

Oracle® Solaris 11.2 ディレクトリサービスと
ネームサービスでの作業: LDAP

ORACLE®

Part No: E53901
2014 年 7 月

Copyright © 2002, 2014, Oracle and/or its affiliates. All rights reserved.

このソフトウェアおよび関連ドキュメントの使用と開示は、ライセンス契約の制約条件に従うものとし、知的財産に関する法律により保護されています。ライセンス契約で明示的に許諾されている場合もしくは法律によって認められている場合を除き、形式、手段に関係なく、いかなる部分も使用、複写、複製、翻訳、放送、修正、ライセンス供与、送信、配布、発表、実行、公開または表示することはできません。このソフトウェアのリバース・エンジニアリング、逆アセンブル、逆コンパイルは互換性のために法律によって規定されている場合を除き、禁止されています。

ここに記載された情報は予告なしに変更される場合があります。また、誤りが無いことの保証はいたしかねます。誤りを見つけた場合は、オラクル社までご連絡ください。

このソフトウェアまたは関連ドキュメントを、米国政府機関もしくは米国政府機関に代わってこのソフトウェアまたは関連ドキュメントをライセンスされた者に提供する場合は、次の通知が適用されます。

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

このソフトウェアもしくはハードウェアは様々な情報管理アプリケーションでの一般的な使用のために開発されたものです。このソフトウェアもしくはハードウェアは、危険が伴うアプリケーション（人的傷害を発生させる可能性があるアプリケーションを含む）への用途を目的として開発されていません。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用する場合、安全に使用するために、適切な安全装置、バックアップ、冗長性（redundancy）、その他の対策を講じることは使用者の責任となります。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用したことに起因して損害が発生しても、オラクル社およびその関連会社は一切の責任を負いかねます。

OracleおよびJavaはOracle Corporationおよびその関連企業の登録商標です。その他の名称は、それぞれの所有者の商標または登録商標です。

Intel, Intel Xeonは、Intel Corporationの商標または登録商標です。すべてのSPARCの商標はライセンスをもとに使用し、SPARC International, Inc.の商標または登録商標です。AMD, Opteron, AMDロゴ, AMD Opteronロゴは、Advanced Micro Devices, Inc.の商標または登録商標です。UNIXは、The Open Groupの登録商標です。

このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することがあります。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

目次

このドキュメントの使用方法	7
1 LDAP ネームサービスの概要	9
この Oracle Solaris リリースの LDAP	9
LDAP ネームサービスの概要	10
LDAP での情報の格納方法	11
比較: LDAP ネームサービスとその他のネームサービス	12
LDAP コマンド	12
一般的な LDAP コマンド	13
LDAP 操作に固有の LDAP コマンド	13
2 LDAP と認証サービス	15
LDAP ネームサービスのセキュリティーモデル	15
Transport Layer Security	17
クライアント資格レベル	18
enableShadowUpdate スイッチ	19
LDAP クライアントの資格ストレージ	20
LDAP ネームサービスの認証方法	21
LDAP 内の特定のサービスの認証方法の指定	23
プラグイン可能な認証方法	24
LDAP サービスモジュール	24
pam_unix_* サービスモジュール	26
Kerberos サービスモジュール	28
PAM およびパスワードの変更	28
LDAP アカウント管理	29
pam_unix_* モジュールによる LDAP アカウント管理	30
アカウント管理に pam_ldap モジュールを使用した pam_conf ファイルの例	31
3 LDAP ネームサービスの計画要件	33
LDAP 計画の概要	33

LDAP クライアントプロファイル構成の計画	35
LDAP ネットワークモデル	35
ディレクトリ情報ツリー	36
セキュリティー上の考慮点	37
LDAP マスターサーバーおよび複製サーバーの配備計画	38
LDAP データ生成の計画	40
サービス検索記述子とスキーママッピング	40
SSD の説明	41
サマリー: LDAP実装を準備するデフォルトのクライアントプロファイル属性	43
LDAP を構成するための空白のチェックリスト	43
4 Oracle Directory Server Enterprise Edition への LDAP クライアントの設定	45
ディレクトリサーバーの構成に関する情報の準備	45
LDAP のサーバー情報	45
LDAP のクライアントプロファイル情報	46
インデックス表示の使用	47
ディレクトリツリー定義の作成	47
▼ LDAP ネームサービスを使用するように Oracle Directory Server Enterprise Edition を構成する方法	48
LDAP のサーバー構成例	49
ディレクトリ情報ツリーの構築	49
サービス検索記述子の定義	56
LDAP サーバーへのデータの移入	57
▼ サーバーにデータを移入する方法	58
追加のディレクトリサーバー構成タスク	59
メンバー属性を使用したグループメンバーシップの指定	59
追加プロファイルを使用してディレクトリサーバーを生成する	60
ディレクトリサーバーを構成してアカウント管理を有効にする	61
5 LDAP クライアントの設定	67
LDAP クライアント設定の準備	67
LDAP とサービス管理機能	68
ローカル LDAP クライアント属性の定義	69
LDAP クライアントの管理	70
LDAP クライアントの初期化	70
LDAP クライアント構成の変更	73
LDAP クライアントの初期化解除	73
クライアント認証での LDAP の使用	74
PAM の構成	74

TLS のセキュリティーの設定	76
6 LDAP のトラブルシューティング	79
LDAP クライアントステータスのモニタリング	79
ldap_cachemgr デーモンが実行中であることの確認	79
現在のプロファイル情報の確認	81
基本的なクライアント/サーバー間通信の検証	82
クライアント以外のマシンからのサーバーデータの確認	82
LDAP の構成で発生する問題とその解決方法	82
未解決のホスト名	82
LDAP ドメイン内のシステムにリモートアクセスできない	83
ログインできない	83
検索が遅すぎる	84
ldapclient コマンドがサーバーにバインドできない	84
デバッグでの ldap_cachemgr デーモンの使用	85
設定中に ldapclient コマンドがハングアップする	85
ユーザー別の資格情報を使用したときの問題の解決	85
syslog ファイルが 82 Local Error を示している	85
Kerberos が自動的に初期化されない	86
syslog ファイルが無効な資格証明を示している	86
スイッチチェック時に ldapclient init コマンドに失敗する	86
LDAP ネームサービス情報の検出	86
すべての LDAP コンテナを表示する	87
すべてのユーザーエントリ属性を表示する	88
7 LDAP ネームサービス (リファレンス)	89
LDAP 用の IETF スキーマ	89
RFC 2307bis ネットワーク情報サービススキーマ	90
メールエイリアススキーマ	95
ディレクトリユーザーエージェントのプロファイル (DUAProfile) スキーマ	95
Oracle Solaris スキーマ	98
プロジェクトスキーマ	98
役割ベースのアクセス制御と実行プロファイルスキーマ	99
LDAP 用の Internet Printing Protocol 情報	100
Internet Print Protocol 属性	101
Internet Print Protocol ObjectClass	107
プリンタ属性	108
Sun プリンタ ObjectClass	108

LDAP 用の汎用ディレクトリサーバーの要件	109
LDAP ネームサービスで使用するデフォルトフィルタ	109
8 NIS+ から LDAP への移行	113
NIS から LDAP への移行サービスの概要	113
NIS から LDAP への移行用ツールとサービス管理機能	114
NIS から LDAP への移行の対象読者	115
NIS から LDAP への移行サービスを使用しない場合	115
NIS から LDAP への移行サービスがユーザーに与える影響	116
NIS から LDAP への移行に関する用語	117
NIS から LDAP への移行コマンド、ファイル、およびマップ	117
サポートされる標準マッピング	118
NIS から LDAP への移行 (タスクマップ)	119
NIS から LDAP への移行のための前提条件	120
NIS から LDAP への移行サービスの設定	121
▼ 標準マッピングを使用して N2L サービスを設定する方法	122
▼ カスタムマッピングまたは非標準マッピングを使用して N2L サービスを設定する方法	124
カスタムマップの例	127
Oracle Directory Server Enterprise Edition での NIS から LDAP への移行のベストプラクティス	129
Oracle Directory Server Enterprise Edition での仮想リスト表示 (VLV) インデックスの作成	129
Oracle Directory Server Enterprise Edition でのサーバータイムアウトの回避	131
Oracle Directory Server Enterprise Edition でのバッファオーバーランの回避	131
NIS から LDAP への移行に関する制限	132
NIS から LDAP への移行のトラブルシューティング	132
よくある LDAP エラーメッセージ	133
NIS から LDAP への移行に関する問題	134
NIS に戻す方法	138
▼ 以前のソースファイルに基づくマップに戻す方法	138
▼ 現在の DIT 内容に基づくマップに戻す方法	139
用語集	141
索引	149

このドキュメントの使用方法

- 概要 - LDAP ネームサービス、その使用を計画する方法、および LDAP を実装する手順について説明します。
- 対象読者 - システム管理者。
- 必要な知識 - LDAP に関連する概念および技術への精通。

製品ドキュメントライブラリ

この製品の最新情報や既知の問題は、ドキュメントライブラリ (<http://www.oracle.com/pls/topic/lookup?ctx=E36784>) に含まれています。

Oracle サポートへのアクセス

Oracle のお客様は、My Oracle Support を通じて電子的なサポートを利用することができます。詳細は、<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> を参照してください。聴覚に障害をお持ちの場合は、<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> を参照してください。

フィードバック

このドキュメントに関するフィードバックを <http://www.oracle.com/goto/docfeedback> からお聞かせください。

◆◆◆ 第 1 章

LDAP ネームサービスの概要

Lightweight Directory Access Protocol (LDAP) は、ディレクトリサーバーにアクセスして分散型ネームサービスやその他のディレクトリサービスを使用するために使用される、セキュアなネットワークプロトコルです。この標準ベースのプロトコルは、階層的なデータベース構造をサポートしています。同じプロトコルを使用して、UNIX とマルチプラットフォームの両方の環境でネームサービスを提供できます。

注記 - LDAP という用語は、プロトコル自体よりはむしろ、ネームサービスを指すようになりました。この本では、LDAP という用語はプロトコルよりはむしろ、サービスを指す際に使用されません。

背景については、次のソースを参照してください。

- *Oracle Directory Server Enterprise Edition 配備ガイド*
- *Oracle Directory Server Enterprise Edition 管理ガイド*
- 使用しているバージョンの Oracle Directory Server Enterprise Edition に対応したインストールガイド

この章では、LDAP サービスの概要について説明します。

この Oracle Solaris リリースの LDAP

Oracle Solaris 11.2 では、既存の Oracle Solaris RBAC スキーマに `SolarisQualifiedUserAttr` オブジェクトクラスが追加されました。このクラスには複数の値を指定できる属性が含まれているため、このクラスによって現行の `SolarisUserQualifier` クラスが拡張されます。新しいオブジェクトクラスを使用して変更された RBAC スキーマを表示するには、[99 ページの「役割ベースのアクセス制御と実行プロファイルスキーマ」](#)を参照してください。

SolarisQualifiedUserAttr クラスが使用可能になる前に既存の LDAP 構成がすでに存在している場合は、`ldapadd` コマンドを使用してこのクラスをその構成に追加できます。

LDAP ネームサービスの概要

Oracle Solaris では、Oracle Directory Server Enterprise Edition (以前の Sun Java System Directory Server) とともに、LDAP がサポートされています。ただし、一般的なディレクトリサーバーも LDAP サーバーとして機能します。この本では、*ディレクトリサーバー*と *LDAP サーバー*という用語は同義語であり、交互に使用されています。

LDAP ネームサービスは、Oracle Solaris でサポートされているさまざまなネームサービスの 1 つです。その他のネームサービスについては、『[Oracle Solaris 11.2 ディレクトリサービスとネームサービスでの作業: DNS と NIS](#)』で説明しています。Oracle Solaris のさまざまなネームサービスの比較については、[12 ページの「比較: LDAP ネームサービスとその他のネームサービス」](#)を参照してください。

LDAP は、次のサービスを実行します。

- ネームサービス - LDAP はクライアントリクエストに従ってネームデータを提供します。たとえば、ホスト名を解決する際に、LDAP では完全修飾ドメイン名を指定することで DNS などが機能します。ドメイン名が `west.example.net` であると仮定します。`gethostbyname()` または `getnameinfo()` を使用してホスト名がアプリケーションからリクエストされる場合、LDAP は値 `server.west.example.net` を返します。
- 認証サービス - LDAP はクライアントの識別情報、認証、およびアカウントに関する情報を管理および提供します。つまり、LDAP は認証済みの要求元のみ情報を提供するようにセキュリティ対策を実装します。

LDAP ネームサービスには、次のような利点があります。

- アプリケーション固有のデータベースを置き換えることで、情報は連結され、管理する個別のデータベースの数が削減されます。
- さまざまなネームサービスでデータを共有できます。
- データ用の集中的なリポジトリが使用されます。
- マスターと複製との間で、より頻繁にデータの同期化を実行できます。
- LDAP には、プラットフォーム間およびベンダー間の互換性があります。

LDAP ネームサービスには、次の制限事項が適用されます。

- LDAP サーバーをそのクライアントとして使用することはできない。
- 同時に NIS と LDAP のクライアントの両方になることはできません。

注記 - 制限が不足すると、LDAP ネームサービスの設定と管理が複雑になるため、注意深い計画が必要になります。

LDAP での情報の格納方法

LDAP で提供される情報は、ディレクトリ情報ツリー (DIT) に格納されます。データ自体の形式は、LDAP データ交換形式 (LDIF) です。DIT は、定義された LDAP スキーマに従った、階層的に構造化された情報のコンテナで構成されます。

通常、LDAP を使用したほとんどのネットワークでは、大部分の DIT に従ったデフォルトスキーマで十分です。ただし、DIT には柔軟性があります。DIT のデフォルト構造は、クライアントプロファイルに検索記述子を指定することでオーバーライドできます。検索記述子の詳細は、[40 ページの「サービス検索記述子とスキーママッピング」](#)を参照してください。

次の表には、DIT のコンテナおよび各コンテナに格納される情報のタイプを示します。

表 1-1 デフォルト DIT コンテナ内の情報タイプ

デフォルトコンテナ	情報タイプ
ou=Ethers	bootparams, ethers
ou=Group	group
ou=Hosts	ホストの hosts, ipnodes, publickey
ou=Aliases	aliases
ou=Netgroup	netgroup
ou=Networks	networks, netmasks
ou=People	ユーザーの passwd, shadow, user_attr, audit_user, publickey
ou=Protocols	protocols
ou=Rpc	rpc
ou=Services	services
ou=SolarisAuthAttr	auth_attr
ou=SolarisProfAttr	prof_attr, exec_attr

デフォルトコンテナ	情報タイプ
ou=projects	project
automountMap=auto_*	auto_* (自動マウントのマップ)

比較: LDAP ネームサービスとその他のネームサービス

LDAP ネームサービスに加えて、その他のタイプのネーミングサービスも一般に使用されます。

次の表には、各ネームサービスの機能の比較を示します。これらのサービスはすべて、Oracle Solaris でサポートされています。

表 1-2 ネームサービスの機能比較

	DNS	NIS	LDAP	ファイル
名前空間	階層	一層	階層	ファイル
データストレージ	ファイル/リソースレコード	2 列のマップ	ディレクトリ (可変) インデックス化したデータベース	テキストベースのファイル
サーバー	マスター/スレーブ	マスター/スレーブ	マスター/複製 複数マスター複製	なし
セキュリティ	DNSSEC (可変)	なし (root またはなし)	Kerberos、TLS、SSL (可変)	なし
トランスポート	TCP/IP	RPC	TCP/IP	ファイル入出力
規模	大域	LAN	大域	ローカルホストのみ
データ	ホスト	すべて	すべて	すべて

LDAP コマンド

Oracle Solaris OS には、2 セットの LDAP 関連のコマンドがあります。1 番目のセットは、LDAP ネームサービスの構成が必要である一般的な LDAP コマンドで構成されます。2 目のセットは、クライアント上の共通の LDAP 構成を使用し、LDAP ネームサービスとともに、またはなしで構成されているクライアント上で実行できます。

次のセクションで、対応するマニュアルページを参照すると、コマンドが一覧表示されます。

一般的な LDAP コマンド

一般的な LDAP コマンドは任意のシステム上で実行でき、システムに LDAP ネームサービスを構成する必要はありません。LDAP コマンド行ツールは、認証やバインドパラメータを含む、一般的なオプションセットをサポートします。このツールでは、LDAP データ交換フォーマット (LDIF) というディレクトリ情報を表現する共通のテキストベース書式がサポートされています。次のコマンドを使用すると、ディレクトリエントリを直接操作できます。

コマンド	説明	マニュアルページ
<code>ldapsearch</code>	LDAP スキーマで指定したエントリを検索します。	ldapsearch(1)
<code>ldapmodify</code>	スキーマ内の LDAP エントリを変更します。	ldapmodify(1)
<code>ldapadd</code>	スキーマに LDAP エントリを追加します。	ldapadd(1)
<code>ldapdelete</code>	スキーマから LDAP エントリを削除します。	ldapdelete(1)

LDAP 操作に固有の LDAP コマンド

次の表には、クライアントシステムを構成する、またはクライアントシステムを構成する必要がある LDAP コマンドを一覧表示します。

コマンド	説明	マニュアルページ
<code>ldapaddent</code>	対応する <code>/etc</code> ファイルからスキーマに LDAP エントリを作成します。	ldapaddent(1M)
<code>ldaplist</code>	LDAP サーバーから取得された情報を表示します。	ldaplist(1)
<code>idsconfig</code>	クライアントに提供するデータを DIT に移入します。	idsconfig(1M)
<code>ldapclient</code>	LDAP クライアントマシンを初期化します。	ldapclient(1M)

◆◆◆ 第 2 章

LDAP と認証サービス

LDAP ネームサービスは、LDAP リポジトリを 2 通りの方法で使用できます。

- ネームサービスと認証サービスの両方のソース
- 厳密にネームデータのソースのみ

この章では、LDAP の認証サービスについて具体的に説明し、次のトピックを扱います。

- [15 ページの「LDAP ネームサービスのセキュリティーモデル」](#)
- [18 ページの「クライアント資格レベル」](#)
- [21 ページの「LDAP ネームサービスの認証方法」](#)
- [24 ページの「プラグイン可能な認証方法」](#)
- [29 ページの「LDAP アカウント管理」](#)

LDAP ネームサービスのセキュリティーモデル

LDAP では、クライアントが入手する情報の完全性および機密性を保証するために、認証や制御されたアクセスなどのセキュリティー機能がサポートされています。

LDAP リポジトリ内の情報にアクセスするには、クライアントはまず、ディレクトリサーバーとの識別情報を確立します。この識別情報は匿名にすることも、LDAP サーバーによって認識されたホストまたはユーザーとして指定することもできます。クライアントの識別情報とサーバーのアクセス制御情報 (ACI) に基づいて、LDAP サーバーは、クライアントによるディレクトリ情報の読み取りを許可します。ACI の詳細については、使用しているバージョンの Oracle Directory Server Enterprise Edition の管理者ガイドを参照してください。

認証には次の 2 種類があります。

- プロキシ認証は、識別情報がリクエストの送信元ホストに基づいていることを意味します。ホストが認証されたあとに、そのホスト上のすべてのユーザーがディレクトリサーバーにアクセスできます。
- ユーザー別の認証は、識別情報が各ユーザーに基づいていることを意味します。ディレクトリサーバーにアクセスして、さまざまな LDAP リクエストを発行するには、すべてのユーザーを認証する必要があります。

PAM (Pluggable Authentication Module) サービスは、ユーザーログインが成功したかどうかを判断します。次のリストで示すように、認証の基盤は使用される PAM モジュールによって異なります。

- `pam_krb5` モジュール - Kerberos サーバーが認証の基盤です。このモジュールの詳細は、[pam_krb5\(5\)](#) のマニュアルページを参照してください。このガイドよりも広範囲にわたって Kerberos について説明している『[Oracle Solaris 11.2 での Kerberos およびその他の認証サービスの管理](#)』も参照してください。
- `pam_ldap` モジュール - LDAP サーバーとローカルホストの両方が認証の基盤として機能します。このモジュールの詳細は、[pam_ldap\(5\)](#) のマニュアルページを参照してください。`pam_ldap` モジュールを使用する場合は、[29 ページの「LDAP アカウント管理」](#)を参照してください。
- 同等の `pam_unix_*` モジュール - 情報はホストから提供され、認証はローカルで決定されます。

注記 - `pam_unix` モジュールは削除されたので、Oracle Solaris ではサポートされていません。このモジュールは、同等またはそれ以上の機能を備えた別のサービスモジュールセットで置き換えられました。このガイドでは、`pam_unix` は `pam_unix` モジュールではなく、同等の機能を備えたモジュールを指します。

`pam_ldap` を使用する場合、ネームサービスおよび認証サービスは別の方法でディレクトリにアクセスします。

- ネームサービスは、事前定義された識別情報に基づくディレクトリから、さまざまなエントリおよびその属性を読み取ります。
- 認証サービスは、正しいパスワードが指定されているかどうかを判断するために、LDAP サーバーに対してユーザー名とパスワードを認証します。

Kerberos と LDAP を同時に使用すると、認証サービスとネームサービスの両方をネットワークに提供できます。Kerberos を使用すると、企業でシングルサインオン (SSO) 環境をサポートできます。また、ユーザーまたはホストごとに LDAP ネームデータのクエリー検索を実行する際にも、同じ Kerberos 識別システムを使用できます。

Kerberos を認証の実行に使用する場合は、ユーザー別モードの要件として、LDAP ネームサービスも有効にする必要があります。これにより、Kerberos は二重の機能を提供できます。ディレクトリへの認証に、サーバーへの Kerberos 認証、および主体 (ユーザーまたはホスト) に対する Kerberos 識別情報が使用されます。これにより、システムの認証に使用されるのと同じユーザー識別情報がディレクトリの認証にも使用され、検索と更新が実行されます。管理者は、必要に応じ、アクセス制御情報 (ACI) をディレクトリ内で使用して、ネームサービスで得られる結果を制限できます。

Transport Layer Security

TLS (Transport Layer Security) を使用すると、LDAP クライアントとディレクトリサーバー間の通信がセキュリティー保護されるため、機密性とデータの完全性の両方を保証できます。TLS プロトコルは、Secure Sockets Layer (SSL) プロトコルのスーパーセットです。LDAP ネームサービスでは、TLS 接続がサポートされています。ただし、SSL を使用するとディレクトリサーバーおよびクライアントに負荷がかかります。

次の一覧は、TLS を使用するための要件を示しています。

- SSL を使用するためのディレクトリサーバーおよび LDAP クライアントの構成。
SSL を使用するように Oracle Directory Server Enterprise Edition を構成する場合は、使用しているバージョンの Oracle Directory Server Enterprise Edition に対応した管理者ガイドを参照してください。
- 必要なセキュリティーデータベースのインストール (特に、証明書および鍵データベースファイル)。
 - Netscape Communicator の古いデータベースフォーマットを使用する場合は、cert7.db と key3.db をインストールします。
 - Mozilla の新しいデータベースフォーマットを使用する場合は、cert8.db、key3.db、および secmod.db をインストールします。

cert* ファイルには、信頼できる証明書が含まれています。key3.db ファイルには、クライアントの鍵が入ります。LDAP ネームサービスクライアントがクライアント鍵を使用しない場合でも、key3.db ファイルをインストールする必要があります。secmod.db ファイルには、PKCS#11 などのセキュリティーモジュールが入ります。

