設定をすべて外部参照に切り替えます。

- **Windows:** ［スタート］>［設定］>［コントロールパネル］>［NetIQeDirectoryサービス］の順にクリックします。［dsrepair.dlm］を選択します。［起動パラメータ］フィールドに、「-XK2 -rd」と入力します。［Start］をクリックします。
- **Linux:** 次のコマンドを入力します。

  ```
  ndsrepair -R -Ad -xk2
  ```

-rdまたは-Rスイッチは、ローカルデータベースとレプリカを修復します。

警告: DSRepairによる高度な復元機能は、正しく使用しないとツリーが破損することがあります。

---

4 修復が終了したら、ロックを解除してデータベースを開きます。次のように実行してください。

```
dsbk restadv -o -k -l logfilename
```

-oはデータベースのオープン、-kはロック解除を表します。

5 iManagerを使って、修復されたサーバをレプリカリングに再追加します。

5a NetIQ iManagerで、［役割およびタスク］ボタン  をクリックします。

5b ［パーティションとレプリカの管理］>［レプリカビュー］をクリックします。

5c 複製したいパーティションの名前とコンテキストを指定し、［OK］をクリックします。

5d ［レプリカの追加］をクリックします。

5e ［サーバ名］フィールドの横にある［参照］ボタン  をクリックし、修復されたサーバを選択します。

5f 必要なレプリカのタイプを選択して、［OK］をクリックしてから、［完了］をクリックします。

5g このサーバが属していた各レプリカリングについて、上記の操作を繰り返します。

6 レプリケーション処理が終わるまでしばらく待ちます。

レプリカの状態が［新規］から［オン］に変われば、レプリケーション処理は終了です。これはiManagerで確認できます。詳細については、163 ページの 「レプリカに関する情報を表示する」を参照してください。

7 NICIセキュリティファイルを復元するには、最初に、NICIファイルだけを復元してから、NDSDサーバを再起動して、DIBを復元します。

8 (状況によって実行)このサーバでロールフォワードログ機能を使うためには、改めて有効に切り替え、障害対策のための書き出し先も設定し直して、ロールフォワードログの環境設定を再作成する必要があります。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

この手順が必要となるのは、復元処理の過程で、ロールフォワードログに関する設定はデフォルトに戻るためです。つまり、ロールフォワードログ機能は無効となり、保存先もデフォルトの場所になるからです。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

ロールフォワードログの詳細については、「453 ページの 「ロールフォワードログを使用する」」を参照してください。

バックアップ/復元の運用例

シナリオ: 単一サーバ構成のネットワークで、eDirectoryを格納しているハードディスクが故障した場合

あるユーザはStationery Supply社で単一サーバ構成のネットワークを管理しています。サーバは1台しかないので、耐障害性を得るためにレプリケーションに頼ることはできません。その場合は、バックアップツール機能を使えば、eDirectoryのバックアップ/復元処理が容易になります。この機能は、サーバに特化されているため、高速です。

eDirectory 8.7.3以降のバージョンで、バックアップツールを実行するためのバッチファイルを使用してサーバの無人バックアップをセットアップしました。

毎週日曜の夜にフルバックアップを取り、さらに平日は毎晩、インクリメンタルバックアップを取るようにしました。また、eDirectoryの無人バックアップのすぐ後に、ファイルシステムのフル/インクリメンタルバックアップを取るようにします。バックアップテープには、ファイルシステムデータのほか、eDirectoryの最新バックアップも保存されることになります。さらに、データ保存サービス会社と契約して、バックアップテープを社外に保管することにしました。

毎週月曜日の朝、バックアップログを調べて、正常にフルバックアップが取れていることを確認します。また、普段から時々、インクリメンタルバックアップの状況をログで調べています。

ロールフォワードログの機能は無効にしています。それは次のような理由によります。

- サーバには独立した記憶デバイスがついていないので、ロールフォワードログを有効にしてもバックアップとしては役に立ちません。記憶デバイスが故障すれば、eDirectoryばかりでなくログも消えてしまうので、いずれにしても復元には使えません。

- ツリー構成が変わることはあまりありません。また、障害が発生しても、前の晩の状態にまで復元できれば充分だと考えています。停止直前の状態までeDirectoryを復元できなくても構いません。
- サーバはレプリカリングに属して他のサーバと連携しているわけではないため、ロールフォワードログがなくても、復元後の検証処理には成功するはずです。

Stationery Supply社では、人事異動などによりツリー構成を大きく変える場合は、その直前と直後に、手動でバックアップすることにしています。日曜日以外でも、必要に応じて臨時のバックアップを取ろうというわけです。これがロールフォワードログに代わる措置です。

必要になればいつでもバックアップ作業ができるよう、時々テストして確かめています。テスト用にもう1台サーバを購入する予算はないので、市内にあるサービス会社と契約し、必要なときだけサーバを使わせてもらえるようにしました。実機と似た構成のサーバにオペレーティングシステムをインストールし、eDirectoryデータベースの環境もできるだけ同じように構築します。このサーバに、実機から取ったバックアップファイルを使って復元し、想定どおりに復元されていることを確認するのです。

ある水曜日の朝、eDirectoryが格納されたハードディスクの故障が見つかりました。そこで新しいハードディスクを手配したほか、日曜日に取ったフルバックアップファイル、月曜日および火曜日に取ったインクリメンタルバックアップファイルを用意しました。次に、ハードディスクを交換し、eDirectoryをインストールしました。その上に、フル/インクリメンタルバックアップファイルから復元しました。水曜日の朝、故障が起こる前にツリー構成を変更しましたが、これは復元できませんでした。ロールフォワードログを残しておかなかったからです。ただし、昨夜のバックアップに復元できれば十分です。ロールフォワードログを実行することによって管理オーバーヘッドが賄えるとは思っていません。

シナリオ: 複数サーバ構成のネットワークで、eDirectoryを格納しているハードディスクが故障した場合

あるユーザがOutdoor Recreation社でeDirectoryが稼動する10台のサーバを管理しています。毎週日曜の夜にフルバックアップを取り、さらに平日は毎晩、インクリメンタルバックアップを取っています。eDirectoryのバックアップ後すぐに、ファイルシステムバックアップによりテープに保存しています。

すべてのサーバがレプリカリングに参加しています。ロールフォワードログ機能は全サーバで有効です。また、その保存先は、eDirectoryとは別の記憶デバイスに割り当てています。ディスクの空き領域やアクセス権は随時監視して、ストレージデバイスがロールフォワードログでいっぱいにならないよう注意しています。使用済みのロールフォワードログは、時々テープにバックアップして削除し、空き容量を増やすようにしています。

もちろんロールフォワードログ記録を有効にすると管理の手間が増えますが、それを上回る利点があると考えています。サーバがレプリカリングに属している場合、いつでも最新の状態をバックアップしておく必要があるからです。こうしておけば、障害が発生しても、他のサーバとの同期状態も含めて元どおりに復元できます。

さらに、テスト環境で定期的にバックアップファイルからの復元を試み、想定どおりに動作することを確認しています。

ある木曜日の午後2時、Inventory_DB1というLinuxサーバの、eDirectoryを格納しているハードディスクが故障しました。

そこでまず、最新のフルバックアップファイルとそれ以降のインクリメンタルバックアップファイルを集め、昨晩午前1時の状態にまでデータベースを復元します。ロールフォワードログは昨夜のバックアップ以降の変更を記録しています。そこで次に、午前1時以降のロールフォワードログを使って、故障が起こる直前の状態に戻さなければなりません。

次のような手順で作業を進めることにしました。

1. まず、サーバのハードディスクを交換します。
2. 日曜の夜に取ったフルバックアップのテープを用意しました。

   フルバックアップ用のバッチファイルは、毎週日曜の夜にファイル/adminfiles/backup/backupfull.bkにバックアップするようになっています。

   ファイルの容量制限を200MBと設定していたので、次の2つのファイルがありました。

   backupfull.bk.00001 (250MB)

   backupfull.bk.00002 (32MB)
3. さらに、月曜、火曜、水曜に取ったインクリメンタルバックアップのテープも用意しました。

   インクリメンタルバックアップ用のバッチファイルは、平日に毎晩、ファイル/adminfiles/backup/backupincr.bkにバックアップするようになっています。

   毎日同じバッチファイルを使っているので、ファイル名は常に同じです。しかし、テープからサーバにコピーする時に、ファイル名を変更しなければなりません。復元処理の際は、全ファイルを同じディレクトリに集めておく必要があるからです。
4. まず、ハードディスクを交換しました。

   幸いLinuxオペレーティングシステムを格納したハードディスクは故障しなかったので、Linuxの再インストールは必要ありませんでした。
5. バックアップテープを使って、障害を受けたディスクパーティションを復元しました。
6. 次にeDirectoryを再インストールし、仮のツリーを作りました。復元処理では、いったんこのツリー上にデータを復元してから実動ツリーに切り替えることになります。
7. サーバ上に、バックアップファイルを集めておくためのディレクトリ/adminfiles/restoreを作りました。
8. フルバックアップファイル(2つに分割されているもの)を、このディレクトリにコピーしました。
9. さらに、月曜、火曜、水曜のインクリメンタルバックアップファイルもコピーしました。

   どれも同じbackupincr.bkというファイル名なので、次のように名前を変更します。

   backupincr.mon.bk

   backupincr.tues.bk

   backupincr.wed.bk

   注: インクリメンタルバックアップファイルは、必ずしもフルバックアップファイルと同じディレクトリにコピーしなくても構いません。ただし各インクリメンタルバックアップファイルはすべて同じディレクトリに置いておく必要があります。

   ---
10. 次にiManagerを使ってeDirectoryを復元することにしました。
    a. iManagerを起動し、［**eDirectoryの保守**］>［**復元**］の順にクリックします。
    b. サーバにログインしました。コンテキストとしては、仮に作っておいたツリーを使います。
    c. ［復元ウィザード – ファイルの環境設定］画面で次のように操作しました。

バックアップファイルの場所として、「/adminfiles/restore」を指定。

復元処理に関するログファイルの出力先として「/adminfiles/restore/restore.log」を指定。

d. ［復元ウィザード - オプション］画面で次のように操作しました。

［**データベースを復元**］チェックボックスをオン。

［**ロールフォワードログの復元**］チェックボックスをオン。

ロールフォワードログの保存先を入力。

これは普段ロールフォワードログを保存している場所です。eDirectoryとは別のハードディスクなので、今までのロールフォワードログが残っているはずです。

［**セキュリティファイルの復元**］チェックボックスをオン。

［**復元されたデータベースを検証後にアクティブにします**］チェックボックスをオン。

［**復元の完了後にデータベースを開く**］チェックボックスをオン。

これは、復元後の検証に成功したらeDirectoryをオープンするための指定です。

11. 復元処理を起動し、インクリメンタルバックアップファイル名を問い合わせるメッセージが表示されたので入力しました。
12. 復元後の検証処理にも成功し、自動的にデータベースがオープンされ、従来どおりのツリーで動作するようになりました。

    ロールフォワードログはそのまま残っており、その場所を正しく指定したため、停止直前の状態に復元でき、検証も成功しました。
13. 復元後、ロールフォワードログに関する設定をやり直し、改めてフルバックアップを取っておきました。

    ロールフォワードログの機能は、復元処理の過程で無効に戻ってしまうため、ここで有効にする必要があります。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

サーバの稼動状況を調べ、正常に動作していることを確認しました。

シナリオ: 複数サーバ構成のネットワークで、1台のサーバが完全に使えなくなった場合

ユーザはGK Designs社で15台のサーバを管理しています。毎週土曜の夜にフルバックアップを取り、さらに毎晩、インクリメンタルバックアップを取っています。eDirectoryのバックアップ後すぐに、ファイルシステムバックアップによりテープに保存しています。

すべてのサーバがレプリカリングに参加しています。ロールフォワードログ機能は全サーバで有効です。

ある日、漏電による火事のため、ある支店のサーバが1台、完全に使えなくなってしまいました。幸い、このサーバのパーティションは、ひとつを除いてすべて、他のサーバにレプリカが作成されていました。ロールフォワードログ機能は有効にしていましたが、それも使えなくなってしまいました。したがって、停止直前の状態にまでeDirectoryデータベースを復元することはできません。

しかしバックアップファイルがあるので、サーバのeDirectory識別情報は再作成できます。復元にロールフォワードログは使えないので、他のサーバが想定している同期状態と合致しません(「452ページの「遷移ベクトルと復元後の検証処理」」を参照)。そのため復元の検証処理が失敗します。つまり、デフォルトで、復元処理が終わってもeDirectoryデータベースが開きません。

そこで、レプリカリングからいったんこのサーバを外し、DSRepairを使って、サーバの古くなったレプリカ情報をすべて外部参照に変え、それから最新のレプリカを保持しているサーバから複製することによって、このサーバに各パーティションの新しいコピーを追加しなおしました。具体的な手順は「478 ページの 「復元後の検証処理に失敗した場合の対処方法」」を参照してください。

レプリカが作られていなかったパーティションがひとつありました。これは、支店内にあるファックス/プリンタ複合機や大判カラープリンタなど、この支店内のネットワーク印刷オブジェクトを管理しているコンテナです。他のサーバにレプリカがないため、このパーティションは上述の手順では復元できません。このパーティションのオブジェクトはーから作り直さざるをえなかったので、将来に備え、これも他のサーバにレプリカを作っておくことにしました。

そこでロールフォワードログに関する設定をやり直し、改めてフルバックアップを取っておきました。ロールフォワードログの機能は、復元処理の過程で無効に戻ってしまうためです。

シナリオ: 複数サーバ構成のネットワークで、数台のサーバが使えなくなった場合

ユーザは3ヶ所に分けて設置された20台のサーバを管理しています。その1ヶ所で、水道管破裂による水漏れ事故のため、8台のうち5台が使えなくなってしまいました。

幸い、どのサーバについても、eDirectoryのバックアップを取っていました。しかし、すべてのサーバがレプリカリングに属しており、ロールフォワードログはなくなってしまったので、これを使わずにすべてをツリーに戻さなければなりません。最初にどのサーバから着手し、レプリカ間の不整合をどのように解消すればよいか、判断できませんでした。状況が複雑であるため、復元方法を決めるのにNetIQのサポート部門に相談することにしました。

シナリオ: 複数サーバ構成のネットワークで、すべてのサーバが使えなくなった場合

ユーザとそのチームは、Human Resource Consulting社で1ヶ所に設置された50台のサーバを管理しています。

普段から障害対策のため、ツリーの各パーティションについて3つずつレプリカを作成しています。したがって、サーバが1台停止しても、そのパーティションにあるオブジェクトは他のサーバからアクセスできます。さらに、サーバを個別に復元できるよう、バックアップツールで定期的にすべてのサーバをバックアップし、ロールフォワードログ記録を有効にし、そしてバックアップテープは別の建物に保管するように計画しました。

災害に備えるため、チームでは2台のサーバをDSMASTERとして割り当てています。2台を割り当てているのは、ツリーが大きすぎて、1台では全パーティションのレプリカを保持できないからです。ツリーに属するどのパーティションも、いずれかのDSMASTERサーバにレプリカが作成されています。逆に、同じパーティションのレプリカが2台のDSMASTERサーバに作成されることはないようにして、重複を避けています。これが災害対策として重要な点です。

さらにチームでは、テスト環境で定期的にバックアップファイルからの復元を試み、想定どおりに動作することを確認しています。

ある日、台風で社屋が倒壊し、データセンタにあったサーバもすべて壊れてしまいました。

台風が去った後、チームではまず、パーティションすべてのレプリカを保持する、2台のDSMASTERサーバを復元する作業に取りかかりました。最新のフルバックアップファイルおよびそれ以降のインクリメンタルバックアップファイルを使いましたが、ロールフォワードログは使いませ

んでした。サーバが壊れたときに、一緒になくなってしまったからです。DSMASTERサーバを設定する際、この2台が同じレプリカを共有することはないようにしていました。そのため、ロールフォワードログを適用しなくても、復元後の検証処理は問題なく成功したのです。DSMASTERサーバが復元されたことにより、Human Resources Consulting社のツリーに属するオブジェクトはすべてアクセスできるようになりました。

DSMASTERが復元できれば、整合性を損なうことなくツリー全体を再作成できるので、その役割は非常に重要です。

このチームは、ロールフォワードログの機能も有効にしていました。障害が発生する直前の状態にまでサーバを復元でき、レプリカリングに属する他のサーバとの同期状態に不整合が生じないからです。サーバが復旧し、他のサーバと通信できるようになると、停止していた間に行われた更新情報を自動的に受け取り、同期を取ることができます。

しかし今回はそのロールフォワードログを使えません。その場合、レプリカリングに属するサーバのうち、最初に復元処理を実施したものしか正常に復元できないことになります。それ以外のサーバは、他のサーバと同期状態が一致しないということで、復元後の検証処理に失敗してしまうのです(「452 ページの 「遷移ベクトルと復元後の検証処理」」を参照)。検証処理に失敗すると、このeDirectoryデータベースはアクティブになりません。

しかしこのチームは、このような状況もきちんと考慮していました。2台のDSMASTERサーバを設定し、重複して保持するパーティションがないようにして、これを復元作業の起点としたのです。重複がないので検証処理に失敗することはありません。これをマスタとして順次他のサーバにコピーしていけば、レプリカリング全体が復元できることになります。

DSMASTERサーバの復元後、他のサーバを復元するために、いくつか必要な作業があります。このチームは次のような手順で、他のサーバを順次復元していきました。

- DSMASTERサーバ上のレプリカを、マスタレプリカとして割り当てます。
- DSMASTER以外のサーバをレプリカリングから外します。
- フル/インクリメンタルバックアップファイルを使って、DSMASTER以外のサーバを復元します。

  ロールフォワードログがないため、復元後の検証処理に失敗することは分かっています。したがって、データベースは復元されても、まだアクティブになっていません。
- 高度な復元機能を使って、データベースをアクティブにしました。ロックはまだ解除しません。
- DSRepairを使って、他のサーバを参照してレプリカを作る設定に変更しました。
- データベースのロックを解除しました。

  この時点で、各サーバの識別情報は元どおりに戻っていますが、レプリカ情報を同期させようとはしません。他のサーバからレプリカのデータを受け取り、改めて構築できる状態になっています。
- 各サーバはDSMASTERサーバからデータを受け取り、自動的にレプリカを復元してレプリカリングに復帰します。

  各サーバにどのレプリカが置かれていたか、チームではきちんと把握していました。もっとも、最終バックアップ時点の状況は、バックアップファイルのヘッダを見れば確認できます。
- ロールフォワードログに関する設定をやり直し、改めてフルバックアップを取っておきました。ロールフォワードログの機能は、復元処理の過程で無効に戻ってしまうので、ここで有効にしたのです。改めてフルバックアップを取る必要があるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

具体的な手順は「478ページの「復元後の検証処理に失敗した場合の対処方法」」を参照してください。

かなりの作業量でしたが、ツリー自身は比較的早期に使用できるようになり、その時点でサーバ全体を復旧する目処も立っていました。

DSBKを使用した障害復旧計画

障害復旧計画を使用すれば、ディスクを破損した時点の環境設定に戻すことができます。オペレーティングシステムが破損した場合でもサーバを回復できるように、サーバのディスクをリモートの場所にバックアップしておく必要があります。

このセクションでは、eDirectoryサーバの障害復旧計画の例を示します。

- 488 ページの 「Linux上での障害復旧計画」
- 489 ページの 「Windows上での障害復旧計画」

Linux上での障害復旧計画

サーバのディスクのバックアップを取得するには:

1. DSBKを次のように設定します。
   - **1a** /etcでファイルdsbk.confを作成します。
   - **1b** 一時ファイルを作成します。例: /tmp/dsbk.tmp
   - **1c** 前のステップで作成した一時ファイルの場所を/etc/dsbk.confファイルの中で指定します。
2. サーバのディスクを読み書きモードでリモートマシンにマウントして、リモートマシンのディスク上のすべてのバックアップファイルを保存します。

   たとえば、「eDirServer# mount <remote machine IP>:/home/backup/ /mnt/dsbkBkp」と入力します。
3. 次のコマンドを使用してカスタムバックアップの場所を設定します。

   ```
   dsbk setconfig -L -T -r /mnt/dsbkBkp
   ```

   注: サーバ上の/opt/novell/eDirectory/binから、DSBKが実行することを確認します。
4. NICIと一緒にフルバックアップをリモートの場所のファイルシステムに取得します。

   ```
   dsbk backup -f <backup file location> -l <log file location> -e <password for NICI backup> -t -b
   ```

   たとえば、「dsbk backup -f /mnt/dsbkBkp/fb1.bak -l /mnt/dsbkBkp/fb1.log -e novell -t -b」と入力します。

   注: -eオプションは、NICIのバックアップに使用します。例では、novellがNICIバックアップ用のパスワードです。独自のパスワードを選択した場合は、NICIの復元でも同じパスワードを使用する必要があります。
5. 次のコマンドを使用して、インクリメンタルバックアップを取得します。

   ```
   dsbk backup -f <incremental backup file location> -l <incremental log file location> -t -i
   ```

   次に例を示します。

   1日目: dsbk backup -f /mnt/dsbkBkp/ib1.bak -l /mnt/dsbkBkp/ib1.log -t -i

2日目: dsbk backup -f /mnt/dsbkBkp/ib2.bak -l /mnt/dsbkBkp/ib2.log -t -i

注: インクリメンタルバックアップを取得中に、NICIをバックアップする必要はありません。

eDirectoryサーバが破損した場合は、リモートの場所のバックアップを使用してeDirectoryサーバを復旧するための次の手順を実行します。

1. オペレーティングシステムが破損した場合は、オペレーティングシステムをインストールし直します。
2. eDirectoryだけが破損した場合は、eDirectory RPMを削除することによって、eDirectory用のシステムのクリーンアップを実行します。
3. 前と同じeDirectoryをインストールして、1つのサーバダミーツリーを設定します。次に例を示します。

   ndsconfig new -t dummy_bkp_tree -n novell -a admin.novell -w novell
4. フルバックアップファイルからNICIを復元します(-d、-r、-a、-oオプションは使用しません)。

   dsbk restore -f <*backup file location*> -l <*log file location*> -e <*password used to NICI backup*>

   たとえば、「dsbk restore -f /mnt/dsbkBkp/fb1.bak -l /mnt/dsbkBkp/restore1.log -e novell」と入力します。
5. NICIの復元後に、eDirectoryサーバを再起動します。
6. フルバックアップファイルとインクリメンタルバックアップファイルの両方を復元します。次に例を示します。

   dsbk restore -f /mnt/dsbkBkp/fb1.bak -l /mnt/dsbkBkp/restore2.log -d /mnt/dsbkBkp/nds.rfl/ -r -a -e novell -o -i /mnt/dsbkBkp/ib1.bak, /mnt/dsbkBkp/ib2.bak

backupコマンドとrestoreコマンドの詳細については、「461 ページの 「Linux上でDSBKを使用する」」を参照してください。

Windows上での障害復旧計画

サーバのディスクのバックアップを取得するには:

1. サーバのディスクを読み書きモードでリモートマシンにマップします。たとえば、「O:\dsbkBkp」と入力します。
2. DSBKコマンドを実行するには:

   2a NDScons.exeを実行してeDirectoryサーバコンソールを開きます。

   2b ［**サービス**］タブで、［**dsbk.dlm**］をクリックします。

   2c ［**起動パラメータ**］フィールドに、DSBKコマンドを入力します。
3. 次のコマンドを使用してカスタムバックアップの場所を設定します。

   setconfig -L -T -r O:\dsbkBkp
4. NICIと一緒にフルバックアップをリモートの場所のファイルシステムに取得します。

   backup -f <*backup file location*> -l <*log file location*> -e <*password for NICI backup*> -t -b

注: -eオプションは、NICIのバックアップに使用します。例では、novellがNICIバックアップ用のパスワードです。独自のパスワードを選択した場合は、NICIの復元でも同じパスワードを使用する必要があります。

5 次のコマンドを使用して、インクリメンタルバックアップを取得します。

backup -f *<incremental backup file location>* -l *<incremental log file location>* -t -i

次に例を示します。

1日目: backup -f O:\dsbkBkp\ib1.bak -l O:\dsbkBkp\ib1.log -t -i

2日目: backup -f O:\dsbkBkp\ib2.bak -l O:\dsbkBkp\ib2.log -t -i

注: インクリメンタルバックアップを取得中に、NICIをバックアップする必要はありません。

eDirectoryサーバが破損した場合は、リモートの場所のバックアップを使用してeDirectoryサーバを復旧するための次の手順を実行します。

1 オペレーティングシステムが破損した場合は、オペレーティングシステムをインストールし直します。
2 eDirectoryだけが破損した場合は、eDirectory用のシステムのクリーンアップを実行します。
3 前と同じeDirectoryをインストールして、1つのサーバダミーツリーを設定します。
4 フルバックアップファイルからNICIを復元します(-d、-r、-a、-oオプションは使用しません)。

次に例を示します。

restore -f *<backup file location>* -l *<log file location>* -e *<password used for NICI backup>*

たとえば、「restore -f O:\dsbkBkp\fb1.bak -l O:\dsbkBkp restore1.log -e novell」と入力します。

5 NICIの復元後に、eDirectoryサーバを再起動します。
6 フルバックアップファイルとインクリメンタルバックアップファイルの両方を復元します。

次に例を示します。

restore -f O:\dsbkBkp\fb1.bak -l O:\dsbkBkp\restore2.log -d O:\dsbkBkp\nds.rfl\ -r -a -e novell -o -i O:\dsbkBkp\ib1.bak, O:\dsbkBkp\ib2.bak

backupコマンドとrestoreコマンドの詳細については、「463 ページの 「WindowsでDSBKを使用する」」を参照してください。

LDAPベースのバックアップ

LDAPベースのバックアップ機能を使用すると、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	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。

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。

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)

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。

16 Suite BモードでのeDirectoryの設定

Suite Bは、秘密または極秘レベルに分類されたトラフィックを市販品で保護できるようにするために国家安全保障局(NSA)によって標準化された暗号化アルゴリズムのセットです。Suite Bアルゴリズムは、パブリックネットワーク経由で渡される機密情報と非機密情報のセキュリティを確保する手段として機能します。

注: Suite B標準は変更される場合があります。NSAが今後推奨事項を変更する可能性があることを覚えておいてください。eDirectoryにおけるSuite Bのサポートは、NSAの推奨事項の弊社の解釈に基づきます。

Suite Bには、次の暗号化アルゴリズムが含まれています。

- 128ビット鍵または256ビット鍵を使用したAdvancedEncryptionStandard(AES)に基づく暗号化
- P-256曲線とP-384曲線上の楕円曲線デジタル署名アルゴリズム(ECDSA)を使用したデジタル署名
- P-256曲線とP-384曲線上の楕円曲線Diffie Hellman (ECDH)方式を使用した、事前に共有されたまたは動的な鍵交換
- セキュアハッシュアルゴリズム2 (SHA-256とSHA-384)に基づくハッシュ法(デジタル指紋法)

Suite Bの詳細については、「Suite B Cryptography」を参照してください。

eDirectoryでは、Suite Bモードで次のモジュールを個別に設定することができます。

モジュール	説明
NPKI (NetIQ Certificate Server)	Certificate Serverは、eDirectoryにネイティブに統合された公開鍵暗号サービスを提供します。このサービスを使用すれば、ユーザとサーバの両方の証明書を作成、発行、および管理することができます。これらのサービスにより、インターネットなどのパブリック通信チャネルを介した機密データの伝送を保護できます。 Suite BモードでCertificate Serverを設定すると、Certificate ServerはRFC 5759に準拠します。この標準では、Suite B証明書と証明書取り消しリスト(CRL)の基本プロファイルが規定されています。詳細については、495 ページの「Certificate Server上でのSuite Bの有効化」を参照してください。
LDAPサービスとHTTPサービス	LDAPサービスは、LDAPクライアントがeDirectoryに保存された情報にアクセスするためのサーバアプリケーションです。eDirectoryは、クロスプラットフォームの監視および診断機能を、HTTPサービスを利用しているeDirectoryツリー内のすべてのサーバに提供します。 SuiteBモードでこれらのサービスを設定すると、ECDSA証明書のサポートが追加され、RFC 6460で規定されたTLS 1.2暗号とSuite B Cipherの使用が強制されます。詳細については、496 ページの 「ECDSA証明書とSuite B Cipherを使用するためのLDAPサービスとHTTPサービスの設定」を参照してください。

モジュール	説明
NICI	NICIとは、鍵、アルゴリズム、さまざまな鍵保存/使用メカニズム、および大規模な鍵管理システムを提供する暗号化モジュールです。アプリケーションでのデータと鍵の安全な保存と転送を支援するために、NICIでは、3種類の鍵(鍵保管鍵、NICI Security Domain Infrastructure (SDI)鍵、およびセッション鍵)を提供しています。 Suite Bモードでサーバを設定すると、NICIは、256ビットAES鍵を使用してツリー内の機密データを保護します。たとえば、パスワードやチャレンジ/レスポンスデータを保護します。NICI 3.0にアップグレードすると、自動的に、鍵保管鍵とセッション鍵がSuite Bに準拠するように再作成されます。 eDirectoryは、ツリー鍵とも呼ばれるNICI SDI鍵を使用して、ローカルまたはリモートストレージのデータの暗号化に使用される鍵を安全にラップします。この鍵は、ツリー内のサーバがラップ解除できます。データは、eDirectoryの権限と組み合わせることによってセキュリティが確保されます。ツリー鍵は、ツリー内のすべてのサーバが使用できます。同じデータにアクセスするために、複数のサーバが同じNICI SDI鍵を使用します。そのため、この鍵はNICI 3.0のインストールでは自動的に作成されません。この鍵を手動で作成する必要があります。詳細については、499 ページの 「AES 256ビットSDI鍵の作成」を参照してください。
バックグラウンド認証メカニズム	TLS 1.2に基づく標準ベースのバックグラウンド認証メカニズムを、eDirectoryを使用したシングルサインオン認証に提供します。詳細については、499 ページの 「バックグラウンド認証の有効化」を参照してください。

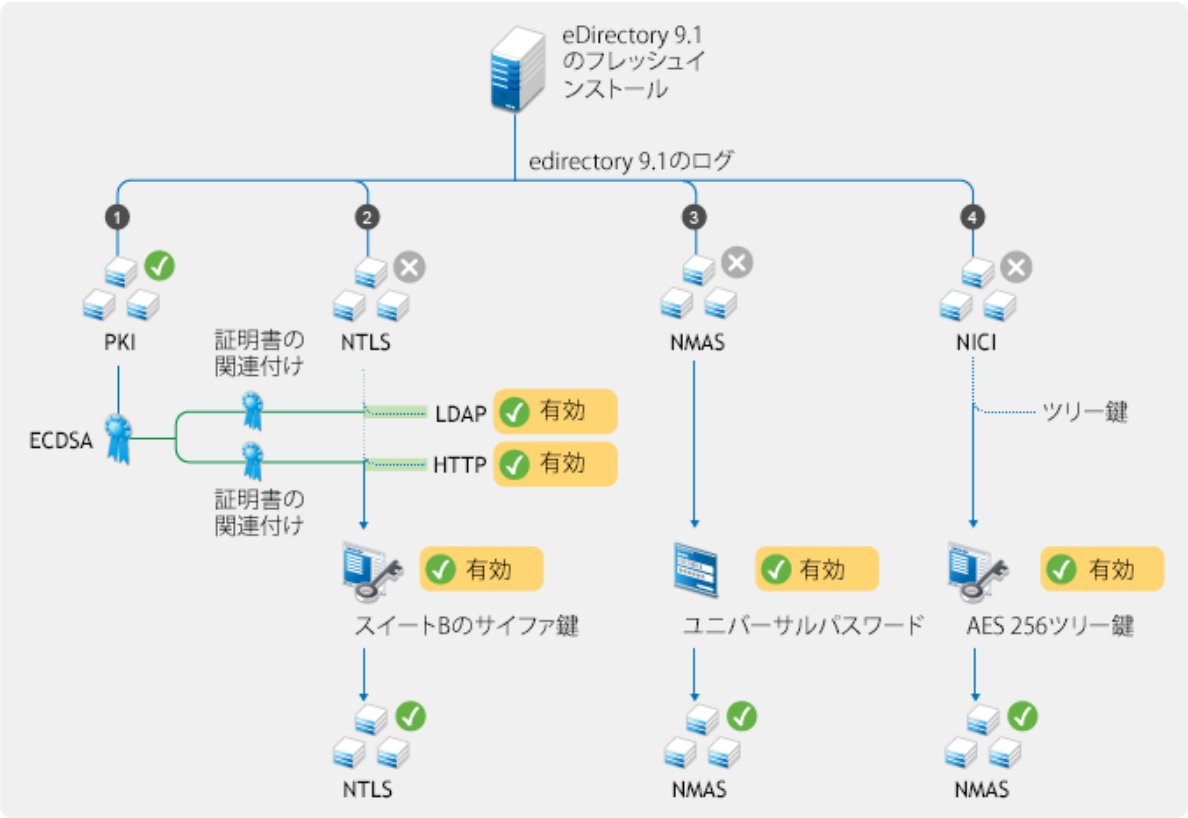
以下の各セクションで、Suite BモードでのeDirectoryモジュールの設定に関する情報について説明します。

- 494 ページの 「新規インストールでのSuite Bの有効化」
- 499 ページの 「既存のサーバ上でのSuite Bの設定」

新規インストールでのSuite Bの有効化

図 16-1に、新しいインストールで、eDirectoryコンポーネントに対してSuite Bを有効にするための一連のタスクを示します。

図16-1 新規インストールでのSuite Bの有効化



Certificate Server上でのSuite Bの有効化

新しいツリーを設定すると、Certificate Serverが、従来のRSA証明書に加えて、ツリー認証局(CA)用のP-384曲線上の自己署名ECDSA証明書を作成します。新しいサーバをツリーに追加するか、古いサーバをeDirectory 9.2にアップグレードすると、Certificate Serverがこれらのサーバにに対してECDSA証明書を発行します。

注: デフォルトで、NetIQ Certificate ServerはP-384曲線上のECDSA証明書を作成します。ただし、P-256曲線上のサーバ証明書を作成することもできます。

Suite Bを有効にせずにECDSA証明書だけを使用することができます。Suite Bの有効化は、RFC 5759に準拠するための追加のステップです。

CA Certificate ServerをSuite Bモードで動作するように設定するには、次の手順を実行します。

1. CA Certificate ServerのEnhanced Background Authenticationを設定します。

   詳細については、499 ページの 「バックグラウンド認証の有効化」を参照してください。
2. iManagerを起動します。
3. 適切な権利を持った管理者としてeDirectoryツリーにログインします。
4. ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**認証局の環境設定**］の順にクリックします。

5 ［**Enable Suite B Mode**］を選択します。

6 **OK**をクリックします。

CA Certificate ServerがSuite Bモードの場合は、認証局がRSA証明書の作成を許可しません。また、サーバの自動プロビジョニングでRSA証明書がこれ以上生成されません。新しいサーバを追加する場合は、サーバがEnhanced Background Authenticationを実行するように設定されていることを確認してください。

ツリー内のすべてのサーバまたはツリーに接続している任意の外部サービスがECDSAサーバ証明書の使用を開始したら、不要なRSA証明書を無効にしたり、削除したりできます。

注: eDirectory 8.8.8 Patch 6で導入されたFollow CAのアルゴリズム機能は、eDirectory 9.0以降では使用できなくなりました。代わりに、eDirectory 9.2サーバではRSA証明書にはSHA-256アルゴリズムを、ECDSA証明書にはSHA-384をデフォルトで使用します。

ECDSA証明書とSuiteBCipherを使用するためのLDAPサービスとHTTPサービスの設定

NTLS (NetIQ Transport Layer Security)は、FIPS準拠OpenSSLモジュールを通してTLS 1.2とSuite B暗号アルゴリズムをサポートします。FIPS準拠OpenSSLモジュールは、LDAP、httpstk (iMonitor)、NCPエンジンなどのeDirectoryコンポーネントで使用されます。詳細については、『*NetIQ eDirectoryインストールガイド*』の「FIPSモードでのeDirectoryの運用」を参照してください。

サーバ上でSuite Bモードを有効にする前に、サーバにECDSA証明書がインストールされており、eDirectory環境内のLDAPクライアント、LDAPブラウザ、およびWebブラウザがTLS1.2、ECDSA証明書、およびSuite B Cipherをサポートしていることを確認します。Suite BモードでLDAPインタフェースとHTTPSインタフェースを設定するには、必要なSuite Bモードでインタフェースを有効にして、該当するECDSAサーバ証明書をそれらに関連付けます。ツリー内のeDirectoryサーバごとにこの手順を繰り返します。サーバの暗号レベルとECDSAサーバ証明書を表示するには、サーバのLDAP設定オブジェクトとhttpstk設定オブジェクト(ldapServerとhttpServer)を使用します。

Suite BモードでLDAPサーバを設定するには:

1 適切な権利を持った管理者としてeDirectoryツリーにログインします。

2 ［**役割およびタスク**］メニューで、［**LDAP**］>［**LDAPオプション**］>［**LDAPサーバの表示**］の順にクリックして、Suite Bモードで設定するLDAPサーバオブジェクトを選択します。

3 ［**接続**］をクリックします。

4 ［**サーバ証明書**］パラメータで、LDAPサーバオブジェクトで使用する楕円曲線証明書をブラウズしてクリックします。

5 LDAPサーバオブジェクトに対して有効にするSuite Bモードに応じて、［**暗号化に際してのバインド制限**］ドロップダウンリストから値を選択します。

サイファに関するバインド制限	サイファスイート	説明
SuiteB Cipher (128ビット)を使用する	◆ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ◆ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	128ビットレベルのセキュリティを使用することで、Suite Bモードの操作を有効にします。このオプションを選択すると、eDirectoryは、ピア(任意のLDAPクライアント)による128ビットレベルと192ビットレベルの両方のセキュリティの使用を許可します。このオプションではECDSA256またはECDSA384のいずれかの証明書を使用できます。
SuiteB Cipher (128ビットのみ)を使用する	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	128ビットレベルのセキュリティを使用することで、Suite Bモードの操作を有効にします。このオプションを選択すると、eDirectoryは、ピア(任意のLDAPクライアント)による192ビットレベルのセキュリティの使用を許可しなくなります。 証明書チェーン内のすべての証明書でP-256曲線上のECDSA鍵を使用する必要があります。これは、サーバでは必須であり、クライアントではクライアント証明書の検証が有効になっている場合に適用されます。
SuiteB Cipher (192ビット)を使用する	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	192ビットレベルのセキュリティを使用することで、Suite Bモードの操作を有効にします。このオプションを選択すると、eDirectoryは、ピア(任意のLDAPクライアント)による192ビットレベルのセキュリティの使用のみを許可します。 証明書チェーン内のすべての証明書でP-384曲線上のECDSA鍵を使用する必要があります。これは、サーバでは必須であり、クライアントではクライアント証明書の検証が有効になっている場合に適用されます。

eDirectoryでは、ldapbindrestrictionsとサイファレベルの値を組み合わせて使用できます。詳細については、402 ページの 表 14-1を参照してください。

6 ［**適用**］をクリックしてから、［**OK**］をクリックします。

7 変更を有効にするには、次のいずれかの操作を実行します。

- eDirectoryを再起動します。
- LDAPサーバをアンロードしてロードします。

Suite BモードでHTTPSインタフェースを設定するには:

1 適切な権利を持った管理者としてeDirectoryツリーにログインします。

2 ［**役割およびタスク**］メニューで、［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。

3 変更するhttpサーバオブジェクトを選択するか、表示するhttpサーバオブジェクトをブラウズしてクリックします。

4 **OK**をクリックします。

5 ［**その他**］タブをクリックしてから、［**値がある属性**］リストから［httpBindRestrictions］を選択します。

6 **編集**をクリックします。

7 httpサーバオブジェクトに対して有効にするSuite Bモードに応じて、表示されたダイアログで値を4、5、または6に変更します。

サイファに関するバインド制限	サイファスイート	説明
4 - SuiteB Cipher (128ビット)を使用する	◆ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ◆ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	128ビットのセキュリティレベル(Suite B Cipher 128ビット)を使用して、Suite Bモード操作を有効にします。このオプションを選択すると、eDirectoryがクライアント(Webブラウザ)による128ビットと192ビットの両方のセキュリティレベルを許可します。このオプションではECDSA256またはECDSA384のいずれかの証明書を使用できます。
5 - SuiteB Cipher (128ビットのみ)を使用する	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	128ビットのセキュリティレベル(Suite B Cipher 128ビットのみ)を使用して、Suite Bモード操作を有効にします。このオプションを選択すると、eDirectoryがクライアント(Webブラウザ)による192ビットのセキュリティレベルを許可しません。 証明書チェーン内のすべての証明書でP-256曲線上のECDSA鍵を使用する必要があります。これは、サーバでは必須であり、クライアントではクライアント証明書の検証が有効になっている場合に適用されます。
6 - SuiteB Cipher (192ビット)を使用する	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	192ビットのセキュリティレベル(Suite B Cipher 192ビット)を使用して、Suite Bモード操作を有効にします。このオプションを選択すると、eDirectoryがクライアント(Webブラウザ)による192ビットのセキュリティレベルのみを許可します。 証明書チェーン内のすべての証明書でP-384曲線上のECDSA鍵を使用する必要があります。これは、サーバでは必須であり、クライアントではクライアント証明書の検証が有効になっている場合に適用されます。

8 ［適用］をクリックします。

9 ［**値がある属性**］リストからhttpKeyMaterialObjectを選択して、［**編集**］をクリックします。

10 HTTPSインタフェースで使用する楕円曲線証明書をブラウズして選択し、［**OK**］をクリックします。

11 **適用**をクリックし、**OK**をクリックします。

12 変更を有効にするためにeDirectoryを再起動します。

AES 256ビットSDI鍵の作成

デフォルトで、NICI SDI鍵は3DES鍵です。ただし、Suite Bモードをサポートするには、AES 256ビットNICI SDI鍵を手動で作成する必要があります。ツリー内のすべてのサーバがeDirectory 9.0以降の場合にのみ、この鍵を作成します。

KAP.Securityコンテナの書き込み可能なレプリカが保存されているサーバがeDirectory 9.2にアップグレードされた場合は、PKIヘルスチェックでこのコンテナにW1オブジェクトが作成されます。ツリー内のすべてのサーバがeDirectory 9.2にアップグレードされた場合は、ツリー管理者がAES 256ビットNICI SDIキーを作成できます。

AES 256ビットNICI SDI鍵を作成するには、『NICI Administration Guide (NICI管理ガイド)』の「Creating an AES 256-Bit Tree Key (AES 256ビットツリーキーを作成する」の手順に従ってください。

AES 256ビットNICI SDI鍵を使用したデータの再暗号化

NMASでは、NICI SDI鍵を使用して、パスワードとチャレンジ/レスポンス設定(質問と回答)が安全に保存されます。また、NMASには、NICISDI鍵を使用するユーザ固有の設定とメソッド固有の設定用の秘密の場所があります。大規模な展開で複数のユーザのパスワードを再暗号化するには、diagpwdユーティリティを使用します。詳細については、804 ページの 「ユニバーサルパスワードの診断ユーティリティ」を参照してください。

重要: eDirectory 9.0より前のバージョンのサーバがeDirectory環境に含まれている場合、それらのサーバはAES 256ビットのツリーキーを使用して暗号化されたパスワードや秘密データを復号化することができず、これらのサーバへのログインは失敗します。

バックグラウンド認証の有効化

eDirectoryは、アクセスを要求しているユーザの識別情報を検証する強力な認証メカニズムを提供します。EnhancedBackgroundAuthenticationの詳細については、「503ページの第17章「Enhanced Background Authenticationの有効化」」を参照してください。

既存のサーバ上でのSuite Bの設定

eDirectoryツリー内の既存のサーバ上でSuite Bを有効にするには、次の操作を実行します。

1. 認証局として機能するサーバをeDirectory 9.2にアップグレードします。

   認証局サーバをアップグレードすると、ECDSA自己署名認証局証明書が作成されます。他のサーバをeDirectory 9.2にアップグレードすると、新しい認証局がこれらのサーバにECDSA証明書を発行します。

2. ツリー内の必要なサーバをeDirectory 9.2にアップグレードします。

   アップグレードプロセスで、アップグレードされたサーバ用のECDSA証明書が生成されます。これらの証明書を使用して、LDAPおよびHTTPプロトコルスタックインタフェースをSuite Bモードにする必要があります。詳細については、496 ページの 「ECDSA証明書とSuite B CipherをするためのLDAPサービスとHTTPサービスの設定」を参照してください。

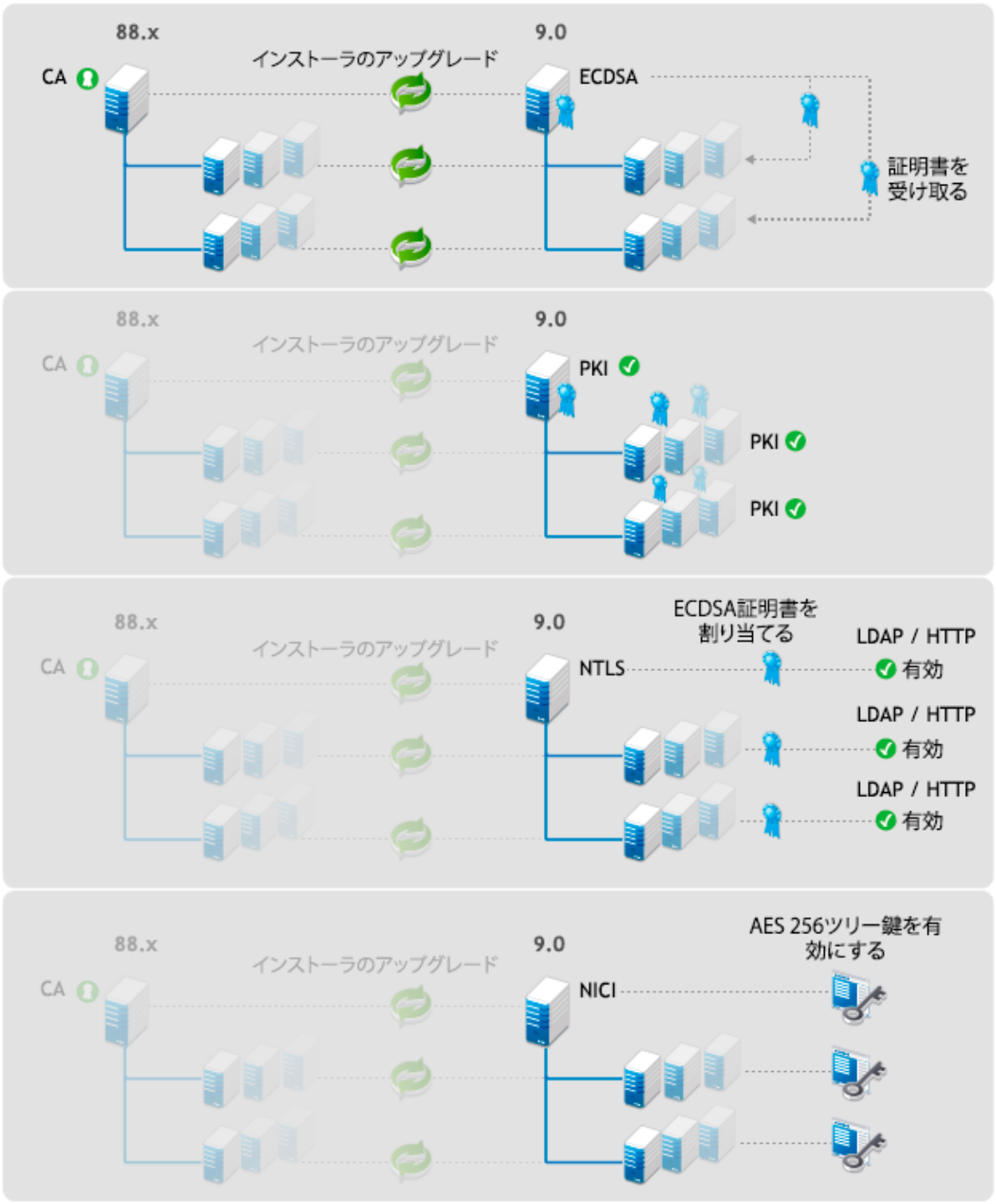
3 AES 256ビットSDI鍵を作成します。詳細については、499 ページの 「AES 256ビットSDI鍵の作成」を参照してください。

4 AES 256ビットNICI SDI鍵を使用してデータを再暗号化します。詳細については、499 ページの 「AES 256ビットSDI鍵の作成」を参照してください。

5 バックグラウンド認証を設定します。詳細については、503 ページの 「Enhanced Background Authenticationの有効化」を参照してください。

図 16-2に、eDirectoryのアップグレード時にSuite Bを有効にするため一連のタスクを示します。

図 16-2 eDirectoryのアップグレード時のSuite Bの有効化



17 Enhanced Background Authenticationの有効化

eDirectoryは、アクセスを要求しているユーザの識別情報を検証する強力な認証メカニズムを提供します。認証は2つのフェーズで構成されます。

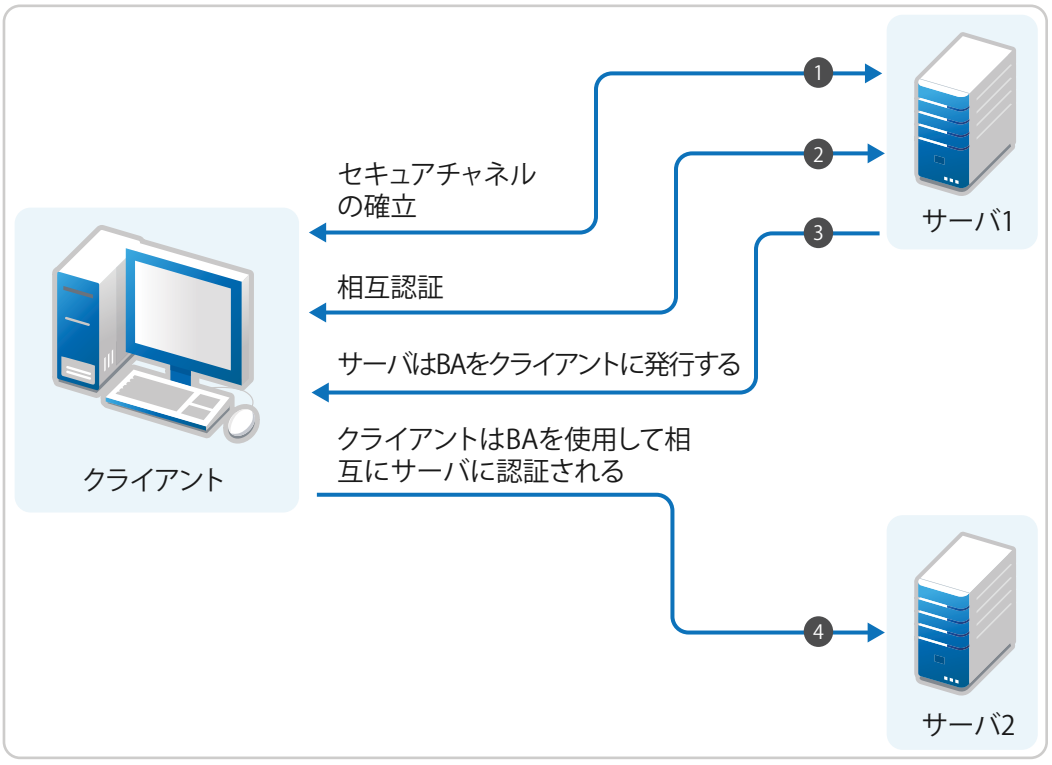
- ログイン
- バックグラウンド認証(BA)

ユーザがログインすると、NMAS (NetIQモジュラー認証サービス)が、ユーザの長期資格情報(パスワードなど)を検証して、BAマテリアルをユーザに発行します。

ツリー内の他のサーバに対する認証中に、ユーザがこのBAマテリアルを使用します。このeDirectoryのシングルサインオン機能を使用すれば、長期資格情報を再度入力しなくても、ツリー内の任意のサーバに対して認証できます。

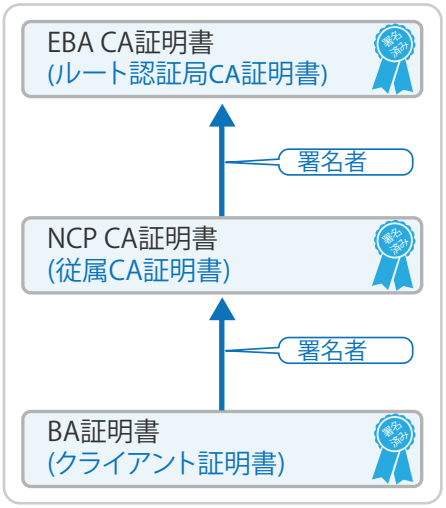
eDirectory 9.0では、専有のBAプロトコルの制限を解決できる標準ベースのBAプロトコルを導入しています。このプロトコルは、Enhanced Background Authentication (EBA)と呼ばれています。EBAが使用されている場合は、NMASがユーザにBAマテリアルとしてX.509認定を発行し、BAプロトコルが相互認証にTLSバージョン1.2を使用します。

図 17-1 *EBA プロセス*



EBA対応eDirectoryツリーでは、EBA CAがEBA用の信頼されたルート証明機関です。EBA CAでは自己署名証明書が使用されます。ツリールートパーティションの書き込み可能なレプリカをEBA CAとして使用して、ツリー内のサーバのいずれかを設定できます。通常は、ツリールートパーティションの書き込み可能なレプリカをホストするツリー内で設定され、EBAを使用して設定された最初のサーバがEBA CAとして機能します。また、ツリールートパーティションの書き込み可能なレプリカを含むツリー内の任意のeDirectory 9.2サーバをEBA CAとして機能するように設定することもできます。

図17-2 EBA認証局



ツリー内の各EBA対応サーバが、EBA CAに従属する認証局になり、NCP CAと呼ばれます。ログイン後に、NMASがNCP CAによって発行されたBA証明書をログインしているユーザに返します。

注: eDirectoryにログインするどのオブジェクトについても、オブジェクトDNのすべてのネーミング属性のOIDがスキーマに設定されている必要があります。

EBAを使用してeDirectoryサーバに対して認証するには、クライアントにツリーのEBA CA証明書が必要です。EBA CA証明書を取得するには、ebaclientinitユーティリティを使用します。これは、edirectory 9.0以降にパッケージ化されている新しいコマンドラインユーティリティです。このユーティリティは、ツリーのEBA CA証明書をダウンロードし、. eba.p12という名前のファイルに保存します。このファイルは、Linux上のユーザのホームディレクトリ($HOME)とWindows上のユーザのプロファイルディレクトリ(%USERPROFILE%)に存在します。

注: EBAを正しく機能させるためには、eDirectory環境内のすべてのEBA対応サーバとクライアント上の時刻を同期させます。

---

ebaclientinitユーティリティを複数のツリーに対して実行すると、eDirectoryツリーに関連付けられたEBA CA証明書が.eba.p12ファイルに追加されます。各eDirectoryツリー用のEBA CA証明書を取得するには、ツリーごとに1回ずつebaclientinitユーティリティを実行します。

EBAの有効化

このセクションでは、eDirectory上でEBAを有効にします。インストールのタイプに応じて、次のセクションのいずれかの手順に従います。

- 505 ページの 「eDirectoryツリー上でのEBAの有効化」
- 506 ページの 「eDirectoryサーバ上でのEBAの有効化」
- 507 ページの 「eDirectoryサーバ上でのEBAの無効化」

eDirectoryツリー上でのEBAの有効化

- 505 ページの 「新しいeDirectoryツリー上でのEBAの有効化」
- 505 ページの 「既存のツリー上でのEBAの有効化」

新しいeDirectoryツリー上でのEBAの有効化

新しいツリー上でEBAを有効にするには、プラットフォームに応じて、次の操作のいずれかを実行します。

- **Linux:** 新しいeDirectoryツリーを設定するときにEBAを有効にするには、コマンドラインで—configure–eba-now引数を指定してndsconfigコマンドを実行します。

  例: ndsconfig new —configure–eba-now *yes*

  この引数がコマンドに渡されなかった場合は、EBAを有効にするよう求めるプロンプトが表示されます。初期設定に基づいて、プロンプトで「**yes**」または「**no**」と入力します。
- **Windows:** インストールプログラムには、eDirectoryの環境設定中にEBAを有効にするオプションが用意されています。EBAを有効にするには、環境設定時に［**EBAを有効にする**］オプションを選択します。

注: eDirectoryでは、EBA対応サーバ上でebaext.dlmモジュールとebassl_srv.dlmモジュールの自動起動を設定することができません。これは、eDirectoryサーバ上でEBAが有効になっていると、DSモジュールが自動的にこれらのモジュールをロードするためです。

非EBA対応サーバ上でebaext.dlmモジュールとebassl_srv.dlmモジュールをロードしようとすると、モジュールは正常にロードされますが、EBA機能は使用できません。

既存のツリー上でのEBAの有効化

既存のeDirectoryツリー上でEBAを有効にするには、プラットフォームに応じて、次の操作のいずれかを実行します。

- **Linux:** ツリールートパーティションの書き込み可能なレプリカが保存されているサーバのいずれかで、—configure–eba-now引数を指定して、ndsconfig upgradeコマンドを実行します。

  例: ndsconfig upgrade —configure–eba-now *yes*
- **Windows:** ツリールートパーティションの書き込み可能なレプリカが保存されているサーバのいずれかのeDirectory 9.2インストールフォルダからeDirectory_910_Windows_x86_64.exeを実行し、eDirectoryの環境設定時に［**EBAを有効にする**］オプションを選択します。

eDirectoryサーバ上でのEBAの有効化

eDirectoryサーバ上でEBAを有効にすると、証明書署名要求(CSR)がEBA CAに送信されます。EBA CAは、CSRを検証して、アクセス制御チェックを実行してから、NCPCA証明書をサーバに発行します。サーバ上でEBAを有効にする前に、次のことを確認します。

- (必須)管理者DNを含むパーティションの書き込み可能なレプリカがツリー内のEBA対応サーバ上に存在する。
- (オプション)サーバオブジェクトを含むパーティションの書き込み可能なレプリカがツリー内のEBA対応サーバ上に存在する。サーバがこの条件を満たしていない場合、EBACAはCSRを保存し、NCP CA証明書を発行しません。これにより、eDirectoryの環境設定が失敗し、管理者がiManagerのEBAプラグインを使用してCSRを承認する必要があります。詳細については、509 ページの 「iManagerを使用したEBA CAの管理」を参照してください。CSRを承認したら、ndsconfig upgradeコマンドを実行することによってEBAを設定します。たとえば、「ndsconfig upgrade --configure-eba-now *yes*」と入力します。
- 506 ページの 「新しいサーバの追加時のEBAの有効化」
- 506 ページの 「設定済みのサーバ上でのEBAの有効化」

新しいサーバの追加時のEBAの有効化

新しいサーバをツリーに追加するときにEBAを有効にするには、プラットフォームに応じて、次の操作のいずれかを実行します。

- **Linux:** —configure–eba-now yes引数を指定して、*ndsconfig add*コマンドを実行します。

  例: ndsconfig add —configure–eba-now *yes*
- **Windows:** eDirectory 9.2のインストールフォルダからeDirectory_910_Windows_x86_64.exeを実行して、eDirectoryの環境設定時に［**EBAを有効にする**］オプションを選択します。

設定済みのサーバ上でのEBAの有効化

設定済みのサーバ上でEBAを有効にするには、プラットフォームに応じて、次の操作のいずれかを実行します。

- **Linux:** —configure–eba-now yes引数を指定して、*ndsconfig upgrade*コマンドを実行します。

  例: ndsconfig upgrade —configure–eba-now *yes*
- **Windows:** eDirectory 9.2のインストールフォルダからeDirectory_910_Windows_x86_64.exeを実行して、eDirectoryの環境設定時に［**EBAを有効にする**］オプションを選択します。

重要: EBA CAとして機能するサーバに加えて、ツリールートパーティションの読み書き可能レプリカを保存するEBA対応サーバを1台以上用意することをお勧めします。EBA CAとして機能するサーバがダウンした場合は、他のEBA対応サーバをEBA CAとして機能するように設定することができます。詳細については、511 ページの 「新しいサーバへのEBA CAの役割の移動」を参照してください。

---

eDirectoryサーバ上でのEBAの無効化

設定済みのサーバ上でEBAを無効にするには、プラットフォームに応じて、次の操作のいずれかを実行します。

- **Linux:**
  - EBAを無効にしてeDirectoryサーバを再起動するには、次のコマンドを実行します。

    ```
    ndsmanage stopall
    export DISABLE_EBA=true
    ndsmanage startall
    ```

  - EBAを有効にしてeDirectoryサーバを再起動するには、次のコマンドを実行します。

    ```
    ndsmanage stopall
    unset DISABLE_EBA
    ndsmanage startall
    ```

  注: RHEL 7.xプラットフォームとSLES 12.xプラットフォームの/etc/opt/novell/eDirectory/conf/ディレクトリに配置されたenvファイルにeDirectoryサービスに必要なすべての環境変数を追加する必要があります。

- **Windows:** ［**コントロールパネル**］>［**システム**］>［**システムの詳細設定**］>［**環境変数**］>［**システム変数**］>［**新規**］の順に移動します。 DISABLE_EBAという新しい変数を追加して、値1を設定し、サーバを再起動します。

重要: EBAを無効にするのはトラブルシューティングの場合だけにしてください。EBAをCAとして動作するeDirectoryサーバで7日以上EBAを無効にすると、eDirectoryツリーのEBA機能が切断されます。詳細については、TID 7017232を参照してください。

EBAに関する情報の表示

EBA対応サーバのさまざまな側面に関する情報を提供するツールとユーティリティを以下に示します。

ユーティリティ	説明
ndstrace	EBA要求の処理やNCPCA証明書の発行などのEBA操作に関する情報を提供します。この情報を表示するには、次の手順を実行します。 Linux上では、ndstraceのEBAタグを有効にします。 Windows上では、NDSCons.exeでEBAタグが有効になっているdstraceモジュールをロードします。
ndsd.log、dhost.log	EBA開始メッセージと停止メッセージに関する情報を提供します。この情報を表示するには、次の手順を実行します。 Linux上では、EBAを設定したサーバのndsd.logファイルを参照します。 Windows上では、この情報がdhost.logファイルに記録されます。

ユーティリティ	説明
ndscheck	サーバ上のEBAステータス(サーバがEBA対応かどうか)を提供します。 サーバがEBA対応の場合は、コマンドの出力にNCP CA証明書の有効性やサーバがEBACAとして機能しているかどうかなどの情報が表示されます。 ndscheckコマンドをリモートで実行する場合は、ツリーのEBA CA証明書がローカルコンピュータにダウンロードされていることを確認してください。詳細については、509 ページの 「ebaclientinitユーティリティの実行」を参照してください。
ndslogin	EBAの環境設定に関するトラブルシューティング情報を提供します。 EBAの環境設定をトラブルシューティングするには、-c引数を指定したndsloginコマンドを使用してeDirectoryにログインします。 例: ndslogin <admin DN> –p <password> –c ログインに成功するためには、ツリーのEBA CA証明書がローカルコンピュータにダウンロードされていることを確認してください。詳細については、509 ページの 「ebaclientinitユーティリティの実行」を参照してください。
schema.log	EBAが設定されているサーバのschema.logファイルに、EBAのスキーマ拡張に関する情報が書き込まれます。
nioutput.log	eDirectoryの環境設定時にEBAが選択されたかどうかを指定します。
iMonitor	iMonitorを使用すれば、EBA対応サーバで次の情報を監視することができます。 ◆ ［エージェント環境設定］ページの［接続情報］タブでEBA対応パラメータを確認することによって、サーバがEBA対応かどうかを判断します。このパラメータの値がtrueの場合は、サーバがEBA対応です。そうでない場合は、このパラメータの値がfalseになります。 ◆ Linux上のndstraceで表示可能なものと同じデバッグ情報を表示します。トレース設定ページに、この情報を表示するためのEBA用のタグが含まれています。 ◆ ［エージェントヘルス］ページで、EBACA証明書とNCPCA証明書の有効性、およびサーバのEBA対応ステータスに関する情報を表示します。これらの項目は、証明書が有効で、EBA属性が影響を受けていなければ、緑色で表示されます。 ◆ ［Verb統計情報］ページで、EBA対応サーバ上のEBA要求動詞を表示します。 ◆ ［iMonitor Health Check Agent］ページで以下を確認します。 ◆ サーバがEBA対応であるかどうか ◆ サーバがEBA CAをホストしているかどうか ◆ EBA CA証明書が有効かどうか ◆ NCP CA証明書が有効かどうか

iManagerを使用したEBA CAの管理

iManagerのEBAプラグインからeDirectoryにアクセスするには、EBA CA証明書をiManagerの信頼されたEBA証明書ストアに配置する必要があります。iManagerを実行しているコンピュータ上にEBA CA証明書をダウンロードするには、iManagerのインストールパッケージからebaclientinitユーティリティを実行します。詳細については、509 ページの 「ebaclientinitユーティリティの実行」を参照してください。

［EBA CA管理］ページを開くには、iManagerにログインして、トップバーで［**役割およびタスク**］アイコンをクリックし、［**役割およびタスク**］ビューを表示してから、左側のナビゲーションパネルで［**拡張バックグラウンド認証**］を選択します。［**EBA CA管理**］をクリックして、［EBA CA管理］ページを開きます。

［EBA CA管理］ページには、EBA CAのさまざまな側面を管理するための以下のタブが表示されます。

- **一般:** EBA CAのIPアドレスとその証明書を表示します。
- **発行された証明書:** NCP CA証明書をIPアドレスおよびポートとともに表示します。

  証明書を取り消すには、証明書を選択して[**取り消し**]をクリックします。証明書を無効にすると、NCPCA証明書を所有しているサーバが機能しなくなるため、このオプションは異常な状況以外は使用しないでください。証明書を無効にする必要があるのはサーバが侵害された場合などです。
- **CSR:** 管理者の承認が保留になっている証明書署名要求を列挙します。証明書署名要求を承認するには、リストから証明書を選択して、［**承認**］をクリックします。

ebaclientinitユーティリティの実行

EBA認証局証明書をコンピュータにダウンロードするには、ebaclientinitユーティリティを実行します。次の表は、ebaclientinitユーティリティで使用できるコマンドラインオプションの一覧です。

コマンドラインオプション	説明
--user-dn	ユーザのDN（ドット形式）。
--パスワード	EBA対応ユーザのパスワード。
--アドレス	ツリー内のNCPサーバのアドレス。構文は<IP address>:<port>です。

たとえば、ebaclientinit --mechanism ebatls --user-dn john.foo.org --password p@$$w0rd --address 111.111.11.1:524

プラットフォームに応じて、次のいずれかの方法を使用してebaclientinitを実行します。

Linux: iManagerはLinuxではnovlwwwユーザとして実行されます。このため、ebaclientinitは、次のコマンドを使用してnovlwwwユーザとして実行してください。

```
sudo -u novlwww -H LD_LIBRARY_PATH=/var/opt/novell/iManager/nps/WEB-INF/bin/linux/
:/opt/netiq/common/openssl/lib64/ /var/opt/novell/iManager/nps/WEB-INF/bin/linux/
ebaclientinit --mechanism ebatls
```

Windows: 次の操作を実行します。

1. iManagerがインストールされているサーバにログインします。
2. C:\Program Files\Novell\Tomcat\webapps\nps\WEBINF\bin\windows\ebaclientinit.exe --mechanism ebatls からebaclientinitを実行します。

   これにより、ユーザのホームディレクトリに.eba.p12ファイルが格納されます。
3. .eba.p12ファイルをC:\Users\novlwwwにコピーします。

注: iManager 3.0 SP1以前を使用している場合は、.eba.p12ファイルを C:\Windows\System32\config\systemprofileにコピーします。Windows上ではTomcatが Systemユーザとして動作するため、この操作を実行する必要があります。

注: iManagerが.eba.p12ファイルでツリー用のEBA CA証明書を見つけられなかった場合、または .eba.p12ファイルが存在しない場合は、iManagerのEBAプラグインから、EBA CAとして機能する サーバのsadmin資格情報を入力するように要求されます。ただし、sadmin資格情報の使用はお勧めできません。

EBAが有効な場合のeDirectory操作の制限

パーティションのマスタ読み書き可能レプリカが保存されているサーバがEBA対応の場合は、そのパーティションもEBA対応と見なされます。eDirectoryでは、パーティションを非EBA対応にする操作が禁止されます。EBA対応サーバでは、パーティションとレプリカに対する操作に次の制限が加えられます。

- 510 ページの 「レプリカタイプの変更に関する制限」
- 511 ページの 「パーティションのマスタの変更に関する制限」
- 511 ページの 「パーティションのマージに関する制限」
- 511 ページの 「EBAが有効になっているサーバの再設定に関する制限」

レプリカタイプの変更に関する制限

- EBACAをホストしているサーバにツリールートパーティションのマスタレプリカが保存されている場合は、eDirectoryがそのレプリカタイプの変更を許可しません。
- EBACAがツリールートパーティションの読み書き可能レプリカが保存されているサーバによってホストされている場合は、レプリカタイプをマスタ以外に変更しないでください。レプリカタイプを［読み込み専用］/［フィルタ済み読み込みのみ］に変更すると、ツリー全体で EBA機能が停止する可能性があります。eDirectoryは、ツリールートパーティションのマスタレプリカが保存されているeDirectoryサーバがEBA対応の場合にこの制限を適用します。

注: 従来のサーバとeDirectory 9.2サーバが混在する環境では、レプリカタイプの変更に成功する場合があります。ただし、これを行うと、EBA機能が停止する可能性があります。

パーティションのマスタの変更に関する制限

パーティションのマスタレプリカがEBA対応サーバ上に存在する場合は、次の操作が失敗します。

- マスタの役割を非EBA対応サーバに移動する。
- サーバがEBA CAとして機能している場合に、マスタの役割を他のサーバに移動する。

パーティションのマージに関する制限

親パーティションが非EBA対応で、子パーティションがEBA対応の場合は、この2つのパーティションをマージしないでください。これを行うと、EBA機能が停止する可能性があります。

EBAが有効になっているサーバの再設定に関する制限

eDirectoryがEBA対応モードのサーバ上で設定されている場合は、この設定がnds.confファイルのn4u.server.eba_enabledパラメータに保存されます。eDirectoryがこのサーバ上で設定解除されてから再び設定された場合は、デフォルトでEBAがオンになります。非EBAモードでサーバを設定するには、サーバ上でeDirectoryを設定する前に、nds.confファイルからこのパラメータを削除します。

EBA対応サーバのバックアップ

EBA対応eDirectoryサーバをバックアップする場合は、「Backing Up and Restoring NetIQ eDirectory」の手順に従ってください。EBA対応サーバのインクリメンタルバックアップまたはフルバックアップを取得するときに、NICI属性とストリーム属性が選択されていることを確認します。そうでない場合は、サーバを復元することができません。

新しいサーバへのEBA CAの役割の移動

EBA CAとして機能しているサーバがダウンした場合は、eDirectoryがツリー内の別のEBA対応サーバにEBA CAの役割を移動できる柔軟性を提供します。EBA CAの役割を新しいサーバに移動する前に、新しいサーバが以下の状態になっていることを確認します。

- EBA対応である。
- EBACAがダウンした時点ですでにレプリカが作成されていたツリールートパーティションの書き込み可能なレプリカが保存されている。

Linuxオペレーティングシステム上の新しいサーバにEBA CAの役割を移動するには、新しいサーバ上のbashシェルから次のコマンドを実行します。

```
ndstrace -c "config ebassl_srv seize_ebaca"
```

eDirectoryには、EBA CAの役割が新しいサーバに移動されたことを示す成功メッセージが表示されます。オリジナルのサーバがまだ機能しているときにこの操作を試すと、失敗します。

Windowsでは、次の手順を実行します。

1. ndscons.exeを開きます。
2. ［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。
3. ［サービス］タブで、ebassl_srv.dlmまでスクロールしてから、［起動パラメータ］フィールドに「seize_ebaca」と入力します。
4. ［設定］をクリックします。

EBACAの役割の転送に関するメッセージを表示するには、EBACA役割の転送操作実行時に、EBAタグを有効にしてdstrace.dlmを実行します。DSTraceに、操作の成功または失敗に応じて適切なメッセージが表示されます。オリジナルのサーバがまだ機能しているときにこの操作を試すと、失敗します。

注

- EBACAの役割が正常に取得されたかどうかを判断するには、新しいサーバ上でndscheckを実行します。ndscheckの出力に「EBACA=true」と表示された場合は、新しいサーバがツリーのEBACAになっています。
- EBACAをホストしているサーバがダウンした場合は、ツリールートパーティションのレプリカリング内の他のサーバをEBACAとして指定します。ダウンしたサーバにツリールートパーティションのマスタレプリカが保存されていた場合は、EBACAとして機能している新しいサーバにマスタの役割を移動することをお勧めします。マスタの役割を移動するには、341 ページの「レプリカの修復」の手順に従います。

---

18 NetIQ eDirectoryのSNMPサポート

SNMP(SimpleNetworkManagementProtocol)は、インターネットを介してデバイスを操作および保守するための標準的なプロトコルです。管理コンソールアプリケーションと管理対象デバイスは、このプロトコルに従って管理情報をやり取りします。管理コンソールアプリケーションとは、IBM Tivoli NetViewやSolstice SunNet Managerなどのアプリケーションを指します。管理対象デバイスには、ホスト、ルータ、ブリッジ、ハブのほかに、NetIQ eDirectoryなどのネットワークアプリケーションも含まれます。

この章では、NetIQ eDirectoryのSNMPサービスについて説明します。この付録には以下のトピックがあります。

SNMPに関する用語の定義

この章で使われる用語の定義を次の表に示します。

用語集	定義
EMANATE	SNMP Research International, Inc.の製品。Enhanced MANagement Agent Through Extensionsの略称です。
［SNMP］	Simple Network Management Protocolの略。ネットワークの稼動状況に関するデータをやり取りするためのプロトコルです。
NAA	Native Agent Adapterの略。ネイティブエージェントアダプタ。
NMS	ネットワーク管理ステーション
MA	Management Agent
SA	サブエージェント
MIB	Management Information Base
NCP	NetWare/Novell Core Protocol
NMA	Network Management Applicationの略。ネットワーク管理アプリケーション。
edir.mib	NetIQ eDirectoryサーバの監視に使うMIBのこと。NetIQ eDirectoryに関するMIBオブジェクトおよびトラップが設定されています。

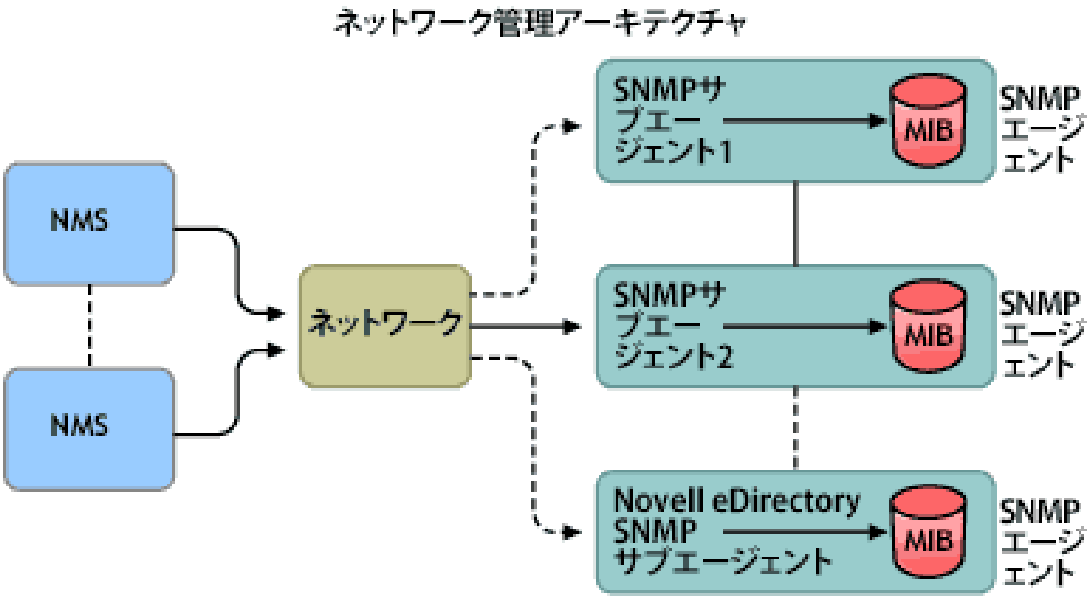
用語集	定義
トラップ	eDirectoryイベントがサーバ上で発生したときに、管理対象デバイス上のエージェントが発する警告のこと。警告を発する条件は、NetIQが提供するMIB(管理情報ベース)で定義されています。

SNMPサービスについて

SNMPは「マネージャ/エージェント」アーキテクチャにもとづくプロトコルです。SNMPを使用して行われるネットワーク管理のアーキテクチャは、次のような要素から成ります。

- NMS(Network Management Station)
- 管理対象デバイス
- マスタエージェント
- サブエージェント
- MIB(Management Information Base)
- ネットワーク管理プロトコル

図18-1 ネットワーク管理アーキテクチャ



ネットワーク管理ステーション

ネットワーク管理ステーション(NMS)とは、ネットワーク管理アプリケーションがインストールされたワークステーションのことです。管理対象デバイスに関する情報をグラフィック表示します。

NMSには次のような機能があります。

- ネットワーク管理システム全体のユーザインタフェースを提供します。この機能により、ネットワーク管理の強固さ、柔軟性、および使いやすさが決まります。

- SNMPGet、GetNext、SNMPGetResponse、およびSetの操作はここから実行します。また、ネットワーク上の管理対象デバイスから送られてくるSNMPトラップを捕捉するのも、やはりNMSの役割です。
- 1つ以上のネットワーク管理アプリケーション(NMA)を同時に監視します。NMSは、管理対象デバイス、テーブルの表示、およびログ記録に関する情報を図を使って表示する機能を備えています。
- NMSに組み込まれているMIBコンパイラで、MIBファイルをコンパイルすることができます。

管理対象デバイス

SNMPがインストールされているデバイスは、すべて管理対象デバイスとして扱うことができます。ホスト、ルータ、ブリッジ、ハブなどが管理対象デバイスになります。NMSは管理対象デバイスを監視し、またデバイスと通信します。

NMSと管理対象デバイスとの間では、サブエージェントおよびマスタエージェントという2種類のエージェントを介して情報をやり取りします。

サブエージェント

サブエージェントには、管理対象デバイスに関する情報を集め、マスタエージェントに渡す役割があります。

マスタエージェント

マスタエージェントには、さまざまなサブエージェントとNMSの間で情報を交換する役割があります。マスタエージェントは、通信相手のサブエージェントと同じホスト上で動作します。

Management Information Base

SNMPでは、プロトコルデータ単位(PDU: Protocol Data Unit)という形でネットワーク情報を交換します。PDUには、管理対象デバイスに保存されている変数に関する情報が含まれています。この変数のことを管理オブジェクトと言い、その値とオブジェクト名がNMSに渡されます。管理オブジェクトはすべて管理情報ベース(MIB)に定義されています。MIBはツリー状の階層構造で表される仮想データベースです。

SNMPのネットワーク管理プロトコル

SNMPの基本関数を次の表に示します。

機能	説明
取得	マネージャがエージェントに情報を要求するために使用します。
Get Next	配列や表から情報を取得する際にマネージャが使用します。
Get Response	マネージャから問い合わせを受けたエージェントが、それに応答するために使用します。
設定	エージェント側のMIBにある変数の値を変更するために、マネージャが使用します。
Trap	あるイベントが発生した際、エージェントがマネージャに通知するために使用します。

SNMPの詳細については、次のWebサイトを参照してください。

- NET-SNMPのホームページ (http://net-snmp.sourceforge.net)
- SNMP FAQ (http://www.faqs.org/faqs/snmp-faq/part1)
- RFC 1157 (http://www.ietf.org/rfc/rfc1157.txt)
- SNMPLink (http://www.snmplink.org)
- SNMPInfo (http://www.snmpinfo.com)
- SNMP RFC Standard MIBs and Informative Links (http://www.wtcs.org/snmp4tpc/snmp_rfc.htm)
- RFC 2605 (http://www.ietf.org/rfc/rfc2605.txt?number=2605)

eDirectoryとSNMP

eDirectoryには、ユーザ、アプリケーション、ネットワークデバイス、データなど、数多くのオブジェクトを格納し、管理することができます。eDirectoryで管理するオブジェクトが増えてくると、オブジェクトの追加や変更に追随する必要性も増してきます。この問題を解決する手段としてSNMPを使用することで、ユーザはeDirectoryサーバを監視し、変化に追随できるようになります。

eDirectoryの管理にSNMPを使う利点

- eDirectoryサーバをリアルタイムに監視
- サードパーティ製SNMP MIBブラウザからeDirectoryを監視
- eDirectoryが正常に稼動しているか、状況を追跡可能
- 起こりうる問題を検知時に特定し、対処が可能
- トラップや統計に関する設定により、対象を選択して監視可能
- eDirectoryに対するアクセス状況をグラフ表示
- SNMPで収集した履歴データを格納し、分析可能
- SNMPのGet要求、GetNext要求を使った統計機能にも対応
- プラットフォームを選ばずSNMPネイティブマスタエージェントを使用可能

eDirectoryでのSNMPの機能について

SNMPをeDirectoryに実装すると、アクセス状況、稼動状況、エラー、キャッシュ性能に関するeDirectoryの統計情報を取得できます。また、イベントが発生するとSNMPからトラップが送信されます。トラップや統計情報はMIBに定義されています。

注: これらの属性へのアクセスには常にセキュリティ保護されたチャネルを使用すると指定している場合は、暗号化された属性へアクセスする際にセキュリティ保護されたチャネル以外は使用できない可能性があります。詳細については、313 ページの 「暗号化属性」を参照してください。

ディレクトリサービス監視MIB

eDirectoryのMIBには、eDirectoryを監視するための統計情報やトラップが定義されています。このMIBには次のoid(オブジェクトID)が割り当てられています。

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).novell(23).mibDoc(2).ndsMIB(98)

［Statistics (統計情報)］

eDirectory MIBは、管理対象オブジェクトを次の4つの異なるテーブルに分けて格納しています。

- **キャッシュデータベース統計テーブル - ndsDbCacheTable:** ディレクトリサーバに関する記述と、サーバにキャッシュされたエントリに関する統計情報の要約を格納します。
- **設定データベース統計テーブル - ndsDbConfigTable:** ディレクトリサーバに関する記述と、サーバで設定されたエントリに関する統計情報の要約を格納します。
- **プロトコル統計テーブル - ndsProtoIfOpsTable** ディレクトリサーバのアプリケーションプロトコルインタフェースごとに、アクセス状況、稼動状況、エラーに関する統計情報の要約を格納します。
- **相互通信統計テーブル - ndsServerIntTable** 監視対象ディレクトリが通信した、あるいは通信を試みたディレクトリサーバを、最新の「N」回分記録しておきます。「N」はローカルで定義する定数です。

注: 統計情報の詳細については、546 ページの 「［Statistics (統計情報)］」を参照してください。

トラップ - ndsTrapVariables

eDirectory MIBには119種類のトラップが定義されています。そのうち117種類はeDirectoryのイベントにマップされています。ほかにndsServerStartおよびndsServerStopというトラップがあり、これはSNMPサブエージェントが直接生成します。この2つのトラップは設定できません。

注: トラップの詳細については、「525 ページの 「トラップ」」を参照してください。

統計情報とトラップの詳細については、「edir.mib」を参照してください。

edir.mibは次のディレクトリにあります。

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

SNMPグループオブジェクト

SNMPグループオブジェクトは、eDirectory SNMPトラップの設定や管理に使います。インストールの過程で、「SNMPGroup*server_name*」という名前のSNMPグループオブジェクトが作られます(ここで*server_name*は、eDirectoryのSNMPサービスをインストールしたサーバ名を表します)。このSNMPグループオブジェクトが作られるのは、サーバオブジェクトと同じコンテナ内です。SNMP設定ユーティリティは、SNMPトラップの設定に使います。

Windowsの場合

SNMPグループオブジェクトを作るには、次のコマンドを実行してください。

rundll32 snmpinst, snmpinst -c <createobj> -a <*userFDN*> -p <*password*> -h <*hostname or IP address*>

パラメータ	説明
-c <*createobj*>	オブジェクトの作成を示すトラップコマンド。
-a <*userFDN*>	管理者権利を持つユーザの完全識別名。
-p <*password*>	認証に使うuserFDNパスワード
-h <*hostname or IP address*>	DNSホスト名またはIPアドレス。

例:

rundll32 snmpinst, snmpinst -c createobj -a admin.mycontext -p mypassword -h 160.98.146.26

SNMPグループオブジェクトを削除するには、次のコマンドを実行してください。

rundll32 snmpinst, snmpinst -c <*deleteobj*> -a <*userFDN*> -p <*password*> -h <*hostname or IP address*>

パラメータについてはオブジェクトを作る場合と同様です。

例:

rundll32 snmpinst, snmpinst -c deleteobj -a admin.mycontext -p mypassword -h 160.98.146.26

Linuxの場合

SNMPグループオブジェクトを作るには、次のコマンドを実行してください。

ndsconfig add -m <*modulename*> -a <*userFDN*>

例:

ndsconfig add -m snmp -a admin.mycontext

eDirectoryのSNMPサービスのインストールと設定

SNMP service for eDirectoryは、eDirectoryをインストールする際に組み込まれます。eDirectoryのSNMPサービスのデフォルト設定の変更にはiManagerを使います。詳細については、521 ページの 「ダイナミック設定」を参照してください。

SNMP Group-Objectという名前の新しいオブジェクトが、eDirectoryのインストール時に、ディレクトリツリーに追加されます。このオブジェクトはNetIQ eDirectory SNMPトラップの設定や管理に使います。詳細については、517 ページの 「SNMPグループオブジェクト」を参照してください。

eDirectoryがインストールされたWindowsにSNMPを組み込む手順

eDirectoryのインストール時にSNMPサービスを除外した場合は、SNMPサブエージェント用ファイルがコピーされるだけで、レジストリは元のままになっています。

あとになってSNMPサービスが必要になった場合は、次のコマンドでレジストリを更新してください。

rundll32 snmpinst, snmpinst -c createreg

SNMPサーバモジュールのロードとアンロード

SNMPサーバモジュールは手動でロード、アンロードできます。デフォルトでは、どのプラットフォームでも、自動でロードされるようになっています。ただし、WindowsとLinuxでは手動でサーバモジュールをロードできます。

SNMPサーバモジュールをロードするには、次のコマンドを入力します。

サーバ	コマンド
Windows	［DHOST (NDSCONS)］画面で、［**ndssnmp.dlm**］を選択し、［**開始**］をクリックします。
Linux	DHOSTのリモート管理ページで、NetIQ eDirectory SNMPトラップサーバの開始用操作アイコンをクリックすると、SNMPトラップサーバがロードされます。 または プロンプトで、次のコマンドを入力します。 `/opt/novell/eDirectory/bin/ndssnmp -l`

SNMPサーバモジュールをアンロードするには、次のコマンドを入力します。

サーバ	コマンド
Windows	［DHOST (NDSCONS)］画面で、［**ndssnmp.dlm**］を選択し、［**停止**］をクリックします。
Linux	DHOSTのリモート管理ページで、**NetIQ eDirectory 9.2 SNMPトラップサーバ**の停止用操作アイコンをクリックすると、SNMPトラップサーバがアンロードされます。 または プロンプトで、次のコマンドを入力します。 `/opt/novell/eDirectory/bin/ndssnmp -u`

サブエージェントの設定

- 519 ページの 「スタティック設定」
- 521 ページの 「ダイナミック設定」

スタティック設定

スタティック設定は、サブエージェントを実際に稼動させる前に行います。WindowsまたはLinux上では、ndssnmp.cfgファイルを編集することによって手動で設定できます。ndssnmp.cfgファイルは次のディレクトリに配置されています。

Windows: *install_directory*\SNMP\

Linux: /etc/opt/novell/eDirectory/conf/ndssnmp/

注: ndssnmp.cfgファイルに変更を加えた場合は、サブエージェントを再起動する必要があります。

サブエージェントの設定は、次のような書式で記述してください。

- INTERACTIVE *status*

  ここで*status*には、「on」または「off」を指定します。「on」を指定すると、サブエージェント起動時にユーザ名とパスワードを要求されるようになります。ステータスが「off」の場合は、ユーザ名とパスワードがセキュリティで保護されたストアから取得されます。デフォルト=オフ.

  例:

  INTERACTIVE on

  INTERACTIVE off

- INTERACTION *value*

  ここで*value*は、インタラクション表のエントリ数を表します。範囲は1～10です。デフォルトは4です。

  例:

  INTERACTION 4

  INTERACTION 2

- MONITOR *status*

  ここで*status*には、「on」または「off」を指定します。デフォルト=オン.

  例:

  MONITOR on

  MONITOR off

- SSLKEY *certificate_file*

  ここで*certificate_file*は、証明書のエクスポート先パスを表します。このとき、エクスポートした証明書が実際に存在しているパスを指定してください。

  例:

  SSLKEY /home/guest/snmp-cert.der (Linux)

  SSLKEY c:\home\guest\snmp-cert.der (Windows)

  注: 共通の証明書を受け入れない複数のインスタンスを監視している場合は、このオプションがサポートされません。

- SERVER *hostname/IP_address:NCP_port*

  ここで*hostname*は、eDirectoryサーバをインストールし、設定したホスト名を表します。指定できるのは、ローカルにインストールしたサーバに限ります。この指定は必須です。指定がなければどのサーバも監視の対象になりません。デフォルト: ローカルサーバのホスト名。

  例:

  SERVER myserver

  SERVER myserver:1524

Linux上でeDirectoryのインスタンスが複数存在する場合、監視するすべてのeDirectoryサーバを次のように指定できます。

SERVER myserver:1524

SERVER myserver:2524

SERVER myserver:6524

注: このコマンドで、コロン(:)の前後にはスペースを入れないでください。

ダイナミック設定

ダイナミック設定は、ディレクトリサービスの稼動中、いつでも次のいずれかの方法で実行できます。

コマンドライン

トラップ設定用のコマンドラインユーティリティを使って、eDirectoryのSNMPトラップを設定できます。

次のような操作が可能です。

- トラップの有効化と無効化
- トラップインターバルの設定
- エラートラップの有効化と無効化
- 有効なトラップ、無効なトラップ、またはすべてのトラップの一覧表示

注: 詳細については、539 ページの 「トラップに関する設定」を参照してください。

iManagerプラグインによる設定

トラップの設定には、NetIQ iManagerを使う方法もあります。NetIQ iManagerはブラウザベースのツールで、eDirectoryオブジェクトを運用、管理、設定するために使用します。NetIQ iManagerを使用すると、ユーザに特定のタスクや責任を割り当てたり、それらのタスクを実行するために必要なツールおよびそれに伴う権利だけを付与したりすることができます。

1. NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**SNMP**］>［**SNMPの概要**］の順にクリックします。
3. ［**SNMPグループオブジェクトを表示**］をクリックして、設定するSNMPグループオブジェクトの名前をクリックします。
4. 一般ページまたはトラップページで、必要なパラメータを設定します。
5. ［**適用**］をクリックし、［**OK**］をクリックすると、今設定した内容が保存されます。

注: 詳細については、NetIQ iManagerのオンラインヘルプを参照してください。

eDirectoryのSNMPサービスの設定

このセクションでは、次のプラットフォーム上でeDirectoryのSNMPサービスをセットアップする方法について説明します。

- 522 ページの 「Windows」
- 523 ページの 「Linux」

eDirectoryのSNMPサービスの設定は、次の手順で行います。

1. マスタエージェントの設定
2. マスタエージェントの起動
3. サブエージェントの設定
4. サブエージェントの起動

Windows

- 522 ページの 「マスタエージェントの設定」
- 522 ページの 「マスタエージェントの起動」
- 523 ページの 「マスタエージェントの停止」
- 523 ページの 「サブエージェントの起動」

マスタエージェントの設定

注: SNMPマスタエージェントは、eDirectoryのインストールに先立って組み込んでおく必要があります。詳細については、「Microsoft SNMP Services (http://technet.microsoft.com/en-us/library/bb726977.aspx)」を参照してください。

---

1 ［Microsoft SNMP Properties］ダイアログボックスを開き、［**エージェント**］タブをクリックします。

2 接続先および場所に関する情報を入力してください。

3 ［トラップ］タブをクリックし、コミュニティ名およびトラップの送り先に関する情報を入力します。

3a コミュニティ名を入力し、［**追加**］をクリックします。

3b トラップの送り先のコンピュータのIPアドレスまたはホスト名を入力してください。

3c ［**追加**］ボタンを押すと、ここで入力したIPアドレスまたはホスト名が追加されます。

4 ［**デスクトップとの対話をサービスに許可する**］オプションを有効にします。

このオプションが無効のままだと、Windows上のSNMPには接続できません。

Windowsプラットフォーム上: ［**スタート**］>［**設定**］>［**コントロール パネル**］>［**管理ツール**］>［**サービス**］の順にクリックします。［**SNMP**］を右クリックし、［**プロパティ**］を選択します。［**ログオン**］タブで、［**デスクトップとの対話をサービスに許可する**］を選択します。

マスタエージェントの起動

1 マスタエージェントを起動するには、次の操作を実行します。

［スタート］>［設定］>［コントロール パネル］>［管理ツール］>［サービス］>［SNMP］>［開始］の順にクリックします。

2 コマンドプロンプトで次のコマンドを入力します。

Net start SNMP

マスタエージェントの停止

マスタエージェントを停止するには、次のいずれかの操作をしてください。

1 ［スタート］>［設定］>［コントロール パネル］>［管理ツール］>［サービス］>［SNMP］>［停止］の順にクリックします。

2 コマンドプロンプトで次のコマンドを入力します。

Net stop SNMP

サブエージェントの起動

Windowsの場合、マスタエージェントを起動すると、サブエージェントも自動的に起動されます。

重要: 最新の ServicePackは、 SNMPサービスのインストール後にインストールする必要があります。

Linux

Linuxの場合は、net-snmpをインストールしておく必要があります。デフォルトで、ほとんどのLinuxシステムにインストールされています。

Linux上でのSNMPサービスのセットアップ

- 523 ページの 「マスタエージェントの設定」
- 524 ページの 「マスタエージェントの起動」
- 524 ページの 「サブエージェントの起動」
- 524 ページの 「サブエージェントの停止」

マスタエージェントの設定

Linux上でマスタエージェントを設定するには、「523 ページの 「snmpd.confの変更」」の説明に従ってsnmpd.confファイルを変更します。

snmpd.confファイルは、SLES上の/etc/snmpディレクトリとその他のLinuxプラットフォーム上の/etcディレクトリに配置されています。

snmpd.confの変更

snmpd.confファイルに、次の行を入力します。

```
trapsink myserver public
```

ここで*myserver*は、トラップの送り先ホスト名を表します。

snmpd.confファイルに、次の行を追加します。

```
master agentx
```

また、次のように変更してください。

元の記述	変更後の記述
com2sec notConfigUser default public	com2sec demouser default public
group notConfigGroup v1 notConfigUser	group demogroup v1 demouser
view systemview included system	view all included .1
access notConfigGroup "" any noauth exact systemview none none	access demogroup "" any noauth exact all all all

上記の内容がsnmpd.confファイルに存在しない場合は追加してください。

重要: 設定ファイルを書き替えた場合、マスタエージェントとサブエージェントを再起動する必要があります。

マスタエージェントの起動

マスタエージェントを起動するには、次のコマンドを実行してください。

/usr/sbin/snmpd -C -c /etc/snmpd.conf

注: SLES 12以上でマスタエージェントを開始するには、/etc/init.d/snmpd startコマンドを実行します。

サブエージェントの起動

サブエージェントを起動するには、次のコマンドを実行してください。

/etc/init.d/ndssnmpsa start

プロンプトが表示されたら、ユーザ名とパスワードを入力します。正常に認証されれば、/etc/opt/novell/eDirectory/conf/ndssnmp/ndssnmp.cfgファイルでINTERACTION = ONという設定になっている場合、次のようなメッセージが表示されます。

```
Do you want to remember password? (Y/N)
```

ここで「Y」と入力すると、パスワードが保存されます。次回からは、パスワードを入力することなくサブエージェントを起動できます。

「N」と入力した場合は、次回からもパスワードを求められます。

注: サーバがダウンすると、マスタエージェントとサブエージェントもダウンします。したがって、サーバのリブート時にマスタエージェントとサブエージェントを開始するには、次のコマンドを実行します。

```
chkconfig snmpd on
chkconfig ndssnmpsa on
```

サブエージェントの停止

サブエージェントを停止するには、次のコマンドを実行してください。

/etc/init.d/ndssnmpsa stop

SNMPによるeDirectoryの監視

eDirectoryの動作を監視するために、SNMPの機能であるトラップや統計を使うことができます。

ただし、そのためには、NCPサーバ、LDAPグループ、LDAPサーバオブジェクトに対して、次のような権利が必要です。

- NCPサーバオブジェクトに対するスーパバイザ権
- LDAPグループオブジェクトの「LDAPクリアテキストパスワードを許可する」属性に対する読み出し権利
- LDAPサーバオブジェクトのLDAP TCP Port属性、LDAP SSL Port属性に対する読み出し権利

通常、管理者としてログインしたユーザならば、SNMPによりeDirectoryサーバを監視する上で問題が生じることはありません。

トラップ

ndsServerStart (2001)およびndsServerStop (2002)を設定できなかったトラップの中から、119個のトラップがSNMPコンポーネントによって生成されます。これらのトラップはデフォルトで有効です。

トラップの生成状況はMIBブラウザで確認できます。

トラップ番号	トラップ名	生成される条件
1	ndsCreateEntry	新規オブジェクトがディレクトリに追加されたとき。 例: LDAPツール、ICE、iManagerなどを使ってオブジェクトを削除したとき。
2	ndsDeleteEntry	オブジェクトが削除されたとき。 例: LDAPツール、ICE、iManagerなどを使ってオブジェクトを削除したとき。
3	ndsRenameEntry	オブジェクト名が変更されたとき。 例: LDAPツール、ICE、iManagerなどを使ってオブジェクト名を変更したとき。
4	ndsMoveSourceEntry	オブジェクトのコンテキストが変わったとき。このトラップにより、変更前のコンテキストが通知されます。 例: ldapmodrdnやldapsdkでオブジェクトを移動したとき。

トラップ番号	トラップ名	生成される条件
5	ndsAddValue	オブジェクトの属性値が追加されたとき。 例: LDAPツール、ICE、iManagerなどを使って、属性に新しい値を追加したとき。 **注:** 返される値がNULLの場合は、セキュリティ保護されたチャネルを経由してディレクトリにアクセスする必要があります。詳細については、539 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。
6	ndsDeleteValue	オブジェクトの属性値が削除されたとき。 例: LDAPツール、ICE、iManagerなどを使って、属性値を削除したとき。 **注:** 返される値がNULLの場合は、セキュリティ保護されたチャネルを経由してディレクトリにアクセスする必要があります。詳細については、539 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。
7	ndsCloseStream	ストリーム属性が変更されたとき。
8	ndsDeleteAttribute	オブジェクトの属性値(単一値と定義されているもの)が削除されたとき。 例: LDAPツール、ICE、iManagerなどを使って、属性値を削除したとき。 **注:** 返される値がNULLの場合は、セキュリティ保護されたチャネルを経由してディレクトリにアクセスする必要があります。詳細については、539 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。
9	ndsCheckSecurityEquiv	あるエントリの同等セキュリティベクトルが検査されたとき。 例: LDAPツール、ICE、iManagerなどを使って、同等セキュリティ属性を変更したとき。
10	ndsUpdateSecurityEquiv	あるエントリの同等セキュリティベクトルが変更されたとき。 例: LDAPツール、ICE、iManagerなどを使って、同等セキュリティ属性を変更したとき。
11	ndsMoveDestEntry	オブジェクトのコンテキストが変わったとき。このトラップにより、変更後のコンテキストが通知されます。 例: ldapmodrdnやldapsdkでオブジェクトを移動したとき。

トラップ番号	トラップ名	生成される条件
12	ndsDeleteUnusedExtref	バックリンクオブジェクトが削除されたとき。
13	ndsAgentOpenLocal	ローカルディレクトリエージェントがオープンされたとき。 例: 標準修復を実行したとき。
14	ndsAgentCloseLocal	ローカルディレクトリエージェントがクローズされたとき。 例: 標準修復を実行したとき。
15	ndsDSABadVerb	DSAgent要求に関連づけられたバーブ番号が正しくないとき。 例: DClient呼び出しを使って、eDirectoryに不正なバーブ要求を送ったとき。
16	ndsMoveSubtree	コンテナオブジェクトがそれに含まれるオブジェクトと共に移動されたとき。 例: LDAPツール、ICE、またはiManagerを使って、パーティションを他のコンテキストに移動したとき。
17	ndsNoReplicaPointer	レプリカにレプリカポインタが関連づけられていないとき。
18	ndsSyncInEnd	インバウンド同期が終了したとき。
19	ndsBacklinkSecurEquiv	バックリンク操作により、オブジェクトの同等セキュリティベクトルが更新されたとき。 例: LDAPツール、ICE、iManagerなどを使って、同等セキュリティ属性を変更したとき。
20	ndsBacklinkOperPrivChg	バックリンク操作により、オブジェクトのコンソールオペレータ権利が変更されたとき。
21	ndsDeleteSubtree	コンテナオブジェクトがそれに含まれるオブジェクトと共に削除されたとき。
22	ndsReferral	参照が作成されたとき。
23	ndsUpdateClassDef	スキーマクラス定義が更新されたとき。 例: 新規クラスまたは属性をプライマリサーバに追加し、セカンダリサーバ側で、LDAPツール、ICE、iManagerなどを使って同期を取ったとき。
24	ndsUpdateAttributeDef	スキーマ属性定義が更新されたとき。 例: 新規属性をプライマリサーバに追加し、セカンダリサーバ側で、LDAPツール、ICE、iManagerなどを使って同期を取ったとき。

トラップ番号	トラップ名	生成される条件
25	ndsLostEntry	eDirectoryのローカルサーバには存在しないはずのエントリに対する更新要求があったとき。■分節拡張■■分節統合■
26	ndsPurgeEntryFail	パージ処理に失敗したとき。
27	ndsPurgeStart	パージ処理を開始したとき。 例: DSTraceを実行し、ndstrace=*jを設定したとき。
28	ndsPurgeEnd	パージ処理が終了したとき。 例: DSTraceを実行し、ndstrace=*jを設定したとき。
29	ndsLimberDone	limber処理が終了したとき。 例: 一定時間の経過後にリンバを起動するようにDSTraceを設定したとき。
30	ndsPartitionSplitDone	パーティション分割処理が終了したとき。 例: iManagerを使用して、パーティションを作成したとき。
31	ndsSyncServerOutStart	ある特定のサーバに同期するアウトバウンド同期処理が起動されたとき。 例: 一定時間の経過後にアウトバウンド同期処理を開始するようにDSTraceを設定したとき。
32	ndsSyncServerOutEnd	ある特定のサーバに同期するアウトバウンド同期処理が終了したとき。 例: 一定時間の経過後にアウトバウンド同期処理を停止するようにDSTraceを設定したとき。
33	ndsSyncPartitionStart	パーティション同期処理が起動されたとき。 例: あるコンテナをパーティション分割したとき。
34	ndsSyncPartitionEnd	パーティション同期処理が終了したとき。 例: あるコンテナをパーティション分割したとき。

トラップ番号	トラップ名	生成される条件
35	ndsMoveTreeStart	サブツリーの移動処理が起動されたとき。 パーティションの移動に伴い、サブツリーも移動します。 例: iManagerを使用して、パーティションを作成し、それを他のコンテナに移動したとき。
36	ndsMoveTreeEnd	サブツリーの移動処理が終了したとき。 パーティションの結合処理に伴い、サブツリーも移動します。 例: iManagerを使用して、パーティションを作成し、それを他のコンテナに移動したとき。
37	ndsJoinPartitionDone	パーティションの結合処理が終了したとき。 例: iManagerを使用して、パーティションを作成し、それを他のパーティションとマージしたとき。
38	ndsPartitionLocked	パーティションがロックされたとき(結合処理の際など)。 例: iManagerを使用して、パーティションを作成したとき。
39	ndsPartitionUnlocked	パーティションのロックが解除されたとき(結合処理が終了したときなど)。 例: iManagerを使用して、パーティションを作成したとき。
40	ndsSchemaSync	スキーマの同期処理が起こったとき。 例: ldapsdk schsyncを使用してスキーマの同期処理をスケジュールしたとき。
41	ndsNameCollision	他のサーバにある別のオブジェクトと名前が重複(衝突)したとき。 例: iMonitorを使い、プライマリサーバとセカンダリサーバのアウトバウンド同期処理を無効にした状態で、LDAPツールを使って両サーバにユーザオブジェクトを作成したとします。こうしておいて、iMonitorでアウトバウンド同期処理を実行すると、衝突が起こります。

トラップ番号	トラップ名	生成される条件
43	ndsChangeModuleState	eDirectoryモジュール(NLM/DLM)がロードまたはアンロードされたとき。 例: nldapモジュールをロードまたはアンロードしたとき。
44	ndsLumberDone	バックグラウンドでのlimber処理が始まったとき。
45	ndsBacklinkProcDone	バックリンク処理が終了したとき。 例: 一定時間の経過後にバックリンクを起動するようにDSTraceを設定したとき。
46	ndsServerRename	サーバ名が変更されたとき。 例: ldapmodrdnまたはldapsdkを使って、サーバ名を変更したとき。
47	ndsSyntheticTime	将来のタイムスタンプを付与したオブジェクトが作成されたとき。eDirectoryサーバの同期に際しては、合成時刻として扱うことになります。 例: ndsconfigを使って、セカンダリサーバをツリーに追加したとき。
48	ndsServerAddressChange	limber処理によりサーバ参照が変更されたとき。 例: サーバのIPアドレスを変更してndsdを再起動したとき。
49	ndsDSARead	エントリが読み出されたとき。 eDirectoryを対象とする操作があれば、必ずこのトラップが生成されます。 例: ldapsearchを実行したとき。
50	ndsLogin	eDirectoryへのログインがあったとき。 例: ndsloginを使ってツリーにログインしたとき。
51	ndsChangePassword	パスワードが変更されたとき。 例: ldapmodifyを使ってユーザオブジェクトのパスワードを変更したとき。

トラップ番号	トラップ名	生成される条件
52	ndsLogout	eDirectoryからログアウトされたとき。 例: Novell Clientからツリーへの接続を切ったとき。
53	ndsAddReplica	サーバパーティションにレプリカが追加されたとき。 例: ndsconfigを使ってツリーに新規レプリカを追加したとき。
54	ndsRemoveReplica	レプリカが削除されたとき。 例: iManagerを使って、あるサーバからレプリカを削除したとき。
55	ndsSplitPartition	パーティションが分割されたとき。 例: iManagerを使用して、パーティションを作成したとき。
56	ndsJoinPartition	ペアレントパーティションにチャイルドパーティションが結合されたとき。 例: iManagerを使用してパーティションを作成し、結合したとき。
57	ndsChangeReplicaType	パーティションレプリカのタイプが変更されたとき。 例: レプリカタイプをマスタから読み書き用に変更したとき。
58	ndsAddEntry	新規オブジェクトが追加されたとき。 例: iManagerを使って、ユーザオブジェクトを追加したとき。
59	ndsAbortPartitionOp	パーティションに関する処理が中断されたとき。 例: コンテナのパーティション分割処理を実行し、途中で中断したとき。
60	ndsRecvReplicaUpdates	同期処理中に、レプリカ側で更新通知を受け取ったとき。 例: 複数サーバツリーセットアップ内のeDirectoryサーバが、保存されているレプリカに対する更新を要求したとき。この操作はiManagerで実行できます。

トラップ番号	トラップ名	生成される条件
61	ndsRepairTimeStamps	レプリカのタイムスタンプが修復されたとき。 例: DSRepair (Linuxの場合はndsrepair、Wiindowsの場合はNSDCons)を使って、タイムスタンプのDIB修復処理を実行したとき。
62	ndsSendReplicaUpdates	同期処理中にレプリカが更新されたとき。 例: 複数のサーバツリーから成る構成のeDirectoryサーバで、レプリカを保持しているサーバに対して更新要求を送った場合。この操作はiManagerで実行できます。
63	ndsVerifyPass	パスワードが正しいと確認されたとき。 例: 無効になったパスワードを変更する際、確認のために入力させた旧パスワードが正しいと確認されたとき。
64	ndsBackupEntry	エントリがバックアップされたとき。 例: バックアップユーティリティ(Linuxの場合はndsbackup、Windowsの場合はNDSCons)を使って、Directoryオブジェクトをバックアップしたとき。
65	ndsRestoreEntry	エントリが復元されたとき。 例: バックアップユーティリティ(Linuxの場合はndsbackup、Windowsの場合はNDSCons)を使って、バックアップされていたDirectoryオブジェクトを復元したとき。
66	ndsDefineAttributeDef	スキーマに属性定義が追加されたとき。 例: eDirectoryツリースキーマに属性定義を追加して拡張したとき。ZENWorks®やNMAS™などのeDirectory依存アプリケーションをインストールすると、スキーマを拡張できます。また、iManagerまたはLinux上のスキーマ拡張ユーティリティndsschを使って拡張することもできます。
67	ndsRemoveAttributeDef	スキーマから属性定義が削除されたとき。 例: eDirectoryツリースキーマから属性定義を削除したとき。属性は、iManagerまたはLinux上のスキーマ拡張ユーティリティndsschを使って削除できます。

トラップ番号	トラップ名	生成される条件
68	ndsRemoveClassDef	スキーマからクラス定義が削除されたとき。 例: eDirectoryツリースキーマからオブジェクトクラス定義を削除したとき。これは、iManagerまたはLinux上のスキーマ拡張ユーティリティndsschを使って削除できます。
69	ndsDefineClassDef	スキーマにクラス定義が追加されたとき。 例: eDirectoryツリースキーマにクラス定義を追加して拡張したとき。ZENWorks、NMASなどといったeDirectory用アプリケーションをインストールすると、スキーマは拡張されます。また、iManagerまたはLinux上のスキーマ拡張ユーティリティndsschを使って拡張することもできます。
70	ndsModifyClassDef	クラス定義が変更されたとき。 例: 既存のオブジェクトクラスや属性定義を変更したとき。
71	ndsResetDSCounters	eDirectoryに内蔵されたカウンタがリセットされたとき。
72	ndsRemoveEntryDir	エントリに関連づけられたディレクトリが削除されたとき。
73	ndsCompAttributeValue	属性値が比較されたとき。 例: 属性値を他のオブジェクトの属性値と比較したとき。ユーザオブジェクトを対象とするLDAP検索により、入力された値と電話番号が一致するかどうか検査するような場合。
74	ndsOpenStream	ストリーム属性がオープンまたはクローズされたとき。 例: ストリームを読み込みまたは書き込み操作用に作成またはオープンしたとき。ユーザオブジェクト用のログインスクリプトを作成したとき。DIBディレクトリ以下にファイルが生成される結果、このトラップが発生します。
75	ndsListSubordinates	コンテナオブジェクトに対して、それに含まれるエントリのリストを取得する処理が実行されたとき。この処理では、コンテナオブジェクトの直下にあるエントリのみが検索の対象となります。 例: iManagerを使って、コンテナオブジェクトをクリックすることにより、これに含まれるオブジェクトを一覧表示しようとしたとき。

トラップ番号	トラップ名	生成される条件
76	ndsListContainerClasses	エントリに対して、これを含めることができるクラスのリストを取得する処理が実行されたとき。 例: あるオブジェクトについて、これを含めることができるクラス(コンテナクラス)を一覧表示しようとしたとき。 ユーザオブジェクトを含めることができるコンテナクラスを検索すれば、Organization(組織)、Organization Unit(部署)、Domain(ドメイン)などといったクラスが表示されるはずです。
77	ndsInspectEntry	エントリの検査処理が実行されたとき。 例: あるエントリについて、これまでにエラーが発生したことがあるかどうかを検査しようとしたとき。バックグラウンドでeDirectoryのフラットクリーナ処理を実行する際にこのイベントが発生する結果、トラップが送られることになります。
78	ndsResendEntry	エントリの再送信処理が実行されたとき。 例: レプリカの作成処理中に、エントリの再送信が起こったとき。サーバ間の接続に問題があり、オブジェクトの送信に失敗したような場合に起こります。
79	ndsMutateEntry	エントリの変換処理が実行されたとき。 例: バインダリオブジェクトクラスからユーザオブジェクトクラスに変換したとき。
80	ndsMergeEntries	2つのエントリがマージされたとき。 例: 2つのユーザオブジェクトをマージしたとき。Entry2 (ndsEntryName2)をEntry (ndsEntryName)にマージしたとき。
81	ndsMergeTree	2つのeDirectoryツリーがマージされたとき。 例: DSMerge(Linuxの場合はndsmerge、Windowsの場合はNDSCons)を使って、2つのeDirectoryツリーをマージしたとき。
82	ndsCreateSubref	サブオーディネートリファレンスが生成されたとき。 例: チャイルドパーティションのレプリカをサーバから削除したとき。自動的にサブオーディネートリファレンスのレプリカが生成され、その結果トラップが発生します。

トラップ番号	トラップ名	生成される条件
83	ndsListPartitions	パーティションのリスト取得処理が実行されたとき。 例: iManagerを使い、パーティションビューやスキーマビューでeDirectoryサーバオブジェクトをクリックすることにより、サーバ上のパーティションを一覧表示したとき。
84	ndsReadAttribute	属性値が読み出されたとき。 例: ツリーの検索処理を実行したとき。
85	ndsReadReferences	エントリの参照が読み出されたとき。
86	ndsUpdateReplica	パーティションレプリカに対して、レプリカの更新処理が実行されたとき。 例: あるサーバからユーザを削除したとき。この削除操作に対して他のレプリカが更新されます。
87	ndsStartUpdateReplica	パーティションレプリカに対して、レプリカの更新開始処理が開始されたとき。 例: あるサーバからユーザを削除したとき。この削除操作に対して他のレプリカが更新されます。
88	ndsEndUpdateReplica	パーティションレプリカに対して、レプリカの更新処理が実行され、終了したとき。 例: あるサーバからユーザを削除したとき。この削除操作に対して他のレプリカが更新されます。
89	ndsSyncPartition	パーティションレプリカに対して、パーティションの同期処理が実行されたとき。 例: あるパーティションからユーザを削除したとき。DSTraceを使うと同期処理の状況を見ることができます。
90	ndsSyncSchema	ルートのマスタレプリカが、そのスキーマをサーバと同期させる要求を受け取ったとき。 例: iManager、LDAPツール、またはndsschユーティリティを使用して、新規クラスを追加したとき。

トラップ番号	トラップ名	生成される条件
91	ndsCreateBackLink	バックリンクが生成されたとき。ローカルに存在しないオブジェクトが参照された場合に、バックリンクが作成されます。 例: マルチサーバシナリオで、複数のユーザを含むパーティションを作成したとき。サーバの1つからこのパーティションを削除すると、サブオーディネートリファレンスが生成されます。このとき、削除されたパーティションに存在していたユーザを参照するバックリンクが生成されます。
93	ndsChangeTreeName	ツリー名が変更されたとき。 例: マージユーティリティDSMerge/ndsmergeを使ってツリー名を変更したとき。
94	ndsStartJoinPartition	パーティションの結合処理が始まったとき。 例: LDAPツールを使って、パーティションをマージまたは結合したとき。
95	ndsAbortJoinPartition	パーティションの結合処理が中断されたとき。 例: LDAPツールを使って、パーティションをマージまたは結合したとき。
96	ndsUpdateSchema	スキーマ更新処理が実行されたとき。 例: iManager、LDAPツール、またはndsschを使用して、新規クラスを追加したとき。
97	ndsStartUpdateSchema	スキーマ更新処理が開始されたとき。 例: iManager、LDAPツール、またはndsschを使用して、新規クラスを追加したとき。
98	ndsEndUpdateSchema	スキーマ更新処理が終了したとき。 例: iManager、LDAPツール、またはndsschを使用して、新規クラスを追加したとき。
99	ndsMoveTree	ツリー移動処理が実行されたとき。 例: パーティションをあるコンテナから別のコンテナに移動したとき。

トラップ番号	トラップ名	生成される条件
101	ndsConnectToAddress	特定のアドレスとの間で接続が確立されたとき。 例: iManagerを使用して、ツリーをブラウズしたとき。
102	ndsSearch	検索処理が実行されたとき。 例: LDAPツールを使ってツリーに対するldapsearchを実行したとき。
103	ndsPartitionStateChange	パーティションが作成または削除されたとき。 例: 新規パーティションを作成する.
104	ndsRemoveBacklink	使われていない外部参照が削除され、該当するオブジェクトを保持しているサーバに対して、バックリンク削除要求が送られたとき。
105	ndsLowLevelJoinPartition	パーティションの結合処理中に、低レベルの結合処理が実行されたとき。 例: iManagerまたはLDAPツールを使って、パーティションをマージまたは結合したとき。
106	ndsCreateNameBase	eDirectoryネームベースが作成されたとき。
107	ndsChangeSecurityEquals	同等セキュリティ属性が変更されたとき。 例: iManagerを使って、任意のユーザの同等セキュリティを変更し、adminと同じにしたとき。
108	ndsRemoveEntry	eDirectoryからエントリが削除されたとき。 例: iManagerを使用して、ユーザを削除したとき。
109	ndsCRCFailure	断片化したNCP要求を構成し直す際に、CRC(冗長巡回検査)エラーが発生したとき。
110	ndsModifyEntry	eDirectoryエントリが変更されたとき。 例: iManagerを使って、ユーザの属性を変更したとき。
111	ndsNewSchemaEpoch	スキーマがDSRepairでリセットされたとき。 例: Linux上で、ndsrepair -S-Adを使って新規スキーマエポックを作成したとき。

トラップ番号	トラップ名	生成される条件
112	ndsLowLevelSplitPartition	パーティションを作成する際に、低レベル分割処理が実行されたとき。 例: iManagerまたはLDAPツールを使って、パーティションを作成したとき。
113	ndsReplicaInTransition	レプリカが追加または削除されたとき。
114	ndsAclModify	オブジェクトのトラスティが変更された、すなわちACL(アクセス制御リスト)オブジェクトが変更されたとき。 例: LDAPツール、ICE、iManagerなどを使って、オブジェクトのトラスティを追加、変更、削除したとき。
115	ndsLoginEnable	ユーザアカウントを有効にする要求をサーバから受け取ったとき。 例: LDAPツール、ICE、iManagerなどを使って、アカウント属性を無効から有効に変更したとき。
116	ndsLoginDisable	ユーザアカウントを無効にする要求をサーバから受け取ったとき。 例: LDAPツール、ICE、iManagerなどを使って、アカウント属性を有効から無効に変更したとき。
117	ndsDetectIntruder	不正侵入を検出したため、ユーザアカウントがロックされたとき。 例: LDAPツール、ICE、iManagerなどを使って不正侵入(Intruder)属性を設定することにより、ユーザアカウントをロックしたとき。
2001	ndsServerStart	サブエージェントがeDirectoryサーバに、正常に再接続できたとき。このトラップには2つの変数が含まれています。 ◆ ndsTrapTime: サブエージェントがeDirectoryサーバに再接続した時刻を、1970年1月1日午前0時(万国標準時)からの経過秒数で表します。 ◆ ndsServerName: サブエージェントが再接続したeDirectoryサーバを表します。 例: サブエージェントが稼動したままの状態でいったんeDirectoryサーバを停止し、再び起動したとき。

トラップ番号	トラップ名	生成される条件
2002	ndsServerStop	サブエージェントとeDirectoryサーバとの接続が失われたとき。 このトラップには2つの変数が含まれています。 ◆ ndsTrapTime: サブエージェントがeDirectoryサーバと切断された時刻を、1970年1月1日午前0時(万国標準時)からの経過秒数で表します。 ◆ ndsServerName: サブエージェントがそれまで接続されていたeDirectoryサーバを表します。 例: サブエージェントが稼動中にeDirectoryサーバを停止したとき。

暗号化属性にアクセスする

eDirectoryでは、特定の重要データをディスクに保存する場合や、ネットワーク上からそのデータにアクセスする場合に、データを暗号化して保護できます。暗号化属性へのアクセスにセキュリティ保護されたチャネルを使用する場合は、事前にそれを指定できます。詳細については、320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。

暗号化属性へのアクセスにセキュリティ保護されたチャネルのみを使用すると指定している場合は、NDS値イベントがブロックされます。値イベントに関連するトラップの値データはNULLになり、暗号化属性の値を取得するにはセキュリティ保護されたチャネルが必要であるということを示すエラー「-6089」が返されます。値データがNULLになるトラップは次のとおりです。

- ndsAddValue
- ndsDeleteValue
- ndsDeleteAttribute

トラップに関する設定

トラップに関する設定の手順はプラットフォームによって異なります。

Platform	ユーティリティ
Windows	ndssnmpcfg
Linux	ndssnmpconfig

Windows

Windowsでは、ndssnmpcfgを使ってトラップに関する設定を行います。このユーティリティは*install_path*\ディレクトリにあります。このユーティリティの機能としては、トラップの有効/無効の切り替え、各トラップ間の時間間隔の設定、デフォルトの時間間隔の設定、操作に失敗した場合のトラップの有効化、すべてのトラップのリスト表示などがあります。

使用率:

ndssnmpcfg -h [*hostname*[:*port*]] -p *password* -a *userFDN* -c *command*

パラメータ	説明
-h	DNSホスト名またはIPアドレス。
-p	認証に使うuserFDNパスワード
-a	管理者権限を持つユーザの完全識別名
-c	トラップコマンド(「540 ページの 「Windowsのトラップコマンド」」を参照)

Windowsのトラップコマンド

トラップコマンド	説明	使用法
DISABLE	トラップを無効にするコマンド。NMSは、トラップが送られてきても受け取らないようになります。	特定のトラップ(次の例では10番、11番、100番)を無効にしたい場合: ndssnmpcfg "DISABLE 10, 11, 100" 特定のトラップ(次の例では10番、11番、100番)以外をすべて無効にしたい場合: ndssnmpcfg "DISABLE ID != 10, 11, 100" ある範囲の番号のトラップ(次の例では20～29番)を無効にしたい場合: ndssnmpcfg "DISABLE 20-29" トラップをすべて無効にしたい場合: ndssnmpcfg "DISABLE ALL"
ENABLE	トラップを有効にするコマンド。NMSは、送られてきたトラップを受け取るようになります。	ndssnmpcfg "ENABLE *trapSpec*" *trapSpec*は次のいずれかの形式で指定してください。 特定のトラップ(次の例では10番、11番、100番)を有効にしたい場合: ndssnmpcfg "ENABLE 10, 11, 100" 特定のトラップ(次の例では10番、11番、100番)以外をすべて有効にしたい場合: ndssnmpcfg "ENABLE ID != 10, 11, 100" ある範囲の番号のトラップ(次の例では20～29番)を有効にしたい場合: ndssnmpcfg "ENABLE 20-29" トラップをすべて有効にしたい場合: ndssnmpcfg "ENABLE ALL"

トラップコマンド	説明	使用法
INTERVAL	時間間隔を設定する、または表示するためのコマンド。 ここでいう時間間隔とは、同じトラップを繰り返し送る場合に、何秒間の間隔をおくかを表すものです。 0～2,592,000の範囲(秒単位)で設定してください。 この範囲外の値を指定した場合、デフォルトの時間間隔が指定されたものとみなします。 設定値を0とすれば、トラップがすべて送られるようになります。	時間間隔の設定値を表示する場合: ndssnmpcfg "213,240,79 INTERVAL" 複数のトラップについて時間間隔を設定する場合(次の例では12番、17番、101番トラップについて5秒と設定): ndssnmpcfg "12 17 101 INTERVAL 5" デフォルトの時間間隔を表示する場合: ndssnmpcfg "DEFAULT INTERVAL" デフォルトの時間間隔を設定する場合: ndssnmpcfg "DEFAULT INTERVAL=10"
LIST	ある条件を満たすトラップ番号を一覧表示するコマンド。	ndssnmpcfg LIST *trapSpec* *trapSpec*には、トラップ番号のほか、以下に述べるキーワードで条件を指定できます。 ALL、ENABLED、DISABLED、FAILED、または論理式 例: 有効なトラップをすべて、名称を添えて表示: ndssnmpcfg LIST ENABLED 無効なトラップをすべて、名称を添えて表示: ndssnmpcfg LIST DISABLED 117種類すべてのトラップについて、名称を添えて表示: ndssnmpcfg LIST ALL 特定の番号(次の例では12番、224番、300番)のトラップについて、名称を添えて表示: ndssnmpcfg LIST ID = 12,224,300 特定の番号(次の例では12番、224番、300番)以外のトラップをすべて、名称を添えて表示: ndssnmpcfg LIST ID != 12,224,300 有効なエラートラップをすべて、名称を添えて表示: ndssnmpcfg LIST FAILED

トラップコマンド	説明	使用法
READ_CFG	環境設定ファイルndstrap.cfgを参照して、ディレクトリ構成を再設定するコマンド。 環境設定ファイルの設定に加えられた変更はすべて有効になります。いくつものコマンドをndstrap.cfgに記述しておき、ひとまとめにして実行する、という使い方を主として想定したユーティリティです。 ndstrap.cfgは*インストールディレクトリ*\SNMPにあります。 ndstrap.cfgファイルでは、トラップの環境設定に使用されるオペレーショナルパラメータを設定し、SNMPトラップの操作を設定する方法を指定します。トラップの環境設定ユーティリティndssnmpcfgがREAD_CFGコマンドで実行される場合には、必ずこのファイルが読み込まれます。	ndssnmpcfg "READ_CFG"
FAILURE	エラートラップをすべて表示するコマンド。 エラートラップとは、イベントの失敗時に生成されるトラップのことです。 **注:** エラートラップをいったん無効にし、「enable trapid」コマンドで再び有効にすると、エラートラップではなく、正常に処理されたことを表すトラップとして扱われるようになります。	ndssnmpcfg "FAILURE *trapSpec*" *trapSpec*には、トラップ番号をコンマまたはスペースで区切って指定するほか、キーワード「ALL」や論理式を指定できます。例: 複数のトラップをエラートラップと設定: ndssnmpcfg "FAILURE 10,11,100" 指定した番号以外のすべてのトラップをエラートラップと設定: ndssnmpcfg "FAILURE ID != 24,30" すべてのトラップをエラートラップと設定: ndssnmpcfg "FAILURE ALL"