TLS セキュリティーを設定する場合は、[76 ページの「TLS のセキュリティーの設定」](#)を参照してください。

クライアント資格レベル

LDAP サーバーは、クライアントの資格レベルに従って LDAP クライアントとの認証を行います。LDAP クライアントは、次の資格レベルのいずれかを割り当てることができます。

anonymous **anonymous** 資格レベルでは、すべてのユーザーが使用可能なデータにのみアクセスできます。LDAP BIND 操作は実行されません。

anonymous 資格レベルには、高いセキュリティリスクがあります。すべてのクライアントが、自分が書き込みアクセス権を持っている DIT 内の情報 (別のユーザーのパスワードや自分の識別情報など) を変更できます。さらに、**anonymous** レベルでは、すべてのクライアントがすべての LDAP ネームエントリおよび属性への読み取りアクセス権を持つことができます。

注記 - Oracle Directory Server Enterprise Edition を使用すると、IP アドレス、DNS 名、認証方法、および時間に基づいてアクセスを制限できます。つまり、セキュリティ対策を実装できます。詳細については、使用しているバージョンの Oracle Directory Server Enterprise Edition の『*管理者ガイド*』のアクセス権の管理に関する章を参照してください。

proxy **proxy** 資格レベルでは、クライアントが LDAP バインド資格の単一の共有セットへのバインドを行います。共有セットは、*プロキシアカウント*とも呼ばれます。プロキシアカウントには、ディレクトリへのバインドを許可されるエントリを設定できます。このアカウントには、LDAP サーバー上でネームサービス機能を実行するのに十分なアクセス権が必要です。

プロキシアカウントは、システムごとに共有されるリソースです。つまり、プロキシアクセスを使用してシステムにログインしているユーザー (root ユーザーなど) は、同じ情報を参照します。**proxy** 資格レベルを使用するすべてのクライアントシステムで、**proxyDN** および **proxyPassword** 属性を構成する必要があります。さらに、**proxyDN** には、すべてのサーバーで同じ **proxyPassword** を指定する必要があります。

暗号化された **proxyPassword** はローカルのクライアントに格納されません。プロキシユーザーのパスワードが変更された場合は、そのプロキシユーザーを使用するすべてのクライアントでパスワードを更新する必要があります。また、LDAP アカウントのパスワード有効期間を使用する場合は、必ずプロキシユーザーを除外してください。

別のクライアントグループに対しては別のプロキシを設定できます。たとえば、すべての販売部門のクライアントが会社全体でアクセス可能なディレクトリおよび販売部門のディレクトリにのみアクセスできるように制限するプロキシを構成できます。給与情報が含まれる人事部門のディレクトリへのアクセスは禁止されます。もっとも極端な例として、各クライアントに別個のプロキシを割り当てることや、すべてのクライアントに同じプロキシを割り当てることも可能です。

さまざまなクライアントに複数のプロキシを設定する計画がある場合は、選択を慎重に検討してください。プロキシエージェントが不足していると、リソースへのユーザーアクセスを制御する能力が制限されることがあります。ただし、プロキシが多過ぎる場合、システムの設定および保守が困難になります。適切な権限をプロキシユーザーに付与する必要がありますが、その程度は環境によって異なります。どの認証方法が構成にもっとも適しているかを判定する方法については、[20 ページの「LDAP クライアントの資格ストレージ」](#)を参照してください。

proxy 資格レベルは、特定のシステム上のすべてのユーザーおよびプロセスに適用されます。異なるネーミングポリシーを使用する必要があるユーザーは、別のシステムにログインするか、ユーザー別の認証モデルを使用する必要があります。

proxy anonymous proxy anonymous 資格レベルは複数值のエントリであり、複数の資格レベルが定義されます。このレベルでは、最初にプロキシ識別情報を使用して、割り当てられたクライアントの認証が試みられます。ユーザーのロックアウトやパスワードの期限切れなどが原因で認証に失敗した場合、クライアントは匿名アクセスを使用します。ディレクトリの構成方法に応じて、さまざまな資格レベルがさまざまなレベルのサービスに関連付けられています。

self self 資格レベルは、ユーザー別モードとも呼ばれます。このモードでは、主体と呼ばれる Kerberos 識別情報を使用して、認証対象のシステムまたはユーザーごとに検索が実行されます。ユーザー別の認証では、システム管理者は、アクセス制御情報 (ACI)、アクセス制御リスト (ACL)、役割、グループ、またはその他のディレクトリアクセス制御メカニズムを使用して、特定のユーザーまたはシステムの特定のネームサービスデータへのアクセスを許可または拒否できます。

ユーザー別の認証モデルを使用するには、次の作業が必要です。

- Kerberos シングルサインオンサービスの配備
- 1 つ以上のディレクトリサーバーでの SASL および SASL/GSSAPI 認証メカニズムのサポート
- Kerberos でホスト名の検索を実行するためにファイルとともに使用される DNS の構成
- nscd デーモンの有効化

enableShadowUpdate スイッチ

クライアント上で enableShadowUpdate スイッチが true に設定されている場合は、シャドウデータを更新するために管理者資格情報が使用されます。シャドウデータは、ディレ

クトリサーバーの `shadowAccount` オブジェクトクラスに格納されます。管理者資格情報は、69 ページの「ローカル LDAP クライアント属性の定義」で説明しているように、`adminDN` および `adminPassword` 属性の値によって定義されます。

管理者資格情報のプロパティは `proxy` 資格情報のプロパティと類似しています。ただし、管理者資格情報の場合、シャドウデータを読み取ったり更新するには、ユーザーはゾーンのすべての特権を持つか、`root` の有効な UID を持っている必要があります。



注意 - 管理者資格情報は、ディレクトリへのバインドが許可されるエントリに割り当てることができます。ただし、LDAP サーバーのディレクトリマネージャー識別情報 (`cn=Directory Manager`) には同じものを使用しないでください。

管理者資格情報が設定されたエントリは、ディレクトリへのシャドウデータの読み取りおよび書き込みに対する十分なアクセス権を持っている必要があります。エントリは、システムごとに共有されるリソースです。したがって、すべてのクライアントで `adminDN` および `adminPassword` 属性を構成する必要があります。

暗号化された `adminPassword` はローカルのクライアントに格納されます。パスワードには、クライアント用に構成された認証方式と同じ方式が使用されます。特定のシステム上のすべてのユーザーおよびプロセスは管理者資格情報を使用して、シャドウデータの読み取りおよび更新を行います。

LDAP クライアントの資格ストレージ

現在の LDAP 実装では、初期化中に設定されたプロキシ資格情報は、クライアントのプロファイルではなく、SMF リポジトリ内に格納されます。この実装によって、プロキシの識別名 (DN) およびパスワード情報に関連するセキュリティが向上します。

SMF リポジトリは `svc:/network/ldap/client` です。プロキシ識別情報を使用するクライアントのプロキシ情報が格納されます。同様に、資格レベルが `self` 以外であるクライアントのシャドウデータの更新も、このリポジトリに保存されます。

ユーザー別の認証を使用するクライアントの場合、認証時に各主体 (各ユーザーまたはホスト) 用の Kerberos 識別情報および Kerberos チケット情報が使用されます。ディレクトリサーバーは Kerberos 主体を DN にマッピングします。この DN の認証には、Kerberos 資格情報が使用されます。次に、ディレクトリサーバーは、必要に応じアクセス制御情報 (ACI) メカニズムを使用して、ネームサービスデータへのアクセスを許可または拒否します。

この環境では、ディレクトリサーバーへの認証に Kerberos チケット情報が使用されます。システムには、認証 DN またはパスワードは格納されません。したがって、`ldapclient` コマンドを使用してクライアントを初期化する場合は、`adminDN` および `adminPassword` 属性を設定する必要がありません。

LDAP ネームサービスの認証方法

`proxy` または `proxy-anonymous` の資格レベルをクライアントに割り当てる場合は、プロキシを認証する方法も選択する必要があります。デフォルトの認証方式は `none` (匿名によるアクセス) です。認証方法には、関連するトランスポートセキュリティオプションが含まれることもあります。

この認証方法は、資格レベルと同様に、複数値にすることができます。たとえば、クライアントプロファイルを設定することにより、クライアントが TLS でセキュリティ保護された `simple` メソッドを最初に使用してバインドを試みるようにできます。これが成功しない場合、クライアントは `sasl/digest-MD5` メソッドを使用してバインドを試みます。この場合、`authenticationMethod` 属性を `tls:simple;sasl/digest-MD5` のように構成します。

LDAP ネームサービスは、いくつかの Simple Authentication and Security Layer (SASL) メカニズムをサポートします。これらのメカニズムを使用すると、TLS なしでセキュアなパスワードを交換できます。ただし、これらのメカニズムはデータの完全性や機密性を保証するものではありません。SASL については、[IETF の Web サイト \(http://datatracker.ietf.org/\)](http://datatracker.ietf.org/) で RFC 4422 を検索してください。

次の認証メカニズムがサポートされています。

<code>none</code>	クライアントは、ディレクトリへの認証を行いません。この方法は、 <code>anonymous</code> 資格レベルと同等です。
<code>simple</code>	クライアントシステムは、ユーザーのパスワードを平文で送信してサーバーへのバインドを実行します。このため、セッションが IPsec により保護されていない限り、パスワードが漏洩しやすくなります。認証方式 <code>simple</code> を使用する主な利点は、すべてのディレクトリサーバーがこの方式をサポートしていること、および設定が容易であるという点です。
<code>sasl/digest-MD5</code>	クライアントのパスワードは認証中に保護されますが、セッションは暗号化されません。 <code>digest-MD5</code> の主な利点は、認証中にパスワードが平文で転送されないこと、 <code>simple</code> 認証方法よりセキュアである

ことです。digest-MD5 については、IETF の Web サイト (<http://datatracker.ietf.org/>) で RFC 2831 を検索してください。digest-MD5 は cram-MD5 よりも改善されています。

sasl/digest-MD5 を使用する場合、認証はセキュリティー保護されますがセッションは保護されません。

注記 - Oracle Directory Server Enterprise Edition を使用している場合は、パスワードをディレクトリ内に平文で格納する必要があります。

sasl/cram-MD5	LDAP セッションは暗号化されませんが、クライアントのパスワードは認証中に保護されます。このような廃止された認証方法は使用しないでください。
sasl/GSSAPI	この認証方法は、ユーザー別の検索を有効にするためにユーザー別モードとともに使用されます。クライアントの資格情報を持つユーザー別の nscd セッションは、sasl/GSSAPI 方法およびクライアントの Kerberos 資格情報を使用して、ディレクトリサーバーへのバインドを実行します。ディレクトリサーバーでは、アクセスをユーザー別に制御できます。
tls:simple	クライアントは simple 方法を使用してバインドを実行し、セッションは暗号化されます。パスワードは保護されます。
tls:sasl/cram-MD5	sasl/cram-MD5 を使用して、LDAP セッションの暗号化およびクライアントによるディレクトリサーバーへの認証が行われます。
tls:sasl/digest-MD5	sasl/digest-MD5 を使用して、LDAP セッションの暗号化およびクライアントによるディレクトリサーバーへの認証が行われます。



注意 - Oracle Directory Server Enterprise Edition で digest-MD5 を使用するには、パスワードを暗号化せずに格納する必要があります。sasl/digest-MD5 または tls:sasl/digest-MD5 認証方法を使用するプロキシユーザーのパスワードは、暗号化せずに格納する必要があります。この場合、userPassword 属性が読み取り可能にならないように、適切な ACI を使用して構成します。

次の表に、さまざまな認証方式およびその特性の概要を示します。

表 2-1 認証方法

方法	バインド	通信時のパスワード	Oracle Directory Server Enterprise Edition でのパスワード	セッション
none	なし	該当なし	該当なし	暗号化なし

方法	バインド	通信時のパスワード	Oracle Directory Server Enterprise Edition でのパスワード	セッション
simple	あり	平文	任意	暗号化なし
sasl/digest-MD5	あり	暗号化	平文	暗号化なし
sasl/cram-MD5	あり	暗号化	該当なし	暗号化なし
sasl/GSSAPI	あり	Kerberos	Kerberos	暗号化
tls:simple	あり	暗号化	任意	暗号化
tls:sasl/cram-MD5	あり	暗号化	該当なし	暗号化
tls:sasl/digest-MD5	あり	暗号化	平文	暗号化

LDAP 内の特定のサービスの認証方法の指定

`serviceAuthenticationMethod` 属性によって、特定のサービスに対応した認証方法が決まります。この属性がサービスに設定されていない場合は、`authenticationMethod` 属性の値が使用されます。

`enableShadowUpdate` スイッチが `true` に設定されている場合は、`ldap_cachemgr` デーモンも同じシーケンスに従って LDAP サーバーへのバインドを実行します。`serviceAuthenticationMethod` 属性が構成されていない場合は、`authenticationMethod` 属性の値を使用します。このデーモンは、`none` 認証方法を使用しません。

次のサービスに対応した認証方法を選択できます。

- `passwd-cmd` - ログインパスワードおよびパスワード属性を変更するために `passwd` コマンドで使用されます。詳細は、[passwd\(1\)](#) のマニュアルページを参照してください。
- `keyserv` - ユーザーの Diffie-Hellman 鍵ペアを作成および変更するために `chkey` および `newkey` ユーティリティーで使用されます。詳細は、[chkey\(1\)](#) および [newkey\(1M\)](#) のマニュアルページを参照してください。
- `pam_ldap` - `pam_ldap` サービスを使用するユーザーを認証するために使用されます。`pam_ldap` では、アカウントの管理がサポートされています。

注記 - ユーザー別モードでは、認証サービスとして Kerberos サービスモジュールが使用され、`ServiceAuthenticationMethod` は必要ありません。

次に示す例は、クライアントプロファイルの 1 セクションです。ここで、ユーザーはディレクトリサーバーへの認証に `sasl/digest-MD5` を使用しますが、パスワードの変更には SSL セッションを使用します。

```
serviceAuthenticationMethod=pam_ldap:sasl/digest-MD5
serviceAuthenticationMethod=passwd-cmd:tls:simple
```

プラグイン可能な認証方法

PAM フレームワークを使用すると、`pam_unix_*`、`pam_krb5`、および `pam_ldap_*` モジュールを含む複数の認証サービスから選択できます。

ユーザー別の認証を使用するには、`pam_krb5` を有効にする必要があります。ただし、ユーザー別の資格レベルを割り当てていない場合でも、`pam_krb5` 認証を使用できます。`proxy` または `anonymous` の資格レベルを使用してディレクトリサーバーのデータにアクセスする場合は、ディレクトリデータへのアクセスをユーザーごとに制限できません。

`anonymous` または `proxy` の認証を選択する場合は、同等の `pam_unix_*` モジュールではなく、`pam_ldap` モジュールを使用してください。`pam_ldap` モジュールは柔軟性が高く、より強固な認証方法をサポートし、アカウント管理を実行できます。

LDAP サービスモジュール

前述のとおり、`serviceAuthenticationMethod` 属性を定義すると、ユーザーによる LDAP サーバーへのバインド方法が決まります。定義しない場合は、`authenticationMethod` 属性が使用されます。`pam_ldap` モジュールによって、ユーザーの識別情報および指定されたパスワードを持つサーバーへのバインドが正常に実行されると、モジュールでユーザーの認証が行われます。

注記 - 以前は、pam_ldap アカウント管理を使用すると、すべてのユーザーがシステムにログインするたびに、認証用にログインパスワードを入力する必要がありました。そのため、ssh などのツールを使用した、パスワードに基づかないログインは失敗していました。

現在は、アカウント管理を実行し、ユーザーがログインしているときに Directory Server への認証を行わずにユーザーのアカウントステータスを取得できます。

Directory Server 上の新しい制御は 1.3.6.1.4.1.42.2.27.9.5.8 です。この制御は、デフォルトで有効になっています。デフォルトの制御構成を変更するには、ディレクトリサーバー上でアクセス制御情報 (ACI) を追加します。例:

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn>Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
allow (read, search, compare, proxy)
(groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

pam_ldap モジュールでは、userPassword 属性が読み取られません。クライアントが UNIX 認証を使用しない場合は、userPassword 属性への読み取りアクセス権を付与する必要があります。同様に、このモジュールでは認証方法として none がサポートされていません。



注意 - simple 認証方法を使用する場合は、第三者が暗号化されていない userPassword 属性を読み取ることができます。

次の表に、認証メカニズム間の主な相違点を示します。

表 2-2 LDAP での認証動作

イベント	pam_unix_*	pam_ldap	pam_krb5
パスワードの送信	passwd サービス認証方式を使用します	passwd サービス認証方式を使用します	パスワードではなく、Kerberos シングルサインオンテクノロジーを使用します
新規パスワードの送信	暗号化される	暗号化しません (TLS を使用しない場合)	Kerberos を使用します。パスワードはネットワークに送信されません
新規パスワードの格納	crypt 形式	Oracle Directory Server Enterprise	パスワードは Kerberos を使って管理されます

イベント	pam_unix_*	pam_ldap	pam_krb5
		Edition で定義されたパスワード格納スキーム	
パスワードの読み取りが必要か	あり	なし	なし
パスワード変更後の sasl/digestMD5 の互換性	ありません。暗号化されていないパスワードは格納されません。ユーザーを認証できません。	あり。デフォルトのストレージスキームが平文 (clear) に設定されていれば、ユーザーを認証できます。	ありません。sasl/GSSAPI が使用されます。Kerberos kdc を使用して LDAP ディレクトリサーバー内のパスワードデータベースを管理する場合を除き、パスワードがネットワーク上に送信されることも、ディレクトリサーバーに保存されることもありません。
パスワードポリシーがサポートされるか	はい。enableShadow Update を true に設定する必要があります。	はい (構成されている場合)。	pam_krb5(5) のマニュアルページ、および Kerberos V5 アカウント管理モジュールを参照してください。

pam_unix_* サービスモジュール

/etc/pam.conf ファイルを構成していない場合は、デフォルトで UNIX 認証が有効になります。

注記 - pam_unix モジュールは削除されたので、Oracle Solaris ではサポートされていません。このモジュールは、同等またはそれ以上の機能を備えた別のサービスモジュールセットで置き換えられました。このガイドでは、pam_unix は pam_unix モジュールではなく、同等の機能を備えたモジュールを指します。

次に示すモジュールは、元の pam_unix モジュールと同等の機能を備えています。対応するマニュアルページを使用すれば、モジュールが一覧表示されます。

[pam_authtok_check\(5\)](#)
[pam_authtok_get\(5\)](#)
[pam_authtok_store\(5\)](#)
[pam_dhkeys\(5\)](#)
[pam_passwd_auth\(5\)](#)

`pam_unix_account(5)`
`pam_unix_auth(5)`
`pam_unix_cred(5)`
`pam_unix_session(5)`

`pam_unix_*` モジュールは、従来の UNIX 認証モデルに従います。

1. クライアントは、ネームサービスからユーザーの暗号化されたパスワードを取得します。
2. ユーザーは、ユーザーパスワードの入力を求められます。
3. ユーザーのパスワードが暗号化されます。
4. クライアントは、暗号化された 2 つのパスワードを比較して、ユーザーを認証するかどうかを決定します。

`pam_unix_*` モジュールには、次の制限があります。

- パスワードは UNIX `crypt` 形式で格納する必要があります。
- `userPassword` 属性は、ネームサービスから読み取り可能でなければなりません。

たとえば、資格レベルを `anonymous` に設定した場合は、すべてのユーザーが `userPassword` 属性を読み取れる必要があります。同様に、資格レベルを `proxy` に設定した場合は、プロキシシユーザーが `userPassword` 属性を読み取れる必要があります。

注記 - UNIX 認証には、`sasl/digest-MD5` 認証方法との互換性がありません。Oracle Directory Server Enterprise Edition で `digest-MD5` を使用するには、パスワードを暗号化せずに格納する必要があります。UNIX 認証では、パスワードを `crypt` 形式で格納する必要があります。

`pam_unix_account` モジュールは、`enableShadowUpdate` スイッチが `true` に設定されている場合はアカウント管理をサポートします。リモート LDAP ユーザーアカウントに対する制御は、`passwd` および `shadow` ファイルで定義されたローカルユーザーアカウントに適用される制御と同じ方法で適用されます。`enableShadowUpdate` モードでの LDAP アカウントでは、LDAP アカウントについてはシステムが更新を行い、パスワードの有効期限管理とアカウントのロックのために LDAP サーバー上のシャドウデータを使用します。ローカルアカウントのシャドウデータはローカルクライアントシステムに適用されるのに対して、LDAP ユーザーアカウントのシャドウデータはすべてのクライアントシステムのユーザーに適用されます。

パスワードの履歴チェックは、ローカルクライアントに対してのみサポートされ、LDAP ユーザーアカウントに対してはサポートされません。

Kerberos サービスモジュール

Kerberos については、次の資料で広範囲にわたって説明されています。

- [pam_krb5\(5\)](#) のマニュアルページ。
- 『Oracle Solaris 11.2 での Kerberos およびその他の認証サービスの管理』

PAM およびパスワードの変更

パスワードを変更するには、`passwd` コマンドを使用します。`enableShadowUpdate` スイッチが有効になっていない場合は、管理者資格情報に加えて、ユーザー資格情報でも `userPassword` 属性が書き込み可能である必要があります。`passwd-cmd` の `serviceAuthenticationMethod` によって、この操作のための `authenticationMethod` がオーバーライドされます。認証方法によっては、現在のパスワードが暗号化されていない場合があります。

UNIX 認証では、新しい `userPassword` 属性が UNIX `crypt` 形式で暗号化されます。この属性は、LDAP に書き込まれる前にタグ付けされます。このため、サーバーへのバインドに使用される認証方法に関係なく、新しいパスワードは暗号化されます。詳細は、[pam_authtok_store\(5\)](#) のマニュアルページを参照してください。

`enableShadowUpdate` スイッチが有効になっている場合は、ユーザーパスワードが変更されると、`pam_unix_*` モジュールでも関連するシャドウ情報が更新されます。`pam_unix_*` モジュールは、ローカルのユーザーパスワードが変更されたときにこれらのモジュールが更新するローカルの `shadow` ファイル内の同じ `shadow` フィールドを更新します。

`pam_ldap` モジュールのパスワード更新のサポートは、`server_policy` オプションを使用した `pam_authtok_store` モジュールに置き換えられました。`pam_authtok_store` を使用すると、新しいパスワードは暗号化されずに LDAP サーバーに送信されます。機密性を保証するには、TLS を使用してください。そうしないと、新しい `userPassword` が詮索されやすくなります。

Oracle Directory Server Enterprise Edition でタグ付けされていないパスワードを設定すると、`passwordStorageScheme` 属性を使用してパスワードが暗号化されます。`passwordStorageScheme` の詳細については、使用しているバージョンの Oracle Directory Server Enterprise Edition の管理者ガイドでユーザーアカウントの管理に関するセクションを参照してください。

NIS、または UNIX 認証を使用するその他のクライアントがリポジトリとして LDAP を使用する場合は、`passwordStorageScheme` 属性に `crypt` を構成する必要があります。また、Oracle

Directory Server Enterprise Edition で `sasl/digest-MD5` の LDAP 認証を使用している場合は、`passwordStorageScheme` を平文に設定する必要があります。

LDAP アカウント管理

`pam_krb5` を使用してアカウントおよびパスワードの管理を実行すると、アカウント、パスワード、アカウントロックアウト、およびその他のアカウント管理の詳細がすべて Kerberos 環境で管理されます。

`pam_krb5` を使用しない場合は、LDAP ネームサービスを構成して、Oracle Directory Server Enterprise Edition のパスワードおよびアカウントロックアウトポリシーのサポートを活用できます。ユーザーアカウントの管理をサポートするように `pam_ldap` を構成できます。適切な PAM 構成で `passwd` コマンドを実行すると、Oracle Directory Server Enterprise Edition のパスワードポリシーで設定されたパスワードの構文規則が適用されます。ただし、`proxy` アカウントに対するアカウント管理は有効にしないでください。

`pam_ldap` では、次のアカウント管理機能がサポートされています。これらの機能は、Oracle Directory Server Enterprise Edition のパスワードとアカウントのロックアウトポリシー構成を利用しています。これらの機能は、何個でも有効にすることができます。

- パスワード経過期間と有効期限の通知 - ユーザーはスケジュールに従って、自分のパスワードを変更する必要があります。変更しなければ、パスワードは期限切れになり、ユーザーの認証に失敗します。
ユーザーが期限切れ警告の期間内にログインすると、常に警告が表示されます。警告には、パスワードの有効期限が切れるまでの残り時間が含まれます。
- パスワードの構文チェック - 新しいパスワードは、最小パスワード長の要件を満たしている必要があります。パスワードを、ユーザーのディレクトリエントリ内の `uid`、`cn`、`sn`、または `mail` 属性の値に一致させることはできません。
- 履歴内のパスワードのチェック - ユーザーはパスワードを再利用できません。LDAP 管理者は、サーバーの履歴リストに保持するパスワードの数を構成することができます。
- ユーザーアカウントのロックアウト - 認証の失敗が指定された回数に達したあとに、ユーザーアカウントをロックアウトできます。管理者がアカウントを非アクティブにした場合も、そのユーザーはロックアウトされます。アカウントのロックアウト時間が経過するか、管理者がふたたびアカウントをアクティブにするまで、認証は引き続き失敗します。

注記 - これらのアカウント管理機能は、Oracle Directory Server Enterprise Edition だけで動作します。サーバー上のパスワードとアカウントのロックアウトポリシーの構成についての詳細は、使用しているバージョンの Oracle Directory Server Enterprise Edition の管理者ガイドでユーザーアカウントの管理に関する章を参照してください。31 ページの「[アカウント管理に pam_ldap モジュールを使用した pam_conf ファイルの例](#)」も参照してください。

Oracle Directory Server Enterprise Edition でパスワードとアカウントのロックアウトポリシーを構成する前に、すべてのホストで pam_ldap アカウント管理による最新の LDAP クライアントが使用されていることを必ず確認してください。さらに、クライアントで pam.conf ファイルが適切に構成されていることを確認してください。これを行わない場合、proxy やユーザーパスワードの有効期限が切れたときに、LDAP ネームサービスでエラーが発生します。

pam_unix_* モジュールによる LDAP アカウント管理

enableShadowUpdate スイッチが有効になっている場合は、ローカルアカウントと LDAP アカウントの両方でアカウント管理機能が使用可能になります。この機能には、パスワードの有効期限管理、アカウントの有効期限管理および通知、ログインに失敗したアカウントのロックなどが含まれます。また、passwd コマンドの -dluNfnwx オプションが LDAP でサポートされるようになりました。これにより、ファイルネームサービスでの passwd コマンドと pam_unix_* モジュールのすべての機能が LDAP ネームサービスでサポートされます。enableShadowUpdate スイッチを有効にすると、ファイルと LDAP スコープの両方で定義されているユーザーに対して一貫性のあるアカウント管理を実装できます。

pam_ldap モジュールと pam_unix_* モジュールには互換性がありません。pam_ldap モジュールでは、ユーザーがパスワードを変更できる必要があります。pam_unix_* モジュールでは、その反対のことが必要です。つまり、同じ LDAP ネームドメインで 2 つを同時に使用することはできません。すべてのクライアントが pam_ldap モジュールを使用するか、またはすべてのクライアントが pam_unix_* モジュールを使用するかのどちらかです。この制限の結果として、たとえば、Web や電子メールアプリケーションでユーザーが LDAP サーバーで自分のパスワードを変更する必要がある場合に、専用の LDAP サーバーを使用しなければならないことがあります。

enableShadowUpdate を実装するには、すべてのクライアントの svc:/network/ldap/client サービスに管理者資格情報 (adminDN および adminPassword) をローカルに格納する必要があります。

アカウント管理に pam_unix_* モジュールを使用する場合は、/etc/pam.conf ファイルを変更する必要はありません。デフォルトの /etc/pam.conf ファイルで十分です。

アカウント管理に pam_ldap モジュールを使用した pam_conf ファイルの例

このセクションでは、pam_conf ファイルの例を示します。

```
#
# Authentication management
#
# login service (explicit because of pam_dial_auth)
#
login  auth requisite      pam_authtok_get.so.1
login  auth required      pam_dhkeys.so.1
login  auth required      pam_unix_cred.so.1
login  auth required      pam_dial_auth.so.1
login  auth binding       pam_unix_auth.so.1 server_policy
login  auth required      pam_ldap.so.1
#
# rlogin service (explicit because of pam_rhost_auth)
#
rlogin auth sufficient     pam_rhosts_auth.so.1
rlogin auth requisite     pam_authtok_get.so.1
rlogin auth required     pam_dhkeys.so.1
rlogin auth required     pam_unix_cred.so.1
rlogin auth binding       pam_unix_auth.so.1 server_policy
rlogin auth required     pam_ldap.so.1
#
# rsh service (explicit because of pam_rhost_auth,
# and pam_unix_auth for meaningful pam_setcred)
#
rsh    auth sufficient     pam_rhosts_auth.so.1
rsh    auth required      pam_unix_cred.so.1
rsh    auth binding       pam_unix_auth.so.1 server_policy
rsh    auth required      pam_ldap.so.1
#
# PPP service (explicit because of pam_dial_auth)
#
ppp    auth requisite     pam_authtok_get.so.1
ppp    auth required     pam_dhkeys.so.1
ppp    auth required     pam_dial_auth.so.1
ppp    auth binding       pam_unix_auth.so.1 server_policy
ppp    auth required     pam_ldap.so.1
#
# Default definitions for Authentication management
# Used when service name is not explicitly mentioned for authentication
#
other  auth requisite     pam_authtok_get.so.1
other  auth required     pam_dhkeys.so.1
other  auth required     pam_unix_cred.so.1
other  auth binding       pam_unix_auth.so.1 server_policy
other  auth required     pam_ldap.so.1
#
# passwd command (explicit because of a different authentication module)
```

```
#
passwd auth binding          pam_passwd_auth.so.1 server_policy
passwd auth required        pam_ldap.so.1
#
# cron service (explicit because of non-usage of pam_roles.so.1)
#
cron    account required    pam_unix_account.so.1
#
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
other   account requisite   pam_roles.so.1
other   account binding     pam_unix_account.so.1 server_policy
other   account required    pam_ldap.so.1
#
# Default definition for Session management
# Used when service name is not explicitly mentioned for session management
#
other   session required    pam_unix_session.so.1
#
# Default definition for Password management
# Used when service name is not explicitly mentioned for password management
#
other   password required   pam_dhkeys.so.1
other   password requisite  pam_authtok_get.so.1
other   password requisite  pam_authtok_check.so.1
other   password required   pam_authtok_store.so.1 server_policy
#
# Support for Kerberos V5 authentication and example configurations can
# be found in the pam_krb5(5) man page under the "EXAMPLES" section.
#
```

◆◆◆ 第 3 章

LDAP ネームサービスの計画要件

この章では、サーバーとクライアントの設定およびインストール処理を開始する前に実行する必要のある上流工程の計画について説明します。

この章で扱う内容は、次のとおりです。

- [33 ページの「LDAP 計画の概要」](#)
- [35 ページの「LDAP クライアントプロファイル構成の計画」](#)
- [38 ページの「LDAP マスターサーバーおよび複製サーバーの配備計画」](#)
- [40 ページの「LDAP データ生成の計画」](#)
- [40 ページの「サービス検索記述子とスキーママッピング」](#)
- [43 ページの「サマリー: LDAP実装を準備するデフォルトのクライアントプロファイル属性」](#)

LDAP 計画の概要

LDAP 計画は主に、LDAP クライアントプロファイルに配置する情報の決定で構成されます。クライアントはプロファイル内の構成情報の集合体を使用して、LDAP サーバーからネームサービス情報にアクセスします。構成情報は、LDAP サーバー上にプロファイルを構築する際に指定します。サーバーの設定中に、情報を求めるプロンプトが表示されます。プロンプトが表示される情報の一部は必須ですが、その他の情報はオプションです。ほとんどの場合、すでに指定されているデフォルト値をそのまま使用します。プロファイルを求めるプロンプトが表示される各種情報は、**クライアント属性**と呼ばれます。

プロファイルの構成情報を収集する際には、[43 ページの「LDAP を構成するための空白のチェックリスト」](#)で示すテンプレートチェックリストを使用できます。これらのチェックリストは、LDAP サーバーを設定する際に参照として使用できます。

次の表には、LDAP クライアントプロファイル属性を示します。

表 3-1 LDAP クライアントのプロファイル属性

属性	説明
cn	プロファイル名。デフォルト値はありません。必ず指定する必要があります。
preferredServerList	優先使用されるサーバーのホストアドレスの、空白で区切られたリスト。(ホスト名は使用しない)。defaultServerList 内のサーバーより「前に」、接続が成功するまで、このリスト内のサーバーへの接続が順番に試みられます。デフォルト値はありません。preferredServerList または defaultServerList に 1 つ以上のサーバーを指定する必要があります。 注記 - ホスト名を使用して defaultServerList と preferredServerList の両方を定義している場合は、ホストサーバー参照の検索に LDAP を使用しないでください。svc:/network/name-service/switch サービスの config/host プロパティには、値 ldap を構成しないでください。
defaultServerList	デフォルトサーバーのホストアドレスの、空白で区切られたリスト。(ホスト名は使用しない)。preferredServerList 内のサーバーへの接続試行後に、接続が確立されるまで、クライアントのサブネット上のデフォルトサーバーへの接続、続いて残りのデフォルトサーバーへの接続が試みられます。preferredServerList または defaultServerList に 1 つ以上のサーバーを指定する必要があります。このリスト内のサーバーへの接続は、優先サーバーリストのサーバーへの接続試行後に試みられます。デフォルト値はありません。
defaultSearchBase	よく知られたコンテナの検索に使用する相対識別名。デフォルト値はありません。ただし、この値は serviceSearchDescriptor 属性で指定されたサービスでオーバーライドできます。
defaultSearchScope	クライアントによるデータベース検索の適用範囲を定義します。この値は、serviceSearchDescriptor 属性でオーバーライドできます。指定可能な値は one または sub です。デフォルト値は、単一レベルの検索です。
authenticationMethod	クライアントが使用する認証方式を示します。デフォルトは none (anonymous) です。詳細は、21 ページの「LDAP ネームサービスの認証方法」を参照してください。
credentialLevel	クライアントが認証に使用する証明書タイプを示します。選択肢は、anonymous、proxy、または self (「ユーザー別」とも呼ばれます) です。デフォルトは anonymous です。
serviceSearchDescriptor	クライアントがネームデータベースを検索する方法および場所を定義します (たとえば、クライアントが DIT 内の 1 つ以上の場所を検索するかどうか)。デフォルトでは、SSD は定義されていません。
serviceAuthenticationMethod	クライアントが特定のサービスで使用する認証メソッド。デフォルトでは、サービス認証メソッドは定義されていません。サービスで serviceAuthenticationMethod が定義されていない場合、authenticationMethod の値がデフォルトになります。
attributeMap	クライアントが使用する属性マッピング。デフォルトでは、attributeMap は定義されていません。

属性	説明
objectclassMap	クライアントが使用するオブジェクトクラスマッピング。デフォルトでは、objectclassMap は定義されていません。
searchTimeLimit	クライアントが許可する、タイムアウトまでの最長検索時間 (秒)。これにより、検索が完了するまでの LDAP サーバーの許容時間は影響を受けません。デフォルト値は 30 秒
bindTimeLimit	クライアントがサーバーとのバインドに許可する最長時間 (秒)。デフォルト値は 30 秒
followReferrals	クライアントが LDAP リフェラルに準拠するかどうかを指定します。指定可能な値は、TRUE または FALSE です。デフォルト値は TRUE です。
profileTTL	ldap_cachemgr(1M) により実行される、LDAP サーバーからのクライアントプロファイルのリフレッシュ間隔。デフォルト値は 43200 秒 (12 時間) です。値が 0 の場合、プロファイルは決してリフレッシュされません。

これらの属性は、サーバー上で `idsconfig` コマンドを実行すると自動的に設定されます。

その他のクライアント属性は、`ldapclient` コマンドを使用することでクライアントシステム上にローカルに設定できます。これらの属性の詳細は、[69 ページの「ローカル LDAP クライアント属性の定義」](#)を参照してください。

LDAP クライアントプロファイル構成の計画

LDAP のネームサービスを適切に設定するには、まず、LDAP クライアントプロファイルの構成を計画する必要があります。ほとんどのネットワークでは、プロファイル属性のデフォルト値で十分です。ただし、一部のプロファイル属性には、独自のネットワークポロジに基づいてデフォルト以外の値を指定できます。このセクションでは、構成する可能性のあるさまざまな属性について説明します。

LDAP ネットワークモデル

LDAP ネットワークモデルの計画とは、LDAP ネームサービスで配備される物理サーバーを決定することを指します。可用性およびパフォーマンスを保証するには、ネットワークのサブネットごとに LDAP サーバーを 1 台ずつ配備して、そのサブネット内のクライアントにサービスを提供する必要があります。このモデルを計画する際は、次の点を考慮してください。

- LDAP サーバーとして配備されるシステムの数

どのサーバーが指定されたマスターサーバーで、どのサーバーがバックアップとして機能する複製サーバーであるのか。

■ サーバーへのアクセス方法

すべての LDAP サーバーで、クライアントリクエストによるアクセスの優先度を等しくするべきかまたは、サーバーごとに優先度が別々で、優先度の高いサーバーが最初にアクセスするのかサーバーへのアクセスが等しくない場合は、これらのサーバーがアクセスする順序を一覧表示します。

指定された情報は、`defaultServerList` および `preferredServerList` 属性で管理されます。

■ タイムアウト係数

タイムアウト値は次のように決定します。

- `bindTimeLimit` 属性は、TCP 接続リクエストが削除されるまで存続する期間を決定します。
- `searchTimeLimit` 属性は、LDAP 検索操作が取り消されるまで継続する期間を決定します。
- `profileTTL` 属性は、クライアントがサーバーからプロファイルをダウンロードする頻度を決定します。

たとえば、低速ネットワークでは、TCP 接続リクエストを検索および許可する時間が長くなる可能性があります。開発環境では、クライアントがプロファイルをダウンロードする頻度を制限することがあります。

ディレクトリ情報ツリー

LDAP ネームサービスでは、デフォルトのディレクトリ情報ツリー (DIT) を使用して情報が格納されます。DIT 自体は、LDAP スキーマに基づいています。

DIT は、階層的に構造化された情報のコンテナで構成されます。この構造は、[RFC 2307](http://tools.ietf.org/html/rfc2307) (<http://tools.ietf.org/html/rfc2307>) および [RFC 4876](http://tools.ietf.org/html/rfc4876) (<http://tools.ietf.org/html/rfc4876>) で説明する標準の LDAP スキーマに準拠します。

ほとんどのネットワーク設定では、DIT のデフォルト構造で十分に LDAP を実装できます。デフォルトの構造では、次の点だけを決定する必要があります。

- ネームサービスが特定のドメインに関する情報を検索するツリーのベースノード識別名 (DN)。ベースノードの情報は、`defaultSearchBase` 属性で管理されます。

- ネームサービス検索機能で実行される検索の範囲。この範囲には、DN の 1 レベル下と DN の下のサブツリー全体のどちらかしか含めることができません。この情報は、`defaultSearchScope` 属性で管理されます。

DIT には、データを格納するためのより複雑な構造を含めることもできます。たとえば、ユーザーアカウントに関するデータを DIT の別の部分に格納できます。デフォルトの検索順序をオーバーライドする検索操作 (使用するベース DN、範囲、フィルタなど) の動作をカスタマイズする方法を決定してください。カスタマイズされた検索順序の情報は、`serviceSearchDescriptor`、`attributeMap`、および `objectclassMap` 属性で管理されます。検索順序の操作をカスタマイズする方法の詳細は、40 ページの「サービス検索記述子とスキーママッピング」を参照してください。

複数のサーバーで単一の DIT を処理できます。この手順では、DIT のサブツリーが複数のサーバーに分散される可能性があります。つまり、リクエストされた情報を提供できる適切な LDAP サーバーにクライアントリクエストが適切にリダイレクトされるように、LDAP サーバーをさらに構成する必要があります。適切なサーバーにクライアントリクエストをリダイレクトする方法に関する情報は、`followReferrals` 属性で管理されます。

特定のドメインにすべてのネームデータを提供する単一の LDAP サーバーを配備する方法は、通常の推奨される設定です。ただし、このようなシナリオでも、有用な目的のために `followReferrals` 属性を構成できます。リフェラルを使用すると、大部分の情報リクエストに対応する読み取り専用の複製サーバーまでクライアントを誘導できます。読み取りおよび書き込み操作を実行するためのマスターサーバーへのアクセス権は、例外的にしか付与されません。リフェラル構成では、マスターサーバーが過負荷になることが避けられます。

セキュリティ上の考慮点

ディレクトリ情報に対するリクエストを処理する LDAP 操作のセキュリティを確保するために、次の点を考慮する必要があります。

- 情報にアクセスするためにクライアント自身を識別する方法。識別方法は、クライアントに指定された資格レベルによって決まります。資格レベルは `credentialLevel` 属性によって管理され、この属性には次のいずれかの値を割り当てることができます。
 - `anonymous`
 - `proxy`
 - `proxy anonymous`

- self

それぞれの値の詳細は、18 ページの「クライアント資格レベル」を参照してください。

- クライアントを認証する方法。指定された方法は、authenticationMethod 属性で管理されます。認証方法は、次のオプションのいずれかを割り当てることで指定できます。

- none
- simple
- sasl/digest-MD5
- sasl/cram-MD5
- sasl/GSSAPI
- tls:simple
- tls:sasl/cram-MD5
- tls:sasl/digest-MD5

それぞれの値の詳細は、21 ページの「LDAP ネームサービスの認証方法」を参照してください。

クライアントに割り当てる資格レベルおよび使用する認証方法に加えて、次の点も考慮してください。

- Kerberos およびユーザー別の認証を使用するかどうか。
- サーバーの passwordStorageScheme 属性に指定する値
- アクセス制御情報を設定するかどうか
ACI の詳細は、使用しているバージョンの Oracle Directory Server Enterprise Edition に対応した『管理者ガイド』を参照してください。
- LDAP アカウント管理の実行に pam_unix_* と pam_ldap モジュールのどちらを使用するか
この考慮事項は、LDAP ネームサービスに NIS との互換性があるかどうかに関連しています。

LDAP マスターサーバーおよび複製サーバーの配備計画

マスターサーバーおよび複製サーバーは、次の方法で配備できます。

- 単一マスター複製

- 浮動マスター複製
- 複数マスター複製

次の表では、LDAP マスターサーバーおよび複製サーバーを配備する際の 3 つの方針を比較します。

表 3-2 LDAP マスターサーバーと複製サーバー

方針	説明	リスク
単一マスター複製	特定のネットワークまたはサブネットワークに 1 つのマスターサーバーが存在します。マスターサーバーには、ディレクトリの書き込み可能コピーが格納されます。複製サーバーには、読み取り専用コピーが格納されます。マスターサーバーのみが書き込み操作を実行できます。	単一障害点。マスターサーバーが使用不可になった場合、その他のサーバーは書き込み操作を実行できません。
浮動マスター複製	単一マスター複製と同様です。ただし、マスターサーバーが使用不可になった場合は、別の複製サーバーが書き込み操作を実行できます。書き込み操作を継承する複製サーバーは、アルゴリズムに基づいて選択されます。	この方針には、ネットワーク構成の変更に対する柔軟性がありません。たとえば、ネットワークがサブネットワークに分割されているとします。両方のサブネットワーク上の複製サーバーがマスターサーバーになります。その後、サブネットワークが再結合された場合、浮動マスター複製方針を使用してサーバーを再配備する再構成プロセスが複雑になります。
複数マスター複製	複数のマスターサーバーに、同じディレクトリの読み取り書き込みコピーが格納されます。	異なるマスターサーバーで、同じディレクトリの更新競合が発生する可能性があります。この方針を採用する場合は、「最終書き込み者優先」などの更新競合の解決ポリシーを確立する必要があります。

複製サーバーを設定する方法については、使用しているバージョンの Oracle Directory Server Enterprise Edition に対応した管理者ガイドを参照してください。大規模なエンタープライズ配備には、複数マスター複製が推奨されるオプションです。

LDAP データ生成の計画

適切な DIT およびスキーマを使用して LDAP サーバーを構成したあとは、DIT にデータを移入する必要があります。データのソースは、複数のシステムの /etc ファイルです。DIT にデータを移入する際に使用する方法を検討する必要があります。

- 特定のデータ型の /etc ファイルを、そのデータ型の単一ファイルにマージします (たとえば、さまざまなシステムにあるすべての /etc/passwd ファイルを単一の /etc/passwd ファイルにマージします)。その後、マージされた /etc ファイルがすべて格納される単一のホストから、サーバーにデータを移入します。
- サーバーにデータを移入するには、ディレクトリサーバーにアクセスする各クライアントシステムから適切なコマンドを発行します。

ディレクトリサーバーにデータを移入する手順については、[57 ページの「LDAP サーバーへのデータの移入」](#)を参照してください。

サービス検索記述子とスキーママッピング

すでに説明したように、LDAP ネームサービスは、DIT が特定の 방법으로構造化されていると想定されています。必要に応じて、サービス検索記述子 (SSD) を使用して、DIT 内のデフォルト以外の場所で検索するよう LDAP ネームサービスに指示することができます。また、デフォルトのスキーマで指定された属性やオブジェクトクラスの代わりに、別の属性やオブジェクトクラスを指定して使用することもできます。デフォルトフィルタのリストについては、次のコマンドを使用します。

```
ldaplist -v
```

注記 - デフォルトフィルタの一覧は [109 ページの「LDAP ネームサービスで使用されるデフォルトフィルタ」](#)にもあります。

スキーママッピングは、注意深くかつ一貫した方法で使用する必要があります。マッピングされた属性の構文が、マッピング先の属性との一貫性を保持していることを確認してください。つまり、単一値の属性が単一値の属性にマッピングされ、属性の構文が一致しており、マッピングされたオブジェクトクラスが適正な必須 (通常はマッピングされた) 属性を保持することを確認します。