Linux

Linuxでは、ndssnmpconfigを使ってトラップに関する設定を行います。これは/etc/ndssnmp/ディレクトリにあります。このユーティリティの機能としては、トラップの有効/無効の切り替え、各トラップ間の時間間隔の設定、デフォルトの時間間隔の設定、操作に失敗した場合のトラップの有効化、すべてのトラップのリスト表示などがあります。

使用率:

ndssnmpconfig -h [*hostname*[*:port*]] -p *password* -a *userFDN* -c *command*

パラメータ	説明
-h	DNSホスト名またはIPアドレス。
-p	認証に使うuserFDNパスワード
-a	管理者権利を持つユーザの完全識別名。
-c	トラップコマンド(「543 ページの 「Linuxトラップコマンド」」を参照)

Linuxトラップコマンド

トラップコマンド	説明	使用法
DISABLE	トラップを無効にするコマンド。NMSは、トラップが送られてきても受け取らないようになります。	特定のトラップ(次の例では10番、11番、100番)を無効にしたい場合: ndssnmpconfig "DISABLE 10, 11, 100" 特定のトラップ(次の例では10番、11番、100番)以外をすべて無効にしたい場合: ndssnmpconfig "DISABLE ID != 10, 11, 100" ある範囲の番号のトラップ(次の例では20～29番)を無効にしたい場合: ndssnmpconfig "DISABLE 20-29" トラップをすべて無効にしたい場合: ndssnmpconfig "DISABLE ALL"

トラップコマンド	説明	使用法
ENABLE	トラップを有効にするコマンド。NMSは、送られてきたトラップを受け取るようになります。	ndssnmpconfig "ENABLE *trapSpec*" *trapSpec*は次のいずれかの形式で指定してください。 特定のトラップ(次の例では10番、11番、100番)を有効にしたい場合: ndssnmpconfig "ENABLE 10, 11, 100" 特定のトラップ(次の例では10番、11番、100番)以外をすべて有効にしたい場合: ndssnmpconfig "ENABLE ID != 10, 11, 100" ある範囲の番号のトラップ(次の例では20～29番)を有効にしたい場合: ndssnmpconfig "ENABLE 20-29" トラップをすべて有効にしたい場合: ndssnmpconfig "ENABLE ALL"
INTERVAL	時間間隔を設定する、または表示するためのコマンド。 ここでいう時間間隔とは、同じトラップを繰り返し送る場合に、何秒間の間隔をおくかを表すものです。 0～2,592,000の範囲(秒単位)で設定してください。 この範囲外の値を指定した場合、デフォルトの時間間隔が指定されたものとみなします。 設定値を0とすれば、トラップがすべて送られるようになります。	時間間隔の設定値を表示する場合: ndssnmpconfig "213,240,79 INTERVAL" 複数のトラップについて時間間隔を設定する場合(次の例では12番、17番、101番トラップについて5秒と設定): ndssnmpconfig "12 17 101 INTERVAL 5" デフォルトの時間間隔を表示する場合: ndssnmpconfig "DEFAULT INTERVAL" デフォルトの時間間隔を設定する場合: ndssnmpconfig "DEFAULT INTERVAL=10"

トラップコマンド	説明	使用法
LIST	ある条件を満たすトラップ番号を一覧表示するコマンド。	ndssnmpconfig LIST <*trapSpec*> *trapSpec*には、トラップ番号のほか、以下に述べるキーワードで条件を指定できます。 ALL、ENABLED、DISABLED、FAILED、または論理式 例: 有効なトラップをすべて、名称を添えて表示: ndssnmpconfig LIST ENABLED 無効なトラップをすべて、名称を添えて表示: ndssnmpconfig LIST DISABLED 117種類すべてのトラップについて、名称を添えて表示: ndssnmpconfig LIST ALL 特定の番号(次の例では12番、224番、300番)のトラップについて、名称を添えて表示: ndssnmpconfig LIST ID = 12,224,300 特定の番号(次の例では12番、224番、300番)以外のトラップをすべて、名称を添えて表示: ndssnmpconfig LIST ID != 12,224,300 有効なエラートラップをすべて、名称を添えて表示: ndssnmpconfig LIST FAILED

トラップコマンド	説明	使用法
READ_CFG	環境設定ファイルndstrap.cfgを参照して、ディレクトリ構成を再設定するコマンド。 環境設定ファイルの設定に加えられた変更はすべて有効になります。いくつものコマンドをndstrap.cfgに記述しておき、ひとまとめにして実行する、という使い方を主として想定したユーティリティです。 ndstrap.cfgファイルは/etc/ndssnmp/に配置されています。 ndstrap.cfgファイルでは、トラップの環境設定に使用されるオペレーショナルパラメータを設定し、SNMPトラップの操作を設定する方法を指定します。トラップの環境設定ユーティリティndssnmpcfgがREAD_CFGコマンドで実行される場合には、必ずこのファイルが読み込まれます。	ndssnmpconfig "READ_CFG"
FAILURE	エラートラップをすべて表示するコマンド。 エラートラップとは、イベントの失敗時に生成されるトラップのことです。 **注:** エラートラップをいったん無効にし、「enable trapid」コマンドで再び有効にすると、エラートラップではなく、正常に処理されたことを表すトラップとして扱われるようになります。	ndssnmpconfig "FAILURE *trapSpec*" *trapSpec*には、トラップ番号をコンマまたはスペースで区切って指定するほか、キーワードALLや論理式を指定できます。 例: 複数のトラップをエラートラップと設定: ndssnmpconfig "FAILURE 10,11,100" 指定した番号以外のすべてのトラップをエラートラップと設定: ndssnmpconfig "FAILURE ID != 24,30" すべてのトラップをエラートラップと設定: ndssnmpconfig "FAILURE ALL"

[Statistics (統計情報)]

- 547 ページの 「ndsDbCache」
- 547 ページの 「ndsDbConfig」
- 548 ページの 「ndsProtoIfOps」
- 549 ページの 「ndsServerInt」

ndsDbCache

ディレクトリ以下にある管理対象オブジェクト	説明
ndsDbSrvApplIndex	eDirectoryサーバアプリケーションを固有に識別するインデックス。
ndsDbDibSize	eDirectoryデータベースの容量(KB単位)。
ndsDbBlockSize	eDirectoryデータベースのブロック容量(KB単位)。
ndsDbEntryCacheMaxSize	エントリキャッシュの最大容量(KB単位)。
ndsDbBlockCacheMaxSize	ブロックキャッシュの最大容量(KB単位)。
ndsDbEntryCacheCurrentSize	現在のエントリキャッシュ容量。
ndsDbBlockCacheCurrentSize	現在のブロックキャッシュ容量。
ndsDbEntryCacheCount	キャッシュ内のエントリ数。
ndsDbBlockCacheCount	キャッシュ内のブロック数。
ndsDbEntryCacheOldVerCount	キャッシュ内に残っている旧バージョンのエントリ数。
ndsDbBlockCacheOldVerCount	キャッシュ内に残っている旧バージョンのブロック数。
ndsDbEntryCacheOldVerSize	旧バージョンのエントリキャッシュ容量。
ndsDbBlockCacheOldVerSize	旧バージョンのブロックキャッシュ容量。
ndsDbEntryCacheHits	キャッシュ内のエントリがヒットした回数。
ndsDbBlockCacheHits	キャッシュ内のブロックがヒットした回数。
ndsDbEntryCacheHitLooks	キャッシュ内のエントリがヒットするかどうか試みられた回数。
ndsDbBlockCacheHitLooks	キャッシュ内のブロックがヒットするかどうか試みられた回数。
ndsDbEntryCacheFaults	キャッシュ内のエントリがヒットしなかった回数。
ndsDbBlockCacheFaults	キャッシュ内のブロックがヒットしなかった回数。
ndsDbEntryCacheFaultLooks	キャッシュ内のエントリがヒットしないかどうか試みられた回数。
ndsDbBlockCacheFaultLooks	キャッシュ内のブロックがヒットしないかどうか試みられた回数。

ndsDbConfig

ディレクトリ以下にある管理対象オブジェクト	説明
ndsDbCfgSrvApplIndex	eDirectoryサーバアプリケーションを一意に識別するインデックス。
ndsDbCfgDynamicCacheAdjust	動的キャッシュ調整が有効かどうか。0 = off 1 = on

ディレクトリ以下にある管理対象オブジェクト	説明
ndsDbCfgDynamicCacheAdjustPercent	動的キャッシュ調整に、空きメモリの何%を割り当てるか。
ndsDbCfgDynamicCacheAdjustMin	動的キャッシュ調整に使う最小容量。キャッシュ容量制限をKB単位で表したもの。
ndsDbCfgDynamicCacheAdjustMinToLeave	動的キャッシュ調整に使う最小容量のうち、利用可能なメモリから差し引く容量(KB単位)。
ndsDbCfgHardLimitCacheAdjust	キャッシュ調整に割り当てるメモリ容量にハード制限を設定するかどうか。0 = off 1 = on
ndsDbCfgHardLimitCacheAdjustMax	キャッシュの最大容量(KB単位)。これはハードメモリ制限を表します。
ndsDbCfgBlockCachePercent	ブロックキャッシュに割り当てる比率。
ndsDbCfgCacheAdjustInterval	キャッシュ調整を行う時間間隔(秒単位)。
ndsDbCfgCacheCleanupInterval	キャッシュのクリーンアップを行う時間間隔(秒単位)。
ndsDbCfgPermanentSettings	常時接続の設定が有効かどうか。0 = off 1 = on

ndsProtoIfOps

ディレクトリ以下にある管理対象オブジェクト	説明
ndsProtoIfSrvApplIndex	eDirectoryサーバアプリケーションを一意に識別するインデックス。
ndsProtoIfIndex	eDirectoryサーバのプロトコルインタフェースに対応するエントリを一意に識別するインデックス。
ndsProtoIfDescription	DSプロトコルインタフェースに使うポート番号
ndsProtoIfUnauthBinds	認証を省略した匿名バインド要求を受け取った回数。
ndsProtoIfSimpleAuthBinds	バインド要求のうち、簡易認証手続きにより認証に成功したものの回数。簡易認証手続きとは、パスワードを暗号化して、または平文のまま送ることにより行うものです。
ndsProtoIfStrongAuthBinds	バインド要求のうち、強度の高い認証手続きであるSASLおよびX.500の認証に成功したものの回数。外部認証手続きによるものも数に含みます。
ndsProtoIfBindSecurityErrors	バインド要求のうち、認証手続きが適切でない、あるいは資格情報が無効であるために拒否したものの回数。
ndsProtoIfInOps	DUA(ディレクトリユーザエージェント)または他のeDirectoryサーバから受け取った要求の回数。
ndsProtoIfReadOps	受け取った読み出し要求の数。
ndsProtoIfCompareOps	受け取った比較要求の数。
ndsProtoIfAddEntryOps	受け取ったエントリ追加要求の数。

ディレクトリ以下にある管理対象オブジェクト	説明
ndsProtoIfRemoveEntryOps	受け取ったエントリ削除要求の数。
ndsProtoIfModifyEntryOps	受け取ったエントリ変更要求の数。
ndsProtoIfModifyRDNOps	受け取ったRDN(相対識別名)変更要求の数。
ndsProtoIfListOps	受け取ったリスト要求の数。
ndsProtoIfSearchOps	受け取った検索要求(ベースオブジェクト検索、1レベル検索、サブツリー全体の検索)の数。
ndsProtoIfOneLevelSearchOps	受け取った1レベル検索要求の数。
ndsProtoIfWholeSubtreeSearchOps	受け取ったサブツリー全体の検索要求の数。
ndsProtoIfExtendedOps	拡張処理の回数。
ndsProtoIfReferrals	処理要求に応じて返した参照の個数。
ndsProtoIfChainings	このeDirectoryサーバから他のeDirectoryサーバに転送した処理の数。
ndsProtoIfSecurityErrors	受け取った要求のうち、セキュリティ保護方針に合致しなかったものの数。
ndsProtoIfErrors	受け取った要求のうち、エラーのため応じなかったものの数。ただしセキュリティ保護エラー、参照エラーを除きます。一部でも処理ができたものは数に含めません。たとえば、名前づけや更新、属性、サービスに関連するエラーがあります。
ndsProtoIfReplicationUpdatesIn	eDirectoryサーバから取得した、または受け取ったレプリカ作成更新の数。
ndsProtoIfReplicationUpdatesOut	eDirectoryサーバに送った、または検知されたレプリカ作成更新の数。
ndsProtoIfInBytes	インタフェース上の受信トラフィック(バイト単位)。DUA(ディレクトリユーザエージェント)からの要求、他のeDirectoryサーバからの応答などといったトラフィックがこれに当たります。
ndsProtoIfOutBytes	インタフェース上の送信トラフィック(バイト単位)。DUAやeDirectoryサーバへの応答、他のeDirectoryサーバへの要求などといったトラフィックがこれに当たります。

ndsServerInt

ディレクトリ以下にある管理対象オブジェクト	説明
ndsSrvIntSrvApplIndex	eDirectoryサーバアプリケーションを一意に識別するインデックス。
ndsSrvIntProtoIfIndex	eDirectoryサーバのプロトコルインタフェースに対応するエントリを一意に識別するインデックス。

ディレクトリ以下にある管理対象オブジェクト	説明
ndsSrvIntIndex	このオブジェクトはndsSrvIntSrvApplIndexおよびndsSrvIntProtoIfIndexと組み合わせて使います。ndsSrvIntSrvApplIndexで示されるeDirectoryサーバと、特別なプロトコルを使うピアeDirectoryサーバとの間でやり取りされる情報を格納した、仮想的な行を一意的に識別するためのキーとなります。
ndsSrvIntURL	ピアeDirectoryサーバのURL。
ndsSrvIntTimeOfCreation	この行が作成された時刻。1970年1月1日午前0時(万国標準時)からの経過秒数で表します。
ndsSrvIntTimeOfLastAttempt	ピアeDirectoryサーバとの接続を試みた直近の時刻。1970年1月1日午前0時(万国標準時)からの経過秒数で表します。
ndsSrvIntTimeOfLastSuccess	ピアeDirectoryサーバと正常に接続できた直近の時刻。1970年1月1日午前0時(万国標準時)からの経過秒数で表します。
ndsSrvIntFailuresSinceLastSuccess	ピアeDirectoryサーバと正常に接続した直近の時刻以降に発生したエラーの数。まだ一度も正常に接続できていない場合は、このエントリが作成されて以来のエラー数。
ndsSrvIntFailures	このエントリが作成されて以来、ピアeDirectoryサーバとの接続に失敗した回数。
ndsSrvIntSsuccesses	このエントリが作成されて以来、ピアeDirectoryサーバとの接続に成功した回数。

トラブルシューティング

問題を迅速に解決できるよう、実際に発生したエラー状況、その解決に役立つ情報が、ログファイルに記録されています。詳細については、935ページの「SNMPのトラブルシューティング」を参照してください。

表 18-1に、Linuxプラットフォーム用のサーバログファイルのデフォルトの場所を示します。ndsd.logファイルの場所を特定するには、eDirectoryインスタンスに対してndsconfig get n4u.server.log-fileコマンドを実行します。

***表 18-1** [ログファイルの場所]*

Platform	サブエージェント	サーバ	マスタ
Windows	*install_directory*\nds\snmp\dssnmpsa.log	*install_directory*\nds\snmp\dssnmpsrv.log	NA
Linux	/var/opt/novell/eDirectory/log/ndssnmpsa.log	/var/opt/novell/eDirectory/log/ndsd.log	/var/log/messages

19 NetIQ eDirectoryのメンテナンス

NetIQ eDirectoryのパフォーマンスを最適にするには、定期的なヘルスチェック手順を実行し、必要に応じてハードウェアのアップグレードや交換を行ってディレクトリをメンテナンスする必要があります。

この章では、次のメンテナンスに関するトピックについて説明します。

パフォーマンス

- 551 ページの 「詳細参照コスト」

ヘルスチェック

- 560 ページの 「eDirectoryの正常動作の維持」
- 563 ページの 「監視のためのリソース」

ハードウェアの交換

- 563 ページの 「ハードウェアのアップグレードやサーバの交換」

eDirectoryの回復

- 570 ページの 「ハードウェア障害後のeDirectoryの復元」

詳細参照コスト

サーバアプリケーションの多くは、組み込みクライアント(Dclient)経由で他のサーバと通信します。これは、1つのサーバに、アプリケーションが動作するのに必要なすべてのeDirectoryデータが保存されているわけではないためです。1つの例が、要求をチェーンするように設定されたNLDAPです。

サーバアプリケーションがローカルサーバに保存されていないデータを要求した場合、サーバは要求されたデータが保存されている別のサーバを特定してから、クライアントに関するデータを取得します。このプロセスは「ツリーウォーキング」と呼ばれます。通常、サーバがツリーウォーキング経由で要求を満たすまでに時間がかかります。eDirectoryツリー設計に関するベストプラクティスのガイドラインを使用すればツリーウォーキングの必要性が最小限に抑えられますが、それでも必要な場合があります。

図 19-1 詳細参照コスト

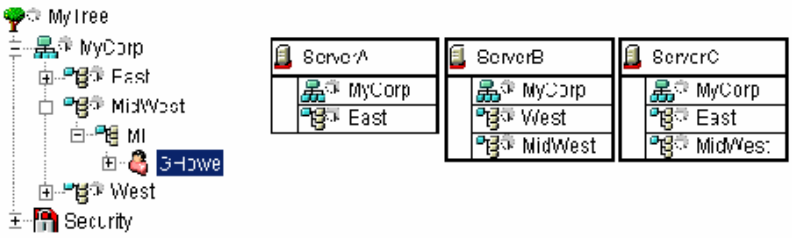


図 19-1は、O=MyCorpから始まる、サーバAに対するcn=GHoweのLDAPサブツリー検索を示しています。ただし、cn=GHoweオブジェクトは、サーバA上に存在しないou=MidWestパーティションに配置されています。

クライアントの要求を満たすために必要なデータが保存されたサーバを特定するには、サーバAがサーバBまたはサーバCからデータを取得する必要があります。これを行うには、サーバAがサーバBとサーバCのどちらかに要求を送信する必要があります。サーバAはサーバBを選択しました。サーバ選択プロセスは予測不能であることに注意してください。サーバBはネットワーク上で使用可能で、要求を受け入れますが、要求を迅速に処理できないため、サーバCも必要なデータを提供できたとしても、サーバAはサーバBを待機することになります。サーバBが要求を満たすか、ネットワーク上で使用できなくなるまで、サーバAからの要求が待たされることになります。

以下のセクションで、eDirectoryサーバのパフォーマンスを改善する方法について説明します。

- 552 ページの 「サーバ間接続の向上」
- 554 ページの 「参照コストのメリット」
- 555 ページの 「ARCの展開」
- 556 ページの 「詳細参照コストの有効化」
- 556 ページの 「詳細参照コストの調整」
- 557 ページの 「詳細参照コストの監視」

サーバ間接続の向上

詳細参照コスト(ARC)は高度なコストアルゴリズムです。ARCの主な目的は、サーバの機能停止を回避することです。ARCのメリットを以下に示します。

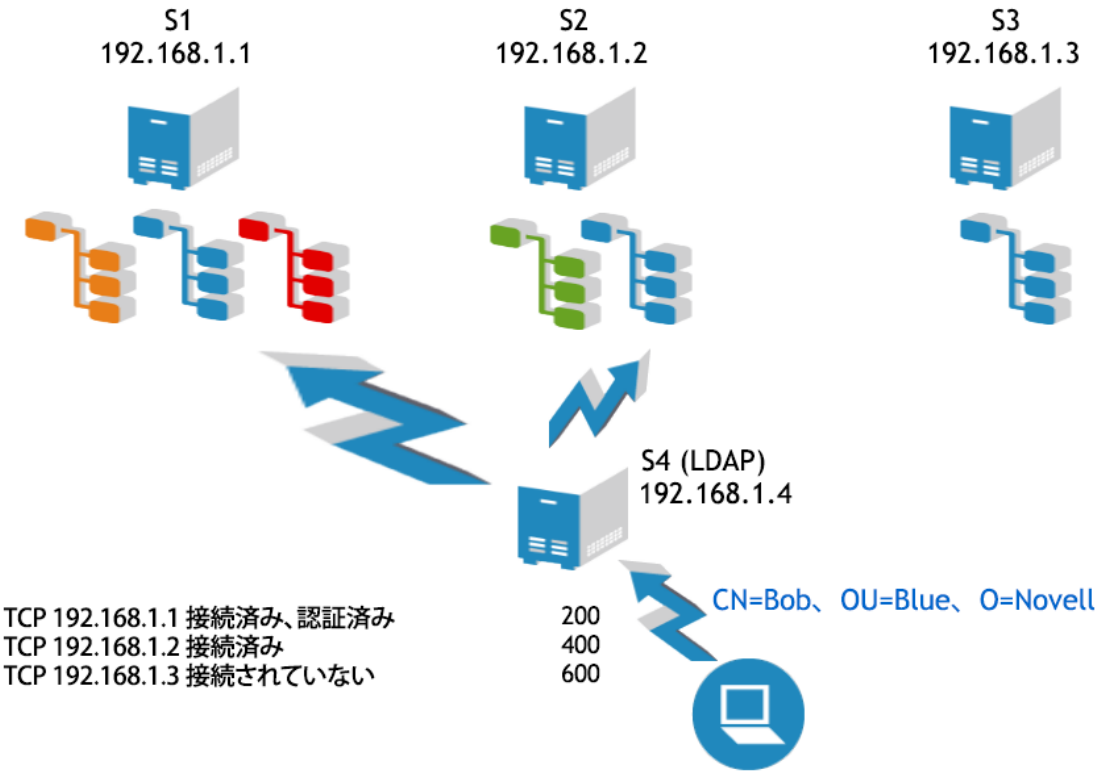
- サーバのパフォーマンスと耐障害性の向上
- サーバ間通信の改善
- 負荷分散
- リモートサーバヘルスモニタリング
- 通信問題の分離と特定の簡素化

ARCを使用すべきなのは誰か?

オブジェクトまたはサービスのローカルコピーが保存されていないサーバは、他のサーバと頻繁に通信するため、ツリーでARCからもたらされた情報を探索する必要があります。ARCは、LDAP環境、特に、優先チェーン処理中に非常に効率的に動作します。

たとえば、図 19-2に示すように、サーバは要求を送り続ける別のサーバから悩まされる場合があります。

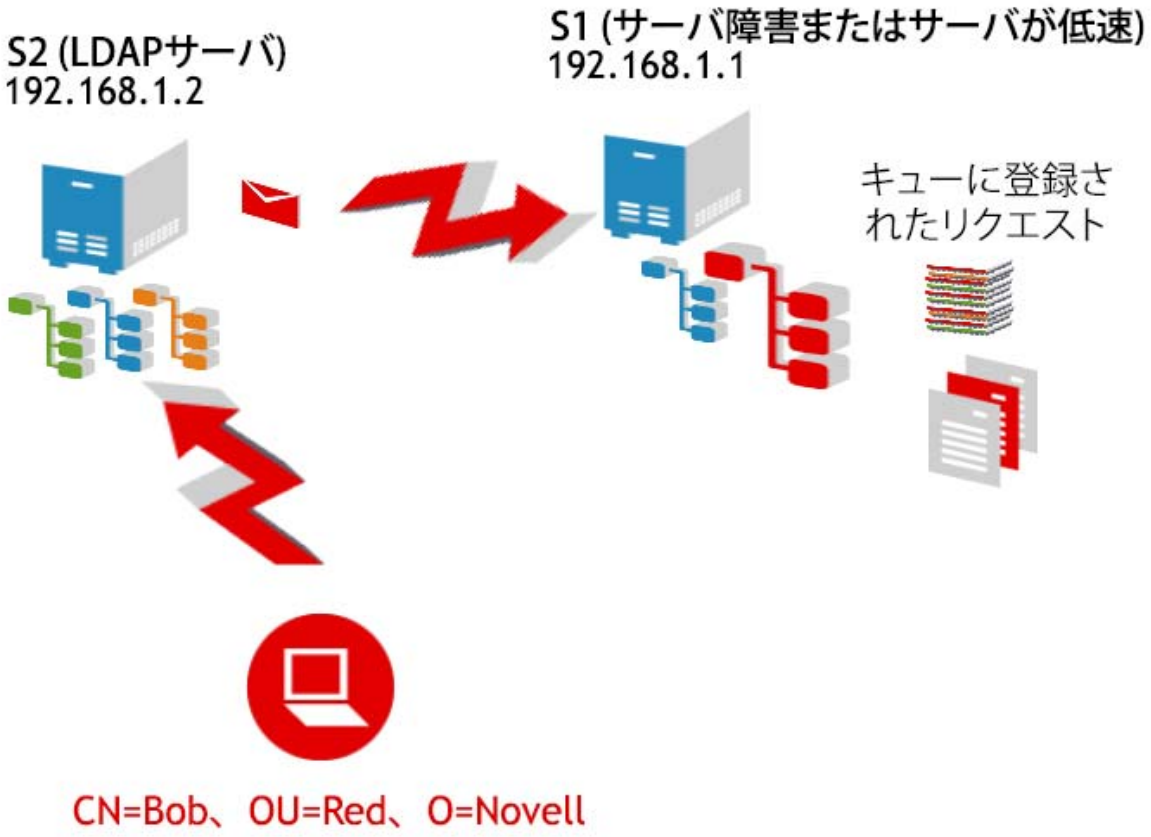
図19-2　ワンストップサーバの影響



必要なオブジェクトのレプリカが保存された使用可能なサーバが他にあったとしても、このサーバが優先されると思われます。これは、サービスまたはレプリカを要求しているサーバがすでにこのサーバに接続されており、処理可能なすべての要求がこのサーバに集中する傾向があるためです。図 19-2は、S4からのすべての要求がS1に送信される様子を示しています。S4はすでにS1に接続されており、S1に対して認証されているため、S2とS3がその要求に応えることができたとしても、S4は青色のパーティションに対するすべての要求をS1に送信し続けます。ARCを使用すれば、より迅速に対応可能なサーバに負荷を分散することによって、このような状況を回避できます。このサーバを必要とするリモートサーバ(S4)上でARCを有効にする必要があります。または、すべてのサーバ上でARCを有効にすることができます。

図19-3は、「カスケーディングサーバ」の影響を示すもう1つのシナリオを示しています。ここで、サーバS1は頻繁に応答を返しませんが、ダウンしているわけではありません。S1がダウンすると、要求がタイムアウトして、通信が停止します。サーバがまだトランスポートレベルでアップしているが、データベースが低速またはビジーの場合は、他のサーバからの新しい要求を受け付けてキューに入れ続けます。そのため、最終的に、追加のサーバ(S2)がスレッドを使い果たすことになります。未処理の要求がそれぞれリモートサーバでスレッドを取得し、スレッドが使い果たされた段階で、サーバが応答を返さなくなります。ARCは最も高速なサーバに要求を分散することによってこの問題を解決します。これは、低速なまたは不具合のあるサーバは要求の処理に高いコストがかかるためです。

図19-3 カスケーディングサーバの影響



加えて、ARCは、耐障害性の向上にも役立ちます。サーバの通信問題を簡単に特定する機能を備えています。

参照コストのメリット

- これは、リモートサーバへのほとんどの名前解決要求を計時/ルーティングします。
- アドレスごとの名前解決要求時間をミリ秒単位で平均化します。これにより、ARCは、より細かいレベルでより積極的に参照のコストを調整できます。タイミングが秒単位ではなくミリ秒単位で追跡されるため、低速なサーバをすばやく検出することもできます。
- 未処理要求を追跡することによって、要求に時間がかかりすぎているかどうかをすばやく判断できます。サーバで時間がかかっていることを確認するために、要求が完了するまで待つ必要はありません。
- アドレス単位で応答時間を追跡します。1台のサーバが同じアドレスに何回も接続するのが普通です。接続単位ではなくアドレス単位で追跡することによって、1つの接続で他の接続から収集された統計情報を参考にできます。

注: LDAP要求を理解するために、ARCはプライベート接続の応答性も考慮します。

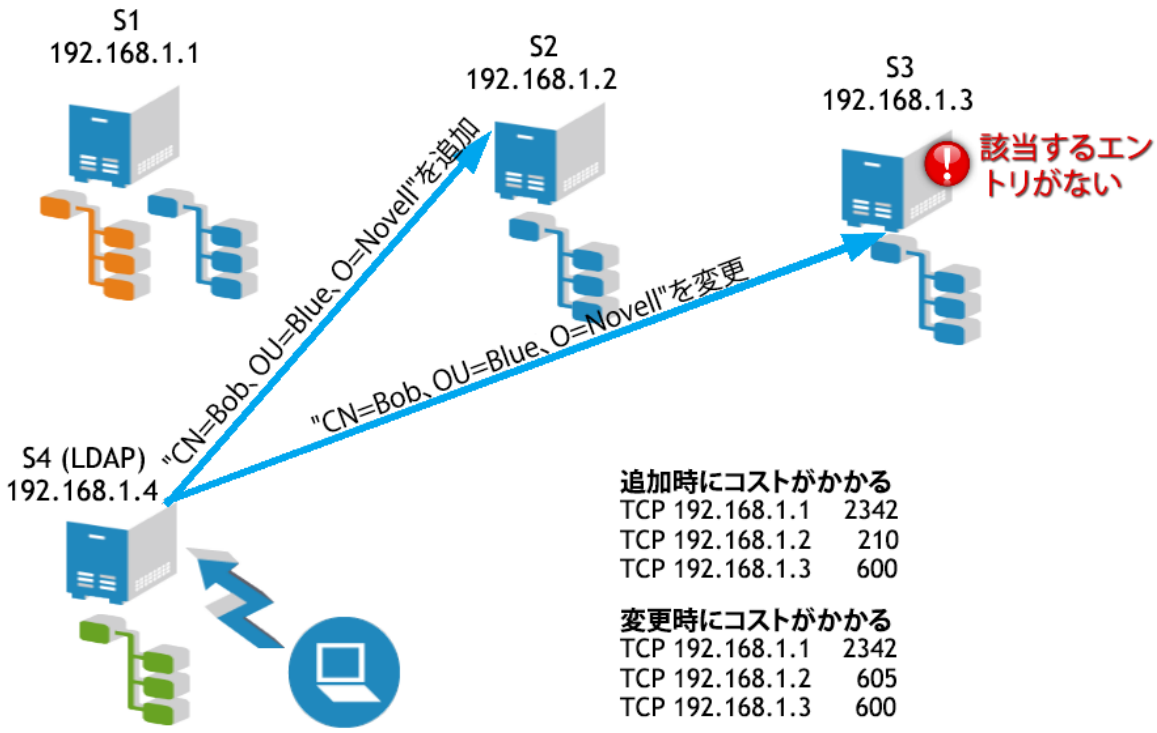
ARCの展開

ARCは、通常、サーバ単位で展開されます。ARC対応のこれらのサーバは新しいコスト情報を入手することができます。環境内のすべてのサーバでARCを有効にする必要があります。

展開に関する考慮事項

すべてのサーバ上でARCを有効にすることが役に立つとは限りません。図 19-4は、LDAPサーバの有効性に影響を与える状況を示しています。図では、S4に青色のパーティションではなく緑色のパーティションのコピーが保存されています。青色のパーティションに関する情報が必要なチェーンLDAP要求は、S1、S2、またはS3サーバに送信され、処理される必要があります。これはほとんどのケースで動作します。ARCは、まさにこのような状況に合わせて設計されています。

図 19-4 ARC展開に関する考慮事項



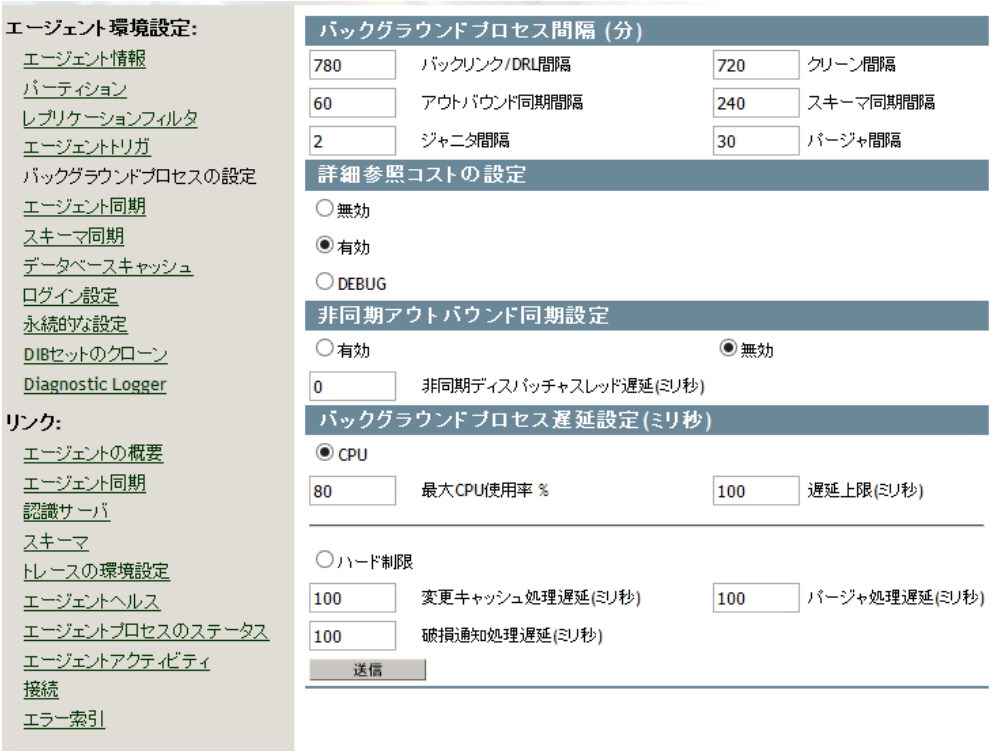
ただし、特定のLDAP操作の実行には困難が伴います。Bob.Blue.Novellなどのユーザを追加することはできますが、Bobを変更するために急いで戻ろうとすると操作が失敗します。図はS2上にBobが追加されたことを示していますが、S3上でBobを変更しようとしても、S3がまだS2と同期していないために操作が失敗して、S3はBobを受け取ることができません。ARCはユーザを別のサーバに誘導する機能を備えています。これは、ARCの方がオリジナルのコスト計算手法より動的なためです。

この設定は、サーバコストがあまり変化せず、正常に同期しているシナリオでうまく動作します。S4上でARCを無効にするとこの問題が解決されます。

詳細参照コストの有効化

ARCは、デフォルトで、eDirectoryに対して有効になっています。NDS iMonitorを使用してARCを設定するには、［**エージェント環境設定**］>［**バックグラウンドプロセスの設定**］の順にクリックします。加えて、［**有効**］、［**無効**］、および［**デバッグ**］オプションを使用できます。

図 19-5 *NDS iMonitorエージェントの環境設定画面*



NDSTrace

すべてのUNIXプラットフォームで、NDSTraceツールを使用してARCを有効にします。

表 19-1 *UNIX プラットフォーム上でのARCの有効化*

set NDSTRACE =!ARC	デバッグ用のgv_ResolveTimesTableを表示します。
set NDSTRACE =!ARC0	詳細参照コストを無効にします。
set NDSTRACE =!ARC1	詳細参照コストを有効にします。
set NDSTRACE =!ARC2	詳細参照コストをデバッグモードで有効にして、コストが決定されるたびに、名前解決DSTraceフラグに対する参照のコストを表示します。

詳細参照コストの調整

デフォルトで、ARCは調整する必要がありません。ただし、ARCの機能を変更したり、特定の機能を有効/無効にしたりするための調整可能なパラメータがARC内に存在します。ARCにとって重要なコンポーネントが3つあります。

詳細コスト

特定のアドレスのコストを見積もるように要求されたら、ARCは、接続に関する既知の情報を使用して特定の参照のコストを計算します。ARCがオンになっている場合は、参照のコスト計算に常に詳細コストが使用されます。

バックグラウンド監視

バックグラウンドスレッドは、定期的にタイマ情報をチェックして誤差がないことを確認します。サーバが低速の場合は、そのコストが上昇して、通信が停止する可能性が高くなります。バックグラウンドスレッドは、定期的(デフォルトでは1分ごと)に、テーブル内のサーバが更新されていないかどうかをチェックします。過去3分以内にサーバが更新されていなかった場合は、サーバがそれ自体に名前解決要求を発行してサーバのヘルスをチェックします。これにより、最新のサーバのコストが計算され、サーバがビジー状態を脱したのかどうか、つまり、正常に戻ったのかどうかも検出されるため、クライアントはサーバのヘルスをチェックする必要がありません。バックグラウンドスレッド用の変更可能な永続的な環境設定パラメータが2つあります。

- **ARC_MAX_WAIT:** サーバのヘルスをチェックするためのサーバへの要求を発行するまでのタイマ値(デフォルトは180秒)
- **ARC_BG_INTERVAL:** バックグラウンドスレッドの実行間隔(デフォルトは60秒。0は無効になっていることを意味し、スレッドは実行されません)。

詳細については、セクション8.4.24の永続的な環境設定パラメータの設定に関する説明を参照してください。

リモートヘルス情報

ARCを使用したサーバは、定期的に、リモートサーバにヘルス情報を要求します。これらは、ネットワーク上に追加で発行される要求ではなく、サーバが頻繁に発行する標準の名前解決要求で返される追加のヘルス情報です。この情報は、高負荷状態にあるサーバへの対応を迅速化するコストアルゴリズムで使用されます。名前解決要求がリモートサーバに発行されると、前回の更新から15秒以上経過していた場合は、ヘルス情報がリモートサーバに要求され、名前解決要求の応答に追加されます。

リモートヘルスモニタリングには調整可能なパラメータが1つあります。

- **ARC_DS_INFO_INTERVAL:** これは、ARC内のロック(ヘルス)情報の要求間隔です(デフォルトは15秒)。

詳細参照コストの監視

ResolveTimesテーブルを出力して、操作における詳細参照コストを確認することができます。

ResolveTimesテーブルは次のコマンドを使用して出力します。

- set DSTRACE = +DBG
- set DSTRACE = !ARC

このコマンドは、Resolve Timesテーブルとサーバごとの現在保存されている情報を出力します。トランスポートアドレス、アドレスが最後に使用された以降の経過時間(ミリ秒)、参照決定で使用された最後のコスト、およびそのアドレスに対する未処理要求の数が表示されます。

未処理要求の数が多くても、必ずしも問題ではありません。単に、そのサーバの使用頻度が高いこと示しているにすぎない場合もあります。

トラブルシューティングでのARCの使用

ARCの最も有用な機能の1つがサーバに伴う通信問題を迅速に特定する機能です。

ResolveTimesテーブルのプリントアウトの例を以下に示します。

ARCは現在有効になっています。

***表 19-2** 解決時間コスト*

Slot	トランスポートアドレス	Cost	最後の使用	オン	要求数	待機数	ロック時間
1	tcp:151.155.134.27:524	214	14	14	0	0	0
2	tcp:151.155.134.11:524	0	0	0	0	0	0
3	udp:151.155.134.11:524	0	0	0	0	0	0
4	cp:151.155.134.13:524	554759	280	0	0	27	582
5	tcp:151.155.134.59:524	0	179	179	0	0	0
6	udp:151.155.134.59:524	0	119	119	0	0	0
7	tcp:151.155.134.28:524	1543	119	119	0	0	0
8	tcp:151.155.134.15:524	124	14	14	0	0	0

このプリントアウトは、このサーバの視点から151.155.134.13で問題が発生していることを示しています。問題がトランスポートではなくサーバにある可能性が高いこともわかります。サーバでは、27件の要求がデータベースへのアクセス待ちであり、それらがデータベースロックを取得するのに時間がかかっています。このサーバでは、2件の要求がリモートサーバからの応答を受け取っていません。

151.155.134.11と151.155.134.59は、非常に高速なサーバか、あまりビジーではないかのどちらかまたはその両方であることもわかります。151.155.134.59と151.155.134.11の両方でTCP経由の通信問題が1回発生したが、UDP接続が使用できるため現在は正常に戻っていることもわかります。サーバへのUDP接続は、TCP経由でサーバに通知できない場合にのみ、試行されます。

それぞれの数字の意味を以下に示します。

トランスポートアドレス: リモートサーバのアドレス。

Cost: リモートサーバの現在のコスト。

最後の使用: サーバとの最後の通信以降の経過時間(秒)。

オン: リモートサーバからの最後のヘルス情報以降の経過時間(秒)。

要求数: リモートサーバへの未処理要求数。

待機数: データベースのロックを待っているリモートサーバへの要求数。

ロック時間: プロセスがリモートサーバ上でデータベースのロックを維持していた時間。

次のプリントアウトは通信の問題を迅速に特定するためのもう1つの例を示しています。サーバはTCP経由で151.155.134.13に通信できないことがわかります。

ARCは現在有効になっています。

表 19-3 解決時間コスト

Slot	トランスポートアドレス	Cost	最後の使用	オン	要求数	待機数	ロック時間
1	tcp:151.155.134.27:524	394	92	14	0	0	0
2	tcp:151.155.134.11:524	0	0	0	0	0	0
3	udp:151.155.134.11:524	0	0	0	0	0	0
4	tcp:151.155.134.13:524	5000000	180	180が不正なアドレスキャッシュ内にあります			

これらの表を参照する際は、以下の点にご留意ください。

- 未処理の要求があっても問題とは限りません。単にサーバが多くの要求に対応している場合もあるからです。コストが高いサーバ上の未処理の要求は問題です。
- サーバのヘルスを示す第一の指標は現在のコストであり、問題が発生しているサーバを特定するのに役立ちます。

注: すべての要求の往復時間と未処理期間が測定されます。これは、トランスポート時間もコストの一部であることを意味します。この表でサーバに問題があるように見えても、他のサーバからは問題がないように見える場合、それはトランスポートの問題を示唆している可能性があります。

バックグラウンドスレッドトレース

ARCBackgroundResolveTimerThreadの動作を示すトレースを以下に示します。

```
ARCBackGroundResolveTimerThread started Interval = 60 MaxWait = 180000

Updating timer info for tcp:151.155.134.11:524

Updating timer info for udp:151.155.134.11:524

Updating timer info for tcp:151.155.134.13:524 ARCBackGroundResolveTimerThread
error -635 in DCConnectToAddress for tcp:151.155.134.59:524

ARCBackGroundResolveTimerThread completed in 0 seconds

8-total timers 4-stale timers 3-timers updated
```

上記のメッセージから、次のことが分かります。

- TCP:151.155.134.11は3分を超える期間使用されていません。
- UDP:151.155.134.11は3分を超える期間使用されていません。
- TCP: 151.155.134.13は3分を超える期間使用されていません。

上記のすべてのサーバでタイマー情報が更新され、次のような結果になりました。

- TCP: 151.155.134.59は依然としてこのサーバから到達できません。

新しいコストは非常に動的でとても頻繁に変化します。この動きを監視するには、詳細参照コストパラメータをデバッグモードに設定します。

注: 監視が終わったら、seNDSTRACE=!ARC1コマンドを実行して、ARCを非デバッグモードにリセットしてください。印刷が必要なければ、オーバーヘッドの印刷コストはないに越したことはありません。

DSTraceまたはNDSTraceでは、詳細参照コストと+RSLVがオンになっている場合、個々の参照コストが表示されます。残りのタグはset NDSTrace = nodebugコマンドを使用してオフにします。

```
Sorted results from DCAdjustCostAndSort follow:

137.65.10.3 cost of 217

137.65.10.9 cost of 222

137.65.10.10 cost of 400
```

リモートサーバが低速または過負荷になると、数値がすぐに変化します。ExRefサーバのコストは毎秒動的に調整されるため、一定期間のコストを監視するには、ログファイルをトレースする必要があります。

eDirectoryの正常動作の維持

ディレクトリサービスのヘルスはあらゆる組織にとって極めて重要です。NetIQ iMonitorを使用して定期的にヘルスチェックすることで、ディレクトリの円滑な機能が維持され、アップグレードやトラブルシューティングがずっと容易になります。

ヘルスチェックを実行する時期

一般に、ネットワークを頻繁に変更しない場合(2～3ヶ月程度の頻度でしかサーバとパーティションを追加せず、単純な変更だけを頻繁に行う場合)は、ヘルスチェックは月に1度実行します。

ネットワークの変更が頻繁に発生する場合(パーティションやサーバが毎週追加される、あるいは組織の再編成を行っている場合)、ヘルスチェックは週に1度実行します。

環境の変更に応じて、ヘルスチェックの頻度を調整します。ヘルスチェックの実行頻度に影響する要素を次に示します。

- パーティションとレプリカの数
- サーバを保持しているレプリカの安定度
- eDirectoryパーティション内の情報量
- オブジェクトのサイズと複雑さ
- 以前のDSRepairs内のエラー数

ヘルスチェックを実行すると、所有する権利に基づき、iMonitorがすべてのサーバから情報を集めます。なお、ヘルスチェックレポートを実行すると、ネットワークトラフィックが発生し、ディスク容量を消費する場合があることに注意してください。

ヘルスチェックの概要

完全なヘルスチェックでは、次の情報がチェックされます。

- eDirectoryのバージョン

  同じサーバ上で異なるバージョンのNDSやeDirectoryを実行していると、同期の問題が発生する可能性があります。NDSまたはeDirectoryのバージョンが古い場合は、Patches & Security Webサイト (http://support.novell.com/patches.html)から最新のソフトウェアパッチをダウンロードしてください。
- 時刻同期

  すべてのeDirectoryサーバは、正確な時刻を維持する必要があります。タイムスタンプが各オブジェクトおよびプロパティに割り当てられ、これによりオブジェクトおよびプロパティの更新が正しい順序で行われます。eDirectoryでは、タイムスタンプを使用して、同期が必要なレプリカを判別します。
- 同期の許容範囲

  インバウンドやアウトバウンドのデータ変更により同期を行ってから経過した期間で、どれだけのデータが未処理となっているかなどをチェックします。
- バックグラウンド処理

  プロセスはさまざまなタスクを実行しますが、その中には変更の複製およびシステム情報の保守があります。
  - 外部参照
  - 破損通知
  - eDirectoryスキーマ

これらのチェックを実行するための詳細な手順については、次のセクション(561 ページの「iMonitorを使用したeDirectoryのヘルスチェック」)を参照してください。

iMonitorを使用したeDirectoryのヘルスチェック

環境設定によっては、eDirectoryサーバのヘルスチェックをiMonitorの次の2つの方法のいずれかを使用して実行できます。

- ナビゲータフレームを使用する
- アシスタントフレームを使用する

ナビゲータフレームを使用する

1. iMonitorへアクセスする

   詳細については、241 ページの 「iMonitorへのアクセス」を参照してください。
2. ナビゲータフレームで、［レポート］アイコン  をクリックします。
3. アシスタントフレームで、［**レポート設定**］リンクをクリックします。

   データフレームに、実行可能レポートリストが表示されます。
4. 必要なサーバ情報の［レポートの設定］アイコン  をクリックします。

データフレームに、サーバ情報レポートが表示されます。このレポートを使用して、レポートに必要なオプションを選択します。

5 ［ヘルスのサブレポート］チェックボックスをオンにします。

6 指定した間隔でレポートを実行するには、データフレームの［レポートのスケジュール］セクションで、必要なオプションを選択します。

重要: スケジュールされたレポートを実行する場合は、Publicユーザとして実行され、認証済みユーザとして実行する場合よりも得られる情報が少なくなる可能性があります。

7 ［レポートの実行］をクリックして、レポートを処理します。

アシスタントフレームを使用する

1 iMonitorへアクセスする

詳細については、241 ページの 「iMonitorへのアクセス」を参照してください。

2 アシスタントフレームで、［エージェントヘルス］をクリックします。

iMonitorが情報を取得するサーバ(接続先のサーバとは限りません)のヘルスチェック情報が、データフレームに表示されます。

レポート情報の検討

レポートが生成されたら、データフレームにレポート結果が表示されます。ツリー内に正常でないサーバがある場合、レポートは次の3つのカテゴリに分けられます(グループ化はヘルス状態が悪いサーバから始まります)。

- 警告のあるサーバ
- 疑わしいサーバ
- 正常なサーバ

警告のあるサーバや疑わしいサーバがない場合は、これらのカテゴリは表示されません。

正常に動作していないサーバがある場合は、そのサーバの横の［エージェントヘルスサブレポート］リンクをクリックできます。オンラインの文脈依存型ヘルプを使用して、問題を解決します。このヘルプは、個々のオプションの意味、それが重要である理由、問題の解決方法、範囲の調整方法、およびヘルスチェックに追加するオプションがあるかどうかを確認するのに役立ちます。

重要: 警告のあるサーバがある場合、その問題を解決することを強くお勧めします。疑わしいサーバについても、評価することをお勧めします。

その他の情報

eDirectoryの正常な動作を維持するために使用するツールとテクニックについては、『NetIQ eDirectory Tools & Diagnostics Course 3007』を参照してください。このコースでは、次の方法について学習します。

- eDirectoryヘルスチェックの実行方法
- eDirectoryの正しい操作方法

- eDirectoryの問題の適切な診断、トラブルシューティング、および解決の方法
- eDirectoryトラブルシューティングのツールおよびユーティリティの使用方法

このコースの詳細については、NetIQトレーニングサービスのWebサイト (https://www.netiq.com/training/)を参照してください。

監視のためのリソース

NetIQ DSTraceユーティリティはWindowsとLinuxで動作します。このツールは、eDirectoryの膨大なリソースを監視するのに役立ちます。DSTraceの詳細については、次を参照してください。

- 253 ページの 「トレースを環境設定する」
- “Looking Into the Directory Services Trace (DSTrace) Options” (http://support.novell.com/techcenter/articles/anp20010801.html)
- “More on Using the DSTrace Command” (http://support.novell.com/techcenter/articles/anp20010901.html)

また、eDirectory環境用の他の管理ソリューションを提供するサードパーティの製品も使用できます。詳細については、次のWebサイトを参照してください。

- Symantec社 (http://www.symantec.com/compliance/)
- Blue Lance (http://www.bluelance.com)
- Quest (http://www.quest.com/active-directory/)

弊社のパートナーが提供していないeDirectoryの特性をモニタまたは監査する必要がある場合には、NetIQコンサルティングサービスが、NetIQ Event Systemを使用してカスタマイズされた評価と監査を行うためのお手伝いをいたします。

ハードウェアのアップグレードやサーバの交換

このセクションでは、ハードウェアをアップグレードまたは交換する際に、特定のサーバ上のeDirectoryを移す、または保護するための情報について説明します。ここでの説明は、「439 ページの 「NetIQ eDirectoryのバックアップと復元」」の情報に基づいています。

Backup eDirectory Management Toolを使用すれば、次の操作を行うためのeDirectory情報を作成できます。

- 564 ページの 「サーバを交換しないでハードウェアまたはストレージデバイスを計画的にアップグレードする」
- 566 ページの 「サーバの計画的な交換」

サーバを交換しないでハードウェアまたはストレージデバイスを計画的にアップグレードする

記憶デバイスやRAMなどのハードウェアのアップグレードを計画している場合、BackupeMtoolを使用してeDirectoryおよびファイルシステムのコールドバックアップを行います。これにより、サーバのeDirectory識別情報とファイルシステムデータが保護されます。このバックアップには、次の利点があります。

- 記憶デバイスを交換する場合、バックアップによって古い記憶デバイスから新しい記憶デバイスに情報を移すことができます。
- eDirectoryが格納されたディスクパーティションまたはディスクボリュームを含む記憶デバイスを交換する場合、このバックアップ情報を用いれば、復元プロセスを使用してeDirectoryデータベースを新しい記憶デバイス上に再構築できます。
- eDirectoryのコールドバックアップを実行し、その後でデータベースをクローズしておけば、バックアップ後のデータベースの変更を心配することなくハードウェアをアップグレードし、データベースを移すことができます。
- 何か問題が発生した場合、バックアップを使用して復元できます。

eDirectoryのコールドバックアップを実行する場合、オプションを使用してサーバ上のeDirectoryをロックし、使用不可にする必要があります。これにより、バックアップ後のデータ変更を防げます。このサーバと通信している他のサーバからは、このサーバは停止しているように見えます。通常サーバに送信されるeDirectory情報は、そのサーバと再び通信できるようになるまで、ツリー内の別のサーバに保存されます。保存された情報は、サーバがオンライン状態に戻ったときに、サーバを同期するために使用されます。

注: eDirectoryツリー内の他のサーバは、このサーバがすぐにオンライン状態に戻ると期待しているため、アップグレードをすばやく完了させ、できるだけ早くサーバ上のeDirectoryデータベースをオープンする必要があります。

ハードウェアのアップグレードを計画的に実行するには、次の手順に従います。

1. アップグレードによりサーバに問題が発生するかもしれないと心配なら、必要に応じて、使用する別のコンピュータを準備するとよいでしょう。

   詳細については、566 ページの 「1. サーバ交換の準備」を参照してください。

2. eDirectoryデータベースのコールドバックアップを実行し、その後でデータベースをクローズし、ロックしたままにしておくには、クライアントコマンドを次のように使用します。NICIを使用する場合は、セキュリティファイルもバックアップします。

   ```
   backup -f backup_filename_and_path
   -l log_filename_and_path -t -c -o -d
   ```

   NICIを使用する場合は、NICIファイルをバックアップします。クライアントとスイッチの使用についての詳細は、「463 ページの 「DSBKによる手動バックアップ」」と「467 ページの 「バックアップ/復元のコマンドラインオプション」」を参照してください。

   これで、eDirectoryデータベースはロックされました。手順を完了するまでは、サーバ上で新たなデータ変更が実行されないように、データベースをロックしたままにしておく必要があります。

   サーバが使用できない時間を最小限に抑えるために、以降の手順をすばやく完了させます。

3. お好みのバックアップツールを使用して、ファイルシステムをバックアップします。

データベースをバックアップした*後*で、ファイルシステムのバックアップを行うのは重要です。これにより、eDirectoryバックアップファイルが、他のファイルシステムと一緒にテープに保存されます。

4 サーバを停止させ、ハードウェアを交換します。

5 ハードウェアを交換した後で、ハードウェア変更の種類に応じた以下の手順を実行します。

ハードウェア変更の種類...	実行する手順
記憶デバイスに変更がない場合	サーバを起動し、データベースのロック解除を行います。
記憶デバイスの交換を行ったが、eDirectoryが格納されたディスクパーティション/ボリュームに変更はない場合	1. サーバとeDirectoryを起動します。 2. 交換した記憶デバイス上にあったディスクパーティション/ボリュームのファイルシステムだけを復元します。 3. eDirectoryデータベースのロックを解除します。
eDirectoryが保存されたストレージデバイスを交換した場合	1. 必要に応じてオペレーティングシステムをインストールします。 2. 記憶デバイスの変更により影響を受けたディスクパーティション上に、ファイルシステムを復元します。 3. 新しい記憶デバイス上の、新しい一時的なツリー内に、eDirectoryをインストールします。 4. バックアップからeDirectoryを復元します(元のツリー内に配置されます)。このとき、復元した後でeDirectoryがクローズされ、ロックされたままになるようにオプションを指定します。restore-r-f *backup_filename_and_path* -l *log_filename_and_path*などのコマンドを使用します。インクルードファイルに列挙されたファイルをバックアップしてから、NICIファイルを別個に復元する場合は、-uオプションを追加します。 5. eDirectoryデータベースのロックを解除します。 6. NICIセキュリティファイルを復元した場合は、復元を完了した後で、サーバを再起動してセキュリティシステムを再初期化します。 7. サーバが通常どおりに応答するかをチェックします。iMonitorを使用して、サーバとその同期をチェックします。 8. このサーバでロールフォワードログを使用していた場合、復元を完了した後で、ロールフォワードログ設定を再作成します。ロールフォワードログ記録を有効にしてから、改めてフルバックアップも取る必要があります。復元した後は、設定がデフォルトの状態にリセットされます。つまり、ロールフォワードログ記録がオフになります。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

サーバが通常どおりに応答しない場合、次にいずれかの方法によって回復する必要がある場合があります。

- 変更前のハードウェア環境設定が機能していたことから、これを再作成します。
- 作成したeDirectoryとファイルシステムのバックアップを使用して、このサーバの識別情報を別のマシンに移します。詳細については、566 ページの 「サーバの計画的な交換」を参照してください。

サーバの計画的な交換

次に示す手順は、サーバのeDirectory資格情報とファイルシステムデータを別のマシンに移して、実際にサーバを置き換えた場合です。ここでは、古いサーバをサーバAとし、それに置き換わるサーバをサーバBとしています。

Backup eMToolを使用してeDirectoryのコールドバックアップ(データベースをクローズした状態でのバックアップ)を実行し、さらにお好みのツールを使用してファイルシステムのバックアップをして、サーバの交換に備えます。このバックアップ情報を用いれば、復元プロセスを使用して、新しいコンピュータ上にサーバを再構築できます。

eDirectoryのコールドバックアップを実行する場合、オプションを使用してサーバA上のeDirectoryをロックし、使用不可にする必要があります。これにより、バックアップ後のデータ変更を防げます。このサーバと通信している他のサーバからは、このサーバは停止しているように見えます。通常サーバに送信されるeDirectory情報は、そのサーバと再び通信できるようになるまで、ツリー内の別のサーバに保存されます。保存された情報は、新しいコンピュータであるサーバB上で、サーバがオンライン状態に戻ったときに同期するために使用されます。

注: eDirectoryツリー内の他のサーバは、このサーバがすぐにオンライン状態に戻ることを期待しているため、できるだけ早く交換してサーバにeDirectory情報を復元する必要があります。

サーバを置き換えるための手順の概要を次に示します。

1. 交換する際のサーバAの停止時間を短くするには、「566ページの「1.サーバ交換の準備」」で説明しているようにサーバBにオペレーティングシステムをインストールするなどして、交換前にできるだけサーバBの準備を整えておきます。
2. 「567 ページの 「2. eDirectoryのバックアップの作成」」の説明に従って、サーバAのeDirectoryとシステムファイルをバックアップします。
3. 「568 ページの 「3. サーバ交換におけるeDirectory情報の復元」」の説明に従って、サーバBに情報を移します。

1. サーバ交換の準備

次に示すサーバAとサーバBのチェックリストを使用して、サーバAを交換する準備ができているかを確認します。開始する前にサーバBの準備をしておけば、あるコンピュータから別のコンピュータへ転送する間のサーバの停止時間を減らすことができます。

サーバAの準備

❒ サーバAに最新のバージョンのオペレーティングシステムがインストールされていることを確認します。

- ❒ Treeパーティションのマスタを保持しているサーバでDSRepairを実行し、さらに時刻同期を実行して、サーバAのツリーが正常に機能していることを確認します。
- ❒ サーバAのデータベースでDSRepairを実行します。サーバAが完全に同期されていることを確認します。

サーバBの準備

- ❒ 最新バージョンのオペレーティングシステムをインストールします。このオペレーティングシステムは、サーバAのものと同じである必要があります。
- ❒ サーバBを新しい一時的なツリーに配置し、eDirectoryをインストールします。

  (「568 ページの 「3. サーバ交換におけるeDirectory情報の復元」」の過程でeDirectoryを復元するには、サーバBをサーバAが配置されていた元のツリー内に配置します)。

次のセクション(567 ページの 「2. eDirectoryのバックアップの作成」)の手順に進みます。

2. eDirectoryのバックアップの作成

サーバ交換の前に、eDirectoryのバックアップを作成する必要があります。「566 ページの 「1. サーバ交換の準備」」が完了した後は Clientを使用し、バックアップの後でデータベースを使用不可にしてロックする詳細オプションを設定して、サーバA上のeDirectoryデータベースのコールドバックアップを実行します。

eDirectoryのコールドバックアップ(データベースがクローズ中のバックアップ)を作成し、その後でデータベースをクローズのままにしておくには、次の手順に従います。

1. が完了していることを確認します。566 ページの 「1. サーバ交換の準備」
2. クライアントで、-c、-o、および-dスイッチを指定した次のようなbackupコマンドを用いてサーバA上のeDirectoryデータベースのコールドバックアップを実行し、完了後もデータベースをクローズしてロックしたままにします。

   backup -f *backup_filename_and_path* -l *log_filename_and_path* -t -c -o -d

   NICIを使用する場合は、NICIファイルをバックアップします。クライアントとスイッチの使用についての詳細は、「463 ページの 「DSBKによる手動バックアップ」」と「467 ページの 「バックアップ/復元のコマンドラインオプション」」を参照してください。

   サーバAのeDirectoryデータベースは現在ロックされています。データベースをサーバB上に復元しツリー内に戻すまでは、サーバ上で新たなデータ変更が実行されないように、データベースをロックしたままにしておく必要があります。

   サーバアップグレードまたはサーバ交換の残りの手順を迅速に完了させ、サーバが使用できない時間を最小限に抑えます。
3. サーバAのファイルシステムのフルバックアップを作成します。

   データベースをバックアップした*後*で、ファイルシステムのバックアップを行うのは重要です。これにより、eDirectoryバックアップファイルが、残りのファイルシステムと一緒にテープに保存されます。

   SMSの使用方法の詳細については、『*Storage Management Services Administration Guide (Storage Management Services管理ガイド)* (http://www.novell.com/documentation/oes/smsadmin/data/hjc2z4tu.html)』を参照してください。

4 サーバA上のeDirectoryデータベースをロックし、サーバAをネットワークから外します。

続いて「568 ページの 「3. サーバ交換におけるeDirectory情報の復元」」の手順を実行します。

3. サーバ交換におけるeDirectory情報の復元

サーバAのeDirectory識別情報およびファイルシステムをサーバBに移すには、次の手順に従います。

1 「566 ページの 「1. サーバ交換の準備」」および「567 ページの 「2. eDirectoryのバックアップの作成」」が完了していることを確認します。

2 サーバBが起動し、eDirectoryが実行されていることを確認します。

3 次のように、restore を使用して、サーバAのeDirectory識別情報とファイルシステムをサーバBに移します。

3a サーバAのeDirectoryコールドバックアップファイルをサーバBにコピーします。

サードパーティのファイル圧縮ツールは圧縮性能が良いので、そのようなツールを使用した場合、バックアップファイルはとても小さくなることがあります。これにより、ファイルのコピーを早くできる場合があります。

3b 複製したeDirectoryのバックアップファイルを使用して、サーバAのeDirectoryデータベースをサーバB上に復元します。それには、コマンドラインクライアントで、次のようなコマンドを使用します。

restore -r -f *backup_filename_and_path* -l *log_filename_and_path*

NICIを使用する場合は、NICIファイルを復元します。インクルードファイルに列挙されたファイルをバックアップしてあった場合は、-uオプションを追加します。クライアントとスイッチの使用についての詳細は、「466ページの「DSBKによるバックアップファイルの復元作業」」と「467 ページの 「バックアップ/復元のコマンドラインオプション」」を参照してください。

復元にはロールフォワードログを含める必要はありません。なぜなら、コールドバックアップを実行し、その後でデータベースをクローズしてあるからです。データベースではどのようなトランザクションも実行されていません。データベースはクローズされており、バックアップ以降、ロールフォワードログは作成されていません。

3c バックアップされたサーバAのファイルシステムデータをサーバBに移します。

4 NICIを使用している場合は、サーバを再起動してNICIを再初期化し、復元されたNICIセキュリティファイルが使用されるようにします。

5 eDirectoryデータベースのロックを解除します。

6 復元が完了した後は、サーバBがサーバAの識別情報を正しく引き継ぎ、通常どおりに応答しているかチェックします。iMonitorを使用してサーバとその同期をチェックします。

サーバの応答が通常どおりなら、サーバの交換は完了です。これで、サーバAからeDirectoryをアンインストールしてeDirectory識別情報を削除し、このコンピュータを別の目的に使用できます。サーバAをネットワークに戻すのは、eDirectoryを削除した後にしてください。そうしないと、eDirectoryの同期でネットワークが混乱してしまいます。なぜなら、サーバAとサーバBの同じ識別情報により、競合が発生するためです。

7 (特定条件における処理)このサーバでロールフォワードログを使用していた場合、復元を完了した後で、ロールフォワードログ設定を作成し直します。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

   復元した後は、設定がデフォルトの状態にリセットされます。つまり、ロールフォワードログがオフになっています。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

サーバBが正常に動作せず、サーバAの識別情報およびファイルシステムを直ちに使用できるようにする必要がある場合は、次を実行します。

1 サーバBのネットワークケーブルを外すか、サーバBを停止します。
2 サーバAをネットワークに再接続し、起動してから、eDirectoryデータベースをオープンします。

   DSRepairの実行を要求するシステムメッセージを無視します。
3 サーバBからeDirectoryを削除し、再度アップグレードを試みます。

サーバのIPアドレスの変更

サーバのIPアドレスが変更されることはあまりありません。IPアドレスが変更された場合は、すべてのeDirectoryインスタンスのnds.confファイルを新しいIPアドレスで更新する必要があります。IPアドレスが頻繁に変更される場合は、nds.confでIPアドレスの代わりにインタフェース名を使用する必要があります。

例: n4u.server.interfaces=eth0@1524

IPアドレスが変更されても、サーバのIPベースのキーマテリアルオブジェクト(KMO)は自動的に更新されません。古いKMO(名前にIPが含まれている)を削除する必要はありませんが、削除すればツリーが見やすくなります。ndsconfig upgradeコマンドを実行して、KMOを再作成し、それらをNCPサーバオブジェクトとLDAPサーバオブジェクトにリンクさせます。

注: ndsconfig upgradeを実行すると、eDirectoryインスタンスが再起動されます。

これで、サーバは新しいアドレスをリスンするようになります。ツリー内に複数のサーバが存在する場合は、DSRepairネットワーク修復オプションを実行します。

ndsrepair -N

修復オプションの実行後に、eDirectoryサーバを再起動します。

サーバのIPアドレスの変更に関する詳細については、TID# 3201067 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3201067&sliceId=SAL_Public&dialogID=360088499&stateId=0%200%2036014447)を参照してください。

ハードウェア障害後のeDirectoryの復元

eDirectoryが配置されたディスクパーティションまたはディスクボリュームを含むハードディスクの障害は、サーバからeDirectoryが削除された状態と同じです。幸い、複数サーバ環境では、1つのサーバがダウンしても、そのレプリカリング内の残りのサーバが正常に稼働していれば問題はありません。

eDirectoryが格納されたディスクパーティションまたはディスクボリュームの障害の後でeDirectoryを復元するには、「457 ページの「復元処理の準備」」および「606 ページの「iManagerによるバックアップファイルの復元作業」」(または、「466 ページの 「DSBKによるバックアップファイルの復元作業」」)で説明している手順に従って、バックアップファイルから復元します。

ハードディスクの新規インストールでは、製造元から提供されている指示に従って、サーバのハードディスクが動作することを検証します。新しいハードディスクには、少なくとも置き換えられる元のドライブと同じ記憶容量が必要です。ローカルサーバ情報のファイルを使用して、環境設定情報を確認します。

注

- ウイルス対策またはバックアップソフトウェアのプロセスから、eDirectoryサーバ上のDIBディレクトリを除外することをお勧めします。DIBディレクトリのバックアップは、eDirectoryバックアップツールを使って行えます。eDirectoryのバックアップの詳細については、439 ページの 「NetIQ eDirectoryのバックアップと復元」を参照してください。
- サーバのバックアップファイルがない場合は、Xbrowseを使用して、サーバ情報の回復に役立つ情報をeDirectoryに問い合わせてください。この作業は、サーバオブジェクトやその関連オブジェクトをツリーから削除する前に実行する必要があります。Xbrowseの詳細については、NetIQサポートのWebサイト (http://support.novell.com/docs/Readmes/InfoDocument//2960653.html)を参照してください。

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 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。

コンテナの準備状況

エントリキャッシュの使用率を最適化し、属性検索操作のパフォーマンスを向上させるため、FLAIMは、値のサイズが大きい属性または値の個数が多い属性を、属性コンテナと呼ばれる別の場所に格納します。デフォルトでは、次の条件を満たす属性がコンテナに自動的に移されます:

- 値の数が25個を超えている
- 値のサイズが2048バイトを超える

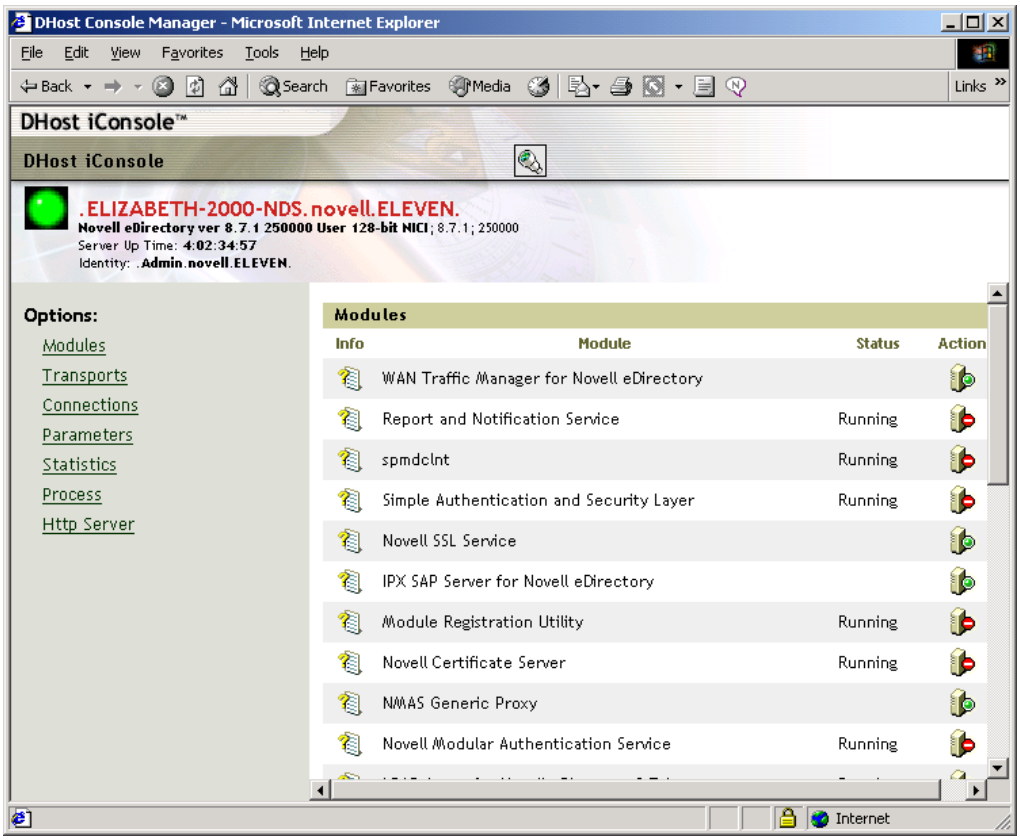
eDirectoryには、別の属性コンテナへの属性の移動を制御するための柔軟性が備えられています。管理者は、必要に応じて、属性の移動をスケジュールできます。詳細については、『NetIQ eDirectory Tuning Guide』の「FLAIM Attribute Containerization」を参照してください。

20 DHost iConsole Manager

DHost iConsole ManagerはWebベースのブラウザを使用した管理ツールで、次のことが行えます。

- DHostモジュールの管理
- DHost環境設定パラメータの照会
- DHost接続情報の表示
- スレッドプール統計情報の表示
- DHostプロトコルスタックマネージャにより登録されたプロトコルに関する詳細情報の表示

図 20-1 DHost iConsole Manager



この章では、次の情報について説明します。

- 574 ページの 「DHostについて」
- 574 ページの 「DHost iConsoleの実行」
- 575 ページの 「eDirectoryモジュールの管理」
- 577 ページの 「DHost情報の照会」
- 579 ページの 「プロセススタック」

DHostについて

WindowsとLinux向けのNetIQ eDirectoryソフトウェアはすべて同じコアコードに基づいてビルドされています。WindowsおよびLinux版のeDirectoryが別のバージョンのeDirectoryと適切にやり取りするには、NCP (NetWare Core Ptotocol)サービスのサブセットをサポートしている必要があります。このサブセットを操作するプログラムはDHostと呼ばれます。DHostは、eDirectory下で動作し、NCPがネイティブで備えている機能を提供します。

DHostは次のサービスを提供します。

サービス	説明
NCPエンジン	クライアントがeDirectoryサーバに要求を送信したり、eDirectoryサーバから応答を受信したりできるようにするパケットベースのプロトコル。 詳細については、「NetWare Core Protocols NDK (http://developer.novell.com/documentation/ncp/index.html)」を参照してください。
ウォッチドッグ	ワークステーションがeDirectoryサーバに接続された状態であることを確認するために使用するパケットです。 詳細については、「Watchdog Packet Spoofing」を参照してください。
接続テーブル	eDirectoryサーバに付随するあらゆるプロセス、プリントサーバ、アプリケーション、ワークステーション、またはその他のエンティティに割り当てられる固有の番号です。この番号は、接続が行われるごとに異なる可能性があります。接続番号は、ネットワークセキュリティの実装やネットワークアカウントに使用されます。この番号は、ファイルサーバ接続テーブル内でのオブジェクトの場所を反映しています。さらにこの番号を使用すると、ネットワークにログインしたオブジェクトに関する情報の識別や取得が容易になります。
イベントシステム	個々のサーバのアクティビティを監視する手段をアプリケーションに提供します。
スレッドプール	独立したエンティティとして実行され、システムソフトウェアによってスケジュールされる一連の命令です。
NCP拡張	サーバアプリケーション開発者が、NCPとして実装するNLM™ソフトウェアを作成できるようにします。 詳細については、NCP NDKの「NCP Extension (http://developer.novell.com/documentation/ncp/ncp__enu/data/alne6tm.html)」を参照してください。
メッセージ処理	ドキュメントを圧縮または凝縮した形式、またはドキュメントの要約で、大きなドキュメントの電子指紋として機能します。メッセージ処理は、個々のドキュメントに固有のデジタル署名を作成するために使用されます。

DHost iConsoleの実行

- 575 ページの 「WindowsでDHost iConsoleを実行する」
- 575 ページの 「LinuxでDHost iConsoleを実行する」

WindowsでDHost iConsoleを実行する

1 Webブラウザを開きます。

2 アドレス(URL)フィールドに、次の形式で入力します。

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

たとえば、次のように入力します。

```
http://MyServer:80/dhost
```

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

```
http://137.65.135.150:80/dhost
```

3 ユーザ名、コンテキスト、パスワードを指定します。

LinuxでDHost iConsoleを実行する

1 Webブラウザを開きます。

2 アドレス(URL)フィールドに、次の形式で入力します。

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

次に例を示します。

```
http://MyServer:80/dhost
```

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

```
http://137.65.135.150:80/dhost
```

3 ユーザ名、コンテキスト、パスワードを指定します。

eDirectoryモジュールの管理

DHost iConsoleのモジュールページでは、使用可能なeDirectoryサービスとその状態についての情報が表示されます。また、このモジュールページからこれらのサービスを開始または停止(ロードまたはアンロード)できます。

ロードやアンロードができるのは、LDAP、SNMP、HTTPSTKなどの非対話型モジュールだけです。

モジュールページには、次に示す属性があります。

属性	説明
Info	 をクリックして、選択したモジュールのモジュールの説明、ファイル名、モジュールハンドル、属性、および共有オブジェクト名を表示します。
モジュール	モジュール名を表示します。
ステータス	モジュールが実行されているかどうかを表示します。
アクション	モジュールが実行可能かどうかを示します。モジュールのステータスは、次の3つのうちのどれかになります。 •  は、モジュールがシステムモジュールで、アンロードできないことを示します。 •  は、モジュールがロード可能で、ロードの準備ができていることを示します。 •  は、モジュールが実行中であることを示します。

- 576 ページの 「Windowsでモジュールをロードまたはアンロードする」
- 577 ページの 「Linuxでモジュールをロードまたはアンロードする」

NetIQ iManagerを使用したeDirectoryサービスのロードやアンロードについての詳細は、209 ページの 「eDirectory Service Manager」を参照してください。

Windowsでモジュールをロードまたはアンロードする

1 Webブラウザを開きます。

2 アドレス(URL)フィールドに、次の形式で入力します。

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

たとえば、次のように入力します。

```
http://MyServer:80/dhost
```

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

```
http://137.65.135.150:80/dhost
```

3 ユーザ名、コンテキスト、パスワードを指定します。

4 ［モジュール］をクリックします。

5  をクリックしてモジュールをロードするか、  をクリックしてモジュールをアンロードします。

Linuxでモジュールをロードまたはアンロードする

1 Webブラウザを開きます。

2 アドレス(URL)フィールドに、次の形式で入力します。

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

たとえば、次のように入力します。

```
http://MyServer:80/dhost
```

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

```
http://137.65.135.150:80/dhost
```

3 ユーザ名、コンテキスト、パスワードを指定します。

4 ［**モジュール**］をクリックします。

5  をクリックしてモジュールをロードするか、  をクリックしてモジュールをアンロードします。

DHost情報の照会

DHost iConsoleマネージャを使用すれば、次に示す情報を照会できます。

- 環境設定パラメータ
- PSTACKマネージャを使用して登録されたプロトコル
- 接続プロパティ
- スレッドプールの概要

環境設定パラメータを表示する

環境設定パラメータは、Linuxに特有のものです。

DHost iConsole Managerで、［**パラメータ**］をクリックします。詳細については、575 ページの「LinuxでDHost iConsoleを実行する」を参照してください。

環境設定パラメータには、次の情報が表示されます。

オプション	説明
パラメータ名	環境設定パラメータの名前を表示します。
［デフォルト値］	環境設定パラメータのデフォルト値を表示します。
設定する値	現在の設定値を表示します。
Minimum value	パラメータに設定できる最小値を表示します。
Maximum value	パラメータに設定できる最大値を表示します。
タイプ	パラメータに設定できる値のタイプを表示します。

詳細については、『「NetIQ Directoryインストールガイド」』の「*環境設定パラメータ*」を参照してください。

プロトコル情報を表示する

DHost iConsole Managerで、［**トランスポート**］をクリックします。

次のプロトコル情報が表示されます。

- ID
- プロトコル
- トランスポート

接続プロパティを表示する

DHost iConsole Managerで、［**接続**］をクリックします。

次の接続プロパティが表示されます。

- 接続
- フラグ
- ID
- 表示名
- トランスポート
- 認証名
- SEV回数
- 最終アクセス
- ロック状態

スレッドプールの統計情報を表示する

DHost iConsole Managerで、［**統計情報**］をクリックします。

次のスレッドプール統計情報が表示されます。

- Spawned Threads(生成スレッド)
- Dead Threads(停止スレッド)
- Idle Threads(アイドルスレッド)
- Worker Thread(動作スレッド)
- Peak Worker Thread(ピーク動作スレッド)
- Ready for Work Thread(動作待機スレッド)
- Ready Queue Peak Worker Threads(待機キューピーク動作スレッド)
- Ready Queue Max Wait Time(待機キュー最大待ち時間)
- Schedule Delay Minimum Time(最小スケジュール遅延時間)
- Schedule Delay Maximum Time(最大スケジュール遅延時間)

- Schedule Delay Average Time(平均スケジュール遅延時間)
- Waiting For Work(動作待ち)
- Peaking Waiting For Work(ピーク動作待ち)

プロセススタック

プロセススタックには、DHostのプロセス空間で現在実行されているすべてのスレッドのリストが含まれます。スレッドに関する詳細な情報は、スレッドIDをクリックして取得できます。この機能は、主にNetIQエンジニアやサポート担当者により、ローレベルのデバッグツールとして使用されます。

このオプションは、Windowsでのみ使用できます。

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

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

   たとえば、次のように入力します。

   ```
   http://MyServer:80/dhost
   ```

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

   ```
   http://137.65.135.150:80/dhost
   ```

3. ユーザ名、コンテキスト、パスワードを指定します。
4. ［**プロセス**］をクリックします。
5. スレッドのコールスタックを表示するには、スレッドIDをクリックします。

21 sadminパスワードの設定

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

注: sadminユーザ名は大文字と小文字が区別されます。

---

ndspassstoreユーティリティを使用して、WindowsシステムとLinuxシステム上でsadminパスワードを設定します。

サーバコンソールで次のコマンドを入力します。

ndspassstore -a sadmin -w <*password*>

ここで、sadmin(管理者コンテキスト)は管理権限を持つユーザの完全識別名で、passwordは認証用のパスワードです。複数インスタンスのシナリオでは、該当するインスタンスを選択します。

例: ndspassstore -a sadmin -w pass

デフォルトでndspassstoreは、Windowsでは**C:\Novell\NDS**に、UNIXでは**/opt/novell/eDirectory/bin**にあります。

22 eDirectory Management Toolbox

NetIQ eDirectory管理ツールボックス(eMBox)を使用すると、サーバ上でもリモートでもeDirectoryのバックエンドユーティリティすべてにアクセスできます。

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

重要: 管理者を含むすべてのユーザに対し、iManagerで、タスクの実行のために管理するツリーに、スコープを選択して、役割ベースのサービスを設定する必要があります。

---

iManagerのeDirectoryの保守メニューの下にある次のタスクに対して役割ベースのサービスを設定する必要があります。

- バックアップ環境設定
- ツリーの結合
- eDirectoryの修復
- サーバの修復
- 同期の修復
- レプリカの修復
- レプリカリングの修復
- 復元
- スキーマの保守
- サービスマネージャ
- ツリーのマージ
- ツリー名の変更

すべての機能は、ローカルサーバまたはリモートのいずれからでもコマンドラインクライアントを通じて使用できます。クライアントを使用して、1つのサーバまたはワークステーションから複数のサーバに対するタスクを実行できます。

バックアップ、DSRepair、DSMerge、スキーマの操作、およびeDirectory サービスマネージャなどのすべてのeDirectory Management Tool(eMTool)を実行するには、eDirectoryサーバにeMBoxをロードして実行する必要があります。

注: eMToolの使用方法については、957 ページの 「Linuxでのユーティリティのトラブルシューティング」を参照してください。

この節では、次の項目について説明します。

- 594 ページの 「eMBoxクライアントを使ったバックアップ/復元作業」
- 602 ページの 「NetIQ iManagerを使ったバックアップ/復元作業」

コマンドラインクライアントの使用

にアクセスする方法の1つは、eMBoxのJavaコマンドラインクライアントを使用することです。このコマンドラインクライアントには、対話式モードとバッチモードの2つのモードがあります。対話式モードでは、コマンドを一度に1つづつ実行します。バッチモードでは、コマンドのグループを自動で実行できます。コマンドラインクライアントにはログサービスがあり、いずれのモードでも使用できます。

コマンドラインクライアントは、Javaアプリケーションです。これを実行するには、Azul ZuluOpenJDKの最新バージョン(1.8以上)をインストールする必要があります。また、古いバージョンのJavaすべてで、使用可能なパッチアップグレードをインストールしてアップグレードしてください。最新バージョンのJavaをインストールしたら、次の環境変数をエクスポートします。

- EDIR_JAVA_HOME
- JAVA_HOME
- JRE_HOME

注

- Linuxで前述の環境変数が何も検出されないと、コマンドラインクライアントはデフォルトPATH環境変数でJavaバイナリを検索します。
- eDirectory 9.1 SP2以降では、Azul ZuluOpenJDK 1.8.0_192がサポートされています。

例

環境変数の例のいくつかを以下に記します。

- **Linux**
  - EDIR_JAVA_HOME=/usr/java/java1.8.0_131
  - JAVA_HOME= /usr/java/java1.8.0_131
  - JRE_HOME= /usr/java/java1.8.0_131/jre
- **Windows**
  - EDIR_JAVA_HOME= C:\Program Files\Java\jdk1.8.0_131
  - JAVA_HOME= C:\Program Files\Java\jdk1.8.0_131
  - JRE_HOME= C:\Program Files\Java\jdk1.8.0_131\jre

また、ファイアウォール越しに管理対象のサーバにアクセスできる必要があります。1つのサーバまたはワークステーションから、複数のサーバに対してタスクを実行できます。

注: eDirectory Management Toolboxは、コマンドラインクライアントとコマンドラインヘルプの両方とも、英語にのみ対応しています。

この節では、次の項目について説明します。

コマンドラインヘルプを表示する

クライアントを実行する前に、の一般的なコマンドラインヘルプを表示するには、次の操作を実行します。

- Linux: コマンドラインで、「edirutil -?」と入力します。
- Windows: *drive*\novell\nds\\edirutil.exe -?を実行します。

インタラクティブモードでのインタラクティブなコマンドラインヘルプを表示するには、クライアントのプロンプトで疑問符(?)を入力します。たとえば、「Client> ?」のように入力します。

ヘルプには、591 ページの 「eMBoxコマンドラインクライアントのオプション」で示すようなコマンドラインオプションに関する情報が表示されます。

コマンドラインクライアントを対話式モードで実行する

対話式モードでは、コマンドを一度に1つづつ実行します。

この節では、次の項目について説明します。

eDirectoryサーバでクライアントを実行する

クライアントおよびSun JVM 1.3.1は、eDirectoryと同時にインストールされています。
eDirectoryサーバの対話式モードでクライアントを開始するには、次の操作を行います。

- Linux: コマンドラインで、「edirutil -i」と入力します。
- Windows: *drive*\novell\nds\edirutil.exe -iを実行します。

edirutilファイルは、クライアントを実行するためのショートカットです。これは、Java実行可能ファイルと、eDirectoryでクライアントがインストールされるデフォルトの場所を指しています。この情報は、586 ページの 「クライアント用にパスおよびクラスパスをセットアップする」に記載されているようにして手動で入力することもできます。

管理するサーバに対してコマンドラインクライアントを使用するには、ファイアウォールの後ろ側へのアクセスが必要になります。したがって、リモートからの操作にはVPNアクセスが必要となります。

ワークステーションでクライアントを実行する

eDirectoryサーバではないコンピュータでクライアントを使用するには、次の操作を実行します。

- eMBoxClient.jarファイルをeDirectoryサーバから自分のマシンにコピーします。
  - Windows: \novell\nds\\eMBoxClient.jar
  - Linux: /opt/novell/eDirectory/lib/nds-modules//eMBoxClient.jar
- Sun JVM 1.3.1がインストールされていることを確認します。
- 管理するサーバに対してコマンドラインクライアントを使用するためには、ファイアウォール越しにアクセスできることを確認します。

ワークステーション上では、サーバ上のようにクライアントをインタラクティブモードで開くためのショートカットとしてedirutilコマンドを使用することはできません。パスおよびクラスパス内で環境をセットアップするか、パスをその都度手動で入力します。詳細については、586 ページの 「クライアント用にパスおよびクラスパスをセットアップする」を参照してください。

クライアント用にパスおよびクラスパスをセットアップする

eDirectoryサーバ上でクライアントを実行している場合、JavaファイルまたはeMBoxClient.jarファイルの場所を変更していなければ、クライアントの実行へのショートカットとしてedirutilを使用することができます。詳細については、585 ページの 「eDirectoryサーバでクライアントを実行する」を参照してください。

ただし、デフォルトの場所を変更した場合、またはeMBoxClient.jarファイルをサーバでないマシン上で実行している場合、あるいはクラスパスを手動で入力したい場合は、クライアントのパスおよびクラスパスをこのセクションの説明のようにセットアップする必要があります。

次の操作を実行すれば、クライアントをコンピュータ上のどの場所からでも実行できます。

- Java実行ファイル(Java.exeなど)があるディレクトリをパスに追加するか、またはJavaがすでに実行されていることを確認します。

  サーバの場合、ほとんどはすでに実行されています。Windowsサーバ、Linuxサーバ、およびUNIXサーバでは、実行ファイルのディレクトリをパスに追加する必要があります。

  ワークステーションの場合、手動セットアップが必要となる場合があります。たとえば、Windwosでは、［**スタート**］>［**設定**］>［**コントロール パネル**］>［**システム**］の順にクリックします。［**詳細設定**］タブで、［**環境変数**］をクリックし、［**パス**］変数にパスを追加します。

  パスを手動で入力するには、次の操作を実行します。 Java実行ファイルへのパスが追加されていない場合は、まずコマンドラインでJava実行ファイルが含まれたディレクトリへ移動してから、実行する必要があります。たとえば、Windowsでは、「cd c:\novell\nds\\jre\bin」と入力します。

- eMBoxClient.jarファイルへのパスを、クラスパスに追加します。

  Windowsサーバまたはワークステーション: set CLASSPATH=*path*\eMBoxClient.jar

  Linuxサーバまたはワークステーション: export CLASSPATH=*path*/eMBoxClient.jar

  パスを手動で入力するには、次の操作を実行します。 クラスパスを指定する他の方法としては、次のように、実行するときにその都度Javaの-cpフラグを使用する方法もあります。

  ```
  java -cp path/eMBoxClient.jar -i
  ```

  たとえば、Windowsでは、「java -cp c:\novell\nds\\eMBoxClient.jar -i」と入力します。

これらの手順を実行した後は、次のコマンドを使用して、コンピュータ上のどの場所からでも対話式モードによるeMBoxクライアントを実行できます。

```
java  -i
```

Javaコマンドに関する詳細については、OracleのWebサイト (http://www.oracle.com/technetwork/java/)でJavaのマニュアルを参照してください。

サーバにログインする

サーバにログインするには、サーバ名またはIPアドレス、および特定のサーバへ接続するためのポート番号を指定する必要があります。パブリックログインの場合はユーザ名とパスワードは不要です。

たとえば、クライアントを対話式モードでオープンした後で、次のように入力します。

```
login -s 137.65.123.244 -p 8008 -u admin.mycompany
-w mypassword -n
```

ポート番号についての詳細は、592 ページの 「eDirectoryポート番号を確認する」を参照してください。

使用言語、タイムアウト、およびログファイルを設定する

デフォルトの言語は、クライアントシステムの言語です。そのため、ほとんどの場合、特別に言語を設定する必要はありません。同様に、タイムアウトもほとんどの場合、デフォルトの設定で問題ありません。ログファイルを設定するには、ファイル名とファイルを開くモード(追加または上書き)を指定します。

次の表に、コマンド例を示します。

コマンド	説明
set -L en,de	使用言語を英語、ドイツ語の優先順で設定します。
set -T 100	タイムアウトを100秒に設定します。タイムアウトは、サーバからの応答を待つ時間を設定するものです。
set -l mylog.txt -o	ログファイルとしてmylog.txtを使用し、上書きモードで開きます。 デフォルトの設定は「追加」です。

eMToolとそのサービスを表示する

サーバにログインしたら、listコマンドを使用して、そのサーバ上で使用できるサービスを表示できます。

listコマンドを使用すると、次に示すeMToolとそのサービスが動的に表示されます。

eMTool	説明
バックアップ	NetIQ eDirectory Backup eMTool
DSMerge	NetIQ eDirectory Merge eMTool
DSRepair	NetIQ eDirectory Repair eMTool
DSSchema	NetIQ eDirectory Schema Operations eMTool
service	NetIQ eDirectory Service Manager eMTool

リストを強制的にリフレッシュするには、-rを使用します。サービスの詳細を表示するには、-tを使用します。コマンド形式のみを表示するには、-fを使用します。

次の表に、コマンド例を示します。

コマンド	説明
リスト	サーバ上で使用できるeMToolを表示します。
list -r	eMToolリストをリフレッシュします。
list -t backup	backupサービスの詳細を表示します。
list -t dsrepair	DSRepairサービスの詳細を表示します。
list -t dsmerge -f	DSMergeサービスのコマンド形式だけを表示します。

特定のサービスを実行する

サーバにログインした後は、各eMToolサービスを使用してタスクを実行できます。次に例を示します。

コマンド	説明
dsrepair.rld	ローカルデータベースを修復します。
backup.getconfig	バックアップ設定情報を取得します。

詳細については、次を参照してください。

- 594 ページの 「eMBoxクライアントを使ったバックアップ/復元作業」
- 311 ページの 「クライアントを使用したツリーのマージ」
- 358 ページの 「クライアントを使用したデータベースの修復」
- 209 ページの 「クライアントのサービスマネージャeMToolを使用する」

現在のサーバからログアウトする

現在のセッションからログアウトするには、次のコマンドを使用します。

logout

別のサーバにログインする場合は、このコマンドを使用する必要がありません。現在のサーバから自動的にログアウトされます。

eMBoxクライアントを終了する

eMBoxクライアントを終了するには、次のいずれかのコマンドを使用します。

exit

または

quit

コマンドラインクライアントをバッチモードで実行する

クライアントをバッチモードで実行するには、次の3つの方法があります。

- 589 ページの 「単一タスク」
- 589 ページの 「内部バッチファイル」
- 590 ページの 「システムバッチファイル」

システムバッチファイルと内部バッチファイルを組み合わせて使用することで、コマンドをより自由に実行でき、頻繁に実行するコマンドの編成や再使用が可能です。

単一タスク

コマンドラインから単一のタスクをバッチモードで実行するには、コマンドに-tオプションを使用してツールとタスクを指定し、-iオプション(-iは対話式モードを指定するオプションです)を省くだけです。次に例を示します。

```
java -s 137.65.123.244 -p 8008 -u admin.mycompany
-w mypassword -l mylog.txt -t dsrepair.rld -n
```

異なるサーバ上で複数のタスクを実行する場合や、頻繁に実行するタスクの場合は、内部バッチファイルを使用する方が便利です。詳細については、次のセクション(589 ページの 「内部バッチファイル」)を参照してください。

内部バッチファイル

クライアント内部バッチファイルを使用してクライアントをバッチモードで実行するには、インタラクティブモードで実行するコマンドのグループを記述したファイルを作成する必要があります。

クライアント内部バッチファイルを使用すると、バッチファイルに記述したすべてのコマンドを自動的に実行できます。複数のツールを使用した複数のタスクを、同一のサーバ上でタスクごとにログインとログアウトを繰り返すことなく実行できます。また1つのサーバから、複数のサーバに対して複数のツールを使用したタスクを実行できます。

内部バッチファイルを使用すれば、頻繁に実行するコマンドをまとめ、再利用することができます。それらのコマンドは、実行に際してその都度コマンドラインから手動で入力する必要はありません。

内部バッチファイルを実行するには、コマンドラインでクライアントのコマンドを使用します。たとえば、次のコマンドは、サーバにログインし、mybatch.mbxファイル内に列挙されたコマンドを実行します。

```
java -s 137.65.123.244 -p 8008 -u admin.mycompany -w mypassword -l mylog.txt -o -b
mybatch.mbx -n
```

もう1つの方法は、同様のコマンドをシステムバッチファイル内に記述し、そのファイルがサーバ上で自動実行されるようにスケジュールすることです。詳細については、590 ページの 「システムバッチファイル」を参照してください。

次に、内部バッチファイルの例を示します。このファイルには、実行するコマンドの例および別のサーバへログインする例が記述されています。この例では、クライアントを開いたときに、サーバにログインしているものと仮定しています。それぞれのコマンドは別々の行に入力する必要があります。#で始まる行はコメントです。

```
# This file is named mybatch.mbx.
# This is an example of commands you could use in
# an internal command batch file.

# Backup commands
backup.getconfig
backup.backup -b -f mybackup.bak -l backup.log -t -w

# DSRepair commands
dsrepair.rld

# Log in to a different server
login -s 137.65.123.255 -p 8008 -u admin.mycompany -w mypassword -n

# DSMerge commands
dsmerge.pr -u admin.mycompany -p admin.mycompany -n mypassword # Schema Operations
dsschema.rst
dsschema.dse
dsschema.rls
dsschema.gsu
dsschema.scc
dsschema.irs -n LocalTree

# DSService commands
service.serviceList

# End of example.
```

システムバッチファイル

他のコマンドラインツールと同様に、クライアントコマンドが含まれたシステムバッチファイルを作成し、それらをコマンドラインから手動で実行したり、サーバ上で自動で実行されるようにスケジュールしたりできます。たとえば、597 ページの 「バッチファイルとeMBoxクライアントによる無人バックアップ」で示す例のように、システムバッチファイルを使用して、自動でバックアップを実行できます。

1つのサーバから複数のサーバに対して、複数のツールを使用したタスクを実行できます。

システムバッチファイルでは、クライアントの単一コマンドと内部バッチファイルを組み合わせて使用できます。これにより、コマンドをより自由に実行でき、頻繁に実行するコマンドの編成や再使用ができます。詳細については、589 ページの 「内部バッチファイル」を参照してください。

バッチファイルを自動で実行する方法については、ご使用のオペレーティングシステムのマニュアルまたはサードパーティ製スケジューリングソフトウェアのマニュアルを参照してください。

eMBoxコマンドラインクライアントのオプション

オプション	説明
-? または -h	ヘルプ情報を表示します。
-i	コマンドを一度に1つづつ、対話的に実行します。
-s *server*	サーバの名前またはIPアドレスを指定します。 Default=127.0.0.1
-p *port*	サーバのポート番号を指定します。 Default=8008
-u *user*	ユーザDN. たとえば、admin.mycompanyと指定します。 Default=anonymous
-w *password*	-uで指定したユーザのパスワードを指定します。
-m *mode*	ログインモードを指定します。 Default=dclient
-n	安全なSSL接続を試行しません。保護されていない接続を使用します。 このオプションを使用しない場合、クライアントではSSL接続を確立しようとします。そのため、クラスパスにはJSSEファイルが必要となり、これがない場合はエラーが返されます。詳細については、592 ページの 「クライアントを使用してセキュア接続を確立する」を参照してください。
-l *log file*	ログファイルの名前を指定します。
-o	ログファイルを開いた後は、上書きします。
-T *timeout*	サーバから応答を待つ時間(秒)を指定します。
-L *language*	使用する言語を優先順にカンマで区切って指定した一覧です。たとえば、「en-US,de_DE」のように指定します。このオプションのデフォルトは、クライアントシステムの言語です。
-t [*tool.*]*task options*	この接続での単一のサービスを実行します。-tに続く文字列は、有効なコマンドである必要があります。
-b *batch file*	バッチファイルで指定した一連のサービスを実行します。バッチファイル内のコマンドは、行を分けて記述する必要があります。#で始まる行はコメントです。

クライアントを使用してセキュア接続を確立する

非セキュア接続を使用している場合、ユーザ名やパスワードなどの入力したすべての情報は、クリアテキストでネットワーク上に送信されます。

SSLを使用したセキュア接続を確立するには、次の操作を実行します。

- サーバへログインする際は、コマンドで-nオプションを使用しないでください。このオプションは、非セキュア接続を指定するものです。セキュア接続がデフォルトの設定です。
- クラスパスに、次に示すJSSE(Java Secure Socket Extension)ファイルがあることを確認します。
  - jsse.jar
  - jnet.jar
  - jcert.jar

  これらのファイルがない場合、クライアントは、セキュア接続が確立できないことを示すエラーを返します。

  これらのファイルやJSSEについての情報は、OracleのWebサイト (http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136007.html)から入手できます。

eDirectoryポート番号を確認する

クライアントでサーバにログインするには、ポート番号を指定する必要があります。

eDirectoryをインストールする際にポート番号を指定した場合には、その番号を使用します。

すべてのプラットフォームで、デフォルトの非セキュアポートは8008、セキュアポートは8030です。

次に示すセクションには、eDirectoryに割り当てられたポートを確認するための、その他のヒントがあります。

- 592 ページの 「Windowsの場合」
- 593 ページの 「Linuxの場合」

Windowsの場合

1 ［**スタート**］>［**設定**］>［**コントロールパネル**］の順にクリックします。

2 ［**NetIQeDirectoryサービス**］アイコンをダブルクリックしてから、［**トランスポート**］タブをクリックします。

3 セキュアポート、または非セキュアポートを確認します。
  - 非セキュアポートを確認するには、HTTPの横のプラス記号をクリックします。
  - セキュアポートを確認するには、HTTPSの横のプラス記号をクリックします。

  ［**Bound Transports**］の横のプラス記号をクリックすると、ポート番号が表示されます。

Linuxの場合

次のコマンドを使用して、ポートを表示できます。

ndsconfig get | grep http

http.server.interface、その次にポート番号という表現で記述された行を探します。

ログの記録の使用

ログの記録は、DSBackup、DSMerge、DSRepairなど、すべてのeDirectory管理ツール(eMTool)に関するすべてのイベントを記録するインフラストラクチャモジュールです。このリリースで提供されているログファイルは1つだけです。このログファイルに、すべてのeMToolの操作が記録されます。

ログの記録は、クライアントを実行するときに指定するログファイルを通して提供されるクライアントログ記録サービスとは異なります。このログファイルとは、たとえば、クライアントコマンドで-l mylogfile.txtを指定するときや、iManagerでログファイル名として「mylogfile.txt」と入力するときに指定されるもののことです。現行のログ記録では、eMToolによって実行されるタスクに関するすべてのサーバメッセージが記録されるので、記録されるログ情報は、クライアントログ記録サービスのものより詳細です。これに対して、クライアントログサービスではクライアントメッセージおよびクライアントに送信されたメッセージが記録され、進捗状況の概要がレポートされます。

ログの記録は非同期で実行され、デフォルトではすべての操作が記録されます。

このリリースのログの記録には、次の機能があります。

- ログファイルの名前と場所を変更できます。

  デフォルトでは、ログファイルはeDirectoryのインストール先と同じディレクトリにある\logディレクトリに作成されます。
- 最大ファイルサイズが変更できます。変更後、ログファイルはリセットされます。

  最大ファイルサイズは8MBです。
- ログモードを変更できます。

  すべての新しいメッセージをログファイルに追加するか、または既存のログファイルを上書きするかを選択できます。デフォルトでは、追加のオプションが指定されています。
- ログの記録を開始または停止できます。

  デフォルトでは、が起動するとログの記録は開始モードになります。停止モードの間は、メッセージは記録されません。
- ログファイルの内容をリセットできます。
- クライアントコンピュータからログファイルを読み込むことができます。

このセクションでは、次のトピックについて説明します。

- 593 ページの 「ログの記録コマンドラインクライアントを使用する」
- 594 ページの 「NetIQ iManagerでログの記録機能を使用する」

ログの記録コマンドラインクライアントを使用する

次の表に、ログの記録コマンドラインクライアントのオプションを示します。

オプション	説明
logstart	ログの記録を開始します。
logstop	ログの記録を停止します。
readlog	現在のログファイルを表示します。
getlogstate	現在のログの記録の状態(開始または停止)を表示します。
getloginfo	ログファイルの名前、ログ記録モード(追加または上書き)、最大サイズと現在のサイズを表示します。
setloginfo [-f *filename*] [-s *size in Kilo bytes*] [-a | -o]	次のパラメータを使用して、ログファイルの名前、サイズ、ログモード(追加または上書き)を設定します。 ◆ -f *filename* ログファイルの名前。 ◆ -s *size in KB* ログファイルの最大サイズを設定します。 ◆ -a 新しいログメッセージを現在のログメッセージに追加します。 ◆ -o ログファイルを上書きします。
emptylog	サーバログファイルの内容をクリアします。

NetIQ iManagerでログの記録機能を使用する

1 iManagerで、［**役割およびタスク**］ボタン をクリックします。
2 ［**eDirectoryの保守**］>［**ログファイル**］の順にクリックします。
3 ログファイル操作を実行するサーバを指定してから、［**次へ**］をクリックします。
4 そのサーバに対する認証を行ってから、［**次へ**］をクリックします。
5 実行するログファイル操作を選択します。
詳細については、［**ヘルプ**］をクリックしてください。

eMBoxクライアントを使ったバックアップ/復元作業

eMBoxクライアントはコマンドラインJavaクライアントで、これを使用するとeDirectory Backup eMToolなどのeMBoxツールにアクセスできます。複数サーバ環境でも、ファイアウォール越しのアクセスができれば、1台のコンピュータからバックアップ、復元、ロールフォワードログの設定ができます。これは、ほとんどのバックアップタスクと復元タスクを、ファイアウォールの内側でも

外側でも、iManagerを使用してブラウザでリモートに実行できるようにします。高度な処理は、コマンドラインから実行するJavaクライアントである、eMBox Clientを使い、リモート操作で実行できます。ファイアウォール越しにでも、あるいはVPN経由でも操作できます。

iManagerからは、コールドバックアップ、無人バックアップ、高度な復元機能を除くバックアップ/復元機能を実行できます。詳しくは「602 ページの 「NetIQ iManagerを使ったバックアップ/復元作業」」を参照してください。

eDirectory バックアップツールは、eMBoxツールセットの一部です。eMBoxは、eDirectoryを構成する一部としてサーバにインストールされるサービスです。

バックアップツールは次のファイルで構成されます。

ファイル名	説明
backupcr	バックアップ/復元機能をすべて含むコアライブラリ。 このライブラリにはユーザインタフェースはなく、backuptlプログラムから動的にロード、リンクされる形で動作します。
backuptl	backupcrライブラリへのツールインタフェース。DSBKアーキテクチャを介してバックアップ/復元機能を提供するプログラムです。 これには、iManagerプラグイン、DSBK、Javaコマンドラインクライアントを介してアクセスできます。
dsbackup_en.xlf	バックアップツールから返されるメッセージを含む言語ファイルです。

重要: 復元後の検証処理については、8.5より前のeDirectoryとは互換性がありません。レプリカリングに属するサーバで新しいバックアップ/復元ツールを使う場合は、これに属するサーバすべてをeDirectory 8.5以降にアップグレードする必要があります

eMBoxクライアントはバッチモードで実行できるため、eDirectory Backup eMToolを使用して無人バックアップを行うことができます。

eMBoxClient.jarファイルは、eDirectoryの一部としてサーバにインストールされます。それ以外にも、Sun JVM 1.3.1が動作する環境であれば、eMBoxClient.jarをコピーして動かすことができます。詳細については、583 ページの 「eDirectory Management Toolbox」および586 ページの 「ワークステーションでクライアントを実行する」を参照してください。

eDirectoryのバックアップ/復元作業に先立ち、「440 ページの 「eDirectoryのバックアップ処理に関する確認事項」」を参照して問題点を確認し、効率的に作業できるようにしてください。

前提条件

❒ バックアップ処理を起動するマシンに、ファイルeMBoxClient.jarがあることを確認してください。

ファイルは、eDirectoryインストールの一部としてサーバにインストールされます。それ以外にも、Sun JVM 1.3.1が動作する環境であれば、eMBoxClient.jarをコピーして実行することができます。複数サーバ環境でも、ファイアウォール越しのアクセスが可能であれば、1台のコンピュータからバックアップを実行できます。詳細については、584 ページの 「コマンドラインクライアントの使用」を参照してください。

- ロールフォワードログを作成するのであれば、バックアップを行う前にこの機能を有効にしてください。

  レプリカリングに属するサーバは、ロールフォワードログ機能を有効にしておく必要があります。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないことになります。

  ロールフォワードログの詳細については、「453 ページの 「ロールフォワードログを使用する」」を参照してください。また、この機能を有効にする手順については、599 ページの 「eMBoxクライアントによるロールフォワードログの設定」を参照してください。

- コマンドラインオプションについては、「467 ページの 「バックアップ/復元のコマンドラインオプション」」を参照してください。

- 複数サーバ環境のツリーの場合、このサーバとレプリカを共有するサーバすべてについて、eDirectory 8.5以降にアップグレードする必要があります。

eMBoxクライアントによる手動バックアップ

eMBoxクライアントを使って、eDirectoryデータベースの中身を、指定したファイルにバックアップすることができます。バックアップファイルには、eDirectoryをその時点の状態に復元するために必要な情報がすべて含まれています。また、処理結果は所定のログファイルに記録されます。

eMBoxクライアントを使ってeDirectoryデータベースをバックアップする手順を次に示します。

1. eMBoxクライアントを対話式モードで起動します。

   - Linux: コマンドラインで、「edirutil -i」と入力します。
   - Windows: *drive*\novell\nds\edirutil.exe -iを実行します。

   edirutilファイルは、eMBoxクライアントを実行するためのショートカットです。Java実行可能ファイルと、eDirectoryでeMBoxクライアントがインストールされるデフォルトの場所を指します。この情報は、586 ページの 「クライアント用にパスおよびクラスパスをセットアップする」に記載されているようにして手動で入力することもできます。

   eMBox Clientが開くと、「eMBox Client>」というeMBox Clientプロンプトが現れます。

2. バックアップの対象サーバにログインします。次のように入力してください。

   login -s *server_name_or_IP_address* -p *port_number* -u *username.context* -w *password*

   たとえば、Windowsでは、次のように入力します。

   login -s 151.155.111.1 -p 8009 -u admin.mycompany -w mypassword

   セキュア接続が確立できないというエラーが表示される場合は、「592 ページの 「クライアントを使用してセキュア接続を確立する」」に表示されているJSSEファイルがシステム上にない可能性があります。

   指定するポート番号が分からない場合は、592 ページの 「eDirectoryポート番号を確認する」を参照してください。

   eMBoxクライアントはログインが成功したかどうかを表示します。

3 eMBoxクライアントのプロンプトが出たら、次のような形式でバックアップコマンドを入力します。

backup -b -f *backup_filename_and_path* -l *backup_log_filename_and_path* -u *include_file_filename_and_path* -t -w -a

各スイッチの間にはスペースが必要です。スイッチの順序は重要ではありません。

たとえば、Windowsでは、次のように入力します。

backup -b -f c:\backups\8_20_2001.bak -l c:\backups\backup.log -u c:\backups\myincludefile.txt -t -w -a

この例では、フルバックアップを取ること(-b)、バックアップファイルをc:\backups\8_20_2001.bakとすること、処理結果をc:\backups\backup.logに出力すること、さらに、データベースとともに、次に示す他のファイルもバックアップすることを指定しています。

- 管理者があらかじめ作成したインクルードファイル(-u c:\backups\myincludefile.txt)に列挙されたファイル。
- ストリームファイル(-t)

  さらにこの例ではバックアップファイルの上書き(-w)が指定されているため、同じ名前のバックアップファイルがあればBackup eMToolにより上書きされます。
- -aオプションは、ホット連続バックアップ中に、ロールフォワードログディレクトリから古いログファイルを削除します。

eMBoxクライアントはバックアップが成功したかどうかを表示します。

4 サーバからログアウトするには、次のコマンドを入力します。

logout

5 eMBoxクライアントを終了するには、次のコマンドを入力します。

exit

6 eDirectoryのバックアップ処理が終了したら、すぐにファイルシステムのバックアップ作業を行い、テープに保存しますBackup eMToolによる処理では、サーバ上にバックアップファイルができるだけです。

手動バックアップの詳細については、463ページの「DSBKによる手動バックアップ」を参照してください。

バッチファイルとeMBoxクライアントによる無人バックアップ

バッチファイルを使用して、eMBoxクライアントによるeDirectoryの無人バックアップを実行します。たとえば週1回フルバックアップ、毎晩インクリメンタルバックアップを取る、といった運用が可能です。

バッチモードでeMBoxクライアントを実行するには、システムバッチファイルを使う、eMBoxクライアントの内蔵バッチファイルを使う、両者を組み合わせて使う、という方法があります。詳細については、589 ページの 「コマンドラインクライアントをバッチモードで実行する」を参照してください。

ここではシステムバッチファイルを使う方法を解説します。

1 サーバをバックアップするためのシステムバッチファイルを作成します。次のような書式で、1行に1サーバ分のコマンドを記述してください。

Windows環境とLinux環境で一般的なパターンは次のとおりです。

```
java -cp path/eMBoxClient.jar embox -s server_name -p port_number -u
username.context -w password -t backup.backup -b -f backup_filename_and_path -
l backup_log_filename_and_path -u include_file_filename_and_path -t -w
```

具体例とその解説については、「598 ページの 「無人バックアップ用システムバッチファイルの例」」を参照してください。

毎晩実行するインクリメンタルバックアップにも、フルバックアップに使うのと同じバッチファイルが使えますが、-bスイッチを-iに変更して、フルバックアップではなくインクリメンタルバックアップを実行します。フルバックアップとインクリメンタルバックアップで、保存先バックアップファイル名を異なるものにしておく方がよいでしょう。

指定するポート番号が分からない場合は、「592 ページの 「eDirectoryポート番号を確認する」」を参照してください。セキュア接続を使用する場合は、「592ページの「クライアントを使用してセキュア接続を確立する」」を参照してください。eMBoxクライアントの内蔵バッチファイルの使い方については、「589 ページの 「コマンドラインクライアントをバッチモードで実行する」」を参照してください。

2. このバッチファイルを定期的に起動するよう設定します。具体的な設定方法については、オペレーティングシステムまたはサードパーティ製ソフトウェアの資料を参照してください。
3. eDirectoryのバックアップ後すぐに、ファイルシステムのバックアップ作業を行い、テープに保存できるよう準備してください

   Backup eMToolによる処理では、サーバ上にバックアップファイルができるだけです。
4. バックアップが正常に実行されているか、ログファイルで定期的に確認してください。

無人バックアップ用システムバッチファイルの例

システムバッチファイルの例を以下に示します。

Windows用のバッチファイル例

```
java -cp c:\novell\nds\embox\eMBoxClient.jar embox -s myserver -p 8008 -u
admin.myorg -w mypassword -n -t backup.backup -b -f c:\backup\backup.bak -u
c:\backup\includes\includefile.txt -l c:\backup\backup.log -t -w
```

この例には次のようなオプションが指定されています。

- フルバックアップを取る指定(-b)。
- インクルードファイルの指定(-u)。これはオプションです。データベース以外にもファイルをバックアップしたい場合に使います。インクルードファイルはあらかじめ用意しておいてください。
- ストリームファイル(-t)もバックアップされます。
- 同じ名前のバックアップファイルがあれば上書きする指定(-w)。

重要: 同じバッチファイルを繰り返し使用するなど、同じ名前のバックアップファイルが存在する場合、バックアップが正常に行われるように、-wオプションを使用して、既存のバックアップファイルが上書きされるようにしてください。

バッチモードでは、同じ名前のファイルが存在する場合に-wが指定されていないと、デフォルトの動作として、ファイルは上書きされず、バックアップは作成されません。対話式モードでは、-wが指定されていないと、ファイルを上書きしてよいかどうかを尋ねられます。

---

eDirectoryのフル/インクリメンタルバックアップの都度、すぐにファイルシステムのバックアップを取っているのであれば、前回のバックアップファイルはテープに保存されているはずです。したがって上書きしても問題ありません。

- この例では非セキュアポートが使用されているため(-p 8008)、非セキュア接続が指定されています(-n)。

eMBoxクライアントによるロールフォワードログの設定

eMBoxクライアントを使って、ロールフォワードログに関する設定を変更することができます。次のような設定ができます。

- 現在の設定の確認
- ロールフォワードログ機能の有効/無効の切り替え

  レプリカリングに属するサーバは、ロールフォワードログ機能を有効にしておく必要があります。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないことになります。
- ロールフォワードログの保存先ディレクトリの変更
- ロールフォワードログのファイルサイズの最小値、最大値の設定
- 現在使用中のログ、既に書き出しを終えた最新のログの判別
- ストリームファイルをロールフォワードログに含めるかどうかの切り替え

ロールフォワードログの詳細については、「453ページの「ロールフォワードログを使用する」」を参照してください。

1. eMBoxクライアントを対話式モードで起動します。
   - Linux: コマンドラインで、「edirutil -i」と入力します。
   - Windows: *drive*\novell\nds\edirutil.exe -iを実行します。

   edirutilファイルは、eMBoxクライアントを実行するためのショートカットです。Java実行可能ファイルと、eDirectoryでeMBoxクライアントがインストールされるデフォルトの場所が指定されているほか、必要な-nsオプションも含まれています。これらのオプションは、586 ページの 「ワークステーションでクライアントを実行する」に記載されているようにして手動で入力することもできます。

   正常に起動されると、「eMBox Client>」というプロンプトが現れます。
2. ロールフォワードログの設定を行うサーバにログインします。次のように入力してください。

   login -s *server_name_or_IP_address* -p *port_number* -u *username.context* -w *password*

   たとえば、Windowsでは、次のように入力します。

   ```
   login -s 151.155.111.1 -p 8009 -u admin.mycompany -w mypassword
   ```

   セキュア接続が確立できないというエラーが表示される場合は、「592 ページの 「クライアントを使用してセキュア接続を確立する」」に表示されているJSSEファイルがシステム上にない可能性があります。

   指定するポート番号が分からない場合は、592 ページの 「eDirectoryポート番号を確認する」を参照してください。

   eMBoxクライアントはログインが成功したかどうかを表示します。
3. (オプション)次のコマンドを入力して、現在の設定を検索します。

getconfig

オプション指定は必要ありません。

たとえば次のように表示されます。

```
Roll forward log status OFF
Stream file logging status OFF
Current roll forward log directory C:\rfl\nds.rfl
Minimum roll forward log size (bytes) 104857600
Maximum roll forward log size (bytes) 4294705152
Last roll forward log not used 00000000.log
Current roll forward log 00000001.log
*** END ***
```

4 setconfigコマンドで設定を変更します。次のような形式で入力してください。

setconfig [-L|-l] [-T|-t] -r *path_to_roll-forward_logs* -n *minimum_file_size* -m *maximum_file_size*

各スイッチの間にはスペースが必要です。スイッチの順序は重要ではありません。

ロールフォワードログ専用のディスクパーティション/ボリュームを用意するのが最善です。こうしておけば、ディスク容量やアクセス権を監視しやすくなります。

警告: ロールフォワードログ記録を有効にしたら、デフォルトの保存先は使用しないでください。障害対策のためには、eDirectoryとは別のディスクパーティション/ボリューム、別の記憶デバイスを指定してください。ロールフォワードログディレクトリは、バックアップ環境設定を変更するサーバ上である必要があります。

重要: ロールフォワードログ機能を有効にする場合、ログを保存するボリュームのディスク容量を常に監視してください。これを怠ると、ログの容量は増える一方なので、ディスクパーティション/ボリュームがあふれてしまう恐れがあります。ディスク容量が不足してロールフォワードログを作成できない場合は、eDirectoryはそのサーバに対して応答しなくなります。書き出しが終わったロールフォワードログは、定期的にバックアップし、サーバから削除するようお勧めします。詳細については、456 ページの 「ロールフォワードログのバックアップと削除」を参照してください。

---

5 サーバからログアウトするには、次のコマンドを入力します。

logout

6 eMBoxクライアントを終了するには、次のコマンドを入力します。

exit

eMBoxクライアントによるバックアップファイルの復元作業

eMBoxクライアントを使ってバックアップファイルに保存されたデータからeDirectoryデータベースを復元する手順を解説します。手動あるいはバッチ方式で残しておいたバックアップファイルから、データを復元できます。処理結果は所定のログファイルに記録されます。

eMBoxクライアントを使えば、iManagerでは実現できない高度な復元機能も実行できます。これらは、「467 ページの 「バックアップ/復元のコマンドラインオプション」」のrestoreおよびrestadvの項に記載されています。

eMBoxクライアントを使ってeDirectoryデータベースを復元する手順を示します。

1 必要なバックアップファイルを集めておきます。詳しくは「457 ページの 「復元処理の準備」」を参照してください。

2 eMBoxクライアントを対話式モードで起動します。

- Linux: コマンドラインで、「edirutil -i」と入力します。
- Windows: *drive*\novell\nds\edirutil.exe -iを実行します。

edirutilファイルは、eMBoxクライアントを実行するためのショートカットです。Java実行可能ファイルと、eDirectoryでeMBoxクライアントがインストールされるデフォルトの場所が指定されているほか、必要な-nsオプションも含まれています。この情報は、586 ページの「ワークステーションでクライアントを実行する」に記載されているようにして手動で入力することもできます。

正常に起動されると、「eMBox Client>」というプロンプトが現れます。

3 復元の対象サーバにログインします。次のように入力してください。

login -s *server_name_or_IP_address* -p *port_number* -u *username.context* -w *password*

たとえば、Windowsでは、次のように入力します。

```
login -s 151.155.111.1 -p 8009 -u admin.mycompany -w mypassword
```

セキュア接続が確立できないというエラーが表示される場合は、「592 ページの 「クライアントを使用してセキュア接続を確立する」」に表示されているJSSEファイルがシステム上にない可能性があります。

指定するポート番号が分からない場合は、592 ページの 「eDirectoryポート番号を確認する」を参照してください。

eMBoxクライアントはログインが成功したかどうかを表示します。

4 eMBoxクライアントのプロンプトで、次のような一般的な形式でrestoreコマンドを入力します。

restore -r -a -o -f *full_backup_path_and_filename* -d *roll-forward_log_location* -l *restore_log_path_and_filename*

各スイッチの間にはスペースが必要です。スイッチの順序は重要ではありません。-rスイッチを使用してeDirectoryデータベースそのものを復元します。このスイッチを指定しないと、その他の種類のファイルのみが復元の対象となります。復元処理の終了後にデータベースをアクティブにして開くには、-aおよび-oを指定してください。

ロールフォワードログを使って復元する場合は、ログのフルパスを指定しなければなりません。フルパスは、eDirectoryにより自動的に作成されたディレクトリ(通常は\nds.rfl)を含みます。このディレクトリについて詳しくは455 ページの 「ロールフォワードログの保存先」を参照してください。

次に例を示します。

restore -r -a -o -f sys:/backup/nds.bak -d $HOME/rfldir/nds.rfl -l $HOME/backups/backup.log

この例では、データベースそのものを復元し(-r)、復元の検証が正常終了してから、そのデータベースをアクティブにして(-a)、開く(-o)よう指定しています。-fスイッチでフルバックアップファイルの場所を、-dでロールフォワードログの場所を指定しています。また、復元処理の結果を記録するログファイルを、-lで指定しています。

これによりフルバックアップファイルからの復元処理が実行され、次にインクリメンタルバックアップファイルの指定を求めるプロンプトが現れます。

5 (状況によって実行)インクリメンタルバックアップファイルから復元する場合は、プロンプトに応じて順次、そのパスとファイル名を入力します。

プロンプトには次に指定するべきファイルのIDが表示されます。これはインクリメンタルバックアップファイルのヘッダに記載されているものです。

バックアップ処理が正常終了すれば、その旨の表示が現れます。

6 (状況によって実行)復元処理に失敗した場合は、ログファイルでエラーの原因を確認してください。

復元後の検証に失敗した場合の対処については、「478 ページの 「復元後の検証処理に失敗した場合の対処方法」」を参照してください。

注: レプリカリング中にeDirectory 8.5より前のバージョンが稼動しているサーバがある場合、復元処理は失敗します。エラーコードは-666、すなわち「DSバージョンの不整合」となります。

---

7 サーバからログアウトするには、次のコマンドを入力します。

logout

8 eMBoxクライアントを終了するには、次のコマンドを入力します。

exit

9 (状況によって実行)NICIセキュリティファイルを復元した場合は、復元の完了後、サーバを再起動してNICIを再初期化し、その後でDIBを復元します。

10 ここでサーバが通常どおり要求に応答することを確認しておきます。

11 (状況によって実行)このサーバでロールフォワードログ機能を使うためには、改めて有効に切り替え、障害対策のための書き出し先も設定し直して、ロールフォワードログの環境設定を再作成する必要があります。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

この手順が必要となるのは、復元処理の過程で、ロールフォワードログに関する設定はデフォルトに戻るためです。つまり、ロールフォワードログ機能は無効となり、保存先もデフォルトの場所になるからです。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

ロールフォワードログの詳細については、「453 ページの 「ロールフォワードログを使用する」」を参照してください。

以上で復元作業が終了しました。NICIの再初期化も済んでいるので、暗号化された情報にもアクセスできます。ロールフォワードログ機能を使用する場合は、今後の障害に備えるため、再びこの機能を有効にし、フルバックアップを取っておいてください。

NetIQ iManagerを使ったバックアップ/復元作業

eDirectory バックアップツールのほとんどの機能は、NetIQ iManagerでバックアップやその環境設定、および復元の作業を行う形でも利用できます。iManagerを使うことにより、ファイアウォールの外側にいても、サーバ上の作業をブラウザから実行できます。NetIQManagerの詳細については、『*NetIQ iManager管理ガイド* (https://www.netiq.com/documentation/imanager-3/imanager_admin/)』を参照してください。

ただし、コールドバックアップ(データベースをいったん停止したフルバックアップ)、無人バックアップ、高度な復元機能は、iManagerからは実行できません。これらの作業はDSBKを使用して実行する必要があります。詳しくは、460 ページの 「DSBKの使用」を参照してください。

eDirectoryのバックアップ/復元作業に先立ち、「440 ページの 「eDirectoryのバックアップ処理に関する確認事項」」を参照して問題点を確認し、効率的に作業できるようにしてください。

この節では、次の項目について説明します。

- 603 ページの 「iManagerによる手動バックアップ」
- 604 ページの 「iManagerによるロールフォワードログの設定」
- 606 ページの 「iManagerによるバックアップファイルの復元作業」

iManagerによる手動バックアップ

iManagerのブラウザ画面から［バックアップ］を使用して、eDirectoryデータベースをサーバにバックアップします。フルバックアップ、インクリメンタルバックアップのどちらも実行可能です。

バックアップファイルには、eDirectoryをその時点の状態に復元するために必要な情報がすべて含まれています。バックアップの処理結果は所定のログファイルに記録されます。

iManagerから実行できるのは「ホット」バックアップです。つまり、バックアップ処理中もeDirectoryデータベースは開いたままで、通常どおり利用しながら、バックアップ開始時点の状態を完全に保存できます。

なお、コールドバックアップ(データベースを停止してのバックアップ)や無人バックアップを実行するには、DSBKを使用する必要があります。詳細については、463 ページの 「DSBKによる手動バックアップ」を参照してください。

eDirectoryのバックアップ/復元作業に先立ち、「440 ページの 「eDirectoryのバックアップ処理に関する確認事項」」を参照して問題点を確認し、効率的に作業できるようにしてください。

前提条件

❒ eDirectory以外にも追加でバックアップしたいファイルがあれば、それを列挙したインクルードファイルを作っておいてください。

iManagerの設定画面で該当するチェックボックスをオンにすれば、NICIファイルやストリームファイルもバックアップできます。NICIファイルは常にバックアップするようお勧めします。

それ以外にautoexec.ncfファイルなどをバックアップしたい場合は、そのパスとファイル名をインクルードファイルに列挙します。複数のファイルがある場合はセミコロンで区切ります。改行(ハードリターン)や空白を含めないようにしてください。例:
sys:\system\autoexec.ncf;sys:\etc\hosts;

❒ eDirectoryのバックアップ後すぐに、ファイルシステムのバックアップ作業を行い、テープに保存できるよう準備してくださいバックアップツールによる処理では、サーバ上にバックアップファイルができるだけです。

ヒント: コピー先記憶デバイスに容量の制約がある場合は、あらかじめeDirectoryバックアップファイルの最大サイズを設定すると便利です。また、バックアップファイルの作成後、サードパーティ製ファイル圧縮ツールを使う方法もあります。80%程度は圧縮できます。

❒ ロールフォワードログを作成するのであれば、バックアップを行う前にこの機能を有効にしてください。

レプリカリングに属するサーバは、ロールフォワードログ機能を有効にしておく必要があります。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないことになります。

ロールフォワードログの詳細については、「453 ページの 「ロールフォワードログを使用する」」を参照してください。また、この機能を有効にする手順については、604 ページの「iManagerによるロールフォワードログの設定」を参照してください。

❒ 複数サーバ環境のツリーの場合、このサーバとレプリカを共有するサーバすべてについて、eDirectory 8.5以降にアップグレードする必要があります。

手順

iManagerを使ってeDirectoryデータベースをバックアップする手順を次に示します。

ヒント: iManagerで使用できる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。

---

1 ［**役割およびタスク**］ボタン  をクリックします。

2 ［**eDirectoryの保守**］>［**バックアップ**］の順にクリックします。

3 バックアップを実行するサーバを指定し、［**次へ**］をクリックします。

4 バックアップを実行するサーバのユーザ名、パスワード、コンテキストを指定し、［**次へ**］をクリックします。

5 バックアップファイルのオプションを指定し、［**次へ**］をクリックします。

最後のバックアップの実行後にデータベースに対して行われた変更のみをバックアップする場合は、［**インクリメンタルバックアップを実行します**］をクリックしてください。

6 ホット連続バックアップ中に、ロールフォワードログディレクトリから古いログファイルを削除するには、［**古いRFLファイルを削除**］を選択します。

7 追加でバックアップしたいファイルがあればここで指定します。

追加するファイルが指定されていない場合、eDirectoryデータベースのみがバックアップされます。

NICIファイルは常にバックアップするようお勧めします。

8 表示される指示に従って、バックアップを完了します。

9 eDirectoryのバックアップ処理が終了したら、すぐにファイルシステムのバックアップ作業を行い、テープに保存しますバックアップツールによる処理では、サーバ上にバックアップファイルができるだけです。

iManagerによるロールフォワードログの設定

ブラウザから［バックアップ環境設定］を使用して、ロールフォワードログに関する設定を変更します。次のような設定ができます。

- ロールフォワードログ機能の有効/無効の切り替え

  レプリカリングに属するサーバは、ロールフォワードログ機能を有効にしておく必要があります。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないことになります。
- ロールフォワードログの保存先ディレクトリの変更.
- ロールフォワードログのファイルサイズの最小値、最大値の設定.
- 現在使用中のログ、既に書き出しを終えた最新のログの判別.
- ストリームファイルをロールフォワードログに含めるかどうかの切り替え.