SSD の説明

`serviceSearchDescriptor` 属性は、LDAP ネームサービスクライアントが特定のサービスに関する情報を検索する方法と場所を定義します。`serviceSearchDescriptor` には、サービス名に続き、1 つ以上のセミコロンで区切られたベース - スコープ - フィルタのセットが含まれます。これらのベース - スコープ - フィルタのセットは特定のサービス専用の検索定義に使用され、指定された順番で検索されます。特定のサービスに対して複数のベース - スコープ - フィルタが指定されている場合、このサービスは、特定のエントリを検索する際、指定されたスコープおよびフィルタを保持する各ベースを検索します。

注記 - SSD では、デフォルト位置は SSD に含まれていない限り、サービス (データベース) の検索対象にはなりません。サービスに複数の SSD が指定されている場合、予期しない結果になることがあります。

次の例では、LDAP ネームサービスクライアントは、`ou=west,dc=example,dc=com` 内で `passwd` サービスに対する単一レベルの検索を実行したあとに、`ou=east,dc=example,dc=com` 内で単一レベルの検索を実行します。ユーザーの `username` の `passwd` データを検索するために、各 BaseDN に対してデフォルトの LDAP フィルタ (`&(objectClass=posixAccount)(uid=username)`) が使用されます。

```
serviceSearchDescriptor: passwd:ou=west,dc=example,dc=com;ou=east,dc=example,dc=com
```

次の例では、LDAP ネームサービスクライアントは、`ou=west,dc=example,dc=com` 内で `passwd` サービスに対するサブツリー検索を実行します。ユーザー `username` の `passwd` データを検索するために、LDAP フィルタ (`&(fulltimeEmployee=TRUE)(uid=username)`) を使用してサブツリー `ou=west,dc=example,dc=com` が検索されます。

```
serviceSearchDescriptor: passwd:ou=west,dc=example,dc=com?sub?fulltimeEmployee=TRUE
```

特定のサービスタイプに複数のコンテナを関連付けることもできます。次の例では、サービス検索記述子が 3 つのコンテナでパスワードエントリを検索することを指定しています。

```
ou=myuser,dc=example,dc=com
ou=newuser,dc=example,dc=com
ou=extuser,dc=example,dc=com
```

例の末尾の「,」は、SSD の相対ベースに `defaultSearchBase` が付加されることを意味します。

```
defaultSearchBase: dc=example,dc=com
serviceSearchDescriptor: \
```

```
passwd:ou=myuser,;ou=newuser,;ou=extuser,dc=example,dc=com
```

attributeMap 属性

LDAP ネームサービスでは、1 つ以上の属性名を、そのいずれかのサービスに再マッピングできます。属性を対応づける場合、その属性が元の属性と同じ意味および構文を必ず保持するようにしてください。userPassword 属性のマッピングによって問題が発生する可能性があることに注意してください。

既存のディレクトリサーバーで属性をマップする状況では、スキーママッピングを使用する方法が役立つことがあります。大文字小文字のみが異なるユーザー名を使用する場合、大文字小文字を無視する uid 属性を、大文字小文字を無視しない属性に対応づける必要があります。

この属性の書式は、service:attribute-name=mapped-attribute-name です。

指定されたサービスに対して複数の属性を対応づける場合は、複数の attributeMap 属性を定義できます。

次の例では、uid および homeDirectory 属性を passwd サービスで利用する場合、常に employeeName および home 属性が使用されます。

```
attributeMap: passwd:uid=employeeName  
attributeMap: passwd:homeDirectory=home
```

次の例で示すように、passwd サービスの gecos 属性を複数の属性にマップできることに注意してください。

```
attributeMap: gecos=cn sn title
```

この例では、gecos 値が、空白で区切られた cn、sn、および title 属性値のリストにマップされています。

objectclassMap 属性

LDAP ネームサービスでは、オブジェクトクラスを、そのいずれかのサービスに再マッピングできます。特定のサービス用に複数のオブジェクトクラスを対応づける場合、複数の objectclassMap 属性を定義できます。次の例では、posixAccount オブジェクトクラスを使用する場合、常に myUnixAccount オブジェクトクラスが使用されます。

```
objectclassMap: passwd:posixAccount=myUnixAccount
```

サマリー: LDAP実装を準備するデフォルトのクライアントプロファイル属性

次のリストでは、LDAP ネームサービスを実装するように一般的な構成を行う重要な属性を示します。これらの属性をすべて構成する必要があるわけではないことに注意してください。リストの中で値を指定する必要がある属性は、cn、defaultServerList、および defaultSearchBase のみです。残りの属性については、デフォルト値をそのまま使用することも、その他の属性を構成しないままにすることもできます。

- cn
- defaultServerList
- preferredServerList
- bindTimeLimit
- searchTimeLimit
- profileTTL
- defaultSearchBase
- defaultSearchScope
- serviceSearchDescriptor
- attributeMap
- objectclassMap
- followReferrals
- credentialLevel
- authenticationMethod
- serviceCredentialLevel
- serviceAuthenticationMethod

LDAP を構成するための空白のチェックリスト

表 3-3 サーバー変数の定義のための空白のチェックリスト

変数	ネットワークの定義
インストールしたディレクトリサーバーインスタンスのポート番号 (389)	

変数	ネットワークの定義
サーバーの名前	
複製サーバー (IP 番号:ポート番号)	
ディレクトリマネージャ [dn: cn=directory manager]	
サービスされるドメイン名	
クライアント要求の処理がタイムアウトするまでの時間 (秒)	
各検索要求で返されるエントリの最大数	

表 3-4 クライアントプロフィール変数の定義のための空白のチェックリスト

変数	ネットワークの定義
プロフィール名	
サーバーリスト (デフォルトはローカルサブネット)	
優先されるサーバーリスト (優先順に記載)	
検索範囲 (検索するディレクトリツリーレベルの数、指定可能な値は One または Sub です。)	
サーバーへのアクセスに使用する資格。デフォルトは anonymous です。	
リフェラルに従うかどうか(リフェラルはメインサーバーが使用できない場合の別のサーバーへのポインタです。)デフォルトは no です。	
サーバーが情報を返すのを待つサーチ時間の制限 (秒単位)。デフォルトは 30 秒です。	
サーバーに接続するためのバインド制限の時間 (秒単位)。デフォルトは 30 秒です。	
認証方法。デフォルトは none です。	

◆◆◆ 第 4 章

Oracle Directory Server Enterprise Edition への LDAP クライアントの設定

この章では、LDAP クライアントをサポートするように Oracle Directory Server Enterprise Edition を構成する方法について説明します。この情報は、Oracle Directory Server Enterprise Edition に固有の情報です。

注記 - LDAP クライアントを操作できるように構成する前に、Oracle Directory Server Enterprise Edition がすでにインストールおよび構成されている必要があります。この章では、Oracle Directory Server Enterprise Edition のすべての機能については説明しません。より詳細な情報については、使用している特定のディレクトリサーバーのドキュメントを参照してください。

この章で扱う内容は、次のとおりです。

- [45 ページの「ディレクトリサーバーの構成に関する情報の準備」](#)
- [47 ページの「ディレクトリツリー定義の作成」](#)
- [49 ページの「LDAP のサーバー構成例」](#)
- [59 ページの「追加のディレクトリサーバー構成タスク」](#)

ディレクトリサーバーの構成に関する情報の準備

LDAP ネームサービスを使用するようにディレクトリサーバーを構成するには、2 組の情報 (サーバー情報とクライアントプロファイル情報) が入手可能である必要があります。

LDAP のサーバー情報

ディレクトリサーバーを構成するときに、サーバーに関する次の情報を求めるプロンプトが表示されます。

- ディレクトリサーバーインスタンスのポート番号。デフォルトでは、ポート番号は 389 です。
- サーバー名。
- 複製サーバーの IP アドレスとポート番号。
- ディレクトリマネージャー (変数 `cn` で表記)。デフォルトでは、`cn` は `directory manager` に設定されます。
- サービスされるドメイン名。
- クライアントリクエストの処理がタイムアウトするまでの時間の最大長 (秒)。
- 検索リクエストごとに提供されるレコード情報の最大数。

サーバーに関する情報の一部は、[35 ページの「LDAP クライアントプロファイル構成の計画」](#)で説明した LDAP クライアントプロファイルの属性です。

サーバー情報の準備を容易にするには、割り当てる次の変数および対応する値を一覧表示するサンプルチェックリスト ([43 ページの「LDAP を構成するための空白のチェックリスト」](#)) を使用します。

LDAP のクライアントプロファイル情報

LDAP クライアントプロファイル属性に関する情報が必要です。次の属性によって、情報を要求する際のサーバーへのクライアントアクセスが制限されます。これらの属性については、[35 ページの「LDAP クライアントプロファイル構成の計画」](#)を参照してください。

- クライアントプロファイル名。
- LDAP サーバーのリスト。
- サーバーがアクセスする際の優先順位。

通常、サーバーリストとそのアクセス順序は、サーバーの IP アドレスで構成されます。代わりに、サーバーのホスト名を指定することもできます。ただし、ホスト名を使用する場合は、ホスト参照の操作に LDAP を使用しないでください。つまり、`svc:/network/name-service/switch` サービスの `config/host` プロパティに `ldap` を構成してはいけません。LDAP および SMF (Service Management Facility) の詳細は、[68 ページの「LDAP とサービス管理機能」](#)を参照してください。

- ディレクトリツリー上の検索範囲。デフォルト値は `one` ですが、`sub` も指定できます。
- サーバーにアクセスするための資格証明
- その他の LDAP サーバーへのリフェラル (ディレクトリ内の情報が複数のサーバーに分散されている場合)。値は `No`、デフォルト値、または `Yes` のいずれかです。

- リクエストに対するサーバー応答の受信がタイムアウトするまでの待ち時間。
- サーバーへの接続がタイムアウトするまでの最長時間。
- 認証方法。

注記 - クライアントプロファイルはドメインごとに定義されます。指定されたドメインで、1 つ以上のプロファイルを定義する必要があります。

クライアントプロファイル情報の準備を容易にするには、割り当てる次の変数および対応する値を一覧表示するサンプルチェックリスト (43 ページの「LDAP を構成するための空白のチェックリスト」) を使用します。

インデックス表示の使用

Oracle Directory Server Enterprise Edition のインデックス表示機能は、仮想リスト表示 (VLV) と呼ばれます。VLV を使用すると、クライアントは長いリストからエントリのサブセットを参照できるため、すべてのクライアントの検索時間が短縮されます。

ツリーへの VLV 作成プロセスの終了時に、ディレクトリ情報ツリーが作成されます。画面に、VLV を作成するためのコマンドを発行する手順が表示されます。ディレクトリサーバー上で次のコマンドを発行する必要があります。

ディレクトリツリー定義の作成

必要なサーバーおよびクライアントプロファイルの情報を収集したあとに、LDAP を使用するように Oracle Directory Server Enterprise Edition を設定します。idsconfig を使用して、チェックリストの定義を含むディレクトリ情報ツリーを構築します。

idsconfig コマンドを使用して DIT を作成すると、表3-1「LDAP クライアントのプロファイル属性」で示すように、クライアントプロファイルとその属性を効率的に構築できます。クライアントプロファイルを LDAP サーバー上の既知の場所に格納します。サーバー上に単一のプロファイルを格納する利点は、そのサーバーを使用するすべてのクライアントの構成が定義されることです。プロファイル属性への以降の変更はすべて、自動的にクライアントに反映されます。指定されたドメインのルート DN には、nisDomainObject のオブジェクトクラスと、クライアントのドメインを含む nisDomain 属性が含まれている必要があります。すべてのプロファイルは、このコンテナと相対的な関係にある ou=profile コンテナ内に配置されます。これらのプロファイルは、匿名で読み取り可能にする必要があります。

ディレクトリ定義は、ネットワーク上の任意の Oracle Solaris システムから作成できます。ただし、この場合、idsconfig コマンドの出力にディレクトリマネージャーのパスワードが平文で含まれます。パスワードの公開を避けるための代替方法として、ディレクトリサーバー自体でコマンドを発行します。

idsconfig コマンドの詳細は、[idsconfig\(1M\)](#) のマニュアルページを参照してください。

注記 - ディレクトリツリーの作成とともに、サービス検索記述子 (SSD) も作成できます。どちらの操作も、同じコマンド (idsconfig コマンド) で開始されます。ただし、必要な場合は、個別の操作として SSD を作成できます。SSD とその目的については、[40 ページの「サービス検索記述子とスキーママッピング」](#)を参照してください。

▼ LDAP ネームサービスを使用するように Oracle Directory Server Enterprise Edition を構成する方法

1. ターゲットの Oracle Directory Server Enterprise Edition が実行中であることを確認します。
2. ディレクトリ情報ツリーを構築します。

```
# /usr/lib/ldap/idsconfig
```

3. プロンプトが表示されたら、情報を入力します。
4. 画面の指示に従って、VLV インデックスを構築します。

VLV インデックスは、DIT 作成の終了後に別の操作として構築されます。画面には、適切なコマンド構文が表示されます。必ずサーバー上で次の手順を実行してください。idsconfig プロセスが完了すると、次のように手順が表示されます。

Note: idsconfig has created entries for VLV indexes.

For DS5.x, use the directoryserver(1m) script on myserver to stop the server. Then, using directoryserver, follow the directoryserver examples below to create the actual VLV indexes.

For DSEE6.x, use dsadm command delivered with DS on myserver to stop the server. Then, using dsadm, follow the dsadm examples below to create the actual VLV indexes.

idsconfig コマンドの実行時の完全な出力については、[49 ページの「ディレクトリ情報ツリーの構築」](#)の画面例を参照してください。

LDAP のサーバー構成例

このセクションでは、LDAP ネームサービスを使用するための Oracle Directory Server Enterprise Edition の構成におけるさまざまな側面の例を示します。この例では、全国に支店を持つ Example, Inc. という会社を取り上げます。具体的には、この会社の西海岸部門 (ドメイン名は west.example.com) の LDAP 構成に焦点を当てます。

ディレクトリ情報ツリーの構築

次の表には、west.example.com のサーバー情報を示します。

表 4-1 west.example.com ドメインに定義されているサーバー変数

変数	サンプルネットワークの定義
インストールしたディレクトリサーバーインスタンスのポート番号	389 (デフォルト)
サーバーの名前	myserver (FQDN myserver.west.example.com または 192.168.0.1 のホスト名)
複製サーバー (IP 番号:ポート番号)	192.168.0.2 [myreplica.west.example.com の場合]
ディレクトリマネージャー	cn=directory manager (デフォルト)
サービスされるドメイン名	west.example.com
クライアント要求の処理がタイムアウトするまでの時間 (秒)	1
各検索要求で返されるエントリの最大数	1

次の表には、クライアントプロファイル情報を示します。

表 4-2 west.example.com ドメインに定義されているクライアントプロファイル変数

変数	サンプルネットワークの定義
プロファイル名 (デフォルト名は「default」)	WestUserProfile
サーバーリスト (デフォルトはローカルサブネット)	192.168.0.1
優先されるサーバーリスト (優先順に記載)	none
検索範囲 (ディレクトリツリー内のレベルの数、one、デフォルト、または sub)	one (デフォルト)
サーバーへのアクセスに使用する資格。デフォルトは anonymous です。	proxy
リフェラルに従うかどうか (メインサーバーが使用できない場合の別のサーバーへのポインタ)。デフォルトは no です。	Y

変数	サンプルネットワークの定義
検索時にサーバーが情報を返すまでの待機時間の制限 (デフォルトは 30)	default
サーバーとの通信時のバインド時間の制限 (デフォルトは 10 秒)	default
認証方法。デフォルトは none です。	simple

この情報を使用すると、ディレクトリツリーを作成できます。

```
# usr/lib/ldap/idsconfig
It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's hostname to setup: myserver
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
Checking LDAP Base DN ...
Validating LDAP Base DN and Suffix ...
No valid suffixes were found for Base DN dc=west,dc=example,dc=com
Enter suffix to be created (b=back/h=help): [dc=west,dc=example,dc=com]
Enter ldbm database name (b=back/h=help): [west]
sasl/GSSAPI is not supported by this LDAP server
Enter the profile name (h=help): [default] WestUserProfile
Default server list (h=help): [192.168.0.1]
Preferred server list (h=help):
Choose desired search scope (one, sub, h=help): [one]
The following are the supported credential levels:
1 anonymous
2 proxy
3 proxy anonymous
4 self
Choose Credential level [h=help]: [1] 2
The following are the supported Authentication Methods:
1 none
2 simple
3 sasl/DIGEST-MD5
4 tls:simple
5 tls:sasl/DIGEST-MD5
6 sasl/GSSAPI
Choose Authentication Method (h=help): [1] 2

Current authenticationMethod: simple
Do you want to add another Authentication Method? n
Do you want the clients to follow referrals (y/n/h)? [n]
Do you want to modify the server timelimit value (y/n/h)? [n] y
Enter the time limit for DSEE (current=3600): [-1]
Do you want to modify the server sizelimit value (y/n/h)? [n] y
```

```

Enter the size limit for DSEE (current=2000): [-1]
Do you want to store passwords in "crypt" format (y/n/h)? [n] y
Do you want to setup a Service Authentication Methods (y/n/h)? [n]
Client search time limit in seconds (h=help): [30]
Profile Time To Live in seconds (h=help): [43200]
Bind time limit in seconds (h=help): [10]
Do you want to enable shadow update (y/n/h)? [n]
Do you wish to setup Service Search Descriptors (y/n/h)? [n]

      Summary of Configuration

1  Domain to serve           : west.example.com
2  Base DN to setup         : dc=west,dc=example,dc=com
   Suffix to create         : dc=west,dc=example,dc=com
   Database to create       : west
3  Profile name to create    : WestUserProfile
4  Default Server List      : 192.168.0.1
5  Preferred Server List    :
6  Default Search Scope     : one
7  Credential Level         : proxy
8  Authentication Method     : simple
9  Enable Follow Referrals   : FALSE
10 DSEE Time Limit          : -1
11 DSEE Size Limit          : -1
12 Enable crypt password storage : TRUE
13 Service Auth Method pam_ldap :
14 Service Auth Method keysevr :
15 Service Auth Method passwd-cmd:
16 Search Time Limit        : 30
17 Profile Time to Live     : 43200
18 Bind Limit               : 10
19 Enable shadow update     : FALSE
20 Service Search Descriptors Menu

Enter config value to change: (1-20 0=commit changes) [0]
Enter DN for proxy agent: [cn=proxyagent,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for proxyagent:
Re-enter passwd:

WARNING: About to start committing changes. (y=continue, n=EXIT) y

1. Changed timelimit to -1 in cn=config.
2. Changed sizelimit to -1 in cn=config.
3. Changed passwordstoragescheme to "crypt" in cn=config.
4. Schema attributes have been updated.
5. Schema objectclass definitions have been added.
6. Database west successfully created.
7. Suffix dc=west,dc=example,dc=com successfully created.
8. NisDomainObject added to dc=west,dc=example,dc=com.
9. Top level "ou" containers complete.
10. automount maps: auto_home auto_direct auto_master auto_shared processed.
11. ACI for dc=west,dc=example,dc=com modified to disable self modify.
12. Add of VLV Access Control Information (ACI).
13. Proxy Agent cn=proxyagent,ou=profile,dc=west,dc=example,dc=com added.
14. Give cn=proxyagent,ou=profile,dc=west,dc=example,dc=com read permission

```

```
for password.
15. Generated client profile and loaded on server.
16. Processing eq,pres indexes:
uidNumber (eq,pres) Finished indexing.
ipNetworkNumber (eq,pres) Finished indexing.
gidnumber (eq,pres) Finished indexing.
oncrpcnumber (eq,pres) Finished indexing.
automountKey (eq,pres) Finished indexing.
17. Processing eq,pres,sub indexes:
ipHostNumber (eq,pres,sub) Finished indexing.
memberrisnetgroup (eq,pres,sub) Finished indexing.
nisnetgrouptriple (eq,pres,sub) Finished indexing.
18. Processing VLV indexes:
west.example.com.getgrent vlv_index Entry created
west.example.com.gethostent vlv_index Entry created
west.example.com.getnetent vlv_index Entry created
west.example.com.getpwent vlv_index Entry created
west.example.com.getrpcnt vlv_index Entry created
west.example.com.getspent vlv_index Entry created
west.example.com.getauhoent vlv_index Entry created
west.example.com.getsoluent vlv_index Entry created
west.example.com.getauduent vlv_index Entry created
west.example.com.getauthent vlv_index Entry created
west.example.com.getexecent vlv_index Entry created
west.example.com.getprofent vlv_index Entry created
west.example.com.getmailent vlv_index Entry created
west.example.com.getbootent vlv_index Entry created
west.example.com.getethent vlv_index Entry created
west.example.com.getngrpent vlv_index Entry created
west.example.com.getipnent vlv_index Entry created
west.example.com.getmaskent vlv_index Entry created
west.example.com.getprent vlv_index Entry created
west.example.com.getip4ent vlv_index Entry created
west.example.com.getip6ent vlv_index Entry created

idsconfig: Setup of DSEE server myserver is complete.
```

Note: idsconfig has created entries for VLV indexes.

For DS5.x, use the directoryserver(1m) script on myserver to stop the server. Then, using directoryserver, follow the directoryserver examples below to create the actual VLV indexes.

For DSEE6.x, use dsadm command delivered with DS on myserver to stop the server. Then, using dsadm, follow the dsadm examples below to create the actual VLV indexes.

次の画面には、idsconfig 設定を完了するために従う追加の手順が表示されます。

```
directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getgrent
directoryserver -s <server-instance> vlvindex -n west -T west.example.com.gethostent
directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getnetent
directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getpwent
```

```

directoryserver -s <server-instance> vlindex -n west -T west.example.com.getrpcent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getspent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getauhoent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getsoluent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getauduent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getauthent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getexecent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getprofent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getmailent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getbootent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getethent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getngrpent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getipnent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getmaskent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getprent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getip4ent
directoryserver -s <server-instance> vlindex -n west -T west.example.com.getip6ent

```

```

install-path/bin/dsadm reindex -l -t west.example.com.getgrent \
directory-instance-path dc=west,dc=example,dc=com
install-path/bin/dsadm reindex -l -t west.example.com.gethostent \
directory-instance-path dc=west,dc=example,dc=com
.
.
.
install-path/bin/dsadm reindex -l -t west.example.com.getip6ent \
directory-instance-path dc=west,dc=example,dc=com

```

新しいプロファイルの DIT を構築するときにシャドウ更新を有効にするには、idsconfig ユーティリティーを使用できます。シャドウ更新を有効にするには、Do you want to enable shadow update (y/n/h)? [n] と表示されたら **y** を入力する必要があります。Enter passwd for the administrator: と表示されたら、管理者のパスワードを入力する必要があります。

次の例は、idsconfig ユーティリティーを使用してシャドウ更新を有効にする方法を示します。

```

# usr/lib/ldap/idsconfig
It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's hostname to setup: myserver
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
Checking LDAP Base DN ...
Validating LDAP Base DN and Suffix ...
No valid suffixes were found for Base DN dc=west,dc=example,dc=com
Enter suffix to be created (b=back/h=help): [dc=west,dc=example,dc=com]

```

```
Enter ldbm database name (b=back/h=help): [west]
sasl/GSSAPI is not supported by this LDAP server
Enter the profile name (h=help): [default] WestUserProfile
Default server list (h=help): [192.168.0.1]
Preferred server list (h=help):
Choose desired search scope (one, sub, h=help): [one]
The following are the supported credential levels:
1 anonymous
2 proxy
3 proxy anonymous
4 self
Choose Credential level [h=help]: [1] 2
The following are the supported Authentication Methods:
1 none
2 simple
3 sasl/DIGEST-MD5
4 tls:simple
5 tls:sasl/DIGEST-MD5
6 sasl/GSSAPI
Choose Authentication Method (h=help): [1] 2

Current authenticationMethod: simple
Do you want to add another Authentication Method? n
Do you want the clients to follow referrals (y/n/h)? [n]
Do you want to modify the server timelimit value (y/n/h)? [n] y
Enter the time limit for DSEE (current=3600): [-1]
Do you want to modify the server sizelimit value (y/n/h)? [n] y
Enter the size limit for DSEE (current=2000): [-1]
Do you want to store passwords in "crypt" format (y/n/h)? [n] y
Do you want to setup a Service Authentication Methods (y/n/h)? [n]
Client search time limit in seconds (h=help): [30]
Profile Time To Live in seconds (h=help): [43200]
Bind time limit in seconds (h=help): [10]
Do you want to enable shadow update (y/n/h)? [n] y
Do you wish to setup Service Search Descriptors (y/n/h)? [n]
```

Summary of Configuration

```
1 Domain to serve           : west.example.com
2 Base DN to setup          : dc=west,dc=example,dc=com
   Suffix to create         : dc=west,dc=example,dc=com
   Database to create       : west
3 Profile name to create    : WestUserProfile
4 Default Server List       : 192.168.0.1
5 Preferred Server List     :
6 Default Search Scope      : one
7 Credential Level          : proxy
8 Authentication Method     : simple
9 Enable Follow Referrals   : FALSE
10 DSEE Time Limit          : -1
11 DSEE Size Limit          : -1
12 Enable crypt password storage : TRUE
13 Service Auth Method pam_ldap :
14 Service Auth Method keysserv :
15 Service Auth Method passwd-cmd:
```

```

16 Search Time Limit           : 30
17 Profile Time to Live       : 43200
18 Bind Limit                  : 10
19 Enable shadow update       : TRUE
20 Service Search Descriptors Menu

Enter config value to change: (1-20 0=commit changes) [0]
Enter DN for proxy agent: [cn=proxyagent,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for proxyagent: proxy-password
Re-enter passwd: proxy-password
Enter DN for the administrator: [cn=admin,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for the administrator: admin-password
Re-enter passwd: admin-password
WARNING: About to start committing changes. (y=continue, n=EXIT) y

 1. Changed timelimit to -1 in cn=config.
 2. Changed sizelimit to -1 in cn=config.
 3. Changed passwordstoragescheme to "crypt" in cn=config.
 4. Schema attributes have been updated.
 5. Schema objectclass definitions have been added.
 6. Database west successfully created.
 7. Suffix dc=west,dc=example,dc=com successfully created.
 8. NisDomainObject added to dc=west,dc=example,dc=com.
 9. Top level "ou" containers complete.
10. automount maps: auto_home auto_direct auto_master auto_shared processed.
11. ACI for dc=west,dc=example,dc=com modified to disable self modify.
12. Add of VLV Access Control Information (ACI).
13. Proxy Agent cn=proxyagent,ou=profile,dc=west,dc=example,dc=com added.
14. Administrator identity cn=admin,ou=profile,dc=west,dc=example,dc=com added.
15. Give cn=admin,ou=profile,dc=west,dc=example,dc=com read/write access to\
    shadow data.
16. Non-Admin access to shadow data denied.
17. Generated client profile and loaded on server.
18. Processing eq,pres indexes:
uidNumber (eq,pres) Finished indexing.
ipNetworkNumber (eq,pres) Finished indexing.
gidnumber (eq,pres) Finished indexing.
oncrpcnumber (eq,pres) Finished indexing.
automountKey (eq,pres) Finished indexing.
19. Processing eq,pres,sub indexes:
ipHostNumber (eq,pres,sub) Finished indexing.
memberrnisnetgroup (eq,pres,sub) Finished indexing.
nisnetgrouptriple (eq,pres,sub) Finished indexing.
20. Processing VLV indexes:
west.example.com.getgrent vlv_index Entry created
west.example.com.gethostent vlv_index Entry created
west.example.com.getnetent vlv_index Entry created
west.example.com.getpwent vlv_index Entry created
west.example.com.getrpcent vlv_index Entry created
west.example.com.getspent vlv_index Entry created
west.example.com.getauhoent vlv_index Entry created
west.example.com.getsoluent vlv_index Entry created
west.example.com.getauduent vlv_index Entry created
west.example.com.getauthent vlv_index Entry created
west.example.com.getexecent vlv_index Entry created

```

```
west.example.com.getprofent vlv_index  Entry created
west.example.com.getmailent vlv_index  Entry created
west.example.com.getbootent vlv_index  Entry created
west.example.com.getethent vlv_index  Entry created
west.example.com.getngrpent vlv_index  Entry created
west.example.com.getipnent vlv_index  Entry created
west.example.com.getmaskent vlv_index  Entry created
west.example.com.getprent vlv_index  Entry created
west.example.com.getip4ent vlv_index  Entry created
west.example.com.getip6ent vlv_index  Entry created
```

idsconfig: Setup of DSEE server myserver is complete.

Note: idsconfig has created entries for VLV indexes.

For DS5.x, use the `directoryserver(1m)` script on myserver to stop the server. Then, using `directoryserver`, follow the `directoryserver` examples below to create the actual VLV indexes.

For DSEE6.x, use `dsadm` command delivered with DS on myserver to stop the server. Then, using `dsadm`, follow the `dsadm` examples below to create the actual VLV indexes.

シャドウ更新を有効にするために LDAP クライアントを初期化する方法については、[70 ページの「LDAP クライアントの初期化」](#)を参照してください。LDAP クライアントを初期化するときには、DIT の構築時に指定した管理者の DN およびパスワードと同じものを使用する必要があります。

サービス検索記述子の定義

Example, Inc. 社の以前の LDAP 構成では、ディレクトリツリーの `ou=Users` コンテナにユーザー情報が格納されていました。このマニュアルで説明した Oracle Solaris リリースでは、ユーザーエントリは `ou=People` コンテナに格納されると見なされます。したがって、`passwd` サービスが検索され、クライアントが `ou=People` コンテナを検索する場合は、情報を入手できません。

会社の既存のディレクトリ情報ツリーを再作成する複雑さと、ほかの操作への影響を避けるために、代わりにサービス検索記述子 (SSD) を作成できます。これらの SSD は、デフォルトのコンテナではなく、`ou=Users` コンテナからユーザー情報を検索するように LDAP クライアントに指示します。

検索記述子については、[40 ページの「サービス検索記述子とスキーママッピング」](#)を参照してください。

SSD を作成するために、`idsconfig` コマンドも使用します。SSD を参照するプロンプト行は、次のように表示されます。

```
Do you wish to setup Service Search Descriptors (y/n/h? y
A Add a Service Search Descriptor
D Delete a SSD
M Modify a SSD
P Display all SSD's
H Help
X Clear all SSD's

Q Exit menu
Enter menu choice: [Quit] a
Enter the service id: passwd
Enter the base: service ou=user,dc=west,dc=example,dc=com
Enter the scope: one[default]
A Add a Service Search Descriptor
D Delete a SSD
M Modify a SSD
P Display all SSD's
H Help
X Clear all SSD's

Q Exit menu
Enter menu choice: [Quit] p

Current Service Search Descriptors:
=====
Passwd:ou=Users,ou=west,ou=example,ou=com?

Hit return to continue.

A Add a Service Search Descriptor
D Delete a SSD
M Modify a SSD
P Display all SSD's
H Help
X Clear all SSD's

Q Exit menu
Enter menu choice: [Quit] q
```

LDAP サーバーへのデータの移入

DIT が作成されたら、情報ツリーにデータを移入します。データは、/etc ファイルを含むすべてのシステムから継承されます。したがって、このタスクはサーバー上ではなく、これらのシステム上で実行する必要があります。情報ツリーにデータを投入する方法は、[40 ページの「LDAP データ生成の計画」](#)で説明した計画によって異なります。

データが情報ツリーに入力されるファイルの例を次に示します。

■ aliases

- auto_*
- bootparams
- ethers
- group
- hosts

同様に、/etc 内の権限関連ファイル (user_attr、~/security/auth_attr、~/security/prof_attr、および ~/security/exec_attr など) からの情報も情報ツリーに追加されます。

情報ツリーにデータを移入するには、`ldapaddent` コマンドを使用します。また、ツリー上にロードしているデータが含まれる /etc ファイルまたはデータベースも指定します。高いパフォーマンスを実現するために、一部のファイルは順番にロードする必要があります。ファイルとそのロード順序は、次のとおりです。

1. passwd
2. shadow
3. networks
4. netmasks
5. bootparams
6. ethers

オートマウント情報をロードする際は、ファイルまたはデータベース名で `auto_*` の名前付け形式 (`auto_home` など) が使用されることに注意してください。

注記 - `pam_unix_*` モジュールを使用している場合は、ディレクトリサーバーにデータを生成する前に、パスワードを UNIX Crypt 形式で格納するようにサーバーを構成する必要があります。`pam_ldap` を使用している場合、任意の形式でパスワードを格納できます。UNIX crypt 形式でのパスワード設定の詳細は、Oracle Directory Server Enterprise Edition のドキュメントを参照してください。`ldapaddent` コマンドの詳細は、[Ldapaddent\(1M\)](#) のマニュアルページを参照してください。

▼ サーバーにデータを移入する方法

ここでは、クライアントシステムの /etc ファイルから、サーバー上の情報ツリーにデータを移入する手順について説明します。このタスクでは、さまざまなクライアントシステムにある /etc ファイ

ルは単一のファイルにマージされないことが前提となっています。このタスクは、サーバーに移入されるソース /etc ファイルを含むすべてのシステムで実行する必要があります。

このタスクでは、[49 ページの「LDAP のサーバー構成例」](#)でクライアントプロファイルを準備する際に使用された `west.example.com` ドメインが使用されます。

始める前に すでに Oracle Directory Server Enterprise Edition が設定されていることを確認してください。具体的には、[48 ページの「LDAP ネームサービスを使用するように Oracle Directory Server Enterprise Edition を構成する方法」](#)で説明するように、ディレクトリ情報ツリーが `idsconfig` コマンドを使用して構成されていることを確認します。

1. 管理者になります。

詳細は、『Oracle Solaris 11.2 でのユーザーとプロセスのセキュリティー保護』の「割り当てられている管理権利の使用」を参照してください。

2. /etc の各ファイルまたはデータベースから、サーバーにデータを移入します。

```
# ldapaddent -D "cn=directory manager" -f /etc/filename container
```

ここで、*container* には *filename* と同じ名前が含まれます (`passwd` など)。

追加のディレクトリサーバー構成タスク

サーバーに DIT が作成され、必要に応じて SSD が定義されたら、次の追加タスクを実行できます。

メンバー属性を使用したグループメンバーシップの指定

RFC ドラフト `rfc2307bis` は、`groupOfMembers` オブジェクトクラスをグループサービスの LDAP エントリのための便利な構造クラスとしても使用できると規定しています。これにより、グループエントリの識別名 (DN) に、グループメンバーシップを指定するメンバー属性値を含めることができます。Oracle Solaris の LDAP クライアントはこのようなグループエントリをサポートしており、グループメンバーシップの解決のためにメンバー属性値を使用します。

これらの LDAP クライアントはまた、`groupOfUniqueNames` オブジェクトクラスと `uniqueMember` 属性を使用するグループエントリもサポートしています。ただし、このオブジェクトクラスと属性の使用はお勧めできません。

`posixGroup` オブジェクトクラスと `memberUid` 属性を持つグループエントリを定義する既存の方法も引き続きサポートされています。このタイプのグループエントリは引き続き、グループサービスのために LDAP サーバーにデータを生成するときに `ldapaddent` コマンドによって作成されるエントリです。グループエントリに `member` 属性は追加されません。

`groupOfMembers` オブジェクトクラスと `member` 属性値を持つグループエントリを追加するには、`ldapadd` ツールと、次のような入力ファイルを使用します。

```
dn: cn=group1,ou=group,dc=mkg,dc=example,dc=com
objectClass: posixGroup
objectClass: groupOfNames
objectClass: top
cn: group1
gidNumber: 1234
member: uid=user1,ou=people,dc=mkg,dc=example,dc=com
member: uid=user2,ou=people,dc=mkg,dc=example,dc=com
member: cn=group2,ou=group,dc=mkg,dc=example,dc=com
```

LDAP クライアントは、`memberUid`、`member`、および `uniqueMember` 属性のいずれかまたはすべてを含むグループエントリや、どの属性も含まないグループエントリを処理します。メンバーシップの評価結果として、グループに、3 つのすべての属性の和集合から重複が削除されたメンバーシップが与えられます。つまり、グループエントリ `G` がユーザー `U1` と `U2` を参照する `memberUid` 値、ユーザー `U2` を参照する `member` 値、およびユーザー `U3` を参照する `uniqueMember` 値を持っている場合、グループ `G` には `U1`、`U2`、および `U3` の 3 つのメンバーが含まれます。また、入れ子のグループもサポートされます。つまり、メンバー属性は、ほかのグループを指し示す値を持つことができます。

グループメンバーシップを効率的に評価して、ユーザーがメンバーになっているグループ (入れ子のグループを含む) を確認するには、LDAP サーバー上で `memberOf` プラグインが構成され、有効になっている必要があります。そうでない場合は、含んでいるグループ (入れ子のグループを除く) のみが解決されます。デフォルトでは、`memberOf` プラグインは ODSEE サーバーによって有効になります。このプラグインが有効になっていない場合は、ODSEE の `dsconf` ツールを使用して有効にします。

追加プロファイルを使用してディレクトリサーバーを生成する

指定された属性に基づいて構成プロファイルの LDIF (LDAP Data Interchange Format) 表現を作成するには、`genprofile` オプションを指定して `ldapclient` コマンドを使用します。作成したプロファイルは、次に LDAP サーバーに読み込まれ、クライアントプロファイルとして使用

されます。クライアントプロファイルは、`ldapclient init` を使うことによりクライアントからダウンロードできます。

`ldapclient genprofile` の使用については、[ldapclient\(1M\)](#) を参照してください。

▼ ldapclient コマンドを使用してディレクトリサーバーに追加のプロファイルを生成する方法

1. 管理者になります。
詳細は、『Oracle Solaris 11.2 でのユーザーとプロセスのセキュリティー保護』の「割り当てられている管理権利の使用」を参照してください。

2. `ldapclient` コマンドを `genprofile` オプションとともに使用します。

```
# ldapclient genprofile \  
-a profileName=myprofile \  
-a defaultSearchBase=dc=west,dc=example,dc=com \  
-a "defaultServerList=xxx.xxx.x.x yyy.yyy.y.y:portnum" \> myprofile.ldif
```

3. 新規プロファイルをサーバーにアップロードします。

```
# ldapadd -h xxx.xxx.x.x -D "cn=directory manager" -f myprofile.ldif
```

ディレクトリサーバーを構成してアカウント管理を有効にする

`pam_ldap` を使用するクライアントと `pam_unix_*` モジュールを使用するクライアントに対してアカウント管理を実装できます。



注意 - 同じ LDAP ネームドメイン内で `pam_ldap` と `pam_unix_*` モジュールの両方を使用しないでください。すべてのクライアントが `pam_ldap` を使用するか、またはすべてのクライアントが `pam_unix_*` モジュールを使用するかのどちらかです。この制限により、専用の LDAP サーバーが必要になる場合があります。

pam_ldap モジュールを使用するクライアントのアカウント管理

`pam_ldap` が正しく動作するには、パスワードとアカウントのロックアウトポリシーがサーバー上で正しく構成されている必要があります。ディレクトリサーバーコンソール、または `ldapmodify` を使

用して、LDAP ディレクトリのアカウント管理ポリシーを構成できます。手順と詳細情報については、使用しているバージョンの Oracle Directory Server Enterprise Edition の管理者ガイドで「ユーザーアカウントの管理」の章を参照してください。

注記 - 以前は、`pam_ldap` アカウント管理を使用すると、すべてのユーザーがシステムにログインするたびに、認証用にログインパスワードを入力する必要がありました。そのため、`ssh` などのツールを使用した、パスワードに基づかないログインは失敗していました。

現在は、アカウント管理を実行し、ユーザーがログインしているときに Directory Server への認証を行わずにユーザーのアカウントステータスを取得できます。

Directory Server 上の新しい制御は 1.3.6.1.4.1.42.2.27.9.5.8 です。この制御は、デフォルトで有効になっています。デフォルトの制御構成を変更するには、ディレクトリサーバー上でアクセス制御情報 (ACI) を追加します。例:

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
allow (read, search, compare, proxy)
(groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

`proxy` ユーザー用のパスワードは、期限が切れてはいけません。`proxy` パスワードが期限切れになった場合、`proxy` 資格レベルを使用するクライアントはサーバーからネームサービス情報を取り出すことができません。`proxy` ユーザーのパスワードの期限が切れないことを保証するために、次のスクリプトを記述して `proxy` アカウントを変更します。

```
# ldapmodify -h ldapserver -D administrator_DN \
-w administrator-password <<EOF
dn: proxy-user-DN
DNchangetype: modify
replace: passwordexpirationtime
passwordexpirationtime: 20380119031407Z
EOF
```

注記 - pam_ldap のアカウント管理は、Oracle Directory Server Enterprise Edition をもとにユーザーのパスワードやアカウントの有効期限情報を維持し、ユーザーに知らせます。ディレクトリサーバーは、シャドウエントリの対応するデータを解釈してユーザーアカウントを検証することはありません。ただし、pam_unix_* モジュールはシャドウデータを検査して、アカウントがロックされているか、またはパスワードの期限が切れているかどうかを判定します。シャドウデータが LDAP ネームサービスやディレクトリサーバーによって最新の状態に保持されるわけではないため、これらのモジュールは、シャドウデータに基づいてアクセスを許可するべきではありません。シャドウデータは、proxy 識別情報を使用して取得されます。そのため、proxy ユーザーに userPassword 属性への読み取りアクセスを許可しないでください。proxy ユーザーの userPassword への読み取りアクセス権を拒否することにより、PAM サービスが無効なアカウントの検証を行うことはなくなります。

pam_unix_* モジュールを使用するクライアントのアカウント管理

LDAP クライアントがアカウント管理に pam_unix_* モジュールを使用できるようにするには、シャドウデータの更新を有効にするようにサーバーを設定する必要があります。pam_ldap のアカウント管理とは異なり、pam_unix_* モジュールには追加の構成手順が必要ありません。すべての構成は、idsconfig ユーティリティを実行して行うことができます。

次の例は、2 つの idsconfig 実行の出力を示しています。

最初の idsconfig 実行では、既存のクライアントプロファイルを使用します。

```
# /usr/lib/ldap/idsconfig

It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's hostname to setup: myserver
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
Checking LDAP Base DN ...
Validating LDAP Base DN and Suffix ...
sasl/GSSAPI is not supported by this LDAP server

Enter the profile name (h=help): [default] WestUserProfile

Profile 'WestUserProfile' already exists, it is possible to enable
shadow update now. idsconfig will exit after shadow update
```

```
is enabled. You can also continue to overwrite the profile
or create a new one and be given the chance to enable
shadow update later.

Just enable shadow update (y/n/h)? [n] y
Add the administrator identity (y/n/h)? [y]
Enter DN for the administrator: [cn=admin,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for the administrator:
Re-enter passwd:
ADDED: Administrator identity cn=admin,ou=profile,dc=west,dc=example,dc=com.
Proxy ACI LDAP_Naming_Services_proxy_password_read does not
exist for dc=west,dc=example,dc=com.
ACI SET: Give cn=admin,ou=profile,dc=west,dc=example,dc=com read/write access
to shadow data.
ACI SET: Non-Admin access to shadow data denied.

Shadow update has been enabled.
```

2 つ目の `idsconfig` 実行では、後で使用するための新しいプロファイルを作成します。出力の一部のみが表示されています。

```
# /usr/lib/ldap/idsconfig

It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's hostname to setup: myserver
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
Checking LDAP Base DN ...
Validating LDAP Base DN and Suffix ...
sasl/GSSAPI is not supported by this LDAP server

Enter the profile name (h=help): [default] WestUserProfile-new
Default server list (h=help): [192.168.0.1]
.
.
.
Do you want to enable shadow update (y/n/h)? [n] y

Summary of Configuration

1 Domain to serve          : west.example.com
2 Base DN to setup        : dc=west,dc=example,dc=com
Suffix to create          : dc=west,dc=example,dc=com
3 Profile name to create   : WestUserProfile-new
.
.
```

```
.
19 Enable shadow update          : TRUE
.
.
.
Enter DN for the administrator: [cn=admin,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for the administrator:
Re-enter passwd:

WARNING: About to start committing changes. (y=continue, n=EXIT) y

1. Changed timelimit to -1 in cn=config.
2. Changed sizelimit to -1 in cn=config.
.
.
.
11. ACI for dc=test1,dc=mpklab,dc=sfbay,dc=sun,dc=com modified to
disable self modify.
.
.
.
15. Give cn=admin,ou=profile,dc=west,dc=example,dc=com write permission for shadow.
...
```


◆◆◆ 第 5 章

LDAP クライアントの設定

この章では、LDAP ネームサービスクライアントを設定する方法について説明します。この章で扱う内容は、次のとおりです。

- 67 ページの「LDAP クライアント設定の準備」
- 69 ページの「ローカル LDAP クライアント属性の定義」
- 57 ページの「LDAP サーバーへのデータの移入」
- 70 ページの「LDAP クライアントの管理」
- 74 ページの「クライアント認証での LDAP の使用」

LDAP クライアント設定の準備

Oracle Solaris クライアントがネームサービスとして LDAP を使用するための要件は、次のとおりです。

- クライアントのドメイン名が LDAP サーバーによって処理されている必要があります。
- ネームサービススイッチが、必要なサービスの LDAP を指し示している必要があります。
- クライアントに、その動作を定義するパラメータがすべて構成されている必要があります。
- `ldap_cachemgr` がクライアント上で実行されている必要があります。
- クライアントが構成されているサーバーが少なくとも 1 つ起動され、実行されている必要があります。

`ldapclient` ユーティリティは、サーバーの起動を除く、上記の構成手順をすべて実行します。この章では、`ldapclient` ユーティリティを使用して LDAP クライアントを設定する方法や、その他のさまざまな LDAP ユーティリティを使用して LDAP クライアントに関する情報を取得する方法の例を示します。

LDAP とサービス管理機能

Oracle Solaris のサービス管理機能 (SMF) は、LDAP クライアントサービスを管理します。SMF の詳細については、『Oracle Solaris 11.2 でのシステムサービスの管理』を参照してください。詳細は、[svcadm\(1M\)](#) および [svcs\(1\)](#) のマニュアルページも参照してください。