ロールフォワードログの詳細については、「453ページの「ロールフォワードログを使用する」」を参照してください。

ヒント: iManagerで使用できる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。

1 ［役割およびタスク］ボタン をクリックします。

2 ［eDirectoryの保守］>［バックアップ環境設定］の順にクリックします。

3 設定を変更するサーバを指定し、［次へ］をクリックします。

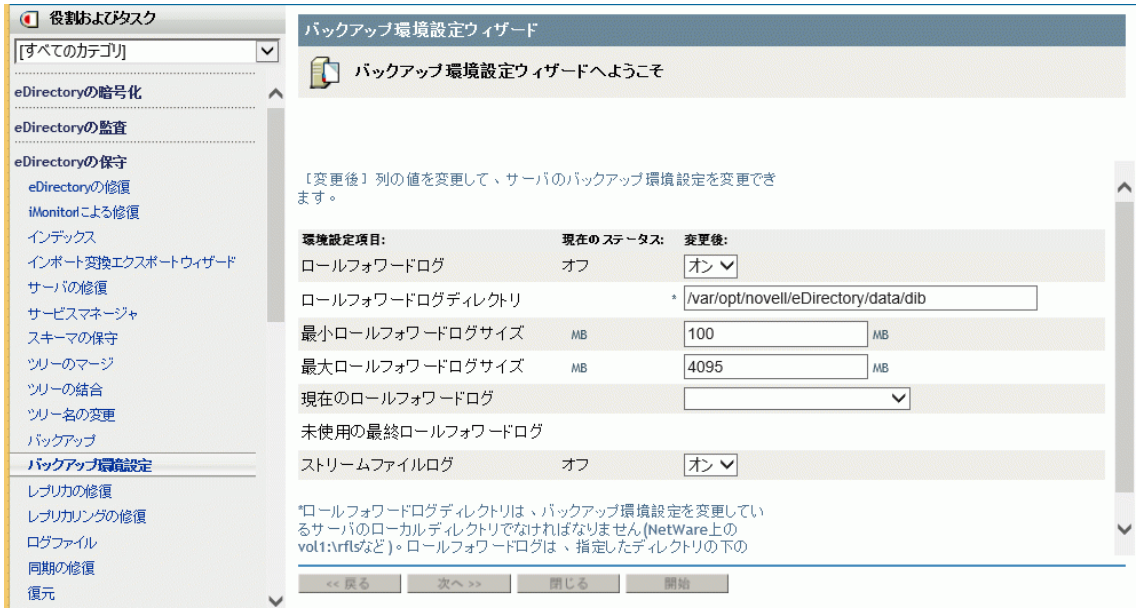
4 設定を変更するサーバのユーザ名、パスワード、コンテキストを指定し、［次へ］をクリックします。

5 必要に応じてサーバのバックアップ環境設定を変更します。

警告: ロールフォワードログ記録を有効にしたら、デフォルトの保存先は使用しないでください。障害対策のためには、eDirectoryとは別のディスクパーティション/ボリューム、別の記憶デバイスを指定してください。ロールフォワードログディレクトリは、バックアップ環境設定を変更するサーバ上である必要があります。

重要: ロールフォワードログ機能を有効にする場合、ログを保存するボリュームのディスク容量を常に監視してください。これを怠ると、ログの容量は増える一方なので、ディスクパーティション/ボリュームがあふれてしまう恐れがあります。ディスク容量が不足してロールフォワードログを作成できない場合は、eDirectoryはそのサーバに対して応答しなくなります。書き出しが終わったロールフォワードログは、定期的にバックアップし、サーバから削除するようお勧めします。詳細については、456 ページの 「ロールフォワードログのバックアップと削除」を参照してください。

画面例を次に示します。



6 表示される指示に従って、操作を完了します。

iManagerによるバックアップファイルの復元作業

ブラウザから［復元］を使用して、保存されたバックアップファイルのデータからeDirectoryデータベースを復元します。復元の処理結果は所定のログファイルに記録されます。

復元プロセスの詳細については、445 ページの 「バックアップツールによる復元作業の概要」を参照してください。

高度な復元オプションはDSBKから実行する必要があります。詳しくは460ページの 「DSBKの使用」を参照してください。

前提条件

- ❒ 必要なバックアップファイルをすべて、復元対象サーバ上の、適当なディレクトリに集めておく必要があります。

  457 ページの 「復元処理の準備」および458 ページの 「復元に必要なバックアップファイルの収集」を参照してください。
- ❒ eDirectoryを復元対象のサーバにインストールし、稼動させておいてください。

  たとえば記憶デバイスの障害の場合、デバイスを交換し、改めてeDirectoryをインストールすることになります。故障したサーバごと交換する、あるいは単に新しいサーバに移行する場合は、新しいサーバにオペレーティングシステムをインストールした上で、eDirectoryも準備します。
- ❒ 復元処理の詳細については、「445 ページの 「バックアップツールによる復元作業の概要」」を参照してください。

手順

ヒント: iManagerで使用できる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。

---

iManagerを使ってeDirectoryデータベースを復元する手順を次に示します。

1. 必要なバックアップファイルを集めておきます。詳しくは、457 ページの 「復元処理の準備」を参照してください。
2. ［**役割およびタスク**］ボタン  をクリックします。
3. ［**eDirectoryの保守**］>［**復元**］の順にクリックします。
4. 復元を実行するサーバを指定し、［**次へ**］をクリックします。
5. 復元を実行するサーバのユーザ名、パスワード、コンテキストを指定し、［**次へ**］をクリックします。
6. バックアップファイル名、ログファイル名を指定し、［**次へ**］をクリックします。
7. 必要な復元オプションを指定し、［**次へ**］をクリックします。

   通常、少なくとも次のチェックボックスはオンにする必要があります。

   - **データベースを復元**
   - **検証後に復元されたデータベースをアクティブにします**
   - **復元の完了後にデータベースを開きます**
   - **セキュリティファイルの復元**(NICIファイルの復元)

NICIファイルは必ずバックアップしておくようお勧めします。これがないと、復元に成功しても、暗号化されたファイルは読めません。

ロールフォワードログを使って復元する場合は、ログのフルパスを指定しなければなりません。フルパスは、eDirectoryにより自動的に作成されたディレクトリ(通常は\nds.rfl)を含みます。このディレクトリについて詳しくは455 ページの 「ロールフォワードログの保存先」を参照してください。

8 表示される指示に従って、復元を完了します。

復元後の検証に失敗した場合の対処については、「478 ページの 「復元後の検証処理に失敗した場合の対処方法」」を参照してください。

注: レプリカリング中にeDirectory 8.5より前のバージョンが稼動しているサーバがある場合、復元処理は失敗します。エラーコードは-666、すなわち「DSバージョンの不整合」となります。

---

9 NICIセキュリティファイルを復元した場合は、復元完了後にNICIを再初期化するため、サーバを再起動します。

10 ここでサーバが通常どおり要求に応答することを確認しておきます。

11 (状況によって実行)このサーバでロールフォワードログ機能を使うためには、改めて有効に切り替え、障害対策のための書き出し先も設定し直して、ロールフォワードログの環境設定を再作成する必要があります。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

この手順が必要となるのは、復元処理の過程で、ロールフォワードログに関する設定はデフォルトに戻るためです。つまり、ロールフォワードログ機能は無効となり、保存先もデフォルトの場所になるからです。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

ロールフォワードログの詳細については、「453 ページの 「ロールフォワードログを使用する」」を参照してください。

以上で復元作業が終了しました。NICIの再初期化も済んでいるので、暗号化された情報にもアクセスできます。ロールフォワードログ機能を使用する場合は、今後の障害に備えるため、再びこの機能を有効にし、フルバックアップを取っておいてください。

23 eDirectoryイベントの監査

以下のいずれかの方法で、eDirectoryイベントを監査することができます。

Novell Auditを使った監査

Novell Auditパッケージを使用すると、eDirectoryが生成したイベントを外部監査クライアントにモニタリング目的で送信することができます。

eDirectory 9.2にはeDirectory Instrumentationがバンドルされています。このパッケージは、Novell Auditを使用してeDirectoryイベントを監査する場合にインストールする必要があります。

LinuxサーバとWindowsサーバ上で、Novell Auditをインストール、設定、またはアンインストールするには、次の情報を参照してください。

サポートされているプラットフォーム

サポートされているプラットフォームとインストール手順については、『*NetIQ eDirectoryインストールガイド*』を参照してください。

前提条件

- ❒ eDirectory 9.2監査には、最低でも、Novell Audit Platform Agent 2.0.2.80が必要です。
- ❒ Novell Audit iManagerプラグインのインストールと使用には、iManager 3.0以降が必要です。詳細については、iManagerのドキュメントページを参照してください。

Novell Auditパッケージのインストール

- 610 ページの 「Linux」
- 611 ページの 「Windows」

Linux

ルートユーザとしてのeDirectory Instrumentationのインストール

Audit Platform Agent環境設定ファイル(logevent.conf)が/etcにすでに存在する場合、Auditパッケージをインストールする前にファイルをバックアップしてください。これは新しいパッケージが既存の環境設定を上書きするためです。

Auditモジュールがすでにロードされている場合、ndstrace -c "unload auditds"コマンドを使って、auditdsモジュールをアンロードします。

64ビットAuditパッケージの場合:

1. Linuxプラットフォーム用のeDirectoryビルドを抽出したセットアップディレクトリから、novell-AUDTplatformagent-2.0.2-80.x86_64.rpmをインストールします。

   ```
   #rpm -ivh /root/eDirectory/setup/novell-AUDTplatformagent-2.0.2-80.x86_64.rpm
   ```

2. Linuxプラットフォーム用のeDirectoryビルドを抽出したセットアップディレクトリから、novell-AUDTedirinst-9.2-*xx*.x86_64.rpmをインストールします。

   注: eDirectoryサーバのアップグレードの場合、novell-AUDTedirinst-9.2-xx.x86_64.rpmは、すでにインストールしてあるなら自動でアップグレードされます。

   ```
   #rpm -ivh <eDirectory build extracted folder>/eDirectory/setup/novell-AUDTedirinst-9.2-xx.x86_64.rpm
   ```

ndstrace -c "load auditds"を実行して、auditdsモジュールをロードします。

非ルートユーザとしてのeDirectory Instrumentationのインストール

64ビットAuditパッケージの場合:

1. 非ルートユーザとして、プラットフォームエージェント(PA)をインストールします。PAのインストールについては、NetIQダウンロードのWebサイトと『Novell Audit Platform Agent Guide (Novell Audit Platform Agentガイド)』(Sentinelプラグイン2011.1 r 3)を参照してください。
2. eDirectoryサーバを停止します。
3. 次のコマンドを使用して、eDirectory Instrumentation rpmを抽出します。:

```
#rpm2cpio novell-AUDTedirinst-9.2-xx.x86_64.rpm | cpio -div
```

4 抽出されたファイルを、非ルートでインストールされているlib64ディレクトリに次のコマンドを使用してコピーします。

```
cp -r ./opt/novell/eDirectory/lib64/* <eDirectory build extracted folder>/
eDirectory/opt/novell/eDirectory/lib64/
```

5 eDirectoryサーバを再起動します。

6 ndstrace -c "load auditds"を実行して、auditdsモジュールをロードします。

Windows

Audit Platform Agent環境設定ファイル(logevent.cfg)がC:\WINDOWSにすでに存在する場合、インストラメンテーションをインストールする前にファイルをバックアップしてください。これは新しいパッケージが既存の環境設定を上書きするためです。

64ビットAuditパッケージおよびAudit Platform Agentのインストールの場合、<installerFolder>windows/x/windows/x64/auditds/からNovell_Audit_PlatformAgent_Win64.exeを実行します。

注

- eDirectory Instrumentationがインストールされ ているeDirectoryサーバをアップグレードすると、eDirectory Instrumentationは自動的にアップグレードされます。現在使用しているのがeDirectory 9.0 SP2以前の場合、eDirectoryサーバをアップグレードする前にInstrumentationファイルを手動でアップグレードする必要があります。
- 非ルートユーザとしてeDirectoryサーバをアップグレードする場合、eDirectoryサーバをアップグレードする前にInstrumentationファイルを手動でアップグレードする必要があります。

Novell Audit iManager Plug-inのインストール

Novell Audit Platform Agentを使って、eDirectoryイベントの監査を環境設定するには、最初にiManagerに対して、Novell Auditプラグインをインストールする必要 があります。

Novell Audit iManagerプラグインのインストールと使用には、iManager 3.0以降が必要です。iManagerのインストール要件とダウンロード手順については、『*iManagerインストールガイド*』を参照してください。

Novell Audit iManagerプラグインは、eDirectory 9.2プラグインにバンドルされています。eDirectory 9.2プラグインは、ダウンロードサイト (https://download.novell.com/Download?buildid=G_8Eymx0QtI~)からダウンロードできます。

インストール手順は、iManager 3.2用eDirectory 9.2プラグインのダウンロードページ (https://download.novell.com/Download?buildid=G_8Eymx0QtI~)で入手できます。

Novell Audit Platform Agentの設定

Audit Platform Agentがまだ設定されていない場合、Platform Agent環境設定ファイルを編集して、LogHostでAudit Serverのホストアドレスを設定します。デフォルトで、環境設定ファイルは次のディレクトリに配置されます。

- Linux: /etc/logevent.conf
- Windows: *Windows_directory*\logevent.cfg

たとえば、LogHost属性を次のように編集します。

```
LogHost=192.168.1.8
```

詳細については、『*Novell Audit 2.0 Administration Guide*』の「Configuring the Audit Platform Agent」のセクションを参照してください。

eDirectoryに対するNovell Auditの設定

iManagerを使用してNovell Audit Platform AgentによるeDirectoryイベントの監査を設定するには、監査するeDirectoryイベントのタイプを選択します。

1. 次のURLを使って、iManagerにログインします。

   ```
   https://ip_address_or_DNS/nps/
   ```

   ここで、*ip_address_or_DNS*は、iManagerサーバのIPアドレスまたはDNS名を指しています。次に例を示します。

   ```
   https://111.111.1.1/nps/
   ```

2. ［**役割およびタスク**］で［**eDirectoryの監査**］>［**監査の環境設定**］の順に選択します。
3. イベントを収集するeDirectoryサーバに対応するNCP Serverオブジェクトをブラウズして選択します。［**OK**］をクリックします。
4. ［**Novell Audit**］タブをクリックして、［eDirectory Instrumentationの設定］ページを表示します。
5. eDirectoryからレプリカリング内の別のレプリカに複製されたイベントを送信しないようにするには、［**複製されたイベントを送信しない**］を選択します。

   このオプションを使って、不要なイベントノイズを除外し、ログサイズを小さくすることができます。
6. インラインプレイベントレポーティングを有効にするには、［**イベントをインラインで登録する**］を選択します。

   このオプションを選択すると、eDirectoryのパフォーマンスが低下する可能性があるという点に注意してください。
7. 監査するイベントタイプを選択します。
8. 1つ以上の特定オブジェクトクラスに対するイベントをフィルタする場合は、次の操作を実行してください。

   8a 次のいずれかのハイパーリンクオブジェクトをクリックします。

   - ［**オブジェクト**］>［**作成**］
   - ［**オブジェクト**］>［**削除**］
   - ［**属性**］>［**値の追加**］

- ［属性］>［値の削除］
- ［LDAP］>［LDAP追加］
- ［LDAP］>［LDAP変更］
- ［LDAP］>［LDAP削除］
- ［LDAP］>［LDAP変更DN］

8b ［使用可能なオブジェクトクラス］リストで、イベントを監査するオブジェクトクラスを選択し、右矢印をクリックします。

8c ［OK］を2回クリックします。

9 1つ以上の特定属性に対するイベントをフィルタする場合は、次の手順を実行してください。

9a 次のいずれかのハイパーリンクオブジェクトをクリックします。

- ［属性］>［値の追加］
- ［属性］>［値の削除］

9b ［使用可能な属性］リストで、イベントを監査する属性を選択し、右矢印をクリックします。

9c ［OK］を2回クリックします。

注: eDirectoryはすべてのフィルタに対してイベントを個別に評価します。このため、イベントが1つのフィルタだけしか一致しない場合でも、eDirectoryはそのイベントをクライアントに送信します。イベントのフィルタリングについては、「616 ページの「eDirectory監査イベントのフィルタ処理について」」を参照してください。

---

10 ［適用］をクリックし、［OK］をクリックします。

監査設定に対する変更は、3分以内に有効になります。Auditモジュールをアンロードしてから、リロードし直して、変更を直ちに適用することもできます。Auditモジュールの詳細については、「629 ページの 「モジュールのロードとアンロード」」を参照してください。

注: メタイベントを生成する［値の追加］および［値の削除］属性を確認します。

Auditモジュールのロード

Auditモジュールをロードまたはアンロードするには、プラットフォームに応じて、次の手順のいずれかを使用します。

- 613 ページの 「Linux」
- 614 ページの 「Windows」

Linux

1 Auditモジュールがロードされていない場合は、次のコマンドを実行してロードします。

```
ndstrace -c "load auditds"
```

2 Auditモジュールをアンロードするには、次のコマンドを実行します。

```
ndstrace -c "unload auditds"
```

3 eDirectoryの起動時にAuditモジュールを自動的にロードするには、/etc/opt/novell/eDirectory/conf/ndsmodules.conf ファイルを編集し、次の行をこのファイルに追加します。

```
auditds     auto     #eDirectory instrumentation
```

Windows

1 Auditモジュールをロードします。

1a **［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。

1b ［Services］タブから［**nauditds**］を選択し、［**Start**］をクリックします。

2 Auditモジュールをアンロードします。

2a **［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。

2b ［サービス］タブから［**nauditds**］を選択し、［**中止**］をクリックします。

3 eDirectoryの起動時にAuditモジュールを自動的にロードするには、次の操作を実行します。

3a **［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。

3b ［**サービス**］タブから［**nauditds**］を選択し、［**起動**］をクリックします。

3c ［**自動**］をオンにして、［**OK**］をクリックします。

4 eDirectoryの起動時のAuditモジュールの自動ロードを無効にするには、次の操作を実行します。

4a **［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。

4b ［**サービス**］タブから［**nauditds**］を選択し、［**起動**］をクリックします。

4c ［**自動**］チェックボックスをオフにして、［**OK**］をクリックします。

eDirectoryイベントレポートについて

eDirectoryは*ジャーナル*と*インライン*という2種類の異なるイベントレポートシステムを使って、イベントを記録します。 デフォルトでは、eDirectoryはジャーナルイベントレポートを使って、イベントを記録しますが、iManagerでインラインイベントレポートを有効にすることができます。インラインイベントレポートの有効化の詳細については、「612 ページの 「eDirectoryに対するNovell Auditの設定」」を参照してください。

ジャーナル: このレポートシステムは、同期型イベント後レポート機能を提供します。ジャーナルイベントレポートを有効にすると、eDirectoryはイベントをジャーナルイベント処理キューに追加します。次にeDirectoryは個別のスレッドを使って、キュー内のイベントを処理し、そのイベントを監査クライアントに送信します。

インライン: このレポートシステムは、同期型イベント前レポート機能を提供します。インラインイベントレポートを有効にすると、eDirectoryは同じスレッドを使用して、クライアントに直接イベントを送信します。インラインイベントレポートを有効にすると、eDirectoryのパフォーマンスが影響を受ける可能性があることに注意してください。

eDirectoryイベントタイプについて

イベントを次のカテゴリに記録するように、eDirectoryを設定できます。

- メタ
- オブジェクト
- 属性
- スキーマ
- 接続
- エージェント
- その他
- バインダリ
- レプリカ
- パーティション
- LDAP

次のイベントタイプのデフォルトセットを監査することをお勧めします。

カテゴリ	イベントタイプ
メタ	すべてのイベントタイプ
オブジェクト	◆ 追加するプロパティ ◆ ログインの許可 ◆ パスワードの変更 ◆ セキュリティ等号の変更 ◆ 作成 ◆ 削除 ◆ プロパティの削除 ◆ ログイン ◆ ログアウト ◆ RDNの変更 ◆ 移動(ターゲット) ◆ 移動(ソース) ◆ 削除 ◆ 名前の変更 ◆ 復元 ◆ 検索 ◆ パスワードの確認
属性	すべてのイベントタイプ

カテゴリ	イベントタイプ
エージェント	◆ DS再ロード ◆ ローカルエージェントクローズ ◆ ローカルエージェントオープン ◆ NLMロード
その他	◆ CAキーの生成 ◆ 公開キーの再認証
LDAP	◆ LDAPバインド ◆ LDAP変更 ◆ LDAPパスワード変更 ◆ LDAPレスポンスの追加 ◆ LDAPアンバインド ◆ LDAP削除 ◆ LDAP DNの変更 ◆ LDAPレスポンスの変更 ◆ LDAP検索 ◆ LDAPレスポンスのバインド ◆ LDAPレスポンスの削除 ◆ LDAP追加 ◆ LDAP応答の検索 ◆ LDAP DNレスポンスの変更

eDirectory監査イベントのフィルタ処理について

1つまたは複数の固有オブジェクトクラスまたは属性に対し、イベント種類に応じて、イベントをフィルタ処理することができます。eDirectoryは生成されたすべてのイベントを、eDirectoryサーバ上で設定されているフィルタを基準にして評価し、そのフィルタと一致するイベント*だけ*を、監査クライアントに送信します。

複数のフィルタを使用して、eDirectoryイベントを個別にフィルタ処理できます。たとえば、特定のオブジェクトクラスと属性(1つまたは複数)の両方にフィルタを設定した場合、eDirectoryは*いずれか*のフィルタと一致するすべてのイベントをクライアントに送信します。ユーザはフィルタを変更できないため、eDirectoryは特定のオブジェクトクラス*と*特定の属性だけをクライアントに送信します。eDirectoryイベントをフィルタするオブジェクトクラスまたは属性は複数選択できます。

注: オブジェクトクラスと属性を組み合わせて最大256個までフィルタできます。

ハイパーリンクが設定された次のいずれかのイベントタイプをクリックして、そのイベントタイプをフィルタする1つ以上のオブジェクトクラスまたは属性を選択します。

カテゴリ	イベントタイプ	フィルタのタイプ
オブジェクト	◆ 作成 ◆ 削除	オブジェクトクラス
属性	◆ 値の追加 ◆ 値の削除	オブジェクトクラスまたは属性
LDAP	◆ LDAP変更 ◆ LDAP削除 ◆ LDAP DNの変更 ◆ LDAP追加	オブジェクトクラス

たとえば、別のユーザがeDirectoryでユーザアカウントを作成した場合に通知を受信する場合は、iManagerを使ってフィルタを作成し、Userオブジェクトを作成するCreate Obejectイベントだけを検索します。

iManagerで［役割およびタスク］>［eDirectoryの監査］>［監査の環境設定］と移動し、監視するNCPサーバを選択して、［Novell Audit］タブをクリックします。オブジェクトリストで、［作成］ハイパーリンクをクリックします。［使用可能なオブジェクトクラス］リストで、［ユーザ］を選択し、右矢印をクリックして、［ユーザ］を［選択されたオブジェクトクラス］リストに移動し、［OK］をクリックします。

フィルタが設定されている場合、eDirectoryはユーザが作成したイベントに対して、生成されたすべてのイベントをチェックし、該当するイベントをクライアントに送信します。他のイベントタイプを選択しない場合、または他のオブジェクトクラスや属性に対してフィルタを設定していない場合、eDirectoryは、ユーザが作成したイベント*だけ*を監査します。

ObjectとLDAPカテゴリフィルタはオブジェクトクラスだけをフィルタしますが、Attributeカテゴリフィルタはオブジェクトクラスと属性クラスの両方をフィルタすることができます。

上記のイベントタイプのいずれかを選択し、フィルタするオブジェクトクラスまたは属性を指定しなかった場合、eDirectoryは該当するイベントタイプのすべてのイベントをクライアントに送信します。

Sentinelを使ったeDirectoryイベントの監視

NetIQ Sentinelは、eDirectoryイベントの収集と監査を行うコレクタを提供します。Sentinelで特定のeDirectoryイベントを監視するには、特定のeDirectory監査設定が適切に構成されていることを確認する必要があります。

監査設定の設定の詳細については、「612 ページの 「eDirectoryに対するNovell Auditの設定」」を参照してください。

eDirectoryイベントを収集するようにSentinelを設定するには、Sentinel Plug-insサイト (http://support.novell.com/products/sentinel/secure/sentinelplugins.html)にある『*Sentinel Collector Guide for NetIQ eDirectory*』を参照してください。

Create Objectイベントの監査

アカウントとして使用するオブジェクトを作成する場合、eDirectoryは最初に汎用オブジェクトを作成し、次にAdd Valueイベントを使って、オブジェクトクラスをユーザタイプに変更します。Sentinelがイベントを適切に収集するように設定するには、iManagerでAdd Valueイベントの監査を有効にする必要があります。Add Valueイベントの監査を有効にしない場合、SentinelのCollectorはCreate Objectイベントを解析することができないためSentinelで「Configuration Error」イベントが生成されます。

オブジェクトの作成イベントを有効にするには、iManagerを起動し、［eDirectoryの監査］>［監査の環境設定］>［NovellAudit］ウィンドウの順に移動します。［オブジェクト］>［作成］と［属性］>［値の追加］の両方を選択します。

LDAPイベントの監査

eDirectoryは各LDAPリクエストをトランザクションと見なし、リクエストが開始された場合、レスポンスを受信した場合、およびトランザクションが完了した場合に、イベントを生成します。

ただしSentinelでは、各リクエストレスポンスペアは1つのイベントとして処理されます。SentinelでeDirectoryのLDAPイベントタイプを監視するには、リクエストイベントとレスポンスイベントの両方に対して監査を有効にする必要があります。たとえばLDAPバインドリクエストを監査するには、iManagerでLDAP BindイベントとLDAP Bind Responseイベントの両方の監査を設定する必要があります。

Failed Loginイベントの監査

eDirectoryでFailed Loginイベントを監視する場合は、iManagerを使って、eDirectoryサーバ上のAdd Valueイベントの監査を有効にする必要があります。また、eDirectoryコンテナやFailed Loginイベントを監査するコンテナの［不正侵入者検出］を有効にする必要があります。

重要: 監視するコンテナのレプリカが存在するサーバごとに、［不正侵入者検出］と［値の追加］のイベント監査を有効にする必要があります。

コンテナで［不正侵入者検出］を有効にするには、次の手順を実行してください。

1. iManagerにログインします。
2. ［役割およびタスク］で［ディレクトリ管理］>［オブジェクトの変更］の順に選択します。
3. 監査するeDirectoryコンテナをブラウズして選択します。［OK］をクリックします。
4. ［一般］タブで、［不正侵入者検出］をクリックします。
5. ［Intruder Detection］をオンにします。
6. ［OK］をクリックします。

注

- 他のまたは［不正侵入者検出］関連の設定を設定したり、［検出後にアカウントをロック］設定を有効にする必要はありません。
- NMAS経由で行われるログインの失敗ログインイベントを監視するには、NMASコレクタの［終了ログイン状況］を確認する必要があります。詳細については、689ページの「NMASイベントの監査」を参照してください。

Novell Auditパッケージのアンインストール

次のセクションでは、Novell Auditパッケージのアンインストール方法について説明します。

- 619 ページの 「LinuxのAuditパッケージをアンインストールする」
- 619 ページの 「WindowsのAuditパッケージをアンインストールする」

LinuxのAuditパッケージをアンインストールする

LinuxのAuditパッケージをアンインストールするには、次の手順を実行します。

1. ndstrace -c unload auditdsコマンドを使って、Auditモジュールをアンロードします。
2. novell-AUDTedirinst-9.2.0-*xx*.rpmをアンインストールします。

   ```
   #rpm -e --nodeps novell-AUDTedirinst-9.2.0-xx
   ```

3. /etc/opt/novell/eDirectory/conf/ndsmodules.confファイルを編集して、auditdsに対応する行(存在する場合)を削除することで、eDirectoryの起動時のAuditモジュールの自動ロードを無効にします。auditdsに対応する行を次に示します。

   ```
   auditds     auto     #eDirectory Instrumentation
   ```

注: 他にインストールされている監査がない場合は、#rpm -e novell-AUDTplatformagent-2.0.2-80コマンドを使ってnovell-AUDTplatformagent-2.0.2-80 Audit Platform Agentをアンインストールします。

WindowsのAuditパッケージをアンインストールする

WindowsのAuditパッケージをアンインストールするには、次の手順を実行します。

1. 次のようにAuditモジュールをアンロードします。
   - **1a** ［スタート］>［コントロールパネル］>［Novell eDirectoryサービス］の順に移動します。
   - **1b** ［サービス］を選択します。
   - **1c** nauditds.dlmをクリックし、次に［中止］をクリックします。
2. C:\Novell\NDSディレクトリからnauditds.dlmを削除します。 directory.
3. C:\Novell\NDSディレクトリからediraudit.schファイルを削除します。

注: 他のインストラメンテーションがインストールされていない場合は、C:\Novell\NDSからlogevent.dllファイルを削除することで、Audit Platform Agentをアンインストールします。

XDASを使用した監査

XDAS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。XDAS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。XDAS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。XDAS分類は一連のフィールドを定義します。そのうちの主要なフィールドは、observer、initiator、およびtargetです。XDASイベントは、異なるアプリケーションの監査記録を理解しやすくするのに役立ちます。

重要: XDASによる監査のサポートは、eDirectory 9.2以降では非推奨となっています。初めてeDirectory 9.2をインストールする場合、XDASによる監査のオプションを使用することはできなくなります。eDirectoryを以前のバージョンからアップグレードする場合、XDASを使用することはできますが、CEF監査に移行することをお勧めします。新たに追加した9.2サーバでXDASを使用する場合は、古いバージョンのeDirectoryからXDAS rpmをコピーして、新しいサーバを設定する必要があります。古いバージョンのeDirectoryのconfフォルダから、xdasconfig.propertiesファイルを最新バージョンにコピーしてください。

XDASを使用するようにeDirectoryを設定すると、次のようなメリットがあります。

- セキュリティで保護された監査サービスを分散システムに提供します。
- グローバルな分散システムレベルで一連の一般イベントを定義します。
- 分散システムの複数のコンポーネントからの監査情報のマージと分析に役立つ、共通のポータブルな監査レコードフォーマットを定義します。
- 分析アプリケーションで使用可能な、監査イベントの共通のフォーマットを定義します。
- XDAS監査証跡を記録します。
- イベント事前選択基準とイベント廃棄アクションを設定します。
- XDASサービスを実行するプラットフォームに関係なく、共通の監査フォーマットを提供します。
- 異機種混在環境をサポートします。そのために、現在のオペレーティングシステムやアプリケーション固有の監査サービス実装を再設計する必要はありません。
- 適正なユーザの義務の分離をサポートします。
- 特定の管理役割またはセキュリティ役割を担っているプリンシパルだけが監査ログにアクセスできるようにすることで、監査ログを保護します。
- オプションで、エージェントと監査サーバ間で通信障害が発生した場合にエージェントで監査イベントをローカルでキャッシュに保存し、通信が再確立されてからイベントを再送信します。

XDASの設定

eDirectoryインストールキットには、ダウンロードパッケージの一部としてLinux版とWindows版の両方のXDASクライアントが付属しています。eDirectoryのインストールプログラムは、オペレーティングシステム上にXDASパッケージをインストールします。XDASパッケージには、次のファイルが含まれています。

- Linux
  - novell-edirectory-xdaslog

- novell-edirectory-xdaslog-conf
- novell-edirectory-xdasinstrument

- Windows
  - xdasauditds.dlm
  - xdaslog.dll

注: OES 11 SP2リリースから、XDAS RPMがOpen Enterprise Serverにバンドルされています。

システム要件

NetIQ Audit iManagerプラグインをインストールして使用するには、iManager 3.0以降が必要です。要件とダウンロード手順については、NetIQ iManagerの製品ページを参照してください。

XDAS用のiManagerプラグインのインストールまたはアップグレード

XDAS用のiManagerプラグインは、eDirectoryプラグインにバンドルされています。または、NetIQダウンロードサイトからeDirectoryプラグインをダウンロードできます。

プラグインを最新バージョンにアップグレードするには:

1. 次のURLを使用して、Webブラウザからを開きます。

   `https://ip_address_or_DNS/nps/iManager.html`

   ここで、*ip_address_or_DNS*は、iManagerサーバのIPアドレスまたはDNS名を指しています。

   次に例を示します。

   `http://111.111.1.1/nps/iManager.html`

2. ユーザ名とパスワードを使用してiManagerにログインします。

   NetIQ iManagerのすべての機能を利用するには、管理者としてツリーにログインします。管理者ユーザだけが、すべての機能への完全アクセス権を持っています。管理者ユーザ以外は、権利が割り当てられている役割にのみアクセスできます。

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

3. ［**役割およびタスク**］>［**監査の環境設定**］を選択します。

   iManagerに、XDASの新しい変更点に関する警告メッセージが表示されます。

4. **OK**をクリックします。

   アップグレード中に、新しいiManagerのファイルがインストールされ、環境設定が変更されます。アップグレードが完了したら、インストールの成功または失敗のステータスを示すメッセージが表示されます。

XDASプロパティファイルの設定

eDirectoryメディアでは、サンプルプロパティファイルであるxdasconfig.properties.templateファイルがconfigdir (n4u.server.configdir)ディレクトリに格納されています。

表 23-1に、Linuxオペレーティングシステムと Windowsオペレーティングシステム上のxdasconfig.propertiesファイルのデフォルトの場所を示します。

表 23-1 XDAS環境設定ファイル

オペレーティングシステム	プロパティファイルの場所
Linux	`/etc/opt/novell/eDirectory/conf/xdasconfig.properties` 非ルートインストールでは、XDASプロパティファイルがconfディレクトリに配置されます。
Windows	`<Install Path>/novell/nds/xdasconfig` 通常は、プロパティファイルはeDirectoryのインストールディレクトリに配置されます。

プロパティファイルを設定してから、環境をeDirectory 9.2にアップグレードする場合、インストーラはプロパティファイルを置き換えません。代わりに、アップグレードプロセスがこのファイル(xdasconfig.properties.template)を更新してカスタマイズ内容が保持されるようにします。

iManagerのインストール後、XDASを設定できます。XDAS環境設定は、単純なテキストベースのxdasconfig.properties環境設定ファイルに保存されます。実際の要件に応じてこのファイルをカスタマイズできます。

XDASプロパティファイルには次の情報が含まれています。

Linux

```
# Set the level of the root logger to DEBUG and attach appenders.
#log4j.rootLogger=debug, S, R

# Defines appender S to be a SyslogAppender.
#log4j.appender.S=org.apache.log4j.net.SyslogAppender

# Defines location of Syslog server.
#log4j.appender.S.Host=localhost
#log4j.appender.S.Port=port

# Specify protocol to be used (UDP/TCP/SSL)
#log4j.appender.S.Protocol=UDP

# Specify SSL certificate file for SSL connection.
# File path should be given with double backslash.
#log4j.appender.S.SSLCertFile=/etc/opt/novell/mycert.pem

# Minimum log-level allowed in syslog.
#log4j.appender.S.Threshold=INFO

# Defines the type of facility.
#log4j.appender.S.Facility=USER

# Defines caching for SyslogAppender.
# Inputs should be yes/no
#log4j.appender.S.CacheEnabled=no

# Cache location directory
# Directory should be available for creating cache files
#log4j.appender.S.CacheDir=/var/opt/novell/eDirectory
```

```
# Cache File Size
# Cache File Size should be in the range of 50MB to 4000MB
#log4j.appender.S.CacheMaxFileSize=500MB

# Layout definition for appender Syslog S.
#log4j.appender.S.layout=org.apache.log4j.PatternLayout
#log4j.appender.S.layout.ConversionPattern=%c : %p%m%n

# Defines appender R to be a Rolling File Appender.
#log4j.appender.R=org.apache.log4j.RollingFileAppender

# Log file for appender R.
#log4j.appender.R.File=/var/opt/novell/eDirectory/log/xdas-events.log

# Max size of log file for appender R.
#log4j.appender.R.MaxFileSize=100MB

# Set the maximum number of backup files to keep for appender R.
# Max can be 13. If set to zero, then there will be no backup files.
#log4j.appender.R.MaxBackupIndex=10

# Layout definition for appender Rolling log file R.
#log4j.appender.R.layout=org.apache.log4j.PatternLayout
#log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c : %p%m%n
```

Windows

```
# Brief description for appenders and their options are provided.
# For detailed decriptions refer to log4cxx documentation.

# Set the level of the root logger to DEBUG and attach appenders.
#log4j.rootLogger=debug, S, R

# Defines appender S to be a SyslogAppender.
#log4j.appender.S=org.apache.log4j.net.SyslogAppender

# Defines location of Syslog server.
#log4j.appender.S.Host=localhost
#log4j.appender.S.Port=port

# Specify protocol to be used (UDP/TCP/SSL).
#log4j.appender.S.Protocol=UDP

# Specify SSL certificate file for SSL connection.
# File path should be given with double backslash.
#log4j.appender.S.SSLCertFile=C:\\Novell\\mycert.pem

# Minimum log-level allowed in syslog.
#log4j.appender.S.Threshold=INFO

# Defines the type of facility.
#log4j.appender.S.Facility=USER

# Defines caching for SyslogAppender.
# Inputs should be yes/no
#log4j.appender.S.CacheEnabled=yes

# Cache location directory
# Directory should be available for creating cache files
#log4j.appender.S.CacheDir=C:\\NetIQ\\eDirectory
```

```
# Cache File Size
# Cache File size should be in the range of 50MB to 4000MB
#log4j.appender.S.CacheMaxFileSize=500MB

# Layout definition for appender Syslog S.
#log4j.appender.S.layout=org.apache.log4j.PatternLayout
#log4j.appender.S.layout.ConversionPattern=%c: %p%m%n

# Defines appender R to be a Rolling File Appender.
#log4j.appender.R=org.apache.log4j.RollingFileAppender

# Log file for appender R.
# File path should be given with double backslash.
#log4j.appender.R.File=C:\\xdas-events.log

# Max size of log file for appender R.
#log4j.appender.R.MaxFileSize=100MB

# Set the maximum number of backup files to keep for appender R.
# Max can be 13. If set to zero, then there will be no backup files.
#log4j.appender.R.MaxBackupIndex=10

# Layout definition for appender Rolling log file R.
#log4j.appender.R.layout=org.apache.log4j.PatternLayout
#log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c : %p%m%n
```

xdasconfig.propertiesファイルの内容を検討する前に、以下の考慮事項を確認することをお勧めします。

- 文字のSとRは、それぞれSyslogアペンダとローリングファイルアペンダを意味します。
- エントリは大文字と小文字が区別されません。
- エントリは任意の順序で表示できます。
- ファイル内の空白行は有効です。
- ハッシュ(#)で始まるすべての行はコメントアウトされた行です。

次の表に、xdasconfig.propertiesファイル内設定に関する情報を示します。

重要: 環境設定の変更後は、eDirectoryを再起動する必要があります。

設定	説明
log4j.rootLogger=**debug, S, R**	ルートのログの記録レベルをデバッグに設定して、RまたはSという名前のアペンダをアタッチします。SはSyslogアペンダを、Rはローリングファイルアペンダを意味します。
log4j.appender.S=**org.apache.log4j.net.SyslogAppender**	アペンダSをSyslogアペンダとして指定します。
log4j.appender.S.Host=**localhost**	XDASイベントの記録先のSyslogサーバの場所を指定します。 IFor example,log4j.appender.S.Host=192.168.0.1

設定	説明
log4j.appender.S.Port=**port**	XDASがSyslogサーバに接続するポートです。 このポートは1～65535の値をサポートします。無効な値が指定された場合は、ポートがデフォルトで514に設定します。 XDASとSyslogサーバ間の接続が失われた場合は、接続が回復するまでIdentity Managerはイベントを記録できません。
log4j.appender.S.Protocol=UDP	使用するプロトコルを指定します。たとえば、UDP、TCP、またはSSLなどです。
log4j.appender.S.SSLCertFile=**/etc/opt/novell/mycert.pem**	SSL接続用のSSL証明書ファイルを指定します。ファイルのパスを指定する場合は二重の円記号を使用します。この設定の指定は任意です。
log4j.appender.S.Threshold=**INFO**	Syslogアペンダで許可される最小ログレベルを指定します。現在は、INFOログレベルがサポートされています。
log4j.appender.S.Facility=**USER**	ファシリティのタイプを指定します。ファシリティは、メッセージを分類するために使用されます。現在、USERファシリティがサポートされています。これらの値は大文字または小文字で指定することができます。
log4j.appender.S.layout=**org.apache.log4j.PatternLayout**	Syslogアペンダ用のレイアウト設定です。
log4j.appender.S.layout.ConversionPattern=**%c : %p%m%n**	Syslogアペンダ用のレイアウト設定です。変換パターンとその説明については、「logging.apache.org」を参照してください。
log4j.appender.R=**org.apache.log4j.RollingFileAppender**	アペンダRをローリングファイルアペンダとして指定します。
log4j.appender.R.File=**/var/opt/novell/eDirectory/log/xdas-events.log**	ローリングファイルアペンダ用のログファイルの場所です。
log4j.appender.R.MaxFileSize=**100MB**	ローリングファイルアペンダ用のログファイルの最大サイズ(MB単位)です。この値はクライアントで許可される最大サイズに設定します。
log4j.appender.R.MaxBackupIndex=**10**	ローリングファイルアペンダ用のバックアップファイルの最大数を指定します。バックアップファイルの最大数は10にすることができます。0の値はバックアップファイルなしを意味します。
log4j.appender.R.layout=**org.apache.log4j.PatternLayout**	ローリングファイルアペンダ用のレイアウト設定です。
log4j.appender.R.layout.ConversionPattern=**%d{MMM dd HH:mm:ss} %c : %p%m%n**	ローリングファイルアペンダ用のレイアウト設定です。簡易日付フォーマットパターンについては、表23-2を参照してください。 変換パターンとその説明については、「logging.apache.org」を参照してください。

表 23-2に、米国で解釈される日付と時刻のパターンの例を示します。指定されている日付と時刻は、米国太平洋タイムゾーンの2012年7月4日12時8分56秒です。

表 23-2 日付と時刻のパターンの例

日付と時刻のパターン	結果
"yyyy.MM.dd G 'at' HH:mm:ss z"	2012.07.04 AD at 12:08:56 PDT
"EEE, MMM d, "yy"	Wed, Jul 4, '01
"h:mm a"	12:08 PM
"hh 'o''clock' a, zzzz"	12 o'clock PM, Pacific Daylight Time
"K:mm a, z"	0:08 PM, PDT
"yyyyy.MMMMM.dd GGG hh:mm aaa"	02012.July.24 AD 12:08 PM
"EEE, d MMM yyyy HH:mm:ss Z"	Wed, 24 Jul 2012 12:08:56 -0700
"yyMMddHHmmssZ"	120724120856-0700
"yyyy-MM-dd'T'HH:mm:ss.SSSZ"	2012-07-04T12:08:56.235-0700

Syslogアペンダの有効化

監査メッセージを一カ所で集中管理するには、Syslogアペンダを使用します。加えて、Syslogサーバは災害発生時に優れたバックアップサポートを提供します。

Syslogアペンダを有効にするには、xdasxconfig.propertiesファイルに次の変更を加えます。

1. 次のエントリをSに変更して、Syslogアペンダをアタッチします。

   log4j.rootLogger=debug, S

2. 次のエントリをコメントアウトします。

   ```
   log4j.appender.S=org.apache.log4j.net.SyslogAppender
   log4j.appender.S.Host=localhost
   log4j.appender.S.Port=port
   log4j.appender.S.Protocol=UDP
   log4j.appender.S.SSLCertFile=/etc/opt/novell/mycert.pem
   #log4j.appender.S.Threshold=INFO
   #log4j.appender.S.Facility=USER
   #log4j.appender.S.layout=org.apache.log4j.PatternLayout
   #log4j.appender.S.layout.ConversionPattern=%c : %p%m%n
   ```

3. iManagerにログインして、ログイベントを変更します。XDASイベントの設定方法については、628 ページの 「監査するXDASイベントの設定」を参照してください。

注: SyslogAppenderに対してUDPプロトコルを使用するXDASキャッシングは機能しません。

Syslog SSL接続用の証明書の生成

Syslog接続用の証明書を生成するには:

1. 次のOpenSSLコマンドを使用して証明書を作成します。

   ```
   openssl s_client -host LOG_SERVER  -port 1443 -showcerts
   ```

2. /etc/opt/novell/eDirectory/conf/xdasconfig.propertiesファイルで作成した証明書ファイルの場所を指定します。

ローリングファイルアペンダの有効化

監査ソリューションが個別のサーバに制限されている場合は、ファイルアペンダをお勧めします。また、このソリューションは、セットアップするコンポーネントの数が少なく立ち上げが容易なため、デモンストレーションに向いています。

ローリングファイルアペンダを有効にするには、xdasconfig.propertiesファイルに次の変更を加えます。

1 次のエントリをRに変更して、ローリングファイルアペンダをアタッチします。

   log4j.rootLogger=debug, R

2 次のエントリをコメントアウトします。

   ```
   log4j.appender.R=org.apache.log4j.RollingFileAppender
   log4j.appender.R.File=/var/opt/novell/eDirectory/log/xdas-events.log
   log4j.appender.R.MaxFileSize=100MB
   log4j.appender.R.MaxBackupIndex=10
   log4j.appender.R.layout=org.apache.log4j.PatternLayout
   log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c : %p%m%n
   ```

3 iManagerから必要なイベントを選択します。

   XDASイベントの設定方法については、628 ページの 「監査するXDASイベントの設定」を参照してください。

監査用のXDASの設定

iManagerプラグインを使用したXDASの設定

1 次のURLを使用してWebブラウザからiManagerを開きます。

   `https://`*`ip_address_or_DNS`*`/nps/iManager.html`

   ここで、*ip_address_or_DNS*は、iManagerサーバのIPアドレスまたはDNS名を指しています。

   次に例を示します。

   ```
   http://111.111.1.1/nps/iManager.html
   ```

2 自分のユーザ名とパスワードを使用してログインします。

NetIQ iManagerのすべての機能を利用するには、管理者としてツリーにログインします。管理者ユーザだけが、すべての機能への完全アクセス権を持っています。管理者ユーザ以外は、権利が割り当てられている役割にのみアクセスできます。

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

3 ［**役割およびタスク**］>［**監査の環境設定**］を選択します。

4 ［**NCPサーバ**］にeDirectoryサーバの名前を指定してから、［**オブジェクトセレクタ**］アイコンをクリックしてeDirectoryサーバをブラウズします。

5 **OK**をクリックします。

［XDAS監査］ページが表示されます。620 ページの 「XDASの設定」に進みます。

監査するXDASイベントの設定

1 ユーザ名とパスワードを使用してiManagerにログインします。

2 ［**役割およびタスク**］>［**監査の環境設定**］を選択します。

3 ［**XDAS**］タブを選択します。

4 XDASイベントを設定します。

- **基本イベント環境設定:** 環境に必要なイベントに基づいて、次のオプションの値を指定します。

  注: デフォルトでは、［基本イベント環境設定］セクションの下に個々のイベントカテゴリが折りたたまれます。個々のイベントを選択するには、各カテゴリを展開できます。

オプション	説明
アカウント管理イベント	ログに記録するアカウント管理イベントを選択します。アカウントの作成、削除、有効化、無効化のイベントに加えて、アカウントの照会や変更に関するイベントをログに記録します。
トラスト管理イベント	ログに記録するイベントのトラスト管理イベントを選択します。トラストを作成、削除、照会、および変更するイベントをログに記録します。
アカウントデータイベント	ログに記録するイベントのアカウントデータイベントを選択します。データ項目を作成および削除したり、データ項目の属性を変更および照会したりするイベントをログに記録します。
セキュリティイベント	ログに記録するイベントのアカウントセキュリティイベントを選択します。アクセスの付与または取り消し、ログイン、パスワード変更、および照会のイベントをログに記録します。このイベントセットは、eDirectoryシステムにおける不正侵入者を検出するためにも役立ちます。

- **詳細:** 環境に必要なイベントに基づいて、次のオプションの値を指定します。
  - **Global:** 重複したエントリのグローバル設定を選択またはクリアすることができます。
    - **複製されたイベントを送信しない:** 他のサーバからの複製に起因する重複イベントの受信を停止する場合にこのオプションを選択します。

- **ログイベントの値:** イベントがテキストファイルに記録されます。サイズが768バイトを超えるイベントの値が「大きい値」と見なされます。どんなサイズのイベントでもログに記録できます。
  - **大きい値をログに記録:** このオプションは、サイズが768バイトを超えるイベントをログに記録する場合に選択します。
  - **大きい値をログに記録しない:** このオプションを選択して、サイズが768バイトより小さいイベントをログに記録します。

  注: イベントサイズがこのサイズを超えている場合は、イベントの値が切り詰められてログファイルに保存されます。

- **高度なイベント環境設定:** 環境に必要なイベントに基づいて、次のオプションの値を指定します。

オプション	説明
サービスまたはアプリケーション管理イベント	ログに記録するサービスまたはアプリケーション管理イベントを選択します。サービスを有効にする、無効にする、起動する、終了するイベントをログに記録します。
オペレーショナルイベント	ログに記録するオペレーショナル管理イベントを選択します。システムを開始およびシャットダウンするイベント、データストアをバックアップおよびリストアするイベント、内部オペレーションを監査したり、プロセスのコンテキストを変更したりするイベントをログに記録します。

対応するXDASイベントにマッピングされたeDirectoryの内部イベントについては、881 ページの 「eDirectoryイベントとXDASイベントのマッピング」を参照してください。

注: イベントを選択してから、NCPサーバ上で設定変更が有効になるまで最大3分かかります。NCPサーバ上で設定変更をすぐに実装するには、xdasauditdsモジュールをアンロードしてからロードします。

モジュールのロードとアンロード

XDASイベントを設定したら、次のコマンドを実行して、XDASモジュールをロードまたはアンロードします。

ndsdサーバの起動時に自動的にxdasauditdモジュールをロードするには:

- **Linux**

  xdasauditdsを/etc/opt/novell/eDirectory/conf/ndsmodules.confファイルに追加します。

- **Windows**

  ndscons.exeを実行して、使用可能なモジュールのリストから［xdasauditds］を選択し、［スタートアップ］をクリックしてから、起動のタイプに［自動］を選択します。

xdasauditdsモジュールを手動でロードまたはアンロードするには:

- **Linux**

  ロードするには、ndstrace -c "xdasauditds"を実行します。

アンロードするには、ndstrace -c "unload xdasauditds"を実行します。

- **Windows**

  ロードするには、ndscons.exeを実行して、使用可能なモジュールのリストから［**xdasauditds**］を選択し、［**開始**］をクリックします。

  アンロードするには、ndscons.exeを実行して、使用可能なモジュールのリストから［**xdasauditds**］を選択し、［**停止**］をクリックします。

NMASをインストールしてNMAS監査を有効にした場合は、NMASサーバが自動的にXDASライブラリをロードします。

XDASイベントキャッシングの有効化

eDirectory 9.2では、必要に応じて、XDASイベントをエージェントのSyslogアペンダキャッシュにローカルに保存することができます。イベントをキャッシュに保存することにより、エージェントが監査サーバと通信できない場合にも、生成された監査イベントが保持され、監査データが消失しないように守られます。エージェントコンピュータが監査サーバと再び通信できるようになると、エージェントは、キャッシュに保存されたイベントの再送信を試みます。

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。イベントキャッシングを有効にするには、次の手順を実行します。

1. エージェントコンピュータで、XDASプロパティファイルの場所に移動します。xdasconfig.propertiesファイルは、デフォルトで、/etc/opt/novell/eDirectory/conf/xdasconfig.propertiesに配置されています。非ルートインストールでは、XDASプロパティファイルがデフォルトでconfディレクトリに配置されます。
2. テキストエディタを使用してxdasconfig.propertiesファイルを開きます。
3. プロパティファイル内で、log4j.appender.S.CacheEnabledプロパティに移動して、このプロパティ値をyesに変更します。
4. (状況によって実行)特定のディレクトリでイベントをキャッシュに保存する場合は、そのディレクトリパスを指すようにlog4j.appender.S.CacheDirプロパティの値を変更します。ディレクトリを指定する場合は、そのディレクトリパスがサーバ上の有効な場所であることを確認します。log4j.appender.S.CacheDirプロパティが設定されていないと、Syslog Appenderによって、特定のインスタンスのdibディレクトリにキャッシュイベントのログが記録されます。
5. (状況によって実行)キャッシュのカスタムファイルサイズを指定する場合は、log4j.appender.S.CacheMaxFileSizeプロパティの値を変更します。デフォルト値は500MBです。最小値は50MBで、最大値は4GBです。
6. xdasconfig.propertiesファイルを保存して閉じます。

XDASイベントのコレクタの使用

XDASイベントを収集するためのコレクタの使用方法については、Sentinelプラグインのページを参照してください。

XDAS監査イベントのフィルタリングについて

XDASは、フィルタとイベント通知を使用して、特定のタイプのイベントが発生したとき、または、発生しなかったときにレポートを作成できます。1つまたは複数の固有オブジェクトクラスまたは属性のイベントを、イベントタイプに応じてフィルタ処理することもできます。XDASは、生成されたすべてのイベントをeDirectoryサーバで設定済みのフィルタに照らして評価し、それらのフィルタに一致するイベントのみをログに記録します。

XDASアカウント、XDASトラスト、およびXDASデータ項目のフィルタとイベント通知を設定できます。XDASアカウントとトラストの場合、選択したオブジェクトクラスはそれぞれのイベントカテゴリにマッピングされます。たとえば、アカウントのフィルタに［**ユーザ**］クラスを選択すると、このクラスは自動的にアカウント管理イベントカテゴリにマップされます。デフォルトでは、アカウントやトラストにマップされないオブジェクトクラスは、データ項目管理イベントカテゴリにマップされます。

このセクションでは、システムフィルタと通知の設定に必要な情報を提供します。

XDASアカウント管理イベントのフィルタリング

アカウント用のフィルタリングを設定して、特定のイベントのみを検索することができます。たとえば、誰かがeDirectoryでユーザアカウントを作成したら通知が届くようにするには、新しいユーザオブジェクトの作成に関するイベントをログに記録するため、ユーザオブジェクトクラスを選択するフィルタを作成できます。

アカウントフィルタリングを設定するには、［アカウント管理イベント］リンクをクリックして、クラスを選択してから、［**OK**］をクリックしてアプリケーションを終了します。

アカウント管理イベントのフィルタを設定するには:

1. iManagerで、［**役割およびタスク**］>［**eDirectoryの監査**］>［**監査の環境設定**］に移動します。
2. 監視するNCPサーバを選択してから、［**OK**］をクリックします。

   デフォルトで、［**XDASイベント**］タブが選択されています。
3. ［**アカウント管理イベント**］をクリックします。

   ［XDASアカウント環境設定フィルタリング］ウィンドウが表示されます。
4. ［**使用可能なクラス**］リストで、任意のオブジェクトクラスを選択して、右矢印をクリックして対象オブジェクトクラスを［**選択されたクラス**］リストに移動し、［**OK**］をクリックします。デフォルトでは、［**構成員**］、［**人物**］、［**ユーザ**］のオブジェクトクラスが選択されます。
5. ［**使用可能な属性**］リストで、選択したオブジェクトクラスの属性を任意の数だけ選択します。属性を選択し、右矢印をクリックしてその属性を選択された属性のリストに追加します。

   アカウント管理イベントのフィルタが設定されます。

設定済みのフィルタを使用して、XDAS監査モジュールは選択済みオブジェクトクラスと属性に関して生成されたイベントすべてをチェックし、それらのイベントをログに記録します。

XDASトラスト管理イベントのフィルタリング

［トラスト管理イベント］リンクをクリックし、トラスト管理イベントのフィルタを設定します。たとえば、誰かがeDirectoryで新しいトラストを作成したら通知が届くようにするには、新しいトラストの作成に関するイベントをログに記録するため、グループオブジェクトクラスを選択するフィルタを作成できます。

トラスト管理イベントのフィルタを設定するには:

1 iManagerで、［役割およびタスク］>［eDirectoryの監査］>［監査の環境設定］に移動します。

2 監視するNCPサーバを選択してから、［OK］をクリックします。

デフォルトで、［XDASイベント］タブが選択されています。

3 ［トラスト管理イベント］をクリックします。

［XDASトラスト環境設定フィルタリング］ウィンドウが表示されます。

4 ［使用可能なクラス］リストで、イベントを収集するオブジェクトクラスを選択し、右矢印をクリックしてそれらを［選択されたクラス］リストに移動します。デフォルトでは、［dynamicGroup］、［dynamicGroupAux］、［グループ］、［LDAPグループ］、［職種］オブジェクトクラスが選択されています。

5 ［使用可能な属性］リストで、選択したオブジェクトクラスの属性を任意の数だけ選択します。属性を選択し、右矢印をクリックしてその属性を選択された属性のリストに追加します。

注: オブジェクトクラスを選択すると、そのオブジェクトクラスのすべての属性のトラストイベントすべてが選択されます。この場合は、選択したオブジェクトクラスのすべての属性に関するすべてのトラスト管理イベントを取得することになります。

---

6 ［OK］をクリックします。

フィルタを設定すると、XDAS監査モジュールはすべての選択済みオブジェクトクラスと属性に関して生成されたイベントすべてをチェックし、それらのイベントをログに記録します。

XDASデータ項目管理イベントのフィルタリング

［データ項目管理イベント］リンクをクリックし、XDASデータ項目のフィルタを設定します。XDASイベントを収集するオブジェクトのXDASデータ項目を設定できます。オブジェクトクラスを選択し、それらの属性を設定できます。

データ項目管理イベントのフィルタを設定するには:

1 iManagerで、［役割およびタスク］>［eDirectoryの監査］>［監査の環境設定］に移動します。

2 監視するNCPサーバを選択してから、［OK］をクリックします。

デフォルトで、［XDASイベント］タブが選択されています。

3 ［データ項目管理イベント］をクリックします。

［XDASデータ環境設定フィルタリング］ウィンドウが表示されます。

4 ［使用可能なクラス］リストで、イベントを収集するオブジェクトクラスを選択し、右矢印をクリックしてそれらを［選択されたクラス］リストに移動します。デフォルトでは、アカウントやトラストにマップされないオブジェクトクラスは、データ項目管理イベントカテゴリにマップされます。

注: オブジェクトクラスが選択されていない場合は、すべての使用可能なオブジェクトクラスのイベントが生成されます。

---

5 ［使用可能な属性］リストで、選択したオブジェクトクラスの属性を任意の数だけ選択します。属性を選択し、右矢印をクリックしてその属性を選択された属性のリストに追加します。

6 ［OK］をクリックします。

設定済みのフィルタを使用して、XDAS監査モジュールはすべての選択済みオブジェクトクラスと属性に関して生成されたイベントをチェックし、それらのイベントをログに記録します。

除外フィルタを使用したeDirectoryイベントのフィルタリング

［除外フィルタ］リンクをクリックして、イベントを生成する必要がないオブジェクトクラスと属性のためのフィルタを設定します。オブジェクトクラスを選択し、それらの属性を設定できます。

不要なeDirectoryイベントのフィルタを設定するには:

1 iManagerで、［役割およびタスク］>［eDirectoryの監査］>［監査の環境設定］に移動します。

2 監視するNCPサーバを選択してから、［OK］をクリックします。

デフォルトで、［XDASイベント］タブが選択されています。

3 ［除外リスト］をクリックします。

［XDAS除外フィルタリング］ウィンドウが表示されます。

4 ［使用可能なクラス］リストで、イベントを収集しないオブジェクトクラスを選択し、右矢印をクリックしてそれらを［選択されたクラス］リストに移動します。

5 ［使用可能な属性］リストで、選択したオブジェクトクラスの属性を任意の数だけ選択します。属性を選択し、右矢印をクリックしてその属性を選択された属性のリストに追加します。

6 ［OK］をクリックします。

設定済みのフィルタを使用して、XDAS監査モジュールは、すべての選択済みオブジェクトクラスと属性に関するイベントの生成を停止します。

XDASスキーマ

XDASスキーマは、次のように定義されます。

XDAS JSONスキーマ

```
{
    "id":"XDAS",
    "title":"XDAS Version 2 JSON Schema",
    "description":"A JSON representation of an XDAS event record.",
    "type":"objectr",
    "properties":{
      "Source":{
        "description":"The original source of the event, if applicable.",
        "type":"string",
        "optional":true
      },
      "Observer":{
        "description":"The recorder (ie., the XDAS service) of the event.",
        "type":"object",
        "optional":false,
        "properties":{
          "Account":{"$ref":"account"},
          "Entity":{"$ref":"entity"}
        }
```

```
      },
      "Initiator":{
        "description":"The authenticated entity or access  that causes an event.",
        "type":"object",
        "optional":false,
        "properties":{
          "Account":{"$ref":"account","optional":true},
          "Entity":{"$ref":"entity"},
          "Assertions":{
            "description":"Attribute/value assertions about an identity.",
            "type":"object",
            "optional":true
          }
        }
      },
      "Target":{
        "description":"The target object, account, data item, etc of the event.",
        "type":"object",
        "optional":true,
        "properties":{
          "Account":{"$ref":"account"},
          "Entity":{"$ref":"entity"},
          "Data":{
            "description":"A set attribute/value pairs describing the target
object.",         *
            "type":"object",
            "optional":true
          }
        }
      },
      "Action":{
        "description":"The action describes the event in a uniform manner.",
        "type":"object",
        "optional":false,
        "properties":{
          "Event":{
            "description":"The event identifier in standard XDAS taxonomy.",
            "type":"object",
            "optional":false,
            "properties":{
              "Id":{
                "description":"The XDAS taxonomy event identifier.",
                "type":"string",
                "optional":false,
                "pattern":"/^[0-9]+(\.[0-9]+)*$/"
              },
              "Name":{
                "description":"A short descriptive name for the specific event.",
eg. a new replica is added
                "type":"string",
                "optional":true
              },
      "CorrelationID":{
          "description":"Correlation ID, source#uniqueID#connID",
                 "type":"string",
                 "optional":true
      }
     },
     "SubEvent":{
      "type":object
```

```
      "description": "Describes the actual domain specific event that has
occured.",
      "optional":true,
      "properties":{
        "Name"":{
                    "description":"A short descriptive name for this event.",
                    "type":"string",
                    "optional":true
                  },
      }
            }
          }
          "Log":{
            "description":"Client-specified logging attributes.",
            "optional":true,
            "properties":{
              "Severity":{"type":"integer", "optional":true},
              "Priority":{"type":"integer", "optional":true},
              "Facility":{"type":"integer", "optional":true}
            }
          }
          "Outcome":{
            "description":"The XDAS taxonomy outcome identifier.",
            "type":"string",
            "optional":false,
            "pattern":"/^[0-9]+(\.[0-9]+)*$/"
          }
          "Time":{
            "description":"The time the event occurred.",
            "type":"object",
            "optional":false,
            "properties":{
              "Offset":{
                "description":"Seconds since Jan 1, 1970.",
                "type":"integer"
              },
              "Sequence":{
                "description":"Milliseconds since last integral second.",
                "type":"integer",
                "optional":true
              },
              "Tolerance":{
                "description":"A tolerance value in milliseconds.",
                "type":"integer",
                "optional":true
              },
              "Certainty":{
                "description":"Percentage certainty of tolerance.",
                "type":"integer",
                "optional":true,
                "minimum":0,
                "maximum":100,
                "default":100,
              },
              "Source":{
                "description":"The time source (eg., ntp://time.nist.gov).",
                "type":"string",
                "optional":true
              },
              "Zone":{
```

```
                "description":"A valid timezone symbol (eg., MST/MDT).",
                "type":"string",
                "optional":true
              }
            }
      "ExtendedOutcome":{
            "description":"The XDAS taxonomy outcome identifier.",
            "type":"string",
            "optional":false,
            "pattern":"/^[0-9]+(\.[0-9]+)*$/"
           }
        }
      }
    }
  },
  {
    "id":"account",
    "description":"A representation of an XDAS account.",
    "type":"object",
    "properties":{
      "Domain":{
       "description":"A (URL) reference to the authority managing this account.",
/* lets take it as the partition?
        "type":"string"
      },
      "Name":{
        "description":"A human-readable account name.",        - DN
        "type":"string",
        "optional":true
      },
      "Id":{
        "description":"A machine-readable unique account identifier value.",  -
EntryID
        "type":"integer"
      }
    }
  },
  {
    "id":"entity",                     - Server details for Target, client address
details for the initiator
    "description":"A representation of an addressable entity.",
    "type":"object",
    "properties":{
      "SysAddr":{"type":"string","optional":true},
      "SysName":{"type":"string","optional":true},
      "SvcName":{"type":"string","optional":true},
      "SvcComp":{"type":"string","optional":true},
    }
  }
```

XDASフィールドの定義

スキーマ内のこれらのフィールドは、XDAS監査イベント用に定義されたフィールドです。これらのフィールドの一部または全部が他のタイプのイベントに関係している場合もありますが、監査サービスにはこの種の情報が不可欠です。XDAS JSONレコードフォーマットはオープンです。つまり、新しいフィールドは、それがXDAS標準で監査用に定義されたフィールド値と競合しない限り、レコードの任意の場所に追加することができます。そのため、特定のワークフローまたはクライアント

セッション内のイベント間の相関データポイントとして使用可能なワークフロー識別子やセッション識別子などの特定のタイプの相関データが存在する場合は、それらのフィールドを追加することができます。フィールドの競合していない名前を選択するだけです。

***表 23-3** XDAS フィールドの定義*

XDASフィールド	説明
Source (オプション)	イベントのソースは、そのイベントが最初に定義されてからXDASイベントに変換された別のシステムのイベントサービスを示します。多くのイベントはXDASクライアントによって直接生成されるため、sourceフィールドはオプションです。
Initiator	イベントのイニシエータは、イベントの作成を最初に呼び出した認証済みのエンティティです。イニシエータは識別する必要がないことに注意してください。エンティティが識別できない場合は(その場合はおそらくエンティティがログインを試みて、オブザーバによるログインイベントの生成を引き起こしている可能性があります)、イベントの発生元に関する情報をできるだけ多く指定する必要があります。注: ログインイベントの特殊なケースでは、ログイン試行が成功するまで、イニシエータの認証された識別情報が判明しない場合があります。そのため、失敗したログインイベントがターゲットアカウントのIDをイニシエータのIDとして提供しないようにする必要があります。 イニシエータは、アカウントとエンティティ(以下参照)だけでなく、オプションのアサーションセットによっても記述されます。これらのアサーションでは、名前と値のペアのセットによって、イニシエータの識別情報の属性が記述されます。一部のイニシエータは、特定のアカウントから認識されず、アクターの権限を記述するアサーションのセット(SAML2など)から認識されます。アサーションは、クラスによって異なるうえ、個々のオブジェクトによっても異なる可能性があるため、これらのアサーションに対してはスキーマは定義されません。
アクション	アクションは記録されるイベントを識別します。このフィールドには、XDASイベント識別子だけでなく、結果コード(成功または失敗クラス)とイベントの発生時刻が、できるだけ正確に示されます。
イベント	eventフィールドは、XDASイベントにとって重要なフィールドです。イベントは、分類識別子と人が判読可能な短い記述名をカプセル化します。
ID	イベントIDコードは、XDAS標準のイベント分類で定義されたイベント識別子と、Novell CSS製品で定義された拡張子を表します。
名前	イベント名は、イベント識別子を表す、人が読んで理解できる名前です。イベント名はオプションですが、理解しやすいものにするために指定することが勧められています。
Data	イベントデータは、イベントに関する追加の記述的情報を提供します。
ログ	logフィールドには、標準のsyslogに似たログレベルの値が、SeverityとFacilityの数値識別子として格納されます。logフィールドと、logフィールド内のすべてのサブフィールドはオプションです。これらの値は、インスツルメンタの一部に対する判定を表すことが多いため、必要な場合以外は使用しないでください。このような判定は、イベントデータの収集後に、分析ソフトウェアやエンジニアに委ねることをお勧めします。
Outcome	結果コードの詳細については、639 ページの 「結果コード」を参照してください。

XDASフィールド	説明
時刻	イベント時刻は、イベントがイベントサービスにコミットされた時点で、オブザーバによって記録された時間です。時刻の値は、XDASクライアントヘルパーライブラリで収集されます。ヘルパーライブラリはできるだけ正確に時刻情報を生成することを試みるので、このフィールドに格納された値について懸念する理由はありません。
オフセット	offsetフィールドには、1970年1月1日午前0時(Linuxエポックとも呼ばれる)以降の秒数を表す値が格納されます。
シーケンス	sequenceフィールドには、あるイベントと、同じ秒内に記録された別のイベントを区別する固有の数値が格納されます。大抵の場合、この値は、0から始まり、次の秒境界に向かって単調に増加していく数値と見なすことができます。秒境界に達したところでまた0から再出発します。
トレランス	許容値は、0～100の値で、offsetで時間を記録するために使用されるクロックの許容誤差を表します。0の値は、クロックが極めて正確なことを表します。100の値は、クロックを信頼すべきではないことを表します。
Certainty	確実性の値は、0～100の値で、許容値の確実性をパーセンテージで表したものです。0は、許容値の確実性がないこと、つまり、正確さの点で少しも信頼できないことを意味します。100の値は、許容値が極めて正確であることを意味します。
ソース	タイムソースは、オブザーバシステムの時間のソースを示す情報です。これは、タイムサーバのURLにすることも、単にハードウェアクロックなどのローカルタイムソースにすることもできます。
ゾーン	タイムゾーンは、このクロックのタイムゾーンを表す新しいタイムゾーン文字列です。
Target (オプション)	イベントのターゲットは、イニシエータが処理しようとしてイベントの生成が誘発されるアカウントまたは保護されたリソースです。ターゲットは、アカウントとエンティティ(下記参照)だけでなく、オプションの不特定のデータオブジェクトによっても記述されます。データオブジェクトは、アクターのクラス固有の属性を表す名前と値のペアのセットです。スキーマでは実際のフィールドは定義されません。これは、クラスごとに固有なデータ属性のセット(もしあれば)が割り当てられるためです。
Observer	イベントのオブザーバは、システムを監視して、イニシエータのアクションに基づいてイベントを生成するエンティティ(サービス)の認証されたIDです。オブザーバは、アカウントとエンティティ(下記参照)によって記述されます。
Referenced Classes	observer、initiator、およびtargetの各フィールドには、スキーマ内で別々に定義されたアカウントクラスとエンティティクラスへの参照が格納されます。これ以外のクラスは、監査イベント内の3つのプライマリアクターのキー属性を識別します。
Account Class	アカウントクラスは、アクターのIDを表します。このIDは、認証レルムまたはドメインに関連します。アカウント名とアカウントIDの両方が提供されますが、実際に必要なのはIDだけです。名前は、人が理解できるようにするために提供されます。
Account Domain	アカウントドメインは、アクターの認証局を定義します。認証局がなければ、アカウント識別子にはほとんど意味がありません。
アカウント名	アカウント名はオプションです。これは、それが何かを人が理解するために役立ちます。

XDASフィールド	説明
アカウントID	アカウントIDは、認証ドメイン内のアカウントの固有の識別子です。
Entity Class	エンティティクラスは、アクターの場所を記述します。この場所は、システムアクセスエンドポイント(IPネットワーク)アドレスとシステムアクセスエンドポイント(ホスト/ドメイン)名によって定義されます。上記エンドポイントを管理するソフトウェア内のサービス名とコンポーネント名を記述するための別のフィールドも使用できます。
Entity SysAddr	ソフトウェアアクターのアクセスエンドポイントを記述したIPアドレスです。このIPアドレスは「IPアドレス:ポート」として表示されます。次に例を示します。 ◆ IPv4: 194.99.188.103:34564 ◆ IPv6: [2015::15]:43333 内部イベントIPアドレスは0.0.0.0:0として表示されることに注意してください。
Entity SysName	ソフトウェアアクターのアクセスエンドポイントを表すホスト/ドメイン名です。
Entity SvcName	上記エンドポイントを管理するサービスをさらに詳しく表すサービス名です。
Entity SvcComp	上記サービス内のコンポーネントを表すサービスコンポーネント名です。

結果コード

結果コードは、イベントコードによく似た階層数値です。結果コードは、成功または失敗クラスと理由を表します。成功階層は、0.x sub-arcでカプセル化されます。失敗クラスは、1.x階層で表現されます。拒否コードは、2.x階層で表現されます。

イベントの例

イベントの例を以下に示します。

```
Mar 16 21:46:40 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "164.99.179.142","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" : {"SysAddr" :
"164.99.179.142:43230"}},"Target" : {"Data" : {"ClassName" : "Tree Root","Name" :
"TREEUPGRADE","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.3.2","Name" :
"QUERY_DATA_ITEM_ATTRIBUTE","CorrelationID" : "eDirectory#5#","SubEvent" :
"DSE_LIST_PARTITIONS"},"Time" : {"Offset" : 1489681000},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

XDASイベント

XDASイベントについて詳しくは、881ページの付録H「eDirectoryイベントとXDASイベントのマッピング」 を参照してください。

XDASのトラブルシューティング

インストールと設定に関する問題のトラブルシューティングの詳細については、933 ページの「XDASのトラブルシューティング」を参照してください。

CEFによる監査

共通イベント形式(CEF)は、分散システムレベルで複数のコンポーネントからの監査情報をマージしたり分析したりする操作を容易にする標準のイベント形式です。CEF形式では、転送メカニズムとしてSyslogメッセージ形式が使用されます。

CEFは、テキストベースの拡張可能な形式で、オンプレミスのデバイスやクラウドベースのサービスなど、複数のデバイスタイプをサポートするよう設計されています。CEFイベントは、異なるアプリケーションの監査記録を理解しやすくするのに役立ちます。

CEFを使用するようにeDirectoryを設定すると、次のようなメリットがあります。

- セキュリティで保護された同一の監査サービスを分散システムに提供します。
- CEFでは、ログ管理を簡素化する標準メッセージ形式を使用します。
- 新しいイベントの形式は、Sentinelとシームレスに統合します。

注: eDirectory 9.1をIdentity Manager 4.7と併用する場合、CEFとXDASのどちらかの監査モジュールを有効にできます。Identity Managerを以前のバージョンから4.7にアップグレードする場合、eDirectoryでCEFを使用するにはXDAS監査モジュールを無効にします。

この次のセクションでは、eDirectoryでCEFを設定する方法について説明します。

- 640 ページの 「CEFの設定」

CEFの設定

eDirectoryインストールキットには、ダウンロードパッケージの一部としてLinux版とWindows版の両方のCEFクライアントが付属しています。eDirectoryのインストールプログラムは、オペレーティングシステム上にCEFパッケージをインストールします。CEFパッケージには、次のファイルが含まれています。

- Linux
  - novell-edirectory-xdaslog
  - novell-edirectory-xdaslog-conf
  - novell-edirectory-cefinstrument-9.2.0-0.x86_64.rpm
- Windows
  - cefauditds.dlm
  - xdaslog.dll

このセクションでは、次のトピックについて説明します。

- 641 ページの 「システム要件」
- 641 ページの 「CEF用のiManagerプラグインのインストール」
- 641 ページの 「CEFプロパティファイルの設定」
- 647 ページの 「監査用のCEFの設定」
- 649 ページの 「モジュールのロードとアンロード」
- 650 ページの 「CEFイベントキャッシングの有効化」

- 650 ページの 「CEFイベントタイプについて」
- 652 ページの 「CEFイベントのコレクタの使用」
- 653 ページの 「CEF監査イベントのフィルタ処理について」
- 654 ページの 「CEF実装スキーマ」
- 659 ページの 「CEFイベント」

システム要件

NetIQ Audit iManagerプラグインをインストールして使用するには、iManager 3.1以降が必要です。要件とダウンロード手順については、NetIQ iManagerの製品ページを参照してください。

CEF用のiManagerプラグインのインストール

CEF用のiManagerプラグインは、eDirectory 9.2プラグインにバンドルされています。または、NetIQダウンロードサイトからeDirectoryプラグインをダウンロードできます。

iManagerプラグインをインストールするには:

1 次のURLを使用して、Webブラウザからi Managerを開きます。

```
https://ip_address_or_DNS/nps/iManager.html
```

ここで、*ip_address_or_DNS*は、iManagerサーバのIPアドレスまたはDNS名を指しています。

次に例を示します。

```
http://111.111.1.1/nps/iManager.html
```

2 ユーザ名とパスワードを使用してiManagerにログインします。

NetIQ iManagerのすべての機能を利用するには、管理者としてツリーにログインします。管理者ユーザだけが、すべての機能への完全アクセス権を持っています。管理者ユーザ以外は、権利が割り当てられている役割にのみアクセスできます。

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

CEFプロパティファイルの設定

eDirectoryメディアでは、サンプルプロパティファイルであるauditlogconfig.properties.templateファイルがconfigdir (n4u.server.configdir)ディレクトリに格納されています。

表 23-1に、Linuxオペレーティングシステムと Windowsオペレーティングシステム上のauditlogconfig.propertiesファイルのデフォルトの場所を示します。

表 23-4 CEF環境設定ファイル

オペレーティングシステム	プロパティファイルの場所
Linux	`/etc/opt/novell/eDirectory/conf/auditlogconfig.properties` 非ルートインストールでは、CEFプロパティファイルがconfディレクトリに配置されます。
Windows	`<Install Path>/novell/nds/auditlogconfig.properties` 通常は、プロパティファイルはeDirectoryのインストールディレクトリに配置されます。

プロパティファイルを設定してから、環境をeDirectory 9.2から最新バージョンにアップグレードする場合、インストーラはプロパティファイルを置き換えません。代わりに、アップグレードプロセスがこのファイル(auditlogconfig.properties)を更新してカスタマイズ内容が保持されるようにします。

iManagerのインストール後、CEFを設定できます。CEF環境設定は、単純なテキストベースのauditlogconfig.properties環境設定ファイルに保存されます。実際の要件に応じてこのファイルをカスタマイズできます。

CEF auditlogconfig.propertiesファイルには次の情報が含まれています。

Linux

```
# Set the level of the root logger to DEBUG and attach appenders.
#log4j.rootLogger=debug, S, R

# Defines appender S to be a SyslogAppender.
#log4j.appender.S=org.apache.log4j.net.SyslogAppender

# Defines location of Syslog server.
#log4j.appender.S.Host=localhost
#log4j.appender.S.Port=port

# Specify protocol to be used (UDP/TCP/SSL)
#log4j.appender.S.Protocol=TCP

# Specify SSL certificate file for SSL connection.
# File path should be given with double backslash.
#log4j.appender.S.SSLCertFile=/etc/opt/novell/mycert.pem

# Minimum log-level allowed in syslog.
#log4j.appender.S.Threshold=INFO

# Defines the type of facility.
#log4j.appender.S.Facility=USER

# Defines caching for SyslogAppender.
# Inputs should be yes/no
#log4j.appender.S.CacheEnabled=no

# Cache location directory
# Directory should be available for creating cache files
#log4j.appender.S.CacheDir=/var/opt/novell/eDirectory
```

```
# Cache File Size
# Cache File Size should be in the range of 50MB to 4000MB
#log4j.appender.S.CacheMaxFileSize=500MB

# Layout definition for appender Syslog S.
#log4j.appender.S.layout=org.apache.log4j.PatternLayout
#log4j.appender.S.layout.ConversionPattern=%c: %m%n

# Defines appender R to be a Rolling File Appender.
#log4j.appender.R=org.apache.log4j.RollingFileAppender

# Log file for appender R.
#log4j.appender.R.File=/var/opt/novell/eDirectory/log/cef-events.log

# Max size of log file for appender R.
#log4j.appender.R.MaxFileSize=100MB

# Set the maximum number of backup files to keep for appender R.
# Max can be 13. If set to zero, then there will be no backup files.
#log4j.appender.R.MaxBackupIndex=10

# Layout definition for appender Rolling log file R.
#log4j.appender.R.layout=org.apache.log4j.PatternLayout
#log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c %m%n
```

Windows

```
# Brief description for appenders and their options are provided.
# For detailed decriptions refer to log4cxx documentation.

# Set the level of the root logger to DEBUG and attach appenders.
#log4j.rootLogger=debug, S, R

# Defines appender S to be a SyslogAppender.
#log4j.appender.S=org.apache.log4j.net.SyslogAppender

# Defines location of Syslog server.
#log4j.appender.S.Host=localhost
#log4j.appender.S.Port=port

# Specify protocol to be used (UDP/TCP/SSL).
#log4j.appender.S.Protocol=SSL

# Specify SSL certificate file for SSL connection.
# File path should be given with double backslash.
#log4j.appender.S.SSLCertFile=C:\\Novell\\mycert.pem

# Minimum log-level allowed in syslog.
#log4j.appender.S.Threshold=INFO

# Defines the type of facility.
#log4j.appender.S.Facility=USER

# Defines caching for SyslogAppender.
# Inputs should be yes/no
#log4j.appender.S.CacheEnabled=yes

# Cache location directory
# Directory should be available for creating cache files
#log4j.appender.S.CacheDir=C:\\NetIQ\\eDirectory
```

```
# Cache File Size
# Cache File size should be in the range of 50MB to 4000MB
#log4j.appender.S.CacheMaxFileSize=500MB

# Layout definition for appender Syslog S.
#log4j.appender.S.layout=org.apache.log4j.PatternLayout
#log4j.appender.S.layout.ConversionPattern=%c: %m%n

# Defines appender R to be a Rolling File Appender.
#log4j.appender.R=org.apache.log4j.RollingFileAppender

# Log file for appender R.
# File path should be given with double backslash.
#log4j.appender.R.File=C:\\cef-events.log

# Max size of log file for appender R.
#log4j.appender.R.MaxFileSize=100MB

# Set the maximum number of backup files to keep for appender R.
# Max can be 13. If set to zero, then there will be no backup files.
#log4j.appender.R.MaxBackupIndex=10

# Layout definition for appender Rolling log file R.
#log4j.appender.R.layout=org.apache.log4j.PatternLayout
#log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c %m%n
```

auditlogconfig.propertiesファイルの内容を検討する前に、以下の考慮事項を確認することをお勧めします。

- 文字のSとRは、それぞれSyslogアペンダとローリングファイルアペンダを意味します。
- エントリは大文字と小文字が区別されません。
- エントリは任意の順序で表示できます。
- ファイル内の空白行は有効です。
- ハッシュ(#)で始まるすべての行はコメントアウトされた行です。

次の表に、auditlogconfig.propertiesファイル内設定に関する情報を示します。

重要: 環境設定の変更後は、eDirectoryを再起動する必要があります。

設定	説明
log4j.rootLogger=**debug, S, R**	ルートのログの記録レベルをデバッグに設定して、RまたはSという名前のアペンダをアタッチします。SはSyslogアペンダを、Rはローリングファイルアペンダを意味します。
log4j.appender.S=**org.apache.log4j.net.SyslogAppender**	アペンダSをSyslogアペンダとして指定します。
log4j.appender.S.Host=**localhost**	CEFイベントの記録先のSyslogサーバの場所を指定します。 IFor example,log4j.appender.S.Host=192.168.0.1

設定	説明
log4j.appender.S.Port=**port**	CEFがSyslogサーバに接続するポートです。 このポートは1～65535の値をサポートします。無効な値が指定された場合は、ポートがデフォルトで514に設定します。 CEFとSyslogサーバ間の接続が失われた場合は、接続が回復するまでIdentity Managerはイベントを記録できません。
log4j.appender.S.Protocol=TCP	使用するプロトコルを指定します。たとえば、UDP、TCP、またはSSLなどです。
log4j.appender.S.SSLCertFile=**/etc/opt/novell/mycert.pem**	SSL接続用のSSL証明書ファイルを指定します。ファイルのパスを指定する場合は二重の円記号を使用します。この設定の指定は任意です。
log4j.appender.S.Threshold=**INFO**	Syslogアペンダで許可される最小ログレベルを指定します。現在は、INFOログレベルがサポートされています。
log4j.appender.S.Facility=**USER**	ファシリティのタイプを指定します。ファシリティは、メッセージを分類するために使用されます。現在、USERファシリティがサポートされています。これらの値は大文字または小文字で指定することができます。
log4j.appender.S.layout=**org.apache.log4j.PatternLayout**	Syslogアペンダ用のレイアウト設定です。
log4j.appender.S.layout.ConversionPattern=**%c : %p%m%n**	Syslogアペンダ用のレイアウト設定です。変換パターンとその説明については、「logging.apache.org」を参照してください。
log4j.appender.R=**org.apache.log4j.RollingFileAppender**	アペンダRをローリングファイルアペンダとして指定します。
log4j.appender.R.File=**/var/opt/novell/eDirectory/log/cef-events.log**	ローリングファイルアペンダ用のログファイルの場所です。
log4j.appender.R.MaxFileSize=**100MB**	ローリングファイルアペンダ用のログファイルの最大サイズ(MB単位)です。この値はクライアントで許可される最大サイズに設定します。
log4j.appender.R.MaxBackupIndex=**10**	ローリングファイルアペンダ用のバックアップファイルの最大数を指定します。バックアップファイルの最大数は10にすることができます。0の値はバックアップファイルなしを意味します。
log4j.appender.R.layout=**org.apache.log4j.PatternLayout**	ローリングファイルアペンダ用のレイアウト設定です。
log4j.appender.R.layout.ConversionPattern=**%d{MMM dd HH:mm:ss} %c : %p%m%n**	ローリングファイルアペンダ用のレイアウト設定です。簡易日付フォーマットパターンについては、表23-2を参照してください。 変換パターンとその説明については、「logging.apache.org」を参照してください。

表 23-2に、米国で解釈される日付と時刻のパターンの例を示します。指定されている日付と時刻は、米国太平洋タイムゾーンの2012年7月4日12時8分56秒です。

表 23-5 日付と時刻のパターンの例

日付と時刻のパターン	結果
"yyyy.MM.dd G 'at' HH:mm:ss z"	2012.07.04 AD at 12:08:56 PDT
"EEE, MMM d, "yy"	Wed, Jul 4, '01
"h:mm a"	12:08 PM
"hh 'o''clock' a, zzzz"	12 o'clock PM, Pacific Daylight Time
"K:mm a, z"	0:08 PM, PDT
"yyyyy.MMMMM.dd GGG hh:mm aaa"	02012.July.24 AD 12:08 PM
"EEE, d MMM yyyy HH:mm:ss Z"	Wed, 24 Jul 2012 12:08:56 -0700
"yyMMddHHmmssZ"	120724120856-0700
"yyyy-MM-dd'T'HH:mm:ss.SSSZ"	2012-07-04T12:08:56.235-0700

Syslogアペンダの有効化

Syslogアペンダを使用して、リアルタイムイベントを表示できます。加えて、Syslogサーバは災害発生時に優れたバックアップサポートを提供します。

Syslogアペンダを有効にするには、auditlogconfig.propertiesファイルに次の変更を加えます。

1. 次のエントリをSに変更して、Syslogアペンダをアタッチします。

   log4j.rootLogger=debug, S

2. 次のエントリをコメントアウトします。

   ```
   log4j.appender.S=org.apache.log4j.net.SyslogAppender
   log4j.appender.S.Host=localhost
   log4j.appender.S.Port=port
   log4j.appender.S.Protocol=SSL
   log4j.appender.S.SSLCertFile=/etc/opt/novell/mycert.pem
   #log4j.appender.S.Threshold=INFO
   #log4j.appender.S.Facility=USER
   #log4j.appender.S.layout=org.apache.log4j.PatternLayout
   #log4j.appender.S.layout.ConversionPattern=%c: %m%n
   ```

3. iManagerにログインして、ログイベントを変更します。CEFイベントの設定方法については、648 ページの 「監査するCEFイベントの設定」を参照してください。

注: SyslogAppenderに対してUDPプロトコルを使用するCEFキャッシングは機能しません。

Syslog SSL接続用の証明書の生成

Syslog接続用の証明書を生成するには:

1. 次のOpenSSLコマンドを使用して証明書を作成します。

   ```
   openssl s_client -host LOG_SERVER  -port 1443 -showcerts
   ```

2. /etc/opt/novell/eDirectory/conf/auditlogconfig.propertiesファイルで作成した証明書ファイルの場所を指定します。

ローリングファイルアペンダの有効化

監査ソリューションが個別のサーバに制限されている場合は、このファイルアペンダをお勧めします。ローリングファイルアペンダはローカルファイルシステムにイベントを格納し、イベントの損失を防止するため、syslogアペンダより信頼性が向上します。また、このソリューションは、セットアップするコンポーネントの数が少なく立ち上げが容易なため、デモンストレーションに向いています。

注: CEFにファイルコネクタを使用している場合は、ローリングファイルアペンダの変換パターンが、次のようなSyslogアペンダと同様であることを確認します。

```
log4j.appender.R.layout.ConversionPattern=%c: %m%n
```

ローリングファイルアペンダを有効にするには、auditlogconfig.propertiesファイルに次の変更を加えます。

1 次のエントリをRに変更して、ローリングファイルアペンダをアタッチします。

   log4j.rootLogger=debug, R

2 次のエントリをコメントアウトします。

   ```
   log4j.appender.R=org.apache.log4j.RollingFileAppender
   log4j.appender.R.File=/var/opt/novell/eDirectory/log/cef-events.log
   log4j.appender.R.MaxFileSize=100MB
   log4j.appender.R.MaxBackupIndex=10
   log4j.appender.R.layout=org.apache.log4j.PatternLayout
   log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c %m%n
   ```

3 iManagerから必要なイベントを選択します。

   CEFイベントの設定方法については、648 ページの 「監査するCEFイベントの設定」を参照してください。

監査用のCEFの設定

iManagerプラグインを使用したCEFの設定

1 次のURLを使用してWebブラウザからiManagerを開きます。

`https://ip_address_or_DNS/nps/iManager.html`

ここで、*ip_address_or_DNS*は、iManagerサーバのIPアドレスまたはDNS名を指しています。

次に例を示します。

`http://111.111.1.1/nps/iManager.html`

2 自分のユーザ名とパスワードを使用してログインします。

NetIQ iManagerのすべての機能を利用するには、管理者としてツリーにログインします。管理者ユーザだけが、すべての機能への完全アクセス権を持っています。管理者ユーザ以外は、権利が割り当てられている役割にのみアクセスできます。

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

3 ［**役割およびタスク**］>［**監査の環境設定**］を選択します。

4 ［**NCPサーバ**］にeDirectoryサーバの名前を指定してから、［**オブジェクトセレクタ**］アイコンをクリックしてeDirectoryサーバをブラウズします。

5 **OK**をクリックします。

［CEF監査］ページが表示されます。640 ページの 「CEFの設定」 に進みます。

監査するCEFイベントの設定

1 ユーザ名とパスワードを使用してiManagerにログインします。

2 ［**役割およびタスク**］>［**eDirectory監査**］>［**監査の環境設定**］を選択します。

3 ［**CEF**］タブを選択します。

4 CEFイベントを設定します。

- **Global:** 重複したエントリのグローバル設定を選択またはクリアすることができます。
  - **複製されたイベントを送信しない:** 他のサーバからの複製に起因する重複イベントの受信を停止する場合にこのオプションを選択します。
- **ログイベントの値:** イベントがテキストファイルに記録されます。サイズが768バイトを超えるイベントの値が「大きい値」と見なされます。どんなサイズのイベントでもログに記録できます。
  - **大きい値をログに記録:** このオプションは、サイズが768バイトを超えるイベントをログに記録する場合に選択します。
  - **大きい値をログに記録しない:** このオプションを選択して、サイズが768バイトより小さいイベントをログに記録します。
  - **属性値のログ記録:** 属性値を表示するにはこのオプションを選択します。これは、［**値の追加**］イベントと［**値の削除**］イベントにのみ適用されます。
  - **属性値をログに記録しない:** 属性値を抑止するにはこのオプションを選択します。これは、［**値の追加**］イベントと［**値の削除**］イベントにのみ適用されます。デフォルトでは、このオプションが選択されています。
  - **暗号化属性値のログ記録:** 暗号化された属性値を表示するにはこのオプションを選択します。これは、［**値の追加**］イベントと［**値の削除**］イベントにのみ適用されます。
  - **暗号化属性値をログに記録しない:** 暗号化された属性値を抑止するにはこのオプションを選択します。これは、［**値の追加**］イベントと［**値の削除**］イベントにのみ適用されます。デフォルトでは、このオプションが選択されています。

注: イベントサイズがこのサイズを超えている場合は、イベントの値が切り詰められてログファイルに保存されます。

- **基本イベント環境設定:** 環境に必要なイベントに基づいて、次のオプションの値を指定します。

注: デフォルトでは、［基本イベント環境設定］セクションの下に個々のイベントカテゴリが折りたたまれます。個々のイベントを選択するには、各カテゴリを展開できます。

オプション	説明
セキュリティイベント	イベントをログに記録するセキュリティイベントを選択します。メンバーの追加または削除、不正侵入者の検出、パスワード変更、ユーザの認証などのイベントをログに記録できます。
オブジェクトイベント	イベントをログに記録するオブジェクトイベントを選択します。オブジェクトの作成、削除、名前変更、移動、検索を行うイベントをログに記録できます。
属性イベント	イベントをログに記録する属性イベントを選択します。属性の読み込みと削除、属性値の追加、削除、比較を行うイベントをログに記録できます。
LDAPイベント	イベントをログに記録するLDAPイベントを選択します。

対応するCEFイベントにマッピングされたeDirectoryの内部イベントについては、917 ページの 「eDirectoryイベントとCEFイベントのマッピング」を参照してください。

注: イベント環境設定を変更してから、NCPサーバ上で設定変更が有効になるまで最大3分かかります。NCPサーバ上で設定変更をすぐに有効にするには、cefauditdsモジュールをアンロードしてからロードする必要があります。

モジュールのロードとアンロード

CEFイベントを設定したら、次のコマンドを実行して、CEFモジュールをロードまたはアンロードします。

ndsdサーバの起動時に自動的にcefauditdsモジュールをロードするには:

- **Linux**

  cefauditdsを/etc/opt/novell/eDirectory/conf/ndsmodules.confファイルに追加します。

- **Windows**

  ndscons.exeを実行して、使用可能なモジュールのリストから［cefauditds］を選択し、［**スタートアップ**］をクリックしてから、起動のタイプに［**自動**］を選択します。

cefauditdsモジュールを手動でロードまたはアンロードするには:

- **Linux**

  ロードするには、ndstrace -c "load cefauditds"を実行します。

  アンロードするには、ndstrace -c "unload cefauditds"を実行します。

- **Windows**

ロードするには、ndscons.exeを実行して、使用可能なモジュールのリストから［**cefauditds**］を選択し、［**開始**］をクリックします。

アンロードするには、ndscons.exeを実行して、使用可能なモジュールのリストから［**cefauditds**］を選択し、［**停止**］をクリックします。

CEFイベントキャッシングの有効化

eDirectory 9.2では、必要に応じて、CEFイベントをエージェントのSyslogアペンダキャッシュにローカルに保存することができます。イベントをキャッシュに保存することにより、エージェントが監査サーバと通信できない場合にも、生成された監査イベントが保持され、監査データが消失しないように守られます。エージェントコンピュータが監査サーバと再び通信できるようになると、エージェントは、キャッシュに保存されたイベントの再送信を試みます。

CEF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。イベントキャッシングを有効にするには、次の手順を実行します。

1. エージェントコンピュータで、CEFプロパティファイルの場所に移動します。auditlogconfig.propertiesファイルは、デフォルトで、/etc/opt/novell/eDirectory/conf/auditlogconfig.propertiesに配置されています。非ルートインストールでは、CEFプロパティファイルがデフォルトでconfディレクトリに配置されます。
2. テキストエディタを使用してauditlogconfig.propertiesファイルを開きます。
3. プロパティファイル内で、log4j.appender.S.CacheEnabledプロパティに移動して、このプロパティ値をyesに変更します。
4. (状況によって実行)特定のディレクトリでイベントをキャッシュに保存する場合は、そのディレクトリパスを指すようにlog4j.appender.S.CacheDirプロパティの値を変更します。ディレクトリを指定する場合は、そのディレクトリパスがサーバ上の有効な場所であることを確認します。log4j.appender.S.CacheDirプロパティが設定されていないと、Syslog Appenderによって、特定のインスタンスのdibディレクトリにキャッシュイベントのログが記録されます。
5. (状況によって実行)キャッシュのカスタムファイルサイズを指定する場合は、log4j.appender.S.CacheMaxFileSizeプロパティの値を変更します。デフォルト値は500MBです。最小値は50MBで、最大値は4GBです。
6. auditlogconfig.propertiesファイルを保存して閉じます。

CEFイベントタイプについて

イベントを次のカテゴリに記録するように、CEFを設定できます。

- セキュリティ
- オブジェクト
- 属性
- LDAP

次のデフォルトセットのイベントタイプを監査できます。

カテゴリ	イベントタイプ
セキュリティ	◆ ACLが変更されました ◆ メンバーの追加 ◆ メンバーの削除 ◆ 不正侵入者が検出されました ◆ ログインが無効化されました ◆ ログインが有効化されました ◆ ログイン ◆ 同等セキュリティの変更 ◆ 監査の環境設定 ◆ パスワードの変更 ◆ アカウントのロック解除 ◆ ログアウト ◆ 接続 ◆ なりすまし ◆ 認証 ◆ パスワードの確認 ◆ ログイン環境設定の変更 ◆ 資格情報の照会
オブジェクト	◆ オブジェクトの作成 ◆ オブジェクトの削除 ◆ オブジェクトのリネーム ◆ オブジェクトの移動 ◆ DSAの読み取り ◆ 検索
属性	◆ 属性の読み込み ◆ 属性の削除 ◆ 値の追加 ◆ 値の削除 ◆ 属性値の比較

カテゴリ	イベントタイプ
LDAP	◆ LDAPバインド ◆ LDAPレスポンスのバインド ◆ LDAPバインド解除 ◆ LDAP接続 ◆ LDAP検索 ◆ LDAP検索の応答 ◆ LDAP検索エントリの応答 ◆ LDAP追加 ◆ LDAP追加の応答 ◆ LDAP比較 ◆ LDAP比較の応答 ◆ LDAP変更 ◆ LDAPレスポンスの変更 ◆ LDAP削除 ◆ LDAPレスポンスの削除 ◆ LDAP DNの変更 ◆ LDAP DNレスポンスの変更 ◆ LDAP破棄 ◆ LDAP拡張操作 ◆ LDAPシステム拡張操作 ◆ LDAP拡張操作の応答 ◆ LDAPサーバの環境設定の変更 ◆ 不明なLDAP操作 ◆ LDAPパスワードの変更

CEFイベントのコレクタの使用

コレクタを使用してCEFイベントを収集する方法について詳しくは、Sentinel Plug-insページのeDirectoryコレクタ資料を参照してください。

CEF監査イベントのフィルタ処理について

CEFは、フィルタとイベント通知を使用して、特定のタイプのイベントが発生したとき、または、発生しなかったときにレポートを作成できます。1つまたは複数の固有オブジェクトクラスまたは属性のイベントを、イベントタイプに応じてフィルタ処理することもできます。CEFは、生成されたすべてのイベントをeDirectoryサーバで設定済みのフィルタに照らして評価し、それらのフィルタに一致するイベントのみをログに記録します。

このセクションでは、システムフィルタと通知の設定に必要な情報を提供します。

- 653 ページの 「CEFオブジェクトイベントのフィルタリング」
- 653 ページの 「CEF属性イベントのフィルタリング」
- 654 ページの 「除外フィルタを使用したeDirectoryイベントのフィルタリング」

CEFオブジェクトイベントのフィルタリング

オブジェクト用のフィルタリングを設定して、特定のイベントのみを検索することができます。たとえば、誰かがeDirectoryでユーザアカウントを作成したら通知が届くようにするには、新しいユーザオブジェクトの作成に関するイベントをログに記録するため、ユーザオブジェクトクラスを選択するフィルタを作成できます。

アカウントフィルタリングを設定するには、［オブジェクトイベント］リンクをクリックして、クラスを選択してから、［OK］をクリックしてアプリケーションを終了します。

アカウント管理イベントのフィルタを設定するには:

1. iManagerで、［役割およびタスク］>［eDirectoryの監査］>［監査の環境設定］に移動します。
2. 監視するNCPサーバを選択してから、［OK］をクリックします。
3. ［イベントオブジェクト］をクリックします。
   ［CEFオブジェクトフィルタリング］ウィンドウが表示されます。
4. ［使用可能なクラス］リストで、任意のオブジェクトクラスを選択して、右矢印をクリックして対象オブジェクトクラスを［選択されたクラス］リストに移動し、［OK］をクリックします。デフォルトでは、［コンピュータ］オブジェクトクラスが選択されます。

設定済みのフィルタを使用して、CEF監査モジュールはすべての選択済みオブジェクトクラスと属性に関して生成されたイベントすべてをチェックし、それらのイベントをログに記録します。

CEF属性イベントのフィルタリング

［属性イベント］リンクをクリックして、属性イベントのフィルタを設定します。たとえば、誰かがeDirectoryで新しい属性値を追加したら通知が届くようにするため、新しい値の追加に関するイベントをログに記録するフィルタを作成できます。

トラスト管理イベントのフィルタを設定するには:

1. iManagerで、［役割およびタスク］>［eDirectoryの監査］>［監査の環境設定］に移動します。
2. 監視するNCPサーバを選択してから、［OK］をクリックします。
3. ［イベント属性］をクリックします。
   ［属性フィルタリング］ウィンドウが表示されます。

4 ［使用可能なクラス］リストで、イベントを収集するオブジェクトクラスを選択し、右矢印をクリックしてそれらを［選択されたクラス］リストに移動します。デフォルトでは、［dynamicGroup］、［dynamicGroupAux］、［グループ］、［LDAPグループ］、［職種］オブジェクトクラスが選択されています。

5 ［使用可能な属性］リストで、選択したオブジェクトクラスの属性を任意の数だけ選択します。属性を選択し、右矢印をクリックしてその属性を選択された属性のリストに追加します。

注: オブジェクトクラスを選択すると、そのオブジェクトクラスのすべての属性の属性イベントすべてが選択されます。この場合は、選択したオブジェクトクラスのすべての属性に関するすべての属性イベントを取得することになります。

6 ［OK］をクリックします。

フィルタを設定すると、CEF監査モジュールはすべての選択済みオブジェクトクラスと属性に関して生成されたイベントすべてをチェックし、それらのイベントをログに記録します。

除外フィルタを使用したeDirectoryイベントのフィルタリング

［除外フィルタ］リンクをクリックして、イベントを生成する必要がないオブジェクトクラスと属性のためのフィルタを設定します。オブジェクトクラスと属性を選択できます。

不要なeDirectoryイベントのフィルタを設定するには:

1 iManagerで、［役割およびタスク］>［eDirectoryの監査］>［監査の環境設定］に移動します。

2 監視するNCPサーバを選択してから、［OK］をクリックします。

3 ［除外フィルタ］をクリックします。

［CEF除外フィルタリング］ウィンドウが表示されます。

4 ［使用可能なクラス］リストで、イベントを収集しないオブジェクトクラスを選択し、右矢印をクリックしてそれらを［選択されたクラス］リストに移動します。

5 ［使用可能な属性］リストで、任意の数の属性を選択します。属性を選択し、右矢印をクリックしてその属性を選択された属性のリストに追加します。

6 ［OK］をクリックします。

設定済みのフィルタを使用して、CEF監査モジュールは、すべての選択済みオブジェクトクラスと属性に関するイベントの生成を停止します。

CEF実装スキーマ

このドキュメントでは、CEFプロトコルを定義し、標準の実装方法の詳細を記します。ここでは、標準で使用されるヘッダと定義済みの拡張について説明します。

SyslogでのCEFの使用

CEFでは、syslogをトランスポートメカニズムとして使用します。次に示すように、syslogプレフィックス、ヘッダ、および拡張で構成される形式を使用します。

```
Jan 18 11:07:53 host CEF:Version|Device Vendor|Device Product|Device
Version|Device Event Class ID|Name|Severity|[Extension]
```

メッセージのCEF:Version部分は、必須のヘッダです。メッセージの残りの部分は、パイプ文字(「|」)で区切られたフィールドを使用してフォーマットします。残りのフィールドはすべて必要で、655 ページの 「CEFフィールドの定義」に従って定義しなければなりません。

メッセージの拡張部分は他のフィールドのプレースホルダで、必須ではありません。他のフィールドは、キーと値のペアとしてログに記録されます。詳細については、655 ページの 「CEFフィールドの定義」を参照してください。

CEFフィールドの定義

スキーマ内のこれらのフィールドは、CEF監査イベント用に定義されたフィールドです。これらのフィールドの一部または全部が他のタイプのイベントに関係している場合もありますが、監査サービスにはこの種の情報が不可欠です。

***表 23-6** CEF フィールドの定義*

CEFフィールド	説明
Device Product	Device Productは、送信元のデバイスを固有に識別する文字列です。2つの製品が、同じデバイス製品のペアを持つことはできません。管理者は、デバイス製品のペアごとに固有の名前を割り当てる必要があります。
Device Version	Device Versionは、送信元のデバイスを固有に識別する文字列です。2つの製品が、同じデバイスバージョンのペアを持つことはできません。管理者は、デバイスバージョンのペアごとに固有の名前を割り当てる必要があります。
Device Vendor	Device Vendorは、送信元のデバイスを固有に識別する文字列です。2つの製品が、同じデバイスベンダーのペアを持つことはできません。管理者は、デバイスベンダーのペアごとに固有の名前を割り当てる必要があります。
Device Event Class ID	Device Event Class IDは、イベントタイプごとの固有のIDです。文字列または整数を指定できます。デバイスイベントクラスIDは、報告されたイベントのタイプを識別します。侵入検知システム(IDS)では、特定の動作を検出する署名または規則ごとに固有のデバイスイベントクラスIDが割り当てられています。これは、他のタイプのデバイスの要件でもあり、イベントを処理するCorrelation Engine instancesでも役立ちます。署名IDとも呼ばれます。
Severity	イベントの重要度を示す、文字列または整数です。有効な文字列値は［**不明**］、［**低い**］、［**中**］、［**高い**］、［**非常に高い**］です。有効な整数値は0-3(低い)、4-6(中)、7-8(高い)、9-10(非常に高い)です。
Version	CEF形式のバージョンを示す整数です。イベントコンシューマは、この情報を使用して、その後に続くフィールドが表す内容を判別します。現在のCEFバージョンは0です。
Device Address	IPネットワーク内でイベントが参照するデバイスのアドレスを識別します。形式は、IPv4アドレスです。
c6a1	このディクショナリ内で適用されるフィールドが他にはない場合にフィールドをマップするために利用できる4つのIPV6アドレスフィールドの1つです。
dvchost	形式は、ノードが使用可能なときに、デバイスノードに関連付けられている完全修飾ドメイン名(FQDN)でなければなりません。たとえば、host.domain.comまたはhostです。
rt	アクティビティに関連するイベントの受信時刻です。形式は、MMM dd yyyy HH:mm:ssまたはエポック以降のミリ秒です。
dtz	イベントを生成するデバイスのタイムゾーン。
sourceServiceName	このイベントの生成を担当するサービス。
sproc	イベントのソースプロセスの名前。

CEFフィールド	説明
src	IPネットワーク内でイベントが参照するソースを識別します。形式は、IPv4アドレスです。たとえば、192.168.10.1。
spt	これは、ソースポート番号です。有効なポート番号は、0から65535です。
shost	IPネットワーク内でイベントが参照するソースを識別します。形式は、ノードが使用可能なときに、ソースノードに関連付けられている完全修飾ドメイン名(FQDN)でなければなりません。たとえば、host.domain.comまたはhost。
suser	名前でソースユーザを識別します。電子メールアドレスも、UserNameフィールドにマップされます。送信者は、sourceUserNameに配置される候補です。
dst	IPネットワークでイベントが参照するあて先アドレスを識別します。形式は、IPv4アドレスです。たとえば、192.168.10.1。
duser	名前で宛先ユーザを識別します。これは、イベントの宛先に関連付けられているユーザです。多くの場合、電子メールアドレスがUserNameフィールドにマップされます。受信者は、destinationUserNameに配置される候補です。
cn1	このディクショナリ内で適用されるフィールドが他にはない場合にフィールドをマップするために利用できる3つの数値フィールドの1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。deviceCustomNumber1とも呼ばれます。
cn2	このディクショナリ内で適用されるフィールドが他にはない場合にフィールドをマップするために利用できる3つの数値フィールドの1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。deviceCustomNumber2とも呼ばれます。
cn3	このディクショナリ内で適用されるフィールドが他にはない場合にフィールドをマップするために利用できる3つの数値フィールドの1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。deviceCustomNumber3とも呼ばれます。
cn1Label	すべてのカスタムフィールドには、フィールド自体を表すことができる対応するラベルフィールドがあります。各フィールドは、そのフィールドの目的を記述する文字列です。deviceCustomNumber1Labelとも呼ばれます。
cn2Label	すべてのカスタムフィールドには、フィールド自体を表すことができる対応するラベルフィールドがあります。各フィールドは、そのフィールドの目的を記述する文字列です。deviceCustomNumber2Labelとも呼ばれます。
cn3Label	すべてのカスタムフィールドには、フィールド自体を表すことができる対応するラベルフィールドがあります。各フィールドは、そのフィールドの目的を記述する文字列です。deviceCustomNumber3Labelとも呼ばれます。
cs1	このディクショナリ内で適用されるフィールドが他にはない場合にフィールドをマップするために利用できる6つの文字列の1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。deviceCustomString1とも呼ばれます。
cs2	このディクショナリ内で適用されるフィールドが他にはない場合にフィールドをマップするために利用できる6つの文字列の1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。deviceCustomString2とも呼ばれます。

CEFフィールド	説明
cs3	このディクショナリ内で適用されるフィールドが他にはない場合にフィールドをマップするために利用できる6つの文字列の1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。deviceCustomString3とも呼ばれます。
cs4	このディクショナリ内で適用されるフィールドが他にはない場合にフィールドをマップするために利用できる6つの文字列の1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。deviceCustomString4とも呼ばれます。
cs5	このディクショナリ内で適用されるフィールドが他にはない場合にフィールドをマップするために利用できる6つの文字列の1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。deviceCustomString5とも呼ばれます。
cs6	このディクショナリ内で適用されるフィールドが他にはない場合にフィールドをマップするために利用できる6つの文字列の1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。deviceCustomString6とも呼ばれます。
cs1Label	すべてのカスタムフィールドには、フィールド自体を表すことができる対応するラベルフィールドがあります。各フィールドは、そのフィールドの目的を記述する文字列です。deviceCustomString1Labelとも呼ばれます。
cs2Label	すべてのカスタムフィールドには、フィールド自体を表すことができる対応するラベルフィールドがあります。各フィールドは、そのフィールドの目的を記述する文字列です。deviceCustomString2Labelとも呼ばれます。
cs3Label	すべてのカスタムフィールドには、フィールド自体を表すことができる対応するラベルフィールドがあります。各フィールドは、そのフィールドの目的を記述する文字列です。deviceCustomString3Labelとも呼ばれます。
cs4Label	すべてのカスタムフィールドには、フィールド自体を表すことができる対応するラベルフィールドがあります。各フィールドは、そのフィールドの目的を記述する文字列です。deviceCustomString4Labelとも呼ばれます。
cs5Label	すべてのカスタムフィールドには、フィールド自体を表すことができる対応するラベルフィールドがあります。各フィールドは、そのフィールドの目的を記述する文字列です。deviceCustomString5Labelとも呼ばれます。
cs6Label	すべてのカスタムフィールドには、フィールド自体を表すことができる対応するラベルフィールドがあります。各フィールドは、そのフィールドの目的を記述する文字列です。deviceCustomString6Labelとも呼ばれます。
flexString1	このディクショナリ内で適用されるフィールドが他にはない場合に文字列データをマップするために利用できる2つの文字列フィールドの1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。通常これらのフィールドはお客様が使用するために予約されていて、必要がない限りベンダーが設定すべきではありません。
flexString2	このディクショナリ内で適用されるフィールドが他にはない場合に文字列データをマップするために利用できる2つの文字列フィールドの1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。通常これらのフィールドはお客様が使用するために予約されていて、必要がない限りベンダーが設定すべきではありません。

CEFフィールド	説明
flexString1Label	このディクショナリ内で適用されるフィールドが他にはない場合に文字列データをマップするために利用できる2つの文字列フィールドの1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。通常これらのフィールドはお客様が使用するために予約されていて、必要がない限りベンダーが設定すべきではありません。
flexString2Label	このディクショナリ内で適用されるフィールドが他にはない場合に文字列データをマップするために利用できる2つの文字列フィールドの1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。通常これらのフィールドはお客様が使用するために予約されていて、必要がない限りベンダーが設定すべきではありません。
flexNumber1	このディクショナリ内で適用されるフィールドが他にはない場合にLongデータをマップするために利用できる2つの数値フィールドの1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。通常これらのフィールドはお客様が使用するために予約されていて、必要がない限りベンダーが設定すべきではありません。
flexNumber2	このディクショナリ内で適用されるフィールドが他にはない場合にLongデータをマップするために利用できる2つの数値フィールドの1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。通常これらのフィールドはお客様が使用するために予約されていて、必要がない限りベンダーが設定すべきではありません。
flexNumber1Label	このディクショナリ内で適用されるフィールドが他にはない場合にLongデータをマップするために利用できる2つの数値フィールドの1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。通常これらのフィールドはお客様が使用するために予約されていて、必要がない限りベンダーが設定すべきではありません。
flexNumber2Label	このディクショナリ内で適用されるフィールドが他にはない場合にLongデータをマップするために利用できる2つの数値フィールドの1つです。控えめに使用し、可能な場合にはより具体的なディクショナリ提供フィールドを使用するようにします。通常これらのフィールドはお客様が使用するために予約されていて、必要がない限りベンダーが設定すべきではありません。
cat	元のデバイスが割り当てたカテゴリを表します。多くの場合、デバイスでは独自のカテゴリスキーマを使用してイベントを分類します。deviceEventCategoryとも呼ばれます。たとえば、/Monitor/Disk/Read。
reason	監査イベントが生成された理由。たとえば、不正なパスワードまたは不明ユーザ。エラーや、戻りコードのこともあります。
outcome	通常、成功または失敗などの結果を表示します。eventOutcomeとも呼ばれます。

イベントの例

イベントの例を以下に示します。