次のリストでは、LDAP クライアントサービスの管理に関連する SMF の機能について詳しく説明します。

- `svcadm` コマンドを使用して、LDAP クライアントサービスを有効化、無効化、または再起動します。

ヒント `-t` オプションを使用してサービスを一時的に無効化すると、そのサービス構成に対していくらかの保護を提供できます。`-t` オプションを使用してサービスを無効にした場合は、リブートのあと、そのサービスの元の設定が復元されます。`-t` なしでサービスを無効にした場合は、リブートのあとも、そのサービスは無効のままになります。

- LDAP クライアントサービスに対する障害管理リソース識別子 (FMRI) は、`svc:/network/ldap/client` です。
- 構成プロセス中は、`network/ldap/client` サービスによって使用されるドメイン名を提供するために、`network/nis/domain` サービスも有効になります。
- `svcs` コマンドを使用して、LDAP クライアントおよび `ldap_cachemgr` デーモンのステータスを照会します。
 - 次の例は、`svcs` コマンドとその出力を示しています。

```
# svcs \*ldap\  
STATE      STIME      FMRI  
online     15:43:46  svc:/network/ldap/client:default
```

- 次の例は、FMRI のインスタンス名を使用したときの `svcs -l` コマンドとその出力を示しています。

```
# svcs -l network/ldap/client:default  
fmri      svc:/network/ldap/client:default  
name      LDAP Name Service Client  
enabled   true
```

```

state      online
next_state none
restarter  svc:/system/svc/restarter:default
manifest   /lib/svc/manifest/network/ldap/client.xml
manifest   /lib/svc/manifest/network/network-location.xml
manifest   /lib/svc/manifest/system/name-service/upgrade.xml
manifest   /lib/svc/manifest/milestone/config.xml
dependency require_all/none svc:/system/filesystem/minimal (online)
dependency require_all/none svc:/network/initial (online)
dependency optional_all/none svc:/network/location:default (online)
dependency require_all/restart svc:/network/nis/domain (online)
dependency optional_all/none svc:/system/name-service/upgrade (online)
dependency optional_all/none svc:/milestone/config (online)
dependency optional_all/none svc:/system/manifest-import (online)
dependency require_all/none svc:/milestone/unconfig (online)

```

- 次のコマンドを使用すると、デーモンの存在をチェックできます。

- サーバー上で、ptree コマンドを使用します。

```

# ptree `pgrep slapd`
6410 zsched
11565 /export/dsee/dsee6/ds6/lib/64/ns-slapd -D /export/dsee/test1 -i /export

```

- クライアント上で、ldapsearch コマンドを使用します。

```

# ldapsearch -h server-name -b "" -s base "objectclass=*" |grep -i context
namingContexts: dc=example,dc=com

```

LDAP クライアントプロファイルで指定された構成情報は、svc:/network/ldap/client サービスが起動されたときに SMF リポジトリに自動的にインポートされます。

ローカル LDAP クライアント属性の定義

第3章「LDAP ネームサービスの計画要件」では、LDAP サーバーを構成するために定義する LDAP クライアントプロファイルの属性について説明しています。これらの属性を含むプロファイルは、idsconfig コマンドを使用してサーバーに設定されます。

その他のクライアント属性は、ldapclient コマンドを使用してローカルに設定できます。次の表に、これらの属性を一覧表示します。

表 5-1 ローカルの LDAP クライアント属性

属性	説明
adminDN	管理者資格の管理者エントリの識別名を指定します。クライアントシステムの enableShadowUpdate スイッチの値が true で、credentialLevel の値が self 以外の場合、adminDN を指定する必要があります。
adminPassword	管理者資格の管理者エントリのパスワードを指定します。クライアントシステム上で enableShadowUpdate スイッチの値が true であり、credentialLevel に self 以外の値が設定されている場合は、adminPassword が定義される必要があります。
domainName	クライアントのドメイン名 (クライアントシステムのデフォルトドメインになる) を指定します。デフォルト値はなく、必ず指定する必要があります。
proxyDN	プロキシの識別名。credentialLevel が proxy に設定された状態でクライアントシステムが構成されている場合は、proxyDN を指定する必要があります。
proxyPassword	プロキシのパスワード。credentialLevel が proxy に設定された状態でクライアントシステムが構成されている場合は、proxyPassword を定義する必要があります。
certificatePath	証明書データベースを含む、ローカルファイルシステム上のディレクトリ。クライアントシステムが TLS を使用して authenticationMethod または service AuthenticationMethod で構成されている場合は、この属性が使用されます。デフォルト値は /var/ldap です。

注記 - SSD 内の BaseDN に末尾のコンマが含まれている場合、その値は defaultSearchBase の相対値として扱われます。検索実行前に、defaultSearchBase の値が BaseDN に付加されます。

LDAP クライアントの管理

このセクションでは、ldapclient コマンドを使用して LDAP クライアントの構成を初期化および修正する方法について説明します。

注記 - LDAP と NIS は network/nis/domain サービスで定義されている同じドメイン名コンポーネントを使用するため、最新の Oracle Solaris リリースは、NIS クライアントとネイティブな LDAP クライアントが同じクライアントシステム上に共存する構成をサポートしていません。

LDAP クライアントの初期化

次の 2 つの方法のいずれかで、ldapclient を使用して LDAP クライアントを初期化できません。

- プロファイルを使用する

ldapclient コマンドを発行するときは、少なくともプロファイルおよびドメインのサーバーアドレスを指定する必要があります。プロファイル指定しなかった場合は、デフォルトのプロファイルが指定されていると見なされます。プロキシと証明書データベースの情報を除いて、必要な情報の残りはプロファイルから提供されます。

クライアントの資格レベルがプロキシまたは匿名プロキシである場合は、プロキシのバインド DN とパスワードを入力してください。詳細は、18 ページの「クライアント資格レベル」を参照してください。シャドウデータの更新を有効にするには、管理者の資格情報 (adminDN および adminPassword) を指定する必要があります。

プロファイルを使用すると、特にエンタープライズ環境で LDAP 構成の複雑さが軽減されます。

- 単一のコマンド行ですべてのパラメータを定義する

プロファイルは存在しません。つまり、クライアント自体でプロファイルを作成します。この方法を使用しても、プロファイル情報はキャッシュファイルに格納されサーバーによってリフレッシュされることはありません。

ldapclient コマンドを使用した別のコマンド構文を使用すると、クライアントを初期化できません。

- デフォルト値で構成されているプロファイルを使用して、クライアントを初期化します。例:

```
# ldapclient init -a profilename=new -a domainname=west.example.com 192.168.0.1
System successfully configured
```

- ユーザー別の資格情報を含むプロファイルが構成されているクライアントを初期化し、sasl/GSSAPI 認証方法を使用します。

この例では、idsconfig コマンドを使用して DIT を構築する際に、適切な認証方法および資格レベル (資格レベルには self、認証方法には sasl/GSSAPI など) が指定されたことが前提となっています。idsconfig コマンドの出力の一部を次に示します。ここでは、サーバー上にユーザー別のプロファイルが作成されています。

```
# /usr/lib/ldap/idsconfig
Do you wish to continue with server setup (y/n/h)? [n] y
Enter the Directory Server's hostname to setup: kdc.example.com
Enter the port number for DSEE (h=help): [389] <Enter your port>
Enter the directory manager DN: [cn=Directory Manager] <Enter your DN>
Enter passwd for cn=Directory Manager: <Enter your password>
Enter the domainname to be served (h=help): [example.com] <Enter your domain>
```

```
Enter LDAP Base DN (h=help): [dc=example,dc=com] <Enter your DN>
GSSAPI is supported. Do you want to set up gssapi:(y/n) [n] y
Enter Kerberos Realm: [EXAMPLE.COM] EXAMPLE.COM
```

プロファイルの名前は `gssapi_EXAMPLE.COM` です。例で示した方法でプロファイルを作成したあとに `ldapclient` コマンドを発行すると、ユーザー別のプロファイルを含むクライアントを初期化できます。

```
# ldapclient init -a profilename=gssapi_EXAMPLE.COM -a \
domainname=example.com 9.9.9.50
```

注記 - Kerberos の構成や DNS サーバーの構成など、ユーザー別の資格情報を使用して構成されたクライアントを初期化して、LDAP を操作する際には、いくつかの要件を満たしている必要があります。Kerberos については、『[Oracle Solaris 11.2 での Kerberos およびその他の認証サービスの管理](#)』を参照してください。DNS の構成については、『[Oracle Solaris 11.2 ディレクトリサービスとネームサービスでの作業: DNS と NIS](#)』の第 3 章「ドメインネームシステムの管理」を参照してください。認証については、第 2 章「LDAP と認証サービス」、DIT の構築については、第 3 章「LDAP ネームサービスの計画要件」を参照してください。

- プロキシ資格情報を使用するクライアントを初期化します。例:

```
# ldapclient init \
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
-a domainname=west.example.com \
-a profilename=pit1 \
-a proxypassword=test1234 192.168.0.1
```

使用されるプロファイルが proxy 用に設定される場合は、`-a proxyDN` と `-a proxyPassword` が必要です。サーバーに保存されているプロファイルにはこの資格情報が含まれていないため、クライアントを初期設定するときは資格情報を入力する必要があります。この方法は、プロキシの資格情報をサーバーに保存していた従来の方法に比べて安全性が高くなります。

これらのプロキシ情報は、`config` および `cred` プロパティグループ内の `svc:/network/ldap/client` サービス内に格納されます。

- クライアントを初期化して、シャドウデータの更新を有効にします。例:

```
# ldapclient init \
```

```
-a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \  
-a adminPassword=admin-password \  
-a domainName=west.example.com \  
-a profileName=WestUserProfile \  
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \  
-a proxyPassword=proxy-password \  
-a enableShadowUpdate=TRUE \  
192.168.0.1  
System successfully configured
```

LDAP クライアント構成の変更

プロファイルなしで `ldapclient` コマンドを使用すると、クライアント構成を変更できます。変更しても限られた数のクライアント属性しか影響を受けないため、選択したすべての属性を変更する単一のコマンド行だけで十分であることが多いです。

- 単純な認証方法が使用されるように、LDAP クライアントを変更します。例:

```
# ldapclient mod -a authenticationMethod=simple
```

- シャドウデータの更新が有効になるように、構成された LDAP クライアントを変更します。例:

```
# ldapclient mod -a enableShadowUpdate=TRUE \  
-a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \  
-a adminPassword=admin-password  
System successfully configured
```

LDAP クライアントの初期化解除

LDAP クライアントの初期化解除は、クライアント名サービスを `init`、`modify`、または `manual` オプションを付けて `ldapclient` コマンドを最後に発行する前のステータスに復元することを意味します。言い換えると、コマンドに `-uninit` オプションを付けると、`ldapclient` コマンドのその他のオプションによって適用された最後の変更が取り消されます。たとえば、`profile1` を使用するようにクライアントを構成したあとで `profile2` を使用するように変更した場合、`ldapclient uninit` を実行すると、クライアントで `profile1` を使用するように構成が元に戻ります。

LDAP クライアントを初期化解除するには、次のコマンド構文を使用します。

```
# ldapclient uninit
System successfully recovered.
```

クライアント認証での LDAP の使用

このセクションでは、LDAP 認証サービスを使用するさまざまな構成タスクについて説明します。

PAM の構成

`pam_ldap` モジュールは、クライアント認証およびアカウント管理を実行するための LDAP の PAM モジュールオプションです。クライアントプロファイルの認証モジュールを `simple` として、資格レベルを `self` として構成した場合は、`pam_krb` モジュールを有効にする必要もあります。次のリソースを参照してください。

- [pam_ldap\(5\)](#) のマニュアルページ
- [pam_krb5\(5\)](#) のマニュアルページ
- 『Oracle Solaris 11.2 での Kerberos およびその他の認証サービスの管理』

UNIX policy を使用するための PAM の構成

`/etc/pam.conf` ファイルは、UNIX policy を使用するための PAM のデフォルト構成ファイルとして機能します。通常は、このファイルの変更を導入する必要はありません。

ただし、`shadow` データによって制御されるパスワードの有効期限とパスワードポリシーが必要な場合は、クライアントを `enableShadowUpdate` スイッチを使用して構成および実行する必要があります。シャドウデータの更新を有効にするための LDAP クライアントの初期化例については、[70 ページの「LDAP クライアントの初期化」](#)を参照してください。

構成ファイルの詳細は、[pam.conf\(4\)](#) のマニュアルページを参照してください。

LDAP `server_policy` を使用するための PAM の構成

LDAP `server_policy` を使用するように PAM を構成する場合は、[31 ページの「アカウント管理に `pam_ldap` モジュールを使用した `pam_conf` ファイルの例](#)」を参照してください。このサンプルファイルを使用して、次の追加手順を実行します。

- `pam_ldap.so.1` を含む行をクライアントの `/etc/pam.conf` ファイルに追加します。
- サンプルファイル内のいずれかの PAM モジュールで `binding` フラグと `server_policy` オプションが指定されている場合は、クライアントの `/etc/pam.conf` ファイル内の対応するモジュールで同じフラグとオプションを使用します。

`binding` 管理フラグを使うことにより、ローカルパスワードがリモート (LDAP) パスワードをオーバーライドします。たとえば、ローカルファイルと LDAP 名前空間の両方にユーザーアカウントが見つかった場合、リモートパスワードよりローカルアカウントのパスワードの方が優先されます。したがって、ローカルパスワードの期限が切れているときは、たとえリモート LDAP パスワードがまだ有効であっても認証に失敗します。

`server_policy` オプションによって、`pam_unix_auth`、`pam_unix_account`、および `pam_passwd_auth` は LDAP 名前空間で検出されたユーザーを無視し、`pam_ldap` による認証やアカウント検証が可能になります。`pam_authtok_store` は、新しいパスワードを暗号化せずに LDAP サーバーに渡します。その後、パスワードはサーバー上で構成されるパスワードの暗号化スキームに基づいたディレクトリに保存されます。詳細は、[`pam.conf\(4\)`](#) および [`pam_ldap\(5\)`](#) を参照してください。

- サービスモジュール `pam_authtok_store.so.1` を含む行に、`server_policy` オプションを追加します。

注記 - 以前は、`pam_ldap` アカウント管理を使用すると、すべてのユーザーがシステムにログインするたびに、認証用にログインパスワードを入力する必要がありました。そのため、`ssh` などのツールを使用した、パスワードに基づかないログインは失敗していました。

現在は、アカウント管理を実行し、ユーザーがログインしているときに Directory Server への認証を行わずにユーザーのアカウントステータスを取得できます。

Directory Server 上の新しい制御は 1.3.6.1.4.1.42.2.27.9.5.8 です。この制御は、デフォルトで有効になっています。デフォルトの制御構成を変更するには、ディレクトリサーバー上でアクセス制御情報 (ACI) を追加します。例:

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
allow (read, search, compare, proxy)
(groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

TLS のセキュリティーの設定

注記 - PEM 証明書ファイルは、すべてのユーザーが読み取ることができる必要があります。これらのファイルを暗号化したり、読み取り権限を制限したりしないでください。そうしなければ、`ldaplist` などのツールが機能しません。

TLS (Transport Layer Security) を使用している場合は、必要な PEM 証明書ファイルをインストールする必要があります。特に、LDAP サーバーの検証やサーバーへのクライアントアクセスの検証に使用される、自己署名されたサーバー証明書および CA 証明書ファイルはすべて必須です。たとえば、PEM CA 証明書 `certdb.pem` を持っている場合は、このファイルが追加され、証明書パスで読み取り可能であることを確認する必要があります。

注記 - TLS を使用している場合は、`ldapclient` を実行する前に、まず、このセクションで説明した必要な PEM 証明書ファイルをインストールします。

PEM 形式の証明書を作成および管理する方法については、使用している Oracle Directory Server Enterprise Edition のバージョンに対応した管理者ガイドの「SSL の管理」の章で、SSL を使用するための LDAP クライアントの構成に関するセクションを参照してください。

構成後に、これらのファイルを LDAP ネームサービスクライアントから要求された場所に格納する必要があります。この場所は、`certificatePath` 属性で決定されます。デフォルトでは、この場所は `/var/ldap` にあります。

たとえば、`certdb.pem` などの必要な PEM 証明書ファイルを作成したあとに、そのファイルを次のようにデフォルトの場所にコピーします。

```
# cp certdb.pem /var/ldap
```

次に、すべてのユーザーに読み取り権を付与します。

```
# chmod 444 /var/ldap/certdb.pem
```

注記 - 証明書パスに複数の証明書ファイルが存在する場合があります。さらに、特定の PEM 証明書ファイルに、連結された複数の PEM 形式の証明書が含まれている場合もあります。詳細は、サーバーのドキュメントを参照してください。証明書ファイルを LDAP ネームサービスクライアントで使用している場合は、証明書ファイルをローカルのファイルシステムに格納する必要があります。

◆◆◆ 第 6 章

LDAP のトラブルシューティング

この章では、LDAP 構成に関する問題について説明し、それらの問題を解決するための方法を提案します。この章では、次の内容について説明します。

- [79 ページの「LDAP クライアントステータスのモニタリング」](#)
- [82 ページの「LDAP の構成で発生する問題とその解決方法」](#)

LDAP クライアントステータスのモニタリング

このセクションでは、LDAP クライアント環境の状態判定に使用するさまざまなコマンドについて説明します。使用可能なオプションの詳細については、関連するマニュアルページも参照してください。

サービス管理機能 (SMF) については、『[Oracle Solaris 11.2 でのシステムサービスの管理](#)』を参照してください。また、詳細については [svcadm\(1M\)](#) および [svcs\(1\)](#) のマニュアルページも参照してください。

ldap_cachemgr デーモンが実行中であることの確認

ldap_cachemgr デーモンは、常に実行中で適切に機能している必要があります。このデーモンが機能していない場合、システムは動作しません。LDAP クライアントサービス `svc:/network/ldap/client` を設定して起動すると、クライアントの SMF メソッドは ldap_cachemgr デーモンを自動的に起動します。LDAP クライアントサービスがオンラインかどうかについては、さまざまな方法で確認できます。

- `svcs` コマンドを使用して、このサービスが有効になっているかどうかを確認します。

```
# svcs \*ldap\*
```

```
STATE          STIME    FMRI
disabled       Aug_24   svc:/network/ldap/client:default
```

- サービスに関するすべての情報を表示するには、`-l` オプションを使用します。

```
# svcs -l network/ldap/client:default
fmri svc:/network/ldap/client:default
name LDAP Name Service Client
enabled false
state disabled
next_state none
state_time Thu Oct 20 23:04:11 2011
logfile /var/svc/log/network-ldap-client:default.log
restarter svc:/system/svc/restarter:default
contract_id
manifest /lib/svc/manifest/network/ldap/client.xml
manifest /lib/svc/manifest/milestone/config.xml
manifest /lib/svc/manifest/network/network-location.xml
manifest /lib/svc/manifest/system/name-service/upgrade.xml
dependency optional_all/none svc:/milestone/config (online)
dependency optional_all/none svc:/network/location:default (online)
dependency require_all/none svc:/system/filesystem/minimal (online)
dependency require_all/none svc:/network/initial (online)
dependency require_all/restart svc:/network/nis/domain (online)
dependency optional_all/none svc:/system/manifest-import (online)
dependency require_all/none svc:/milestone/unconfig (online)
dependency optional_all/none svc:/system/name-service/upgrade (online)
```

- `-g` オプションを `ldap_cachemgr` に渡します。

このオプションでは、問題の診断に役立つより広範なステータス情報が提供されます。

```
# /usr/lib/ldap/ldap_cachemgr -g
cachemgr configuration:
server debug level          0
server log file "/var/ldap/cachemgr.log"
number of calls to ldpcachemgr      19

cachemgr cache data statistics:
Configuration refresh information:
```

```
Previous refresh time: 2010/11/16 18:33:28
Next refresh time:    2010/11/16 18:43:28
Server information:
Previous refresh time: 2010/11/16 18:33:28
Next refresh time:    2010/11/16 18:36:08
server: 192.168.0.0, status: UP
server: 192.168.0.1, status: ERROR
error message: Can't connect to the LDAP server
Cache data information:
Maximum cache entries:      256
Number of cache entries:    2
```

ldap_cachemgr デーモンが無効になっている場合は、次のコマンドを使用して有効にします。

```
# svcadm enable network/ldap/client
```

デーモンの詳細は、[ldap_cachemgr\(1M\)](#) のマニュアルページを参照してください。

現在のプロファイル情報の確認

現在のプロファイル情報を表示するには、スーパーユーザーまたは同等の役割になり、`ldapclient` を `list` オプションを付けて実行します。

```
# ldapclient list
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
NS_LDAP_BINDPASSWD= {NS1}4a3788e8c053424f
NS_LDAP_SERVERS= 192.168.0.1, 192.168.0.10
NS_LDAP_SEARCH_BASEDN= dc=west,dc=example,dc=com
NS_LDAP_AUTH= simple
NS_LDAP_SEARCH_REF= TRUE
NS_LDAP_SEARCH_SCOPE= one
NS_LDAP_SEARCH_TIME= 30
NS_LDAP_SERVER_PREF= 192.168.0.1
NS_LDAP_PROFILE= pit1
NS_LDAP_CREDENTIAL_LEVEL= proxy
NS_LDAP_SERVICE_SEARCH_DESC= passwd:ou=people,?sub
NS_LDAP_SERVICE_SEARCH_DESC= group:ou=group,dc=west,dc=example,dc=com?one
NS_LDAP_BIND_TIME= 5
```

`ldapclient list` コマンドのほかにも、`svccfg` または `svccprop` コマンドを使用して、現在のプロファイル情報を取得することもできます。

基本的なクライアント/サーバー間通信の検証

LDAP クライアントと LDAP サーバー間に通信が存在することを確認するには、`ldaplist` コマンドを使用します。

- オプションを付けずに `ldaplist` コマンドを使用すると、サーバー上の DIT のコンテナがすべて表示されます。
- `ldaplist database` コマンド (`ldaplist passwd username` や `ldaplist host hostname` など) は、特定のデータベースの内容を表示します。

クライアント以外のマシンからのサーバーデータの確認

既存の LDAP クライアントがないシステムに関する情報を確認するには、`ldapsearch` コマンドを使用します。表示される情報は、検索に使用するフィルタに応じて異なります。次の例に、DIT 内のすべてのコンテナを示します。

```
# ldapsearch -h server1 -b "dc=west,dc=example,dc=com" -s one "objectclass=*"
```

`ldapsearch` コマンドで使用可能なオプションおよびフィルタのリストについては、[ldapsearch\(1\)](#) のマニュアルページを参照してください。

LDAP の構成で発生する問題とその解決方法

このセクションでは、発生する可能性のある LDAP 構成に関する問題について説明し、その解決方法を提案します。

未解決のホスト名

LDAP クライアントソフトウェアは、ホスト検索に対して (`gethostbyname()` や `getaddrinfo()` によって返されるホスト名などの) 完全修飾ホスト名を返します。格納済みの名前が指定されている (1 つ以上のドットが含まれている) 場合、クライアントはその名前をそのまま返します。たとえば、格納されている名前が `hostB.eng` であれば、返される名前も `hostB.eng` です。

LDAP ディレクトリに格納された名前が指定されていない (ドットが含まれない) 場合、クライアントソフトウェアは、その名前にドメイン部分を追加します。たとえば、格納されている名前が `hostA` であれば、返される名前は `hostA.domainname` となります。