```
Oct 31 16:29:37 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B035D|AUTHENTICATE|1|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Oct 31 2017 16:29:37 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#DS
src=164.99.179.194 spt=0 suser=CN\=admin,OU\=novell,OU\=co,O\=in
duser=CN\=admin,OU\=novell,OU\=co,O\=in cs2Label=Class Name cs2=User cs3Label=Tree
Name cs3=TEST-CEF-AGN cs4Label=Correlation ID cs4=eDirectory#16# cs6Label=Server
Name cs6=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in flexString2Label=SubEvent
flexString2=DSE_AUTHENTICATE flexNumber2Label=Grouping flexNumber2=309
cat=Security reason=0 outcome=Success
```

CEFイベント

XDASイベントについて詳しくは、917 ページの付録 I「eDirectoryイベントとCEFイベントのマッピング」 を参照してください。

ジャーナルイベントのキャッシング

eDirectoryは、イベントコンシューマがイベントに登録して、それらのイベントが発生したらそれをコンシュームすることができるイベントシステムを備えています。イベントハンドラは、ワーカー、インライン、またはジャーナルとして登録することができます。ジャーナルイベントキューは、発生と同じ順序でイベントを報告することになっています。現在のジャーナルイベントシステムでは、ジャーナルイベントキューがメモリ内に保持されます。イベントのコンシューマが低速の場合やイベントの発生速度が処理速度を上回っている場合は、ジャーナルキューが増加し始めます。その結果、ndsdプロセスのメモリが増大します。

この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用することでイベントを1つのキュー内に保持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。

イベントが原因でメモリが増加する可能性があるのは、*ndstraceが有効*になっている場合か、*監査が有効*になっている場合です。メモリの増大は、イベントシステムキャッシングを有効にすることによって制御できます。

イベントシステムキャッシングの設定

イベントシステムキャッシングのための次の環境変数を設定する必要があります。

- NDSD_EVENT_DISK_CACHE

  この変数は、新しいイベントシステムの使用を制御します。デフォルトで、新しいイベントシステムは無効になっています。新しいイベントシステムを有効にするには、値を*true*または*1*にしてこの変数をエクスポートします。

- (オプション) NDSD_EVENT_DISK_CACHE_DIR

  この変数は、イベントファイルが作成される一時的な場所を指定します。指定されたディレクトリの下に、別のサブディレクトリcdir (存在しなければ)が作成されます。起動時に、このサブディレクトリ内のすべてのファイルがクリーンアップされます。キャッシングディレクトリは、別のディスクパーティション内に設定し、DIBと同じパーティション内には設定しないことをお勧めします。

Linuxでは、NDSD_EVENT_DISK_CACHE_DIRが指定されていない場合や指定されたディレクトリにアクセスできない場合、ndsdはvardirをキャッシングディレクトリとして使用します。デフォルトで、vardir の値は/var/opt/novell/eDirectory/data/です。

Windowsでは、この変数が指定されていない場合や指定されたディレクトリにアクセスできない場合、dhostはDIBFilesディレクトリを使用します。

注: キャッシングディレクトリで十分なディスク容量が使用できることを確認してください。ndsd/dhostは数GBのディスク容量をすぐに消費する可能性があります。

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。

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、NDS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す。アプリケーションにeDirectory LDAPサーバを監査するためのメカニズムを提供するために、eDirectoryにはLDAPイベントサブシステムが組み込まれています。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。

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。

その他の情報

LDAP監査イベントの詳細については、次のマニュアルを参照してください。

- 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。

24 eDirectoryの認証フレームワークについて

このセクションでは、NMASの概要を示します。NMASは、eDirectoryと一緒に自動的にインストールされます。サポートされているプラットフォームとインストール手順の詳細については、『*NetIQ eDirectoryインストールガイド*』を参照してください。

NMASの機能

NMASは、ネットワーク上の情報の保護を支援するように設計されています。パスワード管理ツールに加えて、NMASはNetIQ eDirectoryネットワークに対して認証する手段も兼ね備えています。これにより、ネットワークリソースにアクセスしている人物が本人かどうかを確認できます。

NMASは、認証デバイスに対するワークステーション上でのユーザのセッション中に3つの操作フェーズを使用します。それらのフェーズは次のとおりです。

1. ユーザ識別フェーズ (人物の特定)
2. 認証(ログイン)フェーズ (本人であることの証明)
3. デバイス取り外し検出フェーズ (接続の確認)

この3つの操作フェーズは完全に独立しています。認証デバイスは各フェーズで使用できますが、毎回同じデバイスを使用する必要はありません。

ユーザ識別フェーズ

これは、ユーザ名を収集するプロセスです。また、このフェーズでは、認証フェーズで使用されるツリー名、ユーザのコンテキスト、サーバ名、およびNMASシーケンスの名前も入力されます。この認証情報は、認証デバイスから取得することも、ユーザが手動で入力することもできます。

認証(ログイン)フェーズ

NMASは、**ログインファクタ**と呼ばれる、ネットワークにログインするための3種類のアプローチを使用します。このログインファクタは、ユーザがネットワークに対する認証に使用できる各種の項目または品質を表します。

- パスワード認証 (ユーザが知っていること)
- 物理デバイス認証 (ユーザが持っているもの)
- バイオメトリック認証 (ユーザそのもの)

ログインファクタの詳細については、666 ページの 「ログインメソッドとポストログインメソッドとシーケンス」を参照してください。

パスワード認証

パスワード(ユーザが知っていること)は、ネットワークに対する認証のための重要なメソッドです。NMASには、複数のパスワード認証オプションが用意されています。

- **NDSログインメソッド:** NDSパスワードは非可逆のハッシュ形式で保存され、NDSシステムだけがこのパスワードを使用できます。このオプションは、ユニバーサルパスワードが有効にされていて設定済みであればそれを使用します。
- **SCRAMログインメソッド:** SCRAM (Salted Challenge Response Authentication Mechanism)は、ユーザがeDirectoryサーバにログインしようとしたときに、パスワードのPBKDF2ハッシュを使用してユーザを認証します(RFC 5802)。詳細については、774 ページの 「非可逆パスワードストレージを理解する」を参照してください。

  注: eDirectory 9.2ツリーを新規作成する際に、SCRAMメソッドが自動的にインストールされます。旧バージョンのeDirectoryツリーを9.2にアップグレードする際には、SCRAMメソッドを手動でインストールする必要があります。詳細については、670 ページの 「ログインメソッドのインストール方法」を参照してください。

- **単純パスワード:** 単純パスワードを使用する場合、管理者は、外部のLDAPディレクトリからユーザとパスワード(平文とハッシュ済み)をインポートすることができます。このオプションは、ユニバーサルパスワードが有効にされていて設定済みであればそれを使用します。
- **Digest-MD5 SASL:** Digest-MD5 SASLは、LDAP SASLバインドに使用されるMD5アルゴリズムによってハッシュされたパスワードを検証するIETF標準のDIGEST-MD5 SASLメカニズムを提供します。このオプションは、ユニバーサルパスワードが有効にされていて設定済みであればそれを使用します。
- **チャレンジ/レスポンス方式:** チャレンジ/レスポンス方式は、ユーザが事前に設定された秘密の質問に1回以上回答することによって自分の身元を証明する方法です。

ユニバーサルパスワードは、各種のパスワードと認証のシステムの統合と管理を簡略化して1つの首尾一貫したネットワークを構築するための手段です。ユニバーサルパスワードの詳細については、771ページの第26章「パスワードを管理する」を参照してください。

物理デバイス認証

これまで、いくつかのタイプの物理デバイス(ユーザが持っているもの)向けのNMAS用認証モジュールが、NetIQとサードパーティの認証開発者により作成されてきました。

注: NMASでは、すべての物理デバイス認証メソッド(証明書付きスマートカード、ワンタイムパスワード(OTP)デバイス、近接型カードなど)を指す言葉として用いています。

- **スマートカード:** スマートカードは、クレジットカード大のプラスティックカード、または、データの保存や暗号化機能の実行が可能な組み込み型のプログラマブルマイクロチップを含むUSBデバイスです。NMASを使用すれば、eDirectoryに対する認証時にスマートカードで身元確認を行えます。

  NetIQは、スマートカードを使用するためのNetIQ Enhanced Smart Cardログインメソッドを提供しています。NetIQ Enhanced Smart Cardログインメソッドは、Identity Assurance Clientの一部として提供されます。詳細については、『*NetIQ Enhanced Smart Card Method 3.0 Installation and Administration Guide(NetIQ Enhanced Smart Card Method 3.0インストールおよび管理ガイド)*』を参照してください。
- **ワンタイムパスワード(OTP)デバイス:** OTPデバイスは、その所有者を認証するためのワンタイムパスワードを生成するハンドヘルドハードウェアデバイスです。
- **近接型カード:** 近接型カードは、ユーザが装着するカードです。この技術は、ユーザのワークステーションとカードの近接性に基づいてそのワークステーションをロック/ロック解除します。

  NetIQは、RFID近接型カードをサポートするpcProxログインメソッドを提供しています。pcProxログインメソッドは、NetIQ SecureLogin製品の一部として提供されます。詳細については、『*NMAS Login Method and Login ID Snap-In for pcProx (pcProx用のNMASログインメソッドおよびログインIDスナップイン)*』を参照してください。

バイオメトリック認証

*バイオメトリックス*は、人体の特徴(ユーザそのもの)を測定して統計的に解析するための科学技術です。バイオメトリック方式は、NMASで使用するためにサードパーティ企業から提供されます。

バイオメトリック認証には、リーダーまたはスキャニングデバイス、スキャンされた情報をデジタル形式に変換するソフトウェア、および、入力されたバイオメトリックデータと比較するバイオメトリックデータを保存するためのデータベースまたはディレクトリが必要です。

バイオメトリック入力の変換では、ソフトウェアが特定のデータのポイントを一致ポイントとして識別します。この一致ポイントがアルゴリズムを使用して処理され、ユーザがアクセス権を取得しようとするときにスキャンされるバイオメトリックデータと比較することができる値が作成されます。

バイオメトリック認証の例としては、指紋、網膜、虹彩、および顔の特徴のスキャンが挙げられます。バイオメトリックスにはさらに筆跡、タイピングパターン、音声認識なども含まれます。

デバイス取り外し検出フェーズ

ユーザセッションは、ログインの完了後にこのフェーズに入ります。次の2つのメソッドがあります。

- NetIQ SecureLoginで使用可能なSecure Workstationメソッド。ユーザセッションは、認証デバイス(スマートカードなど)を取り外すと終了できます。このデバイスは他のフェーズで使用する必要はありません。

Secure Workstationメソッドの詳細については、『*NetIQ SecureLogin 7.0 SP3 Administration Guide (NetIQ SecureLogin 7.0 SP3管理ガイド)*』を参照してください。

- NetIQ Enhanced Smart Cardログインメソッドも、スマートカード取り外し検出があります。NetIQ Enhanced Smart Cardログインメソッドの詳細については、『*NetIQ Enhanced Smart Card Method Installation Guide*』を参照してください。

ログインメソッドとポストログインメソッドとシーケンス

ログインメソッドは、ログインファクタの特定の実装です。NMASには、3つのログインファクタ(パスワード、物理デバイス、バイオメトリック認証)に基づく複数のログインメソッドの選択肢があります。

*ポストログインメソッド*は、ユーザがNetIQ eDirectoryに対して認証された後に実行されるセキュリティプロセスです。ポストログインメソッドの1つの例がNetIQ Secure Workstationメソッド(NetIQ SecureLoginで使用可能)です。このメソッドでは、ワークステーションのロック後にコンピュータにアクセスするためにユーザが資格情報を入力する必要があります。

NMASソフトウェアには、NetIQとサードパーティ認証開発者による複数のログインメソッドとポストログインメソッドのサポートが含まれます。ログインメソッドによっては、追加のハードウェアが必要な場合があります。詳細については、サードパーティ製品のマニュアルを参照してください。

メソッドを決定してインストールしたら、それを使用するために、ログインシーケンスに割り当てる必要があります。*ログインシーケンス*は、順序付けられた1つ以上のメソッドのセットです。ユーザは、これらの定義されたログインシーケンスを使用してネットワークにログインします。シーケンスに複数のログインメソッドが含まれる場合、それらのメソッドは指定された順序でユーザに提示されます。ログインメソッドが最初に提示され、その後にポストログインメソッドが提示されます。

NMASには、AndとOrの両方のログインシーケンスが存在します。Andログインシーケンスでは、シーケンス内のすべてのログインメソッドを正常に完了する必要があります。Orログインシーケンスでは、シーケンス内のいずれかのログインメソッドのみを正常に完了する必要があります。Orログインシーケンスの1つの例としては、ユーザが各種の認証デバイスで同じログインシーケンスを使用してワークステーションにログインできるようにしている場合が挙げられます。

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。

これを解決するために、セキュリティコンテナデータがローカルサーバ上のキャッシュに保存されます。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。

NMASソフトウェア

NMASは、NetIQ eDirectoryのバンドル製品として同梱されています。ソフトウェアイメージには以下が含まれます。

- NMASサーバソフトウェア
- ログインメソッドソフトウェア
- ログインシーケンスごとの複数のログインメソッドのサポート
- 段階的認証のサポート
- ユニバーサルパスワード

NMASクライアントソフトウェアは、NetIQ Client for WindowsとNetIQ SecureLoginで使用できます。

- 667 ページの 「サーバソフトウェアとクライアントソフトウェアのインストール」
- 668 ページの 「ログインメソッドソフトウェアとパートナー」
- 668 ページの 「ユニバーサルパスワード」
- 669 ページの 「iManagerの管理」

サーバソフトウェアとクライアントソフトウェアのインストール

NMASサーバ側ソフトウェアは、デフォルトで、eDirectoryと一緒にインストールされます。NMASクライアント側ソフトウェアは、NMASログインメソッドを使用してネットワークにアクセスするすべてのクライアントワークステーションにインストールする必要があります。インストール後は、iManagerを使用してNMASを管理できます。

現在、NMASクライアントソフトウェアはNetIQクライアントと一緒に出荷されています。詳細については、NetIQ Client for Windowsのマニュアルを参照してください。

インストール中に、NMASは、eDirectoryスキーマを拡張して、eDirectoryツリー内のセキュリティコンテナに新しいオブジェクトを作成します。これらの新しいオブジェクトとは、承認済みログインメソッドコンテナ、承認済みポストログインメソッドコンテナ、セキュリティポリシーオブジェクト、およびログインポリシーオブジェクトです。ログインメソッドはすべて承認済みログインメソッドコンテナに保存され、管理されます。ポストログインメソッドはすべて承認済みポストログインメソッドコンテナに保存され、管理されます。

ログインメソッドソフトウェアとパートナー

ソフトウェアとパートナー

現在サポートされているいくつかのログインメソッドが、NMASソフトウェアイメージ上に含まれています。

NMASソフトウェアには、サードパーティの認証開発者による複数のログインメソッドのサポートが含まれています。NetIQパートナーの一覧については、NetIQパートナーWebサイトを参照してください。

NMAS用のログインメソッドを開発しているパートナーは、それぞれ、ユニークな製品の機能と特性を活かしてネットワーク認証を解決しています。そのため、実際のセキュリティ特性はログインメソッドごとに異なります。

NetIQでは、これらのパートナー製品のセキュリティ手法を評価していません。したがって、これらの製品にNetIQ Yes、Tested & Approved、またはNetIQ Directory Enabledロゴの資格が与えられているとしても、それらのロゴは一般的な製品の相互運用性を示しているにすぎません。

自社のセキュリティニーズに最もよく合った製品を見極めるためにも、各パートナーの製品の機能を慎重に検討することをお勧めします。また、ログインメソッドによっては、NMAS製品に同梱されていないハードウェアやソフトウェアが別途必要な場合があることに注意してください。

ログインメソッドのインストール

NMASログインメソッド(サーバソフトウェア、プラグイン、およびスナップイン)は、以下を使用してインストールできます。

- nmasinst (すべてのeDirectoryプラットフォームで利用可能)。これを使用するにはeDirectoryをインストールする必要があります。
- iManagerプラグイン

ログインメソッドのインストール方法については、670 ページの 「ログインメソッドのインストール方法」を参照してください。

ユニバーサルパスワード

ユニバーサルパスワードは、各種のパスワードと認証のシステムの統合と管理を簡略化して1つの首尾一貫したネットワークを構築するための手段です。これを使用すると、eDirectoryへのすべてのアクセスに対して1つのパスワードが提供され、パスワードでの拡張文字の使用、詳細パスワードポリシーの適用、およびeDirectoryから他のシステムへのパスワードの同期が可能となります。

ユニバーサルパスワードの詳細については、771ページの第26章「パスワードを管理する」を参照してください。

iManagerの管理

iManagerを使用してNMASを管理することができます。NetIQ iManagerは、eDirectoryを管理するためのWebベースのユーティリティです。iManager内の特定のプロパティページで、ログインメソッド、ログインシーケンス、登録、および段階的認証を管理できます。

デフォルトで、NMASは標準のNDSパスワードログインメソッドをインストールします。追加のログインメソッドは、iManagerを使用して、また、新しいオブジェクトの作成オプションを通して承認済みログインメソッドコンテナから起動されるウィザードを使用してインストールできます。ポストログインメソッドは、新しいオブジェクトの作成オプションを通して承認済みポストログインメソッドコンテナから起動されるウィザードを使用してインストールできます。

ログインメソッドのインストール方法については、670 ページの 「ログインメソッドのインストール方法」を参照してください。

ログインとポストログインのメソッドとシーケンスの管理

このセクションでは、NMAS用のログインとポストログインのメソッドとシーケンスのインストール、セットアップ、および設定方法について説明します。

NMASには、3つのログインファクタ(パスワード、物理デバイス、バイオメトリック認証)に基づく複数のログインメソッドの選択肢があります。

NMASには、NetIQとサードパーティ認証開発者による複数のログインメソッドとポストログインメソッドのサポートが含まれます。メソッドによっては、追加のハードウェアやソフトウェアが必要な場合があります。使用するメソッドに必要なすべてのハードウェアとソフトウェアが揃っていることを確認してください。

NMASでは、ソフトウェアビルド内にいくつかのログインメソッドが同梱されています。その他のログインメソッドはサードパーティベンダから入手できます。

eDirectoryパートナーの一覧については、NetIQパートナーWebサイトを参照してください。いくつかのパートナーがサードパーティログインメソッドを開発しています。

ログインメソッドのインストール方法

NetIQ eDirectoryで使用するログインメソッドのインストール方法は3種類あります。

- nmasinstユーティリティ(LinuxとWindows)。eDirectoryにログインメソッドをインストールすることができます。
- NetIQ iManager (LinuxとWindows)。eDirectoryにログインメソッドとポストログインメソッドをインストールすることができます。
- 670 ページの 「nmasinstユーティリティを使用したログインメソッドのインストール」
- 670 ページの 「NetIQ iManagerを使用したログインメソッドまたはポストログインメソッドのインストール」

nmasinstユーティリティを使用したログインメソッドのインストール

サーバコンソールのコマンドラインから次のように入力します。

nmasinst -addmethod admin.context treename config.txt_path [-h hostname[:port]] [-w password|file:<filename>|env:<environment_variable>] [-checkversion] [-d]

- *admin.context*: 管理者の名前とコンテキスト。
- *treename*: ログインメソッドをインストールするeDirectoryツリーの名前。
- *config.txt_ path* - ログインメソッドのconfig.txtファイルへの完全パスまたは相対パス。config.txtファイルは各ログインメソッドに付属しています。
- [-h *hostname*[:*port*]]: (オプション)サーバのホスト名とポート。eDirectoryがデフォルトポートで実行していない場合に使用します。IPアドレスを指定することもできます。eDirectory 9.2ではIPv4アドレスとIPv6アドレスの両方がサポートされています。次に例を示します。
  - **IPv4:** -h 127.0.0.1:8443
  - **IPv6:** -h [2001:db8::6]:8443
- [-w *password*|file:<*filename*>|env:<*environment_variable*>]: このオプションを使用すれば、次の方法のいずれかを使用してパスワードを指定することができます。
  - コマンドラインから。例: -w n
  - ファイルを通して。例: -w file:/tmp/passwd
  - 環境変数を通して。例: -w env:PASSWD
- ［-checkversion］: このオプションは、インストールするメソッドバージョンがインストール済みのメソッドバージョンと同じかそれよりも新しい場合にエラーを報告します。
- ［-d］: サポートされていないプラットフォーム用のメソッドを削除します。

ログインメソッドがすでに存在した場合は、nmasinstがそれを更新します。

NetIQ iManagerを使用したログインメソッドまたはポストログインメソッドのインストール

1. NetIQ iManagerを起動します。
2. 管理者または管理権限を持つユーザとして、eDirectoryツリーに対する認証を受けます。
3. ［**役割およびタスク**］メニューで、［**NMAS**］>［**NMASログインメソッド**］の順にクリックします。

4 ［新規作成］をクリックします。

5 インストールするログインメソッド(.zip)ファイルをブラウズして選択してから、［次へ］をクリックします。

6 インストールウィザードに従って完了します。

ログインメソッドとポストログインメソッドの更新

ログインメソッドベンダがログインメソッドまたはポストログインメソッドの更新を提供にしている場合は、次の手順を実行してメソッドを更新することができます。

- 671 ページの 「nmasinstユーティリティを使用したログインメソッドの更新」
- 671 ページの 「iManagerを使用したログインメソッドの更新」

nmasinstユーティリティを使用したログインメソッドの更新

nmasinstユーティリティを使用してログインメソッドをインストールする手順と同じ手順を使用します(671 ページの 「nmasinstユーティリティを使用したログインメソッドの更新」を参照)。新しいconfig.txtファイルへのパスを追加すると、ログインメソッドが更新されます。

iManagerを使用したログインメソッドの更新

1 iManagerを起動します。

2 管理者または管理権限を持つユーザとして、eDirectoryツリーに対する認証を受けます。

3 ［役割およびタスク］メニューで、［NMAS］>［NMASログインメソッド］の順にクリックします。

4 更新するログインメソッドをクリックします。

5 ログインメソッドのプロパティページで、［Update Method］をクリックします。

6 更新ウィザードに従って完了します。

ログインシーケンスの管理

ログインをインストールするときに、インストールするログインメソッドのみを使用するログインシーケンスを作成するかどうかが尋ねられます。［はい］を選択すると、1つのログインメソッドだけを含むログインシーケンスが作成されます。

ログインシーケンスは手動で作成して管理することもできます。ログインメソッドとポストログインメソッドをインストールしたら、iManagerを使用してログインシーケンスを表示、追加、変更、または削除することができます。メソッドが変更または更新されても、ログインシーケンスは作成されません。

NMASでは、シーケンスごとに複数のログインメソッドとポストログインメソッドをセットアップすることができます。ポストログインメソッドを選択するためには、1つ以上のログインメソッドを選択しておく必要があります。

1つのシーケンスに対して複数のメソッドが選択されている場合は、それらが表示順に実行されます。ログインメソッドが先に実行され、その後でポストログインメソッドが実行されます。

ログインシーケンスは、ANDシーケンスまたはORシーケンスにすることができます。ANDシーケンスは、すべてのログインメソッドによってユーザのIDが正常に検証された場合に成功します。ORシーケンスの場合は、いずれかのログインメソッドによってユーザのIDが検証されれば、ログインが成功します。

ポストログインメソッドは、And/Or関係とは無関係に、ログインが成功した場合にのみ実行されます。

シーケンスを作成したら、その新しいシーケンスを使用したeDirectoryへのログインをユーザに許可することができます。

- 672 ページの 「NetIQ iManagerを使用した新しいログインシーケンスの作成」
- 672 ページの 「ログインシーケンスの変更」
- 673 ページの 「ログインシーケンスの削除」

NetIQ iManagerを使用した新しいログインシーケンスの作成

1. iManagerを起動します。
2. 管理者または管理権限を持つユーザとして、eDirectoryツリーに対する認証を受けます。
3. ［**役割およびタスク**］メニューで、［**NMAS**］>［**NMAS Login Sequences**］の順にクリックします。
4. ［**新規**］をクリックして、新しいログインシーケンスの名前を指定します。

   すべての使用可能なメソッドが、［**Available Login Methods**］と［**Available Post-Login Methods**］の下に一覧表示されます。
5. ドロップダウンリストから［**Sequence Type**］を選択します。

   ［*And*］を選択する場合、ユーザは、ログインシーケンスに含まれるすべてのログインメソッドを使用してログインする必要があります。［*Or*］を選択する場合、ユーザは、ログインシーケンスに含まれるログインメソッドのいずれか1つを使用するだけでログインできます。
6. 水平矢印を使用して必要なそれぞれのメソッドをシーケンスに追加します。

   複数のメソッドを使用する場合、実行順序を変更するには垂直矢印を使用します。

   ［**Sequence Grade**］フィールドに、ログインシーケンスのグレードが表示されます。Andシーケンスの場合、シーケンスグレードは、一連のログインメソッドのグレードの和集合になります。Orシーケンスの場合、シーケンスグレードは、一連のメソッドのグレードの共通部分になります。
7. ［**完了**］をクリックしてログインシーケンスを保存します。

ログインシーケンスの変更

1. iManagerを起動します。
2. 管理者または管理権限を持つユーザとして、eDirectoryツリーに対する認証を受けます。
3. ［**役割およびタスク**］メニューで、［**NMAS**］>［**NMAS Login Sequences**］の順にクリックします。
4. ログインシーケンス名をクリックします。

   シーケンスグレードとシーケンスタイプが表示され、ログインメソッドとポストログインメソッドが一覧表示されます。使用可能なすべてのメソッドが、［**Available Login Methods**］リストと［**Available Post-Login Methods**］リストに表示されます。

5 アクションの選択

- シーケンスタイプを変更するには、シーケンスタイプの横にあるドロップダウンリストを使用します。
- ログインメソッドまたはポストログインメソッドをシーケンスに追加したりシーケンスから削除したりするには、左矢印と右矢印を使用します。

注: ポストログインメソッドを選択するためには、1つ以上のログインメソッドを選択しておく必要があります。

- ログインメソッドのシーケンス順序を変更するには、上矢印と下矢印を使用します。
- 変更を保存せずに終了するには、［キャンセル］をクリックします。

重要: 関連付けられたメソッドが存在しないログインシーケンスは保存されません。

6 適用またはOKをクリックします。

ログインシーケンスの削除

1 iManagerを起動します。

2 管理者または管理権限を持つユーザとして、eDirectoryツリーに対する認証を受けます。

3 ［役割およびタスク］メニューで、［NMAS］>［NMAS Login Sequences］の順にクリックします。

4 削除するログインシーケンスを選択して、［削除］をクリックします。

5 適用またはOKをクリックします。

ユーザに対するログインシーケンスの承認

- 673 ページの 「ログインシーケンスの割り当て」
- 674 ページの 「ログインシーケンスの承認」

ログインシーケンスの割り当て

承認済みログインシーケンスとデフォルトログインシーケンスを、ユーザ、コンテナ、パーティションルート、またはログインポリシーオブジェクトに割り当てることができます。NMASは、ユーザオブジェクト、ユーザオブジェクトのコンテナ、ユーザオブジェクトのパーティションルート、およびログインポリシーオブジェクトの順にそれらの属性を読み込むことによって、ユーザの承認済みログインシーケンスまたはデフォルトログインシーケンスを検索します。

ユーザオブジェクトで見つかった属性は、コンテナ、パーティションルート、またはログインポリシーオブジェクトで見つかった属性よりも優先されます。ログインシーケンスがパーティションルートに割り当てられている場合は、そのログインシーケンスがそのパーティションルートの下のすべてのユーザに適用されます。ただしそれは、特定のユーザに個別にログインシーケンスが割り当てられていない場合に限られます。

また、コンテナに割り当てられたログインシーケンスは、そのコンテナ内のシーケンスが割り当てられていないユーザにのみ適用され、そのコンテナのサブコンテナ内のユーザには適用されません。

ログインシーケンスの承認

1 iManagerを起動します。

2 管理者または管理権限を持つユーザとして、eDirectoryツリーに対する認証を受けます。

3 ［役割およびタスク］メニューで、［NMAS］>［NMAS Users］の順にクリックして、ログインシーケンスを承認するユーザを選択してから、［NMAS］タブをクリックします。

4 ログインシーケンスを選択して［Authorize］または［De-authorize］をクリックすることによって、ユーザに対してログインシーケンスを承認または承認解除します。

5 適用またはOKをクリックします。

デフォルトログインシーケンスの設定

ユーザがログイン時にログインシーケンスを指定する必要がないようにデフォルトログインシーケンスを設定するには:

1 iManagerを起動します。

2 管理者または管理権限を持つユーザとして、eDirectoryツリーに対する認証を受けます。

3 ［役割およびタスク］メニューで、［NMAS］>［NMAS Users］の順にクリックして、デフォルトログインシーケンスを設定するユーザを選択してから、［NMAS］タブをクリックします。

4 承認済みログインシーケンスを選択してから、［Make Default］をクリックします。

選択したシーケンスがデフォルトログインシーケンスになります。ユーザがログインシーケンスを使用せずにログインしようとすると、このデフォルトログインシーケンスが使用されます。

5 適用またはOKをクリックします。

注: ワークステーションがユーザのデフォルトログインシーケンスを実行できない場合は、NDSパスワードログインメソッドが使用されます。

ログインシーケンスの割り当て方法については、673 ページの 「ログインシーケンスの割り当て」を参照してください。

ログインメソッドの削除

NMAS Managerプラグインでは、ログインシーケンスの一部になっているログインメソッドを削除できません。ログインメソッドのデフォルトインストールでは、そのメソッドのみを含むログインシーケンスが作成されます。その結果、ほとんどのメソッドが1つ以上のシーケンスに組み込まれます。

注: nmasinstには、NMASメソッドを削除するオプションがありません。これはiManagerを使用して行う必要があります。

ログインメソッドを削除するには、次の2つの手順を実行する必要があります。

- 675 ページの 「すべてのログインシーケンスからログインメソッドを削除する」
- 675 ページの 「ログインメソッドを削除する」

すべてのログインシーケンスからログインメソッドを削除する

iManagerを使用して任意のログインシーケンスのログインメソッドを削除するには:

1 iManagerで、［NMAS］>［NMAS Login Sequences］の順にクリックします。

2 ［NMAS Login Sequences］リスト内のシーケンスごとに、次の手順を実行します。

2a シーケンス名をクリックします。

2b 削除するログインメソッドが［ログインメソッド］リストにも［Post-LoginMethods］リストにも列挙されていないことを確認します。

2c 対象のログインメソッドが、選択されたメソッドの1つとして列挙されている場合は、それを選択して左矢印をクリックすることによってリストから移動することができます。

すべてのログインシーケンスからログインメソッドを削除したら、そのメソッドを削除することができます。詳細については、675 ページの 「ログインメソッドを削除する」を参照してください。

ログインメソッドを削除する

iManagerを使用してログインメソッドを削除するには:

1 iManagerで、［NMAS］>［NMAS Login Methods］の順にクリックします。

2 削除するログインメソッドを選択します(複数選択可)。

3 ［削除］をクリックして、［はい］をクリックします。

ログインシーケンスの削除

1 NetIQ iManagerを起動します。

2 管理者または管理権限を持つユーザとして、eDirectoryツリーに対する認証を受けます。

3 ［役割およびタスク］メニューで、［NMAS］>［NMAS Login Sequences］の順にクリックします。

4 削除するログインシーケンスを選択します。

5 ［削除］をクリックして、［はい］をクリックします。

NMASを使用したネットワークへのログイン

NMASをインストールしたら、ユーザがネットワークにログインする準備が整ったことになります。このセクションでは、ネットワークユーザに周知しておく必要があるログインエクスペリエンスの一部の追加機能について説明します。

- 676 ページの 「パスワードフィールド」
- 676 ページの 「カスタムログイン」
- 677 ページの 「ワークステーションのロック解除」
- 677 ページの 「NMASクライアントトレースの収集」
- 677 ページの 「NMASクリアランスステータスの表示」

パスワードフィールド

NMASクライアントソフトウェアのインストール方法に応じて、Novell Clientのログインダイアログボックスにパスワードフィールドが表示される場合と表示されない場合があります。ユーザがバイオメトリックまたは物理デバイス()ログインファクタを使用している場合は、ネットワークにログインするためのパスワードが不要な場合があります。

パスワードフィールドの非表示に関する詳細については、Novell Client For Windowsのマニュアルを参照してください。

カスタムログイン

NMASログインメソッドを使用してネットワークにログインしているユーザは、必要なクリアランスとログインシーケンスを選択することによって、ログインをカスタマイズすることができます。そうしない場合は、最後のログインシーケンスとクリアランス(もしあれば)が使用されます。クリアランスまたはログインシーケンスが事前に指定されていない場合は、デフォルトが使用されます。

1. Novell Clientのダイアログボックスが表示されたら、［**詳細**］をクリックします。
2. ［**NMAS**］タブをクリックします。
3. ［**ログイン**］ドロップダウンリストから必要なログインシーケンスを選択するか、NetIQ eDirectoryツリーで最新の完全なリストをブラウズします。

   ブラウズできるのは、［**eDirectory**］タブでeDirectoryツリーが指定されている場合だけです。
4. 必要なユーザセッションクリアランスを指定するか、eDirectoryツリーで最新の完全なリストをブラウズします。

   デフォルトで、［**クリアランス**］フィールドは無効になっています。［**クリアランス**］フィールドを有効にするには:

   4a タスクバーで赤色のNを右クリックします。

   4b ［**Novell Client Properties**］>［**Location Profiles**］の順にクリックします。

   4c 必要なプロファイルを選択して、［**プロパティ**］をクリックしてから、［**プロパティ**］をクリックします。

   4d ［**NMAS**］タブで、［**Display Clearance Field**］を選択します。

   4e ［**OK**］を3回クリックします。

   重要: ユーザには、ログインシーケンスごとに複数のセッションクリアランスを割り当てることができます。［**クリアランス**］フィールドに、必要なユーザセッションクリアランスが入力されていることを確認します。

   ---
5. **OK**をクリックします。

ワークステーションのロック解除

ユーザのワークステーションにNMASを追加すると、Windowsワークステーションをロック解除するプロセスが変更されます。通常、ユーザはWindowsの［ディスプレイ］コントロール パネルで設定するスクリーンセーバを使用して各自のワークステーションのパスワード保護を有効にできます。NMASを使用してワークステーションをロック解除するには、ユーザが代わりに最初のログインに使用したのと同じ認証プロセスを通過する必要があります。

たとえば、NMASを使用してネットワークに対する認証を受けてバイオメトリックログインメソッドを使用した場合、ワークステーションのロックを解除して使用するには、再度同じバイオメトリックログインメソッドを使用する必要があります。

Windowsワークステーションを使用している場合は、ツリーへのログインに使用したログインメソッドを使用してワークステーションをロック解除する必要があります。複数のeDirectoryツリーに接続している場合は、いずれかのeDirectoryツリー用のログインシーケンスを使用できます。デフォルトは最初のeDirectoryツリーです。

NMASクライアントトレースの収集

NMASクライアントトレースを収集すれば、NMAS認証の問題のトラブルシューティングに役立ちます。詳細については、「TID # 3331372」を参照してください。

NMASクリアランスステータスの表示

1. タスクバーで赤色のNを右クリックします。
2. ［**Novell Connections**］をクリックします。
3. スクロールオーバーすると、各接続に関連付けられたNMASクリアランスが表示されます。

NetIQパスワードの履歴

これまでは、パスワードの制約事項のために、管理者は複数のパスワード(単純パスワード、NDSパスワード、拡張パスワード)を管理する必要がありました。さらに、複数のパスワードを同期させる必要もありました。

- NDSパスワード:古いNDSパスワードは非可逆のハッシュ形式で保存されます。このパスワードはNDSシステム専用であり、他の任意のシステムで使える別のフォームに変換することはできません。
- 単純パスワード: 単純パスワードは、元々、管理者がActive Directory*やiPlanet*などの外部のLDAPディレクトリからユーザとパスワード(平文とハッシュ済み)をインポートできるようにするために実装されたものです。

  シンプルパスワードの制約は、パスワードポリシー(最小長、満了日など)がいっさい施行されないことです。
- 拡張パスワード: ユニバーサルパスワードの前身である拡張パスワード(現在は未サポート)は、一部のパスワードポリシーを提供しますが、その設計には他のパスワードとの一貫性がありません。このパスワードは、片方向同期を提供し、単純パスワードやNDSパスワードに取って代わるパスワードです。

これらのパスワードの問題を解決するためにユニバーサルパスワードが作成されました。このパスワードには次のような特徴があります。

- 1つのパスワードによるeDirectoryへのアクセス.
- パスワード内で拡張文字を使用することができます。
- 詳細なパスワードポリシーを適用できます。
- eDirectoryから他のシステムへパスワードを同期できます。

ユニバーサルパスワードは、NMASモジュールのコンポーネントであるSecurePasswordManagerによって管理されます。Secure Password Managerは、NetIQ、Novell、およびNetIQパートナーのさまざまな製品におけるパスワードベースの認証スキーマの管理を簡略化します。この管理ツールは、1つのパスワードのみを表示し、下位互換性を維持するためのすべてのバックグラウンドの処理は表示しません。

SecurePasswordManagerとユニバーサルパスワードを管理または利用する他のコンポーネントは、eDirectoryインストールの一部としてインストールされます。ただし、ユニバーサルパスワードはデフォルトで有効になっていません。認証とパスワード設定用のすべてのAPIがユニバーサルパスワードをサポートするように移行されるので、既存のすべての管理ツールは、これらの新しいライブラリを備えたクライアント上で実行すると、自動的にユニバーサルパスワードと連動します。

注: パスワード管理プラグインは、ダウンロードWebサイトからダウンロードできます。

Novell Clientはユニバーサルパスワードをサポートします。また、ネットワーク内の既存システムのために、引き続きNDSパスワードもサポートしています。Novell Clientは、最初のログイン時に自動的にNDSパスワードをユニバーサルパスワードに移行する機能を備えています。

「既存のパスワードがパスワードポリシーに準拠しているかどうかを確認する(ログイン時に検証が実行される)」パスワードポリシールールがtrueに設定されていない場合は、NDSパスワードがユニバーサルパスワードに移行されるときにパスワード期限の時刻が更新されません。

ユニバーサルパスワードの展開と管理に関する詳細については、771ページの第26章「パスワードを管理する」を参照してください。

NMAS HOTPベースのログイン

次の各セクションでは、NMAS HOTPに関する情報を提供します。

概要

HOTPは、HMACベースのワンタイムパスワード(OTP)アルゴリズムです。OTPは、1回のログインセッションまたはトランザクションでのみ有効なパスワードです。OTPに関連したセキュリティ攻撃の発生リスクは比較的小さいので、OTPは従来の(静的な)パスワードよりも優れたパフォーマンスを提供します。不正侵入者が、サービスへのログインやトランザクションの実行に使用されたOTPを記録したとしても、そのOTPはすでに1回使用されていて有効ではなくなっているので、そのOTPを使用することはできません。すべてのOTPベースの認証には、OTPサーバとOTPクライアント(ハードウェア/ソフトウェア)が必要です。NMASのOTPベースの認証の実装は、RFC 4226標準に基づきます。これまで個別にサーバに提示されていたNDSパスワードが、OTPに付加されるようになり、すべてのクライアントコンポーネントとそのユーザインタフェースを維持したままでパスワードベースの認証が拡張されました。eDirectoryサーバに対する認証は、LDAPベースのログインを使用することによって、HOTP機能を通して実行されます。

LDAPベースのログイン

前提条件

- NDSD_TRY_NMASLOGIN_FIRST環境変数がtrueに設定されていることを確認してください。

  詳細については、『「NetIQ eDirectory What's New Guide (NetIQ eDirectory新機能ガイド)」』の「How to Make Your Password Case-Sensitive (パスワードで大文字と小文字を区別する方法)」*のセクション*を参照してください。

注: これはデフォルトで、eDirectory 9.0以降で設定されます。

ログイン方法

HOTP対応ユーザは、NDSパスワードとHOTP値を連結させることによって、LDAPバインドを実行できます。

次に例を示します。

```
ldapsearch -D cn=user1,o=novell -w secret40338314 -h 164.99.91.165 -p 389 -b
"o=novell" -s sub -LLL dn
```

NCPベースのログイン

HOTP対応ユーザは、次のユーティリティのいずれかでNDSパスワードとHOTP値を連結させることによって、NCPログインを実行できます。

- ndslogin

  次に例を示します。

  ```
  ndslogin user1.org -h org.com -p secret40338314
  ```

- iManager
- iMonitor

注: LDAP認証を実行するiManagerプラグインは、HOTP対応ユーザが使用するとエラーになります。

インストール

サーバのインストール

HOTPサーバモジュールは、NMASサーバコンポーネントの一部です。このサーバモジュールがクライアントから提示されたOTPを検証します。

次の属性をNMAS HOTPサーバ上で使用できます。

- sasOTPCounter (ユーザ属性ごと)
- sasOTPEnabled (ユーザ/直接のペアレントコンテナ/パーティションルート/ログインポリシーオブジェクトごと)
- sasOTPDigits (ユーザ/直接のペアレントコンテナ/パーティションルート/ログインポリシーオブジェクトごと)
- asOTPLookAheadWindow (ログインポリシーオブジェクトでツリー全体に対して設定されます)
- sasOTPResync (ユーザ属性あたり9)

nmashotpconfユーティリティの取得および使用方法

nmashotpconfユーティリティは、eDirectoryサーバ上でOTP属性を設定する環境設定ユーティリティです。

注: HOTPユーティリティは、Linux 64ビットプラットフォームでのみ使用できます。

---

nashotpconfユーティリティを実行するには、次の手順を実行します。

1 nmashotpconfユーティリティを入手し、NMASHOTPユーティリティを解凍したディレクトリを指定します。

注: nnmashotpconfユーティリティは、NMASにバンドルされています。このユーティリティをダウンロードするには、https://download.novell.com/Download?buildid=BfnNcVX8U_Iを参照してください。

解凍されたファイルには、32ビットと64ビットのLinuxマシン用のlinuxディレクトリとlinux_x64ディレクトリが含まれています。

Linuxディレクトリとlinux_x64ディレクトリには、nmashotpconf実行可能ファイルとlibnmasext.soファイルが含まれています。

2 Linux 32ビットマシン上ではlinux/finalディレクトリに移動し、Linux 64ビットマシン上ではlinux_x64/finalディレクトリに移動します。

3 ルート認証局証明書をダウンロードして、ローカルに保存します。

詳細については、725 ページの 「ルート認証局または公開鍵証明書のエクスポート」を参照してください。

使用するには:

```
nmashotpconf -h <host_name> [-p <ssl_port>] -D <login_dn> [-w <password>]
 -e <trusted_cert> -t <cert_type> [-r <resync_window>] [-y
 <user_resync_window>] [-u <hotp_dn> [-o <hotp_options>] [-d digits] [-c
 <counter>] [-s <secret> -f <secret_format>]]
```

オプション	説明
host_name	LDAPサーバ名またはサーバのIPアドレスを指定します。
ssl_port	LDAPサーバ上のSSLポートを指定します。デフォルトは636です。
login_dn	ユーザのDNを指定します。
パスワード	ユーザDNのパスワードを指定します。
trusted_cert	ルート認証局証明書ファイルを指定します。
cert_type	ルート認証局証明書のエンコードタイプを指定します。たとえば、DERはderエンコードファイルを意味し、B64はb64エンコードファイルを意味します。
encoded file digits	HOTP値として使用する桁数を指定します。 **注:** この設定がツリー内のすべてのユーザに適用されます。
resync_window	カウンタ再同期先読みウィンドウを指定します。
user_resync_window	カウンタユーザ再同期先読みウィンドウを指定します。
hotp_dn	HOTP属性を設定しているターゲットDNを指定します。ツリーレベルでHOTPを設定するには、ツリーレベルでHOTPを有効/無効にするか、ツリーレベルで［**桁数**］を設定してから、「cn=Login Policy,cn=Security」としてDNを指定します。
hotp_options	**hotp_dn**オプションに対してHOTPを有効または無効にします。HOTPを有効にするにはENABLEを指定し、HOTPを無効にするにはDISABLEを指定します。
counter	HOTPカウンタ値を指定します。カウンタ値の有効範囲は0～2147483647です。カウンタ値は**hotp_dn**オプションを通して設定されます。
hotp_dn secret	OATHHOTPシークレットを指定します。たとえば、16進形式の**シークレット**の未加工のバイト値は31323334353637383930313233343536373839 30で、対応するASCII/拡張ASCII文字列は12345678901234567890です。
secret_format	OATH HOTPシークレットの形式を指定します。 ◆ **STRING:** この形式は、ASCII/拡張ASCII文字列に使用されます。たとえば、「12345678901234567890」と指定します。 ◆ **RAW:** この形式は、16進形式の未加工のバイト値に使用されます。たとえば、31323334353637383930313233343536373839 30の場合は、31が最初の文字の16進値で、32が2つ目の文字の値になります。

カウンタの再同期

サーバのカウンタ値はHOTP認証に成功するとインクリメントされ、クライアントのカウンタは新しいHOTPがユーザから要求されるたびにインクリメントされます。サーバ上のカウンタ値とクライアント上のカウンタは同期していない場合があります。

これを解決するには、ツリー全体の先読みまたは再同期ウィンドウの設定を実施する必要があります。サーバで受信されたHOTPがサーバのカウンタ値に対応していないことが検出された場合は、サーバが再同期ウィンドウ内の次のいくつかのHOTP値を再計算して、それらを受信されたHOTPに照らしてチェックすることができます。一致が確認された場合は、認証が成功して、一致したHOTPに対応するカウンタ値が、サーバカウンタとして設定されます。

認証を成功させるために、サーバカウンタは認証が成功する次のカウンタ値に設定されます。

ツリー全体の再同期ウィンドウの設定は、できるだけ小さくして、攻撃者がHOTP値の再作成を試みる余地を制限する必要があります。クライアントとサーバのカウンタの誤差がツリー全体の再同期ウィンドウの設定を超えている場合は、一時的にユーザ固有の再同期ウィンドウを大きい値に設定してHOTPベースの認証を試みることにより再同期することができます。

HOTPベースの認証を設定するには、nmashotpconfユーティリティを使用する必要があります。詳細については、環境設定のセクションを参照してください。

環境設定

HOTPベースの認証用にeDirectoryユーザをプロビジョニングするには、RFC 4226標準に従って、次の設定手順を実行します。

- ユーザ/コンテナ/パーティションルート/ログインポリシーオブジェクト(この順序は優先順位と同じになります)に対してHOTPを有効にします。
- そのユーザに対してHOTP共有秘密鍵とカウンタを設定します。この2つの設定によって、HOTP値が決定されます。
- ユーザ/コンテナ/パーティションルート/ログインポリシーオブジェクトに対してHOTP値の桁数を設定します。有効な桁数の範囲は6～9です。
- 再同期ウィンドウを次のように設定します。
  - ログインポリシーオブジェクトでツリー全体の再同期ウィンドウを設定します。
  - ユーザレベルでユーザ固有の再同期ウィンドウを設定します。これは、クライアントとサーバが同期していない場合にのみ必要です。

例:

- ユーザオブジェクトに対してシークレットとカウンタを設定するには、次のコマンドを実行します。

```
./nmashotpconf -h 192.168.1.1 -p 636 -D cn=admin,o=novell -w novell   -e   /
var/opt/novell/eDirectory/data/SSCert.der  -t  DER  -u cn=user1,o=novell  -c 0
-s   31323334353637383930313233343536373839 30 -f  RAW
```

- ユーザオブジェクトに対してOTPを有効にするには、次のコマンドを実行します。

```
./nmashotpconf -h 192.168.1.1 -p 636 -D cn=admin,o=novell -w novell   -e   /
var/opt/novell/eDirectory/data/SSCert.der  -t  DER  -u cn=user1,o=novell  -o
ENABLE
```

- ユーザオブジェクトに対してOTPを無効にするには、次のコマンドを実行します。

  ```
  ./nmashotpconf -h 192.168.1.1 -p 636 -D cn=admin,o=novell -w novell   -e   /
  var/opt/novell/eDirectory/data/SSCert.der  -t  DER  -u cn=user1,o=novell  -o
  DISABLE
  ```

  同様に、コンテナ/パーティションまたはルート/ログインポリシーオブジェクトに対してOTPを有効または無効にすることができます。

- ユーザオブジェクトに対してOTP桁を設定するには、次のコマンドを実行します。

  ```
  ./nmashotpconf -h 192.168.1.1 -p 636 -D cn=admin,o=novell -w novell   -e /var/
  opt/novell/eDirectory/data/SSCert.der  -t  DER  -u cn=user1,o=novell  -d 6
  ```

  同様に、ペアレントコンテナ/パーティションルート/ログインポリシーオブジェクトに対してもOTP桁を設定できます。

- ユーザ再同期ウィンドウを設定するには、次のコマンドを実行します。

  ```
  ./nmashotpconf -h 192.168.1.1 -p 636 -D cn=admin,o=novell -w novell   -y 5 -e
  /var/opt/novell/eDirectory/data/SSCert.der  -t  DER  -u cn=user1,o=novell
  ```

- カウンタ再同期先読みウィンドウを設定するには、次のコマンドを実行します。

  ```
  ./nmashotpconf -h 192.168.1.1 -p 636 -D cn=admin,o=novell -w novell   -r 6
  ```

注: 設定をテストするには、HOTP規格に準拠しているハードウェアやソフトウェアによって生成されたHOTPを使用できます。

当バージョンの注意事項

- 683 ページの 「ndsconfig addは、HOTP対応管理者ユーザの場合は失敗します。」
- 683 ページの 「HOTP対応ユーザとしての読み込み専用レプリカへのログインが失敗する」

ndsconfig addは、HOTP対応管理者ユーザの場合は失敗します。

HOTP対応ユーザの場合は、OTP桁が認証に使用されます。ndsconfigユーティリティは、以降の認証に同じOTP桁を使用するため、ndsconfig addが失敗します。同様に、ndsconfig upgradeも失敗します。

この問題を回避するため、ndsconfig add/upgradeを実行するユーザに対してはHOTPを有効にしないでください。

HOTP対応ユーザとしての読み込み専用レプリカへのログインが失敗する

HOTP対応ユーザとして読み込み専用レプリカに要求を送信することによってLDAPログインを実行すると、LDAPチェーンが実行されません。読み込み専用レプリカは、実際のユーザが存在するサーバには要求を転送しません。レプリカは失敗し、不正なレプリカタイプのエラーが表示されます。

nmashotpconfユーティリティは、ユーザ再同期ウィンドウを変更できません。

ユーザ再同期ウィンドウの値がすでに設定(たとえば、2に)されている場合、その値がnmashotpconfユーティリティを使用して変更されると、次のエラーが表示されます。

```
ldap_modify_ext_s on HOTP DN failed: error code=19: Constraint violation
```

エラーの原因の1つは、ユーザ再同期値を変更するために、**-o** (OTPを有効または無効にするオプション)、**-d** (OTP桁)、**-c** (otpcouter)、および**-y** (user_resync_window)オプションの組み合わせを使用していることです。

その他の管理タスク

このセクションでは、NMASのその他の管理タスクについて説明します。

- 684 ページの 「ポリシーリフレッシュレートコマンドの使用」
- 685 ページの 「LoginInfoコマンドの使用」
- 688 ページの 「LDAPに対するNMASベースのログインの無効化」
- 688 ページの 「NMASコマンドの呼び出し」
- 688 ページの 「失敗したログイン試行の遅延時間の設定」
- 689 ページの 「DSTraceの使用」
- 689 ページの 「NMASクライアントの無効化とアンインストール」
- 689 ページの 「NMASイベントの監査」

ポリシーリフレッシュレートコマンドの使用

ログイン試行のたびにではなく、スケジュールしたインターバルで、セキュリティコンテナに保存されたNMASログインポリシーからキャッシュに保存されたNMASログインポリシーをリフレッシュするようにNMASを設定することができます。この設定はNMASポリシーリフレッシュレートコマンドを使用してサーバごとに構成します。

注: サーバは、起動時に1回だけセキュリティコンテナにアクセスしてポリシーをキャッシュに保存します。その後は、設定されたインターバルに基づいて、セキュリティコンテナにアクセスしてポリシーをリフレッシュすることを試みます。

ポリシーリフレッシュレートコマンドの構文は次のとおりです。

nmas RefreshRate *minutes*

ここで、*minutes*は、キャッシュに保存されたNMASログインポリシーを更新する必要があるかどうかをチェックする間隔(分)です。

各NMASサーバプラットフォームでポリシーリフレッシュレートコマンドを呼び出す方法については、688 ページの 「NMASコマンドの呼び出し」を参照してください。

LoginInfoコマンドの使用

NMAS 3.2以降では、LoginInfo <numb>コマンドを使用して、特定のユーザオブジェクトログイン属性の自動更新をオフにすることができます。属性を自動更新すると問題が発生する場合には、手動でこれを行うことができます。次のセクションでは、この機能についてさらに詳しく説明します。

LDAPバインド用のNMASログイン

eDirectory 9.2では、デフォルトで、LDAPバインドのためにNMASログインが有効になっています。NMASログインが有効になっている場合は、eDirectoryがユーザの認証後に自動的にユーザオブジェクトログイン属性を更新します。更新されるログイン属性のリスト(ただし完全に網羅するものではない)を以下に示します。

- ログイン時刻
- ネットワークアドレス
- 最終ログイン時刻

LDAPに対するNMASベースのログインを無効にするには、688ページの 「LDAPに対するNMASベースのログインの無効化」を参照してください。

ユーザオブジェクトログイン属性を自動更新することによって発生する問題

ユーザオブジェクトログイン属性の自動更新は、次のような問題を引き起こす可能性があります。

- 高い使用率
- 無応答
- 特にLDAP環境でビジー状態の認証サーバで見られるクライアントのタイムアウト

これらの問題が発生した場合は、ログイン属性の更新のタイミングを調整する必要があります。この方法については、685 ページの 「LoginInfoコマンドを使用した属性の更新のタイミングの制御」を参照してください。

LoginInfoコマンドを使用した属性の更新のタイミングの制御

ログイン属性の更新タイミングを制御するには、nmas LoginInfo <num>コマンドを実行します。

<num>の値は次のとおりです。

- **0またはoff:** ログイン属性を更新しません。
- **1:** 不正侵入者の検出に必要な属性のみを更新します。
- **2:** 未使用のユーザパスワードポリシー属性を除く、すべてのログイン属性を更新します。
- **3またはon:** すべてのログイン属性を更新します。

NMASサーバプラットフォームごとのLoginInfoコマンドの呼び出し方法については、688 ページの「NMASコマンドの呼び出し」を参照してください。

sasUpdateLoginInfo属性とsasUpdateLoginTimeInterval属性の使用

sasUpdateLoginInfo属性は、LoginInfo属性の更新を制御します。

sasUpdateLoginTimeInterval属性は、指定されたインターバルでユーザのログイン時刻属性が更新されるように制御します。

SasUpdateLoginInfo属性は、次の値に設定することができます。

- **0またはoff:** ログイン属性を更新しません。
- **1:** 不正侵入者の検出に必要な属性のみを更新します。
- **2:** 未使用のユーザパスワードポリシー属性を除く、すべてのログイン属性を更新します。
- **3またはon:** すべてのログイン属性を更新します。

SasUpdateLoginTimeInterval属性は、0～1440分(つまり、1日)の値に設定することができます。

- 値が0の場合は、ログインに成功するたびにログイン時刻属性と最終ログイン時刻属性が更新されます。
- 値が**1**～**1440**分の場合は、指定されたインターバルでログイン時刻属性が更新されます。最終ログイン時刻属性は更新されません。

注: ログイン時刻属性は、インターバル中に続いてログインに成功しても更新されません。ただし、インターバル中ログインに失敗してその後ログインに成功した場合は、ログイン時刻属性が更新されます。ログインの成功からインターバル時間がカウントされます。

sasUpdateLoginTimeInterval属性は、sasUpdateLoginInfo属性値が2または3に設定されている場合にのみ有効になります。

これらの属性は、以下のオブジェクトに対して設定できます。オブジェクトは優先順位順に列挙しています(ユーザの優先順位が最も高くなります)。

- User (ユーザ)
- ユーザのコンテナ
- パーティションルート
- ログインポリシー

ログインポリシーオブジェクトに対してsasUpdateLoginInfoとsasUpdateLoginTimeIntervalを設定した場合は、その次のポリシーリフレッシュサイクルの後に設定が有効になります。ユーザ、コンテナ、パーティションルート、またはログインポリシーに対してこれらの属性が設定されていない場合は、後方互換性を維持するために、コマンドラインを使用してサーバ上で設定された値が使用されます。

eDirectoryサーバ上で属性値を設定する例を以下に示します。

```
#cat nmas.config (The nmas.config file must be in the same directory as the dib
directory.)
nmas LoginInfo 2
nmas UpdateLoginTimeInterval 30
```

パーティションルートで属性値を設定するには:

1 属性をツリーに追加するには、［iManager］>［スキーマ］>［属性の追加］>［ツリールート］に移動します。
2 矢印を使用して必要な属性を［使用可能なオプション属性］リストから［オプション属性］リストに移動します。

パーティションルートで属性の値を設定するには、コマンドラインまたはldifファイルを使用して、ldapmodifyコマンドと次のコマンドを実行します。

```
dn:T=< tree name>
changetype:modify
add:sasUpdateLoginTimeInterval
sasUpdateLoginTimeInterval:35

dn:T=< tree name>
changetype:modify
add:sasUpdateLoginInfo
sasUpdateLoginInfo: 2
```

ユーザ、コンテナ、およびログインポリシーオブジェクトのsasUpdateLoginInfo属性値またはsasUpdateLoginTimeInterval属性値は、iManagerまたはldifファイルを使用して編集することができます。

例:

```
#cat changesasUpdateLoginInfo.ldif
dn: cn=user1,o=org
change type: modify
replace: sasUpdateLoginInfo
sasUpdateLoginInfo: 1

#cat changesasUpdateLoginTimeInterval.ldif
dn: cn=user1,o=org
changetype: modify
replace: sasUpdateLoginTimeInterval
sasUpdateLoginTimeInterval: 60
```

この設定は、user1のログイン時刻属性の更新を前回の更新から60分間無効にします。

iManagerからsasUpdateLoginInfo属性とsasUpdateLoginTimeInterval属性を指定するには:

1 NetIQ iManagerで、［役割およびタスク］ボタン をクリックします。
2 ［ディレクトリ管理］>［オブジェクトの変更］の順にクリックします。
3 コンテナまたはログインポリシーオブジェクトの名前とコンテキストを指定して、［OK］をクリックします。
4 ［一般］タブで、［その他］を選択してから、［値がない属性］リストから［sasUpdateLoginTimeInterval］を選択します。
5 矢印ボタンを使用して、［値がない属性］リストから［値がある属性］リストに［sasUpdateLoginTimeInterval］を移動してから、［適用］をクリックします。

LDAPに対するNMASベースのログインの無効化

eDirectory9.2では、デフォルトで、NMASログインが有効になっています。NMASログインを無効にするには、NDSD_TRY_NMASLOGIN_FIRSTをfalseに設定します。

Windows上でLDAPに対するNMASベースのログインを無効にするには、［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］で、変数を追加して、その値をfalseに設定します。

注: RHEL 7.xプラットフォームとSLES 12.xプラットフォームの/etc/opt/novell/eDirectory/confディレクトリに配置されたenvファイルにeDirectoryサービスに必要なすべての環境変数を追加する必要があります。

NMASコマンドの呼び出し

NMASコマンドを呼び出す方法は、実行しているプラットフォームによって異なります。次のプラットフォームがサポートされています。

- 688 ページの 「Windows」
- 688 ページの 「Linux」

Windows

NMASは、起動時にnmas.cfgファイル内のコマンドを処理します。nmas.cfgファイルは、dibファイルと同じディレクトリ(通常はc:/novell/nds/dibfiles)に配置されている必要があります。

または

NMASが起動したら、次の手順を使用します。

1. NetIQ eDirectory Servicesコンソールで、［nmas.dlm］を選択します。
2. ［**起動パラメータ**］フィールドにコマンドを入力します。
3. ［**Configure (構成)**］をクリックします。

Linux

NMASは、起動時にnmas.configファイル内のコマンドを処理します。nmas.configファイルは、dibディレクトリと同じディレクトリに配置されている必要があります。たとえば、.dibディレクトリのパスが/var/opt/novell/eDirectory/data/dibの場合は、nmas.configファイルのパスは/var/opt/novell/eDirectory/data/nmas.configになります。

失敗したログイン試行の遅延時間の設定

1. NMASプラグインをiManagerにインストールします。

   NMASプラグインは、Novellダウンロードサイトからダウンロードできます。
2. iManagerの［**役割およびタスク**］メニューで、［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。
3. ログインポリシーオブジェクトをブラウズして選択し、［**OK**］をクリックします。

4 ［NMAS］タブをクリックしてから、［設定］をクリックします。

5 失敗したログイン試行から次のログイン試行までの任意のログイン画面表示遅延時間を秒数で入力してから、［OK］をクリックします。

DSTraceの使用

DSTraceユーティリティを使用して、NMASからトレース情報を取得できます。

NMASクライアントトレースを収集する方法については、「TID # 3331372」を参照してください。

NMASサーバトレースを収集する方法については、「TID # 3815371」を参照してください。

NMASクライアントの無効化とアンインストール

NMASクライアントを無効にするには:

1 ワークステーションで、赤色のNを右クリックします。

2 ［Novell Client Properties］をクリックします。

3 ［Advanced Login］タブをクリックします。

4 ［Parameter Groups］リストから、［NMAS Authentication］を選択します。

5 ［設定］で、［オフ］を選択します。

6 OKをクリックします。

NMASクライアントをアンインストールするには、Windowsの［コントロール パネル］で［プログラムの追加と削除］オプションを使用します。

注: NMASを無効にしたり削除したりしても、Novell Client for Windowsからのユニバーサルパスワードの変更のサポートは削除されません。

NMASイベントの監査

NMASイベントを監査するために使用できる製品には、次の2つがあります。

- NetIQ Audit Secure Logging Server

  NetIQ Audit Secure Logging Serverを使用してnmas_en.lscファイルをインストールすることができます。このファイルは、次のディレクトリに配置されています。

  Windows: novell\nds

  Linux: /opt/novell/eDirectory/lib64/nds-schem

  NetIQ Auditのインストール方法と管理方法については、NetIQ Auditのオンラインヘルプを参照してください。
- NetIQ Sentinel

また、iManagerのNMAS 9.0以降のプラグインを使用して、NMAS Auditを有効にする必要があります。Platform AgentでNMAS Auditを有効にするには、次の手順を実行します。

1 NMAS 9.0以降のプラグインをiManagerにインストールします。

NMAS 9.0以降のプラグインは、NetIQダウンロードサイトからダウンロードできます。

2 iManagerの［役割およびタスク］メニューで、［ディレクトリ管理］>［オブジェクトの変更］の順にクリックします。

3 ログインポリシーオブジェクトをブラウズして選択し、［OK］をクリックします。

4 ［NMAS］タブをクリックしてから、［設定］をクリックします。

5 ［Enable auditing］の横にあるボックスをオンにしてから、［OK］をクリックします。

NetIQ Auditと外部証明書の使用

NMASとNetIQ Auditで外部証明書を使用するには、まず、証明書を次の名前の2つの.pemファイルに変換する必要があります。

- nmascert.pem: これは証明書を含むファイルです。
- nmaskey.pem: これは秘密鍵を含むファイルです。

これらのファイルは、システム内の各NMASサーバで、プラットフォームごとに次のディレクトリにコピーする必要があります。

- Linux: /etc
- Windows: GetWindowsDirectoryからの戻り値(通常はc:\windows)

NMASは、ログがオープンの場合、nmascert.pemファイルとnmaskey.pemファイルが存在すればそれらをNetIQ Auditプラットフォームエージェントに提供します。ファイルが存在しない場合は、NMASがNetIQ Auditプラットフォームエージェントに内部証明書と鍵を提供します。

NMASイベントを監査するためのXDASの使用

NMASイベントはXDASを使用して監査できます。詳細については、619ページの 「XDASを使用した監査」を参照してください。

セキュリティ上の考慮事項

このセクションでは、NetIQモジュラー認証サービスのセキュリティに関連した具体的な情報を提供します。以下のサブセクションで構成されています。

パートナーログインメソッド

NetIQは、パートナーのログインメソッドのセキュリティ手法の評価は行っていません。パートナーの製品にNetIQ Yes、Tested & Approved、またはNetIQ Directory Enabledのロゴの表示が認められていても、それらのロゴは一般的な製品の相互運用性を示しているにすぎません。

ログインポリシー

- 承認済みログインシーケンス、デフォルトログインシーケンス、承認済みクリアランス、またはデフォルトクリアランスがパーティションルートではないコンテナに割り当てられている場合、そのポリシーは、そのコンテナ内のユーザオブジェクトに対してのみ有効になり、サブコンテナ内のユーザオブジェクトに対しては有効になりません。
- 承認済みログインシーケンス、デフォルトログインシーケンス、承認済みクリアランス、またはデフォルトクリアランスがパーティションルートであるコンテナに割り当てられている場合、そのポリシーは、それらの値がユーザオブジェクトやオブジェクトのペアレントコンテナに割り当てられていないパーティション内のすべてのユーザに対して有効になります。
- 承認済みログインシーケンス、デフォルトログインシーケンス、承認済みクリアランス、またはデフォルトクリアランスがログインポリシーに割り当てられている場合、そのポリシーは、それらの値がユーザオブジェクト、オブジェクトのペアレントコンテナ、またはオブジェクトのパーティションルートに割り当てられていないツリー内のすべてのユーザに対して有効になります。
- ユーザにパスワードまたはその他の推測可能なログインシークレット(秘密の質問の回答など)が割り当てられている場合は、不正侵入者検出を有効にして、不正侵入者によるログインシークレットの推測を遅らせるかまたは阻止する必要があります。
- デフォルトで、失敗したログイン試行には3秒間の遅延が適用されます。この遅延の目的は、不正侵入者がパスワードを推測する試みを遅らせることです。失敗したログインの遅延の長さは設定によって変更できます。デフォルトの3秒間を使用することをお勧めします。
- 不正侵入者検出、ネットワークアドレス制限、時間制限などのログインポリシーは、すべてのログインシーケンスに適用されます。たとえば、いくつかのNetIQ製品の忘れたパスワードのセルフサービス機能によってチャレンジ/レスポンス方式のログインメソッドが呼び出された場合は、ログインポリシーが適用されます。
- ログイン試行と設定変更を追跡できるように、NMAS™監査を有効にする必要があります。
- ポリシーリフレッシュレートコマンドを使用して、キャッシュに保存されたパスワードポリシーをリフレッシュする必要があるかどうかを、ログインのたびにではなく定義したインターバルでチェックしている場合は、ログインポリシーの変更の適用に遅れが生じます。
- LoginInfoコマンドを使用すると、ログイン中のログイン関連属性の更新を無効にすることができます。これらの属性には、不正侵入者検出属性が含まれます。これらのログイン関連属性の更新を無効にすると、ログインのパフォーマンスが向上します。ただし、これらの属性の更新を無効にすると、システムのセキュリティが低下する可能性があります。
- 不正侵入者検出ポリシーは、ユーザオブジェクトの直接のコンテナまたはユーザオブジェクトのパーティションルート上で設定できます。NMASは、最初に、ペアレントコンテナで不正侵入者検出ポリシーをチェックします。ポリシーが見つからなかった場合は、パーティションルートで不正侵入者検出ポリシーがチェックされます。

NMASInst

ログインメソッドをアップグレードするときに、-checkversionオプションが使用されていなければ、nmasinstが新しいバージョンを古いバージョンに置き換えます。

nmasinstにはコマンドラインでパスワードを指定するオプションがありますが、この方法ではパスワードが漏洩する可能性があるため推奨されていません。eDirectory 9.0以降では、nmasinstによって、ファイルまたは環境変数からパスワードを取得できます。

ユニバーサルパスワード

- セキュリティコンテナにはグローバルポリシーが含まれているため、書き込み可能なレプリカを配置する場所に注意する必要があります。一部のサーバは、eDirectoryツリーで指定されたセキュリティポリシー全体を変更することができます。ユーザがNMASを使用してログインするためには、ユーザオブジェクトとセキュリティコンテナのレプリカをNMASサーバ上に配置する必要があります。
- パスワードポリシーがパーティションルートではないコンテナに割り当てられている場合、そのポリシーは、コンテナ内のユーザオブジェクトに対してのみ有効になり、サブコンテナ内のユーザオブジェクトに対しては有効になりません。
- パスワードポリシーがパーティションルートであるコンテナに割り当てられている場合、そのポリシーは、それらの値がユーザオブジェクトにもオブジェクトのペアレントコンテナにも割り当てられていないパーティション内のすべてのユーザに対して有効になります。
- パスワードポリシーがログインポリシーに割り当てられている場合、そのポリシーは、それらの値がユーザオブジェクト、オブジェクトのペアレントコンテナ、またはオブジェクトのパーティションルートのいずれにも割り当てられていないツリー内のすべてのユーザに対して有効になります。
- 「既存のパスワードがパスワードポリシーに準拠しているかどうかを確認する(ログイン時に検証が実行される)」パスワードポリシールールがtrueに設定されていない場合は、NDSパスワードがユニバーサルパスワードに移行されるときにパスワード期限の時刻が更新されません。
- パスワードポリシーは、ユーザまたはパスワード管理者が文書化されたNMAS LDAP拡張機能を使用してユニバーサルパスワードを読み込むことができるように設定できます。特定のインストールに必要でない限り、これらのオプションは有効にしないでください。ユーザパスワードを読み込み可能にする必要がある場合は、選択されたユーザだけがパスワードを読み込めるようにパスワードポリシーを設定する必要があります。
- 接続されたシステム間でのパスワードの同期にIdentity Manager Password Synchronizationが使用されている場合にのみ、配布パスワードに同期するためのパスワードポリシーを設定する必要があります。

  Identity Manager Password Synchronizationを使用して接続されたシステム間でパスワードを同期する方法については、『*NetIQ Identity Manager 4.5 Password Management Guide (NetIQ Identity Manager 4.5パスワード管理ガイド)*』を参照してください。
- 単純パスワードに同期するようにパスワードポリシーを設定する必要があるのは以下の場合です。
  - ユーザオブジェクトの書き込み可能なレプリカが保存されているサーバがある。
  - ユーザがCIFSやAFPなどのネイティブなファイルアクセスプロトコルを使用してそれらのサーバにアクセスしている。
- パスワードポリシーに対して詳細パスワードルールが有効になっている場合は、ユーザオブジェクトに対する従来のパスワードルールが無視され、ユーザが自分のパスワードを変更するときかログインするときに、パスワードポリシーのルールに合わせて更新されます。
- パスワード除外ルール(パスワード履歴、除外されたパスワード、および許可されていない属性値)は、NMASがランダムパスワードの生成に使用されている場合は適用されません。
- パスワードルールを選択する場合は、推測するのが難しいパスワードにする必要がありますが、覚えられないものにはならないようにしなければなりません。
- 管理者がNDSパスワードを削除するように指定した場合は、NDSパスワードハッシュがeDirectory以外は認識できないランダム値に設定されます。そのランダム値にハッシュ可能なパスワード値は存在することもあれば存在しないこともあります。

- XMLパスワードの複雑さ
  - 重複したルールタグがある場合、ポリシーに照らしたパスワードのチェックとランダムパスワードの生成には、最も制限的なルールが使用されます(他のルールは無視されます)。
  - ランダムパスワードの生成では、ViolationsAllowedとNumberOfCharactersToEvaluateのルール設定属性が無視されます。
  - ランダムパスワードの生成には、XML内の最初のポリシーのみが使用されます。

ユニバーサルパスワードセキュリティの詳細については、「771ページの第26章「パスワードを管理する」」を参照してください。

SDIキー

ツリー鍵とも呼ばれるセキュリティドメインインフラストラクチャ(SDI)鍵をTriple DES鍵(3DES)にする必要があります。SDI鍵は、SDIDiagユーティリティを使用してチェックまたはアップグレードすることができます。771ページの第26章「パスワードを管理する」の「SDIドメインキーサーバ上でNICI 3.0が実行されていることを検証します。」を参照してください。

eDirectory 9.0以降では、AES 256ツリー鍵もサポートされます。詳細については、「Creating an AES 256-Bit Tree Key (AES 256ビットツリーキーを作成する)」を参照してください。

25 Certificate Serverについて

eDirectoryをインストールすると、NetIQ Certificate Serverが自動的にインストールされます。Certificate Serverは、eDirectoryにネイティブに統合された公開鍵暗号サービスを提供します。このサービスを使用すれば、ユーザとサーバの両方の証明書を作成、発行、および管理することができます。これらのサービスにより、インターネットなどのパブリック通信チャネルを介した機密データの伝送を保護できます。

注

- 公開鍵暗号の概念については、「759 ページの 「公開鍵暗号化の基本」」を参照してください。
- RSA暗号化用のMD2およびMD5署名アルゴリズムは、eDirectory 9.2以降ではサポートされません。

NetIQ Certificate Serverの機能

公開鍵暗号はネットワーク管理者にとっての特有の課題です。NetIQ Certificate Serverは、次の特徴によって、これらの課題への対処を助けます。

- ネットワーク上で公開鍵暗号サービスを提供します

  eDirectoryツリー内に組織認証局(CA)を作成することができ、無制限の数のユーザ証明書とサーバ証明書を発行することができます。また、外部認証局のサービスも使用でき、必要に応じて両方を組み合わせて使用することができます。
- 公開鍵証明書の取得と管理に関連したコストを制御します

  組織認証局を作成し、その組織の認証局を通して公開鍵を発行することができます。
- 公開鍵証明書を改ざんから保護しながら公に利用可能にします

  証明書はeDirectoryに保存されるため、eDirectoryのレプリケーション機能とアクセス制御機能を利用できます。
- 署名/復号化操作に秘密鍵を使用するソフトウェアルーチンのみが秘密鍵にアクセスできるようにします

  秘密鍵はNICI (Novell International Cryptography Infrastructure)によって暗号化され、署名/復号化操作にそれらの秘密鍵を使用するソフトウェアルーチンのみがそれらの秘密鍵を使用できるようにされます。
- 秘密鍵を安全にバックアップします

秘密鍵はNICIによって暗号化され、eDirectoryに保存され、標準のeDirectoryバックアップユーティリティを使用してバックアップされます。

- iManagerを使用して証明書を一元管理することができます

  iManagerプラグインが提供されており、これによって、組織認証局から発行された証明書や、PKCS #10形式の証明書署名要求をサポートする他のCAから発行された証明書を管理することができます。

- ユーザが独自の証明書を管理できます

  ユーザは、iManagerを使用して、システム管理者の介在なしに、暗号化対応アプリケーションで使用するキーをエクスポートすることができます。

- 広く使用されている電子メールクライアントとブラウザをサポートします

NetIQ Certificate Serverのコンポーネント

このセクションでは、NetIQ Certificate Serverのコンポーネントについて説明します。

- 696 ページの 「NetIQ Certificate Server」
- 703 ページの 「Novell International Cryptographic Infrastructure」

NetIQ Certificate Server

NetIQ Certificate Serverは、PKIサーバコンポーネントとiManagerへのプラグインモジュールで構成されます。iManagerは、Certificate Serverの管理インタフェースです。

Certificate Serverでは、次のタスクを実行できます。

- eDirectoryツリーと組織に固有の組織認証局を設定します。
- 公開鍵証明書とその関連秘密鍵を要求および管理し、eDirectoryツリーに保存します。

証明書での8192ビットRSAキーの使用

証明書サーバを使用すると、証明書作成手順の一環としてキーサイズを選択できます。eDirectoryは、最大8192ビットのキーサイズをサポートします。アプリケーションでX.509認定と8192ビットRSA公開鍵を使用する場合は、アプリケーションで8192ビットRSA鍵がサポートされている必要があります。サポートされていないと、アプリケーションが期待どおりに機能しない可能性があります。

重要: TLS接続を確立するために8KビットRSA公開鍵のX.509証明書を使用すると、eDirectoryサーバのパフォーマンスに影響します。NetIQでは、8Kビット鍵のRSA証明書を使用するようeDirectoryサーバを構成することを推奨していません。TLSセッションを確立する処理はサーバでの計算量が多くなり、複数のTLSセッションが同時に確立されるとシステムが大幅に低下する可能性があるためです。

8192ビットRSA公開鍵で認証局証明書を作成する前に、eDirectoryツリー内のすべてのサーバを9.1にアップグレードしてください。

注: 8192ビットRSA公開鍵でサーバ証明書を設定する前に、最小でもeDirectory 9.1、iManager 3.1、eDirectory 9.1 PKIプラグインを使用していることを確認します。

ECDSA証明書の使用

Certificate Serverは、RSA証明書のサポートと同様に、楕円曲線デジタル署名アルゴリズム(ECDSA)の証明書とキーの使用および管理をサポートします。

RSA鍵との互換性のあるセキュリティを持つECDSA鍵ペアは、RSA鍵よりもはるかに小さく、TLS接続の確立に使用された場合にパフォーマンスを大幅に向上させます。ECDSAは、楕円曲線暗号システム(ECC)を利用します。ECCは、楕円曲線を使ってキーを生成します。この技術は、RSAやDiffie-Hellmanなどのほとんどの公開鍵暗号化方式と組み合わせて使用できます。ECCベースの署名をデジタル証明書とともに使用することには、サイズとパフォーマンスの両面でメリットがあります。

eDirectoryは、次の曲線を使用したECDSA証明書とキーをサポートします。

- P-256
- P-384
- P-521

Suite Bモードでは、Certificate ServerはRFC 5759に準拠します。このRFCは、すべてのSuite B証明書とCRLには、ECDSAとともに、P-256かP-384のどちらかの曲線を使用して生成されたキーを使用して署名する必要があることを規定しています。

証明書にP-256曲線に基づく鍵が含まれている場合、署名するCAの鍵は、P-256またはP-384曲線に基づいていなければなりません。証明書にP-384曲線に基づく鍵が含まれている場合、署名するCAの鍵は、P-384曲線に基づいていなければなりません。証明書とCRLは、署名するCAのキーのサイズに合わせて、SHA-256またはSHA-384を使用してハッシュする必要があります。

NetIQ Certificate Serverをインストールしたら、iManagerを使用してそれを管理します。

iManagerを使用して次のタスクを実行できます。

- 698 ページの 「組織用の組織認証局を作成する」
- 698 ページの 「暗号化対応アプリケーションごとにサーバ証明書オブジェクトを作成する」
- 699 ページの 「ユーザ証明書の作成」
- 699 ページの 「ルート認証局コンテナの作成」
- 700 ページの 「ルート認証局オブジェクトの作成」
- 700 ページの 「外部のユーザとサーバ用の証明書の作成」
- 700 ページの 「証明書の検証」
- 700 ページの 「証明書取り消しリストの管理」
- 701 ページの 「秘密鍵と証明書のエクスポート」
- 702 ページの 「秘密鍵と証明書のインポート」
- 702 ページの 「SASサービスオブジェクトの作成」

組織用の組織認証局を作成する

eDirectoryツリー内に組織認証局(CA)が存在しなければ、インストール中にそれを作成することもできます。インストールの完了後に組織認証局を再度作成することもできます。

組織認証局オブジェクトには、公開鍵、秘密鍵、証明書、証明書チェーン、およびその他の組織認証局に関する設定情報が含まれています。組織認証局オブジェクトは、eDirectory内のセキュリティコンテナ内に存在します。

サーバが認証局サービスを提供するように設定された後、サーバはeDirectoryツリー全体で認証局サービスを実行します。ツリーに従属認証局証明書が存在しており、サブ認証局をホストするサーバをeDirectory 9.2にアップグレードする場合は、ECDSA認証局証明書は生成されません。管理者は、従属認証局のRSA証明書と同じサブジェクト名を持つ従属認証局のECDSA証明書をインポートする必要があります。認証局として機能しているサーバがeDirectory 9.2の場合は、eDirectoryが組織認証局用のECDSA証明書を作成します。組織CAにECDSA証明書が存在する場合は、eDirectoryが自動的にサーバ用のECDSA証明書を作成します。

組織認証局の作成方法については、「715ページの「組織の認証局オブジェクトを作成する」」を参照してください。

暗号化対応アプリケーションごとにサーバ証明書オブジェクトを作成する

証明書サーバをインストールすると、デフォルトのサーバ証明書オブジェクトが作成されます。

- SSL CertificateDNS - *server_name*
- サーバ上で設定されたIPアドレスごとの証明書(IP AG *xxx.xxx.xxx.xxx - server_name*)
- サーバ上で設定されたDNS名ごとの証明書(DNS AG *www.example.com - server_name*)
- SSL EC CertificateDNS - *server_name*
- サーバ上で設定されたIPアドレスごとの証明書(IP EC AG *xxx.xxx.xxx.xxx - server_name*)
- サーバ上で設定されたDNS名ごとの証明書(DNS EC AG *www.example.com - server_name*)

注: eDirectoryでは、SSL CertificateIPは自動的に作成されません。SSL CertificateDNSには、［サブジェクトの代替名］にリストされているすべてのIPが含まれます。

インストールの完了後に、他のサーバ証明書オブジェクトを作成できます。

サーバ証明書オブジェクトには、公開鍵、秘密鍵、証明書、およびサーバアプリケーションに対してSSLセキュリティサービスを有効にする証明書チェーンが含まれます。サーバ証明書オブジェクトは、組織認証局と外部認証局のどちらかで署名することができます。

サーバは、多数のサーバ証明書オブジェクトをサーバに関連付けることができます。特定のサーバ上で動作している暗号化対応アプリケーションは、そのサーバのサーバ証明書オブジェクトのいずれかを使用するように設定できます。特定のサーバ上で動作している複数のアプリケーションは同じサーバ証明書オブジェクトを使用できますが、サーバ証明書オブジェクトをサーバ間で共有することはできません。

サーバ証明書オブジェクトは、サーバが存在するコンテナ内にのみ作成できます。サーバオブジェクトを移動する場合は、そのサーバに属しているすべてのサーバ証明書オブジェクトも移動する必要があります。サーバ証明書オブジェクトの名前は変更しないでください。どのサーバ証明書オブ

ジェクトがサーバに属しているかは、サーバ証明書オブジェクト名にそのサーバの名前が含まれているかを確認することによって、あるいは、iManagerでサーバ証明書オブジェクトを表示してホストサーバを確認することによって判別できます。

サーバ証明書オブジェクトに保存されている鍵ペアは、その鍵ペアの作成時に入力された名前で参照されます。鍵ペアの名前は、サーバ証明書オブジェクトの名前ではありません。鍵ペアを使用するように暗号化対応アプリケーションを設定する場合、それらのキーは、サーバ証明書オブジェクト名ではなく、鍵ペア名で参照します。

デフォルトサーバ証明書オブジェクトが破損するか無効になった場合は、デフォルト証明書の作成ウィザードを使用してその古いデフォルト証明書を置き換えます。デフォルト証明書の作成ウィザードにアクセスする方法については、「723ページの「デフォルトのサーバ証明書オブジェクトを作成する」」を参照してください。

デフォルトでは、組織CAにECDSA証明書が存在する場合は、eDirectoryがECDSA証明書を作成します。

ユーザ証明書の作成

ユーザは自分のユーザ証明書と秘密鍵にアクセスして、それらを認証、データ暗号化/復号化、デジタル署名、およびセキュリティで保護された電子メールに利用できます。最も一般的な用途の1つが、S/MIME標準を使用してデジタル署名され、暗号化される電子メールの送受信です。

通常は、ユーザ証明書を作成するのに十分な権利を保有するのは、CA管理者だけです。しかし、秘密鍵をeDirectoryからエクスポートしたりダウンロードしたりする権利は、該当ユーザのみが保有します。すべてのユーザが他のユーザの公開鍵証明書をエクスポートできます。

ユーザ証明書は、ユーザのプロパティページの［セキュリティ］タブで作成され、組織認証局によって署名されます。他のCAによって作成された証明書と秘密鍵は、作成後にインポートできます。

複数の証明書をユーザのオブジェクトに保存することができます。

ユーザ証明書の作成方法については、「71ページの 「ユーザ証明書の作成」」を参照してください。

ルート認証局コンテナの作成

ルート認証局は、公開鍵暗号の信頼の基盤です。ルート認証局は、他のCAによって署名された証明書の検証に使用されます。ルート認証局は、SSL、セキュリティで保護された電子メール、および証明書ベースの認証のセキュリティを有効にします。

ルート認証局コンテナは、ルート認証局オブジェクトを含むeDirectoryオブジェクトです。

デフォルトのルート認証局コンテナは、CN=trusted roots.CN=securityです。

ルート認証局コンテナの作成方法については、「711ページの「ルート認証局コンテナの作成」」を参照してください。

ルート認証局オブジェクトの作成

ルート認証局オブジェクトは、認証され、有効であると認められたCAのルート認証局証明書を含むeDirectoryオブジェクトです。ルート認証局証明書は、必要に応じてエクスポートして使用することができます。ルート認証局証明書を使用するように設定されたアプリケーションは、ルート認証局コンテナ内のいずれかのCAによって署名された証明書を有効と見なします。

ルート認証局オブジェクトは、ルート認証局コンテナ内に存在する必要があります。

ルート認証局オブジェクトの作成方法については、「712ページの「ルート認証局オブジェクトの作成」」を参照してください。

外部のユーザとサーバ用の証明書の作成

CA管理者は、組織認証局を使用して、eDirectoryの外部のユーザとサーバの証明書に署名できます。このような証明書は、帯域外の方法でCA管理者に提供されるPKCS #10証明書署名要求(CSR)を使用して要求されます。

CSRを受け取ったCA管理者は、iManagerの証明書発行ツールを使用して、証明書を発行できます。この証明書は、eDirectory内のオブジェクトに保存されません。帯域外の方法で要求元に返す必要があります。

証明書の検証

NetIQ Certificate Serverでは、eDirectoryツリー内のすべての証明書の有効性をチェックできます。証明書検証プロセスは、証明書チェーン内の各証明書を、ルート認証局証明書までたどってチェックして、有効または無効のステータスを返します。

- 組織認証局の証明書の有効性をチェックするには、「721 ページの 「組織認証局の証明書の検証」」を参照してください。
- サーバの証明書の有効性をチェックするには、「730 ページの「サーバ証明書の検証」」を参照してください。
- ユーザの証明書の有効性をチェックするには、「736 ページの「ユーザ証明書の検証」」を参照してください。
- ルート認証局の証明書の有効性をチェックするには、「745 ページの 「ルート認証局オブジェクトの検証」」を参照してください。

現在の時刻が証明書の有効期間内であるか、証明書が取り消されていないか、信頼されている認証局によって署名されているかなど、事前定義された一連の条件を証明書が満たすと、その証明書は有効であると見なされます。

外部認証局によって署名されたCN=trusted roots.CN=security内のユーザ証明書または中間CA証明書を検証する場合、証明書検証が成功するためには、その外部認証局の証明書がルート認証局オブジェクト内に保存されている必要があります。

証明書取り消しリストの管理

証明書取り消しリスト(CRL)は、取り消された証明書とその理由の公開されたリストです。

NetIQ Certificate Serverは、CRLを管理するためのシステムを提供します。これはオプションシステムですが、組織認証局によって作成された証明書を取り消せるようにするには、このシステムを実装する必要があります。CRLの管理方法については、「746 ページの 「証明書取り消しリスト(CRL)のタスク」」を参照してください。

NetIQ Certificate Serverのインストール時に、ユーザがCRLコンテナの作成に必要な権利を持っている場合は、CRLコンテナが作成されます。そうでない場合は、インストールが完了してから、適切な権利を持つユーザが手動でCRLコンテナを作成できます。

CRL設定オブジェクトは、CRLコンテナ内に作成できます。オブジェクトには、eDirectoryツリーで使用可能なCRLオブジェクトに関する設定情報が含まれています。通常、ツリーにはCRL設定オブジェクトが1つだけあります。新しい組織認証局を作成またはロールオーバする場合には、複数のCRL設定オブジェクトが必要になりますが、新しい証明書を作成するために使用できるCRL設定オブジェクトは1つだけです。

CRLオブジェクト(配布ポイントとも呼ばれます)は、eDirectoryツリー内の任意のコンテナに作成できます。ただし、NetIQ CRLオブジェクトは通常、CRLコンテナに存在します。CRL設定オブジェクトを作成すると、CRLオブジェクトが自動的に作成されます。CRLオブジェクトには、CRLの詳細情報が記載されたCRLファイルが含まれています。NetIQCRLオブジェクトの場合、サーバが新しい証明書を発行するたびに、CRLファイルは自動的に作成および更新されます。その他のCRLオブジェクトの場合、サードパーティの認証局からCRLファイルをインポートする必要があります。組織認証局を保持するサーバをeDirectory 9.2にアップグレードするとき、アップグレードプロセスがCRL配布ポイントを自動的に作成します。また、eDirectoryでは、RSAとECDSA証明書用の別個のCRL設定オブジェクトが提供されます。

CRL設定オブジェクトは削除できますが、推奨されていません。CRL設定オブジェクトを削除すると、サーバはCRLファイルを作成しなくなります。CRLオブジェクトで指定された場所にCRLファイルがすでに存在する場合は、有効期限が切れるまで、証明書の検証でそのファイルが使用し続けられます。証明書が期限切れになると、CRL配布ポイントでその既存のCRLファイルを参照しているすべての証明書の検証が失敗します。

CRLオブジェクトを削除すると、サーバが次にCRLファイルを生成するときにCRLオブジェクトが再作成されます。iManagerを使用して作成したCRLオブジェクトを削除しそれをインポートする場合、そのオブジェクトは永続的に失われ、そのオブジェクトを参照するすべての証明書は無効と見なされます。

通常、関連する配布ポイントを含む最後の証明書の有効期限が切れてから1日経過するまで、CRLコンテナ、CRL設定オブジェクト、CRLオブジェクト、CRLファイルは削除しません。

秘密鍵と証明書のエクスポート

ユーザ、サーバ、および認証局キーを作成するときに、それらをエクスポート可能としてマークできます。鍵がエクスポート可能な場合、その鍵を抽出し、関連する証明書と一緒にファイルに配置できます。ファイルは、他のプラットフォームに転送可能な業界標準の形式(PFXまたはPKCS #12)で書き込まれます。秘密鍵を保護するため、ファイルはユーザが指定したパスワードで暗号化されます。

秘密鍵と証明書をエクスポートして、鍵のバックアップコピーを取ったり、鍵を別のサーバに移動したり、またはサーバ間で鍵を共有したりできます。

秘密鍵と証明書をエクスポートする方法の詳細については、735 ページの 「ユーザ証明書と秘密鍵のエクスポート」を参照してください。

秘密鍵と証明書のインポート

サーバ証明書、ユーザ証明書、または認証局オブジェクトの作成時に、新しい鍵を作成するのではなく鍵をインポートすることもできます。鍵とそれに関連付けられた証明書は、PFXまたはPKCS #12形式である必要があります。

認証局オブジェクトをサーバの障害から回復するため、1つのサーバから別のサーバに組織認証局を移動するため、または別の認証局に従属する認証局のために、新しい鍵を作成するのではなく、鍵をインポートすることもできます。

ユーザ証明書または秘密鍵がサードパーティ認証局によって署名されている場合でも、インポートすることができます。

サーバ証明書オブジェクトをサーバの障害から回復するため、鍵と証明書を別のサーバに移動するため、または別のサーバと鍵と証明書を共有するために、新しい鍵を作成するのではなく、鍵をインポートすることもできます。

SASサービスオブジェクトの作成

SASサービスオブジェクトは、サーバとサーバ証明書間の通信を容易にします。サーバをeDirectoryツリーから削除する場合は、サーバに関連付けられたSASサービスオブジェクトを削除する必要があります。サーバをツリーに戻す場合は、そのサーバに属するSASサービスオブジェクトを作成する必要があります。ツリーに戻さない場合は、新しいサーバ証明書を作成することはできません。

SASサービスオブジェクトは、サーバヘルスチェックの一部として自動的に作成されます。このオブジェクトを手動で作成する必要はありません。

新しいSASサービスオブジェクトを作成できるのは、サーバオブジェクトと同じコンテナ内に、正しく名付けられたSASサービスオブジェクトが存在しない場合だけです。たとえば、「WAKE」と名付けられたサーバでは、「SASサービス-WAKE」と名付けられたSASサービスオブジェクトが作成されます。ユーティリティでは、サーバオブジェクトからSASオブジェクトまでのDSポインタ、およびSASオブジェクトからサーバオブジェクトまでのDSポインタが追加されます。また、SASサービスオブジェクト上に正しいACLエントリが設定されます。

SASサービスオブジェクトがすでに正しい名前で存在する場合、新しいSASサービスオブジェクトを作成することはできません。古いSASサービスオブジェクトのDSポインタは、誤っていたり見つからなかったりする場合があります。または、ACLが適切でない場合もあります。この場合、破損したSASサービスオブジェクトを削除し、iManagerを使用して新しいSASサービスオブジェクトを作成できます。このサーバに属するサーバ証明書がある場合、［**その他**］タブを使用して、サーバ証明書をSASサービスオブジェクトへ手動でリンクする必要があります。

SASサービスオブジェクトを作成する方法の詳細については、712ページの「SASサービスオブジェクトの作成」を参照してください。

Novell International Cryptographic Infrastructure

NICI (Novell International Cryptographic Infrastructure)は、NetIQ Certificate Server、NMAS (NetIQモジュラー認証サービス)、およびその他のアプリケーションに暗号化を提供する、基盤となる暗号化インフラストラクチャです。

NetIQ Certificate Serverを正しく機能させるために、サーバにNICIをインストールする必要があります。NICIは、NetIQ Certificate Serverには付属していません。大抵、NetIQ Certificate ServerがOpen Enterprise Server (OES)やeDirectoryなどの別の製品にバンドルされる場合に、NICIの提供およびインストールが行われます。新しいバージョンのNICIを必要とする場合、NetIQダウンロードWebサイトからをダウンロードできます。

NetIQ Certificate Serverの設定

NetIQ Certificate Serverをインストールした後、次のタスクを実行して、ネットワーク上で使用できるように設定する必要があります。

- 703 ページの 「使用する認証局のタイプの決定」
- 704 ページの 「組織の認証局オブジェクトを作成する」
- 706 ページの 「従属認証局」
- 709 ページの 「認証局オブジェクトの作成に関する制限事項」
- 709 ページの 「Suite Bモードでの認証局の設定」
- 709 ページの 「サーバ証明書オブジェクトを作成する」
- 711 ページの 「暗号化対応アプリケーションの設定」
- 711 ページの 「追加コンポーネントの設定」

使用する認証局のタイプの決定

NetIQ Certificate Serverでは、サーバとエンドユーザの両方の証明書を作成できます。組織認証局または外部(サードパーティ)認証局のいずれかによって、サーバ証明書に署名できます。ユーザ証明書への署名は組織認証局でしかできませんが、PKCS#12形式でサードパーティ認証局によって署名されたユーザ証明書をインポートすることもできます。

サーバ証明書オブジェクトの作成プロセス中に、サーバ証明書オブジェクトに署名する認証局のタイプを尋ねられます。

組織認証局は組織固有のものであり、署名操作には組織固有の公開鍵を使用します。秘密鍵は、組織認証局を作成するときに作成されます。

サードパーティ認証局は、eDirectoryツリーの外部でサードパーティによって管理されます。サードパーティ認証局の例として、VeriSignがあります。

認証局の両方のタイプを同時に使用できます。認証局の1つのタイプを使用しても、もう一方を使用できなくなることはありません。

- 704 ページの 「NetIQ Certificate Serverで提供される組織認証局を使用することの利点」
- 704 ページの 「外部認証局を使用することの利点」

NetIQ Certificate Serverで提供される組織認証局を使用することの利点

- **互換性。** 組織認証局は、LDAPサービスなどのNetIQやNovellのアプリケーションと互換性があります。組織認証局によって発行される証明書は、X.509 v3に準拠しており、サードパーティ製のアプリケーションでも使用できます。
- **認証局のコスト削減。** 組織認証局では、コストをかけずにいくらでも公開鍵証明書を作成できます。外部の認証局で単一の公開鍵証明書を取得しようとすると、かなりの費用がかかる可能性があります。
- **すべて揃った互換性のあるソリューションのコンポーネント。** 組織認証局を使用すると、どんな外部サービスにも依存せずに、eDirectoryに組み込まれた完全な暗号化システムを使用できます。さらに、NetIQ Certificate Serverは、さまざまなNetIQまたはNovell製品と互換性があります。
- **証明書の属性およびコンテンツ制御。** 組織認証局は、ネットワーク管理者によって管理されます。ネットワーク管理者は、証明書の有効期間、キーサイズ、署名アルゴリズムなどの公開鍵証明書の属性を決定します。
- **簡単な管理。** 組織認証局は、追加コストや複雑な手順なしに、外部認証局と同様の機能を実行します。

外部認証局を使用することの利点

- **法的責任。** 外部認証局の過失により、秘密鍵が漏洩したり、公開鍵証明書が改ざんされたりした場合に、その認証局が賠償責任を負う可能性があります。
- **可用性。** 外部認証局の証明書は、eDirectoryの外部アプリケーションでも幅広く利用可能で信頼される可能性があります。

組織の認証局オブジェクトを作成する

デフォルトでは、NetIQ Certificate Serverのインストールプロセスで、組織認証局(CA)が作成されます。組織認証局の名前を指定するように求められます。［**完了**］クリックすると、組織認証局がデフォルトのパラメータで作成され、セキュリティコンテナに配置されます。

組織認証局の作成をより細かく制御する場合は、iManagerを使用して組織認証局を手動で作成できます。また、組織認証局を削除した場合、それを再作成する必要があります。

作成プロセス時に、組織認証局オブジェクトの名前を付け、組織認証局サービスをホストするサーバ(組織認証局サービスが実行されるサーバ)を選択するよう求められます。組織認証局サービスをホストするサーバを決定する際、次の点を考慮します。

- 物理的に安全なサーバを選択します。

  認証局サーバへの物理的アクセスは、システムのセキュリティ上、重要な部分になります。認証局サーバが侵害されると、その認証局によって発行されたすべての証明書も侵害されます。
- 可用性、安定性、および堅牢性の高いサーバを選択します。

  認証局サービスが使用できない場合、証明書は作成できません。証明書はインストール時に作成される必要があるため、これは新しいサーバのインストールに影響します。
- 信頼できるソフトウェアのみが実行されているサーバを選択します。

  不明なまたは不審なソフトウェアを実行していると、認証局サービスが侵害される可能性があります。

- ツリーから削除されないサーバを選択します。

  サーバがツリーから削除されると、認証局を削除する前に取ったバックアップを使用して認証局オブジェクトを再作成するか、新しい認証局を作成する必要があります。新しい認証局を作成する場合、既存のサーバとユーザ証明書を置換する必要があります。
- ツリー内の他のサーバと互換性があるプロトコルを実行しているサーバを選択します。

  たとえば、IPです。
- ECDSA証明書で組織認証局を作成します。

組織認証局オブジェクトを作成するには、次の手順を実行します。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
3. ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**認証局の環境設定**］の順にクリックします。

   組織の認証局オブジェクトが存在しない場合、［Create an Organizational Certificate Authority Object］ダイアログボックスとオブジェクトを作成するウィザードが開きます。メッセージに従ってオブジェクトを作成します。ダイアログボックスまたはウィザードページの具体的な説明については、［ヘルプ］をクリックしてください。

   注: ここで指定するCRLファイルパスが、eDirectoryインストールパスと対応していることを確認します。
4. 認証局の作成を完了したら、認証局の公開鍵/秘密鍵のペアのバックアップを作成し、安全な場所に保存することをお勧めします。詳細については、717 ページの 「組織認証局のバックアップ」を参照してください。

注: eDirectoryツリーは組織の認証局を1つしか格納できません。

eDirectoryでは、管理者は、デフォルトのサーバ証明書が生成されるときに使用されるRSA鍵のサイズ、楕円曲線、および証明書を指定できます。認証局オブジェクトの次の3つの属性を使用して、これらのパラメータを指定できます。

- **ndspkiDefaultRSAKeySize:** RSAサーバ証明書の鍵サイズを指定します。このフィールドでは、最大で8192ビットRSA暗号化まで指定できます。

  重要: TLS接続を確立するために8KビットRSA公開鍵のX.509証明書を使用すると、eDirectoryサーバのパフォーマンスに影響します。NetIQでは、8Kビット鍵のRSA証明書を使用するようeDirectoryサーバを構成することを推奨していません。TLSセッションを確立する処理はサーバでの計算量が多くなり、複数のTLSセッションが同時に確立されるとシステムが大幅に低下する可能性があるためです。
- **ndspkiDefaultECCurve:** サーバ証明書のEC制限の曲線を指定します。次のいずれかのECを指定できます。
  - P256
  - P384
  - P521

- **ndspkiDefaultCertificateLife:** デフォルトのサーバ証明書の証明書有効期限を指定します。年単位でサーバ証明書有効期限を指定できます。たとえば、このフィールドに4と指定すると、サーバ証明書有効期限は4年間に設定されます。証明書サーバは、デフォルトのサーバ証明書の最小の有効期間が1年間であることと、最大の有効期間がCAの期限を超えていないことを確認します。

注

- ndspkiDefaultCertificateLife属性は、サーバ証明書にのみ適用できます。
- 新しいeDirectoryサーバを設定する際に古いデフォルト値を渡すと、上記のパラメータは未設定のままになります。
- 上記のパラメータは、既存のデフォルト証明書には影響しません。認証局にこれらのパラメータを指定した後にeDirectoryサーバを9.2にアップグレードする場合、既存のデフォルトサーバ証明書は再作成されません。

新しいeDirectoryツリーを設定する際にこれらのパラメータを指定すると、組織認証局証明書もこれらのパラメータを使用して作成されます。詳細については、『NetIQ eDirectory Installation Guide (NetIQ eDirectoryインストールガイド)』を参照してください。

従属認証局

NetIQ Certificate Serverに、従属認証局のサポートが追加されました。この機能によって、組織認証局をサードパーティ認証局または別のeDirectoryツリーにある認証局のいずれかに従属させることができます。eDirectoryツリーには、組織認証局を1つしか格納できません。

従属認証局を使用する次のような理由があります。

- 組織認証局を既存のサードパーティPKIの一部にすることができます。
- 複数のツリーで、共通のPKIのルート認証局(または信頼アンカー)を共有することができます。
- 認証局をより安全なシステム上に配置することにより、ルート認証局のセキュリティを向上させることができます。
- より緊密に管理されているツリー内にルート認証局を配置することにより、リスクを低減します(たとえば、不正管理者または不正ユーザから保護されているツリー)。

- 706 ページの 「従属認証局の作成」
- 707 ページの 「従属認証局のPKCS #12ファイルの作成」

従属認証局の作成

従属認証局を作成するには、既存の組織認証局を最初に削除する必要があります(721 ページの 「組織認証局の削除」を参照してください)。従属認証局の公開鍵/秘密鍵と証明書チェーンが格納されているPKCS#12ファイルが存在している必要があります。サードパーティ認証局から直接このファイルを取得できます。また、このファイルを作成する方法については、707 ページの 「従属認証局のPKCS#12ファイルの作成」を参照してください。従属認証局を作成するには、iManagerでツリーに接続して認証局の設定タスクを実行し、［インポート］作成方法を使用します。

従属認証局のPKCS #12ファイルの作成

1 サーバ証明書オブジェクト(またはKMO)およびECDSAとRSAキーでPKCS #10 CSRを作成します。

1a iManagerを起動します。

1b ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**サーバ証明書の作成**］の順にクリックします。

1c 認証局をホストするサーバを選択し、証明書のニックネームを指定します。［カスタム］作成方法を選択して［**次へ**］をクリックします。

1d ［**External Certificate Authority**］を選択して、［**次へ**］をクリックします。

1e アルゴリズムおよびキーサイズを選択し、［**秘密鍵のエクスポートを許可**］が選択されていることを確認して、［**次へ**］をクリックします。

重要: eDirectory環境でRSAとECDSAの両方の証明書を使用する場合、使用する証明書ごとにこの手順を繰り返します。NetIQでは、RSAでは2048ビット、ECDSAでは384ビットのキーサイズを使用することをお勧めします。

1f ［**サブジェクト名**］フィールドの右側にある［**編集**］ボタンをクリックして、従属認証局とツリーを表すように［**サブジェクト名**］を編集し、署名アルゴリズムを選択します(NetIQでは、SHA-1より強力なアルゴリズムを使用することをお勧めします)。それから［**次へ**］をクリックします。

1g 概要が正しいことを確認し、［**完了**］をクリックします。

1h ［**証明書署名要求の保存**］をクリックし、プロンプトに従ってCSRをファイルに保存します。

2 CSRに署名を行い証明書を作成します。

2a 従属認証局がサードパーティPKIの一部である場合、サードパーティ認証局にCSRから証明書を作成させます。

または

従属認証局が別のeDirectoryツリー内の認証局によって署名される場合は、ステップ 2b から続行します。

注: ECDSAの場合、CSRはECDSA CAでしか署名できません。

2b iManagerを起動します。

2c ［**役割およびタスク**］メニューで［**NetIQ Certificate Server**］>［**証明書の発行**］の順にクリックします。

2d CSRを含むファイルを選択し、［**次へ**］をクリックします。

2e ［**認証局**］の鍵のタイプを選択し、［**拡張されたキーの使用目的を有効にする**］を選択解除し、［**次へ**］をクリックします。

2f 認証局の証明書タイプを選択し、［**指定なし**］または［**SpecificPath**］長のいずれかを選択して、［**次へ**］をクリックします。

2g サブジェクト名を確認し、必要に応じて編集します。有効期限(推奨は5〜10年です)を指定し、［**次へ**］をクリックします。

2h 証明書の形式を選択し、［**次へ**］をクリックします。

2i 完了をクリックします。

2j ［発行された証明書をダウンロードしてください。］をクリックし、プロンプトに従って証明書を保存します。

3 認証局証明書を取得します。

3a 従属認証局がサードパーティPKIの一部になる場合、サードパーティから認証局証明書を取得します。

または

従属認証局が別のeDirectoryツリー内の認証局によって署名される場合は、ステップ 3bから続行します。

3b iManagerを起動します。

3c ［役割およびタスク］メニューで、［NetIQ Certificate Server］>［認証局の設定］の順にクリックします。

3d ［証明書］タブをクリックして、［自己署名証明書］を選択します。

3e エクスポートをクリックします。

3f 秘密鍵をエクスポートせずに証明書の形式を選択し、［次へ］をクリックします。

3g ［Save the Exported Certificate to a File］をクリックし、プロンプトに従って証明書を保存します。

4 証明書をサーバ証明書オブジェクト(またはKMO)にインポートします。

4a iManagerを起動します。

4b ［役割およびタスク］メニューで、［NetIQ証明書アクセス］>［サーバ証明書］の順にクリックします。

4c 認証局をホストするサーバを選択します。

4d ステップ 1で作成したサーバ証明書オブジェクト(またはKMO)を選択し、［インポート］をクリックします。

4e ステップ 2およびステップ 3で取得した証明書を格納している2つのファイルを選択し、［OK］をクリックします。

重要: eDirectory環境でRSAとECDSAの両方の証明書を使用する場合、使用する証明書ごとにこの手順を繰り返します。

---

5 PKCS #12ファイルに公開鍵/秘密鍵をエクスポートします。

5a ステップ 4eから操作を続け、［エクスポート］をクリックして、秘密鍵を含めることを選択し、［次へ］をクリックします。

5b ［Save the Exported Certificate to a File］をクリックし、プロンプトに従ってPKCS#12ファイルを保存します。

5c このファイルのコピーを作成し、パスワードと一緒に安全な場所に保存します。

6 (オプション)サーバ証明書オブジェクト(またはKMO)を削除します。

7 組織認証局を削除します。詳細については、721 ページの 「組織認証局の削除」を参照してください。

8 サブ認証局証明書と秘密鍵をPKCS #12ファイルからインポートします。詳細については、719 ページの 「組織認証局の復元」を参照してください。

認証局オブジェクトの作成に関する制限事項

eDirectory 9.0以降では、認証局のRSAとECの両方の証明書をサポートします。RSAおよびEC証明書で認証局オブジェクトを作成する際に、次の考慮事項が適用されます。

- RSAおよびEC証明書のサブジェクト名は同じである必要があります。
- RSAとE**C**Aは、混合モードにはできません。RSAとE**C**Aは、ルート認証局またはサブ認証局のいずれかとして使用できます。たとえば、RSACAをルート認証局として使用し、ECCAをサブCAとして使用することはできません。またその逆も同様です。
- eDirectoryでは、eDirectory外部のサードパーティアプリケーションで生成された自己署名認証局証明書をインポートすることはできません。

Suite Bモードでの認証局の設定

Suite Bモードで認証局を設定する前に、認証局がホストされているサーバに、NICI 3.0がインストールされていること、Enhanced Background Authenticationを実行するように設定がなされていることを確認します。

Suite Bモードで動作するように認証局を設定するには、次の手順を実行します。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。
3. ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**認証局の環境設定**］の順にクリックします。
4. ［**Enable Suite B Mode**］を選択します。
5. ［**OK**］をクリックします。

認証局がSuite Bモードのとき、証明書サーバはRSA証明書を作成できません。どのECDSA証明書がサポートされているかについては、696 ページの 「NetIQ Certificate Serverのコンポーネント」を参照してください。

Suite Bで設定されているeDirectory 9.0以降のツリーにeDirectoryの旧バージョンを使用するサーバを追加する場合、サーバにSuite B機能がないため、証明書サーバはそのサーバの証明書を作成しません。これらのサーバでSuite B機能を有効にするには、サーバをeDirectory 9.0以降にアップグレードする必要があります。

サーバ証明書オブジェクトを作成する

サーバ証明書オブジェクトは、サーバのeDirectoryオブジェクトを格納するコンテナに作成されます。必要に応じて、サーバ上にある暗号化対応アプリケーションごとに別個のサーバ証明書オブジェクトを作成することも、そのサーバで使用するすべてのアプリケーションに対して1つのサーバ証明書オブジェクトを作成することもできます。

注: サーバ証明書オブジェクトと暗号化キーオブジェクト(KMO)は同じ意味です。eDirectoryオブジェクトのスキーマ名はNDSPKI:暗号化キーです。

証明書サーバをインストールすると、eDirectoryはデフォルトパラメータで、サーバ証明書オブジェクトを自動的に作成し、ターゲットサーバが存在するコンテナに配置します。デフォルト証明書を上書きまたは新しく作成する必要がある場合は、［デフォルト証明書の作成］ウィザードを使用できます。詳細については、723 ページの 「デフォルトのサーバ証明書オブジェクトを作成する」を参照してください。

サーバ証明書オブジェクトの作成をより細かく制御する場合は、サーバ証明書オブジェクトを手動で作成できます。追加のサーバ証明書オブジェクトを作成することもできます。

- 710 ページの 「サーバ証明書オブジェクトを手動で作成する」
- 710 ページの 「サーバ証明書の作成に関するヒント」

サーバ証明書オブジェクトを手動で作成する

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
3. ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**サーバ証明書の作成**］の順にクリックします。

   この操作により、［Create a Server Certificate］ダイアログボックスと、サーバ証明書オブジェクトを作成する対応するウィザードが開きます。メッセージに従ってオブジェクトを作成します。ダイアログボックスまたはウィザードページの具体的な説明については、［**ヘルプ**］をクリックしてください。

サーバ証明書の作成に関するヒント

サーバ証明書オブジェクトの作成プロセス中に、鍵ペアの名前を指定し、鍵ペアを関連付けるサーバを選択するよう求められます。サーバ証明書オブジェクトは、NetIQ Certificate Serverによって生成され、その名前は選択した鍵ペアの名前に基づきます。

［カスタム］作成方法を選択する場合も、サーバ証明書オブジェクトを、組織の組織認証局または外部認証局のいずれで署名するか指定するよう求められます。この決定方法の詳細については、703 ページの 「使用する認証局のタイプの決定」を参照してください。

組織の組織認証局を使用する場合、サーバ証明書オブジェクトが関連付けられているサーバが、組織認証局をホストするサーバと通信できるようにするか、またはそのサーバと同じである必要があります。これらのサーバでは、同じプロトコル(IP)を実行している必要があります。

外部認証局を使用して証明書に署名する場合は、サーバ証明書オブジェクトが関連付けられているサーバによって、外部認証局に送信する必要がある証明書署名要求が生成されます。

証明書が署名されて返されたら、外部認証局のルート認証局と一緒に、それをサーバ証明書オブジェクトにインストールする必要があります。

サーバ証明書オブジェクトを作成した後、これを使用するアプリケーションを設定できます。(参照先711 ページの 「暗号化対応アプリケーションの設定」.) アプリケーションの設定では、鍵は、サーバ証明書オブジェクトを作成したときに入力した鍵ペアの名前で参照されます。

暗号化対応アプリケーションの設定

NetIQ Certificate Serverを設定した後、個々の暗号化対応アプリケーションを設定して、作成したカスタム証明書を使用できるようにする必要があります。設定手順は個々のアプリケーションに固有のものであるため、具体的な手順についてはアプリケーションのマニュアルを参照することをお勧めします。

追加コンポーネントの設定

NetIQ Certificate Serverには、設定すれば追加機能を提供できる追加コンポーネントが含まれています。

- 711 ページの 「ユーザ証明書の作成」
- 711 ページの 「ルート認証局コンテナの作成」
- 712 ページの 「ルート認証局オブジェクトの作成」
- 712 ページの 「SASサービスオブジェクトの作成」

ユーザ証明書の作成

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**ユーザ証明書の作成**］の順にクリックします。

この操作により、ユーザ証明書の作成を支援するウィザードが開きます。メッセージに従ってオブジェクトを作成します。ウィザードの各ページに関する特定の情報については、［**ヘルプ**］をクリックします。

ルート認証局コンテナの作成

eDirectoryツリーの任意の場所に、ルート認証局コンテナを作成できます。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQCertificateServer**］>［**ルート認証局コンテナの作成**］の順にクリックします。

4 ルート認証局コンテナの名前を指定します。

5 ルート認証局コンテナのコンテキストをブラウズして選択します。

6 ［**OK**］をクリックします。

注: 複数のアプリケーションで、ルート認証局コンテナに特定の名前を指定し、eDirectoryツリーの特定の場所に配置することが必要になる場合があります。NetIQ Certificate Serverでは、ルート認証局コンテナの名前を「ルート認証局」とし、セキュリティコンテナに配置する必要がありま

す。このコンテナ内の証明書は、外部認証局によって署名されたユーザ証明書と、ルート認証局オブジェクトに保存される中間認証局証明書を検証するために使用されます。サーバ証明書と組織認証局証明書は、独自のオブジェクトに保存されている証明書チェーンを使用します。

ルート認証局オブジェクトの作成

ルート認証局オブジェクトは、ルート認証局コンテナにのみ格納できます。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**ルート認証局の作成**］の順にクリックします。

この操作によって、ルート認証局オブジェクトを作成するための［Create a Trusted Root Object］ウィザードが開きます。メッセージに従ってオブジェクトを作成します。ウィザードの各ページに関する特定の情報については、［**ヘルプ**］をクリックします。

注: ルート認証局オブジェクトには、すべてのタイプの証明書を保存できます(認証局証明書、中間認証局証明書、またはユーザ証明書)。

SASサービスオブジェクトの作成

SASサービスオブジェクトは、サーバヘルスチェックの一部として自動的に作成されます。このオブジェクトを手動で作成する必要はありません。手動で作成する必要がある場合、次の手順を実行します。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQCertificateServer**］>［**CreateSASServiceObject**］の順にクリックします。

この操作によって、SASサービスオブジェクトを作成するための［SASサービスオブジェクトの作成］ウィザードが開きます。メッセージに従ってオブジェクトを作成します。ウィザードの各ページに関する特定の情報については、［**ヘルプ**］をクリックします。

NetIQ Certificate Serverの管理

システム管理者として、NetIQ Certificate Serverで提供される公開鍵暗号化サービスを維持するためにいくつかのタスクを実行する必要があります。iManagerを使用して、これらのタスクを実行します。このセクションでは、各タスクの実行に関する簡単な概略と具体的な情報を提供します。

認証局のタスク:

- 715 ページの 「組織の認証局オブジェクトを作成する」
- 715 ページの 「公開鍵証明書の発行」

- 716 ページの 「組織認証局のプロパティの表示」
- 716 ページの 「組織認証局の公開鍵証明書プロパティの表示」
- 716 ページの 「認証局の自己署名証明書プロパティの表示」
- 717 ページの 「組織認証局の自己署名証明書のエクスポート」
- 717 ページの 「組織認証局のバックアップ」
- 719 ページの 「組織認証局の復元」
- 720 ページの 「組織認証局の別のサーバへの移動」
- 721 ページの 「組織認証局の証明書の検証」
- 721 ページの 「組織認証局の削除」
- 722 ページの 「組織認証局のロールオーバー」

サーバ証明書オブジェクトのタスク:

- 723 ページの 「サーバ証明書オブジェクトを作成する」
- 723 ページの 「デフォルトのサーバ証明書オブジェクトを作成する」
- 724 ページの 「サーバ証明書オブジェクトへの公開鍵証明書のインポート」
- 725 ページの 「ルート認証局または公開鍵証明書のエクスポート」
- 726 ページの 「サーバ証明書オブジェクトの削除」
- 727 ページの 「サーバ証明書オブジェクトのプロパティの表示」
- 727 ページの 「サーバ証明書オブジェクトの公開鍵証明書プロパティの表示」
- 728 ページの 「サーバ証明書オブジェクトのルート認証局証明書プロパティの表示」
- 728 ページの 「サーバ証明書オブジェクトのバックアップ」
- 729 ページの 「サーバ証明書オブジェクトの復元」
- 730 ページの 「サーバ証明書オブジェクトとクラスタリング」
- 730 ページの 「サーバ証明書の検証」
- 731 ページの 「ルート認証局または自己署名証明書の取り消し」
- 732 ページの 「別のサーバへのサーバ証明書オブジェクトの移動」
- 732 ページの 「サーバ証明書オブジェクトのキーマテリアルの置換」

ユーザ証明書のタスク:

- 733 ページの 「ユーザ証明書の作成」
- 733 ページの 「ユーザ証明書の一括作成」
- 734 ページの 「ユーザオブジェクトへの公開鍵証明書のインポート(秘密鍵は省略可)」
- 734 ページの 「ユーザ証明書のプロパティの表示」
- 735 ページの 「ユーザ証明書のエクスポート」
- 735 ページの 「ユーザ証明書と秘密鍵のエクスポート」
- 736 ページの 「ユーザ証明書の検証」
- 737 ページの 「ユーザ証明書の取り消し」
- 737 ページの 「ユーザ証明書と秘密鍵の削除」

X.509証明書の自己プロビジョニング:

- 738 ページの 「概要」
- 739 ページの 「ユーザ自己プロビジョニング」
- 740 ページの 「サーバ自己プロビジョニング」
- 741 ページの 「証明書の自己プロビジョニングと証明書の発行タスク」

外部アプリケーションでのeDirectory証明書の使用

- 742 ページの 「PKIヘルスチェック機能」
- 743 ページの 「eDirectory証明書をエクスポートするためのSAS:Serviceオブジェクトの設定」

ルート認証局オブジェクトのタスク:

- 699 ページの 「ルート認証局コンテナの作成」
- 700 ページの 「ルート認証局オブジェクトの作成」
- 744 ページの 「ルート認証局オブジェクトのプロパティの表示」
- 745 ページの 「ルート認証局証明書の置き換え」
- 745 ページの 「ルート認証局オブジェクトの検証」
- 746 ページの 「ルート認証局証明書の取り消し」

証明書取り消しリスト(CRL)のタスク:

- 747 ページの 「手動によるCRLコンテナの作成」
- 747 ページの 「CRLコンテナの削除」
- 748 ページの 「CRL設定オブジェクトの作成」
- 748 ページの 「CRL設定オブジェクトのアクティブ化」
- 749 ページの 「CRL設定オブジェクトのプロパティの表示と変更」
- 751 ページの 「CRL設定オブジェクトの削除」
- 751 ページの 「CRLオブジェクトの作成」
- 752 ページの 「CRLファイルのエクスポート」
- 752 ページの 「CRLファイルの置き換え」
- 753 ページの 「CRLオブジェクトのプロパティの表示」
- 754 ページの 「CRLオブジェクトの削除」

eDirectoryタスク:

- 755ページの 「複数のセキュリティコンテナ、組織認証局、KAPコンテナ、およびW0オブジェクトの解決」
- 755 ページの 「セキュリティコンテナの復元または再作成」
- 756 ページの 「KAPおよびW0の復元または再作成」

アプリケーションのタスク

認証局のタスク

組織の認証局オブジェクトを作成する

このタスクについては、704 ページの 「組織の認証局オブジェクトを作成する」で説明されています。

公開鍵証明書の発行

このタスクでは、サーバ証明書オブジェクトを認識しない暗号化対応アプリケーション用の証明書を生成できます。

組織認証局は、外部認証局と同じ方法で機能します。つまり、証明書署名要求(CSR)から証明書を発行する機能があります。ユーザが署名のためにCSRを送信してきたら、組織認証局を使用して証明書を発行できます。証明書を要求したユーザは、発行された証明書を取得し、暗号化対応アプリケーションに直接インポートします。

公開鍵証明書を発行するには、次の手順を実行します。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
3. ［**役割およびタスク**］メニューで［**NetIQ Certificate Server**］>［**証明書の発行**］の順にクリックします。
4. ［**参照**］ボタンを使用してCSRファイルを見つけ、ファイルを開き、［**次へ**］をクリックします。
5. 鍵のタイプ、鍵の使用方法、および拡張鍵の使用法を指定し、［**次へ**］をクリックします。
6. 証明書の基本制約を指定して、［**次へ**］をクリックします。
7. サブジェクト名、有効期間、有効開始日と有効期限日、および任意のカスタム拡張機能を指定し、［**次へ**］をクリックします。

8 パラメータシートを確認します。正しい場合は、［**完了**］をクリックします。正しくない場合は、変更が必要な箇所まで［**戻る**］をクリックして戻ります。

［**完了**］をクリックすると、証明書が作成されたというメッセージがダイアログボックスに表示されます。Base64形式でシステムクリップボードに、Base64形式のファイルに、またはバイナリDER形式のファイルに証明書を保存できます。［**詳細**］をクリックして、発行された証明書に関する詳細を表示することもできます。

組織認証局のプロパティの表示

任意のeDirectoryオブジェクトで表示できるeDirectoryの権利とプロパティに加え、組織認証局に固有のプロパティ(それに関連付けられた公開鍵証明書や自己署名証明書のプロパティなど)を表示することもできます。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**認証局の設定**］の順にクリックします。

この操作により、組織認証局のプロパティページが表示され、全般ページ、CRLページ、証明書ページが表示されます。

4 表示するタブをクリックします。

組織認証局の公開鍵証明書プロパティの表示

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**認証局の設定**］の順にクリックします。

この操作により、組織認証局のプロパティページが表示され、全般ページ、CRLページ、証明書ページ、その他のeDirectory関連のページが表示されます。

4 ［**証明書**］をクリックして、表示する公開鍵証明書のニックネームをクリックします。

5 証明書チェーンを表示するには、証明書のニックネームの前にあるプラス記号(+)をクリックしてビューを展開します。

6 ［**閉じる**］をクリックします。

認証局の自己署名証明書プロパティの表示

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**認証局の設定**］の順にクリックします。

この操作により、組織認証局のプロパティページが表示され、全般ページ、CRLページ、証明書ページが表示されます。

4 ［**証明書**］をクリックして、表示する自己署名証明書のニックネームをクリックします。

従属認証局の場合、自己署名証明書はありません。

5 証明書チェーンを表示するには、証明書のニックネームの前にあるプラス記号(+)をクリックしてビューを展開します。

6 ［**閉じる**］をクリックします。

組織認証局の自己署名証明書のエクスポート

自己署名証明書は、組織認証局の識別情報と、組織認証局によって署名された証明書の有効性を確認するために使用できます。

組織認証局のプロパティページでは、このオブジェクトに関連付けられた証明書とプロパティを参照できます。［自己署名証明書］プロパティページでは、自己署名証明書を、暗号化対応のアプリケーションで使用するファイルにエクスポートできます。

組織の認証局に存在する自己署名証明書は、組織の認証局によって署名された証明書を持つサーバ証明書オブジェクトのルート認証局証明書と同じものです。組織認証局の自己署名証明書をルート認証局として認識するサービスでは、組織認証局によって署名された有効なユーザやサーバを許可できます。

このタスクは、認証局が従属認証局の場合、適用されません。

組織認証局の自己署名証明書をエクスポートするには、次の手順を実行します。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**認証局の設定**］の順にクリックします。

この操作により、組織認証局のプロパティページが表示され、全般ページ、CRLページ、証明書ページ、その他のeDirectory関連のページが表示されます。

4 ［**証明書**］をクリックして、自己署名証明書を選択します。

5 ［**エクスポート**］をクリックして、証明書をエクスポートするプロンプトに従います。

この操作により、［証明書のエクスポート］ウィザードが起動します。［**秘密鍵のエクスポート**］チェックボックスが選択されていない(チェックマークが付いていない)ことを確認します。

6 ［**完了**］をクリックします。

組織認証局のバックアップ

NetIQでは、組織認証局のホストサーバで回復不能な障害が発生する場合に備え、組織認証局の秘密鍵と証明書をバックアップしておくことをお勧めします。障害が発生した場合、バックアップファイルを使用して、組織認証局をツリー内の任意のサーバに復元できます。

注: 組織認証局をバックアップする機能は、NetIQ Certificate Serverバージョン9.0以上で作成された組織認証局に対してのみ使用できます。証明書サーバの以前のバージョンでは、組織認証局の秘密鍵は、エクスポートできない方法で作成されていました。

バックアップファイルには、認証局の秘密鍵、自己署名証明書、公開鍵証明書、およびこの操作に必要とされるいくつかの他の証明書が含まれています。この情報は、PKCS#12形式(PFXとも呼ばれます)で保存されます。

組織認証局が正常に機能しているときに、組織認証局をバックアップする必要があります。

NetIQ Certificate Server 9.0以降で認証局を完全にバックアップするには、CRLデータベースと発行済み証明書データベースをバックアップする必要があります。

その他のプラットフォームでは、これらのデータベースは両方とも、eDirectory dibファイルと同じディレクトリにあります。これらの場所のデフォルト値は次のとおりです。

- Windowsの場合: c:\novell\nds\dibfiles
- Linuxの場合: /var/opt/novell/edirectory/data/dib

これらのデフォルト値は、eDirectoryのインストール時に変更できます。

CRLデータベースのバックアップ対象ファイルは、crl.db、crl.01、およびcrl.rflディレクトリです。発行済み証明書データベースのバックアップ対象ファイルは、cert.db、cert.lck、cert.01、およびcert.rflディレクトリです。

eDirectory dibディレクトリは、標準および通常バックアップ計画の一部に含める必要があります。

組織認証局をバックアップするには、次の手順を実行します。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
3. ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**認証局の設定**］の順にクリックします。
4. ［**証明書**］をクリックして、［**自己署名証明書**］または［**公開鍵証明書**］のいずれかを選択します。証明書は両方とも、バックアップ操作中にファイルに書き込まれます。

   NetIQでは、RSAとECDSA証明書の［**自己署名証明書**］を別個に選択することをお勧めします。
5. ［**エクスポート**］をクリックします。

   この操作により、証明書をファイルにエクスポートするためのウィザードが開きます。
6. 秘密鍵のエクスポートを選択して、6文字以上の英数字でPFXファイルの暗号化に使用するパスワードを指定し、［**次へ**］をクリックします。
7. ［**Save the Exported Certificate to a File**］リンクをクリックし、ファイル名およびバックアップファイルを保存する場所を指定します。
8. ［**保存**］をクリックします。
9. ［**閉じる**］をクリックします。

   暗号化されたバックアップファイルは、指定した場所に書き込まれます。これで、緊急用に、ファイルを安全な場所に保存する準備ができました。

重要: エクスポートしたファイルは、バックアップメディアに配置し、安全な場所に保存する必要があります。ファイルの暗号化に使用するパスワードは記憶するか、または必要なときに確実に使用でき、かつ他のユーザにはアクセスできない安全な場所に保存しておく必要があります。

組織認証局の復元

組織認証局オブジェクトが削除されたまたは破損した場合、あるいは組織認証局のホストサーバに回復不能な障害が発生した場合、717 ページの 「組織認証局のバックアップ」で作成したバックアップファイルを使用して、完全に復元することができます。

注: 組織認証局のバックアップを作成できなかった場合、NICI 2.*x*がサーバにインストールされ、NICI設定情報のバックアップが作成されているならば、組織認証局を復元できる可能性があります。

NetIQ Certificate Server 9.0で認証局を完全に復元するには、CRLデータベースと発行済み証明書データベースを復元する必要があります。

これらのデータベースは両方とも、eDirectory dibファイルと同じディレクトリにあります。これらの場所のデフォルト値は次のとおりです。

- Windowsの場合: c:\novell\nds\dibfiles
- Linuxの場合: /var/opt/novell/edirectory/data/dib

これらのデフォルト値は、eDirectoryのインストール時に変更できます。

CRLデータベースの復元対象ファイルは、crl.db、crl.01、およびcrl.rflディレクトリです。発行済み証明書データベースの復元対象ファイルは、cert.db、cert.lck、cert.01、およびcert.rflディレクトリです。

eDirectory dibディレクトリは、標準および通常バックアップ計画の一部に含める必要があります。

組織認証局を復元するには、次の手順を実行します。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
3. (状況によって実行)組織認証局オブジェクトが存在する場合は、それを削除する必要があります。

   3a ［**役割およびタスク**］で、［**ディレクトリ管理**］>［**オブジェクトの削除**］の順にクリックします。

   3b 組織認証局オブジェクトをブラウズしてクリックします。

   3c ［**OK**］をクリックします。
4. ［**役割およびタスク**］メニューから、［**NetIQ Certificate Server**］>［**認証局の設定**］の順にクリックします。

   この操作により、［Create an Organizational Certificate Authority Object］ダイアログボックスと、オブジェクトを作成する対応するウィザードが開きます。
5. 作成ダイアログボックスで、組織認証局をホストするサーバおよび組織認証局オブジェクトの名前を指定する必要があります。
6. ［**インポート**］オプションを選択します。

   RSAとECDSAの両方の証明書を選択します。証明書サーバでは、両方の証明書のサブジェクト名が同じである必要があります。

重要: 証明書サーバでは、外部自己署名認証局証明書のインポートをサポートしません。ただし、従属認証局証明書をインポートすることはできます。

7 ［次へ］をクリックします。

8 開くダイアログで、［参照］をクリックし、RSAとECDSAのファイルの名前を選択します。

9 バックアップ実行時に、ファイルを暗号化するために使用したパスワードを入力します。

10 ［OK］をクリックします。

これで組織認証局の秘密鍵と証明書が復元され、認証局が完全に機能するようになります。将来の使用に備え、ここでファイルをもう一度保存できます。

重要: 必ず、バックアップメディアを保護してください。

組織認証局の別のサーバへの移動

717 ページの 「組織認証局のバックアップ」および719 ページの 「組織認証局の復元」で説明されているバックアップと復元の手順を利用して、1つのサーバから別のサーバに組織認証局を移動できます。

NetIQ Certificate Server 3.2以降で、認証局を完全に移動するには、CRLデータベースと発行済み証明書データベースを移動する必要があります。

その他のプラットフォームでは、これらのデータベースは両方とも、eDirectory dibファイルと同じディレクトリにあります。これらの場所のデフォルト値は次のとおりです。

- Windowsの場合: c:\novell\nds\dibfiles
- Linuxの場合: /var/opt/novell/edirectory/data/dib

これらのデフォルト値は、eDirectoryのインストール時に変更できます。

CRLデータベースの移動対象ファイルは、crl.db、crl.01、およびcrl.rflディレクトリです。発行済み証明書データベースの移動対象ファイルは、cert.db、cert.lck、cert.01、およびcert.rflディレクトリです。

1 組織認証局が機能することを確認します

2 組織認証局をバックアップします

3 認証局キーをエクスポートします

4 組織認証局オブジェクトを削除します。

5 両方のサーバでeDirectoryを停止します

6 ソースのcertファイルとcrlファイルを、rflログが含まれるあて先サーバにコピーします

7 両方のサーバでeDirectoryを開始します

8 あて先サーバで組織認証局を再作成します

重要: 必ず、バックアップメディアを保護してください。

組織認証局の証明書の検証

証明書に問題があることが疑われる場合、または失効していると思われる場合は、iManagerを使用して簡単に証明書を検証できます。外部認証局によって発行された証明書を含め、eDirectoryツリー内のすべての証明書を検証できます。

証明書の検証プロセスには、証明書のデータだけでなく、証明書チェーン内のデータに対する複数のチェックが含まれます。証明書チェーンは、ルート認証局証明書と、必要に応じて1つ以上の中間認証局の証明書からなります。

証明書チェーン内のすべての証明書が有効であれば、結果は有効になります。現在の時刻が証明書の有効期間内であるか、証明書が取り消されていないか、信頼されている認証局によって署名されているかなど、事前定義された一連の条件を証明書が満たすと、その証明書は有効であると見なされます。CRL配布ポイント拡張機能またはOCSP AIA拡張機能を使用している証明書に限り、取り消されているかどうかがチェックされます。

証明書チェーン内の1つ以上の証明書が無効であると判明した場合、または有効であると断定できない場合、結果は無効になります。無効であると見なされている証明書およびその理由を示す、これらの証明書に関する追加情報が提供されます。理由に関する詳細については、［**ヘルプ**］をクリックしてください。

証明書を検証するには、次の手順を実行します。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
3. ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**認証局の設定**］の順にクリックします。
4. ［**証明書**］をクリックして、公開鍵証明書または自己署名証明書を選択します。
5. ［**検証**］をクリックします。

   証明書のステータスが［**証明書ステータス**］フィールドにレポートされます。証明書が有効でない場合は、理由が示されます。
6. ［**OK**］をクリックします。

組織認証局の削除

組織認証局オブジェクトの削除は、絶対に必要な場合、またはバックアップから組織認証局を復元する場合にのみ行います(719 ページの 「組織認証局の復元」を参照してください)。オブジェクトを削除する唯一安全な方法は、後で復元できるようにまずバックアップを実行してから行う方法です。

ただし、組織認証局を削除し、復元されないようにする必要がある場合もあります。たとえば、ツリーをマージするとき、結果のツリーには1つの組織認証局だけが存在でき、その他の認証局は削除する必要があります。また、組織認証局のホストサーバが修復できないほど破損しているときに、認証局のバックアップまたはNICI設定が行われていない場合、残されている唯一のオプションは認証局を削除して初めからやり直すことです。

組織認証局オブジェクトを削除するには、次の手順を実行します。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 秘密鍵なしで自己署名証明書をバックアップします。

4 CN=trusted roots.CN=security containerで自己署名証明書を使用して、ルート認証局証明書を作成します。次の情報を参照してください:

5 ［役割およびタスク］で、［ディレクトリ管理］>［オブジェクトの削除］の順にクリックします。

6 組織認証局オブジェクトをブラウズしてクリックします。

7 ［OK］をクリックします。

組織認証局のロールオーバー

組織認証局(CA)証明書を置き換える際に考慮すべき重要な問題が2つあります。

- 管理されている証明書のタイプ
- 認証局を置き換える理由

サーバ証明書オブジェクト(KMO)には、サーバの公開鍵証明書と、公開鍵証明書の署名に使用されたルート認証局証明書の両方が含まれます。ユーザ証明書は、ユーザオブジェクトの属性として保存され、それらに署名したルート認証局とはペアになりません。したがって、ルート認証局証明書が置き換えられても、ルート認証局がまだアクセス可能であるため、サーバ証明書は引き続き有効になります。ただしユーザ証明書は、証明書の検証によって確認できるルート認証局コンテナにルート認証局証明書が配置されていない限り、すぐに無効になります。

認証局を交換する3つの理由があります。

- 認証局がその有効性の終わりに達した(認証局の有効期限が切れた)。
- 認証局が侵害された。
- その他の何らかの理由で認証局証明書を置き換えたい(強力な鍵が必要、新しいセキュリティポリシーで必要とされる、外部で署名された認証局を使用したいなど)。

認証局の有効期限が切れた場合、認証局が署名した証明書の有効期限も切れます。認証局を交換した後、新しい認証局を使用してそれぞれの署名済み証明書を再作成する必要があります。

認証局が侵害された場合、認証局を交換することによって、古い認証局によって署名されたユーザ証明書を無効にします。iManagerでデフォルト証明書の作成タスクを実行することによって、簡単に置き換えることができます。証明書サーバによってデフォルトで作成されたすべての証明書は、新しい認証局で再作成されます。カスタマイズした方法で作成したすべての証明書は、新しい認証局を使用して手動で再作成する必要があります。デフォルトの証明書を作成する方法の詳細については、723 ページの 「デフォルトのサーバ証明書オブジェクトを作成する」を参照してください。

何らかの理由で認証局を再作成する場合は、ルート認証局コンテナにルート認証局証明書を保存することによって、ユーザ証明書を再作成するのに都合の良いときまでユーザ証明書を有効なままにしておきます。

ルート認証局証明書を置き換えるには、次の手順を実行します。

1 後で復元しなければならない場合に備え、現在の認証局をバックアップします。

2 証明書の作成に使用されたルート認証局証明書をエクスポートします。古いシステムではほとんどの場合、これは自己署名証明書でした。

最近では、認証局証明書を外部で署名する機能が追加されました。認証局が外部で署名される場合、公開鍵証明書をエクスポートします。チェーン内のすべての証明書は、ルート認証局コンテナに独自のオブジェクトを持つ必要があります。

認証局が侵害されていない場合は、ルート認証局コンテナにルート認証局証明書を作成します。そうすることにより、置き換えられるまでユーザ証明書は有効になります。

3 古い認証局を削除します。組織認証局の削除方法については、721 ページの 「組織認証局の削除」を参照してください。

4 新しい認証局を作成します。新しい組織認証局の作成方法については、715 ページの 「組織の認証局オブジェクトを作成する」を参照してください。

5 必要に応じて、iManagerでデフォルト証明書の作成タスクを使用してサーバ証明書を再作成します。iManagerでデフォルト証明書を作成する方法については、723 ページの 「デフォルトのサーバ証明書オブジェクトを作成する」を参照してください。

デフォルトでは生成されないその他のサーバ証明書を再作成します。

6 必要に応じて、iManagerでユーザ証明書の作成タスクを使用してまたはユーザプロパティを表示させて、証明書を表示し、［**新規**］をクリックしてユーザ証明書を再作成します。

サーバ証明書オブジェクトのタスク

サーバ証明書オブジェクトを作成する

このタスクについては、709 ページの 「サーバ証明書オブジェクトを作成する」で説明されています。

デフォルトのサーバ証明書オブジェクトを作成する

証明書サーバをインストールすると、デフォルトのサーバ証明書オブジェクトが作成されます。

- SSL CertificateDNS - *server_name*
- サーバで設定したIPアドレスごとの証明書(IPAG*xxx.xxx.xxx.xxx* - *server_name*)
- サーバで設定したDNS名ごとの証明書(DNSAG*www.example.com* - *server_name*)

注: eDirectoryでは、SSL CertificateIPは自動的に作成されません。SSL証明書DNSには、［サブジェクトの代替名］にリストされているすべてのIPが含まれます。PKI iManagerプラグインを使用してデフォルトの証明書を作成または修復しようとしても、デフォルトではSSL CertificateIP証明書は作成または修復されません。ただし、プラグインインタフェースに、デフォルトの動作を上書きして、強制的にSSL CertificateIP証明書の作成/修復を実行することを選択できるチェックボックスがあります。

eDirectory 9.0以降では、組織認証局にECDSA証明書があれば、ECDSA証明書が自動的に作成されます。

何らかの理由でこれらの証明書が破損しているまたは無効になった場合、あるいは既存のデフォルト証明書を置換する場合は、次の手順に従って［Create Default Server Certificates］ウィザードを使用します。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
3. ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**デフォルト証明書の作成**］の順にクリックします。
4. デフォルト証明書を作成するサーバをブラウズして選択し、［**次へ**］をクリックします。
5. 既存のデフォルトサーバ証明書を上書きする場合は［**はい**］を選択し、既存のデフォルトサーバ証明書が有効でないときにのみ上書きする場合は［**いいえ**］を選択します。
6. (単一サーバのみ)既存のデフォルトIPアドレスを使用する場合は、そのオプションを選択します。別のIPアドレスを使用する場合は、そのオプションを選択し新しいIPアドレスを指定します。
7. (単一サーバのみ)既存のDNSアドレスを使用する場合は、そのオプションを選択します。別のDNSアドレスを使用する場合は、そのオプションを選択し新しいDNSアドレスを指定します。
8. ［**次へ**］をクリックします。
9. ［概要］ページの内容を確認し、［**終了**］をクリックします。

サーバ証明書オブジェクトの作成をより細かく制御する場合は、サーバ証明書オブジェクトを手動で作成できます。詳細については、710 ページの 「サーバ証明書オブジェクトを手動で作成する」を参照してください。

サーバ証明書オブジェクトへの公開鍵証明書のインポート

証明書署名要求(CSR)を作成し、認証局(CA)が署名済み公開鍵証明書を返してきた後、公開鍵証明書をインポートします。このタスクは、外部認証局の署名オプションとカスタムオプションを使用して、サーバ証明書オブジェクトを作成したときに適用されます。

認証局が証明書を返す方法はいくつかあります。通常、認証局によって、それぞれ1つずつ証明書を格納した1つ以上のファイルか、複数の証明書を格納した1つのファイルが返されます。これらのファイルは、バイナリのDERエンコードファイル(.der、.cer、.crt、.p7b)か、テキストのBase64エンコードファイル(.cer、.b64)になります。

ファイルに複数の証明書が含まれる場合、サーバ証明書オブジェクトにインポートできるようにするためPKCS #7形式である必要があります。さらに、このファイルには、オブジェクトにインポートされるすべての証明書(ルートレベルの認証局証明書、すべての中間証明書、サーバ証明書)を含める必要があります。

証明書に署名した結果として認証局が複数のファイルを返す場合、各ファイルにはサーバ証明書オブジェクトにインポートする必要がある別個の証明書が格納されます。3つ以上のファイル(1つのルートレベルの認証局、1つ以上の中間認証局、1つのサーバ証明書)がある場合、サーバ証明書オブジェクトにインポートするため、これらのファイルをPKCS #7ファイルにまとめる必要があります。

PKCS #7ファイルを作成する方法はいくつかあります。1つの方法は、Internet Explorerにすべての証明書をインポートする方法です。それらの証明書をインポートした後、Internet Explorerを使用して、サーバ証明書と証明書チェーン内のすべての証明書をPKCS #7形式でエクスポートすることができます。この方法の詳細については、954 ページの 「外部認証局」を参照してください。

一部の認証局は、ルートレベルの認証局証明書をサーバ証明書と一緒に返しません。それらのルートレベルの認証局証明書を取得するには、認証局プロバイダに直接問い合わせるか、テクニカルサポートに連絡します。

サーバ証明書オブジェクトに証明書をインポートするには、次の手順を実行します。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
3. ［**役割およびタスク**］メニューで、［**NetIQ証明書アクセス**］>［**サーバ証明書**］の順にクリックします。
4. 変更するサーバ証明書オブジェクトの横にある［**インポート**］をクリックします。
5. 証明書データファイルをブラウズして選択します。
6. ルート認証局データファイルをブラウズして選択します。

   1つのファイルにすべての証明書が含まれている場合は、このフィールドを空白のままにします。
7. ［**OK**］をクリックします。

ルート認証局または公開鍵証明書のエクスポート

次の理由から、証明書をファイルにエクスポートすることがあります。

- クライアント(インターネットブラウザなど)がそのファイルを使用して、暗号化対応アプリケーションによって送信された証明書チェーンを検証できるようにするため。
- ファイルのバックアップコピーを提供するため。

DERエンコード(.der)とBase64エンコード(.b64)の2つのファイル形式で証明書をエクスポートできます。.crt拡張子も、DERエンコード証明書に使用できます。暗号化対応アプリケーションに証明書を直接貼り付けることができるように、システムクリップボードにBase64形式でエクスポートすることもできます。

ルート認証局または公開鍵証明書をエクスポートするには、次の手順を実行します。

1 iManagerを起動します。

2 適切な権利を持ったユーザとしてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQ証明書アクセス**］>［**サーバ証明書**］の順にクリックします。

4 特定のアプリケーションが使用するように設定されているサーバ証明書オブジェクトを選択します。

5 ［**エクスポート**］をクリックします。

この操作により、証明書をファイルにエクスポートするためのウィザードが開きます。

6 ドロップダウンリストを使用して、エクスポートする証明書を指定します。

7 秘密鍵をエクスポートしないことを選択します。

8 エクスポート形式(バイナリのDERまたはテキストエンコードのBase64)を選択し、［**次へ**］をクリックします。

9 ［**Save the Exported Certificate to a File**］をクリックし、ファイルを任意の場所に保存します。

10 ［**閉じる**］>［**閉じる**］>［**OK**］の順にクリックします。

11 必要に応じてファイルを使用します。

たとえば、Internet Explorerブラウザにルート認証局証明書をインストールする場合は、ファイルをダブルクリックします。この操作により、ルート認証局として認証局を受諾するウィザードが開始します。ルート認証局として認証局を受諾すると、ブラウザは、この認証局によって発行された証明書を使用するサービスでSSL接続を自動的に受け入れるようになります。

サーバ証明書オブジェクトの削除

秘密鍵が侵害されていると思われる場合、鍵ペアを使用する必要がなくなった場合、またはサーバ証明書オブジェクトのルート認証局を信頼できなくなった場合、サーバ証明書オブジェクトを削除する必要があります。

重要: サーバ証明書オブジェクトを削除すると、以前にバックアップが作成されていない限り復元できません。オブジェクトを削除する前に、どの暗号化対応アプリケーションでもそのオブジェクトを使用する必要がないことを確認します。サーバ証明書オブジェクトを再作成することはできますが、古いオブジェクトを参照するすべてのアプリケーションを再設定する必要があります。

サーバ証明書オブジェクトを削除するには、次の手順を実行します。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQ証明書アクセス**］>［**サーバ証明書**］の順にクリックします。

4 削除するサーバ証明書オブジェクトを選択します。

5 ［**OK**］をクリックして、オブジェクトを削除します。

サーバ証明書オブジェクトのプロパティの表示

任意のeDirectoryオブジェクトで表示できるeDirectoryの権利とプロパティに加え、サーバ証明書オブジェクトに固有のプロパティ(存在する場合、それに関連付けられた公開鍵証明書やルート認証局証明書のプロパティも含みます)を表示することもできます。

サーバ証明書オブジェクトのプロパティを表示するには、次の手順を実行します。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQ証明書アクセス**］>［**サーバ証明書**］の順にクリックします。

4 表示するサーバ証明書オブジェクトのニックネームをクリックします。

5 証明書チェーンを表示するには、証明書のニックネームの前にあるプラス記号(+)をクリックしてビューを展開します。

6 ［**キャンセル**］をクリックします。

サーバ証明書オブジェクトの公開鍵証明書プロパティの表示

サーバ証明書オブジェクトの公開鍵証明書プロパティを表示するには、次の手順を実行します。

1 iManagerを起動します。

2 適切な権利を持ったユーザとしてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］で、［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。<ナビゲーションを変更>

4 表示するサーバ証明書オブジェクトをブラウズしてクリックします。

5 ［**OK**］をクリックします。

6 公開鍵証明書をクリックします。

- 公開鍵証明書がインストールされている場合、プロパティページには、サブジェクト名の完全識別名、発行者の完全識別名、および公開鍵証明書の有効期限が表示されます。
- 公開鍵証明書がまだインストールされていない場合、プロパティページにそのことが示されます。

7 証明書チェーンを表示するには、証明書のニックネームの前にあるプラス記号(+)をクリックしてビューを展開します。

8 公開鍵証明書に関する追加情報を表示するには、証明書のニックネームをクリックして［詳細］ページを表示します。

［詳細］ページには、公開鍵証明書に含まれている情報が表示されます。

9 ［**閉じる**］>［**キャンセル**］をクリックします。

サーバ証明書オブジェクトのルート認証局証明書プロパティの表示

サーバ証明書オブジェクトのルート認証局証明書プロパティを表示するには、次の手順を実行します。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。

4 表示するサーバ証明書オブジェクトをブラウズして選択します。

5 ［**OK**］をクリックします。

6 ［**ルート認証局の証明書**］をクリックします。

- ルート認証局証明書がインストールされている場合、プロパティページには、サブジェクト名の完全識別名、発行者の完全識別名、およびルート認証局証明書の有効期限が表示されます。
- ルート認証局証明書がまだインストールされていない場合、プロパティページにそのことが示されます。

7 証明書チェーンを表示するには、証明書のニックネームの前にあるプラス記号(+)をクリックしてビューを展開します。

8 ルート認証局証明書に関する追加情報を表示するには、証明書のニックネームをクリックして［詳細］ページを表示します。

［詳細］ページには、ルート認証局証明書に含まれている情報が表示されます。

9 ［**閉じる**］>［**キャンセル**］をクリックします。

サーバ証明書オブジェクトのバックアップ

NetIQ Certificate Serverでは、サードパーティ認証局によって署名された証明書をサーバ証明書オブジェクトに保存することができます。多くの場合、これらの証明書にはかなりの費用がかかります。残念ながら、証明書を保有するサーバで回復不能なエラーが発生すると、サーバ証明書オブジェクトは使用できなくなります。そのような障害から守るために、外部認証局よって署名されたサーバ証明書とそれに関連付けられている秘密鍵をバックアップできます。障害が発生した場合、バックアップファイルを使用して、サーバ証明書オブジェクトをツリー内の任意のサーバに復元できます。

バックアップファイルには、サーバの秘密鍵、公開鍵証明書、ルート認証局証明書、および保存されているすべての中間認証局証明書が含められます。この情報は、PKCS#12形式(PFXとも呼ばれます)で保存されます。

サーバ証明書オブジェクトが正常に機能しているときに、サーバ証明書オブジェクトをバックアップする必要があります。

サーバ証明書オブジェクトをバックアップするには、次の手順を実行します。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［役割およびタスク］で、［ディレクトリ管理］>［オブジェクトの変更］の順にクリックします。<ナビゲーションを変更>

4 バックアップするサーバ証明書オブジェクトをブラウズしてクリックします。

5 ［OK］をクリックします。

6 ［証明書］タブをクリックします。

7 ルート認証局証明書または公開鍵証明書のいずれかをクリックします。証明書は両方とも、バックアップ操作中にファイルに書き込まれます。

8 ［エクスポート］をクリックします。

この操作により、証明書をファイルにエクスポートするためのウィザードが開きます。

9 秘密鍵をエクスポートするかどうかを確認するメッセージが表示されたら、［はい］を選択し、［次へ］をクリックします。

10 6文字以上の英数字でPFXファイルの暗号化で使用するパスワードを指定します。

11 ［次へ］をクリックします。

12 ［Save the Exported Certificate to a File］をクリックします。ファイル名とバックアップファイルの場所を選択します。

13 ［閉じる］をクリックします。

暗号化されたバックアップファイルは、指定した場所に書き込まれます。これで、緊急用に、ファイルを安全な場所に保存する準備ができました。

重要: エクスポートしたファイルは、バックアップメディアに配置し、安全な場所に保存する必要があります。ファイルの暗号化に使用するパスワードは記憶するか、または必要なときに確実に使用でき、かつ他のユーザにはアクセスできないボールトに保存しておく必要があります。

サーバ証明書オブジェクトの復元

サーバ証明書オブジェクトが削除されたまたは破損した場合、あるいはサーバ証明書オブジェクトを所有するサーバで回復不能な障害が発生した場合、728 ページの 「サーバ証明書オブジェクトのバックアップ」で作成したバックアップファイルを使用して、完全に復元することができます。

サーバ証明書オブジェクトのバックアップを作成できなかった場合、NICI 2.xがサーバにインストールされていて、NICI設定情報のバックアップが作成されていれば、そのサーバ証明書オブジェクトを使用できる可能性があります。NICI設定ファイルのバックアップおよび復元方法については、『*Novell International Cryptographic Infrastructure Administration Guide*』の「Backing Up and Restoring NICI (https://www.netiq.com/documentation/nici27x/nici_admin_guide/data/bwf6d4c.html)」セクションを参照してください。

サーバ証明書オブジェクトを復元するには、次の手順を実行します。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 古いサーバ証明書オブジェクトを削除します。

4 ［役割およびタスク］メニューで、［NetIQ Certificate Server］>［サーバ証明書の作成］の順にクリックします。

この操作によって、オブジェクトを作成する［Create a Server Certificate］ウィザードが開きます。

5 このウィザードで、サーバ証明書オブジェクトを所有するサーバを指定し、サーバ証明書の証明書ニックネームを指定します。サーバには、NetIQ Certificate Server 2.21以降のバージョンがインストールされ、実行されている必要があります。

6 ［**インポート**］オプションを選択し、［**次へ**］をクリックします。

7 バックアップファイルをブラウズして選択し、バックアップファイルのパスワードを入力して［**完了**］をクリックします。

これで、サーバの秘密鍵と証明書が復元され、サーバ証明書オブジェクトは完全に機能するようになります。必要に応じて、将来の使用に備え、再度バックアップファイルを保存できます。

重要: 必ず、バックアップメディアを保護してください。

サーバ証明書オブジェクトとクラスタリング

クラスタ化された環境でサーバ証明書オブジェクトを設定し、サーバ証明書オブジェクトを使用する暗号化対応アプリケーションがそれらに常にアクセスできるようにできます。サーバ証明書オブジェクトのバックアップと復元機能を使用して、オブジェクトのキーマテリアルをクラスタ内の1つのノードからすべてのノードに複製できます。外部認証局によって署名されたキーマテリアルにこのプロセスを使用することによって、クラスタ内のすべてのノードのために新しいキーマテリアルを要求するのではなく1つのサーバ証明書のキーマテリアルを複製できるため、コストを削減できます。

クラスタ環境で機能するようにサーバ証明書を設定するには、次の手順を実行します。

1 組織認証局または任意の外部認証局を使用して、クラスタ内のサーバにサーバ証明書を作成します。詳細については、709 ページの 「サーバ証明書オブジェクトを作成する」を参照してください。

   サーバ証明書オブジェクトを作成する場合、証明書のサブジェクト名の一般名(CN)部分はサービス固有のIPまたはDNS名にする必要があります。そうしないと、URLのIPまたはDNS名が証明書のものと一致していないことを示すブラウザ警告メッセージが表示されます。

   複数のサービスにそれぞれ異なるIPまたはDNSアドレスがある場合、各サービスに対してサーバ証明書を作成する必要があります。

2 クラスタ内の残りのすべてのサーバで、ステップ 1で作成したのと同じ鍵ペア名でサーバ証明書オブジェクトを作成することによって、このサーバ証明書オブジェクトのキーマテリアルをバックアップおよび復元します。

   詳細については、728 ページの 「サーバ証明書オブジェクトのバックアップ」を参照してください。

サーバ証明書の検証

証明書に問題があることが疑われる場合、または失効していると思われる場合は、iManagerを使用して簡単に証明書を検証できます。外部認証局によって発行された証明書を含め、eDirectoryツリー内のすべての証明書を検証できます。

証明書の検証プロセスには、証明書のデータだけでなく、証明書チェーン内のデータに対する複数のチェックが含まれます。証明書チェーンは、ルート認証局証明書と、必要に応じて1つ以上の中間認証局の証明書からなります。

証明書チェーン内のすべての証明書が有効であれば、結果は有効になります。現在の時刻が証明書の有効期間内であるか、証明書が取り消されていないか、信頼されている認証局によって署名されているかなど、事前定義された一連の条件を証明書が満たすと、その証明書は有効であると見なされます。CRL配布ポイント拡張機能またはOCSP AIA拡張機能を使用している証明書に限り、取り消されているかどうかがチェックされます。

証明書チェーン内の1つ以上の証明書が無効であると判明した場合、または有効であると断定できない場合、結果は無効になります。無効であると見なされている証明書およびその理由を示す、これらの証明書に関する追加情報が提供されます。理由に関する詳細については、［ヘルプ］をクリックしてください。

証明書を検証するには、次の手順を実行します。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQ証明書アクセス**］>［**サーバ証明書**］の順にクリックします。

4 検証するサーバ証明書オブジェクトを選択します。

5 ［**検証**］をクリックします。

［**証明書ステータス**］フィールドに、証明書のステータスが表示されます。証明書が有効でない場合は、理由が示されます。

ルート認証局または自己署名証明書の取り消し

鍵または認証局が侵害されている場合、証明書が別の証明書によって置き換えられてしまった場合、証明書がCRLから削除された場合など、さまざまな理由で証明書を取り消す必要があると判断することがあるかもしれません。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。

4 変更するサーバ証明書オブジェクトをブラウズしてクリックします。

5 ［**OK**］をクリックします。

6 ［**証明書**］タブをクリックします。

7 ［**ルート認証局の証明書**］または［**Self Signed Certificate**］をクリックしします。

8 証明書を選択し、［**取り消し**］をクリックします。

この操作により、［証明書を取り消す］ウィザードが起動します。メッセージに従って証明書を取り消します。

9 ［**完了**］をクリックします。

別のサーバへのサーバ証明書オブジェクトの移動

728 ページの 「サーバ証明書オブジェクトのバックアップ」および729 ページの 「サーバ証明書オブジェクトの復元」で説明されているバックアップと復元の手順を利用して、1つのサーバから別のサーバにサーバ証明書オブジェクトを移動できます。

1 サーバ証明書オブジェクトが機能することを確認します。
2 サーバ証明書オブジェクトをバックアップします。
3 目的のサーバに、サーバ証明書オブジェクトを復元します。

重要: 必ず、バックアップメディアを保護してください。

サーバ証明書オブジェクトのキーマテリアルの置換

サーバ証明書オブジェクト内の秘密鍵と証明書を置き換えることができます。それらを置き換える場合、サーバ証明書オブジェクトのバックアップ中に作成された、内部で生成されたPFXファイルのみを使用するようにします。秘密鍵、サーバ証明書、および完全な証明書チェーンが含まれている場合は、外部で生成されたPFXファイルも使用できます。ファイル内の鍵と証明書は、必ずしもオブジェクトのものと一致している必要はありません。ファイル内のデータによって、オブジェクトの鍵と証明書が上書きされます。

サーバ証明書オブジェクト内の秘密鍵と証明書の置換は、慎重に行う必要があります。鍵と証明書がオブジェクトのものと正確に一致しない場合、現在のサーバ証明書オブジェクトを削除して新規に作成するのと同じことになります。オブジェクトを削除することによって生じる結果の詳細については、728 ページの 「サーバ証明書オブジェクトのバックアップ」セクションを参照してください。

鍵および証明書がオブジェクトのものと一致する場合、Secure Authentication Services (SAS)によって使用されるいくつかの属性が再生成される以外は、キーマテリアルの置換によって生じる影響はありません。

サーバ証明書オブジェクトのキーマテリアルを置換するには、次の手順を実行します。

1 万一に備えて、秘密鍵と一緒にサーバ証明書オブジェクトをバックアップします。詳細については、728 ページの 「サーバ証明書オブジェクトのバックアップ」を参照してください。
2 iManagerを起動します。
3 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
4 ［**役割およびタスク**］で、［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。
5 変更するサーバ証明書オブジェクトをブラウズして選択します。
6 ［**OK**］をクリックします。
7 ［**証明書**］タブをクリックします。
8 ［**ルート認証局証明書**］または［**自己署名証明書**］をクリックししします。

   いずれのページからも操作を開始できます。これらの操作により、証明書、秘密鍵、および証明書チェーン内のその他の証明書が置き換えられます。
9 証明書を選択し、［**置換**］をクリックします。

この操作により、PFX(バックアップ)ファイルを指定するためのウィザードが開きます。

10 バックアップファイルをブラウズして選択し、バックアップファイルのパスワードを入力して［OK］をクリックします。

これで、サーバの秘密鍵と証明書が置換されました。サーバ証明書は完全に機能するようになります。必要に応じて、将来の使用に備え、再度バックアップファイルを保存します。

重要: 必ず、バックアップメディアを保護してください。

ユーザ証明書のタスク

- 733 ページの 「ユーザ証明書の作成」
- 733 ページの 「ユーザ証明書の一括作成」
- 734 ページの 「ユーザオブジェクトへの公開鍵証明書のインポート(秘密鍵は省略可)」
- 734 ページの 「ユーザ証明書のプロパティの表示」
- 735 ページの 「ユーザ証明書のエクスポート」
- 735 ページの 「ユーザ証明書と秘密鍵のエクスポート」
- 736 ページの 「ユーザ証明書の検証」
- 737 ページの 「ユーザ証明書の取り消し」
- 737 ページの 「ユーザ証明書と秘密鍵の削除」

ユーザ証明書の作成

このタスクについては、711 ページの 「ユーザ証明書の作成」で説明されています。

ユーザ証明書の一括作成

この機能により、一連の操作で、同時に複数のユーザのユーザ証明書を作成できます。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［役割およびタスク］メニューで、［NetIQ Certificate Server］>［ユーザ証明書の作成］の順にクリックします。

この操作により、ユーザ証明書の作成を支援するウィザードが開きます。

4 ユーザ証明書を作成するすべてのユーザをブラウズして選択します。

5 各ユーザの証明書を作成するウィザードの指示に従います。ウィザードの各ページに関する特定の情報については、［ヘルプ］をクリックします。

ユーザオブジェクトへの公開鍵証明書のインポート(秘密鍵は省略可)

ユーザオブジェクト(たとえば、サードパーティの認証局によって署名された証明書)に、任意の公開鍵証明書をインポートできます。この証明書は、次の2種類のファイルのいずれかとして表示されます。

- **DER:** 公開鍵証明書のみが含まれます。
- **PFXまたはPKCS #12:** 公開鍵証明書と秘密鍵が含まれます。

インポートされると、証明書はユーザオブジェクトに保存され、使用可能な証明書のリストに表示されます。

注: PKCS #12証明書をインポートすると、公開鍵証明書と秘密鍵のみが、ユーザオブジェクトに保存されます。他の証明書は保存されません。ユーザの証明書チェーン内の他の証明書は、CN=Trusted Roots.CN=Securityコンテナに保存されるはずです(チェーン内の各証明書の新しいルート認証局オブジェクトを作成します)。

ユーザオブジェクトに公開鍵証明書をインポートするには、次の手順を実行します。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
3. ［**役割およびタスク**］メニューで、［**NetIQ証明書アクセス**］>［**ユーザ証明書**］の順にクリックします。
4. 公開鍵証明書をインポートするユーザオブジェクトをブラウズして選択します。
5. ［**新規作成**］をクリックします。
6. ユーザ証明書のニックネームを指定します。

   ニックネームは固有のもので、証明書を特定するために役立つものである必要があります。［**証明書ニックネーム**］フィールドには最大64文字まで入力できます。
7. ［インポート］作成方法を選択し、［**次へ**］をクリックします。
8. インポートする証明書をブラウズして選択し、［**OK**］をクリックします。
9. (状況によって実行)秘密鍵と一緒に証明書をインポートする場合、秘密鍵のパスワードを入力し、［**次へ**］をクリックします。
10. ［**完了**］をクリックします。

    これでユーザオブジェクトに証明書が保存され、このユーザが使用できる証明書のリストにその証明書が表示されます。

ユーザ証明書のプロパティの表示

任意のeDirectoryオブジェクトで表示できるeDirectoryの権利とプロパティに加え、ユーザ証明書に固有のプロパティ(発行者、証明書のステータス、秘密鍵のステータス、検証期間など)を表示することもできます。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［役割およびタスク］メニューで、［NetIQ証明書アクセス］>［ユーザ証明書］の順にクリックします。

4 証明書のプロパティを表示するユーザオブジェクトをブラウズして選択します。

5 証明書チェーンを表示するには、証明書のニックネームの前にあるプラス記号(+)をクリックしてビューを展開します。

6 証明書のニックネームをクリックして証明書の詳細を表示します。

7 確認し終わったら、［閉じる］をクリックします。

ユーザ証明書のエクスポート

別のユーザとセキュリティで保護された電子メールを交換するには、まず、そのユーザの公開鍵証明書を入手する必要があります。証明書を入手する1つの方法は、iManagerを使用して証明書をエクスポートすることです。あるいは、LDAPや電子メールを使用して、相手の証明書を入手することもできます。

自分または他のユーザの公開鍵証明書をエクスポートするには、次の手順に従います。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［役割およびタスク］メニューで、［NetIQ証明書アクセス］>［ユーザ証明書］の順にクリックします。

4 証明書をエクスポートするユーザオブジェクトをブラウズして選択します。

5 証明書を選択してから、［エクスポート］をクリックします。

これにより、ユーザ証明書をファイルにエクスポートする手順を示すウィザードが開きます。選択した証明書を所有するユーザとしてログインしている場合は、秘密鍵をエクスポートするかどうか尋ねられたら、［いいえ］を選択します。詳細については、735ページの「ユーザ証明書と秘密鍵のエクスポート」を参照してください。

6 秘密鍵をエクスポートする場合は、［秘密鍵のエクスポート］をクリックし、秘密鍵を保護するパスワードを入力します。

7 秘密鍵をエクスポートしない場合は、エクスポート形式を選択してから［次へ］をクリックします。

8 ［Save the Exported Certificate to a File］をクリックし、ファイルを任意の場所に保存します。

9 ［閉じる］>［閉じる］の順にクリックします。

ユーザ証明書と秘密鍵のエクスポート

セキュリティで保護された電子メール、認証、または暗号化の証明書を使用するには、秘密鍵と証明書の両方が、暗号化対応アプリケーションで使用できるようになっていなければなりません。ユーザ証明書と秘密鍵をエクスポートし、アプリケーションで使用できるよう、そのアプリケーションがアクセスできる場所に配置する必要があります。

ユーザのオブジェクトに含まれる秘密鍵は、そのユーザに属しています。その秘密鍵をエクスポートできるのは、そのユーザとしてログインした場合のみです。その他のユーザは、ネットワーク管理者であっても、他のユーザの秘密鍵をエクスポートする権利はありません。

自分の秘密鍵と証明書をエクスポートするには、次の手順に従います。

1 iManagerを起動します。

2 証明書を所有するユーザとして、eDirectoryツリーにログインします。

このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQ証明書アクセス**］>［**ユーザ証明書**］の順にクリックします。

4 証明書をエクスポートするユーザオブジェクトをブラウズして選択します。

5 証明書を選択してから、［**エクスポート**］をクリックします。

これにより、ユーザ証明書をファイルにエクスポートする手順を示すウィザードが開きます。

6 ［**秘密鍵のエクスポート**］を選択し、秘密鍵を保護するパスワードを入力してから、［**次へ**］をクリックします。

7 (オプション)［**証明書をブラウザにエクスポートしてください。**］をクリックします。

8 ［**閉じる**］>［**閉じる**］の順にクリックします。

暗号化されたファイルが、指定した場所に書き込まれます。これで、暗号化対応アプリケーションにインポートできる状態になります。

重要: バックアップとして使用できるように、エクスポートしたファイルを保持しておくことができます。その場合は、セキュアな場所に保管する必要があります。ファイルの暗号化に使用するパスワードは記憶するか、または必要なときに確実に使用でき、かつ他のユーザにはアクセスできない安全な場所に保存しておく必要があります。

ユーザ証明書の検証

証明書に問題があることが疑われる場合、または失効していると思われる場合は、iManagerを使用して簡単に証明書を検証できます。外部認証局によって発行された証明書を含め、eDirectoryツリー内のすべての証明書を検証できます。

証明書の検証プロセスには、証明書のデータだけでなく、証明書チェーン内のデータに対する複数のチェックが含まれます。証明書チェーンは、ルート認証局証明書と、必要に応じて1つ以上の中間認証局の証明書からなります。

証明書チェーン内のすべての証明書が有効であれば、結果は有効になります。現在の時刻が証明書の有効期間内であるか、証明書が取り消されていないか、信頼されている認証局によって署名されているかなど、事前定義された一連の条件を証明書が満たすと、その証明書は有効であると見なされます。CRL配布ポイント拡張機能またはOCSP AIA拡張機能を使用している証明書に限り、取り消されているかどうかがチェックされます。

証明書チェーン内の1つ以上の証明書が無効であると判明した場合、または有効であると断定できない場合、結果は無効になります。このような場合は、無効と見なされた証明書とその理由に関する追加情報が提供されます。理由に関する詳細については、［ヘルプ］をクリックしてください。

証明書を検証するには、次の手順を実行します。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［役割およびタスク］メニューで、［NetIQ証明書アクセス］>［ユーザ証明書］の順にクリックします。

4 証明書を検証するユーザオブジェクトをブラウズして選択します。

5 検証するユーザ証明書を選択します。

6 ［検証］をクリックします。

［証明書ステータス］フィールドに、証明書のステータスが表示されます。証明書が有効でない場合は、理由が示されます。

注: ユーザ証明書にサードパーティの認証局による署名が付けられている場合、証明書チェーンがセキュリティコンテナ内のルート認証局コンテナに入っていなければ(CN=Trusted Roots.CN=Security)、証明書を正常に検証できません。通常、証明書チェーンは1つのルートレベルの認証局で構成されるか、中間認証局とルートレベルの認証局で構成されます。ルート認証局コンテナの名前は「ルート認証局」であること、そして証明書チェーンに含まれる各証明書が、それぞれ独自のルート認証局オブジェクトに格納されていることが必要です。ルート認証局コンテナおよびルート認証局オブジェクトの作成方法については、711 ページの 「ルート認証局コンテナの作成」および712 ページの 「ルート認証局オブジェクトの作成」を参照してください。

外部認証局によって署名されたユーザ証明書または中間認証局の証明書を検証する場合は、外部認証局の証明書がルート認証局オブジェクトに格納されていなければ、証明書を正常に検証できません。ルート認証局オブジェクトは、「ルート認証局」という名前のルート認証局コンテナ内にあること、そしてそのルート認証局コンテナがセキュリティコンテナに含まれていることが必要です。

ユーザ証明書の取り消し

鍵または認証局が侵害されている場合、証明書が別の証明書によって置き換えられてしまった場合、証明書がCRLから削除された場合など、さまざまな理由で証明書を取り消す必要があると判断することがあるかもしれません。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［役割およびタスク］メニューで、［NetIQ証明書アクセス］>［ユーザ証明書］の順にクリックします。

4 証明書を検証するユーザオブジェクトをブラウズして選択します。

5 取り消すユーザ証明書を選択します。

6 ［取り消し］をクリックします。

この操作により、［証明書を取り消す］ウィザードが起動します。メッセージに従って証明書を取り消します。

7 完了をクリックします。

ユーザ証明書と秘密鍵の削除

ユーザ証明書が無効になった場合、または何らかの形での秘密鍵のセキュリティ侵害が疑われる場合は、ユーザ証明書と秘密鍵を削除する必要があります。

ユーザ証明書と秘密鍵を削除するには、その前に、ユーザ証明書を取り消さなければなりません。詳細については、737 ページの 「ユーザ証明書の取り消し」を参照してください。

ユーザ証明書と秘密鍵を削除するには、次の手順に従います。

1 iManagerを起動します。
2 証明書を所有するユーザとして、または適切な権利を持つ管理者としてeDirectoryツリーにログインします。

このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQ証明書アクセス**］>［**ユーザ証明書**］の順にクリックします。
4 証明書を削除するユーザオブジェクトをブラウズして選択します。
5 削除するユーザ証明書を選択します。
6 **削除**をクリックします。

X.509証明書の自己プロビジョニング

このセクションでは、X.509の自己プロビジョニング機能について説明します。

概要

X.509認定を作成するときには、認証局(CA)が証明書を発行する前に特定して裏付けを取っておく必要のある、多くの重要な情報があります。最も重要なタスクは、以下の2つです。

- 証明書のサブジェクト名の識別情報の検証(証明書を作成する対象の個人またはオブジェクトの識別情報を検証する)。
- 証明書のサブジェクト名の妥当性検証(サブジェクト名が、証明書を作成する対象の個人またはオブジェクトの識別情報を正しく表していることを検証する)。

これら2つのタスクには非常に時間がかかる可能性があり、多くの場合は独立した管理者や管理グループによって行われます。

NetIQ Certificate Serverではこれまで常に、eDirectoryのセキュア識別情報管理機能を利用して、これらの検証に必要な時間を節約し、手間を省いてきました。iManagerでは、管理者がユーザ証明書を一括で作成できるようになっています。つまり、多数のユーザの証明書を一度に作成できます。認証局は、証明書の識別情報がeDirectoryアカウントに関連付けられていることを確認し、それによって証明書のサブジェクトの識別情報を検証します。一方、証明書のサブジェクト名の妥当性は認証局によって検証されていませんでした。このため、NetIQ Certificate Serverで証明書を作成するには、証明書を作成する担当者またはソフトウェアには必ず、組織認証局に対する管理権が必要でした。

自己プロビジョニングにより、ユーザまたはサーバは、認証局に対する管理権がなくても、別の管理者または管理グループの介入なく、組織認証局のセキュリティを維持しながら、証明書を生成できます。

NetIQ Certificate Serverは、証明書の識別情報がeDirectoryアカウントに関連付けられていることを確認することによって、証明書のサブジェクトの識別情報を検証します。認証局はeDirectory内の情報を確認することで、証明書のサブジェクト名の妥当性も検証します。したがって、組織認証局はeDirectoryのセキュリティ識別情報管理機能を利用して、組織認証局のセキュリティを維持しながら、管理タスクを減らすことができます。

ユーザ自己プロビジョニング

これまで、ユーザ証明書を作成するには認証局に対する管理権だけでなく、ユーザオブジェクトに対する権利も必要でした。ユーザ自己プロビジョニングにより、認証局に対する管理権が不要になります。ただし、userCertificate属性、NDSPKI:UserCertificateInfo属性、およびSAS:SecretStore属性に対する読み込み(R)権と書き込み(W)権は引き続き必要です。

証明書の作成を要求するユーザが認証局に対する管理権を持っている場合、証明書の作成は、ユーザ自己プロビジョニングが有効にされているかどうかによって影響を受けることはありません。証明書の作成を要求するユーザが認証局に対する管理権を持っていない場合は、要求に含まれるサブジェクト名が、ユーザのeDirectory DNと、sasAllowableSubjectNames属性に含まれるすべての値と比較されます。

サブジェクト名が一致すると、認証局は、すべてのサブジェクト代替名を調べて適切であることを確認します。認証局はそのために、複数のサブジェクト代替名がないことを確認します。代替名が存在する場合、そのタイプは電子メールの名前でなければならず、ユーザオブジェクトに設定済みの電子メールの名前と一致していなければなりません。これらすべての確認に成功すると、認証局に対する管理権を認証局から要求されることなく、証明書を作成できます。

ユーザ自己プロビジョニングを使用するには、次の手順に従います。

1. eDirectory 9.1以降、およびNetIQ Certificate Server 9.1.0以降のiManager用プラグインがインストールされていることを確認します。
2. ユーザ自己プロビジョニングを有効にします。
   - **2a** iManagerを起動します。
   - **2b** 組織認証局に対する管理権を持つ管理者としてeDirectoryツリーにログインします。
   - **2c** ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**認証局の設定**］の順にクリックします。
   - **2d** ［**ユーザ自己プロビジョニングを有効にする**］を選択します。
   - **2e** **OK**をクリックします。
3. iManagerの「［this］」オブジェクトを有効にして、ユーザの権利継承を設定します。
   - **3a** iManager管理者としてiManagerにログインします。
   - **3b** ［**設定**］アイコンをクリックします。
   - **3c** ［**iManagerサーバ**］>［**iManagerの設定**］の順にクリックします。
   - **3d** ［**その他**］タブをクリックします。
   - **3e** ［**「［これ］」を有効にする**］を選択します。
   - **3f** **保存**をクリックします。

     次に、権利継承を追加する必要があります。
4. 認証局の管理者としてiManagerにログインします。
5. ［**役割およびタスク**］メニューで、［**権利**］>［**トラスティの変更**］の順にクリックします。
6. 継承する権利を持つオブジェクトをブラウズして選択し(たとえば、ツリーのルートやコンテナ)、［**OK**］をクリックします。

7 ［トラスティの追加］をクリックし、「［this］」オブジェクトを選択してから、［OK］をクリックします。

8 ［Assigned Rights］をクリックします。

9 ［プロパティの追加］をクリックします。

10 ［スキーマ内のすべてのプロパティを表示する］を選択します。

11 userCertificate属性を選択してから、［OK］をクリックします。

12 ［読み込み］権と［書き込み］権を選択します。

13 ［継承］を選択します。

14 NDSPKI:UserCertificateInfo属性およびSAS:SecretStore属性について、ステップ6からステップ10を繰り返します。

15 ［完了］>［OK］の順にクリックします。

サーバ自己プロビジョニング

これまで、サーバ証明書を作成するには、認証局に対する管理権だけでなく、サーバ証明書が作成されたコンテキストに対する管理権も必要でした。サーバ自己プロビジョニングにより、認証局に対する管理権が不要になります。ただし、サーバ証明書が作成されたコンテキストに対する管理権は引き続き必要です。

サーバ証明書を作成するには、認証局に対する管理権が必要です。証明書の作成は、サーバ自己プロビジョニングが有効にされているかどうかによって影響を受けることはありません。認証局に対する必要な管理権を持っていない場合は、iManagerの［認証局の設定］タスクで［CAを操作するには読み込み権が必要］オプションを有効にして、認証局を操作してください。次のいずれかに当てはまる場合、認証局に対する管理権は必要ありません。

- 要求に含まれるサブジェクト名が、サーバのeDirectory DNと、DNSまたはeDirectory SLP検索で判断されたIPまたはDNSアドレスと比較される場合。サブジェクト名がこのいずれかと一致した場合、認証局に対する管理権を認証局から要求されることなく、証明書を作成できます。
- サブジェクト名のCN以外のコンポーネントが、認証局証明書のサブジェクト名のCN以外のコンポーネントと一致する場合。
- サブジェクト代替名に、リバースDNS検索で認証局によって再検証されるIPアドレス/DNS名しかない場合。

デフォルトでは、認証局のNDSPKI:Private Key属性に対する書き込み権はサーバに付与されません。iManagerの［認証局の設定］タスクで、［CAを操作するには書き込み権が必要］オプションが有効にされている場合、認証局のNDSPKI:Private Key属性に対する読み込み権をサーバに付与する必要があります。

注: サーバ自己プロビジョニングが有効にされているサーバに対してPKIヘルスチェックが実行されると、サーバのサーバ証明書が自動的に作成されるか(存在しない場合)、置き換えられる(期限切れの場合)ことに注意してください。詳細については、757 ページの 「PKIヘルスチェック」を参照してください。

サーバ自己プロビジョニングを使用するには、次の手順に従います。

1 eDirectory 9.0以降、およびNetIQ Certificate Server 3.2.2以降のiManager用プラグインがインストールされていることを確認します。

eDirectory 8.8と、NetIQ Certificate Server 3.2.2のiManager用プラグインの両方はOES 2に組み込まれていて、OES 2のインストール時にeDirectoryを必要とするコンポーネントのいずれかを選択すると、自動的にインストールされます。

2 サーバ自己プロビジョニングを有効にします。

2a iManagerを起動します。

2b 組織認証局に対する管理権を持つ管理者としてeDirectoryツリーにログインします。

2c ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**認証局の設定**］の順にクリックします。

2d ［**サーバ自己プロビジョニングを有効にする**］を選択します。

2e **OK**をクリックします。

証明書の自己プロビジョニングと証明書の発行タスク

証明書の発行タスクでは、PKCS#10証明書署名要求(CSR)を使用して証明書を作成できます。ユーザはこのタスクを使用して、どのeDirectoryオブジェクトにも関連付けられていない証明書を作成できます。証明書の作成を要求するユーザが認証局に対する管理権を持っている場合、証明書の作成には影響がありません。証明書の作成を要求するユーザが認証局に対する管理権を持っていなければ、証明書の要求はユーザ自己プロビジョニングリクエストとして扱われます。ただし、ユーザがオブジェクトのuserCertificate属性、NDSPKI:UserCertificateInfo属性、およびSAS:SecretStore属性に対する管理権を持っている必要はありません。これは、証明書はeDirectoryに保管されないためです。したがって、オブジェクトに対する権利は必要ありません。

認証局に対する管理権を持たないユーザが証明書を発行するには、ユーザ自己プロビジョニングが有効にされている必要があります。それには、739 ページの 「ユーザ自己プロビジョニング」のステップ1から3に従います。

証明書の発行タスクについては、715 ページの 「公開鍵証明書の発行」を参照してください。

外部アプリケーションでのeDirectory証明書の使用

一部のお客様は、X.509認定と鍵が必要な、eDirectory以外のアプリケーション(たとえば、ApacheやOpenSSL)を使用しています。そのようなアプリケーションのほとんどは、追加の設定を加えなければ自己署名(値なし)証明書を使用するように設定されています。この設定は、アプリケーションを本物のX.509認定と鍵で構成できるようになるまでの一時的なソリューションとして意図されています。

残念ながら、多くの管理者は、時間がかかり過ぎるという理由や難しすぎるという理由で、自己署名証明書を置き換えていません。さらに、X.509認定は定期的に期限切れになるよう設計されているため、定期的に証明書を置き換えるのは、継続的な管理タスクになります。

以降のセクションで、この問題に対するソリューションを説明します。

- 742 ページの 「PKIヘルスチェック機能」
- 743 ページの 「eDirectory証明書をエクスポートするためのSAS:Serviceオブジェクトの設定」

PKIヘルスチェック機能

eDirectory以外のアプリケーションにX.509認定を提供してほしいというお客様からの要望に応え、現在、NetIQ Certificate Serverに組み込まれたPKIヘルスチェックコードでX.509認定と鍵を自動的にファイルシステムにエクスポートして、eDirectoryが生成した証明書とeDirectoryで管理される証明書を、eDirectory以外のアプリケーションが利用できるようになっています。

PKIヘルスチェックが実行されると、証明書の秘密鍵を含め、既存の証明書が自動的に上書きされます。ただし、有効な証明書と秘密鍵が削除されないようにするため、PKIヘルスチェックは既存の証明書と鍵がeDirectoryで設定されているものと同じであるかどうかを判別します。eDirectoryで設定されているものと異なる場合は、PKIヘルスチェックはそれらのファイルをバックアップしてから上書きします。したがって、外部ソース(VeriSign*など)から取得された証明書が削除されることはありません。

SAS:Serviceオブジェクトにサーバの環境設定が作成された後、指定のサーバに関連付けられた鍵と証明書が自動的にファイルシステムにエクスポートされます。eDirectory内で鍵と証明書が置き換えられるか更新される場合(たとえば、サーバ証明書オブジェクトが削除されて、同じ名前で新しいサーバ証明書オブジェクトが作成された場合)、次のPKIヘルスチェックの実行時に新しい鍵と証明書が自動的にファイルシステムにエクスポートされます。

注: NetIQ Certificate Serverに組み込まれたPKIヘルスコードは、NetIQ Certificate Serverがロード/再ロードされるたびに実行されます。NetIQ Certificate Serverを再ロードするには、次のいずれかの方法を使用できます。

- サーバを再起動する
- eDirectoryを再起動する
- 手動でPKIサーバをアンロードしてからロードする
- eDirectory修復(NDSRepair)を実行する

  eDirectory修復の実行中にNetIQ Certificate Serverがシャットダウンし、修復が完了すると再ロードされます。

PKIヘルスチェックの詳細については、757 ページの 「PKIヘルスチェック」を参照してください。

PKIヘルスチェックでX.509認定と鍵を自動的にファイルシステムにエクスポートするには、その前に、SAS:Serviceオブジェクトを設定する必要があります。これは、PKIヘルスチェックがSAS:Serviceオブジェクトの設定を読み込むためです。SAS:Serviceオブジェクトを設定する方法については、743 ページの 「eDirectory証明書をエクスポートするためのSAS:Serviceオブジェクトの設定」を参照してください。

eDirectory証明書をエクスポートするためのSAS:Serviceオブジェクトの設定

eDirectoryのサーバ証明書をファイルシステムにエクスポートするには、その前に、SAS:Serviceオブジェクトにサーバ用の環境設定を作成する必要があります。使用しているeDirectoryサーバによって、自動的に作成できる場合も、手動で作成できる場合もあります。以降のセクションで、これらのオプションについて詳しく説明します。

- 743 ページの 「eDirectory証明書の使用を有効にするためにSAS:Serviceオブジェクトを手動で設定する」

eDirectory証明書の使用を有効にするためにSAS:Serviceオブジェクトを手動で設定する

OES 2をeDirectoryサーバとして使用していない場合、eDirectory証明書をエクスポートするにはSAS:Serviceオブジェクトを手動で設定する必要があります。この環境設定で、サーバ証明書の名前を指定します。複数のサーバ証明書をエクスポートする必要がある場合は、複数の環境設定を作成できます。同じ証明書を異なるファイルパスにエクスポートすることも、異なる証明書をそれぞれ異なるファイルパスにエクスポートすることもできます。

注: ファイルの競合を避けるため、各環境設定で固有のファイルパスを使用する必要があります。公開鍵のパスと秘密鍵のパスは固有にして、互いに異なり、他の環境設定とも異なるようにする必要があります。

SAS:Serviceオブジェクトに環境設定を作成するには、次の手順に従います。

1. iManagerの［**役割およびタスク**］ビューで、［**NetIQ証明書アクセス**］をクリックします。
2. ［**SASサービスオブジェクト**］をクリックします。
3. ［SASサービスオブジェクト］ページで［**参照**  ］アイコンをクリックします。
4. 環境設定を作成するSAS:Serviceオブジェクトをブラウズして選択します。
5. SAS:Serviceオブジェクトをクリックします。
6. ［**新規作成**］をクリックします。

   ［サーバ証明書の同期］ウィンドウが表示されます。
7. ［**証明書**］フィールドで、エクスポートする証明書をブラウズして選択します。
8. ［**公開鍵パス**］フィールドに、アプリケーションが証明書を見つけて使用するためのパスを指定します。例: C:/novell/nds/servercert.pem
9. ［**秘密鍵パス**］フィールドに、アプリケーションが証明書の秘密鍵を見つけて使用するためのパスを指定します。例: C:/novell/nds/serverkey.pem
10. 使用する鍵のタイプを選択します。OpenSSLを実行している場合は、［PKCS#8］を選択します。Apacheを実行している場合は、［PKCS#1］を選択します。
11. **OK**をクリックします。

    環境設定が作成されます。名前、パス、鍵のパス、鍵のタイプが表示されます。

別の環境設定を作成するには、ステップ 6からステップ 11を繰り返します。

OESサーバをeDirectoryサーバとして使用している場合は、サーバがSAS:Serviceオブジェクトに環境設定を作成するように自動的に設定することができます。

注: OES 2のインストール時にeDirectory証明書の使用が有効にされると(デフォルト)、インストールコードによってSSL CertificateDNSオブジェクトの環境設定が作成され、証明書と鍵が以下のファイルにエクスポートされます。

鍵ファイル: /etc/ssl/servercerts/serverkey.pem

証明書ファイル: /etc/ssl/servercerts/servercert.pem

ルート認証局オブジェクトのタスク

- 744 ページの 「ルート認証局コンテナの作成」
- 744 ページの 「ルート認証局オブジェクトの作成」
- 744 ページの 「ルート認証局オブジェクトのプロパティの表示」
- 745 ページの 「ルート認証局証明書の置き換え」
- 745 ページの 「ルート認証局オブジェクトの検証」
- 746 ページの 「ルート認証局証明書の取り消し」

ルート認証局コンテナの作成

このタスクについては、711 ページの 「ルート認証局コンテナの作成」で説明されています。

ルート認証局オブジェクトの作成

このタスクについては、712 ページの 「ルート認証局オブジェクトの作成」で説明されています。

ルート認証局オブジェクトのプロパティの表示

任意のeDirectoryオブジェクトで表示できるeDirectoryの権利とプロパティに加え、ルート認証局オブジェクトに固有のプロパティを表示することもできます。これらのプロパティには、証明書の発行者、ステータス、有効期間があります。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
3. ［**役割およびタスク**］メニューで、［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。
4. 表示するルート認証局オブジェクトをブラウズしてクリックします。
5. **OK**をクリックします。
6. 証明書チェーンを表示するには、証明書のニックネームの前にあるプラス記号(+)をクリックしてビューを展開します。
7. 証明書のニックネームをクリックして証明書の詳細を表示します。
8. ［**キャンセル**］をクリックします。

ルート認証局証明書の置き換え

このタスクによって、ルート認証局オブジェクトに保管されているルート認証局証明書を置き換えることができます。ルート認証局証明書の有効期限が切れている場合は、このタスクを実行する必要があります。

ルート認証局証明書は、ルート認証局オブジェクトのプロパティページで置き換えることができます。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
3. ［**役割およびタスク**］で、［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。
4. 置き換えるルート認証局オブジェクトをブラウズしてクリックします。
5. **OK**をクリックします。
6. 証明書を選択してから、［**置換**］をクリックします。
7. 新しいルート認証局証明書をブラウズして選択します。
8. **OK**をクリックします。

ルート認証局オブジェクトの検証

証明書に問題があることが疑われる場合、または失効していると思われる場合は、iManagerを使用して簡単に証明書を検証できます。外部認証局によって発行された証明書を含め、eDirectoryツリー内のすべての証明書を検証できます。

証明書の検証プロセスには、証明書のデータだけでなく、証明書チェーン内のデータに対する複数のチェックが含まれます。証明書チェーンは、ルート認証局証明書と、必要に応じて1つ以上の中間認証局の証明書からなります。

証明書チェーン内のすべての証明書が有効であれば、結果は有効になります。現在の時刻が証明書の有効期間内であるか、証明書が取り消されていないか、信頼されている認証局によって署名されているかなど、事前定義された一連の条件を証明書が満たすと、その証明書は有効であると見なされます。CRL配布ポイント拡張機能またはOCSP AIA拡張機能を使用している証明書に限り、取り消されているかどうかがチェックされます。

証明書チェーン内の1つ以上の証明書が無効であると判明した場合、または有効であると断定できない場合、結果は無効になります。このような場合は、無効と見なされた証明書とその理由に関する追加情報が提供されます。理由に関する詳細については、［**ヘルプ**］をクリックしてください。

ルート認証局証明書を検証するには、次の手順に従います。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
3. ［**役割およびタスク**］で、［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。
4. 検証するルート認証局オブジェクトをブラウズしてクリックします。
5. **OK**をクリックします。

6 証明書を選択してから、［**検証**］をクリックします。

［**証明書ステータス**］フィールドに、証明書のステータスが表示されます。証明書が有効でない場合は、理由が示されます。

注: オブジェクトに保管されている証明書が自己署名証明書ではない場合、証明書チェーンがセキュリティコンテナ内のルート認証局コンテナに入っていなければ(CN=Trusted Roots.CN=Security)、証明書を正常に検証できません。通常、証明書チェーンは1つのルートレベルの認証局で構成されるか、中間認証局とルートレベルの認証局で構成されます。ルート認証局コンテナの名前は「ルート認証局」であること、そして証明書チェーンに含まれる各証明書が、それぞれ独自のルート認証局オブジェクトに格納されていることが必要です。ルート認証局コンテナおよびルート認証局オブジェクトの作成方法については、711 ページの 「ルート認証局コンテナの作成」および712 ページの 「ルート認証局オブジェクトの作成」を参照してください。

ルート認証局証明書の取り消し

鍵または認証局が侵害されている場合、証明書が別の証明書によって置き換えられてしまった場合、証明書がCRLから削除された場合など、さまざまな理由で証明書を取り消す必要があると判断することがあるかもしれません。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクのための適切な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］で、［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックします。

4 変更するルート認証局オブジェクトをブラウズしてクリックします。

5 **OK**をクリックします。

6 証明書を選択してから、［**取り消し**］をクリックします。

この操作により、［証明書を取り消す］ウィザードが起動します。メッセージに従って証明書を取り消します。

7 **完了**をクリックします。

証明書取り消しリスト(CRL)のタスク

NetIQ Certificate Serverには、証明書取り消しリスト(CRL)を管理するためのシステムが用意されています。これはオプションシステムですが、組織認証局によって作成された証明書を取り消せるようにするには、このシステムを実装する必要があります。

CRLは、取り消された証明書とその理由を公開するリストです。

- 747 ページの 「手動によるCRLコンテナの作成」
- 747 ページの 「CRLコンテナの削除」
- 748 ページの 「CRL設定オブジェクトの作成」
- 748 ページの 「CRL設定オブジェクトのアクティブ化」
- 749 ページの 「CRL設定オブジェクトのプロパティの表示と変更」
- 751 ページの 「CRL設定オブジェクトの削除」
- 751 ページの 「CRLオブジェクトの作成」

- 752 ページの 「CRLファイルのエクスポート」
- 752 ページの 「CRLファイルの置き換え」
- 753 ページの 「CRLファイルの有効期間の延長」
- 753 ページの 「CRLオブジェクトのプロパティの表示」
- 754 ページの 「CRLオブジェクトの削除」

手動によるCRLコンテナの作成

NetIQ Certificate Serverのインストール時に、ユーザがCRLコンテナの作成に必要な権利を持っている場合は、CRLコンテナが作成されます。そうでない場合は、インストールが完了してから、適切な権利を持つユーザが手動でCRLコンテナを作成できます。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**認証局の設定**］の順に選択します。

CRLコンテナがすでに存在する場合は、組織認証局のプロパティページが表示されます。

CRLコンテナが存在しない場合は、CRLコンテナとそのコンテナに格納するCRL設定オブジェクトを作成するためのウィザードが起動します。

4 ウィザードに従って操作を完了します。

注: CRLコンテナがセキュリティコンテナとは別のコンテナに作成されている場合、［CRL］タブのツリー認証局オブジェクト上でndspkiCRLContainerDN属性を手動で入力し、CRLを一覧に含める必要があります。

CRLコンテナの削除

CRLコンテナを削除することはできますが、そうすることはお勧めしません。

通常、関連する配布ポイントを含む最後の証明書の有効期限が切れてから1日経過するまで、CRLコンテナ、CRL設定オブジェクト、CRLオブジェクト、CRLファイルは削除しません。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**ディレクトリ管理**］>［**オブジェクトの削除**］の順に選択します。

4 削除するCRLコンテナをブラウズして選択します。

5 ［**OK**］>［**OK**］をクリックします。

CRL設定オブジェクトの作成

CRL設定オブジェクトは、CRLコンテナ内に作成できます。このオブジェクトは、eDirectoryツリーで使用可能なCRLオブジェクトの環境設定情報を格納するものです。通常、ツリーにはCRL設定オブジェクトが1つだけあります。新しい組織認証局を作成またはロールオーバする場合には、複数のCRL設定オブジェクトが必要になりますが、新しい証明書を作成するために使用できるCRL設定オブジェクトは1つだけです。

CRL設定オブジェクトは、CRLコンテナ内に存在します。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**認証局の設定**］の順に選択し、次のいずれかの操作を行います。

- CRLコンテナが存在しない場合は、CRLコンテナとそのコンテナに格納するCRL設定オブジェクトを作成するためのウィザードが起動します。ウィザードに従って操作を完了します。
- CRLコンテナが存在する一方、CRL設定オブジェクトが存在しない場合は、CRLコンテナに格納するCRL設定オブジェクトを作成するためのウィザードが起動します。ウィザードに従って操作を完了します。
- CRLコンテナとCRL設定オブジェクトが存在する場合は、組織認証局のプロパティページが表示されます。ステップ 4に進みます。

4 ［**CRL**］タブをクリックします。

5 ［**新規作成**］をクリックします。

6 新しいCRL設定オブジェクトの名前を入力してから、［**OK**］をクリックします。

注: ここで指定するCRLファイルパスが、eDirectoryインストールパスと対応していることを確認します。

---

7 ウィザードに従って操作を完了します。

CRL設定オブジェクトのアクティブ化

eDirectoryツリー内で複数のCRL設定オブジェクトを同時にアクティブにすることはできません。複数のCRL設定オブジェクトがある場合は、どのオブジェクトをアクティブにするか選択する必要があります。デフォルトでは、最初に作成されたCRL設定オブジェクトがアクティブになります。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQ Certificate Server**］>［**認証局の設定**］の順に選択します。

4 ［**CRL**］タブをクリックします。

5 CRL設定オブジェクトを選択し、［アクティブにする］をクリックします。

6 ［OK］または［適用］をクリックします。

CRL設定オブジェクトのプロパティの表示と変更

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［役割およびタスク］メニューで、［NetIQ Certificate Server］>［認証局の設定］の順に選択します。

4 ［CRL］タブをクリックします。

5 表示または変更するCRL設定オブジェクトの名前をクリックします。

6 ［OK］または［適用］をクリックします。

注: 証明書の検証中に、CRL設定を無効にすることができます。CRL設定を無効にするには、環境変数NDSD_DISABLE_CRL_CONFIGを任意の値に設定する必要があります。すでにCRLが設定されているeDirectoryツリーを使用する場合は、eDirectoryをアップグレードする前に手動でCRL設定オブジェクト(objectclass: ndspkiCRLConfiguration)およびCRL配布ポイントオブジェクト(objectclass: cRLDistributionPoint)を手動で削除してください。

- 749 ページの 「LDAPマッピング」
- 750 ページの 「HTTP配布ポイントの場所」

LDAPマッピング

証明書取り消しリストの標準LDAPタイプでは、CRLのサイズが64KBに制限されます。この制限を変更するには、NetIQ定義済みタイプのCRLディレクトリエントリを作成する必要があります。LDAP配布ポイントを検索できるようにするために、次の手順に従って、標準LDAPタイプをNetIQ LDAPタイプにマップする必要があります。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryにログインします。

3 ［役割およびタスク］メニューで、［LDAP］>［LDAPオプション］の順に選択します。

4 ［LDAPグループの表示］タブをクリックし、マップする必要があるLDAPグループを選択します。

5 ［**一般**］タブをクリックし、［属性マップ］ページを選択して、次の変更を行います。

5a プライマリLDAP属性certificateRevocationList;binary (およびセカンダリ属性certificateRevocationList)からeDirectory属性certificateAuthorityListへのデフォルトマッピングを、eDirectory属性ndspkiCertificateRevocationListに変更します(つまり、eDirectory属性をcertificateAuthorityListからndspkiCertificateRevocationListに変更します)。

5b プライマリLDAP属性authorityRevocationList;binary (セカンダリ属性authorityRevocationList)からeDirectory属性authorityRevocationListへのデフォルトマッピングを、eDirectory属性ndspkiAuthorityRevocationListに変更します(つまり、eDirectory属性をauthorityRevocationListからndspkiAuthorityRevocationListに変更します)。

5c プライマリLDAP属性deltaRevocationList;binary (セカンダリ属性deltaRevocationList)からeDirectory属性deltaRevocationListへのデフォルトマッピングを、eDirectory属性ndspkiDeltaRevocationListに変更します(つまり、eDirectory属性をdeltaRevocationListからndspkiDeltaRevocationListに変更します)。

6 ［OK］をクリックします。

7 ［**役割およびタスク**］メニューで、［**LDAP**］>［**LDAPオプション**］の順に選択します。

8 ［**LDAPサーバの表示**］タブをクリックし、LDAP配布ポイントをホストしているサーバを選択します。

9 ［**一般**］タブをクリックし、［情報］ページを選択します。

10 更新ボタンをクリックします。

これにより、LDAPサービスが再起動して、CRL属性の適切なマッピングを使用するようになります。

LDAP管理の詳細については、389ページの第14章「LDAP Services for NetIQ eDirectoryの環境設定」を参照してください。

HTTP配布ポイントの場所

HTTP配布ポイントを使用するようにCertificate Serverを設定する際は、証明書を検証するユーザがアクセスできる場所を指定することが重要です。配布ポイントが含まれる証明書のCRLをユーザが見つけられなければ、証明書は無効であると見なされます。配布ポイントを配置しなければならない場所は、配布ポイントのHTTPアドレスで指定されたWebサーバが使用できるディレクトリ内です。そのディレクトリが、認証局をホストしているサーバと同じサーバ上にない場合は、CRLを手動で、またはスクリプトを使用して移動するか、マウント済みのディレクトリ上に作成する必要があります。

CRL設定オブジェクトの削除

CRL設定オブジェクトは削除できますが、推奨されていません。CRL設定オブジェクトを削除すると、サーバはCRLファイルを作成しなくなります。CRLオブジェクトで指定された場所にCRLファイルがすでに存在する場合は、有効期限が切れるまで、証明書の検証でそのファイルが使用し続けられます。証明書が期限切れになると、CRL配布ポイントでその既存のCRLファイルを参照しているすべての証明書の検証が失敗します。

通常、関連する配布ポイントを含む最後の証明書の有効期限が切れてから1日経過するまで、CRLコンテナ、CRL設定オブジェクト、CRLオブジェクト、CRLファイルは削除しません。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**ディレクトリ管理**］>［**オブジェクトの削除**］の順に選択します。

4 削除するCRL設定オブジェクトをブラウズして選択します。

5 ［**OK**］>［**OK**］をクリックします。

CRLオブジェクトの作成

このタスクによって、eDirectory内にサードパーティCRLを保管するためのCRLオブジェクト(cRLDistributionPoint)を作成できます。このオブジェクトは、eDirectoryツリー内の任意のコンテナに作成できます。ただし一般的な規則として、NetIQCRLオブジェクトはCRL設定オブジェクト内にあるので、手動で作成する必要はありません。CRL設定オブジェクトを作成すると、CRLオブジェクトが自動的に作成されます。

CRLオブジェクトには、CRLの詳細情報が記載されたCRLファイルが含まれています。NetIQCRLオブジェクトの場合、サーバが新しい証明書を発行するたびに、CRLファイルは自動的に作成および更新されます。その他のCRLオブジェクトの場合、サードパーティの認証局からCRLファイルをインポートする必要があります。

注: CRL配布ポイントという用語は、さまざまな意味で使用されます。配布ポイントとは、CRLオブジェクトのeDirectoryスキーマオブジェクト名であり、一般用語では、CRL情報が公開される場所を意味するために使用されます。

CRLオブジェクトを作成するには、次の手順に従います。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［**役割およびタスク**］メニューで、［**NetIQCertificateServer**］>［**CRLオブジェクトの作成**］の順に選択します。

4 オブジェクトの名前を入力し、オブジェクトを配置するコンテキストを指定します。

5 CRLをコピーしてフィールドに貼り付けるか、CRLファイルから読み込みます。

6 ［**完了**］をクリックしてオブジェクトを作成します。

CRLファイルのエクスポート

CRL配布ポイントオブジェクトに含まれるCRLは、ファイルにエクスポートすることができます。

NetIQ CRLファイルをエクスポートするには、次の手順に従います。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
3. ［役割およびタスク］メニューで、［NetIQ Certificate Server］>［認証局の設定］の順に選択します。
4. ［CRL］タブをクリックします。
5. CRL設定オブジェクトの名前をクリックし、［詳細］をクリックします。
6. エクスポートをクリックします。
7. 出力フォーマットを選択してから［次へ］をクリックします。
8. エクスポートしたCRLをファイルに保存するには、［保存］をクリックし、ファイルの場所を指定します。
9. ［OK］>［OK］をクリックします。

サードパーティのCRLファイルをエクスポートするには、次の手順に従います。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
3. ［役割およびタスク］メニューで、［ディレクトリ管理］>［オブジェクトの変更］の順に選択します。
4. CRL設定オブジェクトをブラウズして選択し、［OK］をクリックします。
5. エクスポートをクリックします。
6. 出力フォーマットを選択してから［次へ］をクリックします。
7. エクスポートしたCRLをファイルに保存するには、［保存］をクリックし、ファイルの場所を指定します。
8. ［OK］>［OK］をクリックします。

CRLファイルの置き換え

CRLファイルを置き換えることはできますが、そうすることはお勧めしません。

1. iManagerを起動します。
2. 適切な権利を持った管理者としてeDirectoryツリーにログインします。

   このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。
3. ［役割およびタスク］メニューで、［NetIQ Certificate Server］>［認証局の設定］の順に選択します。

4 ［CRL］タブをクリックします。

5 CRL設定オブジェクトの名前をクリックし、［詳細］をクリックします。

6 ［置換］をクリックします。

7 ［OK］をクリックして続行します。

8 新しいCRLファイルをブラウズして選択します。

9 OKをクリックします。

CRLファイルがCRL設定オブジェクトにない場合は、［インポート］ボタンが表示されます。

CRLファイルの有効期間の延長

管理者は、iManagerを使用してCRLファイルの有効期間を延長できます。有効期間を延長するには、次の手順を実行します。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［役割およびタスク］メニューで、［NetIQ Certificate Server］>［認証局の設定］の順に選択します。

4 ［CRL］タブをクリックします。

5 CRLファイルの名前をクリックします。

6 ［次のCRL発行］にある［有効期間を延長する時間］を選択し、次のボックスで時間数を指定します。1から12時間までの任意の値をこのフィールドに入力できます。

7 ［今すぐに発行］をクリックします。

CRLオブジェクトのプロパティの表示

NetIQ CRLオブジェクトのプロパティを表示するには、次の手順に従います。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［役割およびタスク］メニューで、［NetIQ Certificate Server］>［認証局の設定］の順に選択します。

4 ［CRL］タブをクリックします。

5 CRL設定オブジェクトの名前をクリックし、［詳細］をクリックします。

これで、CRLオブジェクトのプロパティを確認できます。

6 プロパティを確認し終わったら、［OK］または［適用］をクリックします。

サードパーティのCRLオブジェクトのプロパティを表示するには、次の手順に従います。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［役割およびタスク］メニューで、［ディレクトリ管理］>［オブジェクトの変更］の順に選択します。

4 表示するCRLオブジェクトをブラウズしてクリックし、［OK］をクリックします。

5 ［編集］をクリックします。

これで、CRLオブジェクトのプロパティを確認できます。

6 プロパティを確認し終わったら、［OK］または［適用］をクリックします。

CRLオブジェクトの削除

CRLオブジェクトを削除すると、サーバが次にCRLファイルを生成するときにCRLオブジェクトが再作成されます。iManagerを使用して作成したCRLオブジェクトを削除しそれをインポートする場合、そのオブジェクトは永続的に失われ、そのオブジェクトを参照するすべての証明書は無効と見なされます。

通常、関連する配布ポイントを含む最後の証明書の有効期限が切れてから1日経過するまで、CRLコンテナ、CRL設定オブジェクト、CRLオブジェクト、CRLファイルは削除しません。

1 iManagerを起動します。

2 適切な権利を持った管理者としてeDirectoryツリーにログインします。

このタスクに必要な権利を確認するには、766 ページの 「タスクを実行するために必要なエントリ権」を参照してください。

3 ［役割およびタスク］で、［ディレクトリ管理］>［オブジェクトの削除］の順にクリックします。

4 削除するCRLオブジェクトをブラウズしてクリックします。

5 ［OK］>［OK］をクリックします。

eDirectoryのタスク

- 755 ページの「複数のセキュリティコンテナ、組織認証局、KAPコンテナ、およびW0オブジェクトの解決」
- 755 ページの 「セキュリティコンテナの復元または再作成」
- 756 ページの 「KAPおよびW0の復元または再作成」

複数のセキュリティコンテナ、組織認証局、KAPコンテナ、およびW0オブジェクトの解決

NetIQ Certificate Serverは、eDirectoryツリー内の複数のサーバにインストールできます。ただし、NetIQ Certificate Serverが適切に機能するためには、ツリー内にセキュリティコンテナ、組織認証局、KAPコンテナ、およびW0オブジェクトがそれぞれ1つだけ存在していなければなりません。

NetIQ Certificate ServerをeDirectoryツリー内の複数のサーバにインストールする場合は、eDirectoryにNetIQ Certificate Serverの各インストール間で複製を許可する必要があります。eDirectoryに複製を許可しなければ別のサーバへのインストールで、ツリーにすでにセキュリティコンテナ、組織認証局、KAPコンテナ、およびW0オブジェクトが存在することが認識されず、これらのオブジェクトが同じeDirectoryツリー内の別のサーバで再作成される可能性があります。

以下の項目で、考えられるシナリオとその解決方法について説明します。

- 同じeDirectoryツリー内に、複数のセキュリティコンテナがあり、それぞれのコンテナに組織認証局が含まれていて、1つのKAPコンテナ内に1つのW0オブジェクトがある場合は、証明書を発行しないでください。この問題を解決するには、テクニカルサポート部門にお問い合わせください。
- 同じeDirectoryツリー内に、2つのKAPコンテナが含まれる1つのセキュリティコンテナがある場合は、証明書を発行しないでください。この問題を解決するには、テクニカルサポート部門にお問い合わせください。
- 同じeDirectoryツリー内に、2つの組織認証局が含まれる1つのセキュリティコンテナがあり、1つのW0オブジェクトが含まれる1つのKAPコンテナがある場合、両方の組織認証局から発行されたすべてのサーバ証明書とユーザ証明書を削除します。次に、両方の認証局を削除してから新しい組織認証局を作成します。必要に応じて、新しいサーバ証明書とユーザ証明書を発行します。
- 同じeDirectoryツリー内に、複数のセキュリティコンテナがあり、それぞれのコンテナに組織認証局が含まれている一方、W0オブジェクトが含まれるKAPコンテナが1つしかない場合は、すべての組織認証局から発行されたすべてのサーバ証明書とユーザ証明書を削除します。さらに、KAPコンテナとW0オブジェクトが含まれていないすべてのセキュリティコンテナを削除します。残りのセキュリティコンテナの名前が*セキュリティ*ではない場合は、名前を*セキュリティ*に変更します。必要に応じて、新しいサーバ証明書とユーザ証明書を発行します。
- 同じeDirectoryツリー内に、複数のセキュリティコンテナがあり、そのうち1つのコンテナだけに、組織認証局とKAPコンテナおよびその中のW0オブジェクトが含まれている場合は、KAPコンテナとW0オブジェクトが含まれていないすべてのセキュリティコンテナを削除します。残りのセキュリティコンテナの名前が*セキュリティ*ではない場合は、名前を*セキュリティ*に変更します。

セキュリティコンテナの復元または再作成

セキュリティコンテナを削除した場合、セキュリティコンテナを復元または再作成するまでは、組織認証局を作成することができません。

セキュリティコンテナを復元するには、セキュリティコンテナが含まれるeDirectoryのパーティションを復元します。

セキュリティコンテナを再作成するには、次の2つの方法のいずれかを使用します。

- iManagerで、［**ディレクトリ管理**］>［**オブジェクトの作成**］の順にクリックします。［**ツリーのセキュリティコンテナ**］をクリックし、［**OK**］をクリックします。コンテナ名は「セキュリティ」でなければなりません。
- eDirectoryツリー内の任意のサーバに、NetIQ Certificate Serverを再インストールします。

KAPおよびW0の復元または再作成

KAPまたはW0オブジェクトを削除しないでください。削除すると、それまでに作成したすべてのユーザ証明書が無効になります。これらのオブジェクトのいずれかを削除した場合は、Novellサポートwebサイト (http://support.novell.com/)にアクセスし、TID番号3032354の「How to Restore or Recreate KAP and W0 Objects」を検索し、KAPおよびW0を復元してこの問題を解決する方法を参照してください。問題が修正されるまでは、NetIQ Certificate Server、Single Sign-on、NMAS、またはeDirectoryをインストールしようとしないでください。

アプリケーションのタスク

このセクションでは、NetIQ証明書を使用するように暗号化対応アプリケーションを設定する方法について説明します。

このセクションに記載する情報の一部は最新のものではありませんが、参考になります。暗号化対応アプリケーションで証明書を使用する方法の最新情報については、アプリケーションのマニュアルを参照してください。

セキュリティで保護された電子メールをアプリケーションで使用できるようにするための一般的なプロセスは、次のとおりです。

1. 組織認証局の自己署名証明書(717 ページの 「組織認証局の自己署名証明書のエクスポート」を参照)、ユーザ証明書、および証明書と一致する秘密鍵を.pfxファイルにエクスポートします(735 ページの 「ユーザ証明書と秘密鍵のエクスポート」を参照)。
2. .pfxファイルを電子メールクライアントにインポートします。
3. 電子メールを保護するように電子メールクライアントを設定します。

ブラウザを使用して、インターネットでサーバに対するSSL接続を作成するためには、ユーザ証明書またはサーバ証明書に署名した認証局を信頼する必要があります。認証局を信頼していなければ、アプリケーションがエラーを表示する可能性があります。一部のアプリケーションでは、警告メッセージで、そのアプリケーションにまだ既知ではない認証局が発行したユーザ証明書またはサーバ証明書の受諾または拒否を選択できるようになっています。企業の組織認証局によって署名されたサーバ証明書またはユーザ証明書は、常にこのような警告およびエラーを生成します。これは、組織認証局が、アプリケーションで信頼する認証局としてリストされていないためです。組織認証局の自己署名証明書をアプリケーションにインストールすることで、このような警告やエラーを防ぐことができます。組織認証局をブラウザにインストールすると、組織認証局が自動的に信頼する認証局として追加されます。

アプリケーションで組織認証局を信頼する認証局として受け入れるようにするには、次の手順に従います。

1. 組織認証局の自己署名証明書をエクスポートします(717 ページの 「組織認証局の自己署名証明書のエクスポート」を参照)。

注: インターネットブラウザは、.derまたは.crtフォーマットの証明書を認識します。

2. ブラウザのマニュアルで説明されている指示に従って、ブラウザに証明書をインポートします。

PKIヘルスチェック

NetIQ Certificate Serverには、Certificate Serverコンポーネントのヘルスと整合性を維持するプロセスが組み込まれています。このプロセスは、PKIヘルスチェックと呼ばれ、次のタイミングで実行されます。

- サーバが再起動するとき。
- eDirectoryが起動するとき。
- DSRepairの実行が終了するとき。

PKIヘルスチェックによって、次のタスクが実行されます。

***表 25-1** PKIヘルスチェックのタスク*

タスク	機能
SASサービスオブジェクトへのサーバのリンクの検証	このタスクでは、サーバオブジェクトからSAS:Serviceオブジェクトへのリンクの有無を確認します。リンクが存在する場合、オブジェクトに適切な名前が付けられていて、オブジェクトがサーバと同じコンテキスト内にあることを確認します。リンクが存在しない場合、適切に名前が付けられたオブジェクトがサーバと同じコンテキスト内にあるかどうかを確認します。そのようなオブジェクトが存在する場合、サーバからオブジェクトへのリンクを作成します。
SASサービスオブジェクトの検証	このタスクでは、SAS:Serviceオブジェクトの有無を確認します。存在しない場合は新しいオブジェクトを作成し、サーバオブジェクトから新規オブジェクトへのリンクを作成します。その後、SAS:ServiceオブジェクトにeDirectoryに対する必要な権利があるかどうかを確認します。必要な権利がなければ、SAS:Serviceオブジェクトに必要な権利を与えようと試みます。
KMOへのリンクの検証	このタスクでは、SAS:Serviceオブジェクトにリンクされているサーバ証明書オブジェクト(KMO)のリストを読み込みます。KMOのすべてに適切な名前が付けられているかどうかを確認し、適切でない名前を修正します。このタスクでは、KMOのすべてがサーバオブジェクトと同じコンテキスト内にあるかどうかも確認し、必要に応じて正しいコンテキストに移動しようと試みます。

タスク	機能
サーバ証明書(KMO)の確認	このタスクでは、サーバオブジェクトと同じコンテナ内にあるすべてのKMOの名前を読み込んでリストに取り込みます。続いて、リストに含まれるKMOごとに次の処理を行います。 ◆ NDSPKI:Not Before属性とNDSPKI:Not After属性に、証明書の有効期限日を取り込もうとします。 ◆ パブリックにホストサーバ属性に対する読み込み権があるかどうかを確認します。 ◆ KMOからサーバへのバックリンクを確認します。バックリンクが異なるサーバを対象としている場合、KMOを無視してリストから削除します。 ◆ 秘密鍵を読み取ってラップ解除を試みます。
KMOへのリンクの再検証	このタスクでは、SAS:Serviceオブジェクトにリンクされているサーバ証明書オブジェクト(KMO)のリストを読み込みます。このリスト内の各KMOを、サーバ証明書(KMO)の確認で作成したリストと照合します。サーバ証明書(KMO)の確認を使用して、リンクされている証明書に問題がないかどうかを確認し、KMOが使用できない場合は証明書のリンクを解除します。このタスクでは、このサーバで使用できるリンク解除済みKMOがあるかどうかを確認し、存在する場合はそのKMOをリンクします。
デフォルト証明書の作成	このタスクでは、サーバ自己プロビジョニングが組織認証局オブジェクトで有効にされているかどうかを確認します。サーバ自己プロビジョニングが有効にされていない場合、このステップはスキップされます。サーバ自己プロビジョニングが有効にされている場合、NPKICreateDefaultCertificates() APIを呼び出します。このAPIは、次の条件に当てはまる場合はSSL CertificateDNS証明書を作成または置換します。 ◆ 証明書が存在しない場合。 ◆ 証明書に有効期限がないか、証明書が間もなく期限切れになる場合。 ◆ 証明書のサブジェクト名が、サーバに設定されているデフォルトのIPアドレスおよびDNSアドレスと一致しない場合。 **注:** eDirectoryでは、SSL CertificateIPは自動的に作成されません。SSL証明書DNSには、［サブジェクトの代替名］にリストされているすべてのIPが含まれます。 さらに、このAPIは、サーバに設定されているIPアドレスおよびDNSアドレスをすべて取得し、次の条件に当てはまる場合は各アドレスの証明書を作成または置換します(IP AG *ip address*、IP DNS *dns nam*など)。 ◆ 証明書が存在しない場合。 ◆ 証明書の有効期限が切れているか、証明書が間もなく期限切れになる場合。

タスク	機能
外部サービスの証明書の同期化	このタスクでは、SAS:Serviceオブジェクトから環境設定を読み込みます。設定済みの各エントリに対して、指定のKMOオブジェクトから証明書と秘密鍵を取得します。指定のディレクトリが存在しない場合、そのディレクトリの作成を試みます。次に、秘密鍵をラップ解除して、暗号化されていないフォーマットに変換します。既存の秘密鍵と証明書ファイルを、指定のKMOのものと比較します。鍵と証明書が同じではない場合、既存の秘密鍵と証明書ファイルのバックアップを作成し、既存の秘密鍵と証明書で上書きします。鍵はPEMフォーマットで書き出されます。
ファイルシステムへのeDirectory認証局証明書のエクスポート	このタスクを実行する方法は、実行しているオペレーティングシステムによって異なります。 SSCert.derおよびSSCert.pemファイルには、組織認証局のRSA証明書が含まれます。組織認証局にECDSA証明書がある場合、eDirectoryはECDSA証明書をSSECCert.derおよびSSECCert.pemファイルにエクスポートして、それらのファイルをSSCert.derおよびSSCert.pemファイルと同じディレクトリに保管します。 ◆ **Windows:** PKI作業ディレクトリ内のSSCert.derおよびSSCert.pemにファイルに、eDirectory内の組織認証局の証明書と同じ証明書が含まれているかどうか確認します。同じでない場合は、ファイルの置換を試みます。 デフォルトのPKI作業ディレクトリ: c:\Novell\NDS\DIBFiles\CertServ\ ◆ **Linux (OES Linux以外)の場合:** eDirectoryデータディレクトリ内のSSCert.derおよびSSCert.pemにファイルに、eDirectory内の組織認証局の証明書と同じ証明書が含まれているかどうか確認します。同じでない場合は、ファイルの置換を試みます。 デフォルトのeDirectoryデータディレクトリ: /var/opt/novell/eDirectory/data ◆ **OES Linux:** /etc/opt/novell/certs/SSCert.derおよび/etc/opt/novell/certs/SSCert.pemファイルに、eDirectory内の組織認証局の証明書と同じ証明書が含まれているかどうか確認します。証明書が同じではない場合、ファイルを置き換えるために、組織認証局の証明書を/etc/ssl/certsディレクトリに追加してから、c_rehashプログラムを実行します。ただし、ファイルを置き換える前に、既存のすべての証明書のバックアップを作成します。

公開鍵暗号化の基本

このセクションでは、公開鍵暗号化の基本について説明します。

- 760 ページの 「概要」
- 760 ページの 「セキュアなデータ転送」

- 760 ページの 「鍵ペア」
- 763 ページの 「信頼関係の確立」

概要

Webページのブラウズや公開チャットフォーラムなど、ほとんどのインターネット通信のコンテンツは、必要なデバイスを持っていれば誰でもモニタすることができます。オンラインショッピングでのクレジットカード情報のやり取りといったデータ転送のコンテンツは、機密にしておかなければなりません。

公開鍵暗号化は、インターネット上でのデータ転送を機密にして保護するために広く使用されている手法です。具体的には、公開鍵暗号化とは、メッセージの送信者を認証するため、そしてメッセージのコンテンツを暗号化するために、「鍵」と呼ばれるデジタルコードを使用するシステムのことを指します。

セキュアなデータ転送

データ転送は、次の2つによって機密かつセキュアになります。

- **認証:** データ受信者が、データ送信者の身元、またはデータ送信者が主張する本人そのものであることを把握します。
- **暗号化:** 送信されるデータは、対象とする受信者だけが読み取れるように暗号化されます。

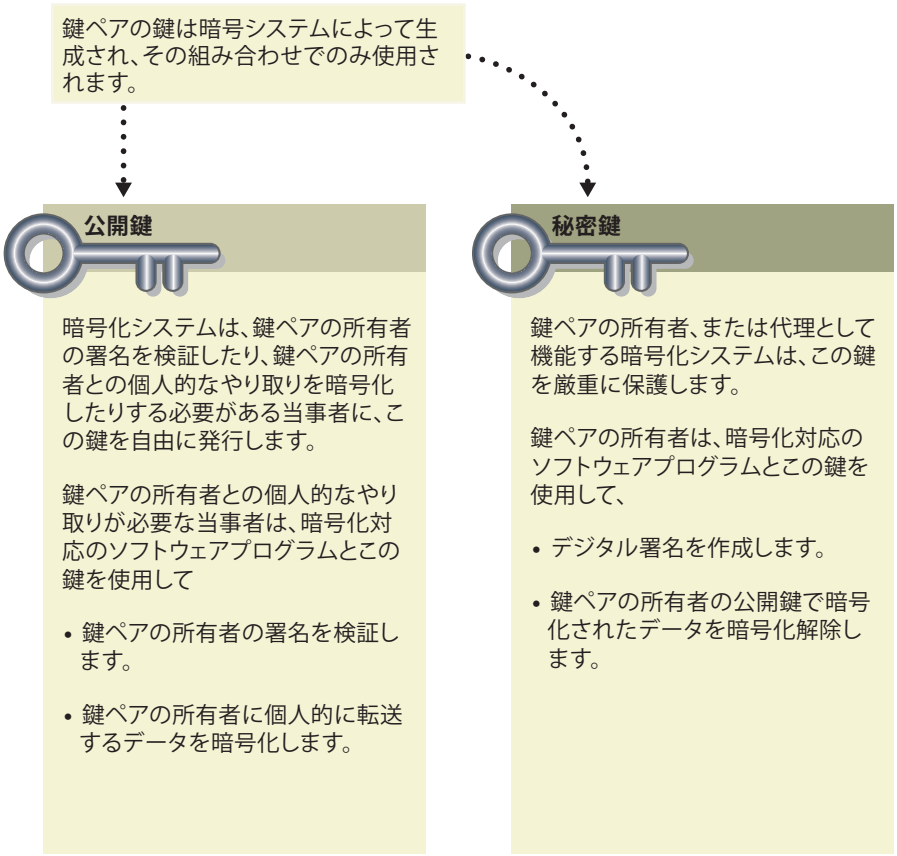
鍵ペア

認証と暗号化はどちらも、関連するデジタルコード、つまり「鍵」のペアを使用して行われます。各ペアの一方の鍵は一般に配布され、もう一方の鍵は厳重に機密保持されます。

データ送信者のそれぞれには、それが個人、ソフトウェアプログラム、また銀行や企業などの機関であるかに関わらず、公開鍵暗号化システムによって鍵ペアが発行されます。

鍵ペアを構成する各鍵の基本的な原則と役割について、以下の図に要約します。

図 25-1 鍵ペアの基本的な説明



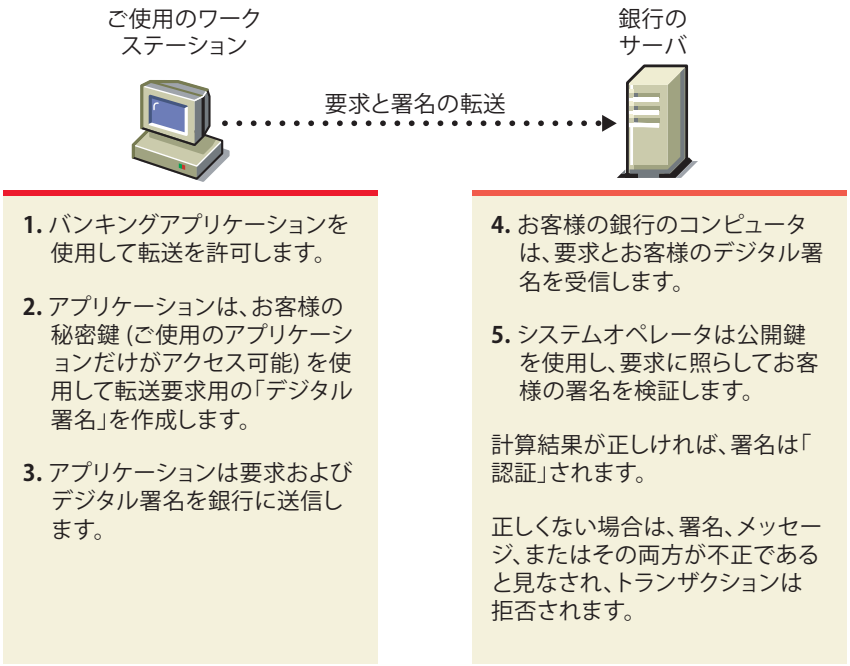
- 761 ページの 「鍵ペアと認証」
- 762 ページの 「鍵ペアと暗号化」

鍵ペアと認証

「認証」とは、データ送信者が誰であるか、またはデータ送信者が主張するデータ送信元を、データ受信者が正確に把握することを意味します。

たとえば、銀行に、自分の口座から別の口座への送金を許可するとします。その場合、銀行は、そのメッセージを送信したのが口座名義人本人であること、そしてメッセージが送信中に改ざんされていないことを証明しなければなりません。以下の図に、公開鍵暗号化を使用したオンライントランザクションのプロセスを示します。

図 25-2　公開鍵によるプロセス



デジタル署名とその検証については、764 ページの 「デジタル署名」を参照してください。

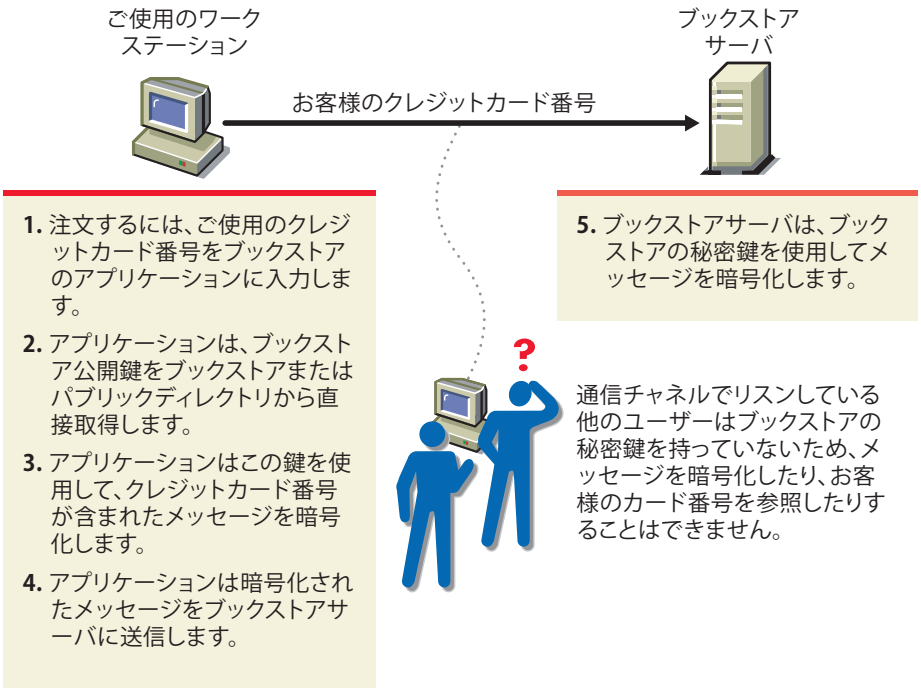
鍵ペアと暗号化

*暗号化*とは、対象とする受信者だけがデータを読み取れることを意味します。

たとえば、インターネットのベンダに本を注文して、その代金の支払にクレジットカードを使用しなければならないとします。対象とする受信者以外には、誰にもクレジットカード番号が読み取られないようにしなければなりません。

以下の図に示す暗号化プロセスが、クレジットカード番号を安全に送信するメカニズムを提供します。

図 25-3　暗号化プロセス



信頼関係の確立

送信者と受信者が互いを知っていて信頼している場合、公開鍵を交換するだけで、認証と暗号化を含めたセキュアなデータ転送を確立できます。この場合、送信者と受信者のそれぞれが、相手の公開鍵と自分の公開鍵を使用します。

しかし通常は、セキュアなデータ転送を必要とする当事者には、互いの識別情報を信頼する基盤がありません。送信者と受信者が共通して信頼するサードパーティに、それぞれの識別情報を証明してもらう必要があります。

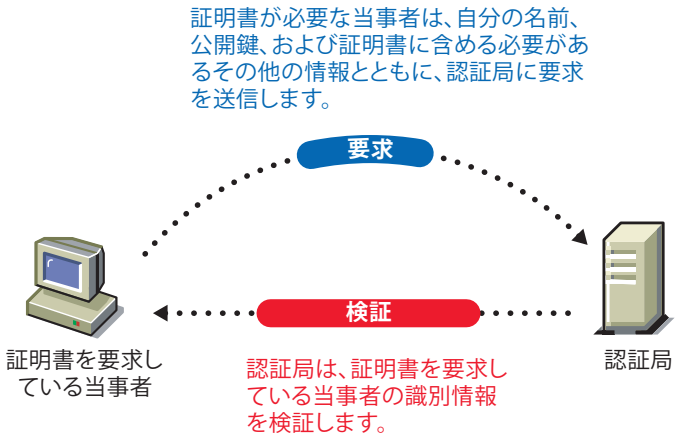
- 763 ページの 「認証局」
- 764 ページの 「デジタル署名」
- 765 ページの 「証明書チェーン」
- 766 ページの 「ルート認証局」

認証局

公開鍵暗号化環境で識別情報を証明する必要がある当事者は、認証局と呼ばれる、信頼できるサードパーティのサービスを利用します。

認証局の主な目的は、当事者の身元または当事者が主張している本人であることを検証してから、その当事者が使用するための公開鍵証明書を発行することです。公開鍵証明書は、その証明書に含まれる公開鍵が、証明書に指名されている当事者に属することを検証するためのものです。

図 25-4　証明書要求



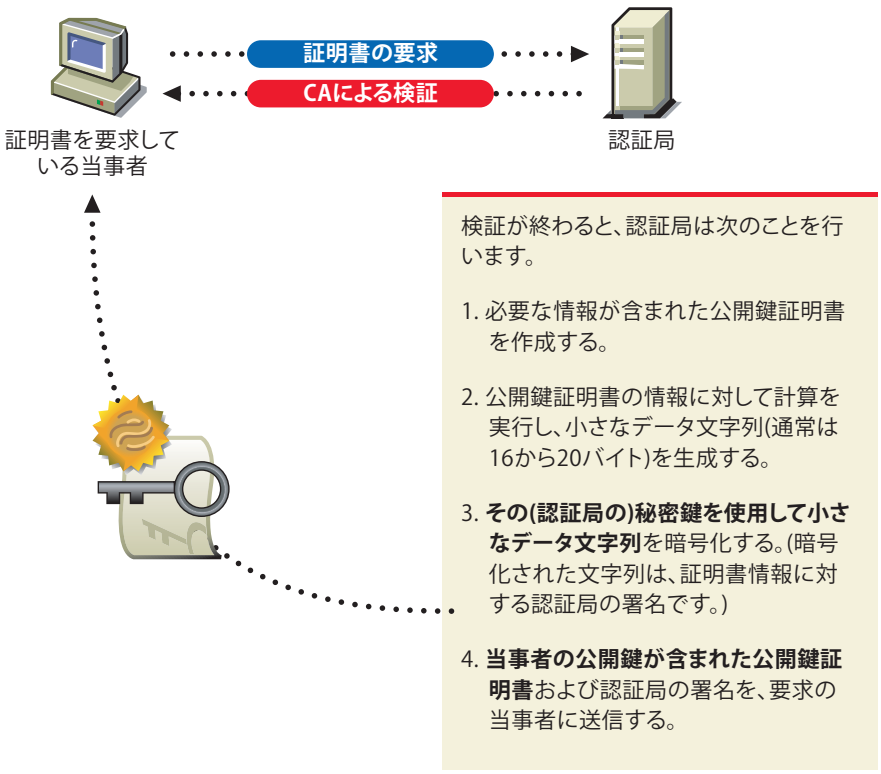
認証局は、証明書を要求している当事者の識別情報が正しいものであると認めると、電子「証明書」を発行し、その証明書にデジタル署名を付けます。

デジタル署名

紙の文書上の個人の署名がその文書の信ぴょう性を表すのと同じく、デジタル署名は電子データの信ぴょう性を表します。

デジタル署名を作成するには、署名の作成に使用されるソフトウェアで、署名を付けたデータを署名者の秘密鍵にリンクします。以下の図に、認証局が公開鍵証明書のデジタル署名を作成するために従うプロセスを示します。

図25-5　デジタル署名



デジタル署名は、署名者とデータを固有にリンクします。署名者以外は、署名者の秘密鍵を持っていないため、署名を複製することはできません。さらに、署名者がデータに署名したことを否認することもできません。これは、「否認防止」と呼ばれます。

認証局が公開鍵証明書に署名を付けるということは、認証局がその公開している確立済みのポリシーに従って、公開鍵の所有者の識別情報を確認したことを保証するということです。

署名付きのデータ(公開鍵証明書など)を受信すると、署名作成ソフトウェアは当初使用した計算と同じ計算をそのデータに適用して、データの信ぴょう性を検証します。データが改ざんされていなければ、両方の計算で同じ結果が出ます。これにより、データも署名も送信中に改ざんされていないと確実に見なすことができます。

証明書チェーン

証明書チェーンとは、順序付けられた証明書のリストのことです。証明書は、サーバ証明書またはユーザ証明書の後に、その証明書を発行した認証局の証明書が続くように順序付けられます。

認証局の証明書には、認証局自体が署名を付ける場合も(つまり、自己署名証明書)、別の認証局が署名を付ける場合もあります。自己署名証明書を使用する認証局は、一般にルート認証局と呼ばれます。自己署名証明書を使用しない認証局は、一般に従属認証局または中間認証局と呼ばれます。

ユーザ証明書またはサーバ証明書が、自己署名証明書を使用する認証局によって署名付けされている場合、証明書チェーンは、エンドエンティティの証明書とルート認証局証明書だけで構成されます。

ユーザ証明書またはサーバ証明書が中間認証局によって署名付けされている場合は、証明書チェーンが長くなります。最初の2つの要素は同じくエンドエンティティの証明書と、その後に続く中間認証局の証明書です。ただし、中間認証局の証明書の後には、その上位認証局の証明書が続きます。

このリストが、最後の証明書がルート認証局証明書になるまで続きます。したがって、証明書チェーンは無限に長くなる可能性があります。しかし実際には、ほとんどの証明書には2つか3つの証明書しかありません。

ルート認証局

ユーザ証明書またはサーバ証明書チェーンを構成する証明書のうち、少なくとも1つの証明書を信頼しなければ、デジタル署名を検証することはできません。ユーザまたはサーバの証明書自体を信頼することも、チェーンを構成する任意の証明書を信頼することもできます。通常、信頼する証明書は、ルート認証局証明書です。

証明書を使用できるアプリケーションソフトウェアの大半には、信頼する証明書のリストがすでにインストールされています。これらの証明書はルート認証局のものなので、「信頼されたルート」と呼ばれます。ルート認証局は一般に、営利目的の認証局です。必要に応じて、信頼する証明書のリストに他の認証局を追加したり、リストから認証局を削除したりできます。

タスクを実行するために必要なエントリ権

以下のリストに、管理者がeDirectoryツリー内でNetIQ Certificate Serverタスクを管理するために必要となる、具体的なエントリ権を記載します。これらの権利は、必要最小限のエントリ権です。

このリストは、会社の証明書認証局および証明書管理の一部またはすべてを管理させるために、管理者が別のユーザに権利を付与する場合にも役立ちます。

***表 25-2** 管理者のエントリ権*

タスク	必要なエントリ権
NetIQ Certificate Serverのインストール	eDirectoryツリーへの初期インストール: ◆ ツリーのルートに対するスーパバイザ 後続のインストール: ◆ W0オブジェクトに対するスーパバイザ ◆ サーバ証明書オブジェクトを作成するために必要な権利 ユーザがサーバ証明書オブジェクトを作成するために必要な権利を持っていない場合、インストールは終了しますが、必要な権利を持つユーザが手動でサーバ証明書オブジェクトを作成し、これらのサーバ証明書を使用するアプリケーションを手動で設定する必要があります。
組織認証局の作成	◆ セキュリティコンテナに対するスーパバイザ
組織認証局のプロパティと証明書の表示	◆ 組織認証局のオブジェクトに対するブラウズ
組織認証局の証明書のエクスポート	◆ 組織認証局のオブジェクトに対するブラウズ

タスク	必要なエントリ権
公開鍵証明書の発行	◆ 組織認証局のオブジェクトのNDSPKI:Private Key属性に対する読み込み ただし、公開鍵証明書を発行しようとしているオブジェクトがNCPサーバの場合は、次の権利が必要です。 ◆ 組織認証局のオブジェクトのNDSPKI:Private Key属性に対する書き込み
組織認証局のバックアップと復元	◆ 組織認証局のオブジェクトに対するスーパバイザ
組織認証局の別のサーバへの移動	◆ 組織認証局のオブジェクトに対するスーパバイザ
組織認証局の証明書の検証	◆ 組織認証局のオブジェクトに対するブラウズ
組織認証局の置き換え	◆ 組織認証局のオブジェクトに対するスーパバイザ
組織認証局の削除	◆ 組織認証局のオブジェクトに対する削除
サーバ証明書オブジェクトの作成	◆ サーバのコンテナに対するスーパバイザ ◆ 組織認証局のオブジェクトのNDSPKI:Private Key属性に対する読み込み(組織認証局を使用する場合のみ) ただし、公開鍵証明書を発行しようとしているオブジェクトがNCPサーバの場合は、次の権利が必要です。 ◆ サーバのコンテナに対するスーパバイザ ◆ 組織認証局のオブジェクトのNDSPKI:Private Key属性に対する書き込み
サーバ証明書オブジェクトへの公開鍵証明書のインポート	◆ サーバ証明書オブジェクトのNDSPKI:Public Key Certificate属性に対する書き込み ◆ サーバ証明書オブジェクトのNDSPKI:Certificate Chain属性に対する書き込み
サーバ証明書オブジェクトの削除	◆ サーバ証明書オブジェクトに対する削除
サーバ証明書オブジェクトからのルート認証局または公開鍵証明書のエクスポート	◆ サーバ証明書オブジェクトに対するブラウズ
サーバ証明書オブジェクトのプロパティと証明書の表示	◆ サーバ証明書オブジェクトに対するブラウズ
サーバ証明書オブジェクトのバックアップと復元	◆ バックアップするサーバ証明書オブジェクトを所有するサーバオブジェクトに対するスーパバイザ ◆ 復元するサーバオブジェクトのコンテナに対する作成

タスク	必要なエントリ権
サーバ証明書の検証	◆ サーバ証明書オブジェクトに対するブラウズ
サーバ証明書の取り消し	◆ 認証局秘密鍵に対する読み込み、サーバ証明書オブジェクトに対する削除、またはホストサーバ(つまり、NCP™サーバオブジェクト)に対するスーパバイザ
サーバ証明書の鍵生成要素の置換	◆ サーバ証明書オブジェクトのNDSPKI:PrivateKey属性に対する書き込み
ユーザ証明書の作成	◆ 組織認証局のオブジェクトのNDSPKI:Private Key属性に対する読み込み ◆ ユーザオブジェクトのNDSPKI:userCertificateInfo属性に対する読み込みと書き込み ◆ ユーザオブジェクトのSAS:SecretStore属性に対する読み込みと書き込み ◆ ユーザオブジェクトのuserCertificate属性に対する読み込みと書き込み ただし、公開鍵証明書を発行しようとしているオブジェクトがNCPサーバの場合は、次の権利が必要です。 ◆ 組織認証局のオブジェクトのNDSPKI:Private Key属性に対する書き込み ◆ ユーザオブジェクトのNDSPKI:userCertificateInfo属性に対する読み込みと書き込み ◆ ユーザオブジェクトのSAS:SecretStore属性に対する読み込みと書き込み ◆ ユーザオブジェクトのuserCertificate属性に対する読み込みと書き込み
ユーザオブジェクトへの公開鍵証明書のインポート	◆ ユーザオブジェクトのNDSPKI:userCertificateInfo属性に対する読み込みと書き込み ◆ ユーザオブジェクトのNDSPKI:userCertificate属性に対する読み込みと書き込み
ユーザ証明書のプロパティの表示	◆ ユーザオブジェクトに対するブラウズ
ユーザ証明書のエクスポート	◆ ユーザオブジェクトに対するブラウズ
ユーザの秘密鍵と証明書のエクスポート	◆ ユーザとしてログインする必要がある
ユーザ証明書と秘密鍵の削除	◆ NDSPKI:userCertificateInfo属性に対する読み込みと書き込み ◆ userCertificate属性に対する読み込みと書き込み
ユーザ証明書の検証	◆ ユーザオブジェクトに対するブラウズ

タスク	必要なエントリ権
ユーザ証明書の取り消し	◆ 認証局証明書の秘密鍵に対する読み込み、ユーザオブジェクトに対する削除、またはそのユーザとしてログインしている場合はuserCertificate属性に対する書き込み
ルート認証局コンテナの作成	◆ セキュリティコンテナに対する作成
ルート認証局オブジェクトの作成	◆ ルート認証局オブジェクトを配置するルート認証局コンテナに対する作成
ルート認証局オブジェクトのプロパティの表示	◆ ルート認証局オブジェクトに対するブラウズ
ルート認証局証明書の置き換え	◆ ルート認証局オブジェクトのNDSPKI:Not After属性に対する読み込みと書き込み ◆ ルート認証局オブジェクトのNDSPKI:Not Before属性に対する読み込みと書き込み ◆ ルート認証局オブジェクトのNDSPKI:SubjectName属性に対する読み込みと書き込み ◆ ルート認証局オブジェクトのNDSPKI:ルート認証局の証明書属性に対する読み込みと書き込み
ルート認証局証明書の検証	◆ ルート認証局オブジェクトに対するブラウズ
ルート認証局証明書の取り消し	◆ 認証局秘密鍵に対する読み込み、またはルート認証局オブジェクトに対する削除
ルート認証局オブジェクトの削除	◆ ルート認証局オブジェクトに対する削除
CRLコンテナの作成	◆ セキュリティコンテナに対するスーパバイザ ◆ 組織認証局のオブジェクトのndspkiCRLContainerDN属性に対する書き込み
CRLコンテナの削除	◆ CRLコンテナに対する削除
CRL設定オブジェクトの作成	◆ CRLコンテナに対するスーパバイザ
CRL設定オブジェクトのアクティブ化	◆ 組織認証局のオブジェクトのndspkiCRLConfigurationDNList属性に対する書き込み

タスク	必要なエントリ権
CRL設定オブジェクトのプロパティの表示と変更	変更: ◆ CRL設定オブジェクトに対するスーパバイザ または ◆ CRL設定オブジェクトで変更する属性に対する書き込み 表示: ◆ CRL設定オブジェクトに対するブラウズ
CRL設定オブジェクトの削除	◆ CRL設定オブジェクトに対する削除
CRLオブジェクトの作成	◆ CRL設定オブジェクトに対するスーパバイザ
CRLファイルのエクスポート	◆ certificateRevocationList属性に対する読み込み
CRLファイルの置き換え	◆ CRLオブジェクトに対するブラウズ
CRLオブジェクトのプロパティの表示	◆ certificateRevocationList属性に対するブラウズ
CRLオブジェクトの削除	◆ CRL配布ポイントに対する削除
セキュリティコンテナの作成	◆ eDirectoryツリーのルートに対する作成
SASサービスオブジェクトの作成	◆ オブジェクトのコンテナに対するスーパバイザ ◆ オブジェクトを作成するサーバのSAS:Service DN属性に対する書き込み

26 パスワードを管理する

このセクションでは、ユニバーサルパスワード、パスワードポリシー、およびパスワードセルフサービスの概要を説明します。

ユニバーサルパスワードについて

ユニバーサルパスワードは、NMAS (NetIQモジュラー認証サービス)モジュールのコンポーネントである、セキュアパスワードマネージャで管理します。セキュアパスワードマネージャは、さまざまなNetIQ製品とNetIQパートナーの製品で、パスワードベースの認証方式の管理を簡素化します。管理ツールは1つのパスワードだけを公開し、下位互換性に対応するための舞台裏の処理をすべて公開することはしません。

セキュアパスワードマネージャと、ユニバーサルパスワードを管理または使用するその他のコンポーネントは、eDirectoryの一部としてインストールされます。ただし、ユニバーサルパスワードはデフォルトで有効になっていません。認証とパスワード設定用のすべてのAPIがユニバーサルパスワードをサポートするように移行されるので、既存のすべての管理ツールは、これらの新しいライブラリを備えたクライアント上で実行すると、自動的にユニバーサルパスワードと連動します。

注: iManager 3.x対応NetIQ eDirectory用のパスワード管理プラグインは、NetIQのダウンロードWebサイトからダウンロードできます。このプラグインをダウンロードしてインストールする方法については、ダウンロードサイトを参照してください。

Novell Clientソフトウェアは、ユニバーサルパスワードをサポートしています。また、ネットワーク内の既存システムのために、引き続きNDSパスワードもサポートしています。ユーザに対してユニバーサルパスワードを設定して有効にすると、Novell Clientの機能によって、自動的にNDSパスワードがユニバーサルパスワードにアップグレード/マイグレートされます。

ユニバーサルパスワードの安全性

他のパスワードシステムとの相互運用を容易にするには、復号可能なユニバーサルパスワード暗号化が必要です。管理者は、そのシステムのコストと利点を評価する必要があります。eDirectoryに保管されたユニバーサルパスワードを使用すると、複数の異なるパスワードを管理しようとする場

合よりも、セキュリティが強化されたり、より便利になったりする可能性があります。NetIQでは、eDirectoryに保管されたユニバーサルパスワードが確実に保護されるよう、複数のレベルでセキュリティを提供しています。

ユニバーサルパスワードは、次の3つのレベルのセキュリティで保護されます。

- パスワード自体の暗号化
- eDirectoryの権利
- ファイルシステムの権利

ユニバーサルパスワードは、ユーザ固有の鍵で暗号化されます。ユニバーサルパスワードとユーザの鍵は、どちらもeDirectoryのみが読み込めるシステム属性に格納されます。ユーザの鍵は、ツリー鍵を使用して暗号化されて保管されます。ツリー鍵は、各マシンで固有のNovell International Cryptographic Infrastructure (NICI)鍵によって保護されます。ツリー鍵もNICI鍵もeDirectory内には保管されないことに注意してください。つまり、これらの鍵と、これらの鍵で保護するデータが一緒に保管されることはありません。

ツリー鍵は各マシン上のツリー内にありますが、ツリーごとにツリー鍵は異なります。したがって、あるツリー鍵で暗号化されたデータは、同じツリー内のマシン上でしか元に戻すことはできません。このように、ユニバーサルパスワードは保管されている間、3重の暗号化によって保護されます。

それぞれの鍵は、eDirectoryの権利によっても保護されます。ユニバーサルパスワードを変更する権利を持つのは、スーパバイザ権を持つ管理者、またはその鍵を所有するユーザだけです。

ファイルシステムの権利は、適切な権利を持つユーザだけに鍵へのアクセスを許可するために使用されます。

デフォルトでは、ユーザ固有の鍵とツリー鍵は3 DES鍵です。eDirectory 9.2では、AES 256ビットキーをサポートしています。AES 256ビットのツリーキーを作成する方法については、『NICI Administration Guide (NICI管理ガイド)』の「Creating an AES 256-Bit SDI Key」を参照してください。管理者は、diagpwdユーティリティを使用してパスワードを再暗号化できます。詳細については、804 ページの 「ユニバーサルパスワードの診断ユーティリティ」を参照してください。

注: このユーティリティを実行するユーザが自分のユニバーサルパスワードを取得できるように、パスワードポリシーが設定されている必要があります。

高度なセキュリティを必要とする環境にユニバーサルパスワードを導入する場合は、次の対策を講じることができます。

1. 次のディレクトリとファイルがセキュリティで保護されていることを確認します。

プラットフォーム	ディレクトリまたはファイル
Windows	◆ %SystemRoot%\SysWOW64\Novell\nici ◆ %SystemRoot%\System32\ (NICI DLLのインストール先)
Linux	◆ /var/opt/novell/nici ◆ /etc/opt/novell/nici64.cfg ◆ /opt/novell/lib64/libccs2.so、および同じディレクトリ内のNICI共有ライブラリ

NICIおよびeDirectoryのファイルの具体的な場所について詳しくは、ご使用のシステムのマニュアルを参照してください。

2. 他のセキュリティシステムの場合と同様に、鍵が保管されているサーバへの物理的アクセスを制限することは非常に重要です。

ユニバーサルパスワード

従来、パスワードのさまざまな制限のために、管理者は複数のパスワード(簡易パスワード、NDSパスワード、拡張パスワード)を管理する必要がありました。さらに、複数のパスワードを同期させる必要もありました。

- NDSパスワード: 古いNDSパスワードは、非可逆性のハッシュ形式で保管されます。このパスワードはNDSシステム専用であり、他の任意のシステムで使える別のフォームに変換することはできません。
- 簡易パスワード: 簡易パスワードは、当初、管理者がユーザとパスワード(平文およびハッシュ化)を外部(Active DirectoryやiPlanetなど)のnds-cluster-configディレクトリからインポートできるようにするために実装されました。

  簡易パスワードには、パスワードポリシー(最小長、有効期限など)が適用されないという制約があります。
- 拡張パスワード: NetIQでは拡張パスワードをサポートしなくなっています。拡張パスワードは、ユニバーサルパスワードの前身です。拡張パスワードには何らかのパスワードポリシーが適用されますが、その設計には他のパスワードとの一貫性がありません。このパスワードは、片方向同期を提供し、単純パスワードやNDSパスワードに取って代わるパスワードです。

NetIQでは、さまざまなパスワードシステムと認証システムを一貫性のあるネットワークに統合して管理する仕組みを簡素化する手段として、ユニバーサルパスワードを導入しました。

ユニバーサルパスワードは、次のような方法でパスワードの問題に対処します。

- 1つのパスワードによるeDirectoryへのアクセスを可能にします。
- パスワードに拡張文字を使用できるようにします。
- 高度なパスワードポリシーの適用を可能にします。
- eDirectoryから他のシステムへのパスワード同期を可能にします。

パスワード管理のほとんどの機能には、ユニバーサルパスワードが有効になっている必要があります。

詳細については、775 ページの 「ユニバーサルパスワードの導入」を参照してください。

パスワードポリシー

ユニバーサルパスワードにより、高度なパスワードポリシーの作成が可能になります。パスワードポリシーは、エンドユーザパスワードの作成および置き換えに関する基準を指定した管理者定義ルールの集まりです。NMASでは、パスワードポリシーをeDirectory内のユーザに割り当てて適用することができます。

パスワードポリシーを管理するには、iManagerを使用します。

詳細については、780 ページの 「パスワードポリシーを使用したパスワードの管理」を参照してください。

パスワード同期

NetIQ Identity Managerには、接続システム間でパスワードを同期する機能が含まれています。この機能には、次の利点があります。

- 双方向パスワード同期
- 接続システムへのパスワードポリシーの適用
- 同期失敗時の電子メール通知
- ユーザのパスワード同期ステータスのチェック機能

詳細については、『NetIQ Identity Manager 4.5 Password Management Guide (NetIQ Identity Manager 4.5パスワード管理ガイド) (https://www.netiq.com/documentation/idm45/idm_password_management/data/bo1o7xz.html)』の第3章「*ConnectedSystemSupportforPasswordSynchronization (接続システムでのパスワード同期のサポート)* (https://www.netiq.com/documentation/idm45/idm_password_management/data/bookinfo.html)」を参照してください。

非可逆パスワードストレージを理解する

ユニバーサルパスワードは暗号化後にeDirectoryに保存され、eDirectoryは必要に応じてこれらのパスワードを取得できます。たとえば、認証時などです。

ユニバーサルパスワードの代替策として、eDirectory 9.2は、パスワードベースのキー導出関数2(PBKDF2)ハッシュアルゴリズム(RFC 2898)を使用する、ハッシュされたパスワードの保存をサポートしています。パスワードのPBKDF2ハッシュが有効になっている場合、ユーザのパスワードを取得することはできません。詳細については、799 ページの 「ユニバーサルパスワードの設定オプション」を参照してください。

重要: eDirectory 9.2以降、パスワードポリシーでユニバーサルパスワードを無効にすると、パスワードのPBKDF2ハッシュが自動的に有効になります。ユニバーサルパスワードが無効になっている既存のパスワードポリシーは、eDirectory 9.2にアップグレードする前はユーザに適用されません。しかし、サーバをeDirectory 9.2にアップグレードすると、これらのパスワードポリシーはツリー内のすべてのユーザに自動的に適用されます。これを回避するには、アップグレードする前に、これらのパスワードポリシーのすべての割り当てを削除します。

NDSパスワードからPBKDF2パスワードへ切り替える場合、SCRAMログインメソッドに手動で切り替える必要もあります。SCRAMログインメソッドの詳細については、664ページの 「パスワード認証」を参照してください。

注

- PBKDF2ハッシュアルゴリズムを使用して作成されたパスワードは大文字と小文字を区別します。この点、大文字と小文字を区別しないNDSパスワードとは異なります。
- PBKDF2ハッシュアルゴリズムで作成されたパスワードは、パスワードポリシーのnspmXCharHistoryLimitとnspmXCharLimitルールをサポートしません。

- デフォルトでは、PBKDF2はSHA-256と繰り返しカウント1を使用するように設定されています。これらは、それぞれnspmPBKDF2HashAlgorithmとnspmPBKDF2IterationCount属性を使用して変更できます。繰り返しカウントを増加させると、ldapバインドのパフォーマンスが低下します。
- SCRAMログインメソッドでは、パスワードへのOTPの追加はサポートされません。NDSログインメソッドをハッシュベースOTP(HOTP)と共に使用するユーザがツリー内にいる場合、そのようなユーザに対してSCRAMログインメソッドの使用を許可しないでください。

非可逆パスワードストレージの有効化

1. NetIQ iManagerを起動します。
2. ［**役割およびタスク**］>［**パスワード**］>［**パスワードポリシー**］の順にクリックします。
3. ［**新規**］をクリックしてパスワードポリシーウィザードを起動します。
4. ポリシーの名前を入力し、［**次へ**］をクリックします。
5. パスワードのPBKDF2ハッシュを有効にするには、［**いいえ**］を選択します。
6. パスワードポリシーウィザードを完了します。

パスワードポリシー

ユニバーサルパスワードにより、高度なパスワードポリシーの作成が可能になります。パスワードポリシーは、エンドユーザパスワードの作成および置き換えに関する基準を指定した管理者定義ルールの集まりです。NMASでは、パスワードポリシーをeDirectory内のユーザに割り当てて適用することができます。

パスワードポリシーを管理するには、iManagerを使用します。

詳細については、780 ページの 「パスワードポリシーを使用したパスワードの管理」を参照してください。

ユニバーサルパスワードの導入

このセクションでは、ユニバーサルパスワードを導入して管理する方法について説明します。

ユニバーサルパスワードを導入するには、セクション2.1からセクション2.8の手順に従います。

ステップ1: ユニバーサルパスワードの必要性を特定する

次の質問のどちらか一方でも答えが「はい」である場合は、ユニバーサルパスワードを導入して使用する計画を立ててください。

- 各国のユーザに、NetIQのWebベースのサービスにアクセスさせること、またはNovell Client for Windowsを使用してNovellファイルとプリントサービスにアクセスさせることを計画していますか。
- NetIQ Identity Managerとその高度なパスワードポリシーおよびパスワード同期機能を使用する予定ですか。

ステップ2: セキュリティコンテナが使用可能であることを確認する

NMASは、実質的にセキュリティドメインであるeDirectoryツリーにグローバルポリシーを保管します。セキュリティポリシーは、ツリー内のすべてのサーバで使用できる必要があります。

NMASは、認証ポリシーとログインメソッド設定データを、［ルート］パーティションから分岐して作成されたセキュリティコンテナに格納します。この情報は、NMASを使用可能なすべてのサーバで読み込みアクセスできる必要があります。セキュリティコンテナの目的は、ログイン、認証、キー管理などのセキュリティプロパティに関するグローバルポリシーを保持することです。

eDirectory 9.0以降には、セキュリティコンテナキャッシング機能が備わっています。この機能により、セキュリティコンテナのデータがローカルサーバのキャッシュに保存されるため、NMASはログインが試行されるたびにセキュリティコンテナにアクセスする必要はありません。666 ページの「セキュリティオブジェクトのキャッシュ」を参照してください。

NMASおよびeDirectory 8.8.*x*以降では、セキュリティコンテナを独立したパーティションとして作成し、作成したコンテナを広い範囲で複製することをお勧めします。このパーティションは、ツリー内の信頼性の高い複数のサーバでのみ、読み書き可能なパーティションとして複製することをお勧めします。

警告: セキュリティコンテナはグローバルポリシーを格納しており、サーバではeDirectoryツリーに指定したセキュリティポリシー全般が変更される可能性があるため、書き込み可能なレプリカを配置するサーバを選択する場合には注意が必要です。ユーザがNMASを使用してログインするためには、ユーザオブジェクトとセキュリティコンテナのレプリカをNMASサーバ上に配置する必要があります。

詳細については、TID 3393169 (http://www.novell.com/support/viewContent.do?externalId=3393169)を参照してください。

ステップ3: SDIドメインキーサーバがユニバーサルパスワードに対応可能であることを検証する

SDIドメインキーサーバが最小構成要件を満たしており、ツリー内の他のサーバによる配布と使用に一貫性のある鍵を使用していることを検証する必要があります。以下の手順は非常に重要です。概説されているとおりに従わないと、ユニバーサルパスワードを有効にしたときに、重大なパスワードの問題が発生する可能性があります。

1 Windowsサーバのコマンドプロンプトで、sdidiag.exeを実行します。

sdidiag.exeは、eDirectoryには付属していません。sdidiag.exeをインストールしてから実行します。このファイルは、TID 2974092 (http://support.novell.com/docs/Readmes/InfoDocument/2974092.html)に関連付けられたセキュリティパッチ()の一部として使用可能になります。

2 管理者として、サーバ(フルコンテキスト)、ツリー名、ユーザ名、およびパスワードを入力してログインします。

3 すべてのサーバが3DESツリー鍵として168ビットの鍵を使用していること、AES 256ビットのツリー鍵として256ビットの鍵を使用していることを確認します。

この要件を満たしていることを確認するには、TID 3364214の指示に従ってください。

4 コマンドCHECK -v >>*インストールフォルダ*\sdinotes.txtを入力します。

画面に、CHECKコマンドの結果が表示されます。

5 問題がない場合は、778 ページの 「ステップ4: SDI鍵の一貫性を確認する」に進みます。

または

インストールフォルダ\sdinotes.txtファイルに記載された説明に従って、構成と鍵の問題を解決してからステップ 6に進みます。

6 SDIドメインキーサーバ上でNICI *3.0*が実行されていることを検証します。

古いバージョンの場合、eDirectoryを9.0以降にアップグレードします。それにより、NICIが3.0以降にアップグレードされます。

7 (オプション)SDIDIAG CHECKコマンドを再実行します。詳細については、ステップ 4を参照してください。

SDIDIAGの使用方法の詳細については、TID 3364214 (http://www.novell.com/support/viewContent.do?externalId=3364214)を参照してください。

SDIドメインキーサーバの追加または削除

SDIドメインキーサーバであるサーバを削除するには、次の手順に従います。

1 sdidiag.exeは、eDirectoryには付属していません。sdidiag.exeは、Novellダウンロードサイト (http://download.novell.com/index.jsp)からダウンロードできます。ダウンロードした後、sdidiag.exeを実行します。

2 セキュリティコンテナとW0.KAP.Securityオブジェクトに対する管理権を持つ管理者として、サーバ(フルコンテキスト)、ツリー名、ユーザ名、およびパスワードを入力してログインします。

3 コマンドRS -s *servername*を入力します。

たとえば、Novell_Incツリー内の組織Novellに含まれるコンテナPRVにserver1が存在する場合は、.server1.PRV.Novell.Novell_Incをサーバ名として入力します。

サーバをSDIドメインキーサーバとして追加するには、次の手順に従います。

1 Windowsサーバで、コマンドプロンプトボックスを開き、sdidiag.exeを実行します。

2 管理者として、サーバ(フルコンテキスト)、ツリー名、ユーザ名、およびパスワードを入力してログインします。

3 コマンドAS -s *servername*を入力します。

たとえば、Novell_Incツリー内の組織Novellに含まれるコンテナPRVにserver1が存在する場合は、.server1.PRV.Novell.Novell_Incをサーバ名として入力します。

ステップ4: SDI鍵の一貫性を確認する

ツリー全体で、暗号鍵のすべてのインスタンスに一貫性があることを検証します。各サーバに、ツリー内の他のサーバとセキュアに通信するために必要な暗号鍵があることを確認するには、次の手順に従います。

1. Windowsサーバのコマンドプロンプトで、sdidiag.exeを実行します。
2. コマンドCHECK -v >> sys:system\sdinotes.txt -n *container DN*を入力します。

   たとえば、Acme_Incツリー内の組織Acmeに含まれるコンテナUSRにユーザBobが存在する場合は、.USR.Acme.Acme_Inc.をコンテナ識別名(DN)として入力します。

   このコマンドは、さまざまなサーバとキードメインの間で鍵の一貫性に関するすべての問題を報告します。

   画面への出力に、CHECKコマンドの結果が表示されます。
3. 問題が報告されていない場合は、ユニバーサルパスワードを有効にできる状態になっています。778 ページの 「ステップ5: ユニバーサルパスワードを有効にする」に進みます。

   または

   問題が報告された場合は、sdinotes.txtファイルの指示に従います。

   ほとんどの場合、コマンドRESYNC-Tを実行するよう求められます。NMASがユニバーサルパスワードの認証中に-1418または-1460エラーを報告した場合は、このコマンドを繰り返し実行できます。

   SDIDIAGのオプションと操作方法の詳細については、以下を参照してください。

   - TID 3364214 (http://www.novell.com/support/viewContent.do?externalId=3364214)
   - TID 7005397 (http://www.novell.com/support/viewContent.do?externalId=7005397)

ステップ5: ユニバーサルパスワードを有効にする

1. NetIQ iManagerを起動します。
2. ［**役割およびタスク**］>［**パスワード**］>［**パスワードポリシー**］の順にクリックします。
3. ［**新規**］をクリックしてパスワードポリシーウィザードを起動します。
4. ポリシーの名前を入力し、［**次へ**］をクリックします。
5. ［**はい**］を選択してユニバーサルパスワードを有効にします。
6. パスワードポリシーウィザードを完了します。

重要: コンテナ パーティションのルートになっているコンテナにポリシーを割り当てると、ポリシー割り当てはサブコンテナのユーザを含めたパーティション内のすべてのユーザに継承されます。コンテナがパーティションルートであるかどうかを知るには、そのコンテナを参照して、隣にパーティションアイコンが表示されているかどうかを確認します。

パーティションのルートではないコンテナにポリシーを割り当てると、そのポリシー割り当ては、その特定のコンテナ内のユーザだけに継承されます。サブコンテナ内のユーザには継承されません。パーティションのルートではないコンテナの下位にあるユーザすべてにポリシーを適用する場合は、それぞれのサブコンテナに個別のポリシーを割り当てる必要があります。

後方互換性

ユニバーサルパスワードは、既存のサービスに対する後方互換性を確保するように設計されています。デフォルトでは、このサービスで変更されたパスワードは、ユーザオブジェクトの簡易パスワードおよびNDSパスワードと同期することができます。パスワード管理プラグインを使用することで、同期するパスワードを選択できます。

ただし、パスワードで国際文字が使用されている場合は例外です。古いクライアントでは国際文字がさまざまに変換されるため、実際の値が一致しなくなります。システム全体の国際文字を使用したパスワードのすべてが正常に機能するよう、すべてのNovell Clientをアップグレードすることをお勧めします。

NetIQおよびサードパーティのバックアップおよび復元アプリケーションには、NetWare SMS (Storage Management Services)インフラストラクチャが使用されます。これらのNetIQおよびサードパーティ製品が混合環境で動作することになっている場合、製品で使用するシステムパスワードに拡張文字を含めることはできません。

注: ユニバーサルパスワード対応のアプリケーションおよびサービスと、拡張文字対応のアプリケーションおよびサービスを調べるには、TID 3065822 (http://www.novell.com/support/viewContent.do?externalId=3065822)を参照してください。多くのアプリケーションやサービスでは、ユニバーサルパスワードを使用しない場合は拡張文字を使用できます。

パスワードの管理

ユニバーサルパスワードを管理するのには、次の手段を使用できます。

- **iManager (推奨):** NetIQ iManagerを使用してパスワードを管理する場合、後方互換性を確保するために、ユニバーサルパスワードは簡易パスワードおよびNDSパスワードの値と同期されるように自動的に設定されます。iManagerのNMASタスクでは、システムにインストールされて設定済みの個々のパスワードと認証方式をきめ細かく管理できます。

  パスワード管理プラグインを使用したiManagerでは、パスワードポリシーを使用して、NDSパスワード、簡易パスワード、および配布パスワードとのユニバーサルパスワードの同期方法を指定できます。さらに、管理者がユーザのユニバーサルパスワードを設定するために使用できるiManagerタスクが用意されています。
- **サードパーティ製のアプリケーション:** NetIQのクロスプラットフォームライブラリに書き込まれ、パスワード管理を行うサードパーティ製アプリケーションも、Novell Client for Windowsに新しいライブラリがインストールされている場合は、ユニバーサルパスワードを設定して他のパスワードと同期します。

注意を要する問題

- ユーザのNDSパスワードを無効にすると、NDSパスワードは、ユーザにとって不明の任意の値に設定されます。以下に、ログインメソッドがこの変更を処理する方法をリストして説明します。
  - NDSパスワードが無効にされても、簡易パスワードメソッドは無効にされません。ユニバーサルパスワードが有効にされて使用可能になっている場合、簡易パスワードメソッドはユニバーサルパスワードを使用します。それ以外の場合は、簡易パスワードを使用します。ユニバーサルパスワードが有効にされていても、設定されていない場合、簡易パスワードメソッドは簡易パスワードを使用してユニバーサルパスワードを設定します。

- NDSパスワードが無効にされても、拡張パスワードメソッドは無効にされません。拡張パスワードメソッドは、ログインにはユニバーサルパスワードを使用しません。
- NDSパスワードが無効にされても、NDSパスワードメソッド(ユニバーサルパスワード)は無効にされません。ユニバーサルパスワードが有効にされて使用可能になっている場合、NDSパスワードメソッドはユニバーサルパスワードを使用します。それ以外の場合は、NDSパスワードを使用します。ユニバーサルパスワードが有効にされていても、設定されていない場合、NDSパスワードメソッドはNDSパスワードを使用してユニバーサルパスワードを設定します。

- 新しいユーザを作成する場合やヘルプデスクへの問い合わせに応答する場合などに、管理者がユーザのパスワードを変更する場合、パスワードポリシーでパスワードを期限切れにする設定が有効になっていると、セキュリティ上の理由からパスワードは自動的に失効します。パスワードを期限切れにする設定とは、パスワードポリシーの［**高度なパスワードルール**］にある［**Numberofdaysbeforepasswordexpires(0-365)**］です。この特定の機能については、日数は重要ではありませんが、この設定を有効にする必要があります。

  注: この振る舞いを無効にするには、パスワードポリシーで［**Do not expire the user's password when the administrator sets the password**］オプションを選択します。

- パスワードポリシーを作成してユニバーサルパスワードを有効にし、さらに高度なパスワードルールを有効にすると、NDSパスワークの既存のパスワード設定ではなく、有効にされた高度なパスワードルールが適用されます。従来のパスワード設定は無視されます。パスワードポリシーを作成しても、以前の設定が自動的にマージまたはコピーされることはありません。

  たとえば、NDSパスワードで使用する猶予ログイン回数を設定している場合、ユニバーサルパスワードを有効にするときに、パスワードポリシーの高度なパスワードルールで猶予ログイン回数の設定を再作成する必要があります。

  NMASでは、ユーザオブジェクトのNDSパスワード設定を、対応するパスワードポリシー設定に置き換えます。たとえば、猶予ログイン回数がユーザオブジェクトでは4に設定されていて、パスワードポリシーでは5に設定されている場合、ユーザがログインした時点、またはパスワードが変更された時点で、そのユーザオブジェクトの猶予ログイン回数は5に変更されます。

パスワードポリシーを使用したパスワードの管理

パスワードポリシーを使用してユーザが自分のパスワードを作成する方法に対するルールを設定することで、セキュリティを強化できます。ユーザ自身でパスワード忘れや、パスワードリセットに対処できるセルフサービスオプションを付加することにより、ヘルプデスクの運用コストの削減にもつながります。

このセクションで説明する内容は以下のとおりです。

- 781 ページの 「パスワードポリシー機能の概要」
- 781 ページの 「パスワードポリシーの計画」
- 785 ページの 「パスワードポリシーを使用するために必要な事前タスク」
- 786 ページの 「パスワードポリシーの作成」
- 801 ページの 「ユーザへのパスワードポリシーの割り当て」
- 803 ページの 「ユーザに適用されているポリシーの識別」
- 803 ページの 「ユーザのパスワードの設定」

- 804 ページの 「ユニバーサルパスワードの診断ユーティリティ」
- 805 ページの 「パスワードポリシーのトラブルシューティング」

パスワード忘れセルフサービスおよびパスワードリセットセルフサービスについては、806 ページの 「パスワードセルフサービス」を参照してください。

パスワードポリシー機能の概要

Password Policy (パスワードポリシー)は、エンドユーザパスワードの作成および交換に関する基準を指定した管理者定義ルールの集まりです。NMASでは、パスワードポリシーをeDirectory内のユーザに割り当てて適用することができます。

パスワードポリシーにパスワード忘れセルフサービス機能を組み込んで、パスワードを忘れた場合のヘルプデスクへの問い合わせ件数を削減することもできます。セルフサービス機能としては、パスワードリセットセルフサービスもあります。パスワードリセットセルフサービスでは、ユーザが管理者によってパスワードポリシーに指定されたルールを確認しながら、自分のパスワードを変更することができます。ユーザはこれらの機能に、Identity Managerユーザアプリケーションまたは iManagerセルフサービス コンソールからアクセスします。

パスワードポリシーで高度なパスワードルール、パスワード同期、およびパスワード忘れセルフサービスのさまざまな機能を使用するには、ユーザのユニバーサルパスワードを有効にする必要があります。ユニバーサルパスワードの導入方法については、775 ページの 「ユニバーサルパスワードの導入」を参照してください。

パスワードポリシーを作成するには、パスワードポリシーウィザードを使用します。iManagerで、［**パスワード**］>［**パスワードポリシー**］>［**新規**］の順にクリックします。パスワードポリシーの作成方法の詳細については、786 ページの 「パスワードポリシーの作成」を参照してください。

パスワードポリシーの計画

- 781 ページの 「ツリー内でパスワードポリシーを割り当てる方法の計画」
- 782 ページの 「パスワードポリシーのルールの計画」
- 783 ページの 「ユーザのログインおよびパスワードメソッド変更の計画」

ツリー内でパスワードポリシーを割り当てる方法の計画

管理を簡素化するために、デフォルトポリシーをツリー全体に割り当て、その他に使用するポリシーをツリーのできるだけ高い階層に割り当てることをお勧めします。

NMASは、ユーザに適用されているパスワードポリシーを判別します。詳細については、801ページの 「ユーザへのパスワードポリシーの割り当て」を参照してください。

パスワードポリシーのルールの計画

パスワードポリシーで高度なパスワードルールを使用することで、パスワードにビジネスポリシーを適用できます。

Novell Client (4.9.1)、Identity Managerユーザアプリケーション、およびiManagerセルフサービスコンソールには、パスワードポリシーに含まれるパスワードルールが表示されることに留意してください。ユーザがLDAPサーバを介して、または接続システムで自分のパスワードを変更する場合に備え、ユーザがパスワードルールをすぐに利用できるようにして、ルールに準拠したパスワードが作成されるようにする必要があります。

Identity Managerのパスワード同期機能を使用する場合は、パスワードポリシーが割り当てられているユーザが、接続システムのパスワード同期に参加させるユーザと一致していることを確認する必要があります。パスワードポリシーはツリー中心で割り当てられます。これに対し、パスワード同期は、各サーバのドライバごとに設定されます。パスワード同期で期待される結果を出すためには、パスワード同期用のドライバを実行するサーバ上の読み書き可能レプリカまたはマスタレプリカに含まれるユーザが、ユニバーサルパスワードが有効にされたパスワードポリシーを割り当てたコンテナと一致するようにします。パーティションルートコンテナにパスワードポリシーを割り当てることによって、そのコンテナとサブコンテナ内のすべてのユーザに確実にパスワードポリシーが割り当てられます。

高度なパスワードルール

高度なパスワードルールでは、ユニバーサルパスワードに次の条件を定義できます。

- パスワードの有効期間: パスワードポリシーは、過去にeDirectoryで提供していたポリシー機能と同じ機能を提供するため、パスワードの変更頻度や再使用可能かどうかを指定できます。
- パスワードに含まれる文字: 文字、数字、小文字または大文字および特殊文字を組み合わせることができます。安全性の低いと思われるパスワード(企業名など)は排除できます。パスワードに含める、以前のパスワードで使用されていない「新しい」文字の数を要件としたり、指定のパスワードで許容するパスワードポリシー違反の数を設定したりすることもできます。

パスワードポリシーで高度なパスワードルールを使用するには、ユニバーサルパスワードを有効にする必要があります。ポリシーにユニバーサルパスワードが有効にされていない場合は、代わりにNDS®パスワードを対象に設定されている制限が適用されます。

注: パスワードポリシーを作成してユニバーサルパスワードを有効にすると、NDSパスワードに対する既存のパスワード設定の代わりに、高度なパスワードルールが適用されます。従来のパスワード設定は無視されます。パスワードポリシーを作成しても、以前の設定が自動的にマージまたはコピーされることはありません。

たとえば、NDSパスワードで使用する猶予ログイン回数を設定している場合、ユニバーサルパスワードを有効にするときに、パスワードポリシーの高度なパスワードルールで猶予ログイン回数の設定を再作成する必要があります。

後でパスワードポリシーでユニバーサルパスワードを無効にすると、既存のパスワード設定は無視されなくなります。既存の設定が、NDSパスワードに適用されることになります。

NMAS 3.1以降では、ユーザオブジェクトのNDSパスワード設定を、対応するパスワードポリシー設定に置き換えます。たとえば、猶予ログイン回数がユーザオブジェクトでは4に設定されていて、パスワードポリシーでは5に設定されている場合、ユーザがログインした時点、またはパスワードが変更された時点で、そのユーザオブジェクトの猶予ログイン回数は5に変更されます。

ポリシーの適用

ツリー内のユーザにパスワードポリシーを割り当てると、そのポリシーの高度なパスワードルールに準拠していない限り、パスワード変更は適用されません。Novell Client 4.9 SP2以降では、ルールも表示されます。アクセスにどちらのメソッドを使用するとしても、ルールに準拠していないパスワードは拒否されます。NMASは、これらのルールを適用するアプリケーションです。

ポリシーに既存のパスワードのコンプライアンスをチェックするように指定することで、ユーザはルールに準拠していない既存のパスワードを変更しなければなくなります。コンプライアンスのチェックオプションが有効にされている場合、パスワードポリシーのルールを満たしていないパスワードには、失効したパスワードとしてマークが付けられます。

ユーザがポータルを介して認証する際に、有効にされているパスワード忘れセルフサービス機能の設定を求めるプロンプトを出すように指定することもできます。これは、認証後サービスと呼ばれます。たとえば、パスワードを忘れた場合に電子メールで送信するパスワードのヒントをユーザに設定させたい場合、認証後サービスを使用して、ユーザのログイン時にパスワードのヒントを設定するよう求めるプロンプトを出すことができます。

認証後サービスの設定は、［パスワードを忘れた場合］プロパティページの最後のオプションです。

ユーザのログインおよびパスワードメソッド変更の計画

ユーザがログインしたりパスワードを変更したりするには、いくつかの方法があります。ユニバーサルパスワードをサポートするためのアップグレードの詳細については、775 ページの 「ユニバーサルパスワードの導入」を参照してください。

このセクションでは、それぞれのケースでユニバーサルパスワードをサポートするための追加要件について説明します。

Novell Client

Novell Clientを使用している場合は、バージョン4.9 SP2以降にアップグレードします。

ユーザはiManagerセルフサービスコンソールや、環境に応じてその他の企業のポータルからログインできるので、Novell Clientの使用は必須ではありません。また、Active Directoryでのパスワード同期に、Novell Clientは必要なくなっています。

以下の表に、ユニバーサルパスワードに関するNovell Clientバージョン間の違いについての説明と、レガシーNovell Clientを操作する際の推奨事項を記載します。

表 26-1 Novell Client でのユニバーサルパスワード

Novell Clientバージョン (Novell Client Version)	ログイン	パスワードの変更
4.9より前	NMASを介さないため、ユニバーサルパスワードはサポートされません。NDSパスワードを使用して直接ログインします。	NMASを介する代わりに、NDSパスワードを直接変更します。 ユニバーサルパスワードを使用している場合、NDSパスワードとユニバーサルパスワードが同期された状態に維持されない可能性があります。この問題を防ぐには、次の3つのオプションがあります。 ◆ すべてのクライアントをバージョン4.9以降にアップグレードします。 ◆ コンテナの属性値を使用して、レガシークライアントがパスワードを変更できないようブロックします。このソリューションの場合、レガシークライアントは引き続きログインできますが、パスワードを変更することはできません。パスワード変更は、必ず新しいバージョンのNovell ClientまたはiManagerを使用して行う必要があります。 ◆ ［RemovetheNDSPasswordwhenSettingUniversalPassword］のパスワードポリシー設定を使用します。この場合、NDSパスワードを使用したログインとパスワード変更がどちらも防止されるので、抜本的な対策になります。
4.9	ユニバーサルパスワードをサポートしています。	ユニバーサルパスワードにパスワードポリシーのルールを適用します。 ユーザがルールに準拠していないパスワードを作成しようとすると、パスワード変更は拒否されます。ただし、ルールのリストは、ユーザには表示されません。
4.9 SP2以降	ユニバーサルパスワードをサポートしています。	ユニバーサルパスワードにパスワードポリシーのルールを適用します。 さらに、ルールに準拠したパスワードを作成できるよう、ユーザにルールを表示します。

Identity ManagerユーザアプリケーションとiManager

Identity ManagerユーザアプリケーションとiManagerが提供するパスワードセルフサービスでは、ユーザがパスワードをリセットしたり、パスワード忘れセルフサービス(パスワードポリシーで指定されている場合)を設定したりできます。パスワードセルフサービスの設定方法の詳細については、806 ページの 「パスワードセルフサービス」を参照してください。

- パスワードポリシーでは、［SynchronizeNDSpasswordwhensettingUniversalPassword］のデフォルト設定を受け入れることをお勧めします。

その他のプロトコル

ユニバーサルパスワードがサポートされるよう、eDirectory、LDAPサーバ、NMAS、およびiManagerがアップグレードされていることを確認します。

ユニバーサルパスワードでAFP、CIFS、およびその他のプロトコルを使用する方法の詳細については、775 ページの 「ユニバーサルパスワードの導入」を参照してください。

接続システム

Identity Managerのパスワード同期を使用する場合は、ユーザパスワード変更が正常に行われるよう、次の要件を満たしていることを確認してください。

- システムのすべてのIdentity Managerドライバが、Identity Managerフォーマットにアップグレードされていること。
- Identity Managerドライバの環境設定に、新しいパスワード同期ポリシーが含まれていること。
- パスワード同期の設定で、ユニバーサルパスワードの使用が設定されていること。双方向パスワード同期が必要な場合は、配布パスワードも指定されていること。
- 必要に応じて、パスワードをキャプチャするパスワードフィルタが接続システムに導入されていること。

詳細については、『NetIQ Identity Manager 4.5 Password Management Guide (NetIQ Identity Manager 4.5パスワード管理ガイド)』の「*Connected System Support for Password Synchronization (接続システムでのパスワード同期のサポート)*」を参照してください。

パスワードポリシーを使用するために必要な事前タスク

パスワードポリシーのすべての機能を利用するには、環境を準備するために行っておかなければならない手順があります。

1. ユニバーサルパスワードをサポートするように環境をアップグレードします。

   詳細については、775 ページの 「ユニバーサルパスワードの導入」を参照してください。

2. ユニバーサルパスワードをサポートするようにクライアント環境をアップグレードします。

   783 ページの 「ユーザのログインおよびパスワードメソッド変更の計画」および775 ページの 「ユニバーサルパスワードの導入」を参照してください。

3. iManagerを設定するときに、iManagerのインストールまたは事後インストールの一環としてiManager設定ウィザードを実行しなかった場合は、iManager設定ウィザードを実行する必要があります。iManager設定ウィザードを実行する方法については、『NetIQ iManager Administration Guide』の「*Role-Based Services*」セクションを参照してください。

   重要: iManager設定ウィザードの実行後は、iManagerがRBSモードで実行されます。この場合、管理者が自分自身に特定の役割を割り当てていない限り、管理者にはタスクが1つも表示されません。管理者には必ず、すべてのiManagerタスクにアクセスできる役割を割り当ててください。

   ---

4. NetIQ iManagerパスワード管理プラグインをインストールします。

   このプラグインは、NetIQダウンロードWebサイト (http://dl.netiq.com/)からダウンロードできます。

重要: eDirectoryをアップグレードせずにNetIQ iManagerパスワード管理プラグインを最新バージョンにアップグレードした後、パスワードポリシーを変更または作成しようとすると、iManagerにエラーが表示されます。

5 iManager WebサーバとeDirectoryが同じコンピュータ上で実行されているとしても、この2つの間にSSLを設定します。

6 eDirectory内に、単純認証に対してTLSを要求するためのLDAPグループサーバオブジェクトを設定します。

これは、iManagerを設定する際のデフォルト設定です。パスワードセルフサービス機能には、単純認証に対してTLSを要求することを強くお勧めします。これは、iManagerのタスク［**パスワード**］>［**Set Universal Password**］を使用する場合は必須です。

単純認証に対してTLSを要求する場合、LDAP SSLポートに必要な追加設定はありません。

重要: 単純認証に対してTLSを要求しないということは、ユーザが平文パスワードを使用してiManagerセルフサービスコンソールにログインすることを許可するということです。

このオプションを使用することもできますが、別のステップが必要になります。

デフォルトで、パスワードセルフサービス機能がLDAP SSLポートとして想定するのは、PortalServlet.propertiesファイル内のSystem.DirectoryAddress設定で指定されているポートです。LDAP SSLポートがそれとは異なる場合は、PortalServlet.propertiesファイルに次の鍵ペアを追加して、正しいポートを指示する必要があります。

`LDAPSSLPort=your_port_number`

たとえば、Tomcatを実行しているとしたら、この鍵ペアをtomcat\webapps\nps\WEB_INFディレクトリ内にあるPortalServlet.propertiesファイルに追加します。

7 パスワード忘れ機能に電子メール通知を有効にするには、820 ページの 「パスワードセルフサービスの電子メール通知の設定」の手順に従います。

SMTPサーバを設定して、電子メールテンプレートをカスタマイズする必要があります。

これで、パスワードポリシーのすべての機能を利用できる状態になりました。786 ページの 「パスワードポリシーの作成」の説明に従って、ポリシーを作成します。

パスワードポリシーの作成

新しいパスワードポリシーを作成するには、iManagerのパスワードポリシーウィザードを使用します。

ウィザードの各ステップの説明については、オンラインヘルプおよび780 ページの 「パスワードポリシーを使用したパスワードの管理」と806 ページの 「パスワードセルフサービス」を参照してください。

1 785 ページの 「パスワードポリシーを使用するために必要な事前タスク」の手順を完了していることを確認します。

その手順によって、パスワードポリシーのすべての機能を利用できるようになります。

2 iManagerの［**役割およびタスク**］ビューで、［**パスワード**］>［**パスワードポリシー**］の順にクリックします。

3 新しいパスワードポリシーを作成するために、［**新規**］をクリックします。

4 ウィザードで表示される指示に従い、ポリシーの高度なパスワードルール、ユニバーサルパスワードの設定オプション、およびパスワード忘れの選択項目を作成します。

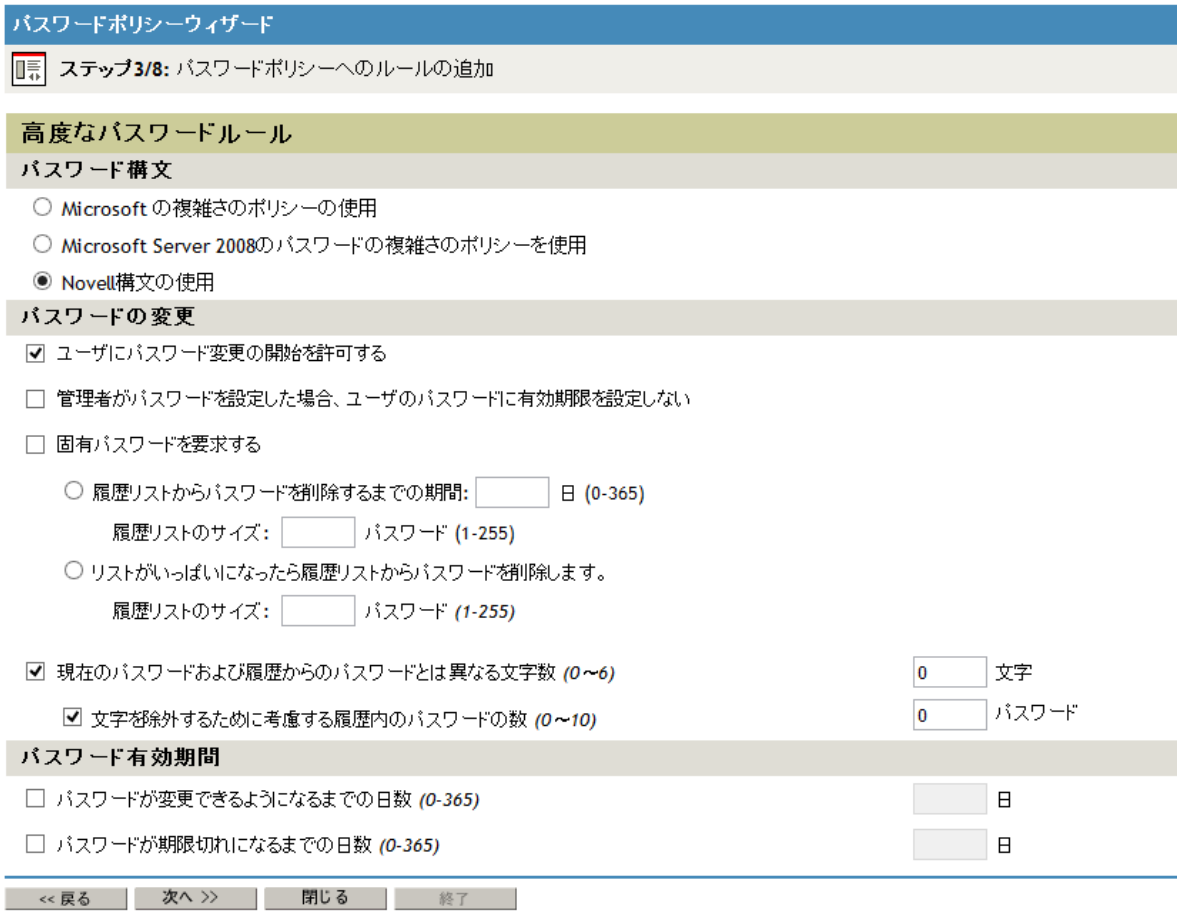
5 必要に応じて、個々のユーザ、組織、または会社全体にパスワードポリシーを割り当てます。

6 新しいポリシーの設定を確認してから、［完了］をクリックし、［閉じる］をクリックしてウィザードを終了します。

高度なパスワードルール

図 26-1に、高度なパスワードルールの最初のセクションを示します。

図 26-1 高度なパスワードルール



パスワードの構文

パスワードポリシーで使用するパスワードの構文には、次の3つのオプションのいずれかを指定できます。

- **Microsoftの複雑さのポリシーを使用する**
- **Use Microsoft Server 2008 Password Policy**
- **Novellの構文を使用する**

警告: iManagerでは、サーバにインストールされているNMASのバージョンに関係なく、Microsoft Server 2008のパスワードポリシーのタイプを使用してポリシーを作成することができます。ただし、このオプションを使用するには、NMAS 3.3.4以降がインストールされている必要があります。これより前のバージョンのNMASがインストールされている場合は、新しいパスワードポリシーは正常に機能しません。

- **Microsoftの複雑さのポリシーを使用する**

  この設定では、Microsoft*の複雑さのポリシーの要件を適用することができます。eDirectoryとMicrosoft Active Directoryの間でパスワードを同期させる必要がある場合は、このオプションを使用します。

  ポリシーにこのオプションが選択されている場合、このポリシーが割り当てられているすべてのユーザは、ユニバーサルパスワードに実装されたMicrosoftの複雑さのポリシーの条件を満たすパスワードを作成しなければなりません。以下の条件があります。

  - 最小パスワード長は6文字です。
  - 最大パスワード長は128文字です。
  - パスワードには、大文字、小文字、数字、および特殊文字の4つのタイプのうち、3つのタイプの文字が少なくとも1つ含まれる必要があります。
    - 大文字 - Basic LatinおよびLatin-1文字セットに含まれる文字の大文字すべて。
    - 小文字 - Basic LatinおよびLatin-1文字セットに含まれる文字の小文字すべて。
    - 数字 - 0、1、2、3、4、5、6、7、8、9。
    - 特殊文字 - その他すべての文字。
  - ユーザ属性CN、GivenName、Surname、FullName、およびdisplayNameの値をパスワードに含めることはできません。
  - eDirectoryアカウントのユーザ属性CNの値そのものをパスワードに含めることはできません。属性の長さが3文字未満の場合、NMASはこのチェックを行いません。

- **Use Microsoft Server 2008 Password Policy**

  この設定では、Microsoft* Windows Server 2008パスワードポリシーの複雑性の要件を適用することができます。eDirectoryとMicrosoft Active Directoryの間でパスワードを同期させる必要がある場合は、このオプションを使用します。

  ポリシーにこのオプションが選択されている場合、このポリシーが割り当てられているすべてのユーザは、ユニバーサルパスワードに実装されたMicrosoft Windows Server 2008の複雑さのポリシーの条件を満たすパスワードを作成しなければなりません。このオプションを選択すると、［高度なパスワードルール］ページのいくつかのオプションが、この複雑さのポリシーの条件を満たすように設定されます。以下の条件があります。

  - 最小パスワード長は、デフォルトでは7文字です。［**Minimum number of characters in password (1-512)**］オプションを使用して、環境の最小パスワード長を設定できます。最小文字数の設定方法の詳細については、794 ページの 「パスワード長」を参照してください。
  - 最大パスワード長は512文字です。
  - パスワードには、大文字、小文字、数字、非英数字、およびその他の文字の5つのタイプのうち、3つのタイプの文字が少なくとも1つ含まれる必要があります。
    - 大文字 - 発音区別符付きを含むヨーロッパ言語の文字、ギリシャ文字、キリル文字の大文字すべて。

- 小文字 - 発音区別符付きを含むヨーロッパ言語の文字、ギリシャ文字、キリル文字の小文字すべて。
- 数字 - 0、1、2、3、4、5、6、7、8、9。
- 非英数字 - 次の特殊文字すべて: ( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? / _
- その他の文字 - 英字として分類されている一方、大文字でも小文字でもないUnicode文字すべて。これには、アジア言語のUnicode文字が含まれます。

- 除外するパスワードのリストに含まれる単語をパスワードに含めることはできません。除外するパスワードの長さが3文字未満の場合、NMASはこのチェックを行いません。除外パスワードの詳細については、793 ページの 「パスワード除外」を参照してください。
- アカウントのCN属性またはFull Name属性の値が3文字以上の1つの単語である場合、CN属性全体またはFull Nama属性の全体または一部をパスワードに含めることはできません。属性の値の一部は3文字以上の連続する文字として定義され、その両端はコンマ、ピリオド、ダッシュ、ハイフン、下線、スペース、シャープ記号、またはタブで区切られます。

  注: Microsoft 2008パスワードポリシーを使用している場合、CN属性とdisplayName属性は、ADにおけるsamAccountNameルールとdisplayNameルールと同様と見なされます。

- パスワードで許容される複雑さのポリシー違反の最大数は、デフォルトでは2です。［**Maximum number of complexity policy violations in password (0-5)**］オプションを使用して、パスワードで許容される複雑さのポリシー違反の最大数を設定できます。違反の最大許容数の設定方法の詳細については、795 ページの 「Password Complexity Violations」を参照してください。

- **Novellの構文を使用する**

  この設定では、パスワードポリシーにNovellの構文を使用できます。このオプションはデフォルトで選択されています。Novellの構文を使用したポリシーの標準設定は、次のとおりです。

  - 最小パスワード長は、デフォルトでは4文字です。［**パスワードの最小文字数(1～512)**］オプションを使用して、環境の最小パスワード長を設定できます。最小文字数の設定方法の詳細については、794 ページの 「パスワード長」を参照してください。
  - 最大パスワード長は、デフォルトでは12文字です。［**Minimum number of characters in password (1-512)**］オプションを使用して、環境の最大パスワード長を設定できます。最大文字数の設定方法の詳細については、794 ページの 「パスワード長」を参照してください。

パスワード構文の優先順位

iManagerパスワード管理プラグインのインタフェース外で、ディレクトリ管理またはLDAPを使用してパスワードポリシーの属性を変更すると、パスワードポリシーの1つ以上のタイプの間に競合が発生する可能性があります。たとえば、LDAPを使用して、同じパスワードポリシーに対してMicrosoftの複雑さのポリシーとMicrosoft Windows 2008パスワードポリシーを有効にするなどです。

競合が発生した場合、eDirectoryは次の優先順位に従います。

- Microsoft Server 2008パスワードポリシー
- Microsoftの複雑さのポリシー
- Novell構文

パスワード管理インタフェース外でのパスワードポリシー変更の詳細については、798 ページの「パスワードポリシーインタフェースの外部でパスワードポリシーを変更する」を参照してください。

パスワードの変更

- **Allow user to initiate password change**

  このオプションにより、ユーザはパスワードセルフサービス機能を使用できるようになります。このオプションはデフォルトで選択されています。パスワードセルフサービスの詳細については、806 ページの「パスワードセルフサービス」を参照してください。

- **Do not expire the user's password when the administrator sets the password**

  このオプションでは、ユーザが自分のパスワードにアクセスして変更することが必要になります。この機能により、デフォルトを上書きできます。パスワードの有効期限が設定されている場合、eDirectoryではデフォルトの振る舞いとして、ユーザのパスワードは、管理者がパスワードを設定する際に失効します。

- **固有パスワードを要求する**

  このオプションが選択されている場合、ユーザはパスワードを履歴リストに含まれているパスワードに変更できなくなります。ユーザがパスワードを変更して履歴リストに含まれているパスワードを再利用しようとすると、そのパスワードはパスワードポリシーによって拒否され、ユーザは別のパスワードを指定するよう求められます。

  次の2つの値のいずれかを使用することで、固有パスワードを強制する方法を指定できます。

  - ［**Remove password from history list after a specified number of days (0-365)**］と［**History list size (1-255)**］。

    固有パスワードを要求する場合は、照合用の履歴リストに以前に使用したパスワードを保管する日数を指定できます。

    たとえば、制限を30日間に指定した場合、ユーザが以前に「mountains99」というパスワードを使用したとすると、そのパスワードが履歴リストに30日間維持されます。この期間中に、ユーザが自分のパスワードを変更して「mountains99」を再利用しようとすると、そのパスワードはパスワードポリシーによって拒否され、ユーザは別のパスワードを指定するよう求められます。30日間が過ぎると、古いパスワードは照合用に保管されなくなり、そのパスワードを再利用しても、パスワードポリシーによって拒否されなくなります。

    固有パスワードを要求する場合、照合用の履歴リストに保管するパスワードの数を指定することもできます。たとえば、値を3に指定すると、ユーザが以前に使用した3つのパスワードが保管されます。履歴リストから削除するまでの日数が経過する前に、ユーザが自分のパスワードを変更して履歴リストに含まれているパスワードを再利用しようとすると、そのパスワードはパスワードポリシーによって拒否され、ユーザは別のパスワードを指定するよう求められます。

    注

    - ［**UseMicrosoftServer2008PasswordPolicy**］オプションを選択すると、デフォルトで［**固有パスワードを要求する**］オプションも選択されます。
    - ［**固有パスワードを要求する**］が選択されていて、［**Removepasswordfromhistorylist after a specified number of days (0-365)**］を選択し、日数を指定しなかった場合、［PasswordLifetime］セクションの［**Numberofdaysbeforepasswordexpires(0-365)**］フィールドに設定した値の8倍の期間中、パスワードが履歴リストに維持されます。どちらのフィールドにも値が設定されていない場合、パスワードは365日間、履歴リストに維持されます。

- パスワード履歴リストのサイズと日数を指定し、パスワード履歴リストのパスワード数が指定したサイズに達している場合、パスワードの期限が切れるまで、ユーザは自分のパスワードを変更できません。管理者は、パスワード履歴リストのサイズに達していても、ユーザのパスワードを変更または設定できます。
- パスワード履歴リストの1つ以上のパスワードが期限切れになって、リストがいっぱいでなくなると、ユーザは再び自分のパスワードを変更できるようになります。この制限が設けられている理由は、ユーザが何度も自分のパスワードを変更したためにパスワードがパスワード履歴リストに追加されなくなり、ユーザが以前に使用したパスワードを再利用できるようになるという事態を防ぐためです。
- パスワード履歴リストのサイズが指定されていない場合、パスワードの履歴がいっぱいになることはありません。
- 指定されたパスワードをパスワード履歴リストの以前に使用されたパスワードを比較する際のeDirectoryの振る舞いはActive Directoryとは異なります。パスワード履歴リストのサイズが「N」に設定されている場合、Active Directoryは、指定されたパスワードを、以前に使用されたN個のパスワードと比較します。一方、eDirectoryは指定されたパスワードを以前に使用された「n+1」個のパスワードと比較します。

- ［**Remove password from history list when the list is full**］と［**History list size (1-255)**］。

  固有のパスワードが必要な場合は、比較のために履歴リストに保存されるパスワードの数を指定できます。このオプションは先入れ先出しで機能し、最も古いパスワードが履歴リストから削除されます。たとえば、履歴リストがいっぱいの場合、履歴リストに現在存在しない新しいパスワードをユーザが作成すると、履歴リスト内の最も古いパスワードが削除されます。

  注

  - ［**Use Microsoft Server 2008 Password Policy**］オプションを選択すると、［**Remove password from history list when the list is full**］オプションもまたデフォルトで選択されます。Microsoft Server 2008構文が有効である場合、**履歴リストサイズ**範囲は0個～24個のパスワードです。
  - このオプションを選択した場合、［**Numberofdaysbeforepasswordcanbechanged**］および［**Numberofdaysbeforepasswordexpires**］の両方のオプションを選択し、それぞれに最小日数を指定してください。
  - パスワード履歴リストのサイズに0を指定すると、NMASは、ユーザが作成した新しいパスワードをそのユーザの現在のパスワードのみと比較します。

- ［**Numberofcharactersdifferentfromcurrentpasswordandpasswordsfromhistory(0-6)**］、および指定した文字数。。

  このオプションを選択した場合、ユーザは、以前のパスワードで未使用の「新しい」文字を少なくともこの指定数含んでいるパスワードを指定する必要があります。このオプションはデフォルトで選択されています。

  次の値を使用して、未使用文字の固有性の程度を指定することができます。

  - ［**Number of passwords in history to be considered for character exclusion (0-10)**］、および指定した文字数

    新しいパスワードに特定数の未使用文字を含めるように要求する場合、使用済み文字の検査時に考慮すべき過去のパスワードの数を指定できます。

    たとえば、少なくとも新しい3文字を含めるように指定し、以前の5つのパスワードを文字除外で考慮するよう指定した場合、ユーザが新しいパスワード「mountains99」を作成したとき、以前の5つのパスワードで未使用の文字が3文字以上そのパスワードに含まれ

る必要があります。ユーザの以前のパスワードが「maintains99」である場合、新しいパスワードと2文字しか異なっていないため、このパスワードはパスワードポリシーによって拒否され、ユーザは別のパスワードを指定するよう促されます。

注

- ［Number of characters different from current password and passwords from history (0-6)］および［Number of passwords in history to be considered for character exclusion (0-10)］の両方のオプションがデフォルトで選択されます。ただし、両方のオプションの値はデフォルトで0に設定されています。
- ［Number of characters different from current password and passwords from history (0-6)］オプションの値が0に設定される場合、このオプションは無効になります。
- ［Number of passwords in history to be considered for character exclusion (0-10)］オプションの値が0に設定される場合、eDirectoryで「新しい」文字が検査されるときに現在のパスワードだけが考慮されます。
- これらのオプションを使用するには、パスワードポリシーでユニバーサルパスワードを有効にする必要があります。

パスワード有効期間

- **Number of days before password can be changed (0-365)**

  このオプションは、指定した時間が経過するまでユーザがユニバーサルパスワードを変更できないように制限します。たとえば、この値が30に設定されている場合、ユーザは同じパスワードを30日間保持した後、それを変更できるようになります。

- **Number of days before password expires (0-365)**

  このオプションは、指定した時間が経過した後、ユーザのパスワードを期限切れにします。たとえば、この値が90に設定されている場合、ユーザのパスワードが設定された時点から90日後に期限切れになります。猶予ログインが有効な場合、ユーザは指定された回数にわたって期限切れパスワードを使ってログインできます。また、［猶予ログイン制限］オプションを選択していない場合、無制限の猶予ログインが許可されます。

注

- ［Use Microsoft Server 2008 Password Policy］オプションを選択した場合、［Number of days before password can be changed］および［Number of days before password expires］オプションもまたデフォルトで選択されます。Microsoft Server 2008構文が有効になっている場合、両方のオプションの範囲は0～999日です。
- 新しいユーザを作成する場合やヘルプデスクへの問い合わせに応答する場合などに、管理者がユーザのパスワードを変更する場合、パスワードポリシーでパスワードを期限切れにする設定が有効になっていると、パスワードは自動的に期限切れになります。この特定の機能については、日数は重要ではありませんが、この設定を有効にする必要があります。［Do not expire the user's password when the administrator sets the password］オプションを選択した場合、このセキュリティ拡張機能がオーバーライドされます。

- **Limit the number of grace logins allowed (0-254)**

  パスワードの期限が切れた場合、この値は、期限切れパスワードを使ってユーザがeDirectoryにログインできる回数を示します。猶予ログインが有効でない場合、パスワードの有効期限が切れた後にユーザはログインできなくなり、管理者の支援でパスワードをリセットする必要が生じます。この値が1以上である場合、ユーザはパスワードの変更を強制される前に、指定の回数にわたってログインする機会を与えられます。ただし、すべ

ての猶予ログインが使用されるまでにユーザがパスワードを変更しない場合、ユーザはロックアウトされて、eDirectoryにログインできなくなります。また、［**Limit the number of grace logins allowed**］オプションを選択していない場合、無制限の猶予ログインが許可されます。

パスワード除外

- **Exclude the following passwords**

  これにより、除外するパスワードを手動で指定できます。このオプションを使用すると、(パターンやeDirectory属性ではなく)特定の単語や単独の文字を除外することができます。また、*、+、%、空白文字などの特定の特殊文字を含むパスワードを除外することもできます。たとえば、パスワード除外リストに「*」文字を追加した場合、ユーザが「Pa55w0rd*!」というパスワードを指定しようとすると、指定したパスワードが無効であるというエラーを受け取ります。この機能は、環境内のアプリケーションで問題の原因となる特殊文字を含むパスワードを指定しないようユーザを制限する必要がある場合に、役立ちます。

  NMAS 3.1.3以降、除外リスト内の文字列をパスワードに含めることはできず、比較では大文字小文字が区別されません。たとえば、除外リストに「test」がある場合、Test、TEST、ltest, test1、latestをパスワードにすることはできません。

  パスワード除外は、セキュリティ上のリスクになると思われる少数の単語に関してのみ役立つことに注意してください。備わっている除外リスト機能は、辞書などの長い用語リストとして使われるよう意図されていません。除外する用語を長いリストにすると、サーバのパフォーマンスに影響を与える可能性があります。パスワードの「辞書攻撃」から防御するには、長い除外リストを使用する代わりに、［高度なパスワードルール］を使用して、パスワードに数値を含めるようにすることをお勧めします。

- **Exclude passwords that match attribute values**

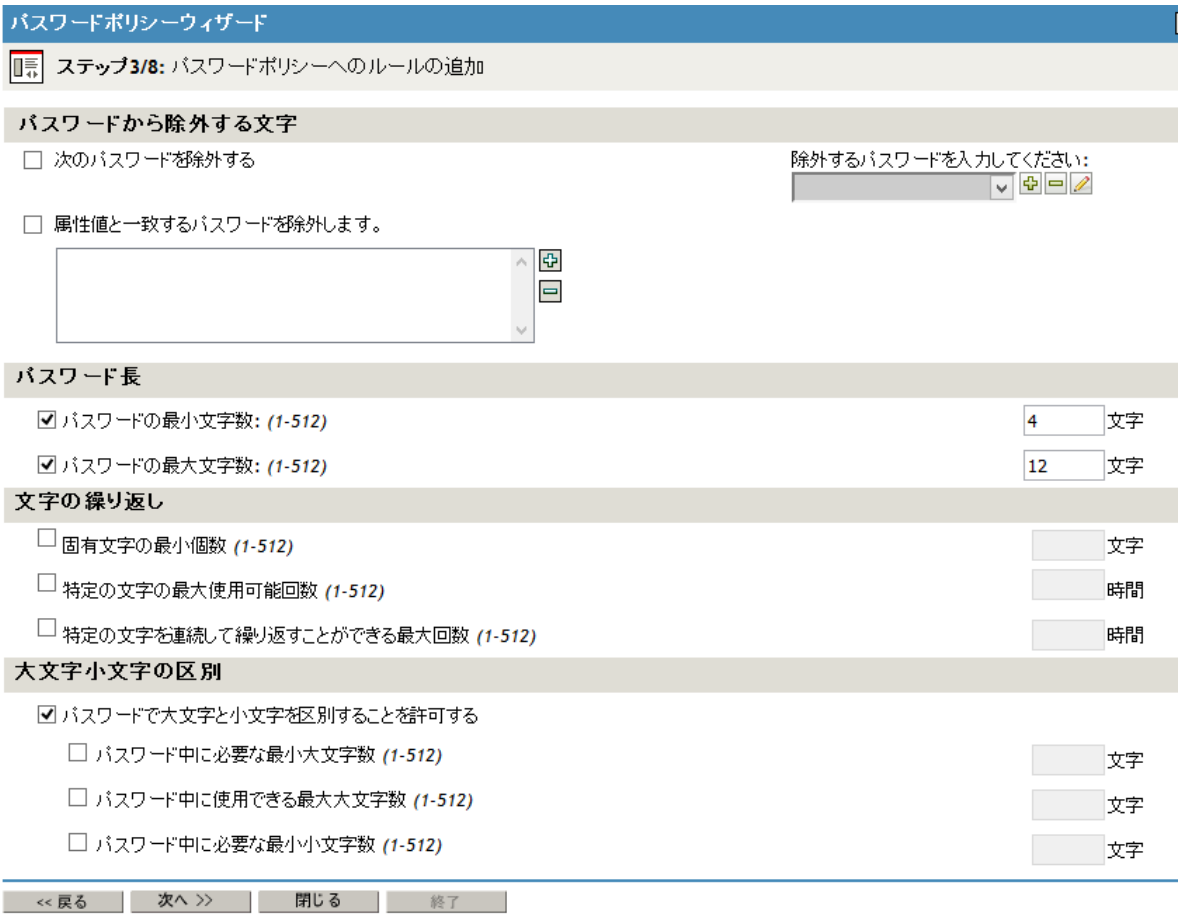
  これにより、パスワードとして使用されないよう除外するユーザオブジェクト属性を選択できます。たとえば、下の名(Given Name)属性をリストに追加し、この属性にFrankという値が含まれる場合、frank、frank1、1frankのどれもパスワードとして使用できません。

  除外するパスワードの長さが3文字未満の場合、NMASはこのチェックを行いません。

  リストで属性値を追加したり削除したりするには、プラスボタンとマイナスボタンを使用します。

注: ［**Use Microsoft complexity policy**］オプションを選択した場合、デフォルトで［**Exclude passwords that match attribute values**］オプションもまた選択されます。Microsoft複雑性ポリシー構文が有効になっている場合、照合する属性値のリストに次の値が入ります: 共通名、表示名、フルネーム、名(ファーストネーム)、姓(ラストネーム)。

図 26-2 高度なパスワードルール(続き)



パスワード長

- **Minimum number of characters in password (1-512)**
- **Maximum number of characters in password (1-512)**

注

- NMASを使用して作成されるパスワードの最大長は512文字です。
- ［**Use Microsoft complexity policy**］オプションを選択した場合、［**Minimum number of characters in password**］、［**Maximum number of characters in password**］のどちらのオプションも使用不可です。
- ［**Use Microsoft Server 2008 Password Policy**］オプションを選択した場合、［**Minimum number of characters in password**］オプションのみが使用可能です。デフォルトではこのオプションが選択されています。
- ［**Use Novell syntax**］オプションを選択した場合、［**Minimum number of characters in password**］および［**Maximum number of characters in password**］の両方のオプションもデフォルトで選択されます。

Password Complexity Violations

- **Maximum number of complexity policy violations in password (0-5)**

  このオプションを使用すると、管理者は、環境内のパスワードに対して許容する複雑性ポリシー違反の数を設定できます。デフォルトで、Microsoft Server 2008パスワードポリシーでは、5種類の文字(大文字、小文字、数字、英数字以外の文字、その他の文字)のうち3種類から少なくとも1つの文字を含む必要があります。したがって、デフォルトで許容される違反の数は2です。Microsoft Server 2008パスワードポリシーのポリシー要件の詳細については、787 ページの 「パスワードの構文」を参照してください。

  パスワードポリシーの制限を厳しくしたり緩めたりするには、許容されるデフォルトの違反数を変更できます。たとえばデフォルト設定を1に変更した場合、すべてのパスワードは、上記の5種類の文字タイプうち4種類からそれぞれ少なくとも1文字を含む必要があります。設定値が4の場合、パスワードは、5種類の文字タイプのうち1種類のみの文字を含む必要があります。

注: ［**Use Microsoft Server 2008 Password Policy**］オプションを選択した場合、［**Maximum number of complexity policy violations in password (0-5)**］オプションのみが使用可能になります。デフォルトではこのオプションが選択されています。

反復する文字

- **Minimum number of unique characters (1-512)**
- **Maximum number of times a specific character can be used (1-512)**
- **Maximum number of times a specific character can be repeated sequentially (1-512)**

注: ［**Use Microsoft complexity policy**］または［**Use Microsoft Server 2008 Password Policy**］のいずれかのオプションを選択した場合、［**Minimum number of unique characters**］、［**Maximum number of times a specific character can be used**］、および［**Maximum number of times a specific character can be repeated sequentially (1-512)**］オプションは使用不可です。

大文字と小文字の区別あり

eDirectoryで［**パスワードで大文字小文字の区別を許可**］オプションを使用すると、eDirectory 9.2にアップグレードされたすべてのクライアントでパスワードの大文字と小文字が区別されます。

注

- ［**Allow the password to be case sensitive**］オプションは、［**Use Novell syntax**］オプションを選択した場合にのみ使用可能になります。デフォルトではこのオプションが選択されています。
- ユニバーサルパスワードを無効にすることを選択した場合は、大文字と小文字を区別するオプションがデフォルトで選択されて無効になります。

［**Allow the password to be case sensitive**］オプションは、［**Use Novell syntax**］オプションを選択した場合にのみ使用可能になります。デフォルトではこのオプションが選択されています。

［**Allow the password to be case sensitive**］を選択した場合、次の4つのオプションがあります。

- **Allow the password to be case sensitive**
  - **Minimum number of upper case characters required in the password (1-512)**

- Maximum number of upper case characters allowed in the password (1-512)
- Minimum number of lower case characters required in the password (1-512)
- Maximum number of lower case characters allowed in the password (1-512)

［Allow the password to be case sensitive］を選択しない場合、パスワードでは大文字小文字が区別されず、次の2つのオプションがあります。

- Minimum number of alphabetic characters allowed in password (1-512)
- Maximum number of alphabetic characters allowed in password (1-512)

重要: ［Allowpasswordstobecasesensitive］オプションを選択しない場合でも、パスワードは大文字小文字を区別して保存され、複数のシステム間で同期される際に大文字小文字が区別されます。［Allowpasswordstobecasesensitive］オプションを選択しない場合、パスワード文字の大文字小文字は無視されます。

図 26-3 高度なパスワードルール(最後)

数字

- Allow numeric characters in password
  - Disallow numeric as first character

- Disallow numeric as last character
- Minimum number of numerals in password (1-512)
- Maximum number of numerals in password (1-512)

注: ［Allownumericcharactersinpassword］オプションは、［UseNovellsyntax］オプションを選択した場合にのみ使用可能です。デフォルトではこのオプションが選択されています。

英数字以外の文字

英数字以外の文字とは、数字(0～9)でも英字(アルファベット文字)でもない文字です。アルファベット文字は、a～z、A～Z、およびLatin-1コードページ850のアルファベット文字と定義されます。

- Allow non-alphanumeric characters in the password
  - Disallow non-alphanumeric character as first character
  - Disallow non-alphanumeric character as last character
  - Minimum number of non-alphanumeric characters (1-512)
  - Maximum number of non-alphanumeric characters (1-512)
- Allow non-US ASCII characters

  このオプションを使用すると、基本ラテン文字セット以外の文字(拡張文字とも呼ばれる)をパスワードに含めることができます。

注: ［Allownon-alphanumericcharactersinthepassword］オプションは、［UseNovellsyntax］オプションを選択した場合にのみ使用可能です。デフォルトではこのオプションが選択されています。

アルファベット以外の文字

アルファベット以外の文字とは、アルファベット文字(英字)ではない文字です。アルファベット文字は、a～z、A～Z、およびLatin-1コードページ850のアルファベット文字と定義されます。

- Allow non-alphabetic characters in the password
  - Minimum number of non-alphabetic characters (1-512)
  - Maximum number of non-alphabetic characters (1-512)

注

- ［Allow non-alphabetic characters in the password］オプションは、［Use Novell syntax］オプションを選択した場合にのみ使用可能です。
- ［アルファベット以外の文字をパスワードで使用することを許可］オプションを使用する場合、ポリシーでパスワードを過度に厳しく制限しないようにしてください。たとえば、複数の非アルファベット文字や数字を要求すると同時に、使用できる非アルファベット文字数を*制限する*ようなポリシーです。

パスワードポリシーインタフェースの外部でパスワードポリシーを変更する

iManagerパスワード管理プラグインを使ってパスワードポリシーの作成、変更、割り当てることに加えて、パスワードポリシーインタフェースの外部でポリシーを変更することもできます。次の方法があります。

- ディレクトリ管理インタフェースを使用してポリシーオブジェクトを直接変更する。
- ldapmodifyコマンドラインツールを使用してポリシーオブジェクトを直接変更する。

ただし、パスワードポリシーインタフェースの外部でパスワードポリシーを操作することは推奨されません。そのような操作ですべての属性を正しく設定しない場合、環境で問題が発生する可能性があるためです。たとえば1つのポリシーに関して複数のポリシータイプを設定した場合、優先順位が「最も高い」ポリシータイプだけが有効になり、eDirectoryは、適用される「より低い」ポリシータイプのポリシールールをすべて無視します。パスワードポリシータイプの優先度の詳細については、789 ページの 「パスワード構文の優先順位」を参照してください。

さらに、パスワードポリシーインタフェースを使用せずにMicrosoft Server 2008パスワードポリシータイプからMicrosoft複雑性ポリシータイプに変更した場合、iManagerはポリシーオブジェクト内の既存のMicrosoft Server 2008パスワードポリシー属性(nspmAD2K8Syntax)を削除しません。代わりに、iManagerはこの属性の値をFalseに設定します。この状況で、eDirectoryは両方のポリシータイプで設定されたすべてのポリシーとルールを無視します。

さらに、LDAPを使用してポリシーの特定のルールを変更するときに、別の問題が発生することがあります。ポリシーを変更した結果として2つのルールが競合するようになった場合、eDirectoryは、ポリシー内の選択されていない(またはFalseに設定されている)競合ルールではなく、選択されている(またはTrueに設定されている)ルールを適用します。

たとえば、あるポリシーを作成した後、数字を禁止してアルファベット以外の文字を許可するようそのポリシーを変更したとします。nspmNonAlphaCharactersAllowed属性の値がTrueに設定されているため、nspmNumericCharactersAllowedがFalseに設定されていても、数字を含むアルファベット以外のすべての文字が許可されます。

パスワードのランダム生成

特定のパスワードを指定する代わりに、ユーザはランダムに生成されるパスワードを要求することもできます。ランダムに生成されるパスワードは、そのユーザに割り当てられている複雑さの要件、および他のパスワードポリシー制限に自動的に準拠します。

ランダムに生成されるMicrosoft Server 2008パスワード

Microsoft Server 2008パスワードポリシー用のランダム生成パスワードは、他のパスワードポリシータイプを使ってランダム生成されるパスワードと比べて、次の点で異なります。

- Microsoft Server 2008パスワードポリシータイプを使用するパスワードポリシーを割り当てられているユーザがランダム生成パスワードを要求する場合、NMASは、ポリシーで許容されるパスワード複雑性違反数に基づいてパスワードを生成します。
- 許容されるパスワード複雑性違反数が最大値(5)に設定されている場合、ランダム生成されるすべてのパスワードは、大文字または小文字のアルファベット文字だけで構成されます。

- パスワード複雑性の要件が極端に厳しく設定されている場合、ランダム生成されたパスワードであっても、パスワードポリシーに対して無効である可能性があります。
- Microsoft Server 2008パスワードポリシーの下でランダム生成されるパスワードの最大長は16文字です(ただしポリシーで設定された最小長が16文字を超える場合を除く)。最小長が16を超える場合、生成されるパスワードの長さは、ポリシーで設定された最小長です。たとえば、Microsoft Server 2008ポリシーを使用してパスワードの最小長が20文字と設定されている場合、ランダム生成されるパスワードの長さは常に20文字になります。

ユニバーサルパスワードの設定オプション

次の図は、ユニバーサルパスワードの設定オプションの例を示しています。

図26-4 環境設定オプション

- **Enable Universal Password**

  このポリシーでユニバーサルパスワードを有効にします。ユニバーサルパスワードを有効にするか無効にするかを選択できます。

- **Enable the Advanced Password Rules**

  このポリシーの［高度なパスワードルール］ページにある［高度なパスワードルール］を有効にします。これらの高度なパスワードルールでは、パスワード有効期間とパスワードに含む文字を制御できるため、環境のセキュリティ向上に役立ちます。

- **パスワード同期**

  - **Remove the NDS password when setting Universal Password**

    このオプションを選択すると、ユニバーサルパスワードが設定されるときにNDSパスワードが無効になります。また、NDSパスワードが設定されるときに、eDirectory以外に知られないランダムな値にNDSパスワードハッシュが設定されます。ランダム値にハッシュ化できるパスワードが存在することも、存在しないこともあります。

  - **Synchronize NDS password when setting Universal Password**

このオプションを選択した場合、ユニバーサルパスワードが設定されるときに、同じパスワードを使って同時にNDSパスワードも設定されます。

- **Synchronize Simple Password when setting Universal Password**

  注: このオプションを設定しても、ICEを使用してユーザパスワードをインポートする機能には影響がありません。

  このオプションを選択した場合、ユニバーサルパスワードが設定されるときに、同じパスワードを使って同時に単純パスワードも設定されます。

- **Synchronize Distribution Password when setting Universal Password**

  Identity Managerメタディレクトリエンジンがe Directory内のユーザのユニバーサルパスワードを取得または設定できるかどうかを決定します。

  このオプションを選択した場合、ユニバーサルパスワードが設定されるときに、同じパスワードを使って同時に配布パスワードも設定されます。

  接続システムに対するパスワード同期を実行するために、配布パスワードをIdentity Managerとともに使用できます。また、このオプションにより、メタディレクトリエンジンはeDirectory内のユーザのユニバーサルパスワードを取得することもできます。

- **Universal Password Retrieval**

  注: ユニバーサルパスワードを無効にすることを選択した場合は、次のオプションはデフォルトで無効になります。

  - **Allow user to retrieve password**

    パスワードを忘れた場合のセルフサービス機能がユーザに代わってパスワードを取得し、それを電子メールでユーザに送信できるかどうかを決定します。このオプションを選択しない場合、パスワードポリシーの［パスワードを忘れた場合］ページの対応する機能がぼかし表示になります。

    このオプションにより、ユーザはNMASLDAP拡張機能を使用して自分のパスワードを取得することができます。

  - **Allow admin to retrieve passwords**

    この機能を使用するサードパーティ製品またはサービスを使ってユーザのパスワードを取得することができます。

    このオプションはお勧めできません。稼働するためにこの機能を必要とする特定のオブジェクト(SAMBAまたはfreeRADIUSサービスオブジェクトなど)にパスワード読み取り権限を割り当てるには、［**Allow the following to retrieve passwords**］オプションを代わりに使用してください。

    ［**Allow admin to retrieve passwords**］が選択されている場合、ターゲットオブジェクトのACL属性に対する書き込み特権を持つユーザはターゲットオブジェクトのパスワードを取り出すことができます。

  - **Allow the following to retrieve passwords**

    パスワードを取得できるオブジェクトを挿入することができます。

    注: 十分な特権を持たないメンバーが、特定のユーザに関して［**パスワード状態のチェック**］タスクを使用すると-672エラーを受け取ります。

- **認証**
  - **Verify whether existing passwords comply with the password policy (verification occurs on login)**

    このオプションを選択した場合、ユーザがiManagerからログインすると、ユーザの既存のパスワードが検査されて、ユーザのパスワードポリシーにある高度なパスワードルールに準拠しているかどうかが確認されます。既存のパスワードが準拠していない場合、ユーザはそれを変更するよう要求されます。ユニバーサルパスワードを無効にすると、このオプションもデフォルトで無効になります。

ユーザへのパスワードポリシーの割り当て

eDirectory内のユーザにパスワードポリシーを割り当てる方法として、(ログインポリシーオブジェクトを使用して)ツリー全体にポリシーを割り当てたり、特定のパーティションやコンテナ、または特定のユーザに割り当てたりすることができます。管理を単純化するために、ツリー内のできるだけ高いレベルでパスワードポリシーを設定することをお勧めします。

重要: eDirectoryツリー全体、またはサブコンテナに非常に多くの(何万もの)ユーザを含むツリーのコンテナにパスワードポリシーを割り当てた場合、iManagerおよびiManagerプラグインがハングすることがあります。

この場合、パスワードポリシー割り当てごとのユーザ数を制御するために、下位レベルのコンテナに個別にパスワードポリシーを割り当てることを考慮できます。

ポリシーは、1つ以上のオブジェクトに割り当てるまでは有効になりません。パスワードポリシーは次のオブジェクトに割り当てることができます。

- ログインポリシーオブジェクト

  ツリー内のすべてのユーザに対し、デフォルトのパスワードポリシーを作成することをお勧めします。これを実行するには、ポリシーを作成して、ログインポリシーオブジェクトに割り当てます。ログインポリシーオブジェクトは、ツリーのルート直下のセキュリティコンテナ内にあります。
- パーティションのルートであるコンテナ

  コンテナ パーティションのルートになっているコンテナにポリシーを割り当てると、ポリシー割り当てはサブコンテナのユーザを含めたパーティション内のすべてのユーザに継承されます。コンテナがパーティションルートであるかどうかを知るには、そのコンテナを参照して、隣にパーティションアイコンが表示されているかどうかを確認します。
- パーティションのルートではないコンテナ

  パーティションのルートではないコンテナにポリシーを割り当てると、そのポリシー割り当ては、その特定のコンテナ内のユーザだけに継承されます。サブコンテナ内のユーザには継承されません。パーティションのルートではないコンテナの下位にあるユーザすべてにポリシーを適用する場合は、それぞれのサブコンテナに個別のポリシーを割り当てる必要があります。
- 特定のユーザ

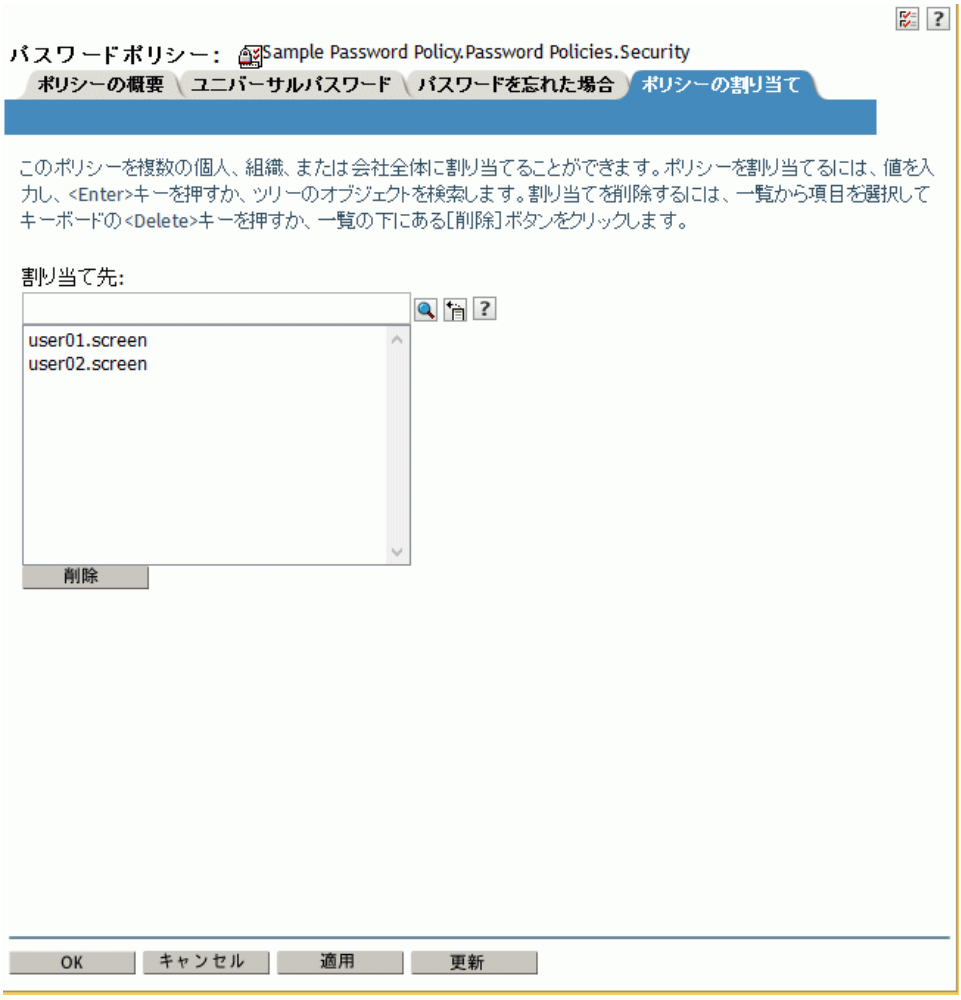
1人のユーザに対して一度に1つのポリシーのみを有効にできます。NMASは、次の順序でポリシーを検索し、最初に見つかったものを適用することで、ユーザに対して有効にするポリシーを決定します。

1. **ユーザごとの割り当て:** パスワードポリシーがユーザに割り当てられている場合、そのポリシーが適用されます。

2. **コンテナ:** パスワードポリシーがユーザに割り当てられていない場合、NMASはそのユーザが存在するコンテナに割り当てられたポリシーを適用します。
3. **パーティションルートのコンテナ:** パスワードポリシーが、ユーザやそのユーザの上位コンテナにも割り当てられていない場合、パーティションルートのコンテナに割り当てられたポリシーが適用されます。
4. **ログインポリシーオブジェクト:** ポリシーが、ユーザやその他のコンテナにも割り当てられていない場合、ログインポリシーオブジェクトに割り当てられたポリシーが適用されます。これはツリー内のすべてのユーザに対するデフォルトポリシーです。

次の図に示すプロパティページの例では、どのオブジェクトパスワードポリシーを割り当てるかを指定します。

***図26-5** オブジェクトにパスワードポリシーを割り当てる*



ユーザに適用されているポリシーの識別

1人のユーザに対して一度に1つのポリシーのみが有効になります。特定のユーザまたはコンテナに対してどのポリシーが有効になっているか検出するには、次の手順を実行します。

1. iManagerの［**役割およびタスク**］ビューで、［**パスワード**］>［**View Policy Assignments**］をクリックします。
2. 該当するユーザをブラウズして選択します。
3. **OK**をクリックします。

ツリー内に複数のポリシーが存在する場合、801 ページの 「ユーザへのパスワードポリシーの割り当て」で説明されている方法で、NMASはユーザに割り当てるポリシーを決定します。

ユーザのパスワードの設定

管理者またはヘルプデスク担当者は、iManagerのタスクを使用してユーザのユニバーサルパスワードを設定できます。このタスクでは、ユーザに適用されているパスワードポリシーのパスワードルールが表示されます。

1. iManagerの［**役割およびタスク**］ビューで、［**パスワード**］>［**Set Universal Password**］をクリックします。
2. 該当するユーザをブラウズして選択します。
3. **OK**をクリックします。

   ユーザにパスワードポリシーがすでに割り当てられ、ユニバーサルパスワードが有効になっている場合は、このタスクを使用してパスワードを変更できます。

   高度なパスワードルールがポリシーで有効になっている場合、準拠すべきルールのリストが表示されます。

   ユーザのユニバーサルパスワードが有効でない場合、iManagerでエラーが表示されます。ユーザにポリシーを割り当てた後でこのタスクに戻るか、［**eDirectory管理**］>［**オブジェクトの変更**］タスクを使用してユーザのNDSパスワードを変更する必要があります。
4. 表示されるすべてのパスワードルールに準拠していることを確認しながら、ユーザのパスワードを作成します。
5. **OK**をクリックします。

   ユーザのユニバーサルパスワードが変更されます。

   パスワード同期が環境で設定されている場合、ユーザの新しいパスワードは、それを受け入れるよう設定されている接続先システムに配布されます。

注: 新しいユーザを作成する場合やヘルプデスクへの問い合わせに応答する場合などに、管理者がユーザのパスワードを変更する場合、パスワードポリシーでパスワードを期限切れにする設定が有効になっていると、パスワードは自動的に期限切れになります。［**Number of days before password expires**］という設定が高度なパスワードルールに含まれています。この特定の機能については、日数は重要ではありませんが、この設定を有効にする必要があります。

［**Do not expire the user's password when the administrator sets the password**］オプションは、この機能をオーバーライドします。

ユニバーサルパスワードの診断ユーティリティ

eDirectoryには、状態をチェックして、ユニバーサルパスワードを再暗号化するためのユーティリティが用意されています。ユニバーサルパスワードの診断ユーティリティ(diagpwd)は、管理者がユーザのユニバーサルパスワード(UP)、簡易パスワード、NDSパスワード、および配布パスワード(DP)の状態を確認できるようにするツールです。これらのパスワードの同期状態もレポートします。diagpwdユーティリティの構文の例を以下に示します。

```
diagpwd LDAP_SERVER_ADDR TLS_PORT CA_CERT_FILE SEARCH_BASE SEARCH_SCOPE BIND_DN
[BIND_PWD] -t
```

オプション	説明
LDAP_SERVER_ADDR	ターゲットLDAPサーバのアドレスを指定します。
TLS_PORT	ターゲットLDAPサーバのLDAPセキュアポート(TLS)を指定します。
CA_CERT_FILE	ターゲットLDAPサーバのルート認証局証明書を含む、PEMエンコードされたファイルのパスを指定します。
SEARCH_BASE	searchbaseを検索の開始ポイントとして使用します。
SEARCH_SCOPE	検索のスコープを指定します。スコープとして、ベースオブジェクトを示す「base」、1レベルを示す「one」、またはサブツリー検索を示す「sub」を指定します。
BIND_DN	管理者のLDAP DNです。たとえば、cn=admin,o=companyと指定します。
BIND_PWD	管理者のLDAPパスワード。 **注:** このパラメータはオプションです。コマンドラインで指定されていない場合は、ユーザに対してプロンプトが表示されます。
-t	これにより、UP、DP、簡易パスワード、およびパスワード履歴が256ビットAESキーを使用して再暗号化されます。AES 256ビットのツリーキーを作成した後に、このオプションを使用します。 **注:** このオプションを使用している場合は、パスワードポリシーを使用して、このユーティリティを実行しているユーザが自分のUPを取得できるようにしてください。

例

サーバ192.168.1.1上のユーザcn=user1,ou=users,o=companyのパスワードの状態を確認するには、次のコマンドを実行します。

```
diagpwd 192.168.1.1 636 /home/user1/cert.pem cn=user1,ou=users,o=company base
cn=admin,o=company
```

ou=users,o=companyサブツリー内のすべてのユーザのパスワードの状態を確認するには、次のコマンドを実行します。

```
diagpwd 192.168.1.1 636 /home/user1/cert.pem ou=users,o=company sub
cn=admin,o=company
```

ou=users,o=companyサブツリー内のすべてのユーザのパスワードをAES 256ビットキーで再暗号化するには、次のコマンドを実行します。

```
diagpwd 192.168.1.1 636 /home/user1/cert.pem ou=users,o=company sub
cn=admin,o=company -t
```

パスワードポリシーのトラブルシューティング

ユーザにパスワードポリシーが割り当てられていないことを示すエラー

ユニバーサルパスワードの設定タスクで、ユーザにパスワードポリシーが割り当てられていないというエラーが表示された場合、実際にはユーザにパスワードポリシーが割り当てられているのであれば、SSLの問題である可能性があります。SSLの問題を診断して解決するには、次のタスクを実行します。

- SSLの環境設定に問題があることを確かめるには、ポリシー割り当て表示タスクを使用して、そのユーザのポリシーを確認します。ポリシー割り当て表示タスクにNMAS転送エラーが表示される場合、これはSSLが正しく設定されていないことを示している可能性があります。
- iManagerを実行するWebサーバとプライマリeDirectoryツリーの間でSSLが正しく設定されていることを確認してください。WebサーバとeDirectoryの間で証明書が設定されていることを確認します。
- 単純認証用にTLSを必要としない場合、786 ページのステップ 6の注記で説明されているように、正しいLDAP SSLポートを確実に指定する必要があります。

秘密の質問の答えを使用する

iManagerでサポートされるブラウザを使用していることを確認してください。

新しいコンテナ内のユーザへのアクセス権限の付与

iManagerまたはいずれのNetIQポータル製品(ユーザアプリケーションなど)をセットアップするときには、ポータルユーザコンテナを指定します。通常は、ツリーのすべてのユーザがポータル機能にアクセスできるように、ツリー内の高いレベルでコンテナを指定します。すべてのユーザがそのコンテナの下にある場合は、すべてのユーザが「パスワードを忘れた場合」および「パスワードのリセット」セルフサービス機能にアクセスできます。

NMAS LDAP転送エラー

マルチサーバ環境でIdentity Managerをインストールしている場合、iManagerでいくつかのパスワード管理プラグインを使用すると、「NMAS LDAP転送エラー」で始まるエラーが表示されることがあります。

このエラーの一般的な原因の1つは、Identity Managerで必要なNMAS拡張機能を持っていないLDAPサーバをPortalServlet.propertiesファイルが参照していることです。PortalServlet.propertiesファイルを開き、LDAPサーバのアドレスがIdentity Managerのインストール場所と同じサーバであることを確認してください。

この他の考えられる原因:

- LDAPサーバが稼働していない。
- プラグインを実行しているiManagerサーバとLDAPサーバの間でLDAP用のSSLが設定されていない。
- リモートIdentity Managerサーバを管理するためにiManagerで他のツリーにログインするとき、リモートサーバのIPアドレスの代わりにサーバ名を使用するとエラーが発生することがあります。
- 認証先となるツリーのルート認証局証明書を、信頼された証明書としてWebサーバにインポートする必要があります。keytool.exeを使用して、証明書をWebサーバにエクスポートできます。

パスワードセルフサービス

このセクションでは、パスワードセルフサービスの設定と管理について説明します。

パスワードセルフサービスの概要

セルフ(自己)サービスを設定すると、ユーザがパスワードを忘れた場合に復元したり、パスワードポリシーで指定済みのルールを見ながらパスワードをリセットしたりできるため、ヘルプデスクの負担を減らすことができます。

パスワードセルフサービスのポリシーを管理するには、次のいずれかを使用します。

- iManager

この章では主に、iManagerを使用してパスワードセルフサービスを管理する方法について説明します。

- Identity Managerユーザアプリケーション

  Identity Managerユーザアプリケーションでパスワードセルフサービスを管理する方法については、『*NetIQ Identity Manager Roles Based Provisioning Module 4.5 User Application User Guide (NetIQ Identity Manager Roles Based Provisioning Module 4.5ユーザアプリケーションのユーザガイド)*』の「Using the Identity Self-Service Tab (［アイデンティティセルフサービス］タブを使用する)」を参照してください。

ユーザは、次のいずれかを使用してパスワードセルフサービス機能にアクセスします。

- iManagerポータル
- Identity Managerユーザアプリケーションのポートレット

  Identity Managerユーザアプリケーションでパスワードセルフサービスを使用する方法については、『*NetIQ Identity Manager Roles Based Provisioning Module 4.5 User Application User Guide (NetIQ Identity Manager Roles Based Provisioning Module 4.5ユーザアプリケーションのユーザガイド)*』の「Using the Identity Self-Service Tab (［アイデンティティセルフサービス］タブを使用する)」を参照してください。
- Novell Client

  Novell Clientでパスワードセルフサービスを使用する方法については、『Novell Client for Windows Administration Guide (Novell Client for Windows管理ガイド)』の「Using Forgotten Password Self-Service (パスワードを忘れた場合のセルフサービスを使用する)」を参照してください。

パスワードセルフサービスを使用するための前提条件

780 ページの 「パスワードポリシーを使用したパスワードの管理」の情報を確認して、785 ページの 「パスワードポリシーを使用するために必要な事前タスク」の前提条件を満たすようにしてください。

ユニバーサルパスワードを展開しなくてもパスワードセルフサービスの一部の機能を使用できますが、パスワードポリシーのすべての機能を使用できるようにするために、環境を準備してユニバーサルパスワードを有効にすることをお勧めします。

また、Novell Clientでもパスワードセルフサービス機能を利用します。『Novell Client for Windows Administration Guide (Novell Client for Windows管理ガイド)』の「Using Forgotten Password Self-Service (パスワードを忘れた場合のセルフサービスを使用する)」を参照してください。

パスワード忘れの管理

次のセクションでは、iManagerを使用して「パスワード忘れ」(パスワードを忘れた場合の機能)を管理する方法について説明します。

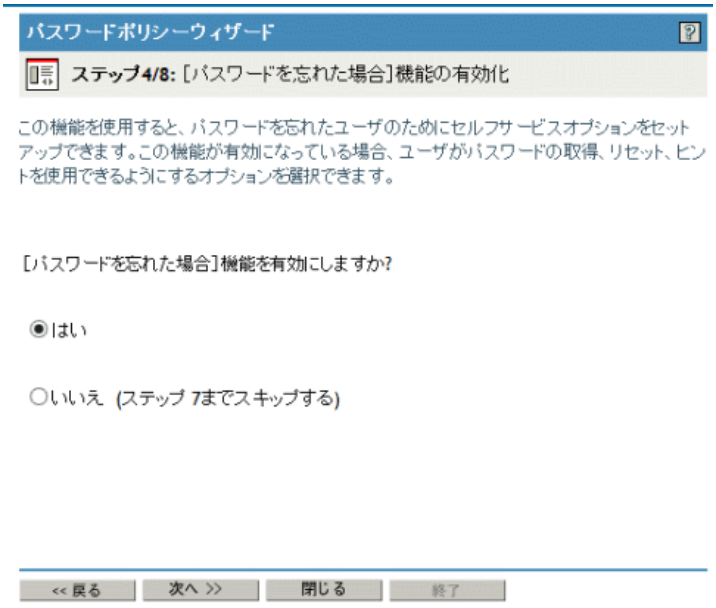
Identity Managerユーザアプリケーションを使用してパスワード忘れを管理する方法については、『*NetIQ Identity Manager 4.5 Password Management Guide (NetIQ Identity Manager 4.5パスワード管理ガイド)*』の「Password Management Configuration (パスワード管理の設定)」を参照してください。

- 808 ページの 「パスワード忘れ機能の有効化」
- 809 ページの 「秘密の質問の作成または編集」
- 811 ページの 「パスワードを忘れた場合のアクションの選択」
- 812 ページの 「「パスワードを忘れた場合」の環境設定」
- 817 ページの 「パスワードを忘れたときにユーザに表示される情報」

パスワード忘れ機能の有効化

ユーザがパスワードを忘れた場合にヘルプデスクに連絡せずに回復できるようにするには、パスワード忘れ機能を有効にします。次の図に示すように、パスワードポリシーウィザードを使用してパスワードポリシーを作成するときに、このオプションが表示されます。パスワードポリシーウィザードの詳細については、810 ページの 「パスワードポリシーウィザードの使用中に秘密の質問を作成するには、次の手順を実行します。」を参照してください。

図 26-6 *パスワードを忘れた場合の処理を有効にする*



また、次のようにして既存のパスワードポリシーでパスワード忘れ機能を有効にすることもできます。

1. iManagerで、［**パスワード**］>［**パスワードポリシー**］の順にクリックします。
2. ポリシーの名前をクリックします。

3 ［パスワードを忘れた場合］タブをクリックします。

4 ［パスワードを忘れた場合の処理を有効にする］を選択し、秘密の質問を選択または作成し、アクションを指定し、［認証］オプションを選択して、［OK］をクリックします。

秘密の質問の作成または編集

秘密の質問とは本人確認のためにユーザが答える質問のセットであり、ユーザがパスワードを使用せずに自分の識別情報を答えとして入力します。秘密の質問はパスワードポリシーに割り当てられ、パスワードポリシーの認証方式の一部として使用されます。これらの秘密の質問に対するユーザの答えでは、大文字小文字が区別されます。

ユーザ向けの「パスワード忘れ」セルフサービス機能の一部として、秘密の質問を使用することができます。忘れたパスワードを受け取る前に秘密の質問に答えるようユーザに要求することで、セキュリティのレベルが追加されます。

パスワードポリシーを作成するときに「パスワード忘れ」セルフサービスを有効にすると、ユーザはヘルプデスクに電話しなくても支援を受けることできます。セルフサービスの安全性を高めるには、秘密の質問を作成して、パスワード忘れの支援をユーザが利用する前に必ず秘密の質問に答えるように指定できます。また、ユーザが質問に答えた後に実行する支援動作(たとえばパスワードのヒントを表示するなど)も指定します。これらのセルフサービス機能は、iManagerを通してユーザに提供されます。選択肢については、811 ページの 「パスワードを忘れた場合のアクションの選択」の説明をブラウズしてください。

秘密の質問を作成するには、次の手順に従います。

1 iManagerで［パスワード］>［Challenge Sets］をクリックします。

2 ［新規作成］をクリックします。

3 ［Challengesetname］フィールドに名前を入力し、秘密の質問が作成されるコンテナを選択して、秘密の質問を選択または作成します。

秘密の質問のデフォルトの質問を選択するには、該当するチェックボックスを選択します。

質問や、答えとして許可される(最小または最大)文字数を編集するには、質問をクリックします。

質問を作成してそれを秘密の質問に追加するには、［Add Question］をクリックします。

ﾕｰｻﾞ定義: このオプションを選択した場合、ユーザは独自の秘密の質問を作成できます。

NMASは、ユーザ定義の質問および答えをeDirectoryに格納します。

必須の質問: ユーザがパスワードセルフサービスを使用するときには、このリストに含まれる質問が常に表示されます。

ランダムな質問: ユーザが初めて秘密の質問に答えることによってパスワード忘れ機能をセットアップするとき、このリストの質問が一度だけ完全なセットとして表示されます。その後、パスワード忘れ機能を利用する必要が生じた場合には、質問セットの一部のみが提示され、ユーザはその質問に答えます。ランダムに表示される質問の数は、指定した数によって決まります。

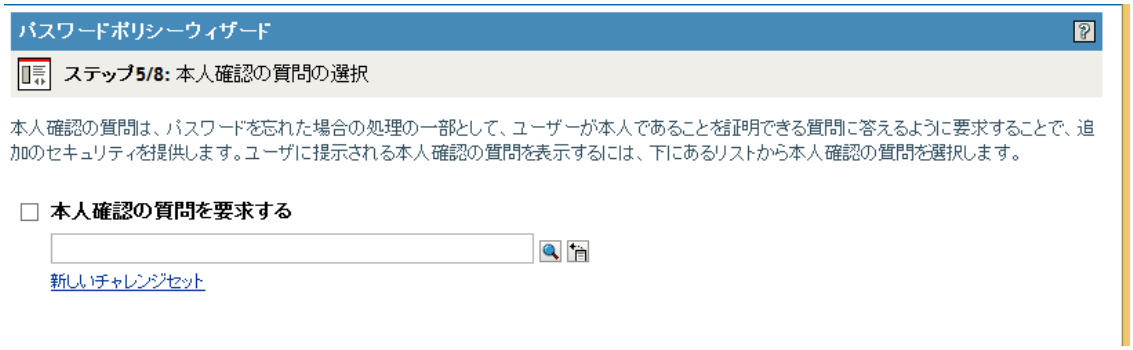
4 OKをクリックします。

パスワードポリシーウィザードの使用中に秘密の質問を作成するには、次の手順を実行します。

1 iManagerで［パスワード］>［パスワードポリシー］>［新規］をクリックしてウィザードを起動します。

2 ステップ4で［はい］をクリックして、パスワード忘れ機能を有効にします。

3 ステップ5で［Require a Challenge Set］を選択して、［New challenge set］をクリックします。



既存の秘密の質問を使用するには、それをブラウズして選択します。

4 作成した秘密の質問が入るコンテナを指定します。［ChallengeSetName］ フィールドに名前を入力して、［次へ］をクリックします。

5 必須またはランダムの秘密の質問を選択するか、作成します。

新しい質問を作成する必要がない場合は、既存の質問を選択してください。

ユーザが独自の質問を追加できるようにするには、［ユーザ定義］を選択します。

新しい質問を作成するには、次の手順を実行します。

5a ［Add Question］をクリックします。

5b ［AdministratorDefinestheQuestion］を選択し、［追加］をクリックし、ドロップダウンメニューから言語を指定し、質問を入力して、［OK］をクリックします。

5c この質問が必須か、それともランダムかを指定します。

5d 必要に応じて最小文字数と最大文字数を指定し、［OK］をクリックします。

6 ランダムな質問の数を指定して、［次へ］をクリックします。

7 パスワードポリシーウィザードの残りのステップを完了します。

既存のパスワードポリシーで秘密の質問を作成するには、次の手順を実行します。

1 iManagerで、［パスワード］>［パスワードポリシー］の順にクリックします。

2 ポリシーの名前をクリックします。

3 ［パスワードを忘れた場合］タブをクリックします。

4 ［パスワードを忘れた場合の処理を有効にする］>［Require a Challenge Set］を選択します。

5 既存の秘密の質問をブラウズして選択するか、新しい秘密の質問を作成してそれを選択します。

新しく作成するには、次の手順を実行します。

5a ［Challenge Sets］リンクをクリックします。

5b ［Challenge Sets］ダイアログボックスで、［新規］をクリックします。

5c ［ChallengeSets］ダイアログボックスで、秘密の質問に名前を付け、作成した秘密の質問が入るコンテナを指定し、必須またはランダムの質問を選択または追加して、ユーザに提示するランダム質問の数を指定します。

5d OKをクリックします。

パスワードを忘れた場合のアクションの選択

1 iManagerで、［パスワード］>［パスワードポリシー］の順にクリックします。

2 ポリシーの名前をクリックします。

3 ［パスワードを忘れた場合］タブをクリックします。

4 ［パスワードを忘れた場合の処理を有効にする］チェックボックスを選択します。

5 アクションを選択します。

- **ユーザがパスワードをリセットできるようにする:** 秘密の質問に答えて自分を識別する情報を入力した後、ユーザは新しいパスワードに変更することを許可されます。ユーザは秘密の質問に答えることによってすでに認証されているため、古いパスワードを入力しなくてもパスワードを変更することができます。このオプションを使用するには、管理者が秘密の質問を要求する必要があります。さらに、ユーザが秘密の質問に答えることによってiManagerポータルでパスワード忘れ機能をすでにセットアップしている必要もあります。
- **現在のパスワードを電子メールでユーザに送信する:** 秘密の質問に答えて自分を識別する情報を入力した後、ユーザは現在のパスワードを電子メールで受け取ります。このオプションを使用するには、次の操作をする必要があります。
  - ポリシーのユニバーサルパスワードを有効にします。これは［ユニバーサルパスワード］の［環境設定オプション］にあります。
  - ［Allow User to Retrieve Password］オプションを有効にします(［ユニバーサルパスワード］の下の［環境設定オプション］)。
  - 820 ページの 「パスワードセルフサービスの電子メール通知の設定」の説明に従って電子メール通知を設定します。

  さらに、ユーザが秘密の質問にすでに答えることで、iManagerのパスワード忘れ機能をセットアップしていなければなりません。
- **ユーザにヒントを送信する:** ユーザはパスワードのヒントを電子メールで受信します。このオプションを使用するには、820 ページの 「パスワードセルフサービスの電子メール通知の設定」の説明に従って電子メール通知をセットアップする必要があります。

  さらに、ユーザがパスワードのヒントをすでに入力した結果として、iManagerのパスワード忘れ機能がセットアップ済みである必要もあります。
- **ヒントをページに表示:** iManagerポータルで、パスワードのヒントがユーザに表示されます。このオプションを使用するには、ユーザがすでにパスワードのヒントを指定して、iManagerのパスワード忘れ機能をセットアップ済みである必要があります。

パスワードのヒント

パスワード忘れ機能のアクションとしてパスワードのヒントを要求するよう指定した場合、ユーザはパスワードを思い出すためのヒントを入力できます。

- 812 ページの 「Password Hint(パスワードヒント)」
- 812 ページの 「ヒントのセキュリティを確保する」

Password Hint(パスワードヒント)

パスワードヒント属性(nsimHint)はパブリックに読み込み可能です。これにより、認証を受けていない、パスワードを忘れたユーザは自分のヒントにアクセスできます。パスワードヒントを使用すると、ヘルプデスクへの問い合わせが非常に少なくなる可能性があります。

セキュリティのため、パスワードヒントにユーザの実際のパスワードが含まれていないかどうか検査されます。ただし、作成したパスワードヒントでユーザがパスワードに関する情報を多くの与えすぎてしまう可能性が依然としてあります。

パスワードヒントを使用する際のセキュリティを強化するには、以下を行います。

- パスワードセルフサービスに使用されるnds-cluster-configサーバ上のnsimHint属性にのみアクセスを許可する。
- 自分だけが理解できるパスワードヒントを作成するようユーザに促す。パスワードポリシーの［パスワード変更メッセージ］は、これを実行する1つの方法です。詳細については、820 ページの 「パスワード変更メッセージの追加」を参照してください。

ヒントのセキュリティを確保する

セキュリティ保護されたヒント属性(nsimPasswordReminder)はパブリックに読み取り可能でないため、より安全です。この場合、ヒントが表示される前に、ユーザは秘密の質問に答える必要があります。

本人確認と回答の要件は、［パスワードポリシー］プロパティの［パスワードを忘れた場合］セクションで設定されます。

パスワードヒントを使用しないことを選択した場合は、どのパスワードポリシーでもそれを決して使用しないでください。

「パスワードを忘れた場合」の環境設定

［**Forgot your password?**］リンクをポータル(デフォルトではhttps://www.*servername*.com/nps)へのログイン時にクリックした場合、以下の条件が満たされない限り、そのユーザのリンクは機能しません。

- 管理者が［パスワードを忘れた場合］を有効にしてパスワードポリシーをすでにセットアップした。
- ［パスワードを忘れた場合］の設定で秘密の質問またはパスワードヒントのいずれかが指定されている場合、ユーザがすでに質問またはヒントをセットアップした。
- 813 ページの 「パスワード忘れ機能をセットアップするようユーザに促す」
- 814 ページの 「ユーザによるパスワード忘れ機能のセットアップ」
- 815 ページの 「既存のパスワードの準拠を要求する」

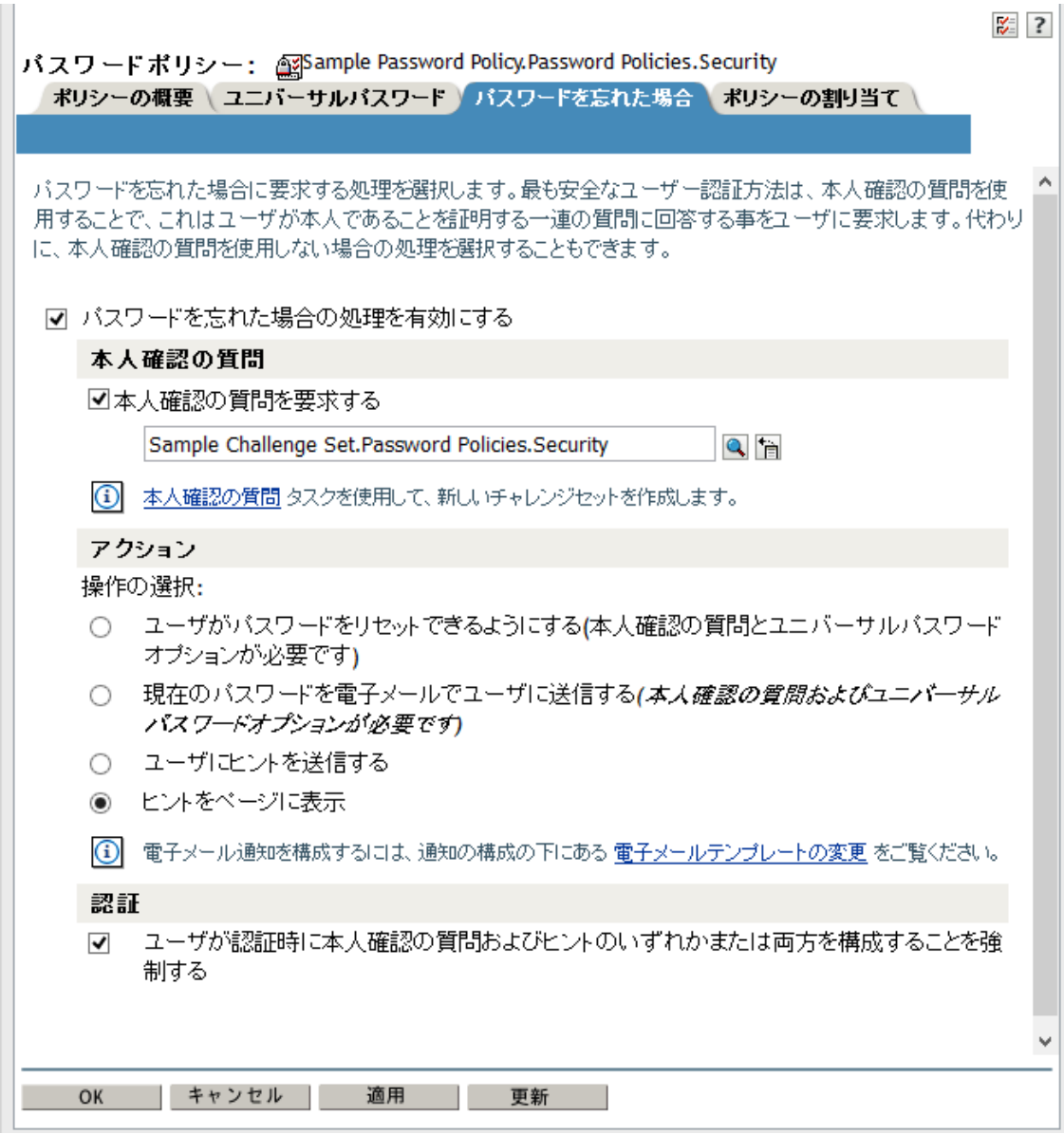
パスワード忘れ機能をセットアップするようユーザに促す

パスワード忘れ機能のアクションによっては、ユーザがパスワード忘れセルフサービスを使用する前に何らかのセットアップをする必要が生じます。たとえば、ユーザを識別するために秘密の質問を使用するようパスワードポリシーで指定されている場合、パスワードを忘れた場合のアクションが「ユーザにパスワードヒントを電子メールで送信する」であれば、まずユーザが秘密の質問に答えてパスワードヒントを作成した後で、パスワード忘れセルフサービスを使用できるようになります。

ユーザはこれらの機能のセットアップをポータルで自主的に開始できます。あるいは、認証後サービス(ポータルへのユーザログイン後に表示されるページ)を使ってユーザにセットアップを要求することもできます。

ログイン時にこれらの機能をセットアップするようユーザに求めるには、パスワードポリシーインタフェースの［パスワードを忘れた場合］ページの下部にある［**Force users to configure Challenge Questions and/or Hint upon authentication**］オプションを選択します。ポリシーを作成するとき、これがデフォルトで選択されます。

図 26-7 パスワードポリシー



ユーザに任意の時点でパスワード忘れ機能をセットアップさせるには、ポータルのURL (たとえばhttps://www.*my_iManager_server*.com/nps)をユーザに提供する必要があります。

ユーザによるパスワード忘れ機能のセットアップ

ユーザ側で設定する方法には、次の2つがあります。

- 814 ページの 「認証後」
- 815 ページの 「ポータル内で」

認証後

管理者は［**パスワードを忘れた場合**］オプションを選択して、ユーザのログイン成功後にパスワード忘れ機能をセットアップするようユーザに要求できます。これにより、認証後に秘密の質問またはヒントを設定するようユーザに強制します。このオプションを選択した場合、ユーザが質問または

ヒントをまだセットアップしていなければ、ユーザが次回にポータルからログインしたとき、パスワード忘れ機能設定ガジェットが表示されます(ポータルのデフォルトはhttps://www.*servername*.com/nps)。これを認証後セットアップといいます。

ポータル内で

ユーザがiManagerポータルからログインするとき、パスワード忘れセルフサービスの秘密の質問とパスワードヒントをセットアップまたは変更するためのガジェットにアクセスできます。これは、ユーザがパスワード変更操作を開始できる場所と同じです。ここから、次のガジェットにアクセスできます。

- ヒントのセットアップ
- 秘密の質問に答える
- (ユニバーサル)パスワードの変更

ユーザは、いつでもこれらの変更を開始できます。ただし、ユーザのパスワードポリシーでヒントや秘密の質問が必要とされない場合は、ユーザはこれらをセットアップできません。オプションを利用できないことを示すメッセージがページに表示されます。

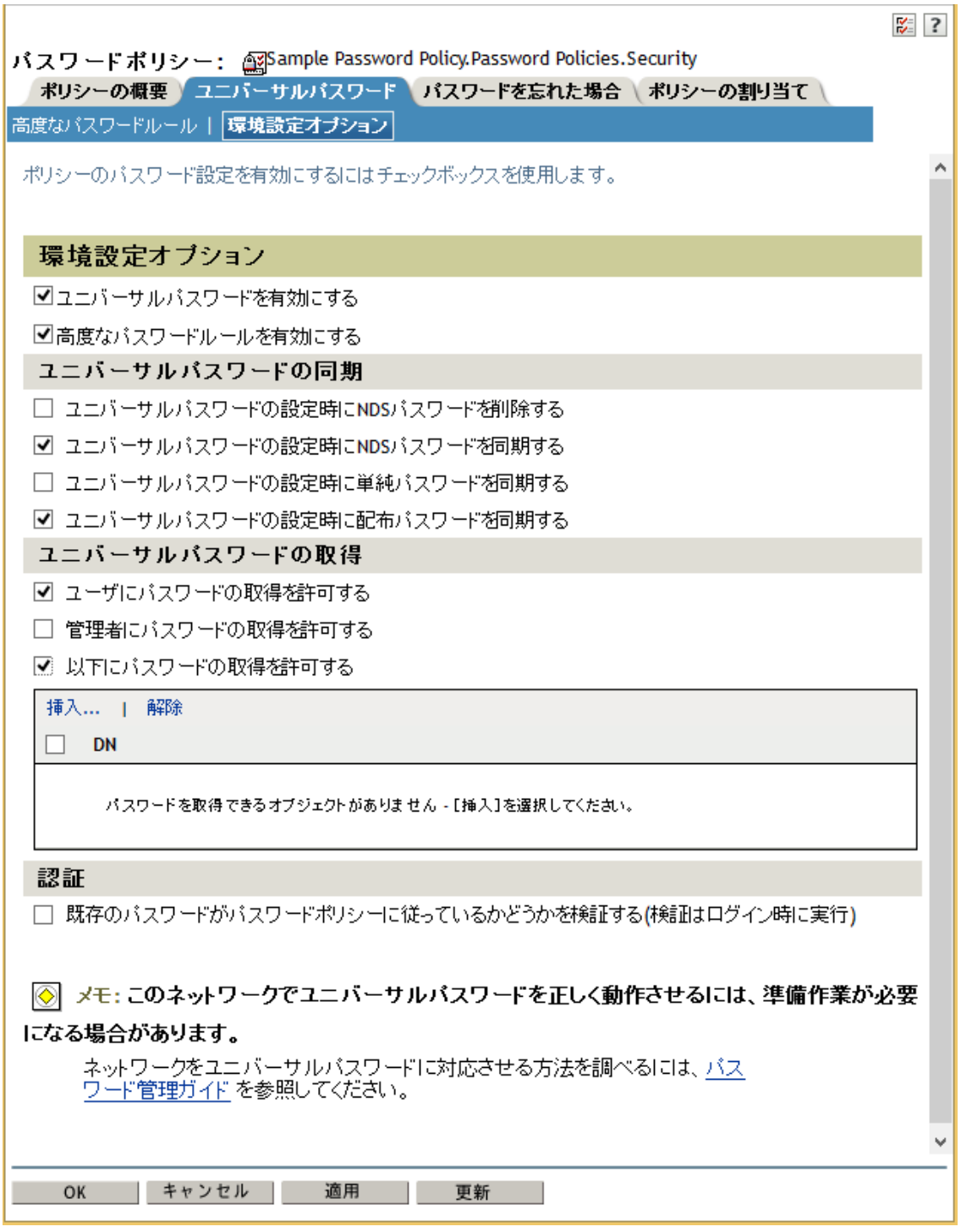
各アプリケーション(iManager 2.02以降、ユーザアプリケーションポートレット、Novell Client)でのこれらのユーザオプションの外観を示す例については、各アプリケーションのマニュアルを参照してください(806 ページの 「パスワードセルフサービスの概要」を参照)。

既存のパスワードの準拠を要求する

パスワードポリシーを作成または変更した場合、ユーザがポータルから次回ログインしたときに、準拠しない既存のパスワードを変更するようユーザに要求できます。

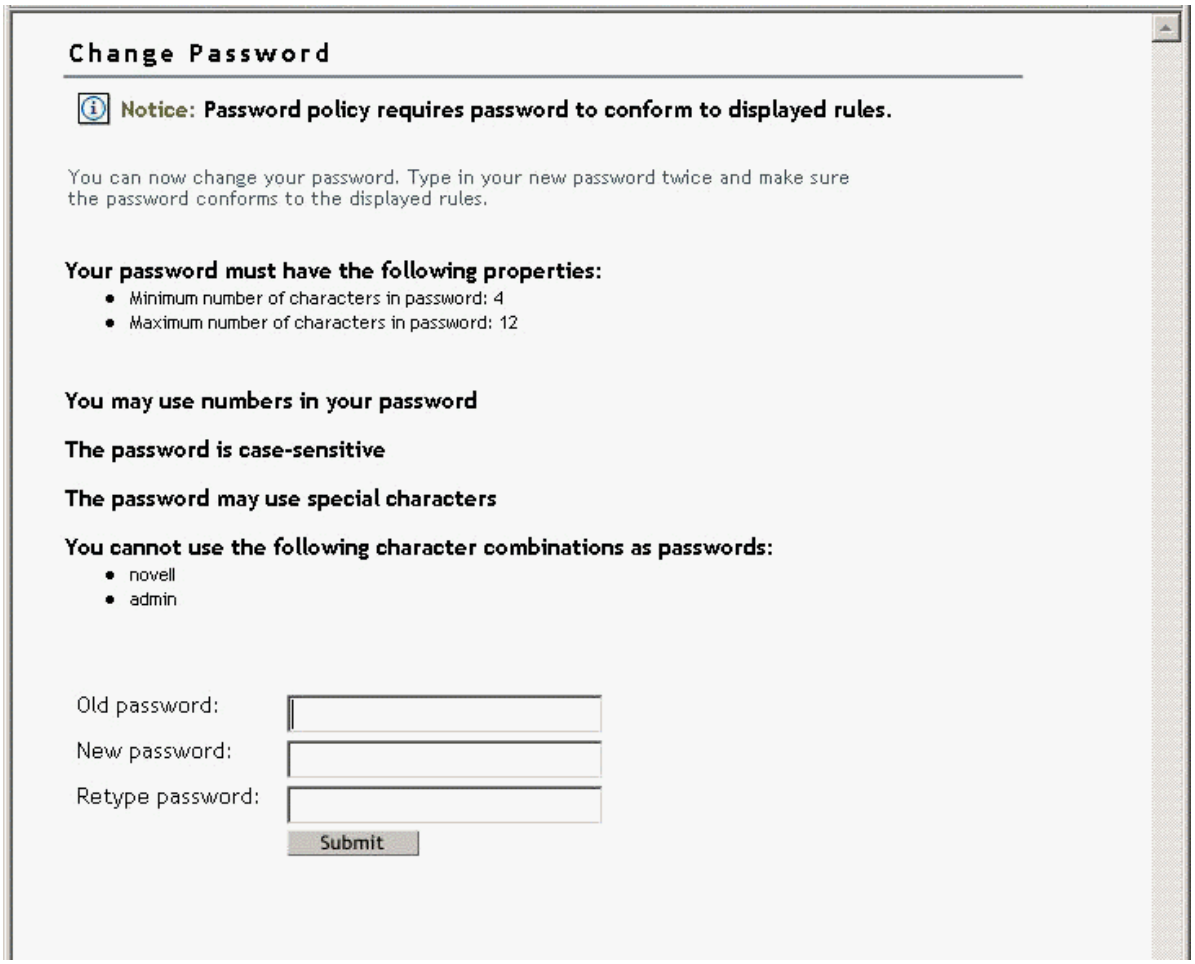
これを行うには、［**環境設定オプション**］の下の［**ユニバーサルパスワード**］タブを使用してパスワードポリシーのオプションを設定します。これは［**Verify whether existing passwords comply with the password policy (verification occurs on login)**］というオプションです。新しいパスワードポリシーを作成するとき、デフォルトでこのオプションは無効です。次の図は、このオプションを設定するページを示しています。

図26-8 既存のパスワードの準拠を要求する



このオプションを設定すると、ユーザが次回ポータルを介してログインしたとき、パスワードがパスワードポリシーに準拠しているかどうか検査されます。パスワードが準拠していない場合、次のようなページが表示され、ユーザはパスワードを変更しない限りログインを許可されません。

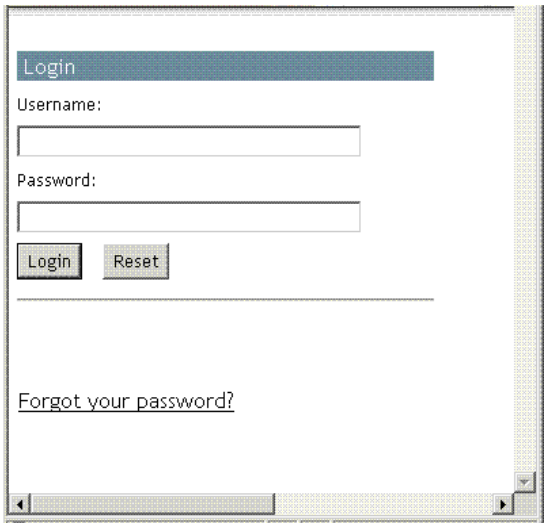
図 26-9 パスワードの変更



パスワードを忘れたときにユーザに表示される情報

Identity Managerに付属のiManagerプラグインをインストールした後、次の図のような［**パスワードを忘れた場合**］リンクがiManagerポータル(デフォルトではhttps://www.*servername*.com/nps)に表示されます。

図 26-10 iManager での［パスワードを忘れた場合］



Novell Clientで認証するときにも、同じようなリンクが表示されます。

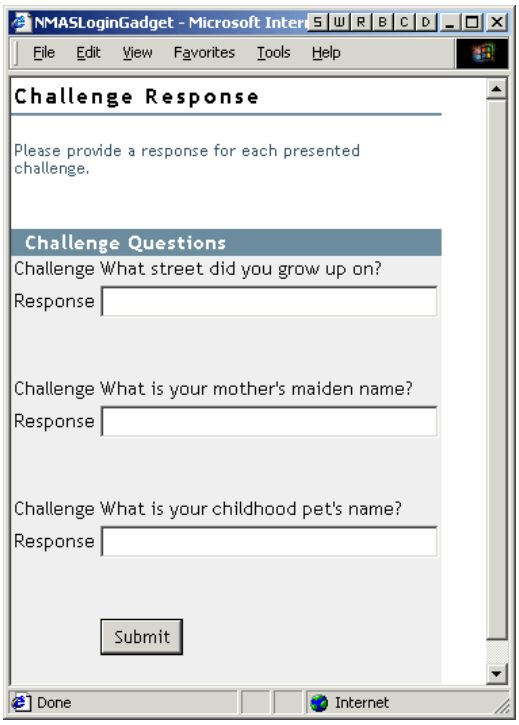
ユーザがこのリンクをクリックすると、次のページが表示され、ユーザ名の入力を求められます。

図 26-11 Virtual Office および Novell Client での［パスワードを忘れた場合］

ユーザ名を入力した後、パスワード忘れ機能の設定に応じて、ユーザに表示される内容が異なります。

たとえば、パスワードポリシーで秘密の質問を使用するよう管理者が指定した場合、次のようなページが表示されます。この場合、ユーザは秘密の質問に答えることで本人確認の情報を提供する必要があります。

図 26-12 パスワードを忘れた場合の秘密の質問



パスワードを忘れた場合のアクションとして［ヒントをページに表示］を管理者が指定した場合、次のようなページが表示されます。

図 26-13 パスワードを忘れた場合のヒント

パスワードを忘れた場合のアクションとして［E-mail Current Password to User］または［E-mail Hint to User］を管理者が指定した場合、パスワードまたはヒントが電子メールですでに送信されたことを示すメッセージが表示されます。

パスワードリセットセルフサービスをユーザに提供する

ユーザが自分のパスワードをリセットできるように、パスワードポリシーを設定することができます。このタスクがどのようにユーザに表示されるかは、ユーザが使用するアプリケーションによって異なります。さまざまなアプリケーションのマニュアルのリンクについては、806 ページの 「パスワードセルフサービスの概要」を参照してください。

パスワード変更メッセージの追加

ユーザは任意の時点で自分のパスワードを変更できますが、通常は、できるだけ長期にわたって同じパスワードを使用しようとします。セキュリティを強化するために、パスワードポリシーを使用してパスワードの変更を要求することができます。パスワード変更メッセージおよびパスワードルールをそのポリシーに含めることができます。ユーザがパスワードを変更するたびに、次のメッセージおよびルールがユーザに表示されます。

パスワードポリシーを編集してこのメッセージを作成するには、次の手順を実行します。

1. iManagerで、［**パスワード**］>［**パスワードポリシー**］の順にクリックします。
2. メッセージの追加先となるパスワードポリシーの名前をクリックします。
3. ［**Policy Summary**］>［**パスワード変更メッセージ**］をクリックします。
4. ユーザに対して表示するメッセージを入力して、［**OK**］をクリックします。

パスワードセルフサービスの電子メール通知の設定

iManagerの「通知の設定」という役割を使用すると、電子メールサーバを指定し、電子メール通知用のテンプレートをカスタマイズすることができます。

パスワード同期およびパスワードセルフサービスから自動化された電子メールをユーザに送信するために、電子メールのテンプレートが提供されています。

テンプレートは作成しません。代わりに、これらを使用するアプリケーションによって用意されています。電子メールテンプレートは、eDirectoryのテンプレートオブジェクトで、通常は、ツリーのルートにあるセキュリティコンテナに配置されています。これらはeDirectoryオブジェクトですが、iManagerインタフェースからのみ編集することをお勧めします。

これはモジュラフレームワークです。電子メールテンプレートを使用する新しいアプリケーションが追加された場合、テンプレートは、それを使用するアプリケーションとともにインストールできます。

Identity Managerには、パスワード同期およびパスワードを忘れた場合の通知用のテンプレートが用意されています。iManagerインタフェースでの選択に基づき、電子メールを送信するかどうかが制御されます。

パスワード忘れ機能では、パスワードを忘れた場合のアクションとして［E-mail Current Password to User］または［e-mail password hint to user］を選択した場合のみ、電子メール通知が送信されます。

このセクションでは、次の点について説明します。

- 821 ページの 「前提条件」
- 821 ページの 「電子メール通知を送信するためのSMTPサーバの設定」
- 821 ページの 「通知のための電子メールテンプレートの設定」

前提条件

- eDirectoryユーザがInternet EMail Address属性に入力済みであることを確認します。

電子メール通知を送信するためのSMTPサーバの設定

1. iManagerで、［**パスワード**］>［**Email Server Options**］の順にクリックします。
2. 次の情報を指定します。
   - ホスト名
   - 電子メールメッセージの［送信者］フィールドに表示する名前(たとえば「管理者」)
   - サーバに対して認証するためのユーザ名とパスワード(必要な場合)
3. **OK**をクリックします。
4. の説明に従い、電子メールテンプレートをカスタ\'83\'7dイズします。821 ページの 「通知のための電子メールテンプレートの設定」

メッセージを送信する機\'94\'5cを使用する場合は、電子メールサーバの設定後、電子メールテンプレートを使用するアプリケーションから電子メールメッセージを送信できます。

通知のための電子メールテンプレートの設定

これらのテンプレートは、独自のテキストでカスタマイズできます。テンプレートの名前は、使用目的を示します。電子メールテンプレートには言語サポートが備わっています。

1. iManagerで、［**パスワード**］>［**EditEmailTemplates**］の順にクリックします。テンプレートのリストが表示されます。
2. 必要に応じてテンプレートを編集します。

   置換タグを追加する場合は、追加の作業が必要となることがあります。

パスワードセルフサービスのテスト

機能が正しく設定されていることを確認するには、パスワードセルフサービスのテストの一部として、次を実行します。

1. 次の特徴を持つポリシーを作成します。これを行う方法については、809 ページの 「秘密の質問の作成または編集」を参照してください。
   - パスワードを忘れた場合の処理を有効にする
   - 秘密の質問を必要とする
   - このオプションを選択すると、ログイン時に秘密の質問の答えとヒントが設定されていることを確認します。
   - テストに使用できる少なくとも1人のユーザを含むコンテナにパスワードポリシーを割り当てます。このユーザは、ユーザオブジェクトの［インターネット電子メールアドレス］属性に電子メールアドレスが示されているユーザです。
2. パスワードポリシーが割り当てられていない、テストで使用できる別のユーザが存在することを確認します。

3 パスワードセルフサービスをテストするには、Identity Managerユーザアプリケーションを使用します。その方法については、『*NetIQ Identity Manager Roles Based Provisioning Module 4.5 User Application User Guide (NetIQ Identity Manager Roles Based Provisioning Module 4.5ユーザアプリケーションのユーザガイド)*』の「Using the Identity Self-Service Tab (［アイデンティティセルフサービス］タブを使用する)」を参照してください。

Windowsユーザの場合は、Novell Clientを使用してパスワードセルフサービスをテストします。その方法については、『*Novell Client for Windows Administration Guide (Novell Client for Windows管理ガイド)*』の「Using Forgotten Password Self-Service (パスワードを忘れた場合のセルフサービスを使用する)」を参照してください。

企業のポータルにパスワードセルフサービスを追加する

パスワードセルフサービスのセクションのほとんどの手順では、(パスワードセルフサービス機能をサポートする最後のiManagerバージョンである)iManager 2.0.2サーバ上でパスワードセルフサービス機能を使用することを想定しています。iManager 2.0.2より後のバージョンを使用している場合は、NetIQのユーザアプリケーションを介してのみ、パスワードセルフサービスを実行できます。NetIQのユーザアプリケーションを使ってパスワードセルフサービスを実行する方法について、詳しくは『*NetIQ Identity Manager Roles Based Provisioning Module 4.5 User Application User Guide (NetIQ Identity Manager Roles Based Provisioning Module 4.5ユーザアプリケーションのユーザガイド)*』の「Using the Identity Self-Service Tab (［アイデンティティセルフサービス］タブを使用する)」を参照してください。

iManager以外の製品を含むさまざまなポータル製品でパスワードセルフサービス機能を使用する方法については、次の表を参照してください。

ユーザがパスワード機能をすでに設定したことの確認

ユーザがiManagerポータル(https://*iManager_server_IP_address*/nps)にログインしたとき、次の条件が当てはまる場合には、いくつかの認証後ページで操作を実行するよう促されます。

- ユーザのパスワードがパスワードポリシーの高度なパスワードルールに準拠していない
- パスワード忘れセルフサービスの使用時に秘密の質問を必要とするようパスワードポリシーで指定されているが、ユーザがこれらの質問をまだ設定していない
- パスワードを忘れた場合のアクションとしてパスワードヒントを表示するようパスワードポリシーで指定されているが、ユーザがヒントをまだ設定していない

たとえば、ユーザがパスワード忘れセルフサービスを確実に使用できるようにするには、これらのプロンプトが必要です。ユーザが秘密の質問に答えるようパスワードポリシーで指定されているが、ユーザが最初にそれらを設定していない場合、ユーザはパスワード忘れセルフサービスにアクセスできません。ユーザがまだパスワードヒントを作成していない場合、ユーザはパスワードを思い出すためのヒントを取得することができません。

他のポータルの製品では認証後機能が自動的に提供されないため、ユーザはiManagerポータルに少なくとも1回ログインし、準拠するパスワードを作成してパスワード管理セットアップを完了する必要があります。さらに、パスワードポリシーを変更したときにも必ずこの操作を再び行う必要があります。

パスワードセルフサービスのトラブルシューティング

- 秘密の質問の答えを使用するには、iManager 2.02でサポートされるブラウザを必ず使用してください。
- SSLを正しくセットアップしていない場合、iManagerやポータルにはログインできません。iManagerに正常にログインでき、単純認証用にTLSを要求している場合には、SSLが正しくセットアップされています。したがってパスワードセルフサービスのトラブルシューティング時にSSL関連の問題の可能性を排除できます。

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を区別させることができます。

- Novell Client 4.9以降
- eDirectory 9.0にアップグレードした管理ユーティリティ以降
- NetIQ iManager 3.0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LDAPSDK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。

- 823 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」
- 824 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」
- 825 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」
- 826 ページの 「その他の情報」

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では、eDirectory 9.0以降にアップグレードされたすべてのクライアントで、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 サーバにアクセスするのを防止できます。

パスワードの大文字と小文字が区別されるようにする方法

eDirectory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でパスワードの大文字と小文字を区別することができます。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、NMAS (NetIQモジュラー認証サービス)を介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。eDirectoryでは、NMASログインがデフォルトで有効になっています。NMASログインを無効にするには、NDSD_TRY_NMASLOGIN_FIRSTをfalseに設定します。

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。

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 9.2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、775 ページの 「ユニバーサルパスワードの導入」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、「825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

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、775 ページの 「ユニバーサルパスワードの導入」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NetIQユーティリティを次に示します。

- Novell Client 4.9
- eDirectory 9.2に付属の管理ユーティリティ
- NetIQ iManager 3.2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を最新バージョンにアップグレードした後、大文字小文字を区別するパスワードをそれらのクライアントで使用できるようになります。eDirectoryでは、既存のパスワードから大文字小文字を区別するパスワードへの移行を簡単かつ柔軟に行うことができます。詳細については、825 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 9.2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。

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、「824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。詳細については、775 ページの 「ユニバーサルパスワードの導入」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「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。

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、iManagerオンラインヘルプを参照してください。

セキュリティ上の考慮事項

他のパスワードシステムとの相互運用を容易にするには、復号可能なユニバーサルパスワード暗号化が必要です。管理者は、システムのコストと利点を評価する必要があります。複数のパスワードを管理しようとするよりも、eDirectoryに保存されたユニバーサルパスワードを使用する方が安全(または便利)である可能性があります。

eDirectory内のユニバーサルパスワードは、パスワード自体のトリプルDES暗号化、eDirectory権限、およびファイルシステム権限の3つのセキュリティレベルで保護されます。

- NICI3.0より前では、ユニバーサルパスワードはトリプルDES、ユーザ固有の鍵で暗号化されました。eDirectoryだけが読み込むことのできるシステム属性に、ユニバーサルパスワードとユーザ鍵の両方が格納されていました。ユーザ鍵(3DES)はツリー鍵で暗号化されて格納され、ツリー鍵は各マシンで固有のNICI鍵によって保護されていました。ツリー鍵とNICI鍵のどちらもeDirectoryの中に保管されなかったことに注意してください。これらは、保護対象のデータと共に保管されませんでした。ツリー鍵はツリー内の各マシンに存在していましたが、ツリーごとにツリー鍵が異なっていたため、ツリー鍵で暗号化されたデータは同じツリー内のマシンでのみ復号可能でした。こうして、ユニバーサルパスワードが保管されるときには3つのレベルの暗号化で保護されていました。

  NICI 3.0はAES 256ビットストレージ鍵をサポートしています。したがって、他の鍵を安全にラップするためにストレージ鍵を使用するアプリケーションは、新しいアルゴリズムを処理できる必要があります。しかし、古い3-DES鍵を使って現在ラップされているデータは、変更なしで引き続きアクセス可能になります。

  NICI 3.0はAES 256ビットツリー鍵をサポートします。しかし、eDirectoryはデフォルトでAES 256ビットツリー鍵を作成しません。バージョン9.0以前の環境でこの鍵を作成すると、ツリー鍵に依存するサービスで問題が発生する可能性があります。キーを作成する前に、すべてのeDirectoryサーバを9.2に更新することをお勧めします。詳細については、「Creating an AES 256-Bit Tree Key (AES 256ビットツリーキーを作成する)」を参照してください。
- それぞれの鍵は、eDirectoryの権利によっても保護されます。ユニバーサルパスワードを変更する権利を持つのは、スーパバイザ権を持つ管理者、またはその鍵を所有するユーザだけです。

注: NMAS/nds-cluster-config拡張機能を使用して、ユーザが自分のパスワードを読み取ったり管理者がユニバーサルパスワードを読み取ったりできるように、パスワードポリシーを設定することができます。デフォルトではこれが有効になっていません。

- ファイルシステム権限は、適切な権限を持つユーザのみが鍵にアクセスできるようにします。

  高度なセキュリティを必要とする環境でユニバーサルパスワードを導入する場合は、次のような追加の対策を実行できます。
  - 次のディレクトリとファイルがセキュリティで保護されていることを確認します。

Windows	%SystemRoot%\SysWOW64\Novell\nici %SystemRoot%\System32\(NICIDLLのインストール先)
Linux	/var/opt/novell/nici /etc/opt/novell/nici64.cfg /opt/novell/lib64/libccs2.so、および同じディレクトリ内のNICI共有ライブラリ

NICIおよびeDirectoryのファイルの具体的な場所について詳しくは、ご使用のシステムのマニュアルを参照してください。

- 他のセキュリティシステムの場合と同様に、鍵が保管されているサーバへの物理的アクセスを制限することは非常に重要です。

パスワード管理に関連するセキュリティ上の考慮事項については、690 ページの 「セキュリティ上の考慮事項」を参照してください。

eDirectoryへのハッシュベースのパスワードのインポート

パスワードは、DIGEST-MD5、crypt、SHA、SSHAハッシュのLDIFによってeDirectoryにインポートできます。MD5ハッシュベースのパスワードをeDirectoryにインポートするには、次の手順を実行します。

1 次のコマンドを使用して、MD5ハッシュをbase64形式で作成します。

```
echo -n <password> | openssl md5 -binary | base64
```

注: eDirectoryがサポートするハッシュベースのパスワードはbase64形式のパスワードのみです。

2 次の例に示されているように、MD5ハッシュの作成時に返されるテキストをLDIFファイルに追加します。

```
dn: cn=sp1,o=novell
control: 2.16.840.1.113719.1.27.101.5
changetype: modify
replace: userPassword
userPassword: {md5}CSbJUP4kfDtGXrE+JY7kaNI5oGU=
```

注: LDIFファイルで変更される、ユーザに適用されているパスワードポリシーがないことを確認します。

3 次の変数をpre_ndsd_startスクリプトに追加し、eDirectoryを再起動します。デフォルトでは、このスクリプトは/opt/novell/eDirectory/sbinにあります。

```
NDSD_TRY_NMASLOGIN_FIRST=true
export NDSD_TRY_NMASLOGIN_FIRST
```

4 単純パスワードメソッドとDIGESTMD5NMASメソッドの両方をインストールし、単純パスワードをデフォルトのメソッドにします。

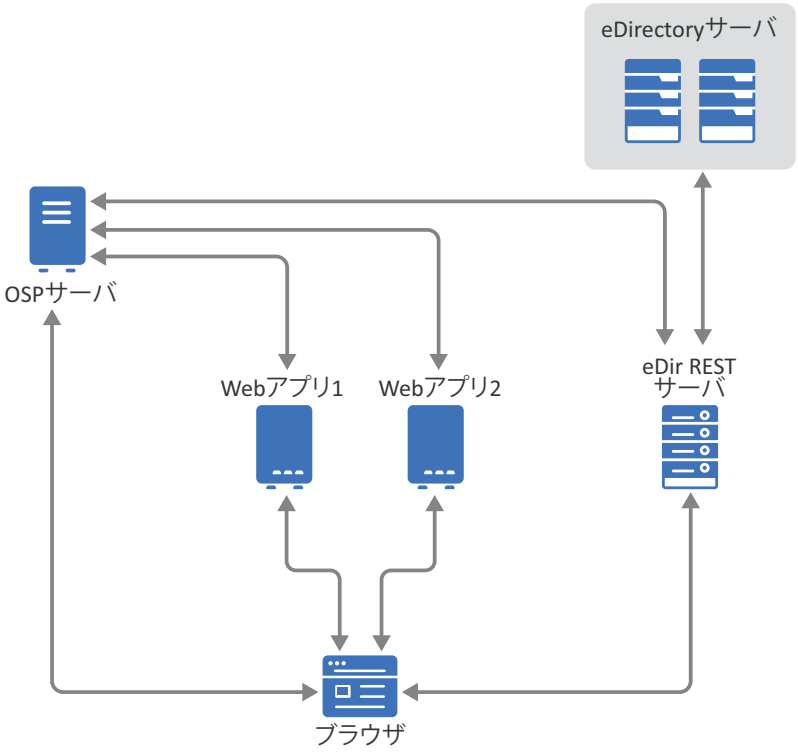
5 次のコマンドを使用して、-lオプション(LDAPターゲットハンドラを表す)を指定してiceを使用します。

```
ice -S LDIF -f ./change_pass.ldiff -D LDAP -s 164.99.163.236 -p 636 -d
cn=admin,o=novell -w n -l -L /var/opt/novell/eDirectory/data/SSCert.der
```

27 RESTサービス

eDirectoryには、REST Webサービスを使用してeDirectoryのさまざまな機能を利用するためのREST APIがいくつか組み込まれています。APIを使用すると、任意の要求を呼び出してeDirectoryサーバからそれぞれの応答を得ることができます。RESTWebサービスは、Dockerコンテナとしてデプロイできます。詳細については次の図を参照してください。これらの図は、eDirectoryでのREST Webサービスのアーキテクチャを示しています。

図 27-1 eDirectory でのREST Web サービスのアーキテクチャ



注: eDirectoryのRESTサービスは、OAUTH2プロトコルを使用して、OneSSOProvider(OSP)による認証を提供します。

このドキュメントでは、次のタスクを実行する方法について説明します。

- 830 ページの 「eDirectory向けのRESTサービスのインストールを計画する」
- 832 ページの 「eDirectoryでのRESTサービスの設定」
- 834 ページの 「データ永続性の管理」
- 834 ページの 「RESTサービスによる監査」
- 835 ページの 「RESTコンテナを使用してLDAPパスワードを変更する」
- 836 ページの 「RESTコンテナを使用してサーバ証明書を変更する」

eDirectory向けのRESTサービスのインストールを計画する

このセクションでは、RESTサービスをインストールする前のセットアップの準備について説明します。RESTをインストールおよび設定するには、次のタスクを実行する必要があります。

- サーバ証明書を.pfx形式で取得してください。外部認証局またはiManagerが生成したサーバ証明書を使用できます。たとえば、iManagerを使用してkeys.pfxのサーバ証明書を生成できます。詳細については、709 ページの 「サーバ証明書オブジェクトを作成する」を参照してください。
- 認証局証明書ファイルを.pem形式で取得してください。たとえば、eDirectory認証局証明書(SSCert.pem)を使用できます。
- (省略可能)RESTサービスをインストールする前に、OSPをインストールして設定します。詳細については、「Creating OSP Container」を参照してください。
- 次の環境設定パラメータを使用して、環境設定ファイルを作成します。たとえば、edirapi.confファイルを作成します。環境設定ファイルの値は、要件に応じて変更できます。

```
listen = ":9000"
ldapserver = "192.168.1.1:636"
ldapuser = "cn=admin,o=novell"
pfxpassword = "novell"
ldappassword = "novell"
osp-token-endpoint = "https://10.10.10.10:8543/osp/a/idm/auth/oauth2/
getattributes"
osp-authorize-url = "https://10.10.10.10:8543/osp/a/idm/auth/oauth2/grant"
osp-logout-url = "http://10.10.10.10:8543/osp/a/idm/auth/app/logout"
osp-redirect-url = "https://10.10.10.10:9000/eDirAPI/v1/edirtree/
authcoderedirect"
osp-client-id = "edirapi"
ospclientpass = "novell"
ospcert = "/etc/opt/novell/eDirAPI/conf/ssl/trustedcert/SSCert.pem"
bcert = "/etc/opt/novell/eDirAPI/conf/ssl/trustedcert/SSCert.pem"
loglevel = "error"
check-origin = "true"
origin = "https://10.10.10.10:9000,https://192.168.1.1:9000"
enableaudit = "true"
enableservicestartaudit = "true"
enableservicestopaudit = "true"
enablelogsessioncreationaudit = "true"
enablelogsessionterminationaudit = "true"
auditlogmaxsize = "50 MB"
edirapilogmaxsize = "50 MB"
scope = "ism"
```

表 27-1 環境設定ファイル内の環境設定パラメータの説明

環境設定パラメータ	説明
listen	コンテナ内のRESTサーバの待ち受けポートとして9000を指定します。
ldapserver	eDirectoryホストサーバのIPを指定します

環境設定パラメータ	説明
ldapuser	eDirectoryツリーの管理者権限を持つユーザのユーザ名を指定します
pfxpassword	.pfx証明書ファイルのパスワードを指定します
ldappassword	LDAPサーバのパスワードを指定します
osp-token-endpoint	このURLは、OSPサーバから特定の属性をフェッチして、認証トークンの有効性を検証するために使用します
osp-authorize-url	このURLは、ユーザが認証トークンを取得するために資格情報を提供する際に使用します
osp-logout-url	このURLを使用して、ユーザとOSPサーバ間のセッションを終了します
osp-redirect-url	OSPサーバは、認証トークンを付与した後、ユーザをこのURLにリダイレクトします
osp-client-id	Identity ConsoleをOSPに登録したときに提供されたOSPクライアントIDを指定します
ospclientpass	Identity ConsoleをOSPに登録したときに提供されたOSPクライアントパスワードを指定します
ospcert	OSPサーバの認証局証明書の場所を指定します
bcert	RESTサーバの認証局証明書の場所を指定します
loglevel	ログファイルに含めたいレベルのみを指定します。Debug、Error、Panicなど。
check-origin	これがtrueに設定されている場合、Identity Consoleサーバは、要求のオリジン値を比較します。使用可能なオプションは、trueまたはfalseのいずれかです。
origin	check-originがtrueに設定されている場合、Identity Consoleは要求のオリジン値をこのフィールドに指定された値と比較します。
enableaudit	RESTサービスの監査を有効にするには、このオプションをtrueに設定します。使用可能なオプションは、trueまたはfalseのいずれかです。
enableservicestartaudit	このオプションをtrueに設定すると、RESTサービスの開始イベントが通知されます。使用可能なオプションは、trueまたはfalseのいずれかです。
enableservicestopaudit	このオプションをtrueに設定すると、RESTサービスの停止イベントが通知されます。使用可能なオプションは、trueまたはfalseのいずれかです。
enablelogsessioncreationaudit	このオプションをtrueに設定すると、RESTサービスのセッション作成イベントが通知されます。使用可能なオプションは、trueまたはfalseのいずれかです。

環境設定パラメータ	説明
enablelogsessionterminationaudit	このオプションをtrueに設定すると、RESTサービスのセッション終了イベントが通知されます。使用可能なオプションは、trueまたはfalseのいずれかです。
auditlogmaxsize	それぞれのRESTサービスの監査ログファイルサイズの最大限度を指定します。デフォルトでは、ファイルサイズは50MBです。
edirapilogmaxsize	それぞれのRESTサーバのログファイルサイズの最大限度を指定します。
scope	RESTサーバがOAuth用語で言うところのリソースサーバとして使用されている場合は、そのスコープを指定します。デフォルトでは、edirapi <*tree_name*> に設定されています。

重要

- OSP関連の環境設定パラメータは、OSPとRESTサービスを統合する計画の場合にのみ使用してください。
- RESTサービスの監査を有効にするには、環境設定ファイルに監査関連パラメータを設定する必要があります。
- OSPはHTTPSのCRLは、2048ビットキーが含まれている証明書を使用して検証する必要があります。この検証は、4096または8192ビットキーが含まれている証明書では失敗します。

eDirectoryでのRESTサービスの設定

eDirectory向けのREST APIを設定するには、次の手順を実行します。

1. 次のコマンドを使用して、Dockerイメージをtarballからローカルの Dockerレジストリにロードします。

   ```
   docker load --input <tarball of the image>
   ```

   次に例を示します。

   ```
   docker load --input edirapi.tar.gz
   ```

2. 次のコマンドを使用して、Dockerコンテナを作成します。

   ```
   docker create --name edirapi-container -v <volune name> –p <host port>:9000 -e
   ACCEPT_EULA=Y edirapi:<version>
   ```

   次に例を示します。

   ```
   docker create --name edirapi-container -v my-volume-1 –p 9000:9000 -e
   ACCEPT_EULA=Y edirapi:1.0.0
   ```

   注: ACCEPT_EULA環境変数をYに設定することによって、EULAに同意することができます。対話型モードのDocker createコマンドで-itオプションを使用することにより、コンテナの起動中に画面のプロンプトからEULAに同意することもできます。

3 次のコマンドを使用して、ローカルファイルシステムからコンテナの/etc/opt/novell/eDirAPI/cert/keys.pfxに、サーバ証明書ファイル(.pfx)をコピーします。

```
docker cp <absolute path of server certificate file> edirapi-container:/etc/opt/novell/eDirAPI/cert/keys.pfx
```

次に例を示します。

```
docker cp /home/user/keys.pfx edirapi-container:/etc/opt/novell/eDirAPI/cert/keys.pfx
```

4 次のコマンドを使用して、ローカルファイルシステムからコンテナの/etc/opt/novell/eDirAPI/cert/SSCert.pemに、認証局証明書ファイル(.pem)をコピーします。

```
docker cp <absolute path of CA certificate file> edirapi-container:/etc/opt/novell/eDirAPI/cert/SSCert.pem
```

次に例を示します。

```
docker cp /home/user/SSCert.pem edirapi-container:/etc/opt/novell/eDirAPI/cert/SSCert.pem
```

5 次のコマンドを使用して、ローカルファイルシステムからコンテナの/etc/opt/novell/eDirAPI/conf/edirapi.confに、環境設定ファイル(edirapi.conf)をコピーします。

```
docker cp <absolute path of CA certificate file> edirapi-container:/etc/opt/novell/eDirAPI/conf/edirapi.conf
```

次に例を示します。

```
docker cp /home/user/edirapi.conf edirapi-container:/etc/opt/novell/eDirAPI/conf/edirapi.conf
```

6 次のコマンドで、Dockerコンテナを起動します。

```
docker start -i edirapi-container
```

7 (省略可能)次のスクリプトを実行することにより、RESTコンテナのインストールと設定を行うこともできます(手順2から手順6までスキップします)。

```
configure-edirapi --sscert-file <absolute path of CA certificate file> --conf-file <absolute path of configuration file> --pfx-file <absolute path of server certificate file> --name edirapi-container –p <hosts port>:9000 -v <name of the volume> edirapi:<version>
```

次に例を示します。

```
configure-edirapi --sscert-file my-SSCert.pem --conf-file my-edirapi.conf --pfx-file my-keys.pfx –-name edirapi-container –p 9000:9000 –v myvolume:/config edirapi:1.0.0
```

注

- RESTサーバの認証局証明書は、BEGIN CERTIFICATEで始まり、END CERTIFICATEで終わる必要があります。それ以外の値を指定した場合は、RESTサーバはエラーメッセージを表示します。

- RESTコンテナ内で最大42000の接続をサポートするには、次の3つのコマンドを実行して、ポートの範囲を拡大する必要があります。

```
ulimit -n 999999
cat /proc/sys/net/ipv4/ip_local_port_range
echo 1024 65535 > /proc/sys/net/ipv4/ip_local_port_range
```

データ永続性の管理

RESTコンテナとともに、データ永続性のためのボリュームも作成されます。ボリュームを使用して古いコンテナの環境設定パラメータを使用するには、次の手順を実行します。

1. (省略可能)次のコマンドを使用して、現在のDockerコンテナを停止します。

   ```
   docker stop edirapi-container
   ```

2. 次のコマンドを使用して、2番目のコンテナを作成します。

   ```
   docker create --name container-2 –p 9000:9000 -v my-volume-1:/config
   edirapi:1.0.0
   ```

3. 次のコマンドを使用して、2番目のコンテナを開始します。

   ```
   docker start container-2
   ```

4. (省略可能)これで、次のコマンドを使用して最初のコンテナを削除できるようになりました。

   ```
   docker rm edirapi-container
   ```

RESTサービスによる監査

eDirectory RESTサーバは、SentinelサーバにCEF監査イベントログを送信することができます。RESTサーバは、ArcSight Smart Connectorを使用して監査データを送信します。SmartConnectorの設定と使用方法の詳細については、『ArcSight SmartConnector ユーザガイド』を参照してください。

RESTサービスの監査を有効にするには、環境設定ファイル内の監査関連パラメータを設定する必要があります。詳細については、830 ページの 「eDirectory向けのRESTサービスのインストールを計画する」を参照してください。

RESTイベントを理解する

デフォルトでは、すべてのRESTイベントが有効になっています。ユーザの組織で不要な場合は、特定のイベントを無効にすることができます。eDirectory RESTサーバでは、次のイベントの監査が可能です。

イベント	説明
ENABLESERVICESTARTAUDIT	RESTサービスが開始された場合にイベントが生成されます
ENABLESERVICESTOPAUDIT	RESTサービスが停止した場合にイベントが生成されます

イベント	説明
ENABLELOGSESSIONCREATIONAUDIT	RESTセッションが作成された場合にイベントが生成されます
ENABLELOGSESSIONTERMINATIONAUDIT	RESTセッションが終了した場合にイベントが生成されます

注: ログは/var/opt/novell/eDirAPI/log/edirapi_auditlog.logにあります。

例

次のセッションの作成イベントの例を参照してください。

```
Oct 10 15:37:17 eDirAPI
CEF:0|NetIQ|eDirAPI|1.0|000B0510|SESSION_CREATE|3|dvc=10.71.128.233
dvchost=SLES12SP3-SHREYAS-128233 rt=Oct 10 2019 15:37:17 dtz=IST src=164.99.136.60
spt=59132 suser=cn\=admin,o\=novell duser=cn\=admin,o\=novell
cn1Label=CorrelationID cn1=rtpL9xt-tzBR92fEGt9rrczA_1M2vHrGM4Q_8AjEmSU=
cs1Label=Client Address cs1=164.99.136.60 cs2Label=Tree Name cs2=SHREYAS_TREE2
sproc=eDirAPI sourceServiceName=edirapi reason=201 outcome=Success
```

RESTコンテナを使用してLDAPパスワードを変更する

RESTコンテナを使用してLDAPパスワードを変更するには、次の手順を実行します。

1. 次のコマンドを使用して、コンテナにログインします。

   ```
   docker exec -it <container_name> bash
   ```

2. 次のコマンドを使用して、パスワードストアに新しいパスワードを保存します。

   ```
   LD_LIBRARY_PATH=/opt/novell/lib64/:/opt/novell/eDirectory/lib64/:/opt/netiq/
   common/openssl/lib64/ /opt/novell/eDirAPI/sbin/passwdstore -a <Admin DN>
   ```

   上記のコマンドを使用すると、パスワードを求めるプロンプトが表示されます。新しいパスワードを入力します。

   次に例を示します。

   ```
   LD_LIBRARY_PATH=/opt/novell/lib64/:/opt/novell/eDirectory/lib64/:/opt/netiq/
   common/openssl/lib64/ /opt/novell/eDirAPI/sbin/passwdstore -a admin.novell
   ```

3. 次のコマンドを使用して、コンテナコンソールを終了します。

   ```
   exit
   ```

4. コンテナを再起動します

   ```
   docker restart <container name>
   ```

RESTコンテナを使用してサーバ証明書を変更する

RESTコンテナを使用してサーバ証明書を変更するには、次の手順を実行します。

1. 次のコマンドを実行して、コンテナの任意の場所に新しいサーバ証明書(例: new-keys.pfx)をコピーします。

   ```
   docker cp /path/to/new-keys.pfx <container_id/name>:/tmp/new-keys.pfx
   ```

2. 次のコマンドを使用して、コンテナにログインします。

   ```
   docker exec -it <container_name> bash
   ```

3. NLPCERTを実行して、キーを保存します。

   ```
   LD_LIBRARY_PATH=/opt/novell/lib64/:/opt/novell/eDirectory/lib64/:/opt/netiq/
   common/openssl/lib64/ /opt/novell/eDirAPI/sbin/nlpcert -i /tmp/new-keys.pfx -o
   /etc/opt/novell/eDirAPI/conf/ssl/private/cert.pem
   ```

   上記のコマンドを使用すると、サーバ証明書のパスワード入力を求めるプロンプトも表示されます。パスワードを入力します。

4. 次のコマンドを使用して、コンテナコンソールを終了します。

   ```
   exit
   ```

5. コンテナを再起動します

   ```
   docker restart <container name>
   ```

A NMASの注意事項

この付録では、次のトピックについて説明します。

独立したパーティションとしてのセキュリティコンテナの設定

NMAS (NetIQモジュラー認証サービス)は、NetIQ eDirectoryツリー全体に適用されるポリシーに依存しています。eDirectoryツリーは、実際にはセキュリティドメインとして機能します。セキュリティポリシーは、ツリー内のすべてのサーバで使用できる必要があります。

NMASには、eDirectoryツリーの［ルート］から作成された、セキュリティコンテナ内の認証ポリシーとログイン方式の設定データが格納されます。この情報は、NMASを使用可能なすべてのサーバで読み込みアクセスできる必要があります。セキュリティコンテナの目的は、ログイン、認証、キー管理などのセキュリティプロパティに関するグローバルポリシーを保持することです。

NMASにより、独立したパーティションとしてセキュリティコンテナを作成し、作成したコンテナを広い範囲で複製することを推奨します。このパーティションは、ツリー内の信頼性の高い複数のサーバでのみ、読み書き可能なパーティションとして複製することをお勧めします。

注: セキュリティコンテナはグローバルポリシーを格納しており、サーバではeDirectoryツリーに指定したセキュリティポリシー全般が変更される可能性があるため、書き込み可能なレプリカを配置するサーバを選択する場合には注意が必要です。NMASを使用してユーザがログインするには、ユーザオブジェクトのレプリカがNMASサーバ上に存在する必要があります。

複数のセキュリティコンテナを持つツリーのマージ

一方のツリーまたは両方のツリーにセキュリティコンテナがインストールされているeDirectoryツリーをマージする場合、特に注意が必要です。この手順は時間を要する複雑な作業になる可能性があるため、本当に実行する必要があるかどうか確認してください。

複数のセキュリティコンテナを持つツリーをマージするには次を実行します。

1. iManagerで、マージするツリーを指定します。
2. ソースツリーにするツリーと、ターゲットツリーにするツリーを指定します。

   ソースツリーおよびターゲットツリーについて、次のセキュリティ上の配慮事項に注意してください。

   - ソースツリーの組織の認証局によって署名された証明書をすべて削除すること。
   - ソースツリーの組織の認証局を削除すること。
   - ソースツリー上のNetIQ SecretStoreに保存されたすべてのユーザシークレットを削除すること。

- ソースツリー内のすべてのNMASログインメソッドを削除し、ターゲットツリーに再インストールすること。
- ツリーをマージする際に、ソースツリー内に存在したすべてのNMASユーザを再登録すること。
- ソースツリー内に存在したすべてのユーザおよびサーバに、ツリーをマージする際に新しい証明書を作成すること。
- ソースツリー内に存在したすべてのユーザのシークレットをSecretStoreに再インストールすること。

ソースツリーおよびターゲットツリーの両方がSecurityというコンテナをツリーのルート直下に保持していない場合、またはツリーのうち一方だけがSecurityコンテナを保持している場合、これ以上の処置は不要です。その他の場合には、このセクションの残りの手順を続けます。

注: EBAが有効なサーバが含まれる2つのeDirectoryツリーをマージしないでください。

ツリーのマージ前に実行する製品固有の操作

このセクションでは、次のことを説明します。

NetIQ Certificate Server

製品の使用状況によっては、指定されたオブジェクトと項目が存在しない可能性があります。次の手順で指定されたオブジェクトや項目がソースツリーに存在しない場合には、手順を省略できます。

1 ソースツリー内のルート認証局証明書は、ターゲットツリーにインストールする必要があります。

ルート認証局証明書は、ルート認証局コンテナに含まれる、ルート認証局オブジェクトに格納されています。ルート認証局コンテナはツリー内の任意の場所に作成できます。ただし、セキュリティコンテナ内のルート認証局コンテナに存在するルート認証局証明書は、ソースツリーからターゲットツリーに手動で移動する必要があります。

2 ターゲットツリーにルート認証局証明書をインストールします。

2a ソースツリーのセキュリティコンテナでルート認証局を選択します。

2b ソースツリーで使用されている正確な名前(ステップ 2a)で、ルート認証局コンテナをターゲットツリーのセキュリティコンテナに作成します。

2c ソースツリーで、選択したルート認証局コンテナのルート認証局オブジェクトを開き、証明書をエクスポートします。

重要: 選択した場所とファイル名は、次の手順で使用するため覚えておいてください。

2d ターゲットツリーで、ステップ 2bで作成したコンテナのルート認証局オブジェクトを作成します。ソースツリーと同じ名前を指定し、証明書を求められたら、ステップ 2cで作成したファイルを指定します。

2e ソースツリーのルート認証局オブジェクトを削除します。

2f 選択したルート認証局コンテナ内のすべてのルート認証局オブジェクトがターゲットツリーにインストールされるまで、ステップ 2cからステップ 2eを繰り返します。

2g ソースツリーのルート認証局コンテナを削除します。

2h すべてのルート認証局コンテナがソースツリー内で削除されるまで、ステップ 2aからステップ 2fを繰り返します。

3 ソースツリーの組織の認証局を削除します。

組織の認証局オブジェクトは、セキュリティコンテナ内に存在します。

重要: ソースツリーの組織の認証局によって署名された証明書は、この手順以降は使用できません。これには、ソースツリーの組織の認証局によって署名された、サーバ証明書とユーザ証明書も含まれます。

---

4 ソースツリーの組織の認証局によって署名された証明書を持つ、ソースツリー内の暗号化キーオブジェクト(KMO)をすべて削除します。

他の組織の認証局によって署名された証明書を持つ、ソースツリー内の暗号化キーオブジェクトは引き続き有効で、削除する必要はありません。

暗号化オブジェクトに署名しているCAの識別情報がわからない場合は、暗号化オブジェクトのプロパティページにある［証明書］タブの［ルート認証局証明書］セクションを参照します。

5 ソースツリーの組織の認証局によって署名された、ソースツリー内のユーザ証明書をすべて削除します。

ソースツリー内のユーザがすでに証明書とプライベートキーをエクスポートしている場合、エクスポートされた各証明書とキーは引き続き使用できます。を実行した後では、eDirectory内に残っているプライベートキーと証明書は使用できません。ステップ 3

証明書を持つユーザごとに、ユーザオブジェクトのプロパティを開きます。［セキュリティ］タブの［証明書］セクションの下に、そのユーザのすべての証明書を示すテーブルが表示されます。発行者として組織の認証局が設定されている証明書はすべて削除してください。

NetIQ Single Sign-on

NetIQ Single Sign-onがソースツリー内にあるサーバのいずれかにインストールされている場合、ソースツリーのユーザ用NetIQ Single Sign-Onシークレットをすべて削除する必要があります。

ソースツリーでNetIQ Single Sign-onを使用するすべてのユーザについて、ユーザオブジェクトのプロパティを開きます。［セキュリティ］タブの［SecretStore］セクションの下に、そのユーザのシークレットすべてが表示されます。表示されたシークレットをすべて削除します。

注: 製品の使用状況によっては、指定されたオブジェクトと項目が存在しない可能性があります。指定されたオブジェクトや項目が存在しない場合には、この手順を省略できます。

NMAS

製品の使用状況によっては、指定されたオブジェクトと項目が存在しない可能性があります。指定されたオブジェクトや項目が存在しない場合には、手順を省略できます。

1 ターゲットツリーに、ソースツリーに存在してターゲットツリーには存在しない、NMASログインメソッドをインストールします。

必要なすべてのクライアントとサーバのログインコンポーネントをターゲットツリーに正しくインストールするには、NetIQオリジナルソースやベンダー提供ソースを使用して、新しいログインメソッドすべてをインストールすることをお勧めします。

メソッドは既存のサーバファイルから再インストールできますが、通常NetIQのパッケージまたはベンダー提供のパッケージからクリーンインストールする方が簡単で確実です。

2 ソースツリーで以前に確立されたログインシーケンスをターゲットツリーで使用できるようにするには、対象のログインシーケンスを移行します。

2a iManagerで、ソースツリーのセキュリティコンテナを選択します。

2b ［**ログインポリシー**］オブジェクトを右クリックして、［**プロパティ**］をクリックします。

2c ［**Defined Login Sequences**］ドロップダウンリストに表示されたログインシーケンスごとに、使用するログインメソッド(右側のペインに表示)をメモします。

2d ターゲットツリー内のセキュリティコンテナを選択し、ステップ 2cでメモしたログインメソッドと同じものを使用して、ログインシーケンスを複製します。

2e 操作が終了したら［**OK**］をクリックします。

3 ソースツリーのNMASログインセキュリティ属性を削除します。

3a ソースツリーのセキュリティコンテナで、ログインポリシーオブジェクトを削除します。

3b ソースツリーの許可されたログインメソッドコンテナで、ログインポリシーオブジェクトを削除します。

3c ソースツリーの許可されたログインメソッドコンテナを削除します。

3d ソースツリーの許可されたポストログインメソッドコンテナで、ログインポリシーオブジェクトを削除します。

3e ソースツリーの許可されたポストログインメソッドコンテナを削除します。

注: 許可されたログインメソッドを削除するには、ldapdeleteを使用します。

NetIQセキュリティドメインインフラストラクチャ

製品の使用状況によっては、指定されたオブジェクトと項目が存在しない可能性があります。指定されたオブジェクトや項目が存在しない場合には、手順を省略できます。

1 W0オブジェクトとソースツリーのKAPコンテナを削除します。

KAPコンテナは、セキュリティコンテナ内に存在します。W0オブジェクトは、KAPコンテナ内に存在します。

2 ソースツリー内のすべてのサーバで、Linuxでは/var/opt/novell/nici/uid/nicisdi.keyファイル、Windowsでは%SystemRoot%\SysWOW64\Novell\NICI\nicisdi.keyを削除することにより、セキュリティドメインインフラストラクチャ(SDI)キーを削除します。

重要: ソースツリー内のすべてのサーバで、このファイルを削除したことを確認します。

その他のセキュリティ固有の操作

ソースツリー内にセキュリティコンテナが残っている場合、ツリーをマージする前に、セキュリティコンテナを削除します。

ツリーのマージを実行する

DSMergeユーティリティを使用して、eDirectoryツリーをマージします。詳細については、297ページの第10章「NetIQ eDirectoryツリーのマージ」および843 ページの付録 B「NetIQ eDirectory用のLinuxコマンドとそれらの使用法」を参照してください。

ツリーのマージ後に実行する製品固有の操作

このセクションでは、次のことを説明します。

- 841 ページの 「NetIQ Certificate Server」
- 841 ページの 「NetIQ Single Sign-on」
- 841 ページの 「NMAS」

NetIQ Certificate Server

NetIQ Certificate Serverを使用している場合、ツリーのマージ後に、ソースツリー内に前に存在していたサーバとユーザに対して必要に応じて証明書を再発行します。

NetIQ Single Sign-on

NetIQ Single Sign-onを使用している場合、ツリーのマージ後に、ソースツリー内に前に存在していたユーザのSecretStoreシークレットを必要に応じて再作成する必要があります。

NMAS

NMASを使用している場合、ツリーのマージ後に、ソースツリー内に存在していたNMASユーザを必要に応じて再登録する必要があります。

詳細については、663ページの第24章「eDirectoryの認証フレームワークについて」を参照してください。

B NetIQ eDirectory用のLinuxコマンドとそれらの使用法

この章では、LinuxでのNetIQ eDirectory用の各ユーティリティとそれらの使用法を一覧にまとめています。

一般ユーティリティ

このセクションでは、LinuxでのeDirectoryユーティリティとその使用法についての一覧を提供しています。

注: インストール後に、ユーティリティのndsconfig、ndscheck、およびndsloginをサーバのインストール場所(この場所は、デフォルトでは/opt/novell/eDirectory/binです)から実行してください。インストールパッケージからndsconfigを実行しないでください。

eDirectoryユーティリティの使用法に関する詳細については、各ユーティリティのマニュアルページおよび957 ページの 「Linuxでのユーティリティのトラブルシューティング」を参照してください。

コマンド	説明	使用法
nds-install	NetIQ eDirectoryをインストールするユーティリティです。	`nds-install [-h] [--help] [-i] [-j] [-u]`

コマンド	説明	使用法
ndsconfig	NetIQ eDirectoryを設定します	ndsconfig <new> [-t <treename>] [-n <server context>] [-a <admin FDN>] [-w <password>] [-B ip_address1|interface1@port1,ip_address2|interface2@port2....] [-b port to bind] [-i] [-S <server name>] [-D <instance path>] [-d <path for dib>] [-m <module>] [-e] [-R|-r] [-c] [-L <ldap port>] [-l <SSL port>] [-P <LDAP URLs>] [-o http port] [-O https port] [--config-file <absolute path for configuration file>] [--configure-eba-now <yes/no>] ndsconfig <def> [-t <treename>] [-n <server context>] [-a <admin FDN>] [-w <password>] [-B ip_address1|interface1@port1,ip_address2|interface2@port2....] [-b port to bind] [-i] [-S <server name>] [-D <instance path>] [-d <path for dib>] [-m <module>] [-e] [-R|-r] [-c] [-L <ldap port>] [-l <SSL port>] [-P <LDAP URLs>] [-o http port] [-O https port] [--config-file <absolute path for configuration file>] [--configure-eba-now <yes/no>] ndsconfig add [-t <treename>] [-n <server context>] [-a <admin FDN>] [-w <password>] [-B ip_address1|interface1@port1,ip_address2|interface2@port2....] [-b port to bind] [-E] [-e] [-R|-r] [-c] [-L <ldap port>] [-l <SSL port>] [-P <LDAP URLs>] [-o http port] -O [https port] [-S <server name>] [-D <instance path >] [-d <path for dib>] [-p <IP address[:port]>] [-m <module>] [--config-file <absolute path for configuration file>] [--configure-eba-now <yes/no>] ndsconfig rm [-a <*admin FDN*>] [-w <*admin password*>] [-W <*obfuscated_password_file*>] [-c] [--config-file <*configuration file*>] ndsconfig upgrade [-a <admin FDN>] [-w <password>] [-c] [-j] [--config-file <absolute path for configuration file>] [--configure-eba-now <yes/no>] ndsconfig {set <*valuelist*> | get [<*paramlist*>] | get help [<*paramlist*>]}

コマンド	説明	使用法
ndscheck	ツリーの状態をチェックするユーティリティです。	ndscheck [--help | -?] Display command usage ndscheck [--version | -v] Display version information ndscheck [-h <*hostname port*>] [-a <*admin FDN*>] [-F <*log file*>] [-D] [-q] [-w <*admin password*>] [-W] [--config-file <*file name*>] ndscheck [-a <*admin FDN*>] [-W] [--config-file <*file name*>] 次に例を示します。 ndscheck -a admin.novell -W --config-file /etc/opt/novell/eDirectory/conf-1/nds.conf
ndsmanage	eDirectoryのインスタンスを表示するユーティリティ	ndsmanage [-a] ndsmanage [<*username*>]

コマンド	説明	使用法
ndsbackup	eDirectoryオブジェクトのアーカイブを作成し、eDirectoryオブジェクトを追加または抽出します	ndsbackup c [f <*ndsbackupfile*>] [e] [v] [w] [X<*exclude-file*>] [R] [Replica-server-name] [-a <*admin-user*>] [-I <*include-file*>] [-E <*password*>] [--config-file <*configuration_file_path*>]... [eDirectoryobject] ndsbackup r [f <*ndsbackupfile*>] [e] [v] [w] [X<*exclude-file*>] [R] [Replica-server-name] [-a <admin-user>] [-I <*include-file*>] [-E <*password*>] [--config-file <*configuration_file_path*>]... [eDirectoryobject] ndsbackup t [f <*ndsbackupfile*>] [e] [v] [w] [X<*exclude-file*>] [R] [Replica-server-name] [-a <admin-user>] [-I <*include-file*>] [-E <*password*>] [--config-file <configuration_file_path>]... [eDirectoryobject] ndsbackup x [f <*ndsbackupfile*>] [e] [v] [w] [X<*exclude-file*>] [R] [Replica-server-name] [-a <admin-user>] [-I <*include-file*>] [-E <*password*>] [--config-file <*configuration_file_path*>]... [eDirectoryobject] ndsbackup s [e] [v] [w] [X<*exclude-file*>] [R] [Replica-server-name] [-a <*admin-user*>] [-I <*include-file*>] [-E <*password*>] [--config-file <*configuration_file_path*>]... [eDirectoryobject] ndsbackup --version ndsbackup [option] [file] [-a <*admin FDN*>] [-p passstore] [--config-file <*file name*>] 次に例を示します。 ndsbackup cvf /tmp/test.bak -a admin.novell -p passstore --config-file /etc/opt/novell/eDirectory/conf-1/nds.conf
ndslogin	NetIQ eDirectoryの認証を検証するための診断ユーティリティです	ndslogin [-t treename] [-p password] [-s] [-n] [-c] [[-i] | [-I]] [[-h hostname[:port]] | [--config-file <configuration file>]] <userFDN>
ndsd	NDSデーモン	/opt/novell/eDirectory/sbin/ndsd [--config-file *configfile*]

コマンド	説明	使用法
ndsimonitor	HTTPを使用して、NetIQ eDirectoryツリーにあるサーバを監視および診断します	/opt/novell/eDirectory/bin/ndsimonitor [-l [-d *<path of ndsimonitor conf files>*] | u] [-h *<local_interface:port>*] [--config-file *<configuration_file_path>*]
ndsmerge	2つのNetIQ eDirectoryツリーをマージするユーティリティ	ndsmerge [-m target-tree target-admin source-admin [target-container]] [-c] [-t] [-r target-tree source-admin] [-h *<local_interface:port>*] [--config-file *<configuration_file_path>*]
ndsrepair	レコード、スキーマ、バインダリオブジェクト、および外部参照など、eDirectoryデータベースの問題を修復および修正するためのユーティリティです。	ndsrepair {-U |-E |-C |-P [Ad] |-S [Ad]|-N |-T |-J *<entry_id>*} [-A *<yes/no>*] [-O *<yes/no>*][-F *<filename>*] [-h *<local_interface:port>*] [--config-file *<configuration_file_path>*]
		ndsrepair -R [-l *<yes/no>*][-u *<yes/no>*][-m *<yes/no>*][-i *<yes/no>*][-f *<yes/no>*][-d *<yes/no>*][-t <yes/no>][-o <yes/no>][-r <yes/no>][-v <yes/no>][-c <yes/no>][-A <yes/no>][-O <yes/no>][-F *<filename>*] [-h *<local_interface>*] [--config-file *<configuration_file_path>*]
		ndsrepair –I [--config-file *<configuration_file_path>*]
	使用するために解放できる、データベース内の空き領域に関する情報を表示するように、ndsrepairに指示できます。	
ndssch	NetIQ eDirectoryスキーマ拡張ユーティリティ	ndssch [-h *<hostname>*[:<port>]][-t *<treename>*][-F *<logfile>*] *<admin-FDN>* *<schemafile>* ...
		ndssch [-h *<hostname>*[:<port>]][-t *<treename>*] [-d] *<admin-FDN>* *<schemafile>* [schema description] ...
ndssnmp	NetIQ eDirectoryのSNMPサービスモジュール。	/opt/novell/eDirectory/bin/ndssnmp
ndssnmpconfig	SNMPトラップ環境設定ユーティリティです	ndssnmpconfig [-h *<hostname[:port]>*] [-p *<password>*] [-a *<userFDN>*] [-c *<command>*]
ndssnmpsa	eDirectory SNMPサブエージェントデーモンです	/opt/novell/eDirectory/bin/ndssnmpsa
ndsstat	サーバ情報を表示するユーティリティです	ndsstat { -r -s -p *<partitionname>*} [-n] [[-h *<hostname | IP address>:<port>*] | [--config-file *<configuration file>*]]
ndstrace	サーバのデバッグメッセージを表示するユーティリティです	ndstrace [-l|-u|-c "command1;....."|--version] [-h *<local_interface:port>*] [--config-file *<configuration_file_path>*]
nds-uninstall	NetIQ eDirectoryをアンインストールするユーティリティ	nds-uninstall [-s][-h]

コマンド	説明	使用法
nldap	NDSデーモンのLDAPサービス	/opt/novell/eDirectory/sbin/nldap
nmasinst	NMAS環境設定ユーティリティ	nmasinst -i <*admin-FDN*> <*treename*> [-h <*hostname*>[:port]] nmasinst -addmethod <*admin-FDN*> <*treename*> <*config.txt file*> [-h <*hostname*>[:port]]
npki	Novell公開鍵インフラストラクチャサービス	/opt/novell/eDirectory/sbin/npki

LDAP固有のコマンド

コマンド	説明	使用法
ldapconfig	LDAPサーバおよびLDAPグループオブジェクトを設定するユーティリティです	ldapconfig get [...] | set <*attribute-value-list*> [-t <*treename*> | -p <*hostname*>[:port] | --config-file <*configuration file*>] [-w <*password*>] [-a <*user FDN*>] [-f] ldapconfig [-t <*treename*> | -p <*hostname*>[:port]] [-w <*password*> | --config-file <*configuration file*>] [-a <*user FDN*>] [-V] [-R] [-H] [-f] -v <*attribute*>,<*attribute2*>... ldapconfig [-t <*treename*> | -p hostname[:port] | --config-file <*configuration file*>] [-w <*password*>] [-a <*admin FDN*>] [-V] [-R] [-H] [-f] -s <*attribute*>=<*value*>,...
ldapadd ldapmodify	LDAPサーバからエントリを追加または変更します	ldapmodify [-a] [-c] [-C] [-M] [-P] [-r] [-n] [-v] [-F] [-l <*limit*>] [-M[M]] [-d <*debuglevel*>] [-e <*key filename*>] [-D <*binddn*>] [[-W]|[-w <*passwd*>]] [-h <*ldaphost*>] [-p <*ldap-port*>] [-P <*version*>] [-Z[Z]] [-f <*file*>] ldapadd [-c] [-C] [-l] [-M] [-P] [-r] [-n] [-v] [-F] [-l <*limit*>] [-M[M]] [-d <*debuglevel*>] [-e <*key filename*>] [-D <*binddn*>] [[-W]| [-w <*passwd*>]] [-h <*ldaphost*>] [-p <*ldapport*>] [-P <*version*>] [-Z[Z]] [-f <*file*>]

コマンド	説明	使用法
ldapdelete	LDAPサーバからエントリを削除します	ldapdelete [-n] [-v] [-c] [-r] [-l] [-C] [-M] [-d <*debuglevel*>] [-e <*key filename*>] [-f <*file*>] [-D <*binddn*>] [[-W]| [-w <*passwd*>]] [-h <*ldaphost*>] [-p <*ldapport*>] [-Z[Z]] [dn]...
ldapmodrdn	LDAPのエントリの相対識別名(RDN)変更ツールです	ldapmodrdn [-r] [-n] [-v] [-c] [-C] [-l] [-M] [-s <*newsuperior*>] [-d <*debuglevel*>] [-e <*key filename*>] [-D <*binddn*>] [[-W]|[-w <*passwd*>]] [-h <*ldaphost*>] [-p <*ldapport*>] [-Z[Z]] [-f <*file*>] [dn <*newrdn*>]
ldapsearch	LDAPの検索ツールです	ldapsearch [-n] [-u] [-v] [-t] [-A] [-T] [-C] [-V] [-M] [-P] [-L] [-d <*debuglevel*>] [-e <*key filename*>] [-f <*file*>] [-D <*binddn*>] [[-W]| [-w <*bindpasswd*>]] [-h <*ldaphost*>] [-p <*ldapport*>] [-b <*searchbase*>] [-s <*scope*>] [-a <*deref*>] [-l <*time limit*>] [-z <*size limit*>] [-Z[Z]] filter [attrs....]
ndsindex	NetIQ eDirectoryデータベースインデックスの作成、リスト表示、一時停止、再開、または削除に使用するユーティリティです。	ndsindex list [-h <*hostname*>] [-p <*port*>] [-D <*bind DN*>*] [*-W|[-w <*password*>]] [-l <*limit*>] [-s <*eDirectory Server DN*>] [-Z[Z]] [<*indexName1*>, <*indexName2*>.....] ndsindex add [-h <*hostname*>] [-p <*port*>] [-D <*bind DN*>] -W|[-w <*password*>] [-l <*limit*>] [-s <*eDirectory Server DN*>] [-Z[Z]] <*indexDefinintion1*> *[*<*indexDefinintion2*>.....] ndsindex delete [-h <*hostname*>] [-p <*port*>] [-D <*bind DN*>] [-W|[-w <*password*>]] [-l <*limit*>] [-s <*eDirectory Server DN*>] [-Z[Z]] <*indexName1*> *[*<*indexName2*>.....] ndsindex resume [-h <*hostname*>] [-p <*port*>] -D <*bind DN*> [-W|[-w <*password*>]] [-l <*limit*>] [-s <*eDirectory Server DN*>] [-Z[Z]] <*indexName1*> *[*<*indexName2*>.....] ndsindex suspend [-h <*hostname*>] [-p <*port*>] [-D <*bind DN*>] [-W|[-w <*password*>]] [-l <limit>] [-s <*eDirectory Server DN*>] [-Z[Z]] <*indexName1*> *[*<*indexName2*>.....]

コマンド	説明	使用法

ice	このユーティリティは、エントリをファイルからLDAPディレクトリにインポートし、ファイルのディレクトリ内のエントリを変更し、エントリをファイルにエクスポートし、ファイルの属性とクラス定義を追加します。	`ice -S LDAP -s server1.acme.com -p 636 -L cert-server1.pem -d cn=admin,c=us -w password -F objectClass=* -c sub -D LDIF -f server1.ldif -e des -E secret`
		
		`ice -S LDIF -f server1.ldif -e des -E secret -D LDAP -s server2.acme.com -p 636 -L cert-server2.pem -d cn=admin,c=us -w password`

ユーザ名およびパスワードでの特殊文字

ユーザ名およびパスワードで特殊文字を使用すると、eDirectoryのインストール時またはスキーマ拡張時に値が渡される場合に問題が生じる可能性があります。ユーザ名またはパスワードに$や#などの特殊文字が含まれる場合、その特殊文字の前にバックスラッシュ(\)を付けてエスケープしてください。

たとえば、cn=admin$name.o=containerという管理者ユーザ名は、cn=admin\$name.o=containerで渡す必要があります。

コマンドラインにパラメータ値を入力する場合、その文字をエスケープしたり、その値の前後を一重引用符で囲んだりできます。

次に例を示します。

```
cn=admin\$name.o=container
```

または

```
'cn=admin$name.o=container'
```

C OpenSLP for eDirectoryの設定

この付録では、ネットワーク管理者向けに、Novell Clientが存在しないOpenSLP for NetIQ eDirectoryのインストールに関する適切な環境設定について説明します。

Service Location Protocol

OpenSLPは、IETF Service Location Protocol Version 2.0規格のオープンソースによる実装です。この規格は、IETF Request-For-Comments (RFC) 2608 (http://www.ietf.org/rfc/rfc2608.txt?number=2608)で文書化されました。

SLPv2プロトコルの実装に加え、OpenSLPソースコードが提供するインタフェースは、SLP機能にプログラム的にアクセスするためのもう1つのIETF規格を実装したもので、RFC 2614 (http://www.ietf.org/rfc/rfc2614.txt?number=2614)で文書化されています。

SLPの動作の詳細を理解するためには、この2つのドキュメントを参照し、熟読してください。読みやすい文書ではありませんが、インターネットでのSLPの正しい設定を行うためには重要なドキュメントです。

OpenSLPプロジェクトの詳細については、OpenSLP (http://www.OpenSLP.org)のWebサイトとSourceForge (http://sourceforge.net/projects/openslp)のWebサイトを参照してください。OpenSLPのWebサイトには、環境設定に関する貴重なヒントを含んださまざまな文書があります。ただし、このガイドの作成時点では、これらのドキュメントの多くは未完成です。

SLPの基本

Service Location Protocolでは、次の3種類のコンポーネントが定義されています。

- ユーザエージェント(UA)
- サービスエージェント(SA)
- ディレクトリエージェント(DA)

ユーザエージェントは、クライアントがサービスを問い合わせたり、サービスがそれ自体を通知するためのプログラムインタフェースを提供します。ユーザエージェントはディレクトリエージェントに接続し、指定したスコープ内の指定したサービスクラスに登録されたサービスを問い合わせます。

サービスエージェントは、SLPで登録されたローカルサービスを持続的に格納し、維持する場所を提供します。サービスエージェントは主として、登録済みのローカルサービスをメモリ内データベースとして維持します。この場合、サービスはローカルSAがない限りSLPで登録できません。ク

ライアントがサービスを検出するのはUAライブラリ内のみですが、登録するにはSAが必要です。これは主に、ディレクトリエージェントを受信して登録を維持するためには、登録済みサービスの存在をSAが定期的に表明する必要があるためです。

ディレクトリエージェントは、通知されたサービスに対して長期間持続的にキャッシュを提供し、ユーザエージェントがサービスを検索するためのアクセスポイントとなります。キャッシュ機能を提供するDAは、SAが新しいサービスを通知するのを受信し、これらの通知をキャッシュします。DAのキャッシュは短時間で完了します。ディレクトリエージェントは、期限切れのアルゴリズムを使用してエントリキャッシュを有効期限切れにします。ディレクトリエージェントが起動すると、持続的な格納領域(通常はハードドライブ)からキャッシュを読み込み、アルゴリズムに従ってエントリを有効期限切れにします。新しいDAが起動したり、キャッシュが削除されると、DAはこの条件を検出して受信中のすべてのSAに特別な通知を送信します。SAは、DAが直ちにキャッシュを作成できるようにローカルデータベースをダンプします。

ディレクトリエージェントが存在しない場合、UAはSAが応答できる一般的なマルチキャスト方式のクエリを使用し、DAがキャッシュを作成するのとほぼ同じ方法で、要求されたサービスのリストを作成します。このクエリによって返されるサービスのリストは、DAが提供するリストと比較すると不完全かつ局所的です。特に、多くのネットワーク管理者が使用するマルチキャスト方式でのフィルタ処理では、ブロードキャストおよびマルチキャストの対象がローカルサブネットのみに制限されるためです。

つまり、指定されたスコープに対してユーザエージェントが検索するものは、すべてディレクトリエージェントに依存します。

NetIQ Service Location Providers

NovellのバージョンのSLPでは、強力なサービスアドバータイズ環境を提供するため、SLP標準が一部変更されます。しかし、このために一部の拡張性を犠牲にしています。

たとえば、サービスアドバータイズのフレームワークの拡張性を改善するために、サブネット上でのブロードキャストまたはマルチキャストのパケット数が制限されます。SLPの仕様では、これを管理するために、ディレクトリエージェントのクエリに関してサービスエージェントおよびユーザエージェントに制限を加えています。必要なスコープに対応するための最初に検出されたディレクトリエージェントは、サービスエージェント(つまり結果的にローカルユーザエージェント)がそのスコープ上の将来の要求すべてに使用するエージェントとなります。

NetIQ SLPを実装すると、クエリ情報の検索について既知のディレクトリエージェントをすべてスキャンします。スキャンの所要時間は300ミリ秒とかなり長く、したがって、約3〜5秒以内で10台のサーバしかスキャンできません。SLPがネットワーク上で正しく設定されている場合にはこのような検索の必要はありません。OpenSLPでは、ネットワークが実際にSLPトラフィック用に設定されていると見なされます。OpenSLPの応答タイムアウト値はNetIQのSLPサービスプロバイダの応答タイムアウト値よりも大きい値です。ディレクトリエージェント数は、エージェントの情報が正確で完全であるかどうかに関係なく、最初に応答するディレクトリエージェントに制限されます。

ユーザエージェント

ユーザエージェントの物理形式は、アプリケーションにリンクされたスタティックライブラリまたはダイナミックライブラリです。ユーザエージェントにより、アプリケーションはSLPサービスに対して問い合わせることができます。

ユーザエージェントは、アルゴリズムに従って、クエリの送信先になるディレクトリエージェントのアドレスを取得します。指定したスコープのDAアドレスを取得すると、ユーザエージェントはそのスコープから応答がなくなるまで同じアドレスを使用し続けます。応答がなくなると、ユーザエージェントはそのスコープに対する別のDAアドレスを取得します。ユーザエージェントは、指定されたスコープのディレクトリエージェントのアドレスを次の方法で検索します。

1. 現在の要求のソケットハンドルが、指定したスコープのDAに接続されているかどうかを確認する。複数の要求の場合は、すでにキャッシュ化された接続がある可能性がある。
2. 指定したスコープと一致しているDAの、既知のローカルDAキャッシュをチェックする。
3. 指定したスコープでローカルSAに対してDAを確認し、その後キャッシュに新しいアドレスを追加する。
4. 指定したスコープに一致するDAのネットワーク設定済みのアドレスをDHCPに問い合わせ、その後キャッシュに新しいアドレスを追加する。
5. 既知のポートでDAのディスカバリ要求をマルチキャストし、その後キャッシュに新しいアドレスを追加する。

スコープを指定しない場合、指定スコープは「デフォルト」になります。つまり、SLP設定ファイルで静的に定義されたスコープがなく、クエリでスコープを指定していない場合は、使用されるスコープは「デフォルト」という単語になります。また、eDirectoryの登録ではeDirectoryはスコープを指定しないことに注意してください。つまり、eDirectoryで使用されるスコープは常に「デフォルト」というわけではありません。スコープが静的に設定されている場合、そのスコープがすべてのローカルUA要求およびSA登録に対して、指定したスコープがない場合のデフォルトのスコープになります。

サービスエージェント

サービスエージェントの物理形式は、ホストマシン上での個別のプロセスです。Windowsの場合は、slpd.exeがローカルマシン上のサービスとして実行されます。ユーザエージェントは、既知のポート上のループバックアドレスにメッセージを送信することによって、ローカルサービスエージェントを問い合わせます。

サービスエージェントは、潜在DAアドレスにDA検出要求を直接送信することにより、ディレクトリエージェントおよびそれがサポートするスコープリストを検出してキャッシュします。DA検出要求は、次の方法で送信されます。

1. 静的に設定されたDAアドレスをすべてチェックする(その後SAの既知のDAキャッシュに新しいDAアドレスを追加します)。
2. DHCPからDAとスコープのリストを要求する(その後SAの既知のDAキャッシュに新しいリストを追加します)。
3. 既知のポートでDAの検出要求をマルチキャストする(その後SAの既知のDAキャッシュに新しいポートを追加します)。
4. DAによって定期的にブロードキャストされたDAのアドバータイズパケットを受信する(その後SAの既知のDAキャッシュに新しいアドバータイズパケットを追加します)。

ユーザエージェントは常に最初にローカルサービスエージェントに対して問い合わせます。ローカルサービスエージェントの応答によってユーザエージェントが次の検出段階を続行するかどうかが決定されるため、このことは重要な点です(DHCPのこのケースについては、「853ページの「ユーザエージェント」」の手順3および4を参照してください)。

環境設定パラメータ

SLP環境設定パラメータはslp.confファイルに保存されます。このファイルは、UNIXおよびLinuxプラットフォーム上では/etcにあり、Windowsプラットフォーム上では%systemroot%/slp.confです。これらのパラメータは、ネットワークに関する操作を調整するために変更できます。たとえば、次の各パラメータではDA検出が制御されます。

```
net.slp.useScopes = <comma-delimited scope list>
net.slp.DAAddresses = <comma-delimited address list>
net.slp.passiveDADetection = <"true" or "false">
net.slp.activeDADetection = <"true" or "false">
net.slp.DAActiveDiscoveryInterval = <0, 1, or a number of seconds>
```

useScopesオプションは、SAの通知先のスコープ、および、サービスまたはクライアントアプリケーションで作成された登録またはクエリに指定したスコープが存在しない場合に、クエリが作成されるスコープを示します。eDirectoryは常にデフォルトのスコープに通知し、問い合わせを行うため、このリストがeDirectoryの登録およびクエリのデフォルトのスコープのリストになります。

DAAddressesオプションはコンマで区切られたIPアドレスのリストで、アドレスは10進数とドットで表記されます。このアドレスが他のすべてに対して優先されます。設定されたDAのこのリストが登録またはクエリのスコープをサポートしない場合、検出を無効にしていない限りは、SAおよびUAはマルチキャスト方式でDAを検出します。

passiveDADetectionオプションのデフォルトは「TRUE」です。ディレクトリエージェントは、設定に応じて定期的にそれ自体の存在をサブネットの既知のポート上にブロードキャストします。これらのパケットはDAAdvertパケットと名付けられます。このオプションに「FALSE」を設定した場合、ブロードキャスト方式のすべてのDAAdvertパケットはSAに無視されます。

activeDADetectionオプションのデフォルトも「TRUE」です。この設定により、SAはすべてのDAに対して、指示されたDAAdvertパケットで応答するように、定期的にブロードキャスト方式で要求できます。指示されたパケットはブロードキャストではありませんが、この要求に対する応答ではSAに直接送信されます。このオプションに「FALSE」を設定した場合、SAは定期的なDAの検出要求をブロードキャストしません。

DAActiveDiscoveryIntervalオプションはtry-stateパラメータです。デフォルト値は1です。これは、初期化の際に、SAがDAの検出要求を1回送る設定であることを意味する特別な値です。このオプションに0を設定すると、activeDADetectionオプションに「FALSE」を設定した場合と結果は同じです。その他の値は、検出をブロードキャストする間隔を秒数で表します。

このオプションを正しく使用すると、サービスアドバータイズに使用するネットワーク帯域幅を適切に設定できます。ただし、デフォルト設定は平均的なネットワークで拡張性を最適化するように設計されています。

注: デフォルトでは、SLPに対してIPV4プロトコルが有効になっており、IPV6は無効になっています。IPV6を有効にするには、slp.confファイル内の次の行のコメントを外します。

net.slp.useIPv6 = true

OpenSLP 2.0が付属しているのはWindowsだけであるため、この設定はWindowsでのみ有効です。

slptoolユーティリティ

このユーティリティは、OpenSLPで提供されているコマンドラインユーティリティです。slptoolは、サービスの登録または登録解除と、スコープ、サービスタイプ、属性、および使用可能なサービスの問い合わせに使用できます。

次に例を示します。

- サービスを登録するには、次の構文を使用します。

  構文: slptool register url *[attrs]*

  ```
  slptool register service:myserv.x://myhost.com "(attr1=val1),(attr2=val2)"
  ```

- サービスを登録解除するには、次の構文を使用します。

  構文: slptool deregister *url*

  ```
  slptool deregister service:myserv.x://myhost.com
  ```

- 使用可能なサービスを検索するには、次の構文を使用します。

  構文: slptool findsrvs *service-type [filter]*

  ```
  slptool findsrvs service:myserv.x
  ```

  ```
  slptool findsrvs service:myserv.x "(attr1=val1)"
  ```

- 設定済みのスコープを検索するには、次の構文を使用します。

  構文: slptool findscopes

D NetIQ eDirectoryでのDNSの使用方法

クライアントがサーバにNetIQ eDirectoryツリーに存在しない完全修飾名(たとえば、admin.novell.novell_inc)の解決を要求する場合、またはNetIQ iManager for LinuxやeDirectoryのインストールアプリケーションなどのスタンドアロンアプリケーションを使用してツリー内の名前を解決する場合で、通信するサーバがまだ存在しない場合は、eDirectoryではサービスディスカバリプロトコルを使用して名前を解決します。サービスディスカバリプロトコルはネットワークアプリケーションのクラスで、分散コンポーネントを使用してネットワーク内の必要なサービスを検索して使用できます。

eDirectoryは、従来SAPおよびSLPを使用してネットワークサービスを検索し、通知してきました。DNSはディスカバリプロトコルとしてeDirectory 8.7.1で追加されました。この追加機能では、eDirectoryで認識していないツリー名(通信しているサーバにツリーのコピーが保持されていないか、スタンドアロンアプリケーションを使用しているため)を問い合わせる場合、検出を試みるマシンが、スタンドアロンアプリケーションを実行しているマシンであるか、NetIQ iManagerなどのJClientアプリケーションを実行しているマシンであるか、またはサーバであるかに関係なく、eDirectoryのディスカバリプロトコルを次の順序で使用します。

1. DNS (Domain Name System)
2. SLP (Service Location Protocol)
3. SAP (Service Advertising Protocol)

eDirectoryでは、DNSプロトコルを使用する場合、名前(たとえば、「prod_server4.provo.novell.novell-_inc」などのサーバ名)が渡されるとそれを使用して、その名前全体の解決をそのままで試みます。次に、eDirectoryでは検出マシンのDNS検索リストにそれぞれの名前を追加してから、マシンのDNSサーバにその名前のアドレスが存在するかどうかをそのDNSサーバに問い合わせます。たとえば、検出マシンのDNS検索リストに「dev.novell.com」および「test.novell.com」が含まれている場合、eDirectoryではprod_server4.provo.novell.novell_inc.dev.novell.comおよびprod_server4.provo.novell.novell_inc.test.novell.comを検索します。

その後、eDirectoryは渡された名前からコンポーネントを切り離します。たとえば、「prod_server4.provo.novell.novell_inc」を解決する場合、eDirectoryはprovo.novell.novell_inc、novell.novell_inc、novell_incの順に試みます。eDirectoryは、各々の異なる検索コンテキストに対して検索を行い、最終的にツリーのルートの単一コンポーネントに検索を試みます。クライアントは接続が成功するまで各アドレスを試行します。アドレスの試行には、DNSサーバから戻されたレコードの順序を使用します。検出を試みるコンピュータがeDirectory 8.7.1以降を実行している限り、レプリカリング内のサーバがどのコードリビジョンを実行しても問題ありません。

eDirectoryツリー名は、クライアントが名前解決のために使用するDNSドメインの下のA、AAAA、またはサービス(SRV)リソースレコードを使用するDNSに加えることをお勧めします。AまたはAAAAレコードを使用する場合、eDirectoryサーバはデフォルトの524ポートで実行する必要があります。サーバが他のポートを使用する場合は、SRVレコードを使用します。

次のリソースレコードのサンプルでは、ツリー名は「novell_inc」でDNS検索コンテキストは「provo.novell.com」です。

レコード	例
マシンは、	novell_inc.provo.novell.com.IN A 192.168.1.2
AAAA	novell_inc.provo.novell.com.IN AAAA 4321:0:1:2:3:4:567:89ab
SRV	_ldap._tcp.novell_inc.provo.novell.com.SRV 0 0 389 server1.novell_inc.provo.novell.com SRV 10 0 389 server2.novell_inc.provo.novell.com

冗長性を維持するため、または複数のホスト(レプリカリング内のサーバ)をAレコードに指定するためには、Aレコードを2つ以上作成します。eDirectoryは、それらすべてを検索します。A、AAAA、およびSRVレコードの詳細については、「DNS resource records」を参照してください。

DNSサーバのレコードエントリを、対応するパーティションルートを保持している何かに指示させる必要はありません。検出するマシンがツリーを認識しているサーバと通信でき次第、ツリー全体を参照して名前を解決できます。たとえば、DNSに「novell_inc」を設定している場合、「novell_inc」ルートを保持するサーバのいずれにも設定する必要はありません。必要なのは「novell_inc」ツリー内の任意のサーバを参照することだけです。これは、ツリー内でそのサーバに接続できれば、そのサーバがツリー周辺でユーザを参照するためです。

E eDirectoryでのGSSAPIの設定

NetIQ eDirectoryのSASL-GSSAPIメカニズムを使用すれば、LDAPを通じてKerberosチケットによってeDirectoryから認証を受けることができます。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サーバから認証を受けることによって取得する必要があります。

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。

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。

次のセクションでは、GSSAPIの設定方法と、eDirectoryでKerberosを使用して実行できるさまざまなタスクについて説明し、その他の有用な情報も提供します。

概念

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。

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。

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。

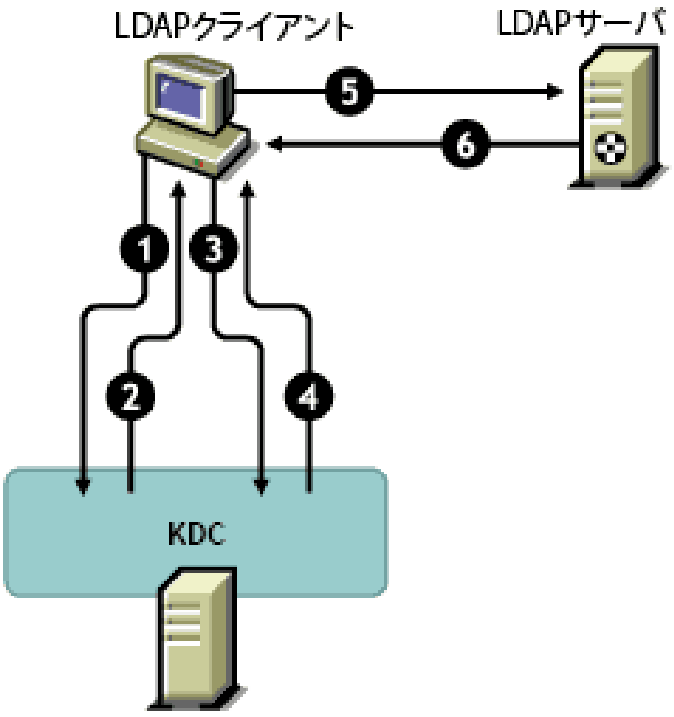
GSS APIの形式に関する詳細については、RFC 1964 (http://www.ietf.org/rfc/rfc1964.txt?number=1964)を参照してください。

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。

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E-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。

GSSAPIを設定するための前提条件

GSSAPIを設定するには、まず次の作業を行う必要があります。

- **SASL-GSSAPIメソッド:** SASL-GSSAPIメソッドをインストールします。『*NetIQ Modular Authentication Services 3.3 Administration Guide (NetIQ Modular Authentication Services 3.3管理ガイド)* (https://www.netiq.com/documentation/edir88/nmas88/data/bookinfo.html)』の「Installing a Login Method(ログインメソッドのインストール)」セクションを参照してください。

  注: eDirectory SASL-GSSAPIメソッドは、Domain Services for Windowsがインストールされた Open Enterprise Server (OES)バージョン2または11のインストール環境には機能しません。

  SASL-GSSAPIがコンピュータにインストールされているかどうかを確認するには、次のように入力します。

  ldapsearch -x -h osg-dt-srv9 -b " " -s base | grep -i sasl

  SASL-GSSAPIがインストールされている場合、コマンドの出力は次のようになります。

  ```
  supportedSASLMechanisms: NMAS_LOGIN

  supportedSASLMechanisms: GSSAPI
  ```

- **iManager用のKerberosプラグイン:** iManager用のKerberosプラグインをインストールします。詳細については、「862 ページの 「iManager用のKerberosプラグインのインストール」」を参照してください。
- **キー配布センター(KDC: Key Distribution Center):** Kerberos KDC(MITまたはActive Directory)をネットワーク上にインストールします。

  Microsoft KDC (Active Directory)を使用する場合は、Kerberosツールをインストールしておく必要があります。これらのツールはWindowsインストールの一部であり、Windowsインストール CD上の\support\tools\setup.exe(Windows XP)または \support\tools\suptools.msi(Windows 2003)からインストールできます。

❒ **時刻同期:** このメソッドを機能させるために、NMASクライアントマシン、NMASサーバマシン、およびKDCマシンの時刻を同期します。ネットワーク時刻の同期の詳細については、98 ページの 「ネットワーク時刻の同期」を参照してください。

❒ **Kerberos LDAP拡張** Kerberos LDAP拡張を追加します。詳細については、863 ページの「KerberosのLDAP拡張の追加」を参照してください。

重要

- Open Enterprise Server (OES)で、Domain Services for WindowsまたはDNSサービスが設定されているサーバ上にKerberos LDAP拡張を追加しないでください。
- Kerberosの管理で収集されるKerberos情報では、大文字と小文字が区別されるため、大文字と小文字を正確に指定する必要があります。

ネットワークの特性に関する前提

SASL-GSSAPIメカニズムは次の前提に基いて動作します。

- ネットワーク上のすべてのコンピュータの時刻がある程度正確に同期されている。言い換えると、システム時刻が5分以上異なる2台のコンピュータがネットワーク上に存在しない。
- MAN環境やWAN環境では時刻同期に関するこのような要件を満たすことが難しいため、SASL-GSSAPIメカニズムは主にLANでの使用を想定している。ただし、このメカニズムはLANのみに限定されていない。
- KerberosサーバとKerberos管理者を検証なしで無条件に信頼する。
- DoS(Denial-of-Service)攻撃に対抗する手段にはならない。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。

iManager用のKerberosプラグインのインストール

1 ブラウザを開きます。

2 ブラウザウィンドウのアドレスフィールドに、次のURLを入力します。

`http://`*`hostname`*`/nps/`

*ホスト名*は、SASL-GSSAPI用のiManagerプラグインをインストールするiManagerサーバのサーバ名またはIPアドレスです。

注: 問題が発生した場合は、TomcatおよびWebサーバが正しく設定されていることを確認します。詳細については、『*NetIQ iManager 2.7 Administration Guide (NetIQ iManager 2.7管理ガイド)* (https://www.netiq.com/documentation/imanager/imanager_admin/data/bookinfo.html)』を参照してください。

---

3 eDirectoryにログインするためのユーザ名とパスワードを指定して、［ログイン］をクリックします。

4 iManagerツールバーで、［設定］ をクリックします。

5 左側のペインで、［プラグインのインストール］>［利用できるNetIQプラグインモジュール］の順にクリックします。

6 追加をクリックします。

7 kerberosPlugin.npmファイルの場所を指定するか、［参照］をクリックしてこのファイルの場所を選択します。

Kerberos管理プラグインが、eDirectory 88の単一NPM(eDir_88_iMan27_Plugins.npm)の一部として使用でき、またNovellダウンロードサイト (https://download.novell.com/Download?buildid=G_8Eymx0QtI~)からダウンロードすることもできます。

kerberosPlugin.npmファイルを別の場所に移動した場合は、その場所をブラウズして選択してください。

8 ［開く］をクリックし、［OK］をクリックします。

9 ［インストール］をクリックします。

このインストールには数分かかります。

10 モジュールが正しく保存されたことを示すメッセージが表示されたら、iManagerサーバを再起動します。

iManagerを無制限アクセスモードで実行している場合(ツリーにRBSコレクションがない場合)は、ステップ 11からステップ 17をスキップしてください。

注: iManagerサーバの再起動については、『*NetIQiManager管理ガイド*』を参照してください。

---

11 iManagerにログインして、［設定  ボタンをクリックします。

12 左側のペインで、［役割ベースサービス］>［RBSの設定］の順にクリックします。

13 (状況によって実行)RBSコレクションがない場合は、次の操作を実行します。

13a ［新規］>［コレクション］の順にクリックします。

13b コレクションで使用する名前を指定します。

13c 役割ベースサービスを作成するコンテナを選択して、［OK］をクリックします。

13d 再度[OK]をクリックします。

14 ［iManager 2.xコレクション］タブで、使用するコレクションの［モジュール］カラム内の番号をクリックします。

15 ［Kerberosモジュール］を選択して、［インストール］をクリックします。

16 ［OK］をクリックして続行します。

17 iManagerによるモジュールのインストールが完了したら、［OK］をクリックします。

18 iManagerツールバーで、［役割およびタスク］をクリックします。

Kerberos管理の役割が左側の画面に表示されます。

Kerberos管理の役割が表示されない場合は、iManagerサーバを再起動します。

KerberosのLDAP拡張の追加

KerberosのLDAP拡張では、Kerberosキーの管理機能が提供されています。

KerberosのLDAP拡張を使用するには、C言語用のLDAPライブラリをインストールする必要があります。詳細については、「LDAP Libraries for C (http://www.novell.com/developer/ndk/ldap_libraries_for_c.html)」を参照してください。

KerberosのLDAP拡張を追加または削除するには、krbLdapConfigユーティリティを使用します。スタンドアロンのeDirectoryパッケージがディレクトリに抽出された場合、このファイルのパスはextracted_folder/nmas/NmasMethods/Novell/GSSAPI/Kerberos_ldap_extensions/Linux/krbLdapConfigです。

例: /misc/eDir88/Linux/nmas/NmasMethods/Novell/GSSAPI/Kerberos_ldap_extensions/Linux/krbLdapConfig

Kerberos LDAP拡張を追加するには、次の構文を使用します。

```
krbldapconfig {-i | -u} -D bind_DN [-w bind_DN_password] [-h ldap_host] [-p
ldap_port] [-e trusted_root_cert]
```

krbldapconfigユーティリティのパラメータについて、次の表で説明します。

パラメータ	説明
-i	Kerberos LDAP拡張をeDirectoryに追加します。
-u	Kerberos LDAP拡張をeDirectoryから削除します。
-D *bind_fdn*	管理者または管理者と同等の権利を持つユーザのFDNを指定します。 この指定は、cn=admin,o=orgの形式で指定する必要があります。
-w *bind_fdn_password*	バインドFDN(bind_fdn)のパスワードを指定します。
-h *ldap_server*	Kerberos LDAP拡張をインストールする必要があるLDAPサーバのホスト名またはIPアドレスを指定します。
-p *port*	LDAPサーバが動作しているポートを指定します。
-e *trusted_root_file*	SSLバインド用のルート認証局証明書のファイル名を指定します。 SSLポートを使用する場合は、-eオプションを指定してください。 詳細については、865ページの「ルート認証局証明書のエクスポート」を参照してください。

注: -hオプションを指定しなかった場合は、krbldapconfigの起動元のローカルホストの名前がデフォルトとして使用されます。

LDAPサーバポートとルート認証局証明書を指定しなかった場合は、ポート389がデフォルトで使用されます。

LDAPサーバポートを指定せずにルート認証局証明書を指定した場合は、ポート636がデフォルトで使用されます。

この拡張を追加するには次のように入力します。

```
krbldapconfig -i -D cn=admin,o=org -w password -h ldapserver -p 389
```

削除するには次のように入力します。

```
krbldapconfig -u -D cn=admin,o=org -w password -h ldapserver -p 389
```

重要: インストールによる変更を有効にするには、LDAPサーバを手動でリフレッシュする必要があります。詳細については、406 ページの「LDAPサーバをリフレッシュする」を参照してください。

ルート認証局証明書のエクスポート

1 iManagerで、［**ディレクトリ管理**］>［**オブジェクトの変更**］の順にクリックして、［オブジェクトの変更］ページを開きます。
2 ［オブジェクトセレクタ］を使用して、サーバのサーバ証明書オブジェクトを選択します。
3 **OK**をクリックします。
4 ［**証明書**］タブをクリックし、［**ルート認証局の証明書**］を選択して証明書の詳細を表示します。
5 **エクスポート**をクリックします。
6 ［**証明書**］ドロップダウンメニューをクリックして、エクスポートする証明書を選択します。
7 秘密鍵をエクスポートするかどうかを指定します。秘密鍵をエクスポートする場合、秘密鍵を保護するためのパスワードを指定する必要があります。
8 **次へ**をクリックします。
9 ［**Save the exported certificate**］をクリックします。
10 ［**Save File (ファイルの保存)**］をクリックします。
11 **閉じる**をクリックします。

SASL-GSSAPIメソッドの設定

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。Kerberos管理に使用するLDAPサーバのSSLルート認証局証明書をiManagerに追加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 Administration Guide (NetIQ iManager 2.7管理ガイド)* (https://www.netiq.com/documentation/imanager/imanager_admin/data/bookinfo.html)』を参照してください。
2 次の手順を順序どおりに実行します。
   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 LDAPサービスプリンシパルを作成する。
   2d 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。
   2e eDirectoryでサービスプリンシパルオブジェクトを作成する。
   2f 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。

SASL-GSSAPIメソッドを使用して設定されたeDirectoryツリーをマージする

ツリーのどちらか一方または両方がSASL-GSSAPIメソッドを使用して設定された2つのツリーをマージする場合は、ソースツリーにあるすべてのKerberosオブジェクトをターゲットツリー内で手動で作成する必要があります。

SASL-GSSAPIメソッドの管理

iManagerでは、Kerberosに関する次の操作を実行できます。

- 866 ページの 「Kerberosスキーマの拡張」
- 866 ページの 「Kerberosレルムオブジェクトの管理」
- 868 ページの 「サービスプリンシパルの管理」
- 872 ページの 「外部プリンシパルの編集」
- 872 ページの 「MIT Kerberos KDCでeDirectoryをバックエンドとして使用する場合の、SASL GSSAPI認証の設定」

Kerberosスキーマの拡張

この作業を行うと、Kerberosのオブジェクトクラスと属性定義を使用してeDirectoryスキーマを拡張できます。

1 スキーマがまだ拡張されていない場合は、［**OK**］をクリックしてスキーマを拡張します。

2 iManagerで、［**Kerberos管理**］>［**スキーマの拡張**］の順にクリックして、［スキーマの拡張］ページを開きます。

スキーマが既に拡張されている場合は、ステータスと一緒にメッセージが表示されます。

3 **閉じる**をクリックします。

Kerberosレルムオブジェクトの管理

レルムとは、複数のKDC(Key Distribution Center)によって管理される論理ネットワークです。つまり、レルムとは、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です。慣例的に、レルム名はすべて大文字で記述され、インターネットドメインと区別されます。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。

このセクションでは次のことについて説明します。

- 866 ページの 「新しいレルムオブジェクトの作成」
- 867 ページの 「レルムオブジェクトの編集」
- 868 ページの 「レルムオブジェクトの削除」

新しいレルムオブジェクトの作成

サポートされているデフォルトの暗号化タイプはDES-CBC-CRCです。

1 iManagerで、［**Kerberos管理**］>［**レルムの新規作成**］の順にクリックして、［レルムの新規作成］ページを開きます。

2 作成するケルベロスレルムの名前を指定します。

レルム名は、このログインメソッドを設定する際に指定するレルム名と一致している必要があり、RFC 1510の命名規則に準拠している必要があります。

3 レルムのマスタパスワードを指定して、パスワードを確認します。

注: マスタパスワードには必ず強力なパスワードを使用してください。

4 Kerberosレルムに設定するサブツリーおよびプリンシパルコンテナ参照を指定するか、［**オブジェクトセレクタ**］アイコンを使用してそれらを選択します。

これは、このレルムのeDirectoryサービスプリンシパルを格納するサブツリーまたはコンテナのFDNです。このサブツリーはユーザプリンシパルには適用できません。

5 サブツリー検索の範囲を次のように指定します。

- **1レベル**:レルムサブツリーの直下を検索します。
- **サブツリー**:レルムサブツリー以下のサブツリー全体を検索します。

6 **OK**をクリックします。

注: SASL-GSSAPIでは［**KDCサービス**］ボックスは使用しません。

注: eDirectoryコンテナ管理者がLDAP SASL GSSAPI認証用のKerberosレルムをツリーに設定する必要がある場合、ツリー管理者は次の手順を実行する必要があります。

1. セキュリティコンテナオブジェクト(cn=security)にオブジェクトクラスのkrbContainerRefAuxが含まれており、krbContainerReference属性がKerberosコンテナに設定されていることを確認します。
2. コンテナ管理者にkrbContainerReference属性に対する読み込みアクセス権を付与します。
3. Kerberosコンテナの下にレルムコンテナを作成します。コンテナの名前は作成する新規レルムの名前と同じにする必要があり、オブジェクトクラスはkrbRealmContainerにする必要があります。
4. コンテナ管理者にレルムコンテナに対するスーパバイザ権を付与します。

iManagerにコンテナ管理者としてログインし、［**Kerberos管理**］>［**マスタキーの設定**］の順に選択して［マスタキーの設定］ページを開きます。［**MITKDCRealm**］を選択して、マスタパスワードを指定します。

レルムオブジェクトの編集

1 iManagerで、［**Kerberos管理**］>［**レルムの編集**］の順にクリックして、［レルムの編集］ページを開きます。

2 編集するKerberosレルムの名前を指定するか、［**オブジェクトセレクタ**］アイコンを使用してKerberosレルムを選択します。

3 **OK**をクリックします。

4 Kerberosレルムに設定するサブツリーを指定するか、［**オブジェクトセレクタ**］アイコンを使用してサブツリーを選択します。

これは、このレルムのeDirectoryサービスプリンシパルを格納するサブツリーまたはコンテナのFDNです。このサブツリーはユーザプリンシパルには適用できません。

5 サブツリー検索のスコープを指定します。

- **1レベル**:レルムサブツリーの直下を検索します。
- **サブツリー**:レルムサブツリー以下のサブツリー全体を検索します。

6 OKをクリックします。

7 (オプション)別のレルムを編集するには、［タスクの繰り返し］をクリックします。

注: SASL-GSSAPIでは［KDCサービス］ボックスは使用しません。

レルムオブジェクトの削除

1 iManagerで、［Kerberos管理］>［レルムの削除］の順にクリックして、［レルムの削除］ページを開きます。

2 削除するレルムを選択します。

複数のレルムを選択するには、<Shift>キーを押しながらレルムを選択するか、<Shift>キーを押しながら矢印キーを押します。

3 OKをクリックします。

4 もう一度［OK］をクリックして削除操作を確定するか、［キャンセル］をクリックして削除操作をキャンセルします。

重要: レルムオブジェクトを削除すると、そのレルムにあるすべてのサービスプリンシパルオブジェクトが削除されます。

サービスプリンシパルの管理

このセクションでは次のことについて説明します。

LDAPサーバ用のサービスプリンシパルの作成

KDCに付属するKerberos管理ツールを使用して、暗号化タイプとsaltタイプをそれぞれAES256-CTSとNormalに設定してeDirectoryサービスプリンシパルを作成します。

プリンシパルの名前は、ldap/*MYHOST.MYDNSDOMAIN@REALMNAME*の形式にする必要があります。

MIT KDCを使用している場合は、次のようなコマンドを実行します。

kadmin:addprinc -randkey -e aes256-cts:normal ldap/server.novell.com@MITREALM

重要: 作成したサービスプリンシパルのホスト名は、小文字でなければなりません。ホスト名が大文字の場合、認証は失敗します。たとえば、ホスト名が「myHost.com」の場合、LDAPサービスプリンシパルのホスト名の構文は、ldap/myhost.com@<realmname>のようになります。

ベストプラクティス

- すべてのキーのタイプをAES256にすることをお勧めします。
- LDAPサービスプリンシパルキーを定期的に変更します。LDAPサービスプリンシパルキーを変更した場合は、必ずeDirectory内のプリンシパルオブジェクトを更新してください。

eDirectory用のサービスプリンシパルキーの抽出

KDCに付属するKerberos管理ツールを使用して、868ページの「LDAPサーバ用のサービスプリンシパルの作成」で作成したLDAPサービスプリンシパルのキーを抽出し、ローカルファイルシステムに保存します。この作業を行うには、Kerberos管理者の協力が必要です。

MIT KDCを使用している場合は、次のようなコマンドを実行します。

kadmin: ktadd -k */directory_path/keytabfilename* -e aes256-cts:normal ldap/server.novell.com@MITREALM

Microsoft KDCを使用している場合は、たとえばActive DirectoryでldapMYHOSTというユーザを作成してから、次のコマンドを実行します。

ktpass -princ ldap/MYHOST.MYDNSDOMAIN@MYREALM -mapuser ldapMYHOST -pass *mypassword* -out *MYHOST.keytab*

このコマンドを実行すると、プリンシパル(ldap/MYHOST.MYDNSDOMAIN@MYREALM)がユーザアカウント(ldapMYHOST)にマップされ、ホストプリンシパルのパスワードがmypasswordに設定され、MYHOST.keytabファイルに鍵が抽出されます。

eDirectoryでのサービスプリンシパルオブジェクトの作成

で指定した名前を使用してKerberosサービスプリンシパル(ldap/*MYHOST.MYDNSDOMAIN@MYREALM*)を作成する必要があります。868 ページの 「LDAPサーバ用のサービスプリンシパルの作成」

ベストプラクティス

eDirectory用のサービスプリンシパルは、SASL GSSAPIメカニズムを使用できるすべてのサーバからいつでもアクセスできるようになっている必要があります。セキュリティコンテナ内のKerberosレルムコンテナの下にこれらのeDirectoryサービスプリンシパルを作成しない場合は、これらのeDirectoryサービスプリンシパルを含むコンテナを独立したパーティションとして作成し、そのコンテナを広範囲で複製することをお勧めします。

1. iManagerで、［**Kerberos管理**］>［**プリンシパルの新規作成**］の順にクリックして、［プリンシパルの新規作成］ページを開きます。
2. 作成するプリンシパルの名前を指定します。

   プリンシパルの名前は、ldap/*MYDNSDOMAIN@REALMNAME*の形式にする必要があります。
3. プリンシパルオブジェクトを作成するコンテナの名前を指定するか、［**オブジェクトセレクタ**］アイコンを使用してコンテナを選択します。
4. レルムの名前を指定します。

   ステップ 2でレルムの名前を指定した場合は、このフィールドを空白のままにします。
5. 次のいずれかを実行します:
   - keytabファイル名を指定するか、［**参照**］をクリックしてkeytabファイルが保存されている場所を選択します。

このファイルには、869 ページの 「eDirectory用のサービスプリンシパルキーの抽出」で抽出されたキーが保存されています。

- パスワードを指定して確定し、暗号化タイプとソルトタイプの組み合わせを選択します。

  パスワードと暗号化/ソルトタイプの組み合わせは、KDCデータベース内のサービスプリンシパルを作成したときに指定した組み合わせと一致させる必要があります。

6 **OK**をクリックします。

Kerberosサービスのプリンシパルキーの表示

1 iManagerで、［**Kerberos管理**］>［**キー情報の表示**］の順にクリックして、［View Principal Keys］ページを開きます。

2 表示するプリンシパルキーの名前を指定するか、［**オブジェクトセレクタ**］アイコンを使用してプリンシパルキーを選択します。

プリンシパルキーについて次の情報が表示されます。

- プリンシパル名
- 鍵情報
  - 番号:キーテーブル内の鍵のシリアル番号
  - バージョン:キーのバージョン
  - キータイプ:このプリンシパルキーのタイプ
  - Saltタイプ:このプリンシパルキーのSaltタイプ

3 **OK**をクリックします。

Kerberosサービスのプリンシパルオブジェクトの削除

1つまたは複数のオブジェクトを削除できます。また、削除するプリンシパルオブジェクトの高度な選択を行えます。

単一のプリンシパルオブジェクトを削除する

1 iManagerで、［**Kerberos管理**］>［**プリンシパルの削除**］の順にクリックして、［プリンシパルの削除］ページを開きます。

2 ［**単一オブジェクトの選択**］をクリックします。

3 削除するプリンシパルオブジェクトの名前を指定するか、［**オブジェクトセレクタ**］アイコンを使用してプリンシパルオブジェクトを選択します。

4 **OK**をクリックします。

5 もう一度［**OK**］をクリックして削除操作を確定するか、［**キャンセル**］をクリックして削除操作をキャンセルします。

複数のオブジェクトを削除するには、次の操作を実行します。

1 iManagerで、［**Kerberos管理**］>［**プリンシパルの削除**］の順にクリックして、［プリンシパルの削除］ページを開きます。

2 ［**複数オブジェクトの選択**］をクリックします。

3 削除するプリンシパルオブジェクトの名前を指定するか、［**オブジェクトセレクタ**］アイコンを使用してオブジェクトを選択します。

4 削除するプリンシパルを選択します。

5 OKをクリックします。

6 もう一度［OK］をクリックして削除操作を確定するか、［キャンセル］をクリックして削除操作をキャンセルします。

高度な選択方法でプリンシパルオブジェクトを削除するには、次の操作を実行します。

1 iManagerで、［Kerberos管理］>［プリンシパルの削除］の順にクリックして、［プリンシパルの削除］ページを開きます。

2 ［高度な選択］をクリックします。

3 オブジェクトクラスを選択します。

4 プリンシパルオブジェクトが格納されているコンテナを指定するか、［オブジェクトセレクタ］アイコンを使用してコンテナを選択します。

5 ステップ 3で指定したコンテナのサブコンテナも含める場合は、［サブコンテナを含める］をクリックします。

6 ［  ］をクリックして、［高度な選択条件］ウィンドウを開きます。

7 ドロップダウンリストから属性タイプと演算子を選択して、対応する値を入力します。

8 論理グループをさらに選択条件に含めるには、［行の追加  をクリックします。

9 ［OK］をクリックしてフィルタを設定します。

10 ［プレビューの表示］をクリックして、高度な選択のプレビューを表示します。

11 OKをクリックします。

12 もう一度［OK］をクリックして削除操作を確定するか、［キャンセル］をクリックして削除操作をキャンセルします。

Kerberosサービスプリンシパルのパスワードの設定

KDCでeDirectoryサービスのプリンシパルキーがリセットされた場合は、eDirectoryでもそのプリンシパルキーを更新する必要があります。

キーの抽出については、869 ページの 「eDirectory用のサービスプリンシパルキーの抽出」を参照してください。

1 iManagerで、［Kerberos管理］>［プリンシパルパスワードの設定］の順にクリックして、［プリンシパルパスワードの設定］ページを開きます。

2 個別にパスワードを設定する必要があるプリンシパルオブジェクトの名前を指定するか、［オブジェクトセレクタ］アイコンを使用してプリンシパルオブジェクトを選択します。

3 keytabファイル名を指定するか、［参照］をクリックしてkeytabファイルが保存されている場所をブラウズします。

4 次のいずれかを実行します:

- プリンシパルキーが含まれているkeytabファイルの名前を指定するか、［参照］をクリックしてkeytabファイルが格納されている場所を選択します。

サービスプリンシパルの作成およびキーの抽出の詳細については、868 ページの「LDAPサーバ用のサービスプリンシパルの作成」および869 ページの 「eDirectory用のサービスプリンシパルキーの抽出」を参照してください。

- パスワードを指定して確定し、暗号化タイプとソルトタイプの組み合わせを選択します。

5 ［OK］をクリックしてパスワードを設定します。

6 (オプション)別のプリンシパルのパスワードを設定するには、［タスクの繰り返し］をクリックします。

外部プリンシパルの編集

iManagerを使用して、Kerberosプリンシパル名をeDirectoryに追加できます。

1 iManagerで、［Kerberos管理］>［外部プリンシパルの編集］の順にクリックして、［外部プリンシパルの編集］ページを開きます。

2 有効なユーザオブジェクトのFDNを指定するか、［オブジェクトセレクタ］アイコンを使用してユーザオブジェクト参照を選択します。

3 OKをクリックします。

4 外部プリンシパル名を指定して、［追加  をクリックします。

プリンシパル名は、principalname@*REALMNAME*の形式にする必要があります。

外部プリンシパル名を削除するには、名前を選択して、［削除  をクリックします。

5 OKをクリックします。

注: Kerberosのプリンシパル名は、ツリー内で固有にする必要があります。eDirectoryをKDCレルムへのLDAPバックエンドとして設定する場合、外部プリンシパル名をそのレルムのeDirectoryに設定しないでください。代わりに、次のコマンドを使用して、既存のKerberosプリンシパル名をeDirectoryのユーザDNに関連付けることができます。

kadmin.local -q 'modprinc -x linkdn=<eDir DN> <principal>@<realm>'

Kerberosプリンシパル名は、プリンシパルの作成時に次のコマンドのいずれかを使用して、eDirectoryのユーザDNに関連付けることもできます。

kadmin.local -q 'ank -x dn=<eDir DN> <principal>@<realm>'

kadmin.local -q 'ank -x linkdn=<eDir DN> <principal>@<realm>'

MITKerberosKDCでeDirectoryをバックエンドとして使用する場合の、SASL GSSAPI認証の設定

MITKerberosKDCでeDirectoryをバックエンドとして使用する場合に、SASLGSSAPIを使用してMIT KDCプリンシパルにeDirectoryから認証を受けることができるようにするには、MIT KDCの設定後に次の手順を実行します。

1 iManagerで、セキュリティコンテナオブジェクト(cn=security)を次のように編集します。

1a オブジェクトクラスのkrbContainerRefAuxをセキュリティコンテナに追加します。

1b krbContainerReference属性をKerberosのコンテナを指示するように設定します。

次に例を示します。

```
cn=Kerberos,cn=Security
```

2 iManagerで、［**Kerberos管理**］>［**マスタキーの設定**］の順に選択して［マスタキーの設定］ページを開きます。

重要: MIT KDCで使用されるマスタキーを選択します。

3 MIT KDCレルムを選択して、パスワードを指定します。このパスワードは、kdb5_ldap_utilを使用してそのMITKDCレルムを作成した際にマスタパスワードとして使用したパスワードです。

注: Kerberosレルムがツリー管理者ではないユーザによって作成されている場合、ツリー管理者はKerberosコンテナに対するエントリの作成権をそのユーザに付与する必要があります。

ログインシーケンスの作成

ログインシーケンスの作成については、669 ページの 「ログインとポストログインのメソッドとシーケンスの管理」を参照してください。

LDAPでのSASL-GSSAPIの使用方法

SASL-GSSAPIをインストールすると、SASL-GSSAPIが他のSASL方式と共にrootDSEのsupportedSASLMechanisms属性に追加されます。

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SASLGSSAPI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
```

エラーメッセージ

SASL-GSSAPIのエラーメッセージは次の場所に記録されます。

- Linuxの場合: ndsd.log

詳細については、968 ページの 「eDirectory のエラーログを管理する」を参照してください。

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 E-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。

F セキュリティ上の考慮事項

この付録では、次のトピックについて説明します。

LDAPバインド

LDAPバインドは、安全な接続を使用して実行してください。常にSSL/TLS接続を使用し、次の考慮事項に留意することをお勧めします。

- 回線上で転送されたキーが見破られることがあります。したがって、企業ネットワークを傍受またはパケットスニッフィングから物理的に保護する必要があります。
- 権限を持つ担当者のみが物理的にアクセスできる安全な場所にサーバを配置する必要があります。
- 企業のファイアウォールの外でユーザがこの製品を使用する場合は、VPNを使用する必要があります。
- サーバが企業ネットワークの外部からアクセスできる場合は、サーバへの直接アクセスを防ぐためにファイアウォールを設定する必要があります。
- 監視ログを定期的に確認する必要があります。
- 異なる管理任務を、別々の個人に割り当てる必要があります。管理の委任では、ディレクトリオブジェクトをきめ細かく制御できます。
- Kerberosの管理には特定のLDAPサーバを正しいサーバとして指定することをお勧めします。サーバ名はiManagerで指定できます。

重要: ユーザはサーバのIPアドレスではなく、DNS名を使用してLDAPサーバにアクセスする必要があります。これは、IPアドレスからDNS名への変換が保護されていないためです。

Nessusのスキャン結果

Nessusのポートスキャンによって、次の脆弱性が報告されました。

• 正しく設定されていないLDAPサーバによって、ユーザがそのLDAPサーバに接続して情報を問い合わせることができる

説明: eDirectory LDAPサーバでは、Nullバインドがデフォルトで有効になっていますが、そのサーバ上で無効にすることができます。サーバのセキュリティを向上させるには、LDAPサーバのポート389に対してNULLバインドを無効にします。詳細については、393 ページの 「LDAPオブジェクトを環境設定する」を参照してください。

解決策: Nullバインドをサーバで無効にしてください。

- **正しく設定されていないLDAPサーバによって、ディレクトリベースがNullで設定される**

  説明: ディレクトリ構造の事前の知識がなくても情報を取得することができます。匿名ユーザは、Nullバインドを利用して「LdapMiner」などのツールによってLDAPサーバに問い合わせることができます。

  解決策: この状態が発生しないようにする方法はありませんが、このようなセキュリティ上の脅威は、Nullバインドを無効にすることによって最小限に抑えることができます。

- **リモートサービスで弱いSSL暗号スイートの使用がサポートされている**

  説明: リモートホストで弱い暗号化を提供しているか、または暗号化をまったく提供していないSSL暗号の使用がサポートされています。

  解決策: 影響を受けるアプリケーションで弱い暗号を使用しないように再設定してください(可能な場合)。

- **リモートのディレクトリサーバで情報が漏洩されている**

  説明: このホストはNetIQ eDirectoryサーバで、PUBLICオブジェクトに対するブラウズ権限を保持しています。

  解決策: eDirectoryを使用するアプリケーションがPUBLIC権利の保持に依存しない場合、PUBLICに与えられる権利を認証済みユーザ(ROOT)のみに割り当ててください。これが外部システムの場合は、インターネットからのポート524へのアクセスをブロックすることをお勧めします。ただし、パブリックブラウズ権を削除しても、ツリーおよびサーバ名にはアクセスできます。

- **SSL証明書が不明な認証局で署名されている**

  説明: リモートホストのX.509認定が、よく知られているパブリック認証局によって署名されていません。リモートホストが実稼働中の公開ホストの場合、これによりSSLの使用が無効にされます。これは、誰でもがその通信の途中で接続を確立してリモートホストに対して攻撃できるためです。

  解決策: この状態は、そのサーバの証明書に署名した認証局の証明書が、クライアントアプリケーションの信頼された証明書ストアにない場合に発生します。そのサーバに対してよく知られている認証局から証明書を購入し、その証明書を展開します。また、そのサーバの証明書がツリーの組織の認証局、あるいは外部またはサードパーティの認証局から発行されていた場合は、アプリケーションの信頼された証明書ストアに、その認証局の証明書をインポートまたは追加します。

  詳細については、703 ページの 「使用する認証局のタイプの決定」を参照してください。

G Kerberosパスワードエージェントの設定

MIT Kerberosのキー配布センター(KDC)は、Kerberosプリンシパルを格納するためにeDirectoryを使用するように設定できます。Kerberosプリンシパルはeディレクトリユーザに関連付けられ、各Kerberosプリンシパルには KDCによって要求されるKerberosキーが保持されます。これらのキーはユーザのKerberosパスワードから取得され、ユーザのeDirectoryパスワードとは異なる場合があります。

Kerberosパスワードエージェント(KPA)は、eDirectoryサーバ内でロードできるモジュールです。KPAでは、ユーザのKerberosキーをeDirectoryパスワードと同期します。

ユニバーサルパスワードの詳細については、771ページの第26章「パスワードを管理する」を参照してください。

Kerberosパスワードを設定するための前提条件

- ❒ MIT Kerberos KDCは、そのプリンシパルを格納するためにeDirectoryを使用するように設定する必要があります。

  Kerberosの設定方法の詳細については、866 ページの 「Kerberosスキーマの拡張」および「*MIT Kerberos Documentation*」を参照してください。

- ❒ Kerberosプリンシパルを関連付けたeDirectoryユーザに対して、ユニバーサルパスワードを有効にする必要があります。

  ユニバーサルパスワードを有効にする方法の詳細については、『*NetIQ Password Management Administration Guide (NetIQ Password Management管理ガイド)* (https://www.netiq.com/documentation/edir88/pwm_administration88/data/bookinfo.html)』の「Deploying Universal Password (ユニバーサルパスワードの展開)」セクションを参照してください。

Kerberosレルムに対するKPA機能の有効化

1. NetIQ iManagerで、［**役割およびタスク**］ボタンをクリックします。
2. ［**Kerberos管理**］>［**レルムの編集**］の順にクリックします。
3. オブジェクトセレクタを使用して、レルムコンテナオブジェクトをブラウズして選択します。
4. ［レルムの編集］ウィンドウで、［**ユニバーサルパスポートを使用する**］を選択します。

詳細については、iManagerのオンラインヘルプを参照してください。

注: 新規プリンシパルを追加すると、Kerberosパスワードとユニバーサルパスワードは同期されません。Kerberosキーは、プリンシパルの追加時に指定したパスワードから生成されます。Kerberosパスワードをユニバーサルパスワードと同じにするには、プリンシパルの作成後にユーザのユニバーサルパスワードを変更します。ユニバーサルパスワードは、eDirectoryで設定または変更できます。

Kerberosパスワードエージェント

KPAをインストールして、パスワードの変更を実行するeDirectoryサーバにロードする必要があります。

KPAを開始するには、「kpa -l」と入力します。

KPAを停止するには、「kpa -u」と入力します。

Miscタグがndstraceで有効にされると、パスワードエージェントによって記録されたメッセージが表示されます。このメッセージは、eDirectoryサーバに設定されているログファイルにも記録されます。

重要: マシンまたはeDirectoryが再起動された場合、Kerberosパスワードエージェントは自動的にはロードされません。Kerberosパスワードエージェントは、手動でロードする必要があります。

キーの生成

ユニバーサルパスワードからKerberosキーを生成するために、Kerberosパスワードエージェントによって使用される暗号化タイプとSaltタイプは、次のものに基づいています。

- プリンシパルにKerberosキーがある場合、既存キーの生成に使用された暗号化タイプとSaltタイプが、ユニバーサルパスワードから新しいキーを生成するために使用されます。
- プリンシパルでKerberosパスワードが設定されなかった場合、レルムに設定されたデフォルトの暗号化タイプとSaltタイプが鍵の生成に使用されます。

レルムに対してデフォルトのキータイプが設定されていない場合、使用されるキータイプは、DES3-HMAC-SHAI:NORMALおよびDES-CBC-CRC:NORMALです。

サポートされる暗号化タイプとSaltタイプを次に示します。

暗号化タイプ

- DES-CBC-CRC:CRC-32を使用したDES CBCモード
- DES-CBC-MD4:RSA-MD4を使用したDES CBCモード
- DES-CBC-MD5:RSA-MD5を使用したDES CBCモード
- DES3-CBC-SHA1-KD:HMAC/sha1を使用したTriple DES CBC モード
- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- RC4-HMAC

Saltタイプ

- normal: Kerberosバージョン5のデフォルト
- v4: Kerberosバージョン4で使用される唯一のタイプ。Saltなし
- norealm: デフォルトと同じ。レルム情報の使用なし
- onlyrealm: Saltとしてレルム情報のみを使用
- special 非常に特殊なケースでのみ使用。完全にはサポートされていない

ユニバーサルパスワードに関する考慮事項

- ユニバーサルパスワードが有効になっている場合、プリンシパルのパスワードの変更中は、ユニバーサルパスワードを設定するためのrandkeyオプションは使用できません。
- あるユーザオブジェクトに関連付けられているプリンシパルのパスワードを設定すると、ユニバーサルパスワードが有効になっていて、そのユーザオブジェクトに関連付けられているプリンシパルすべてのKerberosパスワードとして、そのユニバーサルパスワードが設定されます。
- ユニバーサルパスワードが有効になっている場合、コンピュータまたはeDirectoryが再起動されるたびに、Kerberosパスワードエージェントモジュールをロードする必要があります。
- KPAでは、パスワードに拡張文字はサポートされていません。Kerberosパスワードがユニバーサルパスワードと統合されている場合、ユニバーサルパスワードも拡張文字を含むことはできません。

H eDirectoryイベントとXDASイベントのマッピング

このセクションでは、次の情報について説明します。

- 881 ページの 「eDirectoryイベントとXDASイベントのマッピング」
- 890 ページの 「XDASイベント」

eDirectoryイベントとXDASイベントのマッピング

表 H-1は、対応するXDASイベントにマッピングされたeDirectoryの内部イベントを一覧で示しています。各eDirectoryイベントとそれらの説明については、eDirectoryサービスのページを参照してください。XDASイベントについては、「890 ページの 「XDASイベント」」を参照してください。

注:

- eDirectory 9.0 SP3以降は、XDASイベント用のSentinel分類に従います。詳細については、https://www.novell.com/developer/plugin-sdk/sentinel_taxonomy.htmlを参照してください。
- XDAS環境設定ページを使用して、NMASとeDirectoryの両方のイベントを設定できます。詳細については、619 ページの 「XDASを使用した監査」を参照してください。
- eDirectoryコレクタを使用して、eDirectoryとNMASの両方のイベントを監視します。NMASコレクタは、プラットフォームエージェントでのみ必要です。

表 H-1 *eDirectoryイベントと対応付けられたXDASイベント*

XDASイベント	eDirectoryイベント
CREATE_ACCOUNT	DSE_CREATE_ENTRY
このイベントの例については、892 ページの 「アカウントの作成」を参照してください。	DSE_ADD_ENTRY
DELETE_ACCOUNT	DSE_REMOVE_ENTRY
このイベントの例については、893 ページの 「アカウントを削除する」を参照してください。	
ENABLE_ACCOUNT	DSE_ADD_VALUE
このイベントの例については、894 ページの 「アカウントを有効にする」を参照してください。	
DISABLE_ACCOUNT	DSE_ADD_VALUE
このイベントの例については、894 ページの 「アカウントを無効にする」を参照してください。	

XDASイベント	eDirectoryイベント
QUERY_ACCOUNT このイベントの例については、894 ページの 「アカウントを問い合わせる」を参照してください。	DSE_INSPECT_ENTRY DSE_LIST_SUBORDINATES DSE_READ_REFERENCES DSE_SEARCH DSE_REFERRAL DSE_COMPARE_ATTR_VALUE DSE_READ_ATTR DSE_STREAM
MODIFY_ACCOUNT このイベントの例については、895 ページの 「アカウントを変更する」を参照してください。	DSE_ADD_VALUE DSE_MOVE_SOURCE_ENTRY DSE_DELETE_VALUE DSE_MOVE_SUBTREE DSE_MERGE_ENTRIES DSE_MOVE_DEST_ENTRY DSE_MUTATE_ENTRY DSE_RENAME_ENTRY DSE_ADD_PROPERTY DSE_MODIFY_ENTRY DSE_DELETE_PROPERTY DSE_RESEND_ENTRY DSE_CREATE_BACKLINK DSE_REMOVE_BACKLINK
CREATE_TRUST このイベントの例については、896 ページの 「トラストの作成」を参照してください。	DSE_CREATE_ENTRY DSE_ADD_ENTRY
DELETE_TRUST このイベントの例については、897 ページの 「トラストの削除」を参照してください。	DSE_REMOVE_ENTRY

XDASイベント	eDirectoryイベント
QUERY_TRUST	DSE_INSPECT_ENTRY
このイベントの例については、897 ページの 「トラストの照会」を参照してください。	DSE_SEARCH
	DSE_LIST_SUBORDINATES
	DSE_READ_REFERENCES
	DSE_REFERRAL
	DSE_COMPARE_ATTR_VALUE
	DSE_READ_ATTR
	DSE_STREAM
MODIFY_TRUST	DSE_MOVE_SUBTREE
このイベントの例については、897 ページの 「トラストの変更」を参照してください。	DSE_MERGE_ENTRIES
	DSE_RENAME_ENTRY
	DSE_MOVE_SOURCE_ENTRY
	DSE_MOVE_DEST_ENTRY
	DSE_MUTATE_ENTRY
	DSE_ADD_VALUE
	DSE_ADD_PROPERTY
	DSE_DELETE_VALUE
	DSE_DELETE_PROPERTY
	DSE_RESEND_ENTRY
	DSE_CREATE_BACKLINK
	DSE_REMOVE_BACKLINK
	DSE_MODIFY_ENTRY
CREATE_DATA_ITEM	DSE_CREATE_ENTRY
このイベントの例については、899 ページの 「データ項目の作成」を参照してください。	DSE_ADD_ENTRY
	DSE_ADD_REPLICA
	DSE_DEFINE_ATTR_DEF
	DSE_DEFINE_CLASS_DEF
DELETE_DATA_ITEM	DSE_REMOVE_ENTRY
このイベントの例については、900 ページの 「データ項目の削除」を参照してください。	DSE_REMOVE_REPLICA
	DSE_REMOVE_CLASS_DEF
	DSE_REMOVE_ATTR_DEF

XDASイベント	eDirectoryイベント
QUERY_DATA_ITEM_ATTRIBUTE このイベントの例については、900 ページの 「データ項目の属性の問い合わせ」を参照してください。	DSE_DSA_READ DSE_INSPECT_ENTRY DSE_SEARCH DSE_LIST_PARTITIONS DSE_LIST_CONT_CLASSES DSE_LIST_SUBORDINATES DSE_READ_REFERENCES DSE_REFERRAL DSE_COMPARE_ATTR_VALUE DSE_READ_ATTR DSE_STREAM

XDASイベント	eDirectoryイベント
MODIFY_DATA_ITEM_ATTRIBUTE	DSE_UPDATE_SCHEMA
このイベントの例については、900 ページの 「データ項目の属性の変更」を参照してください。	DSE_CHANGE_TREE_NAME
	DSE_MOVE_SUBTREE
	DSE_MOVE_TREE
	DSE_MERGE_ENTRIES
	DSE_RENAME_ENTRY
	DSE_MOVE_SOURCE_ENTRY
	DSE_MOVE_DEST_ENTRY
	DSE_MUTATE_ENTRY
	DSE_ADD_VALUE
	DSE_REMOVE_BACKLINK
	DSE_ADD_PROPERTY
	DSE_DELETE_VALUE
	DSE_DELETE_PROPERTY
	DSE_UPDATE_CLASS_DEF
	DSE_UPDATE_ATTR_DEF
	DSE_CHANGE_REPLICA_TYPE
	DSE_MODIFY_CLASS_DEF
	DSE_RESEND_ENTRY
	DSE_MERGE_TREE
	DSE_CREATE_SUBREF
	DSE_CREATE_BACKLINK
	DSE_MODIFY_ENTRY
ASSOCIATE_TRUST	DSE_ADD_MEMBER
このイベントの例については、904 ページの 「トラストの関連付け」を参照してください。	DSE_ADD_VALUE
DEASSOCIATE_TRUST	DSE_DELETE_MEMBER
このイベントの例については、905 ページの 「トラストの関連付け解除」を参照してください。	DSE_DELETE_VALUE

XDASイベント	eDirectoryイベント
MODIFY_ACCOUNT_SECURITY_TOKEN このイベントの例については、905 ページの 「アカウントセキュリティトークンの変更」を参照してください。	DSE_CHGPASS DSE_NMAS_LOG_SET_PWD DSE_NMAS_LOG_SET_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_LOGIN_SECRET DSE_NMAS_LOG_SET_LOGIN_SECRET DSE_NMAS_LOG_SET_DIST_PWD DSE_NMAS_LOG_DELETE_DIST_PWD DSE_NMAS_LOG_DELETE_PWD DSE_NMAS_LOG_CHANGE_PWD DSE_NMAS_LOG_DELETE_ALL_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_ALL_LOGIN_SECRET
QUERY_ACCOUNT_SECURITY_TOKEN このイベントの例については、905 ページの 「アカウントセキュリティトークンの照会」を参照してください。	DSE_NMAS_LOG_GET_LOGIN_CONFIG DSE_NMAS_LOG_GET_PWD_STATUS DSE_NMAS_LOG_GET_DIST_PWD DSE_NMAS_LOG_GET_PWD DSE_NMAS_LOG_GET_PWD_HISTORY DSE_NMAS_LOG_GET_ALL_LOGIN_CONFIG DSE_NMAS_LOG_GET_ALL_LOGIN_SECRET DSE_NMAS_LOG_CHECK_PWD_SYNTAX_POLICY
CREATE_CONNECTION このイベントの例については、906 ページの 「接続の作成」を参照してください。	DSE_CONNECTION
TERMINATE_CONNECTION このイベントの例については、906 ページの 「接続の停止」を参照してください。	DSE_CONNECTION
CREATE_SESSION このイベントの例については、906 ページの 「セッションの作成」を参照してください。	DSE_LOGIN_EX DSE_NMAS_LOG_SRVR_BEGIN_LOGIN DSE_NMAS_LOG_FINISH_LOGIN_STATUS DSE_NMAS_LOG_SASL_MECHANISM_RESULT
TERMINATE_SESSION このイベントの例については、906 ページの 「セッションの停止」を参照してください。	DSE_LOGOUT

XDASイベント	eDirectoryイベント
AUTHENTICATE_SESSION このイベントの例については、907 ページの 「認証セッション」を参照してください。	DSE_AUTHENTICATE DSE_IMPERSONATE DSE_EBA_BA_FAILURE DSE_VERIFY_PASS
GRANT_TRUST_ACCESS このイベントの例については、907 ページの 「トラストアクセスの付与」を参照してください。	DSE_ADD_VALUE
REVOKE_TRUST_ACCESS このイベントの例については、907 ページの 「トラストアクセスを取り消す」を参照してください。	DSE_DELETE_VALUE
INTRUDER_LOCKOUT このイベントの例については、908 ページの 「不正侵入者ロックアウト」を参照してください。	DSE_ADD_VALUE
ACCOUNT_UNLOCK このイベントの例については、908 ページの 「アカウントのロック解除」を参照してください。	DSE_DELETE_VALUE
GRANT_ACCOUNT_ACCESS このイベントの例については、908 ページの 「アカウントアクセスを付与する」を参照してください。	DSE_ADD_VALUE
REVOKE_ACCOUNT_ACCESS このイベントの例については、909 ページの 「アカウントアクセスを取り消す」を参照してください。	DSE_DELETE_VALUE
AUDIT_CONFIG このイベントの例については、909 ページの 「監査の環境設定」を参照してください。	DSE_ADD_VALUE DSE_DELETE_VALUE
ENABLE_SERVICE このイベントの例については、912 ページの 「サービスの有効化」を参照してください。	DSE_CHANGE_MODULE_STATE DSE_NMAS_LOG_PWD_POLICY_AGENT_REG DSE_NMAS_LOG_DIST_PWD_AGENT_REG DSE_NMAS_LOG_PWD_AGENT_REG DSE_NMAS_LOG_LTSS_AGENT_REG DSE_NMAS_LOG_PWD_CHANGE_AGENT_REG

XDASイベント	eDirectoryイベント
DISABLE_SERVICE このイベントの例については、912 ページの 「サービスの無効化」を参照してください。	DSE_CHANGE_MODULE_STATE DSE_REMOTE_SERVER_DOWN DSE_NMAS_LOG_PWD_POLICY_AGENT_DEREG DSE_NMAS_LOG_DIST_PWD_AGENT_DEREG DSE_NMAS_LOG_PWD_AGENT_DEREG DSE_NMAS_LOG_LTSS_AGENT_DEREG DSE_NMAS_LOG_PWD_CHANGE_AGENT_DEREG
INVOKE_SERVICE このイベントの例については、912 ページの 「サービスの起動」を参照してください。	DSE_BACKLINK_PROC_DONE DSE_LIMBER_DONE DSE_MOVE_TREE_START DSE_PURGE_START DSE_RECV_REPLICA_UPDATES DSE_SEND_REPLICA_UPDATES DSE_START_JOIN DSE_START_UPDATE_REPLICA DSE_START_UPDATE_SCHEMA DSE_SYNC_PART_START DSE_SYNC_SVR_OUT_START
TERMINATE_SERVICE このイベントの例については、912 ページの 「サービスの停止」を参照してください。	DSE_REMOVE_ATTR_DEF DSE_ABORT_JOIN DSE_END_UPDATE_REPLICA DSE_END_UPDATE_SCHEMA DSE_JOIN_DONE DSE_MOVE_TREE_END DSE_PURGE_END DSE_SCHEMA_SYNC DSE_SYNC_PART_END DSE_SYNC_SVR_OUT_END

XDASイベント	eDirectoryイベント
MODIFY_SERVICE_CONFIG	DSE_ALLOW_LOGIN
このイベントの例については、913 ページの 「サービスの環境設定の変更」を参照してください。	DSE_UPDATE_REPLICA
	DSE_EBA_MOVE_EBA_CA
	DSE_GEN_CA_KEYS
	DSE_RECERT_PUB_KEY
	DSE_EBA_REQ_BA_MATERIAL
	DSE_EBA_REQ_SERVER_BA_MATERIAL
	DSE_NAME_COLLISION
	DSE_SERVER_RENAME
	DSE_SERVER_ADDRESS_CHANGE
	DSE_SYNC_PARTITION
	DSE_SYNC_SCHEMA
	DSE_EBA_ENABLE_PURE_MODE
	DSE_EBA_ISSUE_NCPCA_CERT
	DSE_EBA_REVOKE_NCPCA_CERT
START_SYSTEM	DSE_AGENT_OPEN_LOCAL
このイベントの例については、915 ページの 「システムの起動」を参照してください。	DSE_RELOAD_DS
SHUTDOWN_SYSTEM	DSE_AGENT_CLOSE_LOCAL
このイベントの例については、915 ページの 「システムのシャットダウン」を参照してください。	
BACKUP_DATA_STORE	DSE_BACKUP_ENTRY
このイベントの例については、915 ページの 「データストアのバックアップ」を参照してください。	
RECOVER_DATA_STORE	DSE_RESTORE_ENTRY
このイベントの例については、915 ページの 「データストアの回復」を参照してください。	

XDASイベント	eDirectoryイベント
INTERNAL_OPERATIONS このイベントの例については、916 ページの 「内部操作」を参照してください。	DSE_CRC_FAILURE DSE_DELETE_SUBTREE DSE_DELETE_UNUSED_EXTREF DSE_DSA_BAD_VERB DSE_LOST_ENTRY DSE_NEW_SCHEMA_EPOCH DSE_NO_REPLICA_PTR DSE_PURGE_ENTRY_FAIL DSE_EBA_ISSUE_CRL
MODIFY_PROCESS_CONTEXT このイベントの例については、916 ページの 「プロセスコンテキストの変更」を参照してください。	DSE_PARTITION_STATE_CHG DSE_LDAP_MODLDAPSERVER DSE_PART_STATE_CHG_REQ DSE_REPAIR_TIME_STAMPS DSE_RESET_DS_COUNTERS DSE_SET_NEW_MASTER DSE_SYNTHETIC_TIME DSE_SPLIT_DONE DSE_SPLIT_PARTITION DSE_JOIN_PARTITIONS DSE_ABORT_PARTITION_OP DSE_LOW_LEVEL_JOIN

XDASイベント

XDASイベントは、次のカテゴリに分類されます。

- 891 ページの 「アカウント管理イベント」
- 895 ページの 「トラスト管理イベント」
- 898 ページの 「データ項目管理イベント」
- 901 ページの 「セキュリティイベント」
- 910 ページの 「サービスまたはアプリケーション管理イベント」
- 913 ページの 「オペレーショナルイベント」

アカウント管理イベント

アカウント管理イベントは、プリンシパルアカウントの管理に適用できます。プリンシパルは、エンドユーザの場合があります。デフォルトでは、構成員、人物、ユーザの各オブジェクトクラスがアカウントにマップされます。

注: アカウントセキュリティトークンの変更イベントは、アカウントの変更の観点から定義することもできましたが、アカウントセキュリティトークンの変更が監査セキュリティに不可欠と考えられるため、それ自体のイベントが与えられます。

***表 H-2** アカウント管理イベントの分類*

イベント名	イベント ID	対応するeDirイベント	説明	使用対象:
アカウントの作成	0.0.0.0	DSE_CREATE_ENTRY DSE_ADD_ENTRY	新規アカウントを作成します	アカウントが作成されると、このイベントが生成されます。
アカウントを削除する	0.0.0.1	DSE_REMOVE_ENTRY	既存のアカウントを削除します	このイベントには、アカウント作成の反対のセマンティック上の意味があります。アカウントが削除されると、このイベントが生成されます。
アカウントを無効にする	0.0.0.2	DSE_ADD_VALUE	既存のアカウントを無効にします	このイベントは、アカウントが管理者または自動セキュリティプロセスによって無効にされると生成され、再度有効にされるまで使用できません。
アカウントを有効にする	0.0.0.3	DSE_ADD_VALUE	既存の無効なアカウントを有効にします	このイベントは、上で定義されているアカウントの無効化イベントと対になるイベントです。
アカウントの問い合わせ	0.0.0.4	DSE_INSPECT_ENTRY DSE_LIST_SUBORDINATES DSE_READ_REFERENCES DSE_SEARCH DSE_REFERRAL DSE_COMPARE_ATTR_VALUE DSE_READ_ATTR DSE_STREAM	既存のアカウントを問い合わせます	このイベントは、特定のアカウントの属性情報が要求されるたびに生成されます。

イベント名	イベントID	対応するeDirイベント	説明	使用対象:
アカウントの変更	0.0.0.5	DSE_ADD_VALUE DSE_MOVE_SOURCE_ENTRY DSE_DELETE_VALUE DSE_MOVE_SUBTREE DSE_MERGE_ENTRIES DSE_MOVE_DEST_ENTRY DSE_MUTATE_ENTRY DSE_RENAME_ENTRY DSE_ADD_PROPERTY DSE_MODIFY_ENTRY DSE_DELETE_PROPERTY DSE_RESEND_ENTRY DSE_CREATE_BACKLINK DSE_REMOVE_BACKLINK	既存のアカウントを変更します	このイベントは、特定のアカウントの属性情報を変更する要求が行われるたびに生成されます。

アカウント管理イベントの例

このセクションでは、次のアカウント管理イベントの例を示します。

- 892 ページの 「アカウントの作成」
- 893 ページの 「アカウントを削除する」
- 894 ページの 「アカウントを無効にする」
- 894 ページの 「アカウントを有効にする」
- 894 ページの 「アカウントを問い合わせる」
- 895 ページの 「アカウントを変更する」

注: 次の各セクションで紹介する例は、参考のためにのみ示しています。

アカウントの作成

［**アカウントの作成**］をクリックして、ユーザアカウントを作成するためのイベントを生成します。JSON形式の次のような出力が生成されます。

```
Mar 15 12:08:35 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:0"}},"Target" : {"Data" : {"ClassName" : "User"},"Account" : {"Domain"
: "TREEUPGRADE","Name" : "CN=user1,O=novell","Id" : "32864"}},"Action" : {"Event" :
{"Id" : "0.0.2.0","Name" : "CREATE_ACCOUNT","CorrelationID" :
"eDirectory#29#87e32af4-e717-4607-a541-f42ae38717e7","SubEvent" :
"DSE_CREATE_ENTRY"},"Time" : {"Offset" : 1489559915},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

前の例は、XML形式では(JSON形式から変換した場合)次のように表示されます。

```
<Source>eDirectory#DS</Source>
  <Observer>
    <Account>
      <Domain>MYTREE</Domain>
      <Name>CN=SLES11-SP2,O=mycom</Name>
    </Account>
    <Entity>
      <SysAddr>100.1.1.2</SysAddr>
      <SysName>SLES11-SP2.my.com</SysName>
    </Entity>
  </Observer>
  <Initiator>
    <Account>
      <Name>CN=admin,O=mycom</Name>
      <Id>32805</Id>
    </Account>
  </Initiator>
  <Target>
    <Data>
      <ClassName>User</ClassName>
      <Name>CN=USER,O=mycom</Name>
    </Data>
  </Target>
  <Action>
    <Event>
      <Id>0.0.2.0</Id>
      <Name>CREATE_ACCOUNT</Name>
      <CorrelationID>eDirectory#25#0ef05b4c-e864-4d4c-f7a9-4c5bf00e64e8</
CorrelationID>
      <SubEvent>DSE_CREATE_ENTRY</SubEvent>
    </Event>
    <Time>
      <Offset>1389173763</Offset>
    </Time>
    <Log>
      <Severity>7</Severity>
    </Log>
    <Outcome>0</Outcome>
    <ExtendedOutcome>0</ExtendedOutcome>
  </Action>
```

アカウントを削除する

［**アカウントの削除**］をクリックして、次の例に示すように、ユーザアカウントの削除に関するイベントを生成します。

```
Mar 13 16:40:50 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,O=novell","Id" : "32872"},"Entity" : {"SysAddr" :
"100.1.2.194:16600"}},"Target" : {"Data" : {"ClassName" : "User","Version" :
"2"},"Account" : {"Domain" : "VLV_MEM","Name" : "CN=user1,O=novell","Id" :
"203366"}},"Action" : {"Event" : {"Id" : "0.0.0.1","Name" :
"DELETE_ACCOUNT","CorrelationID" : "eDirectory#18#f2bb6a04-b1a5-43c2-a990-
046abbf2a5b1","SubEvent" : "DSE_REMOVE_ENTRY"},"Time" : {"Offset" :
1489403450},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

アカウントを無効にする

［**アカウントの無効化**］をクリックして、次の例に示すように、ユーザアカウントを無効にするためのイベントを生成します。

```
Mar 08 17:39:31 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,OU=novell,OU=co,O=in","Id" : "32863"},"Entity" : {"SysAddr" :
"100.1.2.194:39382"}},"Target" : {"Data" : {"Attribute Name" : "Login
Disabled","ClassName" : "User","Version" : "2"},"Account" : {"Domain" : "LNX-TREE-
BUILD101","Name" : "CN=rrrr,OU=novell,OU=co,O=in","Id" : "32906"}},"Action" :
{"Event" : {"Id" : "0.0.0.2","Name" : "DISABLE_ACCOUNT","CorrelationID" :
"eDirectory#91#2a382b1e-9d96-4990-9341-1e2b382a969d","SubEvent" :
"DSE_ADD_VALUE"},"Time" : {"Offset" : 1488974971},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

アカウントを有効にする

［**アカウントの有効化**］をクリックして、次の例に示すように、ユーザアカウントを有効にするためのイベントを生成します。

```
Mar 07 18:13:09 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,OU=novell,OU=co,O=in","Id" : "32863"},"Entity" : {"SysAddr" :
"100.1.2.194:18902"}},"Target" : {"Data" : {"Attribute Name" : "Login
Disabled","ClassName" : "User","Version" : "2"},"Account" : {"Domain" : "LNX-TREE-
BUILD101","Name" : "CN=raghu,OU=novell,OU=co,O=in","Id" : "32893"}},"Action" :
{"Event" : {"Id" : "0.0.0.3","Name" : "ENABLE_ACCOUNT","CorrelationID" :
"eDirectory#72#eecfbf13-9f36-4c09-b468-13bfcfee369f","SubEvent" :
"DSE_ADD_VALUE"},"Time" : {"Offset" : 1488890589},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

アカウントを問い合わせる

［**アカウントの照会**］をクリックして、次の例に示すように、ユーザアカウントを問い合わせるためのイベントを生成します。

```
Mar 06 16:40:00 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,OU=novell,OU=co,O=in","Id" : "32863"},"Entity" : {"SysAddr" :
"100.1.2.194:0"}},"Target" : {"Data" : {"Attribute Name" : "ACL","ClassName" :
"User","Version" : "2"},"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" :
"CN=admin,OU=novell,OU=co,O=in","Id" : "32863"}},"Action" : {"Event" : {"Id" :
"0.0.0.4","Name" : "QUERY_ACCOUNT","CorrelationID" : "eDirectory#59#","SubEvent" :
"DSE_READ_ATTR"},"Time" : {"Offset" : 1488798600},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


アカウントを変更する

［**アカウントの変更**］をクリックして、次の例に示すように、ユーザアカウントの変更に関するイベントを生成します。


```
Mar 07 16:24:45 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-
BUILD101","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr"
: "100.1.2.194:0"}},"Target" : {"Data" : {"Attribute Name" :
"pwdFailureTime","ClassName" : "User","Syntax" : "24","Version" : "2"},"Account" :
{"Domain" : "LNX-TREE-BUILD101","Name" : "CN=admin,OU=novell,OU=co,O=in","Id" :
"32863"}},"Action" : {"Event" : {"Id" : "0.0.0.5","Name" :
"MODIFY_ACCOUNT","CorrelationID" : "eDirectory#0#678d790d-c19f-4364-b821-
0d798d679fc1","SubEvent" : "DSE_DELETE_ATTRIBUTE"},"Time" : {"Offset" :
1488884085},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


トラスト管理イベント

トラスト管理イベントは、トラスト関係を管理するために使用します。トラストは、グループまたは役割を介してインスタンスを生成できます。デフォルトでは、dynamicGroup、dynamicGroupAux、グループ、LDAPグループ、職種の各オブジェクトクラスがトラストにマップされます。

たとえば、ドメインAの識別情報により、ドメインBが管理するサービスに要求を送る場合、2つのドメイン間にトラストの関連付けが必要になります。これをトラスト関係と呼びます。ドメインBに識別情報を設定し、ドメインAの識別情報から送られる要求のプロキシとしてそれが使用されるようにすることにより、トラスト関係を設定します。

表 H-3 *トラスト管理イベントの分類*

イベント名	イベントID	対応するeDirイベント	説明	使用対象:
トラストの作成	0.0.1.0	DSE_CREATE_ENTRY DSE_ADD_ENTRY	トラストの作成。	このイベントは、新しいトラストが作成されると報告されます。
トラストの削除	0.0.1.1	DSE_REMOVE_ENTRY	トラストの削除。	このイベントは、トラストが削除されると報告されます。

イベント名	イベントID	対応するeDirイベント	説明	使用対象:
トラストの照会	0.0.1.2	DSE_INSPECT_ENTRY DSE_SEARCH DSE_LIST_SUBORDINATES DSE_READ_REFERENCES DSE_REFERRAL DSE_COMPARE_ATTR_VALUE DSE_READ_ATTR DSE_STREAM	トラストに関連付けられている属性の要求。	トラストに関連付けられている属性の要求が行われると、このイベントが報告されます。
トラストの変更	0.0.1.3	DSE_MOVE_SUBTREE DSE_MERGE_ENTRIES DSE_RENAME_ENTRY DSE_MOVE_SOURCE_ENTRY DSE_MOVE_DEST_ENTRY DSE_MUTATE_ENTRY DSE_ADD_VALUE DSE_ADD_PROPERTY DSE_DELETE_VALUE DSE_DELETE_PROPERTY DSE_RESEND_ENTRY DSE_CREATE_BACKLINK DSE_REMOVE_BACKLINK DSE_MODIFY_ENTRY	トラストに関連付けられている属性の変更。	トラストに関連付けられている属性に関して変更が行われると、このイベントが報告されます。

トラスト管理イベントの例

次の各セクションに、トラスト管理イベントの例を示します。

- 896 ページの 「トラストの作成」
- 897 ページの 「トラストの削除」
- 897 ページの 「トラストの照会」
- 897 ページの 「トラストの変更」

トラストの作成

［**トラストの作成**］をクリックして、次の例に示すように、新しいトラストが作成された場合にイベントを生成します。

Mar 16 20:56:39 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" : {"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" : {"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" : "100.1.2.194:43936"}},"Target" : {"Data" : {"ClassName" : "LDAP Group","Name" : "CN=LDAP Group - server2,O=novell","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.1.0","Name" : "CREATE_TRUST","CorrelationID" : "eDirectory#41#2a670625-1950-48cf-8abf-2506672a5019","SubEvent" : "DSE_CREATE_ENTRY"},"Time" : {"Offset" : 1489677999},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}

トラストの削除

［**トラストの削除**］をクリックして、次の例に示すように、既存のトラストが削除された場合にイベントを生成します。

Mar 16 22:02:46 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" : {"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" : {"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" : "100.1.2.194:26571"}},"Target" : {"Data" : {"ClassName" : "dynamicGroup","Name" : "CN=group1,O=novell","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.1.1","Name" : "DELETE_TRUST","CorrelationID" : "eDirectory#55#8f230203-1c8f-41f7-8456-0302238f8f1c","SubEvent" : "DSE_REMOVE_ENTRY"},"Time" : {"Offset" : 1489681966},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}

トラストの照会

［**トラストの照会**］をクリックして、次の例に示すように、トラストに関連付けられている属性が要求される場合にイベントを生成します。

Mar 16 16:49:35 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" : {"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" : {"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" : "100.1.2.194:31967"}},"Target" : {"Data" : {"Attribute Name" : "LDAP Allow Clear Text Password","ClassName" : "LDAP Group","Name" : "CN=LDAP Group - SLE12-142,O=novell","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.1.4","Name" : "QUERY_TRUST","CorrelationID" : "eDirectory#46#","SubEvent" : "DSE_READ_ATTR"},"Time" : {"Offset" : 1489663175},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}

トラストの変更

［**トラストの変更**］をクリックして、次の例に示すように、トラストに関連付けられている属性の変更が行われる場合にイベントを生成します。

Mar 16 22:02:46 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" : {"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" : {"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" : "100.1.2.194:26571"}},"Target" : {"Data" : {"Attribute Name" : "Obituary","Attribute Value" : "72061996379406335","ClassName" : "dynamicGroup","Name" : "CN=group1,O=novell","Syntax" : "9","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.1.5","Name" : "MODIFY_TRUST","CorrelationID" : "eDirectory#55#8f230203-1c8f-41f7-8456-0302238f8f1c","SubEvent" : "DSE_DELETE_VALUE"},"Time" : {"Offset" : 1489681966},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}

データ項目管理イベント

このイベントセットは、ドメイン内のデータ項目とリソースエレメントの作成および管理に関連しています。データ項目またはリソースエレメントのタイプは、ドメインによってまったく異なります。デフォルトでは、アカウントやトラストにマップされないオブジェクトクラスは、データ項目にマップされます。

たとえば、オペレーティングシステム内のファイルとディレクトリ、デバイスの特殊なファイル、および共有メモリセグメント、データベース内のテーブルとレコード、電子メールシステム内のメッセージです。データ項目という用語は、このコンテキストで任意のタイプのリソースエレメントを指すために使用されます。

***表 H-4** データ項目管理イベントの分類*

イベント名	イベント ID	対応するeDirイベント	説明	使用対象:
データ項目の作成	0.0.3.0	DSE_CREATE_ENTRY DSE_ADD_ENTRY DSE_ADD_REPLICA DSE_DEFINE_ATTR_DEF DSE_DEFINE_CLASS_DEF	データ項目を作成します	データ項目が作成されるたびに、このイベントが報告されます。
データ項目の削除	0.0.3.1	DSE_REMOVE_ENTRY DSE_REMOVE_REPLICA DSE_REMOVE_CLASS_DEF DSE_REMOVE_ATTR_DEF	データ項目を削除します	このイベントは、セキュリティ関連のデータ項目またはリソースエレメントが削除されるたびに報告されます。
データ項目の属性の照会	0.0.3.2	DSE_DSA_READ DSE_INSPECT_ENTRY DSE_SEARCH DSE_LIST_PARTITIONS DSE_LIST_CONT_CLASSES DSE_LIST_SUBORDINATES DSE_READ_REFERENCES DSE_REFERRAL DSE_COMPARE_ATTR_VALUE DSE_READ_ATTR DSE_STREAM	データ項目に関連付けられた属性の要求。	このイベントは、セキュリティ関連のデータ項目またはリソースエレメント(値、またはデータ項目の属性のいずれか)が照会されるたびに報告されます。

イベント名	イベントID	対応するeDirイベント	説明	使用対象:
データ項目の属性の変更	0.0.3.3	DSE_UPDATE_SCHEMA DSE_CHANGE_TREE_NAME DSE_MOVE_SUBTREE DSE_MOVE_TREE DSE_MERGE_ENTRIES DSE_RENAME_ENTRY DSE_MOVE_SOURCE_ENTRY DSE_MOVE_DEST_ENTRY DSE_MUTATE_ENTRY DSE_ADD_VALUE DSE_REMOVE_BACKLINK DSE_ADD_PROPERTY DSE_DELETE_VALUE DSE_DELETE_PROPERTY DSE_UPDATE_CLASS_DEF DSE_UPDATE_ATTR_DEF DSE_CHANGE_REPLICA_TYPE DSE_MODIFY_CLASS_DEF DSE_RESEND_ENTRY DSE_MERGE_TREE DSE_CREATE_SUBREF DSE_CREATE_BACKLINK DSE_MODIFY_ENTRY	データ項目に関連付けられた属性の変更。	このイベントは、セキュリティ関連のデータ項目またはリソースエレメント(値、またはデータ項目の属性のいずれか)が変更されるたびに報告されます。

データ項目管理イベントの例

次のセクションに、データ項目管理イベントを生成するための例をいくつか示します。

- 899 ページの 「データ項目の作成」
- 900 ページの 「データ項目の削除」
- 900 ページの 「データ項目の属性の問い合わせ」
- 900 ページの 「データ項目の属性の変更」

データ項目の作成

［**データ項目の作成**］をクリックして、次の例に示すように、データ項目を作成するためのイベントを生成します。

Mar 16 20:56:24 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" : {"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" : {"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" : "100.1.2.194:42144"}},"Target" : {"Data" : {"ClassName" : "NCP Server","Name" : "CN=server2,O=novell","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.3.0","Name" : "CREATE_DATA_ITEM","CorrelationID" : "eDirectory#39#7e296d99-d6a7-4206-8f23-996d297ea7d6","SubEvent" : "DSE_CREATE_ENTRY"},"Time" : {"Offset" : 1489677984},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}

データ項目の削除

［**データ項目の削除**］をクリックして、次の例に示すように、データ項目を削除するためのイベントを生成します。

Mar 16 21:46:32 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" : {"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" : {"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" : "100.1.2.194:26571"}},"Target" : {"Data" : {"Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.3.1","Name" : "DELETE_DATA_ITEM","CorrelationID" : "eDirectory#55#9509dc1f-ecf1-4306-8fec-1fdc0995f1ec","SubEvent" : "DSE_REMOVE_ENTRY"},"Time" : {"Offset" : 1489680992},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}

データ項目の属性の問い合わせ

［**データ項目の属性の照会**］をクリックして、次の例に示すように、データ項目の属性を照会するためのイベントを生成します。

Mar 03 14:01:36 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" : {"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" : "SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194:0"}},"Target" : {"Data" : {"Attribute Name" : "EBATreeConfiguration","ClassName" : "Tree Root","Name" : "LNX-TREE-BUILD101","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.3.2","Name" : "QUERY_DATA_ITEM_ATTRIBUTE","CorrelationID" : "eDirectory#0#","SubEvent" : "DSE_READ_ATTR"},"Time" : {"Offset" : 1488529896},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}

データ項目の属性の変更

［**データ項目の属性の変更**］をクリックして、次の例に示すように、データ項目の属性を変更するためのイベントを生成します。

Mar 03 14:05:06 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" : {"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" : "SLES12-194-12"}},"Initiator" : {"Account" : {"Name" : "CN=admin,OU=novell,OU=co,O=in","Id" : "32863"},"Entity" : {"SysAddr" : "100.1.2.194:214"}},"Target" : {"Data" : {"Attribute Name" : "modifiersName","Attribute Value" : "CN=admin,OU=novell,OU=co,O=in","ClassName" : "NCP Server","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in","Syntax" : "3","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.3.3","Name" : "MODIFY_DATA_ITEM_ATTRIBUTE","CorrelationID" : "eDirectory#32#f2dbd583-1f5c-459a-8c37-83d5dbf25c1f","SubEvent" : "DSE_ADD_VALUE"},"Time" : {"Offset" : 1488530106},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}

セキュリティイベント

このイベントセットは、eDirectoryのセキュリティ操作の監査に適用できます。セキュリティ操作には、アクセスの付与や取り消し、ログイン、パスワード変更、照会があります。このイベントセットは、eDirectoryシステムにおける不正侵入者を検出するためにも役立ちます。

***表 H-5** セキュリティイベントの分類*

イベント名	イベントID	対応するeDirectoryイベント	説明	使用対象:
トラストの関連付け	0.0.1.2	DSE_ADD_MEMBER DSE_ADD_VALUE	アカウントにトラストパーミッションを付与する、トラストとのアカウントの関連付け。	このイベントは、新しいトラストの関連付けが作成されると報告されます。たとえば、グループにメンバーを追加する場合。
トラストの関連付け解除	0.0.1.3	DSE_DELETE_MEMBER DSE_DELETE_VALUE	アカウントとトラストの関連付けを解除します。	このイベントは、既存のトラストの関連付けが削除されると報告されます。たとえば、グループからメンバーを削除する場合。
アカウントセキュリティトークンの変更	0.0.0.6	DSE_CHGPASS DSE_NMAS_LOG_SET_PWD DSE_NMAS_LOG_SET_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_LOGIN_SECRET DSE_NMAS_LOG_SET_LOGIN_SECRET DSE_NMAS_LOG_SET_DIST_PWD DSE_NMAS_LOG_DELETE_DIST_PWD DSE_NMAS_LOG_DELETE_PWD DSE_NMAS_LOG_CHANGE_PWD DSE_NMAS_LOG_DELETE_ALL_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_ALL_LOGIN_SECRET	既存のアカウントセキュリティトークンを変更します.	アカウントセキュリティトークンは、パスワード、またはユーザアカウントに関連付けられた、その他のタイプの認証用データの場合があります。この場合、ユーザアカウントとは、ユーザ、アプリケーション、またはシステムサービスが認証を受けるために使用するアカウントで、認証後にそのアカウントの権限を使用して処理するようなアカウントのタイプを意味しています。

イベント名	イベントID	対応するeDirectoryイベント	説明	使用対象:
アカウントセキュリティトークンの照会	0.0.12.3	DSE_NMAS_LOG_GET_LOGIN_CONFIG DSE_NMAS_LOG_GET_PWD_STATUS DSE_NMAS_LOG_GET_DIST_PWD DSE_NMAS_LOG_GET_PWD DSE_NMAS_LOG_GET_PWD_HISTORY DSE_NMAS_LOG_GET_ALL_LOGIN_CONFIG DSE_NMAS_LOG_GET_ALL_LOGIN_SECRET DSE_NMAS_LOG_CHECK_PWD_SYNTAX_POLICY	既存のアカウントセキュリティトークンの要求。	アカウントセキュリティトークンは、パスワード、またはユーザアカウントに関連付けられた、その他のタイプの認証用データの場合があります。この場合、ユーザアカウントとは、ユーザ、アプリケーション、またはシステムサービスが認証を受けるために使用するアカウントで、認証後にそのアカウントの権限を使用して処理するようなアカウントのタイプを意味しています。
接続の作成	0.0.12.4	DSE_CONNECTION	システムコンポーネント間の通信チャネルの作成。	通信チャネルがシステムコンポーネントの間で作成されると、このイベントが報告されます。
接続の停止	0.0.12.5	DSE_CONNECTION	システムコンポーネント間の通信チャネルを閉じます。	既存の通信チャネルがシステムコンポーネントの間で停止すると、このイベントが報告されます。
セッションの作成	0.0.2.0	DSE_LOGIN_EX DSE_NMAS_LOG_SRVR_BEGIN_LOGIN DSE_NMAS_LOG_FINISH_LOGIN_STATUS DSE_NMAS_LOG_SASL_MECHANISM_RESULT	新規セッションを作成します。	このイベントは、新規セッションが作成されるたびに報告される必要があります。たとえば、eDirectoryシステムにログインする場合。

イベント名	イベントID	対応するeDirectoryイベント	説明	使用対象:
セッションの停止	0.0.2.1	DSE_LOGOUT	既存のセッションを終了します。	このイベントは、既存セッション(上で定義した)が終了されるたびに報告される必要があります。たとえば、eDirectoryシステムからログアウトする場合。
認証セッション	0.0.2.4	DSE_AUTHENTICATE DSE_IMPERSONATE DSE_EBA_BA_FAILURE DSE_VERIFY_PASS	新しい識別情報がセッションに関連付けられます。	ユーザがセッションを認証すると、新しい識別情報がそのセッションに関連付けられます。その結果、この識別情報は、保護されたリソースの要求を承認するために使用されます。
トラストアクセスの付与	0.0.1.7	DSE_ADD_VALUE	トラストにオブジェクトへのアクセスを付与します。	オブジェクトへのアクセスがトラストに付与されるときに、このイベントが報告されます。
トラストアクセスの取り消し	0.0.1.8	DSE_DELETE_VALUE	トラストからオブジェクトへのアクセスを取り消します。	リソースに対するアクセスがトラストから削除されるときに、このイベントが報告されます。
不正侵入者ロックアウト	0.0.0.9	DSE_ADD_VALUE	アカウントのロックアウト。	このイベントは、アカウントのロックアウト中に報告されます。
アカウントのロック解除	0.0.0.10	DSE_DELETE_VALUE	ロックされたアカウントのロックを解除します。	ロックされたアカウントがロック解除されると、このイベントが報告されます。
アカウントアクセスを付与する	0.0.0.7	DSE_ADD_VALUE	アカウントにオブジェクトへのアクセスを付与します。	オブジェクトへのアクセスがアカウントに付与されるときに、このイベントが報告されます。

イベント名	イベントID	対応するeDirectoryイベント	説明	使用対象:
アカウントアクセスを取り消し	0.0.0.8	DSE_DELETE_VALUE	アカウントからオブジェクトへのアクセスを取り消します。	アカウントからオブジェクトが削除されたときに、このイベントが報告されます。
監査の環境設定	0.0.9.0	DSE_ADD_VALUE DSE_DELETE_VALUE	監査サービスの操作を制御するパラメータの変更。	監査サービスを制御するパラメータが変更されるたびに、このイベントが報告されます。

セキュリティイベントの例

次の各セクションに、セキュリティイベントの例を示します。

- 904 ページの 「トラストの関連付け」
- 905 ページの 「トラストの関連付け解除」
- 905 ページの 「アカウントセキュリティトークンの変更」
- 905 ページの 「アカウントセキュリティトークンの照会」
- 906 ページの 「接続の作成」
- 906 ページの 「接続の停止」
- 906 ページの 「セッションの作成」
- 906 ページの 「セッションの停止」
- 907 ページの 「認証セッション」
- 907 ページの 「トラストアクセスの付与」
- 907 ページの 「トラストアクセスを取り消す」
- 908 ページの 「不正侵入者ロックアウト」
- 908 ページの 「アカウントのロック解除」
- 908 ページの 「アカウントアクセスを付与する」
- 909 ページの 「アカウントアクセスを取り消す」
- 909 ページの 「監査の環境設定」

トラストの関連付け

［**トラストの関連付け**］をクリックして、次の例に示すように、新しいトラストの関連付けが作成された場合にイベントを生成します。

```
Mar 16 21:57:28 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:26571"}},"Target" : {"Data" : {"Attribute Name" : "Member","Name" :
"CN=group1,O=novell","Syntax" : "1","Version" : "2"}},"Action" : {"Event" : {"Id" :
"0.0.1.2","Name" : "ASSOCIATE_TRUST","CorrelationID" : "eDirectory#55#b22140b4-
ad56-4592-942a-b44021b256ad","SubEvent" : "DSE_ADD_VALUE"},"Time" : {"Offset" :
1489681648},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

トラストの関連付け解除

［**トラストの関連付け解除**］をクリックして、次の例に示すように、既存のトラストの関連付けが削除された場合にイベントを生成します。

```
Mar 07 22:20:41 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,OU=novell,OU=co,O=in","Id" : "32863"},"Entity" : {"SysAddr" :
"100.1.2.194:31446"}},"Target" : {"Data" : {"Attribute Name" : "Member","Attribute
Value" : "CN=raghu,OU=novell,OU=co,O=in","ClassName" : "Group","Name" :
"CN=RG,OU=novell,OU=co,O=in","SubTarget" :
"CN=raghu,OU=novell,OU=co,O=in","Syntax" : "1","Version" : "2"}},"Action" :
{"Event" : {"Id" : "0.0.1.3","Name" : "DEASSOCIATE_TRUST","CorrelationID" :
"eDirectory#74#55e2ccc4-d99a-4a6a-b3dd-c4cce2559ad9","SubEvent" :
"DSE_DELETE_VALUE"},"Time" : {"Offset" : 1488905441},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

アカウントセキュリティトークンの変更

［**アカウントセキュリティトークンの変更**］をクリックして、次の例に示すように、ユーザアカウントセキュリティトークンの変更に関するイベントを生成します。

```
Mar 15 13:19:34 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:0"}},"Target" : {"Data" : {"ClassName" : "User","Version" :
"2"},"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=user7,O=novell","Id" :
"32869"}},"Action" : {"Event" : {"Id" : "0.0.0.6","Name" :
"MODIFY_ACCOUNT_SECURITY_TOKEN","CorrelationID" : "eDirectory#25#db042b31-ea70-
49d8-8b7b-312b04db70ea","SubEvent" : "DSE_CHGPASS"},"Time" : {"Offset" :
1489564174},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

アカウントセキュリティトークンの照会

［**アカウントセキュリティトークンの照会**］をクリックして、次の例に示すように、ユーザアカウントセキュリティトークンの照会に関するイベントを生成します。

```
Mar 15 13:19:34 eDirectory : INFO {"Source" : "eDirectory#NMAS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell","Id" :
"0"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" : "SLE12-142","SvcName" :
"nmas"}},"Initiator" : {"Account" : {"Name" : "CN=admin,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194:0"}},"Target" : {"Data" : {"Version" : "2"},"Account" :
{"Domain" : "TREEUPGRADE","Name" : "CN=user8,O=novell"}},"Action" : {"Event" :
{"Id" : "0.0.12.3","Name" : "QUERY_ACCOUNT_SECURITY_TOKEN","CorrelationID" :
"nmas#0#","SubEvent" : "DSE_NMAS_LOG_GET_PWD_STATUS"},"Time" : {"Offset" :
1489564174},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

接続の作成

［**接続の作成**］をクリックして、次の例に示すように、システムコンポーネント間で通信チャネルが作成されるときにイベントを生成します。

```
Mar 07 15:53:25 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-
BUILD101"},"Entity" : {"SysAddr" : "1100.1.2.194:64708"}},"Target" : {"Data" :
{"ConnID" : "63","Module" : "NCP Engine","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in","State" : "Create","Version" : "2"}},"Action" : {"Event" :
{"Id" : "0.0.13.1","Name" : "CREATE_CONNECTION","CorrelationID" :
"eDirectory#4294967295#","SubEvent" : "DSE_CONNECTION"},"Time" : {"Offset" :
1488882205},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

接続の停止

［**接続の停止**］をクリックして、次の例に示すように、システムコンポーネント間で既存の通信チャネルが停止されるときにイベントを生成します。

```
Mar 07 15:46:44 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-
BUILD101"},"Entity" : {"SysAddr" : "100.1.2.194:63684"}},"Target" : {"Data" :
{"ConnID" : "65","Module" : "NCP Engine","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in","State" : "Destroy","Version" : "2"}},"Action" : {"Event"
: {"Id" : "0.0.13.2","Name" : "TERMINATE_CONNECTION","CorrelationID" :
"eDirectory#4294967295#","SubEvent" : "DSE_CONNECTION"},"Time" : {"Offset" :
1488881804},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

セッションの作成

［**セッションの作成**］をクリックして、次の例に示すように、新しいセッションの作成に関するイベントを生成します。

```
Mar 06 16:21:47 eDirectory : INFO {"Source" : "eDirectory#NMAS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in","Id" : "nds:7"},"Entity" : {"SysAddr" :
"100.1.2.194","SysName" : "SLES12-194-12","SvcName" : "nmas"}},"Initiator" :
{"Account" : {"Name" : "CN=admin,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" :
"100.1.2.194:54823"}},"Target" : {"Data" : {"Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in","Version" : "2"}},"Action" : {"Event" : {"Id" :
"0.0.2.0","Name" : "CREATE_SESSION","CorrelationID" : "nmas#262183#","SubEvent" :
"DSE_NMAS_LOG_FINISH_LOGIN_STATUS"},"Time" : {"Offset" : 1488797507},"Log" :
{"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

セッションの停止

［**セッションの停止**］をクリックして、次の例に示すように、セッションの停止に関するイベントを生成します。

```
Mar 16 21:02:23 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Name" :
"[Public]"},"Entity" : {"SysAddr" : "164.99.91.92:8147"},"Assertions" :
{"NetAddress" : "100.1.2.194"}},"Target" : {"Data" : {"Name" : "CN=stdir-vm-
53,O=novell","SubTarget" : "CN=JPass,OU=users,O=novell","Version" : "2"}},"Action"
: {"Event" : {"Id" : "0.0.2.1","Name" : "TERMINATE_SESSION","CorrelationID" :
"eDirectory#42#","SubEvent" : "DSE_LOGOUT"},"Time" : {"Offset" : 1489678343},"Log"
: {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

認証セッション

［**認証セッション**］をクリックして、次の例に示すように、新しい識別情報がセッションに関連付けられる場合にイベントを生成します。

```
Mar 03 15:45:51 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-
BUILD101","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr"
: "100.1.2.194:30404"},"Assertions" : {"NetAddress" :
"1100.1.2.194","NullPassword" : "FALSE","bindery login" : "FALSE"}},"Target" :
{"Data" : {"ClassName" : "NCP Server","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in","SubTarget" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in","Version" : "2"}},"Action" : {"Event" : {"Id" :
"0.0.2.4","Name" : "AUTHENTICATE_SESSION","CorrelationID" :
"eDirectory#28#","SubEvent" : "DSE_AUTHENTICATE"},"Time" : {"Offset" :
1488536151},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

トラストアクセスの付与

［**トラストアクセスの付与**］をクリックして、次の例に示すように、オブジェクトへのアクセスがトラストに付与されるときにイベントを生成します。

```
Mar 03 14:33:06 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,OU=novell,OU=co,O=in","Id" : "32863"},"Entity" : {"SysAddr" :
"100.1.2.194:214"}},"Target" : {"Data" : {"Attribute Name" : "Message
Server","Attribute Value" : "Attribute Read","Name" : "[Public]","SubTarget" :
"CN=raghu,OU=novell,OU=co,O=in","Syntax" : "17","Version" : "2"}},"Action" :
{"Event" : {"Id" : "0.0.1.7","Name" : "GRANT_TRUST_ACCESS","CorrelationID" :
"eDirectory#32#9a868af1-7b8d-4426-ae41-f18a869a8d7b","SubEvent" :
"DSE_ADD_VALUE"},"Time" : {"Offset" : 1488531786},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

トラストアクセスを取り消す

［**トラストアクセスを取り消す**］をクリックして、次の例に示すように、トラストからリソースへのアクセスが削除されるときにイベントを生成します。

```
Mar 16 20:57:33 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:43936"}},"Target" : {"Data" : {"Attribute Name" :
"nsimHint","Attribute Value" : "Attribute Write, Attribute Self, Attribute Inherit
CTL","Syntax" : "17","Version" : "2"}},"Action" : {"Event" : {"Id" :
"0.0.1.8","Name" : "REVOKE_TRUST_ACCESS","CorrelationID" :
"eDirectory#41#156c162f-245b-4751-90da-2f166c155b24","SubEvent" :
"DSE_DELETE_VALUE"},"Time" : {"Offset" : 1489678053},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


不正侵入者ロックアウト

［**不正侵入者ロックアウト**］をクリックして、次の例に示すように、アカウントのロックアウト時にイベントを生成します。


```
Mar 21 09:25:29 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "NET-REPORT","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Name" : "CN=novell-
emp222,OU=novell,OU=co,O=in","Id" : "33795"},"Entity" : {"SysAddr" :
"100.1.2.194:0"}},"Target" : {"Data" : {"Account Locked" : "TRUE","Attribute Name"
: "Login Intruder Address","ClassName" : "User","Intruder Address" : "TCP:
164.99.179.164:49121","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in","Reset
Time" : "03/21/17 09:27:29","Version" : "2"}},"Action" : {"Event" : {"Id" :
"0.0.0.9","Name" : "INTRUDER_LOCKOUT","CorrelationID" : "eDirectory#0#0ae8da6e-
208f-4c44-b515-6edae80a8f20","SubEvent" : "DSE_ADD_VALUE"},"Time" : {"Offset" :
1490068529},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


アカウントのロック解除

［**アカウントのロック解除**］をクリックして、次の例に示すように、ロックされたアカウントがロック解除されるときにイベントを生成します。


```
Mar 21 12:09:00 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "NET-REPORT","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "NET-REPORT","Name" :
"CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" :
"100.1.2.194:0"}},"Target" : {"Data" : {"Attribute Name" : "Locked By
Intruder","Attribute Value" : "True","ClassName" : "User","Name" : "CN=novell-
emp312,OU=novell,OU=co,O=in","Syntax" : "7","Version" : "2"}},"Action" : {"Event" :
{"Id" : "0.0.0.10","Name" : "ACCOUNT_UNLOCK","CorrelationID" :
"eDirectory#0#f5fdd0c4-0595-4e82-8b8f-c4d0fdf59505","SubEvent" :
"DSE_DELETE_VALUE"},"Time" : {"Offset" : 1490078340},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


アカウントアクセスを付与する

［**アカウントアクセスを付与する**］をクリックして、次の例に示すように、オブジェクトへのアクセスがアカウントに付与されるときにイベントを生成します。

```
Mar 16 15:23:16 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:0"}},"Target" : {"Data" : {"Attribute Name" : "Print Job
Configuration","Attribute Value" : "Attribute Read, Attribute Write","ClassName" :
"User","Name" : "CN=usr54412,O=novell","SubTarget" :
"CN=usr54412,O=novell","Syntax" : "17","Version" : "2"}},"Action" : {"Event" :
{"Id" : "0.0.0.7","Name" : "GRANT_ACCOUNT_ACCESS","CorrelationID" :
"eDirectory#40#1718277b-ed75-41f2-8610-7b27181775ed","SubEvent" :
"DSE_ADD_VALUE"},"Time" : {"Offset" : 1489657996},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


注: ユーザアカウントがACLでトラスティと見なされる場合、［**アカウントアクセスを付与する**］イベントが生成されます。

アカウントアクセスを取り消す

［**アカウントアクセスを取り消す**］をクリックして、次の例に示すように、アカウントからオブジェクトが削除されるときにイベントを生成します。


```
Mar 18 22:44:40 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,O=novell","Id" : "32872"},"Entity" : {"SysAddr" :
"100.1.2.194:20966"}},"Target" : {"Data" : {"Attribute Name" :
"Description","Attribute Value" : "Attribute Supervisor","ClassName" :
"User","Name" : "CN=user1,O=novell","SubTarget" : "CN=pc2,O=novell","Syntax" :
"17","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.0.8","Name" :
"REVOKE_ACCOUNT_ACCESS","CorrelationID" : "eDirectory#57#67ba4065-a7de-4581-b62e-
6540ba67dea7","SubEvent" : "DSE_DELETE_VALUE"},"Time" : {"Offset" :
1489857280},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


注: ユーザアカウントがACLでトラスティと見なされる場合、［**アカウントアクセスを取り消す**］イベントが生成されます。

監査の環境設定

［**監査の環境設定**］をクリックして、次の例に示すように、監査サービスを制御するパラメータが変更されるときにイベントを生成します。


```
Mar 03 11:00:23 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,OU=novell,OU=co,O=in","Id" : "32863"},"Entity" : {"SysAddr" :
"100.1.2.194:64213"}},"Target" : {"Data" : {"Attribute Name" :
"xdasConfiguration","Attribute Value" :
"dsaccount=Computer$Organization$Organizational Person$Person$User$$","ClassName"
: "NCP Server","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in","Syntax" :
"3","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.9.0","Name" :
"AUDIT_CONFIG","CorrelationID" : "eDirectory#28#a56628e8-38fc-43c5-93c2-
e82866a5fc38","SubEvent" : "DSE_ADD_VALUE"},"Time" : {"Offset" : 1488519023},"Log"
: {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

サービスまたはアプリケーション管理イベント

このイベントセットは、サービスまたはアプリケーションの管理に関連しています。サービスやアプリケーションには、モジュール、エージェント、およびバックグラウンドプロセスが含まれます。

***表 H-6** サービスまたはアプリケーション管理イベントの分類*

イベント名	イベント ID	対応するeDirイベント	説明	使用対象:
サービスの有効化	0.0.4.5	DSE_CHANGE_MODULE_STATE DSE_NMAS_LOG_PWD_POLICY_AGENT_REG DSE_NMAS_LOG_DIST_PWD_AGENT_REG DSE_NMAS_LOG_PWD_AGENT_REG DSE_NMAS_LOG_LTSS_AGENT_REG DSE_NMAS_LOG_PWD_CHANGE_AGENT_REG	サービスまたはアプリケーションを有効にします。	このイベントは、サービス、操作、または機能が有効にされると報告されます。たとえば、eDirectoryモジュールがロードされる場合です。
サービスの無効化	0.0.4.4	DSE_REMOTE_SERVER_DOWN DSE_CHANGE_MODULE_STATE DSE_NMAS_LOG_PWD_POLICY_AGENT_DEREG DSE_NMAS_LOG_DIST_PWD_AGENT_DEREG DSE_NMAS_LOG_PWD_AGENT_DEREG DSE_NMAS_LOG_LTSS_AGENT_DEREG DSE_NMAS_LOG_PWD_CHANGE_AGENT_DEREG	サービスまたはアプリケーションを無効にします。	このイベントは、サービス、操作、または機能が無効にされると報告されます。たとえば、eDirectoryモジュールをアンロードする場合です。
サービスの起動	0.0.5.0	DSE_BACKLINK_PROC_DONE DSE_LIMBER_DONE DSE_MOVE_TREE_START DSE_PURGE_START DSE_RECV_REPLICA_UPDATES DSE_SEND_REPLICA_UPDATES DSE_START_JOIN DSE_START_UPDATE_REPLICA DSE_START_UPDATE_SCHEMA DSE_SYNC_PART_START DSE_SYNC_SVR_OUT_START	サービスまたはアプリケーションを起動します。	このイベントは、セキュリティ関連のサービスが起動されると報告されます。たとえば、バックグラウンドプロセスをトリガする場合です。

イベント名	イベントID	対応するeDirイベント	説明	使用対象:
サービスの停止	0.0.5.1	DSE_REMOVE_ATTR_DEF DSE_ABORT_JOIN DSE_END_UPDATE_REPLICA DSE_END_UPDATE_SCHEMA DSE_JOIN_DONE DSE_MOVE_TREE_END DSE_PURGE_END DSE_SCHEMA_SYNC DSE_SYNC_PART_END DSE_SYNC_SVR_OUT_END	サービスまたはアプリケーションを停止します。	このイベントは、サービスが停止されると報告されます。たとえば、バックグラウンドプロセスが停止する場合です。
サービスの環境設定の変更	0.0.4.2	DSE_ALLOW_LOGIN DSE_UPDATE_REPLICA DSE_EBA_MOVE_EBA_CA DSE_GEN_CA_KEYS DSE_RECERT_PUB_KEY DSE_EBA_REQ_BA_MATERIAL DSE_EBA_REQ_SERVER_BA_MATERIAL DSE_NAME_COLLISION DSE_SERVER_RENAME DSE_SERVER_ADDRESS_CHANGE DSE_SYNC_PARTITION DSE_SYNC_SCHEMA DSE_EBA_ENABLE_PURE_MODE DSE_EBA_ISSUE_NCPCA_CERT DSE_EBA_REVOKE_NCPCA_CERT	eDirectoryサービスと関連付けられている環境設定データの変更。	このイベントは、環境設定データの変更時に報告されます。たとえば、EBA環境設定に変更が加えられると、このイベントがトリガします。

サービスまたはアプリケーション管理イベントの例

次の各セクションに、サービスまたはアプリケーションの管理に関連するイベントの例を示します。

- 912 ページの 「サービスの有効化」
- 912 ページの 「サービスの無効化」
- 912 ページの 「サービスの起動」
- 912 ページの 「サービスの停止」
- 913 ページの 「サービスの環境設定の変更」

サービスの有効化

［**サービスの有効化**］をクリックして、次の例に示されているように、サービス、操作、または機能が有効にされるときにイベントを生成します。

```
Mar 07 10:03:15 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-
BUILD101","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr"
: "1100.1.2.194:0"}},"Target" : {"Data" : {"Module State" : "Loaded","Name" :
"libxdasauditds.so","Version" : "2"}},"Action" : {"Event" : {"Id" :
"0.0.4.5","Name" : "ENABLE_SERVICE","CorrelationID" :
"eDirectory#4294967295#","SubEvent" : "DSE_CHANGE_MODULE_STATE"},"Time" :
{"Offset" : 1488861195},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome"
: "0"}}
```

サービスの無効化

［**サービスの無効化**］をクリックして、次の例に示されているように、サービス、操作、または機能が無効にされるときにイベントを生成します。

```
Mar 10 11:00:07 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Domain" : "VLV_MEM","Name" :
"CN=stdir-vm-53,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194:0"}},"Target" :
{"Data" : {"Module State" : "Unloading","Name" : "libsnmpinst.so","Version" :
"2"}},"Action" : {"Event" : {"Id" : "0.0.4.4","Name" :
"DISABLE_SERVICE","CorrelationID" : "eDirectory#4294967295#","SubEvent" :
"DSE_CHANGE_MODULE_STATE"},"Time" : {"Offset" : 1489123807},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

サービスの起動

［**サービスの起動**］をクリックして、次の例に示されているように、セキュリティ関連サービスを起動するときにイベントを生成します。

```
Mar 03 14:41:44 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-
BUILD101","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr"
: "100.1.2.194:0"}},"Target" : {"Data" : {"Version" : "2"}},"Action" : {"Event" :
{"Id" : "0.0.5.0","Name" : "INVOKE_SERVICE","CorrelationID" :
"eDirectory#0#","SubEvent" : "DSE_SYNC_PART_START"},"Time" : {"Offset" :
1488532304},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

サービスの停止

［**サービスの停止**］をクリックして、次の例に示すように、サービスを停止するためのイベントを生成します。

Mar 03 14:41:44 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" : {"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" : "SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194:0"}},"Target" : {"Data" : {"Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.5.1","Name" : "TERMINATE_SERVICE","CorrelationID" : "eDirectory#0#","SubEvent" : "DSE_SYNC_PART_END"},"Time" : {"Offset" : 1488532304},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}

サービスの環境設定の変更

［**サービスの環境設定の変更**］をクリックして、次の例に示されているように、環境設定データの変更時に報告されるイベントを生成します。

Mar 16 21:07:46 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" : {"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194:40159"}},"Target" : {"Data" : {"Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.4.2","Name" : "MODIFY_SERVICE_CONFIG","CorrelationID" : "eDirectory#34#","SubEvent" : "DSE_SYNC_PARTITION"},"Time" : {"Offset" : 1489678666},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}

オペレーショナルイベント

オペレーショナルイベントはごくまれに生成され、重要と見なされます。たとえば、企業の重要なサーバのシャットダウンは、誰かの許可なしに起こりえないため例外的です。

***表 H-7** オペレーショナルイベントの分類*

イベント名	イベント ID	対応するeDirイベント	説明	使用対象:
システムの起動	0.0.8.0	DSE_AGENT_OPEN_LOCAL DSE_RELOAD_DS	システムを起動します	このイベントは、サーバ、システム、またはミッションクリティカルなアプリケーションが起動すると報告されます。
システムのシャットダウン	0.0.8.1	DSE_AGENT_CLOSE_LOCAL	システムをシャットダウンします	このイベントは、サーバ、システム、またはミッションクリティカルなアプリケーションがシャットダウンすると報告されます。
データストアのバックアップ	0.0.8.4	DSE_BACKUP_ENTRY	データストアをバックアップします	このイベントは、サーバ、システム、またはミッションクリティカルなアプリケーションが重要なデータストアをバックアップすると報告されます。

イベント名	イベントID	対応するeDirイベント	説明	使用対象:
データストアの回復	0.0.8.5	DSE_RESTORE_ENTRY	データストアを回復します	このイベントは、サーバ、システム、またはミッションクリティカルなアプリケーションが重要なデータストアを回復すると報告されます。
内部操作	0.1.0.3.0.0	DSE_CRC_FAILURE DSE_DELETE_SUBTREE DSE_DELETE_UNUSED_EXTREF DSE_DSA_BAD_VERB DSE_LOST_ENTRY DSE_NEW_SCHEMA_EPOCH DSE_NO_REPLICA_PTR DSE_PURGE_ENTRY_FAIL DSE_EBA_ISSUE_CRL	サービスまたはアプリケーションの操作に関連するイベント。	eDirectory内部操作によって生成されるイベントのログを記録するために使用されます。
プロセスコンテキストの変更	0.0.4.3	DSE_PARTITION_STATE_CHG DSE_LDAP_MODLDAPSERVER DSE_PART_STATE_CHG_REQ DSE_REPAIR_TIME_STAMPS DSE_RESET_DS_COUNTERS DSE_SET_NEW_MASTER DSE_SYNTHETIC_TIME DSE_SPLIT_DONE DSE_SPLIT_PARTITION DSE_JOIN_PARTITIONS DSE_ABORT_PARTITION_OP DSE_LOW_LEVEL_JOIN	処理コンテキストの変更	プロセスコンテキストの属性が変更される場合に、このイベントが報告されます。たとえば、パーティションを作成すると、このイベントがトリガされます。

例外イベントの例

次の各セクションに、例外イベントの例を示します。

- 915 ページの 「システムの起動」
- 915 ページの 「システムのシャットダウン」
- 915 ページの 「データストアのバックアップ」
- 915 ページの 「データストアの回復」

- 916 ページの 「内部操作」
- 916 ページの 「プロセスコンテキストの変更」

システムの起動

［**システムの起動**］をクリックして、次の例に示すように、サーバ、システム、またはミッションクリティカルなアプリケーションが起動するとイベントを生成します。

```
Mar 13 11:20:24 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Domain" : "VLV_MEM","Name" :
"CN=stdir-vm-53,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194:0"}},"Target" :
{"Data" : {"Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.8.0","Name" :
"START_SYSTEM","CorrelationID" : "eDirectory#0#","SubEvent" :
"DSE_AGENT_OPEN_LOCAL"},"Time" : {"Offset" : 1489384224},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

システムのシャットダウン

［**システムのシャットダウン**］をクリックして、次の例に示すように、サーバ、システム、またはミッションクリティカルなアプリケーションがシャットダウンするとイベントを生成します。

```
Mar 13 11:16:23 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Domain" : "VLV_MEM","Name" :
"CN=stdir-vm-53,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194:0"}},"Target" :
{"Data" : {"Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.8.1","Name" :
"SHUTDOWN_SYSTEM","CorrelationID" : "eDirectory#0#","SubEvent" :
"DSE_AGENT_CLOSE_LOCAL"},"Time" : {"Offset" : 1489383983},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

データストアのバックアップ

［**データストアのバックアップ**］をクリックして、次の例に示すように、サーバ、システム、またはミッションクリティカルなアプリケーションが重要なデータストアをバックアップするとイベントを生成します。

```
Mar 14 13:03:29 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,O=novell","Id" : "32872"},"Entity" : {"SysAddr" :
"100.1.2.194:13018"}},"Target" : {"Data" : {"Version" : "2"}},"Action" : {"Event" :
{"Id" : "0.0.8.4","Name" : "BACKUP_DATA_STORE","CorrelationID" :
"eDirectory#43#","SubEvent" : "DSE_BACKUP_ENTRY"},"Time" : {"Offset" :
1489476809},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

データストアの回復

［**データストアの回復**］をクリックして、次の例に示すように、サーバ、システム、またはミッションクリティカルなアプリケーションがデータストアを回復するとイベントを生成します。

Mar 14 14:16:02 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" : {"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Name" : "CN=admin,O=novell","Id" : "32872"},"Entity" : {"SysAddr" : "100.1.2.194:10203"}},"Target" : {"Data" : {"Name" : "OU=users,O=novell","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.8.5","Name" : "RECOVER_DATA_STORE","CorrelationID" : "eDirectory#36#bd5cb85b-0f9f-4268-a221-5bb85cbd9f0f","SubEvent" : "DSE_RESTORE_ENTRY"},"Time" : {"Offset" : 1489481162},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}

内部操作

［**内部操作**］をクリックして、次の例に示すように、eDirectory内部操作によってログイベントが生成されるときにこのイベントを生成します。

Mar 15 13:45:13 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" : {"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194:0"}},"Target" : {"Data" : {"ValidityEnd" : "03/16/2017 01:45:13 PM","ValidityStart" : "03/15/2017 01:45:13 PM","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.12.2","Name" : "INTERNAL_OPERATIONS","CorrelationID" : "eDirectory#0#","SubEvent" : "DSE_EBA_ISSUE_CRL"},"Time" : {"Offset" : 1489565713},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}

プロセスコンテキストの変更

［**プロセスコンテキストの変更**］をクリックして、次の例に示すように、プロセスコンテキストのいずれかの属性が変更された場合にイベントを生成します。

Mar 16 21:07:46 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" : {"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194:0"}},"Target" : {"Data" : {"Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.5.3","Name" : "MODIFY_PROCESS_CONTEXT","CorrelationID" : "eDirectory#0#042b517b-41c4-4c9b-b5b5-7b512b04c441","SubEvent" : "DSE_PARTITION_STATE_CHG"},"Time" : {"Offset" : 1489678666},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}

eDirectoryイベントとCEFイベントのマッピング

このセクションでは、次の情報について説明します。

- 917 ページの 「eDirectoryイベントとCEFイベントのマッピング」
- 921 ページの 「CEFイベント」

eDirectoryイベントとCEFイベントのマッピング

表 I-1は、対応するCEFイベントにマッピングされたeDirectoryの内部イベントを一覧で示しています。各eDirectoryイベントとそれらの説明については、eDirectoryサービスのページを参照してください。CEFイベントについては、921 ページの 「CEFイベント」を参照してください。

表 I-1 *eDirectoryイベントと対応付けられたCEFイベント*

イベントカテゴリ	CEFイベント	eDirectoryイベント
セキュリティ	CONNECTION このイベントの例については、922 ページの 「接続」を参照してください。	DSE_CONNECTION
セキュリティ	LOGIN このイベントの例については、923 ページの「ログイン」を参照してください。	DSE_LOGIN_EX DSE_NMAS_LOG_SRVR_BEGIN_LOGIN DSE_NMAS_LOG_FINISH_LOGIN_STATUS DSE_NMAS_LOG_SASL_MECHANISM_RESULT DSE_EBA_REQ_BA_MATERIAL
セキュリティ	LOGOUT このイベントの例については、923 ページの 「ログアウト」を参照してください。	DSE_LOGOUT
セキュリティ	ADD_MEMBER このイベントの例については、923 ページの 「メンバーの追加」を参照してください。	DSE_ADD_VALUE
セキュリティ	DELETE_MEMBER このイベントの例については、924 ページの 「メンバーの削除」を参照してください。	DSE_DELETE_VALUE

イベントカテゴリ	CEFイベント	eDirectoryイベント
セキュリティ	INTRUDER_DETECTED このイベントの例については、924 ページの 「不正侵入者が検出されました」を参照してください。	DSE_ADD_VALUE
セキュリティ	ACCOUNT_UNLOCK このイベントの例については、924 ページの 「アカウントのロック解除」を参照してください。	DSE_DELETE_VALUE
セキュリティ	LOGIN_DISABLED このイベントの例については、925 ページの 「ログインが無効化されました」を参照してください。	DSE_ADD_VALUE
セキュリティ	LOGIN_ENABLED このイベントの例については、925 ページの 「ログインが有効化されました」を参照してください。	DSE_DELETE_VALUE
セキュリティ	ACL_CHANGED このイベントの例については、925 ページの 「ACLが変更されました」を参照してください。	DSE_ADD_VALUE DSE_DELETE_VALUE
セキュリティ	CHANGE_SECURITY_EQUALS このイベントの例については、926 ページの 「同等セキュリティの変更」を参照してください。	DSE_ADD_VALUE DSE_DELETE_VALUE
セキュリティ	VERIFY_PASSWORD このイベントの例については、926 ページの 「パスワードの確認」を参照してください。	DSE_VERIFY_PASS
セキュリティ	AUDIT_CONFIG このイベントの例については、926 ページの 「監査の環境設定」を参照してください。	DSE_ADD_VALUE DSE_DELETE_VALUE

イベントカテゴリ	CEFイベント	eDirectoryイベント
セキュリティ	CHANGE_PASSWORD このイベントの例については、927 ページの 「パスワードの変更」を参照してください。	DSE_CHGPASS DSE_NMAS_LOG_SET_PWD DSE_NMAS_LOG_SET_DIST_PWD DSDSE_NMAS_LOG_DELETE_PWD DSE_NMAS_LOG_DELETE_DIST_PWD DSE_NMAS_LOG_CHANGE_PWD DSE_NMAS_LOG_DELETE_ALL_LOGIN_SECRET DSE_NMAS_LOG_SET_LOGIN_SECRET DSE_NMAS_LOG_DELETE_LOGIN_SECRET
セキュリティ	CHANGE_LOGIN_CONFIG このイベントの例については、927 ページの 「ログイン環境設定の変更」を参照してください。	DSE_NMAS_LOG_SET_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_ALL_LOGIN_CONFIG
セキュリティ	QUERY_CREDENTIALS このイベントの例については、927 ページの 「資格情報の照会」を参照してください。	DSE_NMAS_LOG_GET_PWD_HISTORY DSE_NMAS_LOG_GET_PWD DSE_NMAS_LOG_GET_LOGIN_CONFIG DSE_NMAS_LOG_CHECK_PWD_SYNTAX_POLICY DSE_NMAS_LOG_GET_ALL_LOGIN_SECRET DSE_NMAS_LOG_GET_PWD_STATUS DSE_NMAS_LOG_GET_ALL_LOGIN_CONFIG DSE_NMAS_LOG_GET_DIST_PWD DSE_NMAS_LOG_GET_PWD_HISTORY
セキュリティ	IMPERSONATE このイベントの例については、927 ページの 「なりすまし」を参照してください。	DSE_IMPERSONATE
セキュリティ	AUTHENTICATE このイベントの例については、928 ページの 「認証」を参照してください。	DSE_AUTHENTICATE
オブジェクト	CREATE_OBJECT このイベントの例については、928 ページの 「オブジェクトの作成」を参照してください。	DSE_CREATE_ENTRY DSE_ADD_ENTRY

イベントカテゴリ	CEFイベント	eDirectoryイベント
オブジェクト	DELETE_OBJECT このイベントの例については、929 ページの 「オブジェクトの削除」を参照してください。	DSE_REMOVE_ENTRY
オブジェクト	RENAME_OBJECT このイベントの例については、929 ページの 「オブジェクトのリネーム」を参照してください。	DSE_RENAME_ENTRY
オブジェクト	MOVE_OBJECT このイベントの例については、929 ページの 「オブジェクトの移動」を参照してください。	DSE_MOVE_SOURCE_ENTRY DSE_MOVE_DEST_ENTRY
オブジェクト	DSA_READ このイベントの例については、930 ページの「DSAの読み取り」を参照してください。	DSE_DSA_READ
オブジェクト	SEARCH このイベントの例については、930 ページの 「検索」を参照してください。	DSE_SEARCH
属性	READ_ATTRIBUTE このイベントの例については、930 ページの 「属性の読み込み」を参照してください。	DSE_READ_ATTR
属性	DELETE_ATTRIBUTE このイベントの例については、931 ページの 「属性の削除」を参照してください。	DSE_DELETE_ATTRIBUTE
属性	ADD_VALUE このイベントの例については、931 ページの「値の追加」を参照してください。	DSE_ADD_VALUE
属性	DELETE_VALUE	DSE_DELETE_VALUE
属性	COMPARE_ATTRIBUTE_VALUE このイベントの例については、932 ページの 「属性値の比較」を参照してください。	DSE_COMPARE_ATTR_VALUE
LDAP	LDAP_BIND	DSE_LDAP_BIND
	LDAP_UNBIND	DSE_LDAP_UNBIND
	LDAP_CONNECTION	DSE_LDAP_CONNECTION

イベントカテゴリ	CEFイベント	eDirectoryイベント
	LDAP_SEARCH	DSE_LDAP_SEARCH
	LDAP_ADD	DSE_LDAP_ADD
	LDAP_COMPARE	DSE_LDAP_COMPARE
	LDAP_MODIFY	DSE_LDAP_MODIFY
	LDAP_DELETE	DSE_LDAP_DELETE
	LDAP_MODIFY_DN	DSE_LDAP_MODDN
	LDAP_ABANDON	DSE_LDAP_ABANDON
	LDAP_EXTENDED_OPERATION	DSE_LDAP_EXTOP
	LDAP_SYSTEM_EXTENDED_OPERATION	DSE_LDAP_SYSEXTOP
	LDAP_PASSWORD_MODIFY	DSE_LDAP_PASSWDMODIFY
	MODIFY_LDAP_SERVER_CONFIGURATION	DSE_LDAP_MODLDAPSERVER
	UNKNOWN_LDAP_OPERATION	DSE_LDAP_UNKNOWNOP
	LDAP_BIND_RESPONSE	DSE_LDAP_BINDRESPONSE
	LDAP_SEARCH_RESPONSE	DSE_LDAP_SEARCHRESPONSE
	LDAP_SEARCH_ENTRY_RESPONSE	DSE_LDAP_SEARCHENTRYRESPONSE
	LDAP_ADD_RESPONSE	DSE_LDAP_ADDRESPONSE
	LDAP_COMPARE_RESPONSE	DSE_LDAP_COMPARERESPONSE
	LDAP_MODIFY_RESPONSE	DSE_LDAP_MODIFYRESPONSE
	LDAP_DELETE_RESPONSE	DSE_LDAP_DELETERESPONSE
	LDAP_MODIFY_DN_RESPONSE	DSE_LDAP_MODDNRESPONSE
	LDAP_EXTENDED_OPERATION_RESPONSE	DSE_LDAP_EXTOP_RESPONSE
EBA	MODIFY_SERVICE_CONFIG	DSE_EBA_ISSUE_NCPCA_CERT
	このイベントの例については、932 ページの 「サービスの環境設定の変更」を参照してください。	DSE_EBA_REVOKE_NCPCA_CERT
		DSE_EBA_MOVE_EBA_CA
		DSE_EBA_ISSUE_CRL
		DSE_EBA_REQ_SERVER_BA_MATERIAL

CEFイベント

CEFイベントは、次のカテゴリに分類されます。

- 922 ページの 「セキュリティイベント」
- 928 ページの 「オブジェクトイベント」

- 930 ページの 「属性イベント」
- 932 ページの 「EBAイベント」

セキュリティイベント

このイベントセットは、eDirectoryのセキュリティ操作の監査に適用できます。セキュリティ操作には、アクセスの付与や取り消し、ログイン、パスワード変更、照会があります。このイベントセットは、eDirectoryシステムにおける不正侵入者を検出するためにも役立ちます。

セキュリティイベントの例:

このセクションには、次のセキュリティイベントの例が含まれています。

- 922 ページの 「接続」
- 923 ページの 「ログイン」
- 923 ページの 「ログアウト」
- 923 ページの 「メンバーの追加」
- 924 ページの 「メンバーの削除」
- 924 ページの 「不正侵入者が検出されました」
- 924 ページの 「アカウントのロック解除」
- 925 ページの 「ログインが無効化されました」
- 925 ページの 「ログインが有効化されました」
- 925 ページの 「ACLが変更されました」
- 926 ページの 「同等セキュリティの変更」
- 926 ページの 「パスワードの確認」
- 926 ページの 「監査の環境設定」
- 927 ページの 「パスワードの変更」
- 927 ページの 「ログイン環境設定の変更」
- 927 ページの 「資格情報の照会」
- 927 ページの 「なりすまし」
- 928 ページの 「認証」

注: 次の各セクションで紹介する例は、参考のためにのみ示しています。

接続

［**接続**］をクリックして、次の例に示すように、システムコンポーネント間で通信チャネルが作成されるときにイベントを生成します。

```
Oct 31 17:00:22 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B035E|CONNECTION|0|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Oct 31 2017 17:00:22 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#DS
src=164.99.179.164 spt=23017 duser=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in
cn1Label=Connection ID cn1=246358976 cn2Label=Created(1)/Terminated(0) cn2=1
cs1Label=Client Address cs1=164.99.179.164:23017 cs2Label=Module cs2=LDAP Server
cs3Label=Tree Name cs3=TEST-CEF-AGN cs4Label=Correlation ID
cs4=eDirectory#4294967295# flexString2Label=SubEvent flexString2=DSE_CONNECTION
cat=Security reason=0 outcome=Success
```

ログイン

［**ログイン**］をクリックして、新しいセッションが作成されるときにイベントを生成します。たとえば、eDirectoryシステムにログインする場合。

```
Oct 31 17:00:22 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B035C|LOGIN|1|dvc=164.99.179.194 dvchost=SLES12SP2-
194 rt=Oct 31 2017 17:00:22 dtz=IST sourceServiceName=CN\=SLES12SP2-
194,OU\=server,OU\=co,O\=in sproc=eDirectory#NMAS src=164.99.179.164 spt=59737
suser=CN\=admin,OU\=novell,OU\=co,O\=in duser=CN\=admin,OU\=novell,OU\=co,O\=in
cs1Label=Client Address cs1=164.99.179.164:59737 cs2Label=Class Name cs2=User
cs3Label=Tree Name cs3=TEST-CEF-AGN cs4Label=Correlation ID cs4=nmas#262183#
cs6Label=Server Name cs6=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in
flexString1Label=Login Method flexString1=0 flexString2Label=SubEvent
flexString2=DSE_NMAS_LOG_FINISH_LOGIN_STATUS flexNumber2Label=Grouping
flexNumber2=386 cat=Security reason=0 outcome=Success
```

ログアウト

［**ログアウト**］をクリックして、既存のセッションが停止するときにイベントを生成します。たとえば、eDirectoryシステムからログアウトする場合。

```
Jan 09 18:34:15 eDirectory
CEF:0|NetIQ|eDirectory|9.1|CEF0B0303|LOGOUT|1|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Nov 03 2017 13:10:32 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#DS
src=164.99.44.5 spt=53738 suser=[Public] duser=CN\=SLES12SP2-
194,OU\=server,OU\=co,O\=in cs1Label=Client Address cs1=164.99.44.5 cs2Label=Class
Name cs2=User cs3Label=Tree Name cs3=TEST-CEF-NOV3 cs4Label=Correlation ID
cs4=eDirectory#17# cs6Label=Object DN cs6=CN\=admin,OU\=novell,OU\=co,O\=in
flexString2Label=SubEvent flexString2=DSE_LOGOUT flexNumber2Label=Grouping
flexNumber2=127 cat=Security reason=0 outcome=Success
```

メンバーの追加

［**メンバーの追加**］をクリックして、次の例に示すように、新しいユーザがグループに追加されるときにイベントを生成します。

```
Jan 09 18:34:15 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B0336|ADD_MEMBER|1|dvc=164.99.179.156
dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 18:34:15 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.158 spt=54936
suser=CN\=admin,OU\=novell,OU\=co,O\=in duser=CN\=grp1,OU\=lnx-
users,OU\=novell,OU\=co,O\=in cs2Label=Class Name cs2=Group cs3Label=Tree Name
cs3=NEW-TREE-9th cs4Label=Correlation ID cs4=eDirectory#14#bc560efc-53d4-4ad9-
85b4-fc0e56bcd453 cs6Label=Member DN cs6=CN\=lynx-user,OU\=lnx-
users,OU\=novell,OU\=co,O\=in flexString2Label=SubEvent flexString2=DSE_ADD_VALUE
flexNumber2Label=Grouping flexNumber2=3676 cat=Security reason=0 outcome=Success
```

メンバーの削除

［**メンバーの削除**］をクリックして、次の例に示すように、ユーザがグループから削除されるときにイベントを生成します。

```
Jan 09 18:35:06 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B0337|DELETE_MEMBER|1|dvc=164.99.179.156
dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 18:35:06 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.158 spt=54936
suser=CN\=admin,OU\=novell,OU\=co,O\=in duser=CN\=grp1,OU\=lnx-
users,OU\=novell,OU\=co,O\=in cs2Label=Class Name cs2=Group cs3Label=Tree Name
cs3=NEW-TREE-9th cs4Label=Correlation ID cs4=eDirectory#14#9136617f-4412-48da-
bf33-7f6136911244 cs6Label=Member DN cs6=CN\=lynx-user,OU\=lnx-
users,OU\=novell,OU\=co,O\=in flexString2Label=SubEvent
flexString2=DSE_DELETE_VALUE flexNumber2Label=Grouping flexNumber2=3687
cat=Security reason=0 outcome=Success
```

不正侵入者が検出されました

［**不正侵入者が検出されました**］をクリックして、次の例に示すように、不正侵入者が検出されるときにイベントを生成します。

```
Jan 09 18:35:06 eDirectory
CEF:0|NetIQ|eDirectory|9.1|CEF0B0357|INTRUDER_DETECTED|5|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Oct 17 2017 19:50:20 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#DS
src=164.99.179.194 spt=0 suser=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in
duser=CN\=raghu,OU\=lens,OU\=QA,OU\=HD,OU\=DSLR,OU\=SLR,OU\=digital,OU\=camera,O\=
sony,L\=tokyo,dc\=co,C\=jp cs1Label=Intruder Address cs1=TCP: 164.99.179.164:33584
cs2Label=Reset Time cs2=10/17/17 19:52:20 cs3Label=Tree Name cs3=TEST-CEF222
cs4Label=Correlation ID cs4=eDirectory#0#349e5670-0b80-4c99-b7f0-70569e34800b
cs6Label=Class cs6=User flexString2Label=SubEvent flexString2=DSE_ADD_VALUE
flexNumber2Label=Grouping flexNumber2=102 cat=Security reason=0 outcome=Success
```

アカウントのロック解除

［**アカウントのロック解除**］をクリックして、次の例に示すように、ロックされたアカウントがロック解除されるときにイベントを生成します。

```
Jan 09 19:10:32 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B035F|ACCOUNT_UNLOCK|2|dvc=164.99.179.156
dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 19:10:32 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.156 spt=0 suser=CN\=SLES12-SP3-156,OU\=lnx-
server,OU\=server,OU\=co,O\=in duser=CN\=rr,OU\=lnx-users,OU\=novell,OU\=co,O\=in
cs2Label=Class Name cs2=User cs3Label=Tree Name cs3=NEW-TREE-9th
cs4Label=Correlation ID cs4=eDirectory#0#ad3a0226-764e-488c-b90a-26023aad4e76
flexString2Label=SubEvent flexString2=DSE_DELETE_VALUE flexNumber2Label=Grouping
flexNumber2=122 cat=Security reason=0 outcome=Success
```

ログインが無効化されました

［**ログインが無効化されました**］をクリックして、次の例に示すように、ユーザアカウントが無効にされるときにイベントを生成します。

```
Jan 09 18:18:48 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B0356|LOGIN_DISABLED|2|dvc=164.99.179.156
dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 18:18:48 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.158 spt=54936
suser=CN\=admin,OU\=novell,OU\=co,O\=in duser=CN\=lynx-user1,OU\=lnx-
users,OU\=novell,OU\=co,O\=in cs2Label=Class Name cs2=User cs3Label=Tree Name
cs3=NEW-TREE-9th cs4Label=Correlation ID cs4=eDirectory#14#f04b6deb-df9b-4f4b-
a8e8-eb6d4bf09bdf flexString2Label=SubEvent flexString2=DSE_ADD_VALUE
flexNumber2Label=Grouping flexNumber2=100 cat=Security reason=0 outcome=Success
```

ログインが有効化されました

［**ログインが有効化されました**］をクリックして、次の例に示すように、ユーザアカウントが有効にされるときにイベントを生成します。

```
Jan 09 18:18:56 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B0355|LOGIN_ENABLED|2|dvc=164.99.179.156
dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 18:18:56 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.158 spt=54936
suser=CN\=admin,OU\=novell,OU\=co,O\=in duser=CN\=lynx-user1,OU\=lnx-
users,OU\=novell,OU\=co,O\=in cs2Label=Class Name cs2=User cs3Label=Tree Name
cs3=NEW-TREE-9th cs4Label=Correlation ID cs4=eDirectory#14#f99f0883-251e-424e-
a724-83089ff91e25 flexString2Label=SubEvent flexString2=DSE_DELETE_VALUE
flexNumber2Label=Grouping flexNumber2=107 cat=Security reason=0 outcome=Success
```

ACLが変更されました

［**ACLが変更されました**］をクリックして、次の例に示すように、オブジェクトのACLが変更されたときにイベントを生成します。

```
Jan 09 18:04:56 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B0354|ACL_CHANGED|3|dvc=164.99.179.156
dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 18:04:56 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.158 spt=52120
suser=CN\=admin,OU\=novell,OU\=co,O\=in duser=CN\=lynx-user,OU\=lnx-
users,OU\=novell,OU\=co,O\=in cn1Label=ACL Added cn1=1 cs1Label=Value cs1=Entry
ID: .CN\=lynx-user.OU\=lnx-users.OU\=novell.OU\=co.O\=in.T\=NEW-TREE-9th.,
Attribute ID: [All Attributes Rights], Privileges: Attribute Read cs2Label=Class
Name cs2=User cs3Label=Tree Name cs3=NEW-TREE-9th cs4Label=Correlation ID
cs4=eDirectory#18#c4f344f7-db17-4366-8a19-f744f3c417db cs6Label=Trustee
cs6=CN\=lynx-user,OU\=lnx-users,OU\=novell,OU\=co,O\=in flexString2Label=SubEvent
flexString2=DSE_ADD_VALUE flexNumber2Label=Grouping flexNumber2=83 cat=Security
reason=0 outcome=Success
```

同等セキュリティの変更

［**同等セキュリティの変更**］をクリックして、次の例に示すように、オブジェクトで同等セキュリティが変更されるときにイベントを生成します。

```
Jan 09 18:29:38 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B0341|CHANGE_SECURITY_EQUALS|3|dvc=164.99.179.
156 dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 18:29:38 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.156 spt=0 suser=CN\=SLES12-SP3-156,OU\=lnx-
server,OU\=server,OU\=co,O\=in duser=CN\=raghu,OU\=lnx-
users,OU\=novell,OU\=co,O\=in cn1Label=Add/Remove cn1=1 cs2Label=Class Name
cs2=User cs3Label=Tree Name cs3=NEW-TREE-9th cs4Label=Correlation ID
cs4=eDirectory#0#6d1355d0-0401-4858-8475-d055136d0104 cs6Label=Equivalent DN
cs6=CN\=grp,OU\=novell,OU\=co,O\=in flexString2Label=SubEvent
flexString2=DSE_ADD_VALUE flexNumber2Label=Grouping flexNumber2=3639 cat=Security
reason=0 outcome=Success
```

パスワードの確認

［**パスワードの確認**］をクリックして、アカウントパスワードが確認されるときにイベントを生成します。

監査の環境設定

［**監査の環境設定**］をクリックして、次の例に示すように、監査サービスを制御するパラメータが変更されるときにイベントを生成します。

```
Jan 09 18:27:12 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B0006|AUDIT_CONFIG|2|dvc=164.99.179.156
dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 18:27:12 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.160 spt=54980 suser=CN\=srv-
160,OU\=server,OU\=co,O\=in duser=CN\=SLES12-SP3-156,OU\=lnx-
server,OU\=server,OU\=co,O\=in cs1Label=Attribute Value cs1=cefEvents\=ACL_CHANGED
$$QUERY_CREDENTIALS cs2Label=Class Name cs2=NCP Server cs3Label=Tree Name cs3=NEW-
TREE-9th cs4Label=Correlation ID cs4=eDirectory#16#8dcd3ede-baf8-4e71-9f1e-
de3ecd8df8ba cs6Label=Attribute Name cs6=cefConfiguration
flexString2Label=SubEvent flexString2=DSE_ADD_VALUE flexNumber2Label=Grouping
flexNumber2=3631 cat=Security reason=0 outcome=Success
```

パスワードの変更

［**パスワードの変更**］をクリックして、次の例に示すように、アカウントパスワードが変更されるときにイベントを生成します。

```
Oct 31 17:06:11 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0290064|CHANGE_PASSWORD|1|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Oct 31 2017 17:06:11 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#NMAS
src=164.99.179.194 spt=0 suser=CN\=admin,OU\=novell,OU\=co,O\=in
duser=raghu,novell,co,in cs2Label=Class Name cs2=User cs3Label=Tree Name cs3=TEST-
CEF-AGN cs4Label=Correlation ID cs4=nmas#0# cs6Label=Server Name
cs6=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in flexString2Label=SubEvent
flexString2=DSE_NMAS_LOG_SET_LOGIN_SECRET flexNumber2Label=Grouping
flexNumber2=405 cat=Security reason=0 outcome=Success
```

ログイン環境設定の変更

［**ログイン環境設定の変更**］をクリックして、次の例に示すように、アカウントのログイン環境設定が変更されるときにイベントを生成します。

```
Nov 02 10:21:00 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0290061|CHANGE_LOGIN_CONFIG|1|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Nov 02 2017 10:21:00 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#NMAS
src=164.99.179.194 spt=0 suser=CN\=admin,OU\=novell,OU\=co,O\=in
duser=raghu,novell,co,in cs2Label=Class Name cs2=User cs3Label=Tree Name cs3=TEST-
CEF-AGN cs4Label=Correlation ID cs4=nmas#0# cs6Label=Server Name
cs6=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in flexString2Label=SubEvent
flexString2=DSE_NMAS_LOG_SET_LOGIN_CONFIG flexNumber2Label=Grouping
flexNumber2=2034 cat=Security reason=0 outcome=Success
```

資格情報の照会

［**資格情報の照会**］をクリックして、次の例に示すように、特定のアカウントの資格情報が要求されるときにイベントを生成します。

```
Nov 02 10:21:00 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0290062|QUERY_CREDENTIALS|1|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Nov 02 2017 10:21:00 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#NMAS
src=164.99.179.194 spt=0 suser=CN\=admin,OU\=novell,OU\=co,O\=in
duser=raghu,novell,co,in cs2Label=Class Name cs2=User cs3Label=Tree Name cs3=TEST-
CEF-AGN cs4Label=Correlation ID cs4=nmas#0# cs6Label=Server Name
cs6=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in flexString2Label=SubEvent
flexString2=DSE_NMAS_LOG_GET_LOGIN_CONFIG flexNumber2Label=Grouping
flexNumber2=2035 cat=Security reason=0 outcome=Success
```

なりすまし

［**なりすまし**］をクリックして、次の例に示すように、アカウントのなりすましが発生するたびにイベントを生成します。

```
Nov 02 10:29:38 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0231|IMPERSONATE|1|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Nov 02 2017 10:29:38 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#DS
src=164.99.179.194 spt=56451 suser=CN\=admin,OU\=novell,OU\=co,O\=in
duser=CN\=raghu,OU\=novell,OU\=co,O\=in cs3Label=Tree Name cs3=TEST-CEF-AGN
cs4Label=Correlation ID cs4=eDirectory#10# cs6=CN\=SLES12SP2-
194,OU\=server,OU\=co,O\=in flexString2Label=SubEvent flexString2=DSE_IMPERSONATE
flexNumber2Label=Grouping flexNumber2=2048 cat=Security reason=0 outcome=Success
```

認証

［**認証**］をクリックして、次の例に示すように、ユーザがセッションを認証するときにイベントを生成します。

```
Nov 02 10:32:39 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B035D|AUTHENTICATE|1|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Nov 02 2017 10:32:39 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#DS
src=164.99.179.194 spt=0 suser=CN\=impuser,OU\=novell,OU\=co,O\=in
duser=CN\=impuser,OU\=novell,OU\=co,O\=in cs2Label=Class Name cs2=User
cs3Label=Tree Name cs3=TEST-CEF-AGN cs4Label=Correlation ID cs4=eDirectory#12#
cs6Label=Server Name cs6=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in
flexString2Label=SubEvent flexString2=DSE_AUTHENTICATE flexNumber2Label=Grouping
flexNumber2=2058 cat=Security reason=0 outcome=Success
```

オブジェクトイベント

このイベントセットは、eDirectoryのオブジェクト関連操作の監査に適用できます。オブジェクト操作には、オブジェクトの作成、削除、リネーム、移動、または照会があります。

オブジェクトイベントの例:

このセクションには、次のオブジェクトイベントの例が含まれています。

- 928 ページの 「オブジェクトの作成」
- 929 ページの 「オブジェクトの削除」
- 929 ページの 「オブジェクトのリネーム」
- 929 ページの 「オブジェクトの移動」
- 930 ページの 「DSAの読み取り」
- 930 ページの 「検索」

注: 次の各セクションで紹介する例は、参考のためにのみ示しています。

オブジェクトの作成

［**オブジェクトの作成**］をクリックして、次の例に示すように、eDirectoryツリーに新しいオブジェクトが作成されるときにイベントを生成します。

```
Oct 23 23:57:19 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0001|CREATE_OBJECT|0|dvc=164.99.179.60
dvchost=WIN-37D8M9SKD2U rt=Oct 23 2017 23:57:19 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.58 spt=52362 suser=CN\=Admin,O\=novell duser=CN\=user001,O\=novell
cs2Label=Class Name cs2=User cs3Label=Tree Name cs3=TREE910W cs4Label=Correlation
ID cs4=eDirectory#17#dc0fee11-5cd9-47d4-b981-cdb8ecd47e07
flexString2Label=SubEvent flexString2=DSE_CREATE_ENTRY flexNumber2Label=Grouping
flexNumber2=677768 cat=Objects reason=0 outcome=Success
```

オブジェクトの削除

［**オブジェクトの削除**］をクリックして、次の例に示すように、eDirectoryツリーからオブジェクトが削除されるときにイベントを生成します。

```
Oct 24 00:02:35 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0309|DELETE_OBJECT|0|dvc=164.99.179.60
dvchost=WIN-37D8M9SKD2U rt=Oct 24 2017 00:02:35 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.58 spt=52362 suser=CN\=Admin,O\=novell duser=CN\=user001,O\=novell
cs2Label=Class Name cs2=User cs3Label=Tree Name cs3=TREE910W cs4Label=Correlation
ID cs4=eDirectory#17#2b97f69d-2984-4f96-a83c-0b6c828bc462
flexString2Label=SubEvent flexString2=DSE_REMOVE_ENTRY flexNumber2Label=Grouping
flexNumber2=677993 cat=Objects reason=0 outcome=Success
```

オブジェクトのリネーム

［**オブジェクトのリネーム**］をクリックして、次の例に示すように、オブジェクトが名前変更されるときにイベントを生成します。

```
Oct 24 02:06:23 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0003|RENAME_OBJECT|0|dvc=164.99.179.60
dvchost=WIN-37D8M9SKD2U rt=Oct 24 2017 02:06:23 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.58 spt=55434 suser=CN\=Admin,O\=novell duser=CN\=u1,O\=novell
cs2Label=Class Name cs2=User cs3Label=Tree Name cs3=TREE910W cs4Label=Correlation
ID cs4=eDirectory#17#28250918-af9c-4098-b56a-5757e456102a cs6Label=New Object DN
cs6=CN\=u1changed,O\=novell flexString2Label=SubEvent flexString2=DSE_RENAME_ENTRY
flexNumber2Label=Grouping flexNumber2=683314 cat=Objects reason=0 outcome=Success
```

オブジェクトの移動

［**オブジェクトの移動**］をクリックして、次の例に示すように、オブジェクトが移動されるときにイベントを生成します。

```
Oct 24 02:18:57 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0004|MOVE_OBJECT|0|dvc=164.99.179.60 dvchost=WIN-
37D8M9SKD2U rt=Oct 24 2017 02:18:57 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.58 spt=55434 suser=CN\=Admin,O\=novell
duser=CN\=u1changed,O\=novell cs2Label=Class Name cs2=User cs3Label=Tree Name
cs3=TREE910W cs4Label=Correlation ID cs4=eDirectory#17#28789395-394f-49d5-bb4e-
b95410b0f9b5 cs6Label=New DN cs6=CN\=u1changed,OU\=org,O\=novell
flexString2Label=SubEvent flexString2=DSE_MOVE_SOURCE_ENTRY
flexNumber2Label=Grouping flexNumber2=683861 cat=Objects reason=0 outcome=Success
```

DSAの読み取り

［**DSAの読み取り**］をクリックして、次の例に示すように、オブジェクトが読み取られるときにイベントを生成します。

```
Oct 24 02:36:27 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0230|DSA_READ|0|dvc=164.99.179.60 dvchost=WIN-
37D8M9SKD2U rt=Oct 24 2017 02:36:27 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.60 spt=20928 suser=CN\=WIN-37D8M9SKD2U-NDS,O\=novell duser=CN\=WIN-
37D8M9SKD2U-NDS,O\=novell cs2Label=Class Name cs2=NCP Server cs3Label=Tree Name
cs3=TREE910W cs4Label=Correlation ID cs4=eDirectory#1# flexString2Label=SubEvent
flexString2=DSE_DSA_READ cat=Objects reason=0 outcome=Success
```

検索

［**検索**］をクリックして、次の例に示すように、検索操作が要求されるときにイベントを生成します。

```
Oct 24 02:36:29 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B033C|SEARCH|0|dvc=164.99.179.60 dvchost=WIN-
37D8M9SKD2U rt=Oct 24 2017 02:36:29 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.60 spt=21184 suser=CN\=WIN-37D8M9SKD2U-NDS,O\=novell
duser=CN\=Security cn1Label=Scope cn1=2 cn2Label=Nodes To Search cn2=100
cs2Label=Class Name cs2=SAS:Security cs3Label=Tree Name cs3=TREE910W
cs4Label=Correlation ID cs4=eDirectory#2# flexString2Label=SubEvent
flexString2=DSE_SEARCH flexNumber2Label=Grouping flexNumber2=684639 cat=Objects
reason=0 outcome=Success
```

属性イベント

このイベントセットは、eDirectoryの属性関連操作の監査に適用できます。属性操作には、属性の作成、削除、リネーム、移動、または検索があります。

属性イベントの例:

このセクションには、次の属性イベントの例が含まれています。

- 930 ページの 「属性の読み込み」
- 931 ページの 「属性の削除」
- 931 ページの 「値の追加」
- 931 ページの 「値の削除」
- 932 ページの 「属性値の比較」

注: 次の各セクションで紹介する例は、参考のためにのみ示しています。

属性の読み込み

［**属性の読み込み**］をクリックして、次の例に示すように、オブジェクトの属性が読み込まれるときにイベントを生成します。

```
Oct 26 11:38:35 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0323|READ_ATTRIBUTE|0|dvc=164.99.179.60
dvchost=WIN-37D8M9SKD2U rt=Oct 25 2017 23:08:35 dtz=India Standard Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.60 spt=18369 suser=CN\=WIN-37D8M9SKD2U-NDS,O\=novell duser=CN\=WIN-
37D8M9SKD2U-NDS,O\=novell cs2Label=Class Name cs2=NCP Server cs3Label=Tree Name
cs3=TREE910W cs4Label=Correlation ID cs4=eDirectory#1# cs6Label=Attribute Name
cs6=cefConfiguration flexString2Label=SubEvent flexString2=DSE_READ_ATTR
cat=Attributes reason=0 outcome=Success
```

属性の削除

［**属性の削除**］をクリックして、次の例に示すように、オブジェクトから属性が削除されるときにイベントを生成します。

```
Oct 24 22:54:36 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0009|DELETE_ATTRIBUTE|0|dvc=164.99.179.60
dvchost=WIN-37D8M9SKD2U rt=Oct 24 2017 22:54:36 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.60 spt=21184 suser=CN\=WIN-37D8M9SKD2U-NDS,O\=novell duser=CN\=WIN-
37D8M9SKD2U-NDS,O\=novell cs2Label=Class Name cs2=NCP Server cs3Label=Tree Name
cs3=TREE910W cs4Label=Correlation ID cs4=eDirectory#2#a9ea8944-6a78-4a69-9c11-
727635aa79e8 cs6Label=Attribute Name cs6=Network Address flexString2Label=SubEvent
flexString2=DSE_DELETE_ATTRIBUTE flexNumber2Label=Grouping flexNumber2=736694
cat=Attributes reason=0 outcome=Success
```

値の追加

［**値の追加**］ をクリックして、次の例に示すように、属性に値が追加されるときにイベントを生成します。

```
Oct 24 02:38:12 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0006|ADD_VALUE|0|dvc=164.99.179.60 dvchost=WIN-
37D8M9SKD2U rt=Oct 24 2017 02:38:12 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.60 spt=0 suser=CN\=WIN-37D8M9SKD2U-NDS,O\=novell duser=.[Pseudo
Server] cs1Label=Attribute Value cs1=720575940530274304 cs3Label=Tree Name
cs3=TREE910W cs4Label=Correlation ID cs4=eDirectory#0#f9787bd7-0541-47ca-9391-
5a4bada90f02 cs6Label=Attribute Name cs6=treeReferral flexString2Label=SubEvent
flexString2=DSE_ADD_VALUE flexNumber2Label=Grouping flexNumber2=684713
cat=Attributes reason=0 outcome=Success
```

値の削除

［**値の削除**］をクリックして、次の例に示すように、属性から値が削除されるときにイベントを生成します。

```
Oct 24 02:38:12 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0007|DELETE_VALUE|0|dvc=164.99.179.60 dvchost=WIN-
37D8M9SKD2U rt=Oct 24 2017 02:38:12 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.60 spt=0 suser=CN\=WIN-37D8M9SKD2U-NDS,O\=novell duser=.[Pseudo
Server] cs1Label=Attribute Value cs1=720575940530274304 cs3Label=Tree Name
cs3=TREE910W cs4Label=Correlation ID cs4=eDirectory#0#1c411e7f-9657-474e-8e8e-
80fc92921f96 cs6Label=Attribute Name cs6=localReferral flexString2Label=SubEvent
flexString2=DSE_DELETE_VALUE flexNumber2Label=Grouping flexNumber2=684714
cat=Attributes reason=0 outcome=Success
```

属性値の比較

［**属性値の比較**］をクリックして、次の例に示すように、属性値が比較されるときにイベントを生成します。

EBAイベント

このイベントセットは、eDirectoryのEBA関連操作の監査に適用できます。EBA関連の操作としては、EBAの有効化や無効化、サーバの追加や削除、サーバ間のEBACAの移動、さらにはndsloginさえもあり得ます。

EBAイベントの例:

このセクションには、次のEBAイベントの例が含まれています。

- 932 ページの 「サービスの環境設定の変更」

注: 次の各セクションで紹介する例は、参考のためにのみ示しています。

サービスの環境設定の変更

次の例に示されているように、eDirectoryツリーにEBA関連の変更がある場合、［**サービスの環境設定の変更**］をクリックしてイベントを生成します。

```
Sep 17 16:34:56 eDirectory
CEF:0|eDirectory|eDirectory|9.2|CEF0B0503|MODIFY_SERVICE_CONFIG|1|dvc=164.99.179.2
16 dvchost=SLESSP1-216 rt=Sep 17 2019 16:34:56 dtz=IST
sourceServiceName=CN\=SLESSP1-216,O\=novell sproc=eDirectory#DS src=164.99.179.216
spt=0 cs1Label=CertAuthOldSvrAddress cs1=164.99.179.216
cs2Label=CertAuthNewSvrAddress cs2=164.99.179.216 cs3Label=Tree Name cs3=TREE216
cs4Label=Correlation ID cs4=eDirectory#4294967295# cs6Label=Server Name
cs6=CN\=SLESSP1-216,O\=novell flexString2Label=SubEvent
flexString2=DSE_EBA_MOVE_EBA_CA flexNumber2Label=Grouping flexNumber2=205
cat=Security reason=0 outcome=Success
```

J トラブルシューティング

XDASのトラブルシューティング

Novell XDASをインストールする際は、次の情報に留意してください。

XDASモジュールを初期化中のエラー

考えられる原因: XDASモジュールの初期化時に、xdasconfig.propertiesファイルに記載したサーバのIPまたはポート番号に接続することはできません。次のメッセージが表示されます。

```
log4cxx: Could not instantiate TCP Socket to <IP>. All logging
will FAIL.

log4cxx: IO Exception : status code = 111
```

アクション: この問題を回避するには次の手順に従ってください。

1. xdasconfig.propertiesファイルに指定したサーバのIPまたはポート番号が正しいかどうかを確認します。
2. リモートサーバが到達可能で、指定したポートで接続を受け付けるかどうかを確認します。
3. xdasauditdsモジュールを再ロードします。

TCP接続が失われる

考えられる原因: リモートサーバが到達可能でないか、指定したポートで接続を受け付けない場合、次のエラーが表示されます。

```
log4cxx: Detected problem with TCP connection to <IP>. All logging
will FAIL.

log4cxx: IO Exception : status code = 32
```

アクション: この問題を回避するには次の手順に従ってください。

1. リモートサーバが到達可能で、指定したポートで接続を受け付けるかどうかを確認します。
2. xdasauditdsモジュールを再ロードします。

SSL証明書ファイルの問題

考えられる原因: SSL証明書ファイルが無効であるか、xdasconfig.propertiesファイルの指定の場所に存在しません。次のエラーが表示されます。

```
log4cxx: could not load verify locations for SSL
```

アクション: この問題を回避するには次の手順に従ってください。

1. 有効な証明書ファイルへの絶対パスを指定します。
2. xdasauditdsモジュールを再ロードします。

リモートサーバへのネットワーク接続が失われる

ソース: 次のエラーが表示されます。

```
log4cxx: SSL write failed for <IP>. All logging will FAIL.
```

アクション: この問題を回避するには次の手順に従ってください。

1. リモートサーバが到達可能で、指定したポートで接続を受け付けるかどうかを確認します。
2. xdasauditdsモジュールを再ロードします。

SSL接続に失敗した

考えられる原因: TLS/SSLハンドシェークが失敗したか、接続障害が発生したため、SSL接続が失敗します。以下のようなエラーメッセージが表示されます。

```
log4cxx: SSL Connect Failed to <IP>
```

アクション: この問題を回避するには次の手順に従ってください。

1. リモートサーバが到達可能で、指定したポートで監視(リスン)しているかどうかを確認します。
2. 証明書が有効かどうかを確認します。
3. xdasauditdsモジュールを再ロードします。

SNMPのトラブルシューティング

必要なトラップが生成されない

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

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

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

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

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

ndssnmpsaを停止するには、次のように入力します。

Linux: /etc/init.d/ndssnmpsa stop

ndssnmpsaを開始するには、次のように入力します。

Linux: /etc/init.d/ndssnmpsa start

SNMPグループオブジェクト

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

ndsconfig *add -m snmp*

WindowsサーバでのSNMPオブジェクト作成エラー

対応しているWindowsプラットフォームのサーバにeDirectoryをインストールしている間に、SNMPグループオブジェクトの作成エラーが発生した場合は、SNMPグループオブジェクトを手動で作成する必要があります。SNMPオブジェクトを手動で作成する手順については、513ページの第18章「NetIQ eDirectoryのSNMPサポート」を参照してください。

eDirectory SNMP初期化コンポーネント。エラーコード: -255または初期化に失敗しました。エラーコード: -255

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

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

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

LDAP SNMP統計が報告されない

匿名バインドが無効になっていると、LDAP SNMP統計が報告されません。

この問題を解決するには、次の操作を行います。

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

サブエージェントにアクセスする際のセグメント化失敗エラー

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

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

eDirectory 8.7.3からeDirectory 9.0にアップグレードした後に発生するの問題

eDirectory 8.7.3からeDirectory 9.0にアップグレードした後に、次のようなエラーが発生する可能性があります。

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

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

eDirectory 9.0ではeDirectoryがlocalhostを監視しないため、このエラーが発生します。以前のバージョンのndssnmp.cfgファイルには、デフォルトでSERVER localhostが設定されていました。

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

たとえば、ndssnmp.cfgファイルに次のように入力します。

```
SERVER test-server
```

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

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

NDSサブエージェントの起動時のエラー

サブエージェントが失敗して次のメッセージが表示される場合があります。

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

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

```
export  SNMP_MAJOR_VERSION=10
```

ndssnmpsaの再起動

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

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

ndssnmpsaを停止するには、次のコマンドを入力します。

```
/etc/init.d/ndssnmpsa stop
```

ndssnmpsaを開始するには、次のように入力します。

```
/etc/init.d/ndssnmpsa start
```

edir.mibのコンパイル

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

SNMP設定ファイルの変更

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

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

新しいツリーをインストールした後のSNMPの使用

eDirectory 9.0 を初めてインストールする(新しいツリーを作成する)際に、サーバにインストールされているWindows SNMPサービスに依存するサービスが1つ以上ある場合、eDirectoryはSNMPサービスをシャットダウンできません。このような場合は、eDirectoryをインストールした後にSNMPを使用することができません。

次の手順に従って、SNMPサービスを再起動してください。

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

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

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

アンインストールを完了するには、次の手順を実行します。

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

eDirectoryをインストールするとWindows 2012上のSNMPが停止する

eDirectoryのインストール後に、SNMPが処理を停止して次のエラーメッセージが表示されます。

SNMP subagent error -672

解決策:

1 eDirectoryをインストールした後で、SNMPサービスをインストールし、設定します。
2 eDirectoryサーバでdssnmpsupport.exeを実行します。

注: MpsSvc serviceがeDirectoryサーバ上で実行されている場合にのみ、dssnmpsupport.exeを適用してください。

---

iMonitorのトラブルシューティング

iMonitorを使用しての2バイト文字を含むオブジェクトの参照

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

単一のサーバツリーでのエージェントヘルスチェック

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

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

perishable_data-active: OFF

および

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

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

iMonitorレポートで1時間ごとのレコードが保存されない

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

作成および変更のタイムスタンプ

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

iMonitorで整列されていないレポート画面レイアウトの実行

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

この問題に対処するには、ページを更新します。

iMonitorがエラー-672を表示する

- **Linux:** dsdumpツールがiMonitorと同時に実行されていると、iMonitorがエラー-672を表示します。この問題を解決するには、dsdumpツールを終了してから、iMonitorを開始します。
- **Windows:** dsbrowseツールまたはdseditツールがiMonitorと同時に実行されていると、iMonitorがエラー-672を表示します。この問題を解決するには、dsbrowseツールおよびdseditツールを終了してから、iMonitorを開始します。

iMonitorがエラー-702を表示する

ユーザオブジェクトにグループエントリのACL権利を割り当てると、iMonitorに、eDirectoryサーバをアップグレードした後のエントリの検証中にエラーメッセージが表示されます。

ndsimonhealth.confファイルのValidACLFlagsの値を手動で更新し、eDirectoryサーバを再起動する必要があります。

タイムスタンプが16進数形式で表示される

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

Internet Explorer 11でのiMonitorトレース設定の問題

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

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

iManagerのトラブルシューティング

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

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

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

破損通知のトラブルシューティング

破損通知は、削除、移動、名前変更、復元などの操作中に、eDirectoryが参照整合性を保持するためにオブジェクトに付加する操作属性です。たとえば、グループAにユーザBというメンバーが含まれているとき、ユーザBが削除されると、ディレクトリは自動的にグループAからユーザBへの参照を削除します。eDirectory 9.0では、削除、移動、および名前変更の操作によって生成される破損通知が、デフォルトで最適化されます。

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

破損通知には大きく分類して3つの種類があります。

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

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

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

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

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

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

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

削除されたオブジェクトの場合、「停止」のプライマリ破損通知に関連するすべての破損通知が最後のステータス(パージ可能)まで進められ、そのステータスがすべてのレプリカに同期された後で、新しい処理がデータベースに残っているエントリハスクの削除を担当します。これらのハスクを削除するために、パージ処理が自動的に実行されます。パージ処理は、手動でスケジュールでき、254ページの「エージェントアクティビティの表示」で説明しているように、その自動スケジュール間隔を変更することもできます。

孤立した破損通知の解決

破損通知オブジェクトを表示した状態で、リング周辺の破損通知を比較しながらレプリカリングを調べます。

- 破損通知のコピーがないレプリカがあり、すべての属性値がパージ可能ではない場合、このオブジェクトはレプリカリング周辺で矛盾しており、破損通知が孤立していると考えられます。
- オブジェクトがすべてのレプリカに矛盾なく存在している場合、同期エラー、または破損通知処理にエラーが発生しているために次のステータスに進まない可能性があります。

この問題を回避するには次の手順に従ってください。

- **推奨される方法:** レプリカリング内のサーバのいずれかにeDirectory 8.6以降のバージョンを使用する場合、iMonitorのオブジェクトを参照し、［Send Single Entry］を選択します。これにより、その他のすべてのレプリカに信頼されていない送信が実行されます。

- **避けるべき方法:** 孤立した破損通知のコピーを持つレプリカリングにあるすべてのサーバがeDirectory 8.6よりも前のバージョンの場合、DSBrowseを-aオプションでロードして、オブジェクトを参照し、エントリにタイムスタンプを設定します。これにより、このサーバに存在するオブジェクトを信頼されたコピーとして指定します。Novellでは、実際にはオブジェクトを信頼されたオブジェクトとして指定することはお勧めしません。

外部参照の孤立した破損通知の解決

オブジェクトの破損通知がこのサーバに保存されていない(該当するオブジェクトが外部参照の)場合、次を実行します。

- 一致する破損通知が実オブジェクトに含まれているかどうかをチェックします。一致する破損通知が含まれていない場合、この破損通知は孤立しています。
- 一致する破損通知が実オブジェクトに含まれている場合、実オブジェクトの破損通知の問題を解決してから、ExtRefパーティションにある破損通知の問題を処理してください。

この問題を回避するには次の手順に従ってください。

- **推奨されない方法:** タイムスタンプオプションが選択されているDSRepairを実行します。
- **推奨されない方法:** 実レプリカをサーバに移動し、使用可能な状態になってから破損通知が処理されるのを待ちます。破損通知が処理されたら、レプリカは削除してもかまいません。

破損通知に関する同期の問題の解決

破損通知が正確に同期するようにするには、次のことを実行してください。

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

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

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

  遷移ベクトルを調査します。

破損通知に関するエラーの検索

エラーを検索するには、エージェントプロセスのステータス: 破損通知を検査してください。

- エージェントプロセスステータス: 破損通知で起こりうる一般的な問題には、次のものがあります。

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

  -601および-603は、適切に削除されていないサーバ、またはサーバオブジェクトに不明なベースクラスが含まれるサーバを示します。
- このページに表示されるエラーは致命的なものではありません。そのパーティションで破損通知処理が次回実行されるときに、この操作が再試行されます。このページに表示された問題を解決して、再試行まで待機してください。

以前の操作

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

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

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

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

NetIQ eDirectoryへの移行

Sun OneスキーマのNetIQ eDirectoryへの移行

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

手順1: スキーマキャッシュの更新操作を実行する

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

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

次に例を示します。

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

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

手順 2: エラーを解決するためにエラーLDIFファイルを訂正する

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

  LDAPエラー: 53 (DSAが動作しません)

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

  LDAPエラー: 16 : (該当する属性はありません)

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

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

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

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

  これを解決するには、次の3つのいずれかのオプションを使用できます。

  オプション1:

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

  次に例を示します。

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

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

  オプション2:

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

  次に例を示します。

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

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

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

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

オプション3:

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

cnをTopに追加するには2つの方法があります。

- **方法1:**

  次のようなファイルを作成し、topsch.ldfと命名します。

  ```
  version : 1

  dn:cn=schema

  changetype :modify

  delete : objectclasses

  objectclasses : ( 2.5.6.0 NAME 'top' STRUCTURAL )

  -

  add:objectclasses

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

  次のNetIQインポート/エクスポート変換コマンドラインを使用します。

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

  次に例を示します。

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

- **方法2:**

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

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

  LDAPエラー: 16 (該当する属性はありません)

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

次に例を示します。

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

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

次のように変更する必要があります(最終行の変更に注意してください):

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

手順3: LDIFファイルをインポートする

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

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

次に例を示します。

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

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

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

これを解決するには、次の手順を実行します。

手順1: スキーマキャッシュの更新操作を実行する

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

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

次に例を示します。

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

手順 2: エラーを解決するためにエラーLDIFファイルを訂正する

失敗したエントリは次のようにerr.ldfファイルに記述されています。

```
dn: cn=schema

changetype: modify

delete: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' )

-

add: objectclasses

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

-
```

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

```
dn: cn=schema

changetype: modify

delete: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' )

-

add: objectclasses

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

手順3: LDIFファイルをインポートする

次のICEコマンドを使用して、変更されたエントリをインポートします。

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

次に例を示します。

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

OpenLDAPからNetIQ eDirectoryへの移行

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

nmasinst -addmethod *admin_context treename configfile* -h *Hostname*:*port*-w *password*

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

OpenLDAPスキーマのeDirectoryへの移行

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

手順1: スキーマキャッシュの更新操作を実行する

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

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

次に例を示します。

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

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

手順 2: エラーを解決するためにエラーLDIFファイルを訂正する

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

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

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

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

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

Open LDAPデータのNetIQ eDirectoryへの移行

次のコマンドを実行してデータを移行します。

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

次に例を示します。

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

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

移行後にPAMをNetIQ eDirectoryで動作可能にする

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

/etc/ldap.confファイルの変更

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

ディレクトリ内のデータの変更

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

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

属性: sasDefaultLoginSequence

値: 単純パスワード

スキーマのトラブルシューティング

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

スキーマのトラブルシューティング

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

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

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

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

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

LDAP構文マッピングのトラブルシューティング

DS構文の中には、LDAP構文に固有にマッピングされないものもあります。これは、eDirectory 9.1以前で発生します。

この問題は、eDirectory 9.1 SP1で修正されています。以前のマッピングに戻る場合は、NDSD_NLDAP_PRE911_SCHEMA環境変数を任意の値に設定します。

DSRepairのトラブルシューティング

Linux上のNFSマウントされたDIBでのDSRepairの実行

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

-Rオプションを指定してDSRepairを実行したときにハングアップする

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

レプリケーションのトラブルシューティング

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

iManagerを使用した暗号化複製の設定

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

暗号化複製を使用したツリーのマージに失敗する

暗号化複製が有効になっている場合、ツリーのマージに失敗します。マージを行う前に、各ツリーでセキュリティ保護された複製を無効にします。ツリーにEBAが有効なサーバが含まれる場合、ツリーのマージが成功することがあります。ただし、マージ後、ツリーが不安定になり、複製が適切ではないため認証が失敗する原因となります。

eDirectoryレプリカ問題から回復する

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

レプリケーションの削除の詳細については、『レプリカの管理NetIQ eDirectory 9.0 管理ガイド』のレプリカを管理する()を参照してください。

クローンDIBに関する問題のトラブルシューティング

クローンDIBの-601および-603エラーによる失敗

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

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

これらの問題を回避するには、暗号化属性と暗号化複製を無効にします。

オフラインのバルクロード処理の直後にクローンDIBに失敗する

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

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

暗号化複製機能を有効にしたクローン作成における問題

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

NetIQ公開鍵インフラストラクチャサービスのトラブルシューティング

PKI操作が機能しない

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

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

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

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

1. NetIQ iManagerで、［**役割およびタスク**］ボタン  をクリックします。
2. ［**eDirectory管理**］>［**オブジェクトの変更**］の順にクリックします。
3. W0オブジェクト名およびコンテキスト(通常は、W0.KAP.Security)を指定して、［**OK**］をクリックします。
4. ［**値がある属性**］カラムで、［**NDSPKI:SDキーサーバDN**］を選択してから、［**編集**］をクリックします。
5. ［**セキュリティドメインキーサーバのDN**］フィールドで別のサーバの名前とコンテキストを指定してから、［**OK**］をクリックします。
6. ［**適用**］をクリックし、［**OK**］をクリックします。

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

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

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

PKIDiagの使用

PKIDiagは、Certificate Serverオブジェクトを診断および修復するために設計されたユーティリティです。PKIDiagを使用すると、次のような処理を行うことができます。

- サーバが移動された場合に、サーバ関連オブジェクトが正しい名前になっていて包含スキームに一致するように、それらのオブジェクトを名前変更または移動する。
- 必要なオブジェクトが存在しない場合に、それらのオブジェクトを作成する。
- オブジェクト間で必要な権限を付与する。
- オブジェクトがリンクされていない場合にリンクする。
- SSL CertificateIP証明書およびSSL CertificateDNS証明書が存在しない場合に、それらを作成する。
- SSL CertificateIP証明書およびSSL CertificateDNS証明書が期限切れになっている場合、期限切れが近づいている場合、または名前が正しくない場合に、それらを修復する。

PKIDiag機能は、iManagerのサーバ自動ヘルスチェックおよびデフォルト証明書の作成タスクという他の2つのプロセスで使用されます。

サーバ自動ヘルスチェックは、サーバが再起動された場合、またはDSREPAIRが実行された場合に必ず実行されます。デフォルト証明書の作成は、Certificate Serverのインストール時に作成されたデフォルト証明書を置き換える場合に使用する処理です。詳細については、723 ページの 「デフォルトのサーバ証明書オブジェクトを作成する」を参照してください。

PKIDiagとその使用方法の詳細については、TID #3640106 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3640106&sliceId=SAL_Public&dialogID=2494290&stateId=1%200%202492620)を参照してください。

サーバが同期するのを待機中

ユーザ証明書が作成された後、クライアントが新しい証明書を組み込むビューを更新できないことがあります。「サーバが同期するのを待機中」というメッセージが示されたダイアログボックスが表示されます。この時点で、ユーザ証明書の作成は完了していますが、その作成に関わったサーバの同期はまだ完了していません。このダイアログボックスは、ユーザの証明書の作成に影響を与えずに閉じることができます。

証明書のニックネーム再利用のエラー

ユーザ証明書の作成中にエラーが発生する場合は、その証明書に別のニックネームの使用を試みてください。指定したニックネームは、再利用できない可能性があります。

ユーザの秘密鍵のエクスポートで-1426エラー

ユーザオブジェクトが存在するパーティションのレプリカを保持するサーバはすべて、同じレベルの暗号化(米国向け/全世界向けNICI、または制限付きNICIをインポート)が必要です。各サーバで同じレベルの暗号化を保持していない場合、キーサイズが大きすぎると、ユーザの秘密鍵をエクスポートする際に、-1426エラーが表示される場合があります。

-1426エラーの発生後にユーザの秘密鍵をエクスポートするには、パーティションのレプリカを保持するサーバの暗号化をアップグレードするか、エクスポート可能な暗号化を保持するサーバからレプリカを削除する必要があります。

サーバが有効期限切れのSSL CertificateIP証明書を使用している

eDirectory 9.0では、SSL CertificateIP証明書はサポートされません。以前のバージョンからeDirectory 9.0にアップグレードする場合、SSL CertificateIP証明書はサーバに関連付けられたままになります。環境内の証明書の有効期限が切れた場合、SSL CertificateIP証明書は自動的には更新されません。

eDirectory 9.0にアップグレードした後ならいつでも、SSL CertificateIP証明書の代わりに、SSL CertificateDNS証明書の使用を開始できます。

外部認証局

VeriSignなどの一部のサードパーティの認証局では、サーバ証明書の署名に中間認証局を使用しています。これらの証明書をサーバ証明書オブジェクトにインポートするには、サーバ証明書とともに中間認証局とルート認証局証明書が、単一のPKCS #7形式のファイル(.P7B)内に含まれている必要があります。ご使用の認証局でこのファイルを提供できない場合は、Internet Explorer 5.5以降がインストールされたクライアントマシン上で次の手順を実行して、このファイルを作成できます。

1. サーバ証明書をInternet Explorerにインポートします。このインポートをするには、ファイルをダブルクリックするか、［**ファイル**］>［**開く**］を選択してから、そのファイル名を選択します。
2. Internet Explorerで、この外部認証局の証明書が信頼された証明機関としてリストされていない場合、中間認証局とルートレベル認証局を同じ方法でインポートします。
3. Internet Explorerで、［**ツール**］>［**インターネットオプション**］の順に選択します。［**コンテンツ**］タブを選択してから、［**証明書**］ボタンを選択します。
4. ［**個人**］タブで、対象のサーバ証明書を探します。そのサーバ証明書を選択して、［**エクスポート**］をクリックします。
5. ウィザードで［エクスポート ファイルの形式］ページが表示されるまでデフォルトを受け入れてから、このページで［Cryptographic Message Syntax Standard - PKCS #7証明書 (.p7b)］形式を選択します。
6. ウィザードを続行します。

   これで、PKCS #7ファイルをサーバ証明書オブジェクトにインポートできるようになります。

サーバの移動

サーバオブジェクトを移動する場合、そのサーバのLDAPオブジェクト、SASサービスオブジェクト、およびサーバ証明書オブジェクト(暗号化キーオブジェクト)も移動する必要があります。しかし、その次にそのサーバを再起動する際に、サーバ自動ヘルスチェック機能によって各オブジェクトは移動されます。

DNSサポート

サーバにDNSが設定されている場合、サーバ証明書のデフォルトのサブジェクト名は、次のようになります。

.CN=<*サーバのDNS名*>.O=<*ツリー名*>

サーバにDNSが設定されていない場合、デフォルトのサブジェクト名はサーバの完全識別名です。デフォルトのサブジェクト名を変更するには、証明書の作成処理中に［カスタム］を選択します。

eDirectoryからサーバを削除する

eDirectory™からサーバを削除し、その後同じ名前の同じコンテキストにそのサーバを再インストールする場合に、削除するサーバを表すSASサービスオブジェクトが存在するときは、そのオブジェクトも削除した場合にのみ、そのサーバの再インストールが正常に実行されます。

このプロセスは、次のように実行する必要があります。

1. デフォルトの証明書をバックアップする必要があるかどうかを判断します。バックアップする場合、それらをバックアップします。
2. デフォルトの証明書を削除します。
3. SASオブジェクトを削除します。

たとえば、MYSERVERという名前のサーバの場合、SASService-MYSERVERという名前のSASオブジェクトがサーバと同じコンテナに存在する可能性があります。サーバをツリーから削除した後で、サーバをツリーに再インストールする前に、このSASオブジェクトを(iManagerを使用して)手動で削除する必要があります。

サーバが組織の認証局またはSDキーサーバの場合、さらにいくつかの手順を実行する必要があります。これらの手順は、「TID #3623407 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3623407&sliceId=SAL_Public&dialogID=2494325&stateId=1%200%202492660)」に記載されています。

このサーバ用に作成されたデフォルトのサーバ証明書も削除する必要があります。これは、サーバが再度挿入されたときにそれらのサーバ証明書が再作成されるようにするためです。

これらの証明書は、「SSLCertificateIP-MYSERVER」および「SSLCertificateDNS-MYSERVER」です。これらの証明書を削除する際は、注意する必要があります。データがこれらの証明書のいずれかを使用して暗号化されていた場合は、証明書を削除する前にデータを取得する必要があります。

認証局のサブジェクト名の制限事項

サブジェクト名に@文字が含まれたサーバ証明書が原因で、SSL接続が失敗する場合があります。この問題の解決方法については、テクニカルサポートに問い合わせてください。

証明書の検証の速度

証明書の検証プロセスには、証明書のデータだけでなく、証明書チェーン内のデータに対する複数のチェックが含まれます。証明書チェーンは、ルート認証局証明書と、必要に応じて1つ以上の中間認証局の証明書からなります。

証明書とその関連付けられた証明書チェーン内の情報を検証することは、時間のかかる処理ではありません。ただし、次の場合、検証にかかる時間が長くなることがあります。

- 証明書が外部認証局によって署名されていた場合、1つ以上の証明書にCRL配布ポイント拡張が含まれています。

  この証明書を検証するには、チェーン内の該当する証明書ごとのCRLを取得する必要があります。この後、CRLを検査して、証明書が取り消されたかどうかを調べる必要があります。

  CRLが多い場合、またはCRL配布ポイントを運用しているサーバがビジー状態の場合、証明書の検証にしばらく時間がかかる場合があります。次のことを1つ以上を行って、必要な時間を短縮できます。

  - 証明書の取り消しステータスを確認するために使用する接続の速度をアップグレードします。
  - 認証局プロバイダに問い合わせます。
- 1つ以上の証明書にOCSP拡張がある場合。OCSPレスポンダがビジー状態のときは、検証にかなりの時間がかかることがあります。
- ユーザ証明書を検証している場合。

  サーバ証明書の場合、証明書チェーン全体がサーバ証明書とともに暗号化キーオブジェクトに保存されます。このため、サーバ証明書が検証済みの場合は、クライアントは1つのオブジェクトを読み込むだけで、必要な証明書すべてを入手できます。ただし、ユーザ証明書は異なる方法で保存されます。ユーザ証明書自体だけがユーザオブジェクトに保存されます。このため、クライアントはユーザ証明書を検証するために、セキュリティコンテナ内に格納されている他のオブジェクトから証明書チェーンを取得する必要があります。

組織の認証局によって署名されたユーザ証明書を検証するには、クライアントは認証局の証明書を取得するために組織の認証局のオブジェクトを読み込む必要があります。外部認証局によって署名されたユーザ証明書を検証するには、クライアントはユーザ証明書に一致する証明書チェーンを作成するために、セキュリティコンテナ内のルート認証局コンテナを読み込む必要があります。後者の場合、ユーザ証明書の検証が成功するように、管理者が外部認証局の証明書をルート認証局コンテナにインポート済みである必要があります。

信頼されなくなった有効期限切れの証明書をルート認証局コンテナから削除することで、ユーザ証明書の検証に要する時間を短縮することができます。

組織の認証局削除後の証明書検証

組織の認証局を削除する(バックアップと復元手順の実行中以外)場合、自己署名証明書をエクスポートして、ルート認証局コンテナ内に新しいルート認証局を作成する必要があります。新しいルート認証局を作成しなかった場合、これらの証明書を検証する際に次の動作が発生します。

- 削除した認証局によって署名されたユーザ証明書が無効になる。これは、ユーザ証明書に署名した認証局の証明書が組織の認証局オブジェクトまたはルート認証局コンテナ内で見つからないためです。これらのユーザ証明書を有効なままにしたい場合は、以前に削除した認証局の自己署名証明書をルート認証局コンテナに追加する必要があります。
- 削除した認証局によって署名されたサーバ証明書は、引き続き有効である。これは、削除した認証局の証明書がサーバ証明書とともに暗号化キーオブジェクトに格納されるためです。

  鍵の暗号漏洩、またはなんらかのセキュリティ違反(抜け穴)のために、組織の認証局を削除する場合、削除した認証局によって署名されたすべてのユーザ証明書およびサーバ証明書をただちに取り消す必要があります。それらの証明書を取り消すことができない場合は、それらを削除して、それぞれの所定の場所に新しい証明書を作成します。また、この組織の認証局の証明書をブラウザにインポートした可能性のあるすべてのユーザに対して、その証明書を削除するように指示する必要もあります。

セキュリティコンテナの名前変更

セキュリティコンテナの名前を変更することはできません。

ツリー認証局を再作成した後、eDirectoryが証明書を検証できない

eDirectoryを最新バージョンにアップグレードした場合、またはカスタムロケーションにインストールした場合、eDirectoryは認証局を再作成した後で証明書を検証することができません。

この問題を回避するため、eDirectoryのインストールパスがC:\NetIQ\eDirectory (Windowsの場合)および/var/opt/novell/eDirectory (Linuxの場合)以外である場合は、ツリー認証局を再作成するとき、またはCRLオブジェクトの作成中に、eDirectoryのインストールパスから見た正しいCRLファイルパスを指定する必要があります。エラーを避けるには、［認証局の設定］ウィザードから認証局を再作成する際にiManagerプラグインでカスタムオプションを選択し、正しいCRLファイルパスを指定する必要があります。たとえばeDirectoryは、デフォルトでCRLファイルをパスC:\NetIQ\eDirectory\htdoc\crl\にインストールします。eDirectoryをカスタムロケーションにインストールすることを選択した場合(C:*CustomLocation*\eDirectory\)、ツリー認証局を再作成する際にCRLファイルパスを忘れずに更新してください。C:*CustomLocation*\eDirectory\htdoc\crl\のように指定します

注: eDirectoryが以前のいずれかのバージョンでデフォルトの場所(C:\Novell\NDS\)にインストールされている場合でも、最新バージョンにアップグレードした後、ツリー認証局を再作成する際に前述の回避策を実行する必要があります。

Linuxでのユーティリティのトラブルシューティング

NetIQインポート/エクスポート変換ユーティリティ

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

ndsmergeユーティリティ

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

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

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

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

フルバックアップを実行する前にインクリメンタルバックアップを実行しようとすると、バックアップ操作が失敗します。

DSTraceユーティリティ

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

ndsbackupユーティリティ

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

ndsbackup sR 164.99.148.82:1524

データのバックアップ中に、eDirectoryから「NDS Error: Requires a Password」というエラーが表示される場合があります。これは、サーバに暗号化をマークする属性があるのに、-Eオプションを有効にしてバックアップデータを暗号化または復号化していないためです。

フルバックアップを実行する前にインクリメンタルバックアップを実行しようとすると、バックアップ操作が失敗します。

エラー - 786 DSRepairの実行中

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

eDirectoryユーティリティからユーザがNDSパスワードを使用して認証するように要求される

ユニバーサルパスワードを使用している場合、すべてのeDirectoryコマンドラインツールを認証するために、ユニバーサルパスワードをNDSパスワードと同期する必要があります。

NMASのトラブルシューティング

NMASのエラーコード

NMASの全エラーコードの一覧は、NMAS NDKにあります。

ログインメソッドおよびログインシーケンスの問題

- 各製品でNMASログインメソッドを正しく使用するには、eDirectoryパーティション内の少なくとも1つのNMASサーバが、NMASを使用する予定のユーザオブジェクトの読み込み/書き込みレプリカを保持する必要があります。
- ログインメソッドまたはポストログインメソッドによっては、それらがアクティブにされた場合に最初の［パスワード］フィールドを使用しないものもあります。パスワードを入力するためのプロンプトが表示されたら、［パスワード］フィールドを無視してプロンプトを閉じることができます。
- Novell Clientが［パスワード］フィールドを表示するように設定されている(デフォルト設定)場合、簡易パスワードやNDSパスワードなどの2つのパスワードメソッドは、ANDシーケンスで使用することができません。

管理に関する問題

- 段階的認証のユーザに対しては、明示的な権限を与える必要があります。継承された権限は機能しません。たとえば、管理者のスーパバイザ権は［ルート］コンテナで定義されます。管理者の権限は、ボリュームオブジェクトでは定義されません。管理者がボリュームのセキュリティラベルを「Logged In」から他のセキュリティラベルに変更した場合、管理者は適切な権限を取得できません。管理者は、ボリューム、ディレクトリ、またはボリュームのファイルに対して明示的な権限を割り当てる必要があります。
- ユニバーサルパスワードが有効になっている場合に、簡易パスワードを設定しようとすると、-1697エラーメッセージが返されます。
- DSBackup(ndsbackup)、DSRepair(ndsrepair)、DSMerge(ndsmerge)などのeDirectoryユーティリティでは、NDSパスワードのみで動作しますが、NMASの簡易パスワードでは動作しません。eDirectory 9.0では、ユニバーサルパスワードを使用します。

  ユニバーサルパスワードの詳細については、『*NetIQ Password Management 3.3.2 Administration Guide (NetIQ Password Management 3.3.2管理ガイド)* (https://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html)』を参照してください。

- ラベルを作成または名前変更する際に、［OK］をクリックするか、またはタブを切り替えると、［Save Changes made for Labels?］プロンプトに［いいえ］と応答した場合でも、常にそのラベルは作成または名前変更されます。変更をキャンセルする場合は、［キャンセル］ボタンをクリックする必要があります。ラベルが作成されると、そのラベルを削除することはできません。ただし、使用しないための名前(Unused_x)などに名前を変更することができます。
- NMASに対してXDAS監査を使用すると、次のイベントのDN形式はLDAP表記では生成されません。
  - 00290035 SASLメカニズムの結果
  - 00290061 Set Loginの設定
  - 00290062 Get Loginの設定
  - 00290064 Set Loginのシークレット

注: lscファイルで示されているように、ID (00290035、00290061など)はNMASイベントIDを指定します。NMASイベントIDは、XDAS形式のsubEventフィールドの一部です。

Linuxでどのメソッドを使用してもログインできない

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

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

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

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

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

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

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

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

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

   変更後:

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

3. 変更内容を保存し、ファイルを閉じます。

または

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

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

変更後:

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

3 変更内容を保存し、ファイルを閉じます。

WindowsでeDirectoryのインストール時に誤ったインストール先パスがインストール先パスのフィールドに表示される

eDirectoryのインストール時に、デフォルトのインストール場所を受け入れるのではなく、［**ブラウズ**］アイコンをクリックして別の場所を選択してから、フォルダを選択せずに［ブラウズ］ダイアログを閉じた場合、誤ったインストール先パスが［**インストール先パス**］フィールドに表示されます。この問題は、eDirectoryをWindows Server 2012 Standard Edition (64ビット)およびWindows Server 2012 R2 (64ビット)にインストール中にのみ発生します。

この問題を回避するには、パスを所要の場所に手動で変更してください。

SLPがWindowsで正しく設定されていない場合、サーバの追加が失敗する

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

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

1 サービスロケーションプロトコルサービスを停止します。
2 C:\Windows\slp.confファイルを削除します。
3 C:\Windows\System32\Novell\eDir\OpenSLPフォルダを削除します。
4 Registry HKLM\SYSTEM\CurrentControlSet\Services\slpdからSLPDサーバのレジストリキーを削除します。
5 管理者の役割で再度セットアップを実行します。

ディレクトリサービスがロードされない場合のHTTPSTKへのアクセス

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

Windowsでsadminパスワードを設定する

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

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

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

   たとえば、次のように入力します。

   ```
   http://MyServer:80/dhost
   ```

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

   ```
   http://137.65.135.150:80/dhost
   ```

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

Linuxでsadminパスワードを設定する

Linuxでsadminパスワードを設定するには、［DHost Remote Management］ページまたはndsconfigユーティリティのいずれかを使用することができます。

DHostリモート管理ページの使用

/dhost URLまたはルートページから［DHost Remote Manager］ページにアクセスして、sadminパスワードを設定します。sadminパスワードを設定または変更するには、eDirectoryサーバを実行している必要があります。

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

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

   たとえば、次のように入力します。

   ```
   http://MyServer:80/dhost
   ```

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

   ```
   http://137.65.135.150:80/dhost
   ```

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

ndsconfigの使用

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

サーバコンソールから、次のように入力します。:

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

ここで*password*は、新しいsadminパスワードです。

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

データ暗号化のトラブルシューティング

NetIQ eDirectory 9.0では、特定の重要データをディスクに保存したり、クライアントがそのデータにアクセスしたりしている間に、データを暗号化できます。この章では、eDirectory 9.0で暗号化属性やレプリケーション機能を使用しているときに発生する場合があるエラーの情報を提供します。

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

-6090 0xFFFFE836 ERR_ER_DISABLED

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

考えられる原因

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

アクション

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

-6089 0xFFFFE837 ERR_REQUIRE_SECURE_ACCESS

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

Source

eDirectoryまたはNDS.

考えられる原因

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

アクション

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

考えられる原因

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

アクション

セキュリティ保護されていないチャネルから暗号化属性にアクセスできるように、暗号化属性ポリシーの設定を変更します。詳細については、313ページの第11章「eDirectoryのデータを暗号化する」を参照してください。

考えられる原因

暗号化されたレプリケーションがパーティションレベルまたはパーティションのレプリカ間で設定されているときにこのエラーを受け取った場合は、レプリカリングはeDirectory 9.0以前のサーバを使用しています。

アクション

レプリカリング内のすべてのサーバをeDirectory 9.0に対応するバージョンにアップグレードします。

-666 FFFFFD66 INCOMPATIBLE NDS VERSION

本文がここに入ります。

考えられる原因

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

アクション

サーバをeDirectoryに対応したバージョンにアップグレードします。

考えられる原因

親パーティションがeDirectory 9.0以前のサーバ(混合バージョンのリング)を使用しており、子パーティションに有効なERがある場合は、マージおよび/またはパーティションの結合操作は許可されず、ERR_INCOMPATIBLE_DS_VERSIONエラーが返されます。

この理由は、チャイルドパーティションにパーティションレベルでERが有効な重要なデータが含まれており、ペアレントパーティションにeDirectory9.0以前のサーバがあるからです。マージ中に、eDirectory9.0サーバ間でのみERが有効になっていると、重要なデータはeDirectory9.0以前のサーバに複製しているとき危険にさらされます。

アクション

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

   または

2. ペアレントまたはチャイルドパーティションでERを無効にします。

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

重複暗号化アルゴリズムの問題

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

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

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

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

ストリーム属性の暗号化

ストリーム属性が平文データとして存在する可能性があります。この原因は、eDirectory 9.0ではストリーム属性を暗号化しないことによります。

iManagerを使用した暗号化複製の設定

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

iManagerを使用した暗号化属性の表示または変更

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

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

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

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

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

暗号化複製が有効になっているツリーのマージに失敗する

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

Limberで-603エラーが表示される

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

この問題を回避するには、次のいずれかの手順を実行します。

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

eDirectory Management Toolbox

NetIQ eDirectory管理ツールボックス(eMBox)を使用すると、サーバ上でもリモートでもeDirectoryのバックエンドユーティリティすべてにアクセスできます。

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

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

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

eMToolサービスを停止できない

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

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

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

復元を実行すると-6020エラーになる

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

移動したオブジェクトの削除

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

ダイナミックグループの移動に関する問題

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

からネットワークアドレスを修復する際の問題

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

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

エラー: 接続できませんでした。エラー: 11004

フランス語のマニュアルページの参照

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

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

移動したオブジェクトの削除

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

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

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

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

DSTrace実行中にTERMによって生じる問題

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

eMBoxで2バイト文字が処理されない

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

SASL-GSSAPIに関する問題のトラブルシューティング

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

複数のユーザオブジェクトによる問題

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

認証ID

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

ログファイル

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

エラーメッセージ

エラーメッセージ	原因
SASL-GSSAPI: Reading Object user_FDN FAILED eDirectory error code	このエラーは、eDirectory内で生成されます。ケルベロスのプリンシパル名がユーザオブジェクト(userdn)にアタッチされていません。
SASL-GSSAPI: Reading Object Realm_FDN FAILED eDirectory error code	このエラーは、eDirectory内で生成されます。レルムオブジェクトは存在しません。
SASL-GSSAPI: Not enough memory	特定の操作を行うためのメモリが不足しています。
SASL-GSSAPI: Invalid Input	クライアントからの入力が不良、または無効です。
SASL-GSSAPI: NMAS error NMAS error code	このエラーは、NMASで生成される初期エラーです。
SASL-GSS: Invalid LDAP service principal name *LDAP_service_principal_name*	LDAPサービスのプリンシパル名が無効になっています。
SASL-GSS: eDirectoryからのLDAPサービスプリンシパルキーの読み込みに失敗しました	**原因:** LDAPサービスのプリンシパルオブジェクトが作成されていません。
	原因: レルムオブジェクトのマスタキーが変更されています。
	原因: LDAPサービスのプリンシパルオブジェクトが、属するレルムのサブツリーで見つかりませんでした。
SASL-GSS: GSSコンテキストの作成に失敗しました	**原因:** クライアント、KDC、およびeDirectoryサーバで、時間が同期していません。
	原因: LDAPサービスプリンシパルのキーは、ケルベロスデータベースで変更されましたが、eDirectoryで更新されていません。
	原因: 暗号化タイプがサポートされていません。
SASL GSSAPI: Invalid user FDN = *user_FDN*	クライアントに提供されたユーザFDNが有効ではありません。
SASL GSSAPI: No user DN is associated with principal *client_principal_name*	サブツリーの下のユーザオブジェクトが、ケルベロスプリンシパル名にアタッチされていません。

エラーメッセージ	原因
SASL GSSAPI: 複数のユーザDNがプリンシパル *client_principal_name*に関連付けられています ldap_simple_bind_s: Invalid credentials major = 1, minor =0	サブツリー下の複数のユーザオブジェクトが、同じプリンシパルに関連付けられています。 **原因:** 原因は、KDCサーバのLDAPサービスプリンシパルとeDirectoryサーバのLDAPサービスプリンシパルの間で、バージョンが一致していないことが考えられます。これは、keytabファイルにLDAPサービスプリンシパルキーを取り出すたびに、キーのバージョンナンバーが増加するためです。 **アクション:** 次の手順を実行します。 1. バージョン番号が同期するように、eDirectoryサーバでキーを更新します。 2. クライアントでチケットを破棄します。 3. プリンシパル用にTGTを再度取得します。 4. LDAP saslバインド操作を実行します。

eDirectory のエラーログを管理する

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。

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。

エラーメッセージ	説明
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。

エラーメッセージ	説明
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。
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。
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。
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での重大度レベルの設定: 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。

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)。重大度レベルの詳細については、968 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設定します。

n4u.server.log-levels=*severity_level*

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

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

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

  注: ログレベル(n4u.server.log-levels)をLogDbgに設定する際に、環境変数NDSD_EVENT_DISK_CACHEをtrueに設定する必要があります。

Linuxでの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
```

Windowsでの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、「968 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**］>［**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。

注: Windowsでは、ドライバトレースレベルの重大度は動作しません。

Windowsでの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Windows上

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。

その他

コンテナのバックアップ

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

eDirectoryへの繰り返しログイン

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

イベントシステム統計を有効にする

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

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

Linuxでのメモリ破損問題のトラッキング

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

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

ndsdでのMALLOC_CHECK_の設定

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

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

異常ログアウト後にTCP接続が終了しない

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

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

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

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

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

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

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

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

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

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

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

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

設定を(再起動後も)永続的なものにするには、以下の手順を行います。

次のエントリを/etc/sysctl.confに追加します。

- net.ipv4.tcp_keepalive_time=120
- net.ipv4.tcp_keepalive_probes=3
- net.ipv4.tcp_keepalive_intvl=20

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

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

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

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

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

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

SecretStoreの無効化Linuxで

eDirectory管理者は、次の処理を使用してLinuxでSecretStoreを無効にできます。

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

   libsss.so
   libssncp.so
   libssldp.so

2. サーバを再起動します。

WindowsでのSecretStoreの無効化

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

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

   lsss.dll
   sss.dlm
   ssncp.dlm
   ssldp.dlm

2. サーバを再起動します。

dsbk環境設定ファイルの場所

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

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

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

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

システムクラッシュの後でndsdが起動しない

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

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

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

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

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

LDAPが匿名検索要求に関するRFCに準拠していない

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

eDirectory 9.0のカスタムインスタンスでのポートのトラブルシューティング

eDirectory 9.0で、インスタンスのデフォルトサーバがダウンしたときに、カスタムロケーションに新しいインスタンスを設定する場合、インスタンスのデフォルトポートが取得されます。デフォルトインスタンスのポートはカスタムロケーションのインスタンスに割り当てられるため、デフォルトインスタンスは開始されません。

ホストを再起動する前に「「eDirectory 8.8のカスタムインスタンスでのポートのトラブルシューティング」」の手順に従ってください。

ホストの再起動

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

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

所定のNCPポート上のループバックアドレスでndsdが監視していない

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

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

重要: eDirectory 9.0にアップグレードする前に、eDirectoryのすべてのインスタンスを起動する必要があります。

LDAPトランザクションOID

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

LDAPトレースの-5871エラーおよび-5875エラー

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

ツリーの名前が変更されるとNDSConsが-625エラーを出す

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

注: ツリー名の変更は、EBA有効のサーバがツリーに含まれている場合にはサポートされない操作です。

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

この問題を回避するには次の手順に従ってください。

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

または

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

Linuxプラットフォームで同時接続ユーザ数を制限できない

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

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

SLPが原因でndsdがシャットダウンに失敗する

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

この問題を解決するには:

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

WindowsでのNLDAPの再起動

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

LDAP経由のSecretStore

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

SecretStoreのロック解除後に、パスフレーズを変更できない

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

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

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

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

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

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

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

HTTPサーバでSSL CertificateIPの有効期限が切れた後もその証明書を使用する

eDirectoryの古いバージョンからeDirectory 9.0にアップグレードした場合、HTTPサーバでSSL CertificateIPの有効期限が切れた後も、引き続きその証明書を使用します。これは、eDirectory 8.8 SP8が、SSL CertificateIPを保守せず、SSL CertificateIPの有効期限が切れたり、SSL CertificateIPが削除されたりした場合でも、その証明書を再発行しないためです。

このため、SSL CertificateIPの有効期限が切れたり、SSL CertificateIPが削除されたりした場合は、SSL CertificateIPを手動で作成する必要があります。この作成は、iManagerプラグインを使用するか、またはSSL CertificateIPではなくSSL CertificateDNSを使用して行います。

eDirectoryに2つの異なるldapsearchバイナリが含まれている

LDAPツールのセット(ldapadd、ldapconfig、ldapdelete、ldapmodify、ldapmodrdn、およびldapsearch)が2つ、eDirectoryがインストールされているSLESシステム上に(openldap2-client rpmとともに)存在します。一方のセットは、SLESオペレーティングシステムによってインストールされて/usr/binにあり、他方のセットは、eDirectoryによってインストールされて/opt/novell/eDirectory/binにあります。

両方のLDAPツールのセットの基本機能は同じですが、それぞれのセットで、基本機能のほかに独自の機能を追加しています。PATH環境変数のパスの設定によって、使用するツールのセットは異なります。このため使用できる機能も異なります。

ldapsearchが何も結果を返さない

バインドユーザが検索フィルタの一部である属性すべての読み込み権限を持っていないと、ldapsearchは結果を何も返しません。

この問題を回避するには、バインドユーザが、検索フィルタの一部である属性すべての読み込み権限があることを確認します。

eDirectory 9.1で仮想一覧の表示にエラーメッセージが表示される

eDirectory 9.1で、仮想一覧の表示(VLV)が実行されているeDirectoryサーバにパーティションレプリカすべてが存在しているわけではない場合、VLVがエラーメッセージを表示されます。

すべてのパーティションレプリカが、VLMが実行されているeDirectoryサーバ内に存在していることを確認します。

Datadirを新しい場所に移動した後、eDirectoryが起動しない

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

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

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

  /usr/lib/systemd/system/ndsdtmpl-etc-opt-novell-eDirectory-conf-ds.conf@.service。
- systemctl daemon-reloadコマンドを使用して、デーモンを再ロードします。
- eDirectoryサーバを再起動します。

Restrictedの実行ポリシーにより、eDirectoryのインストールが失敗する

PowerShellに対するWindowsの実行ポリシーがRestrictedに設定されている場合、eDirectoryのインストールは失敗します。

この問題を回避するには、PowerShellに対するWindows実行ポリシーをRemotesignedに設定します。

IPV6に関する問題のトラブルシューティング

IPv6でのOpenLDAPのセキュアな検索が失敗する

LDAPサーバに関連付けられている証明書の［**サブジェクトの代替名**］フィールドにIPv6アドレスが設定されている場合、IPv6でのOpenLDAPのセキュアな検索は失敗します。

ICEプラグインがIPV6アドレスには使用できない

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

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

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

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

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

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

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

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

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

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

LinuxおよびWindowsの未指定のIPv6アドレスのリスナ

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

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

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

EBAのトラブルシューティング

ユーザDNにOIDのない属性が含まれると、EBAベースのログインが失敗する

ユーザDNにOIDのない属性が含まれると、EBAベースのログインが失敗します。

この問題を回避するには、スキーマのユーザDN属性にOIDを追加する必要があります。