LDAP ドメイン内のシステムにリモートアクセスできない

DNS ドメイン名が LDAP ドメイン名とは異なる場合、格納されたホスト名が完全指定でないかぎり LDAP ネームサービスをホスト名に対して使用することはできません。

ログインできない

LDAP クライアントはログイン中、ユーザー認証に PAM モジュールを使用します。UNIX 標準の PAM モジュールでは、パスワードをサーバーから読み込みクライアント側で検査します。このプロセスは、次のいずれかの理由で失敗することがあります。

- ldap が、ネームサービススイッチ内の passwd データベースに関連付けられていない。
- プロキシエージェントが、サーバーリスト上のユーザーの userPassword 属性を読み取ることができない。プロキシエージェントが比較のためにパスワードをクライアントに返すので、少なくともプロキシエージェントはパスワードを読めなければならない。pam_ldap に関しては、パスワードへの読み取りアクセスを必要としない
- プロキシエージェントが適切なパスワードを保持していない
- 該当するエントリに shadowAccount オブジェクトクラスが定義されていない
- パスワードが定義されていない

ldapaddent を使用する場合、-p オプションを使用してパスワードをユーザーエントリに確実に追加する必要があります。ldapaddent を -p オプションなしで使用すると、ldapaddent を使用して /etc/shadow ファイルも追加しないかぎり、ユーザーのパスワードはディレクトリ内に格納されません。

- LDAP サーバーに到達することができない
サーバーのステータスを確認します。

```
# /usr/lib/ldap/ldap_cachemgr -g
```

- pam.conf の構成が不正である
- LDAP 名前空間でユーザーが定義されていない
- pam_unix_* モジュールに関して NS_LDAP_CREDENTIAL_LEVEL が anonymous に設定されているため、匿名ユーザーが userPassword を使用できない。
- パスワードが crypt 形式で格納されていない
- アカウント管理をサポートするように pam_ldap が構成されている場合は、次のいずれかの原因でログインに失敗します。

- ユーザーのパスワード期限が切れている
- ログインを何回も行なったために、ユーザーアカウントがロックされる
- 管理者がユーザーアカウントを非アクティブにした
- ユーザーが、ssh や sftp などの、パスワードを使用しないプログラムを使用してログインしようとした。
- ユーザー別の認証および sasl/GSSAPI を使用している場合、一部の Kerberos コンポーネントまたは pam_krb5 構成が正しく設定されません。このような問題の解決の詳細は、『Oracle Solaris 11.2 での Kerberos およびその他の認証サービスの管理』を参照してください。

検索が遅すぎる

LDAP データベースは、検索パフォーマンス向上にインデックスを使用します。インデックスが正しく構成されていない場合、大幅にパフォーマンスが低下することがあります。Oracle とその他のベンダーのどちらの LDAP ドキュメントにも、インデックスを作成する必要がある共通の属性セットについて記述されています。また、独自のインデックスを追加して、パフォーマンスの向上を図ることができます。

ldapclient コマンドがサーバーにバインドできない

profileName 属性が指定された init オプションを使用しているときに、ldapclient コマンドがクライアントの初期化に失敗しました。考えられる失敗の原因は次のとおりです。

- コマンド行で不正なドメイン名が指定された
- 指定されたクライアントドメインのエントリポイントを表す nisDomain 属性が DIT (ディレクトリ情報ツリー) 内に設定されていない
- アクセス制御情報がサーバー上で適正に設定されていないため、LDAP データベース内の匿名検索が許可されない
- ldapclient コマンドに渡されたサーバーアドレスが間違っている。ldapsearch コマンドを使用してサーバーアドレスを確認してください。
- ldapclient コマンドに渡されたプロファイル名が間違っている。ldapsearch コマンドを使用して DIT 内のプロファイル名を確認してください。

トラブルシューティングの支援として、クライアントのネットワークインタフェースで snoop を使用して外向きのトラフィックを検査して、どのサーバーにアクセスしているかを確認する。

デバッグでの `ldap_cachemgr` デーモンの使用

`-g` オプションを指定して `ldap_cachemgr` デーモンを実行して、現在のクライアント構成や統計情報を表示すると、デバッグに役立つことがあります。

このコマンドによって、すでに説明したように、すべての LDAP サーバーのステータスを含む現在のクライアント構成および統計が標準出力に出力されます。このコマンドを実行するのに、スーパーユーザーになる必要はありません。

設定中に `ldapclient` コマンドがハングアップする

`ldapclient` コマンドがハングアップした場合、`Ctrl-C` キーを押すと以前の環境を復元したあとで終了します。このようなイベントでは、サーバーが動作していることをサーバー管理者に確認してください。

プロファイルまたはコマンド行に指定されたサーバーリスト属性で、サーバー情報が適正であることを確認してください。

ユーザー別の資格情報を使用したときの問題の解決

ユーザー別の資格証明を使用するには、Kerberos 設定などの追加構成が必要です。ユーザー別のプロファイルを構成する際は、次の注記を参照してください。

`syslog` ファイルが `82 Local Error` を示している

`syslog` ファイルに、次のエラーメッセージが含まれることがあります。

```
libsldap: Status: 7 Mesg: openConnection: GSSSAPI bind failed -82 Local error
```

Kerberos が初期化されていないか、そのチケットの有効期限が切れてる可能性があります。参照するには、`klist` コマンドを発行します。`kinit -p` コマンドまたは `kinit -R` コマンドを発行すると、Kerberos が再初期化されます。

Kerberos が自動的に初期化されない

ログインするたびに `kinit` コマンドが自動的に実行されるようにするには、`/etc/pam.conf` ファイルに `pam_krb5.so.1` を追加します。例:

```
login      auth optional pam_krb5.so.1
rlogin     auth optional pam_krb5.so.1
other      auth optional pam_krb5.so.1
```

syslog ファイルが無効な資格証明を示している

`kinit` コマンドの発行後、`syslog` ファイルに `Invalid credential` が含まれることがあります。次のいずれかの問題が考えられます。

- LDAP ディレクトリに `root` ホストエントリまたはユーザーエントリが存在しない。
- マッピングルールが適切でない。

スイッチチェック時に `ldapclient init` コマンドに失敗する

`ldapclient init` コマンドを発行すると、LDAP プロファイルに `self/sasl/GSSAPI` 構成が存在するかどうかチェックされます。スイッチチェックに失敗した場合、一般にエラーの原因は、ホストデータベースの検索基準として `DNS` が使用されていないことにあります。

- 次の 2 つのコマンドを発行して、`DNS` サービスのステータスをチェックしてから、サービスを有効にします。

```
# svcs -l dns/client
# svcadm enable dns/client
```

- `sasl/GSSAPI` のバインド操作でエラーが発生した場合は、`syslog` ファイルをチェックして問題を特定します。

LDAP ネームサービス情報の検出

`ldaplist` ユーティリティを使用すると、LDAP ネームサービスに関する情報を取得できます。この LDAP ユーティリティは、LDAP サーバーにあるネーミング情報が LDIF 形式で一覧表

示するため、トラブルシューティングで役立つことがあります。詳細は、[ldaplist\(1\)](#) を参照してください。

すべての LDAP コンテナを表示する

`ldaplist` コマンドは、空白行で区切られたレコードを含む出力を表示するため、レコードが複数ある場合に役立ちます。

`ldaplist` の出力は、クライアントの構成によって変わります。たとえば、`ns_ldap_search` の値が `one` ではなく `sub` である場合は、`ldaplist` によって、現在の検索 `baseDN` の下にあるすべてのエントリが一覧表示されます。

次の例は、`ldaplist` の出力サンプルを示します。

```
# ldaplist
dn: ou=people,dc=west,dc=example,dc=com

dn: ou=group,dc=west,dc=example,dc=com

dn: ou=rpc,dc=west,dc=example,dc=com

dn: ou=protocols,dc=west,dc=example,dc=com

dn: ou=networks,dc=west,dc=example,dc=com

dn: ou=netgroup,dc=west,dc=example,dc=com

dn: ou=aliases,dc=west,dc=example,dc=com

dn: ou=hosts,dc=west,dc=example,dc=com

dn: ou=services,dc=west,dc=example,dc=com

dn: ou=ethers,dc=west,dc=example,dc=com

dn: ou=profile,dc=west,dc=example,dc=com

dn: automountmap=auto_home,dc=west,dc=example,dc=com

dn: automountmap=auto_direct,dc=west,dc=example,dc=com

dn: automountmap=auto_master,dc=west,dc=example,dc=com

dn: automountmap=auto_shared,dc=west,dc=example,dc=com
```

すべてのユーザーエントリ属性を表示する

ユーザーの `passwd` エントリなどの特定の情報を一覧表示するには、`getent` コマンドを使用します。例:

```
# getent passwd user1
user1::30641:10:Joe Q. User:/home/user1:/bin/csh
```

`getent` コマンドを使用して、自動マウントテーブルに一覧表示されたデータベースで検索を実行することもできます (例: `getent automount/map [key]`)。例:

```
# getent automount/auto_home user1
user1 server-name:/home/user1
```

前述の例では、`auto_home` は自動マウントマップの名前、`user1` は検索キーです。検索キーを指定しない場合は、指定された自動マウントマップの内容全体が一覧表示されます。

すべての属性をリストするには、`-l` オプションを指定した `ldaplist` コマンドを使用します。

```
# ldaplist -l passwd user1
dn: uid=user1,ou=People,dc=west,dc=example,dc=com
uid: user1
cn: user1
uidNumber: 30641
gidNumber: 10
gecos: Joe Q. User
homeDirectory: /home/user1
loginShell: /bin/csh
objectClass: top
objectClass: shadowAccount
objectClass: account
objectClass: posixAccount
shadowLastChange: 6445
```

◆◆◆ 第 7 章

LDAP ネームサービス (リファレンス)

この章の内容は次のとおりです。

- 89 ページの「LDAP 用の IETF スキーマ」
- 95 ページの「ディレクトリユーザーエージェントのプロファイル (DUAPProfile) スキーマ」
- 98 ページの「Oracle Solaris スキーマ」
- 100 ページの「LDAP 用の Internet Printing Protocol 情報」
- 109 ページの「LDAP 用の汎用ディレクトリサーバーの要件」
- 109 ページの「LDAP ネームサービスで 사용되는デフォルトフィルタ」

LDAP 用の IETF スキーマ

スキーマは、サーバーのディレクトリ内にエントリとして格納可能な情報タイプを記述した定義です。

ディレクトリサーバーが LDAP ネームサービスクライアントをサポートするには、スキーマがクライアントのスキーママッピング機能を使用してマップされていないかぎり、この章で定義されたスキーマがサーバー内で構成されている必要があります。

次のいくつかの必要な LDAP スキーマが IETF によって定義されています: RFC 2307 ネットワーク情報サービススキーマと RFC 2307bis、Lightweight Directory Access Protocol (LDAP) ベースのエージェント用の構成プロファイルスキーマ (RFC 4876)、およびプリンタサービス用の LDAP スキーマ。NIS をサポートするには、これらのスキーマの定義をディレクトリサーバーに追加する必要があります。IETF の Web サイト (<http://www.ietf.org>) で、さまざまな RFC にアクセスできます。

注記 - インターネットドラフト (RFC 2307bis など) は、最大 6 か月間有効なドラフトドキュメントであり、いつでもほかのドキュメントによって更新または廃止される可能性があります。

RFC 2307bis ネットワーク情報サービススキーマ

LDAP サーバーは、改訂された RFC 2307bis をサポートするように構成される必要があります。

nisSchema OID は 1.3.6.1.1 です。RFC 2307bis 属性を次に示します。

```
( nisSchema.1.0 NAME 'uidNumber'  
DESC 'An integer uniquely identifying a user in an  
administrative domain'  
EQUALITY integerMatch SYNTAX 'INTEGER' SINGLE-VALUE )
```

```
( nisSchema.1.1 NAME 'gidNumber'  
DESC 'An integer uniquely identifying a group in an  
administrative domain'  
EQUALITY integerMatch SYNTAX 'INTEGER' SINGLE-VALUE )
```

```
( nisSchema.1.2 NAME 'gecos'  
DESC 'The GECOS field; the common name'  
EQUALITY caseIgnoreIA5Match  
SUBSTRINGS caseIgnoreIA5SubstringsMatch  
SYNTAX 'IA5String' SINGLE-VALUE )
```

```
( nisSchema.1.3 NAME 'homeDirectory'  
DESC 'The absolute path to the home directory'  
EQUALITY caseExactIA5Match  
SYNTAX 'IA5String' SINGLE-VALUE )
```

```
( nisSchema.1.4 NAME 'loginShell'  
DESC 'The path to the login shell'  
EQUALITY caseExactIA5Match  
SYNTAX 'IA5String' SINGLE-VALUE )
```

```
( nisSchema.1.5 NAME 'shadowLastChange'  
EQUALITY integerMatch  
SYNTAX 'INTEGER' SINGLE-VALUE )
```

```
( nisSchema.1.6 NAME 'shadowMin'  
EQUALITY integerMatch  
SYNTAX 'INTEGER' SINGLE-VALUE )
```

```
( nisSchema.1.7 NAME 'shadowMax'  
EQUALITY integerMatch  
SYNTAX 'INTEGER' SINGLE-VALUE )
```

```
( nisSchema.1.8 NAME 'shadowWarning'  
EQUALITY integerMatch  
SYNTAX 'INTEGER' SINGLE-VALUE )
```

```
( nisSchema.1.9 NAME 'shadowInactive'  
EQUALITY integerMatch  
SYNTAX 'INTEGER' SINGLE-VALUE )
```

```
( nisSchema.1.10 NAME 'shadowExpire'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.11 NAME 'shadowFlag'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.12 NAME 'memberUid'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String' )

( nisSchema.1.13 NAME 'memberNisNetgroup'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String' )

( nisSchema.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
SYNTAX 'nisNetgroupTripleSyntax' )

( nisSchema.1.15 NAME 'ipServicePort'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.16 NAME 'ipServiceProtocol'
SUP name )

( nisSchema.1.17 NAME 'ipProtocolNumber'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.18 NAME 'oncRpcNumber'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.19 NAME 'ipHostNumber'
DESC 'IP address as a dotted decimal, eg. 192.168.1.1
      omitting leading zeros'
SUP name )

( nisSchema.1.20 NAME 'ipNetworkNumber'
DESC 'IP network as a dotted decimal, eg. 192.168,
      omitting leading zeros'
SUP name SINGLE-VALUE )

( nisSchema.1.21 NAME 'ipNetmaskNumber'
DESC 'IP netmask as a dotted decimal, eg. 255.255.255.0,
      omitting leading zeros'
EQUALITY caseIgnoreIA5Match
SYNTAX 'IA5String{128}' SINGLE-VALUE )
```

```
( nisSchema.1.22 NAME 'macAddress'
DESC 'MAC address in maximal, colon separated hex
      notation, eg. 00:00:92:90:ee:e2'
EQUALITY caseIgnoreIA5Match
SYNTAX 'IA5String{128}' )

( nisSchema.1.23 NAME 'bootParameter'
DESC 'rpc.bootparamd parameter'
SYNTAX 'bootParameterSyntax' )

( nisSchema.1.24 NAME 'bootFile'
DESC 'Boot image name'
EQUALITY caseExactIA5Match
SYNTAX 'IA5String' )

( nisSchema.1.26 NAME 'nisMapName'
SUP name )

( nisSchema.1.27 NAME 'nisMapEntry'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String{1024}' SINGLE-VALUE )

( nisSchema.1.28 NAME 'nisPublicKey'
DESC 'NIS public key'
SYNTAX 'nisPublicKeySyntax' )

( nisSchema.1.29 NAME 'nisSecretKey'
DESC 'NIS secret key'
SYNTAX 'nisSecretKeySyntax' )

( nisSchema.1.30 NAME 'nisDomain'
DESC 'NIS domain'
SYNTAX 'IA5String' )

( nisSchema.1.31 NAME 'automountMapName'
DESC 'automount Map Name'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )

( nisSchema.1.32 NAME 'automountKey'
DESC 'Automount Key value'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )

( nisSchema.1.33 NAME 'automountInformation'
DESC 'Automount information'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

nisSchema OID は 1.3.6.1.1 です。RFC 2307 objectClasses を次に示します。

```
( nisSchema.2.0 NAME 'posixAccount' SUP top AUXILIARY
  DESC 'Abstraction of an account with POSIX attributes'
  MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )
  MAY ( userPassword $ loginShell $ gecos $ description ) )

( nisSchema.2.1 NAME 'shadowAccount' SUP top AUXILIARY
  DESC 'Additional attributes for shadow passwords'
  MUST uid
  MAY ( userPassword $ shadowLastChange $ shadowMin
        shadowMax $ shadowWarning $ shadowInactive $
        shadowExpire $ shadowFlag $ description ) )

( nisSchema.2.2 NAME 'posixGroup' SUP top STRUCTURAL
  DESC 'Abstraction of a group of accounts'
  MUST ( cn $ gidNumber )
  MAY ( userPassword $ memberUid $ description ) )

( nisSchema.2.3 NAME 'ipService' SUP top STRUCTURAL
  DESC 'Abstraction an Internet Protocol service.
        Maps an IP port and protocol (such as tcp or udp)
        to one or more names; the distinguished value of
        the cn attribute denotes the service's canonical
        name'
  MUST ( cn $ ipServicePort $ ipServiceProtocol )
  MAY ( description ) )

( nisSchema.2.4 NAME 'ipProtocol' SUP top STRUCTURAL
  DESC 'Abstraction of an IP protocol. Maps a protocol number
        to one or more names. The distinguished value of the cn
        attribute denotes the protocol's canonical name'
  MUST ( cn $ ipProtocolNumber )
  MAY description )

( nisSchema.2.5 NAME 'oncRpc' SUP top STRUCTURAL
  DESC 'Abstraction of an Open Network Computing (ONC)
        [RFC1057] Remote Procedure Call (RPC) binding.
        This class maps an ONC RPC number to a name.
        The distinguished value of the cn attribute denotes
        the RPC service's canonical name'
  MUST ( cn $ oncRpcNumber $ description )
  MAY description )

( nisSchema.2.6 NAME 'ipHost' SUP top AUXILIARY
  DESC 'Abstraction of a host, an IP device. The distinguished
        value of the cn attribute denotes the host's canonical
        name. Device SHOULD be used as a structural class'
  MUST ( cn $ ipHostNumber )
  MAY ( l $ description $ manager $ userPassword ) )

( nisSchema.2.7 NAME 'ipNetwork' SUP top STRUCTURAL
  DESC 'Abstraction of a network. The distinguished value of
        the cn attribute denotes the network's canonical name'
  MUST ipNetworkNumber
  MAY ( cn $ ipNetmaskNumber $ l $ description $ manager ) )
```

```
( nisSchema.2.8 NAME 'nisNetgroup' SUP top STRUCTURAL
  DESC 'Abstraction of a netgroup. May refer to other netgroups'
  MUST cn
  MAY ( nisNetgroupTriple $ memberNisNetgroup $ description ) )

( nisSchema.2.9 NAME 'nisMap' SUP top STRUCTURAL
  DESC 'A generic abstraction of a NIS map'
  MUST nisMapName
  MAY description )

( nisSchema.2.10 NAME 'nisObject' SUP top STRUCTURAL
  DESC 'An entry in a NIS map'
  MUST ( cn $ nisMapEntry $ nisMapName )
  MAY description )

( nisSchema.2.11 NAME 'ieee802Device' SUP top AUXILIARY
  DESC 'A device with a MAC address; device SHOULD be
        used as a structural class'
  MAY macAddress )

( nisSchema.2.12 NAME 'bootableDevice' SUP top AUXILIARY
  DESC 'A device with boot parameters; device SHOULD be
        used as a structural class'
  MAY ( bootFile $ bootParameter ) )

( nisSchema.2.14 NAME 'nisKeyObject' SUP top AUXILIARY
  DESC 'An object with a public and secret key'
  MUST ( cn $ nisPublicKey $ nisSecretKey )
  MAY ( uidNumber $ description ) )

( nisSchema.2.15 NAME 'nisDomainObject' SUP top AUXILIARY
  DESC 'Associates a NIS domain with a naming context'
  MUST nisDomain )

( nisSchema.2.16 NAME 'automountMap' SUP top STRUCTURAL
  MUST ( automountMapName )
  MAY description )

( nisSchema.2.17 NAME 'automount' SUP top STRUCTURAL
  DESC 'Automount information'
  MUST ( automountKey $ automountInformation )
  MAY description )

( nisSchema.2.18 NAME 'groupOfMembers' SUP top STRUCTURAL
  DESC 'A group with members (DNs)'
  MUST cn
  MAY ( businessCategory $ seeAlso $ owner $ ou $ o $
        description $ member ) )
```

メールエイリアススキーマ

メールエイリアス情報は、この[インターネットドラフト](#)によって定義されたスキーマを使用します。新しいスキーマが使用可能になるまで、LDAP クライアントは、引き続きこのスキーマをメールエイリアス情報として使用します。

元の LDAP メールグループスキーマには、多数の属性とオブジェクトクラスが含まれています。LDAP クライアントによって使用されるのは、2 つの属性と 1 つのオブジェクトクラスだけです。次にその内容を示します。

メールエイリアス属性を次に示します。

```
( 0.9.2342.19200300.100.1.3
  NAME 'mail'
  DESC 'RFC822 email address for this person'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String(256)'
  SINGLE-VALUE )
```

```
( 2.16.840.1.113730.3.1.30
  NAME 'mgrpRFC822MailMember'
  DESC 'RFC822 mail address of email only member of group'
  EQUALITY CaseIgnoreIA5Match
  SYNTAX 'IA5String(256)' )
```

mailGroup オブジェクトクラスのスキーマを次に示します。

```
( 2.16.840.1.113730.3.2.4
  NAME 'mailGroup'
  SUP top
  STRUCTURAL
  MUST mail
  MAY ( cn $ mailAlternateAddress $ mailHost $ mailRequireAuth $
    mgrpAddHeader $ mgrpAllowedBroadcaster $ mgrpAllowedDomain $
    mgrpApprovePassword $ mgrpBroadcasterModeration $ mgrpDeliverTo $
    mgrpErrorsTo $ mgrpModerator $ mgrpMsgMaxSize $
    mgrpMsgRejectAction $ mgrpMsgRejectText $ mgrpNoMatchAddrs $
    mgrpRemoveHeader $ mgrpRFC822MailMember )
```

ディレクトリユーザーエージェントのプロファイル (DUAPProfile) スキーマ

DUACnfSchemaOID は 1.3.6.1.4.1.11.1.3.1 です。

```
DESC 'Default LDAP server host address used by a DUA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
```

```
SINGLE-VALUE )

( DUAConfSchemaOID.1.0 NAME 'defaultServerList'
  DESC 'Default LDAP server host address used by a DUAList'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

( DUAConfSchemaOID.1.1 NAME 'defaultSearchBase'
  DESC 'Default LDAP base DN used by a DUA'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  SINGLE-VALUE )

( DUAConfSchemaOID.1.2 NAME 'preferredServerList'
  DESC 'Preferred LDAP server host addresses to be used by a
  DUA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

( DUAConfSchemaOID.1.3 NAME 'searchTimeLimit'
  DESC 'Maximum time in seconds a DUA should allow for a
  search to complete'
  EQUALITY integerMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE )

( DUAConfSchemaOID.1.4 NAME 'bindTimeLimit'
  DESC 'Maximum time in seconds a DUA should allow for the
  bind operation to complete'
  EQUALITY integerMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE )

( DUAConfSchemaOID.1.5 NAME 'followReferrals'
  DESC 'Tells DUA if it should follow referrals
  returned by a DSA search result'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
  SINGLE-VALUE )

( DUAConfSchemaOID.1.6 NAME 'authenticationMethod'
  DESC 'A kestring which identifies the type of
  authentication method used to contact the DSA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

( DUAConfSchemaOID.1.7 NAME 'profileTTL'
  DESC 'Time to live before a client DUA
  should re-read this configuration profile'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE )
```

```
( DUACnfSchemaOID.1.9 NAME 'attributeMap'
  DESC 'Attribute mappings used by a DUA'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

( DUACnfSchemaOID.1.10 NAME 'credentialLevel'
  DESC 'Identifies type of credentials a DUA should
  use when binding to the LDAP server'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
  SINGLE-VALUE )

( DUACnfSchemaOID.1.11 NAME 'objectclassMap'
  DESC 'Objectclass mappings used by a DUA'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

( DUACnfSchemaOID.1.12 NAME 'defaultSearchScope'
  DESC 'Default search scope used by a DUA'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

( DUACnfSchemaOID.1.13 NAME 'serviceCredentialLevel'
  DESC 'Identifies type of credentials a DUA
  should use when binding to the LDAP server for a
  specific service'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

( DUACnfSchemaOID.1.14 NAME 'serviceSearchDescriptor'
  DESC 'LDAP search descriptor list used by Naming-DUA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

( DUACnfSchemaOID.1.15 NAME 'serviceAuthenticationMethod'
  DESC 'Authentication Method used by a service of the DUA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

( DUACnfSchemaOID.2.4 NAME 'DUACnfConfigProfile'
  SUP top STRUCTURAL
  DESC 'Abstraction of a base configuration for a DUA'
  MUST ( cn )
  MAY ( defaultServerList $ preferredServerList $
        defaultSearchBase $ defaultSearchScope $
        searchTimeLimit $ bindTimeLimit $
        credentialLevel $ authenticationMethod $
        followReferrals $ serviceSearchDescriptor $
        serviceCredentialLevel $ serviceAuthenticationMethod $
        objectclassMap $ attributeMap $
        profileTTL ) )
```

Oracle Solaris スキーマ

Oracle Solaris プラットフォームに必要なスキーマを次に示します。

- プロジェクトスキーマ
- アクセス制御および実行プロファイルスキーマに基づく役割
- プリントスキーマ

プロジェクトスキーマ

/etc/project ファイルは、プロジェクトに関連付けられた属性のローカルソースです。詳細は、[user_attr\(4\)](#) のマニュアルページを参照してください。

プロジェクト属性を次に示します。

```
( 1.3.6.1.4.1.42.2.27.5.1.1 NAME 'SolarisProjectID'
  DESC 'Unique ID for a Solaris Project entry'
  EQUALITY integerMatch
  SYNTAX INTEGER SINGLE )

( 1.3.6.1.4.1.42.2.27.5.1.2 NAME 'SolarisProjectName'
  DESC 'Name of a Solaris Project entry'
  EQUALITY caseExactIA5Match
  SYNTAX IA5String SINGLE )

( 1.3.6.1.4.1.42.2.27.5.1.3 NAME 'SolarisProjectAttr'
  DESC 'Attributes of a Solaris Project entry'
  EQUALITY caseExactIA5Match
  SYNTAX IA5String )

( 1.3.6.1.4.1.42.2.27.5.1.30 NAME 'memberGid'
  DESC 'Posix Group Name'
  EQUALITY caseExactIA5Match
  SYNTAX 'IA5String' )
```

プロジェクト objectClass を次に示します。

```
( 1.3.6.1.4.1.42.2.27.5.2.1 NAME 'SolarisProject'
  SUP top STRUCTURAL
  MUST ( SolarisProjectID $ SolarisProjectName )
  MAY ( memberUid $ memberGid $ description $ SolarisProjectAttr ) )
```

役割ベースのアクセス制御と実行プロファイルスキーマ

/etc/user_attr ファイルは、ユーザーと役割に関連付けられた拡張属性のローカルソースです。詳細は、[user_attr\(4\)](#) のマニュアルページを参照してください。

役割に基づくアクセス制御の属性を次に示します。

```
( 1.3.6.1.4.1.42.2.27.5.1.4 NAME 'SolarisAttrKeyValue'  
  DESC 'Semi-colon separated key=value pairs of attributes'  
  EQUALITY caseIgnoreIA5Match  
  SUBSTRINGS caseIgnoreIA5Match  
  SYNTAX 'IA5String' SINGLE-VALUE )  
  
( 1.3.6.1.4.1.42.2.27.5.1.7 NAME 'SolarisAttrShortDesc'  
  DESC 'Short description about an entry, used by GUIs'  
  EQUALITY caseIgnoreIA5Match  
  SYNTAX 'IA5String' SINGLE-VALUE )  
  
( 1.3.6.1.4.1.42.2.27.5.1.8 NAME 'SolarisAttrLongDesc'  
  DESC 'Detail description about an entry'  
  EQUALITY caseIgnoreIA5Match  
  SYNTAX 'IA5String' SINGLE-VALUE )  
  
( 1.3.6.1.4.1.42.2.27.5.1.9 NAME 'SolarisKernelSecurityPolicy'  
  DESC 'Solaris kernel security policy'  
  EQUALITY caseIgnoreIA5Match  
  SYNTAX 'IA5String' SINGLE-VALUE )  
  
( 1.3.6.1.4.1.42.2.27.5.1.10 NAME 'SolarisProfileType'  
  DESC 'Type of object defined in profile'  
  EQUALITY caseIgnoreIA5Match  
  SYNTAX 'IA5String' SINGLE-VALUE )  
  
( 1.3.6.1.4.1.42.2.27.5.1.11 NAME 'SolarisProfileId'  
  DESC 'Identifier of object defined in profile'  
  EQUALITY caseExactIA5Match  
  SYNTAX 'IA5String' SINGLE-VALUE )  
  
( 1.3.6.1.4.1.42.2.27.5.1.12 NAME 'SolarisUserQualifier'  
  DESC 'Per-user login attributes'  
  EQUALITY caseIgnoreIA5Match  
  SYNTAX 'IA5String' SINGLE-VALUE )  
  
( 1.3.6.1.4.1.42.2.27.5.1.13 NAME 'SolarisReserved1'  
  DESC 'Reserved for future use'  
  EQUALITY caseIgnoreIA5Match  
  SYNTAX 'IA5String' SINGLE-VALUE )  
  
( 1.3.6.1.4.1.42.2.27.5.1.14 NAME 'SolarisReserved2'  
  DESC 'Reserved for future use'  
  EQUALITY caseIgnoreIA5Match  
  SYNTAX 'IA5String' SINGLE-VALUE )
```

```
( 2.16.840.1.113894.1009.2.100.1.1 NAME 'SolarisUserAttrEntry'  
  DESC 'user_attr file format without username'  
  EQUALITY caseExactIA5Match  
  SYNTAX 'IA5String' )
```

```
( 2.16.840.1.113894.1009.2.100.1.2 NAME 'SolarisUserType'  
  DESC 'specifies whether a normal user or a role'  
  EQUALITY caseExactIA5Match  
  SYNTAX 'IA5String' SINGLE-VALUE )
```

役割に基づくアクセス制御 objectClasses を次に示します。

```
( 1.3.6.1.4.1.42.2.27.5.2.3 NAME 'SolarisUserAttr' SUP top AUXILIARY  
  DESC 'User attributes'  
  MAY ( SolarisUserQualifier $ SolarisAttrReserved1 $ \  
        SolarisAttrReserved2 $ SolarisAttrKeyValue ) )  
  
( 1.3.6.1.4.1.42.2.27.5.2.4 NAME 'SolarisAuthAttr' SUP top STRUCTURAL  
  DESC 'Authorizations data'  
  MUST cn  
  MAY ( SolarisAttrReserved1 $ SolarisAttrReserved2 $ \  
        SolarisAttrShortDesc $ SolarisAttrLongDesc $ \  
        SolarisAttrKeyValue ) )  
  
( 1.3.6.1.4.1.42.2.27.5.2.5 NAME 'SolarisProfAttr' SUP top STRUCTURAL  
  DESC 'Profiles data'  
  MUST cn  
  MAY ( SolarisAttrReserved1 $ SolarisAttrReserved2 $ \  
        SolarisAttrLongDesc $ SolarisAttrKeyValue ) )  
  
( 1.3.6.1.4.1.42.2.27.5.2.6 NAME 'SolarisExecAttr' SUP top AUXILIARY  
  DESC 'Profiles execution attributes'  
  MAY ( SolarisKernelSecurityPolicy $ SolarisProfileType $ \  
        SolarisAttrReserved1 $ SolarisAttrReserved2 $ \  
        SolarisProfileId $ SolarisAttrKeyValue ) )  
  
( 2.16.840.1.113894.1009.2.100.2.1 NAME 'SolarisQualifiedUserAttr'  
  SUP top AUXILIARY  
  DESC 'Host or netgroup qualified user attributes'  
  MAY ( SolarisUserAttrEntry $ SolarisUserType ) )
```

LDAP 用の Internet Printing Protocol 情報

次のセクションでは、Internet Print Protocol とプリンタの属性および ObjectClass について説明します。

Internet Print Protocol 属性

```
( 1.3.18.0.2.4.1140
NAME 'printer-uri'
DESC 'A URI supported by this printer.
This URI SHOULD be used as a relative distinguished name (RDN).
If printer-xri-supported is implemented, then this URI value
MUST be listed in a member value of printer-xri-supported.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )

( 1.3.18.0.2.4.1107
NAME 'printer-xri-supported'
DESC 'The unordered list of XRI (extended resource identifiers) supported
by this printer.
Each member of the list consists of a URI (uniform resource identifier)
followed by optional authentication and security metaparameters.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

( 1.3.18.0.2.4.1135
NAME 'printer-name'
DESC 'The site-specific administrative name of this printer, more end-user
friendly than a URI.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127} SINGLE-VALUE )

( 1.3.18.0.2.4.1119
NAME 'printer-natural-language-configured'
DESC 'The configured language in which error and status messages will be
generated (by default) by this printer.
Also, a possible language for printer string attributes set by operator,
system administrator, or manufacturer.
Also, the (declared) language of the "printer-name", "printer-location",
"printer-info", and "printer-make-and-model" attributes of this printer.
For example: "en-us" (US English) or "fr-fr" (French in France) Legal values of
language tags conform to [RFC3066] "Tags for the Identification of Languages".'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127} SINGLE-VALUE )

( 1.3.18.0.2.4.1136
NAME 'printer-location'
DESC 'Identifies the location of the printer. This could include
things like: "in Room 123A", "second floor of building XYZ".'
EQUALITY caseIgnoreMatch
```

```
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127} SINGLE-VALUE )

( 1.3.18.0.2.4.1139
NAME 'printer-info'
DESC 'Identifies the descriptive information about this printer.
This could include things like: "This printer can be used for
printing color transparencies for HR presentations", or
"Out of courtesy for others, please print only small (1-5 page)
jobs at this printer", or even "This printer is going away on July 1, 1997,
please find a new printer".'
```

```
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127}
SINGLE-VALUE )

( 1.3.18.0.2.4.1134
NAME 'printer-more-info'
DESC 'A URI used to obtain more information about this specific printer.
For example, this could be an HTTP type URI referencing an HTML page
accessible to a Web Browser.
The information obtained from this URI is intended for end user consumption.'
```

```
EQUALITY caseIgnoreMatch ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )

( 1.3.18.0.2.4.1138
NAME 'printer-make-and-model'
DESC 'Identifies the make and model of the device.
The device manufacturer MAY initially populate this attribute.'
```

```
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127} SINGLE-VALUE )

( 1.3.18.0.2.4.1133
NAME 'printer-ipp-versions-supported'
DESC 'Identifies the IPP protocol version(s) that this printer supports,
including major and minor versions,
i.e., the version numbers for which this Printer implementation meets
the conformance requirements.'
```

```
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1132
NAME 'printer-multiple-document-jobs-supported'
DESC 'Indicates whether or not the printer supports more than one
document per job, i.e., more than one Send-Document or Send-Data
operation with document data.'
```

```
EQUALITY booleanMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )

( 1.3.18.0.2.4.1109
NAME 'printer-charset-configured'
```

DESC 'The configured charset in which error and status messages will be generated (by default) by this printer.
Also, a possible charset for printer string attributes set by operator, system administrator, or manufacturer.
For example: "utf-8" (ISO 10646/Unicode) or "iso-8859-1" (Latin1).
Legal values are defined by the IANA Registry of Coded Character Sets and the "(preferred MIME name)" SHALL be used as the tag.
For coherence with IPP Model, charset tags in this attribute SHALL be lowercase normalized.
This attribute SHOULD be static (time of registration) and SHOULD NOT be dynamically refreshed attributetypes: (subsequently).'

EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{63} SINGLE-VALUE)

(1.3.18.0.2.4.1131
NAME 'printer-charset-supported'
DESC 'Identifies the set of charsets supported for attribute type values of type Directory String for this directory entry.
For example: "utf-8" (ISO 10646/Unicode) or "iso-8859-1" (Latin1).
Legal values are defined by the IANA Registry of Coded Character Sets and the preferred MIME name.'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{63})

(1.3.18.0.2.4.1137
NAME 'printer-generated-natural-language-supported'
DESC 'Identifies the natural language(s) supported for this directory entry.
For example: "en-us" (US English) or "fr-fr" (French in France).
Legal values conform to [RFC3066], Tags for the Identification of Languages.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{63})

(1.3.18.0.2.4.1130
NAME 'printer-document-format-supported'
DESC 'The possible document formats in which data may be interpreted and printed by this printer.
Legal values are MIME types come from the IANA Registry of Internet Media Types.'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127})

(1.3.18.0.2.4.1129
NAME 'printer-color-supported'
DESC 'Indicates whether this printer is capable of any type of color printing at all, including highlight color.'
EQUALITY booleanMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE)

(1.3.18.0.2.4.1128
NAME 'printer-compression-supported'
DESC 'Compression algorithms supported by this printer.
For example: "deflate, gzip". Legal values include; "none", "deflate" attributetypes: (public domain ZIP), "gzip" (GNU ZIP), "compress" (UNIX).'

EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{255})

```
( 1.3.18.0.2.4.1127
NAME 'printer-pages-per-minute'
DESC 'The nominal number of pages per minute which may be output by this
printer (e.g., a simplex or black-and-white printer).
This attribute is informative, NOT a service guarantee.
Typically, it is the value used in marketing literature to describe this printer.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

( 1.3.18.0.2.4.1126 NAME 'printer-pages-per-minute-color'
DESC 'The nominal number of color pages per minute which may be output by this
printer (e.g., a simplex or color printer).
This attribute is informative, NOT a service guarantee.
Typically, it is the value used in marketing literature to describe this printer.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

( 1.3.18.0.2.4.1125 NAME 'printer-finishings-supported'
DESC 'The possible finishing operations supported by this printer.
Legal values include; "none", "staple", "punch", "cover", "bind", "saddle-stitch",
"edge-stitch", "staple-top-left", "staple-bottom-left", "staple-top-right",
"staple-bottom-right", "edge-stitch-left", "edge-stitch-top", "edge-stitch-right",
"edge-stitch-bottom", "staple-dual-left", "staple-dual-top", "staple-dual-right",
"staple-dual-bottom".'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1124 NAME 'printer-number-up-supported'
DESC 'The possible numbers of print-stream pages to impose upon a single side of
an instance of a selected medium. Legal values include; 1, 2, and 4.
Implementations may support other values.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 )

( 1.3.18.0.2.4.1123 NAME 'printer-sides-supported'
DESC 'The number of impression sides (one or two) and the two-sided impression
rotations supported by this printer.
Legal values include; "one-sided", "two-sided-long-edge", "two-sided-short-edge".'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1122 NAME 'printer-media-supported'
DESC 'The standard names/types/sizes (and optional color suffixes) of the media
supported by this printer.
For example: "iso-a4", "envelope", or "na-letter-white".
Legal values conform to ISO 10175, Document Printing Application (DPA), and any
IANA registered extensions.'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1117 NAME 'printer-media-local-supported'
```

```

DESC 'Site-specific names of media supported by this printer, in the language in
"printer-natural-language-configured".
For example: "purchasing-form" (site-specific name) as opposed to
(in "printer-media-supported"): "na-letter" (standard keyword from ISO 10175).'
EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1121 NAME 'printer-resolution-supported'
DESC 'List of resolutions supported for printing documents by this printer.
Each resolution value is a string with 3 fields:
1) Cross feed direction resolution (positive integer), 2) Feed direction
resolution (positive integer), 3) Resolution unit.
Legal values are "dpi" (dots per inch) and "dpcm" (dots per centimeter).
Each resolution field is delimited by ">". For example: "300> 300> dpi>.'"
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1120 NAME 'printer-print-quality-supported'
DESC 'List of print qualities supported for printing documents on this printer.
For example: "draft, normal". Legal values include; "unknown", "draft", "normal",
"high".'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1110 NAME 'printer-job-priority-supported'
DESC 'Indicates the number of job priority levels supported.
An IPP conformant printer which supports job priority must always support a
full range of priorities from "1" to "100"
(to ensure consistent behavior), therefore this attribute describes the
"granularity".
Legal values of this attribute are from "1" to "100".'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

( 1.3.18.0.2.4.1118
NAME 'printer-copies-supported'
DESC 'The maximum number of copies of a document that may be printed as a single job.
A value of "0" indicates no maximum limit.
A value of "-1" indicates unknown.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

( 1.3.18.0.2.4.1111
NAME 'printer-job-k-octets-supported'
DESC 'The maximum size in kilobytes (1,024 octets actually) incoming print job that
this printer will accept.
A value of "0" indicates no maximum limit. A value of "-1" indicates unknown.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

( 1.3.18.0.2.4.1113
NAME 'printer-service-person'

```

```
DESC 'The name of the current human service person responsible for servicing this
printer.
It is suggested that this string include information that would enable other humans
to reach the service person, such as a phone number.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127}
SINGLE-VALUE )

( 1.3.18.0.2.4.1114
NAME 'printer-delivery-orientation-supported'
DESC 'The possible delivery orientations of pages as they are printed and ejected
from this printer.
Legal values include; "unknown", "face-up", and "face-down".'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1115
NAME 'printer-stacking-order-supported'
DESC 'The possible stacking order of pages as they are printed and ejected from
this printer.
Legal values include; "unknown", "first-to-last", "last-to-first".'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1116
NAME 'printer-output-features-supported'
DESC 'The possible output features supported by this printer.
Legal values include; "unknown", "bursting", "decollating", "page-collating",
"offset-stacking".'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1108
NAME 'printer-aliases'
DESC 'Site-specific administrative names of this printer in addition the printer
name specified for printer-name.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.6.1.4.1.42.2.27.5.1.63
NAME 'sun-printer-bsdaddr'
DESC 'Sets the server, print queue destination name and whether the client generates
protocol extensions.
"Solaris" specifies a Solaris print server extension. The value is represented b the
following value: server ", destination ", Solaris'.'
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.64
NAME 'sun-printer-kvp'
DESC 'This attribute contains a set of key value pairs which may have meaning to the
print subsystem or may be user defined.
Each value is represented by the following: key "=" value.'
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

Internet Print Protocol ObjectClass

```
objectclasses: ( 1.3.18.0.2.6.2549
NAME 'slpService'
DESC 'DUMMY definition'
SUP 'top' MUST (objectclass) MAY ( )
```

```
objectclasses: ( 1.3.18.0.2.6.254
NAME 'slpServicePrinter'
DESC 'Service Location Protocol (SLP) information.'
AUXILIARY SUP 'slpService')
```

```
objectclasses: ( 1.3.18.0.2.6.258
NAME 'printerAbstract'
DESC 'Printer related information.'
ABSTRACT SUP 'top' MAY ( printer-name
$ printer-natural-language-configured
$ printer-location
$ printer-info
$ printer-more-info
$ printer-make-and-model
$ printer-multiple-document-jobs-supported
$ printer-charset-configured
$ printer-charset-supported
$ printer-generated-natural-language-supported
$ printer-document-format-supported
$ printer-color-supported
$ printer-compression-supported
$ printer-pages-per-minute
$ printer-pages-per-minute-color
$ printer-finishings-supported
$ printer-number-up-supported
$ printer-sides-supported
$ printer-media-supported
$ printer-media-local-supported
$ printer-resolution-supported
$ printer-print-quality-supported
$ printer-job-priority-supported
$ printer-copies-supported
$ printer-job-k-octets-supported
$ printer-current-operator
$ printer-service-person
$ printer-delivery-orientation-supported
$ printer-stacking-order-supported $ printer! -output-features-supported )
```

```
objectclasses: ( 1.3.18.0.2.6.255
NAME 'printerService'
DESC 'Printer information.'
STRUCTURAL SUP 'printerAbstract' MAY ( printer-uri
$ printer-xri-supported )
```

```
objectclasses: ( 1.3.18.0.2.6.257
NAME 'printerServiceAuxClass'
DESC 'Printer information.'
```

```
AUXILIARY SUP 'printerAbstract' MAY ( printer-uri $ printer-xri-supported )
```

```
objectclasses: ( 1.3.18.0.2.6.256  
NAME 'printerIPP'  
DESC 'Internet Printing Protocol (IPP) information.'  
AUXILIARY SUP 'top' MAY ( printer-ipp-versions-supported $  
printer-multiple-document-jobs-supported ) )
```

```
objectclasses: ( 1.3.18.0.2.6.253  
NAME 'printerLPR'  
DESC 'LPR information.'  
AUXILIARY SUP 'top' MUST ( printer-name ) MAY ( printer-aliases) )
```

```
objectclasses: ( 1.3.6.1.4.1.42.2.27.5.2.14  
NAME 'sunPrinter'  
DESC 'Sun printer information'  
SUP 'top' AUXILIARY MUST (objectclass $ printer-name) MAY  
(sun-printer-bsdaddr $ sun-printer-kvp))
```

プリンタ属性

```
ATTRIBUTE ( 1.3.6.1.4.1.42.2.27.5.1.63  
NAME sun-printer-bsdaddr  
DESC 'Sets the server, print queue destination name and whether the  
client generates protocol extensions. "Solaris" specifies a  
Solaris print server extension. The value is represented by  
the following value: server "," destination ", Solaris".'  
EQUALITY caseIgnoreIA5Match  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15  
SINGLE-VALUE  
)
```

```
ATTRIBUTE ( 1.3.6.1.4.1.42.2.27.5.1.64  
NAME sun-printer-kvp  
DESC 'This attribute contains a set of key value pairs which may have  
meaning to the print subsystem or may be user defined. Each  
value is represented by the following: key "=" value.'  
EQUALITY caseIgnoreIA5Match  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Sun プリンタ objectClass

```
OBJECTCLASS ( 1.3.6.1.4.1.42.2.27.5.2.14  
NAME sunPrinter  
DESC 'Sun printer information'  
SUP top  
AUXILIARY  
MUST ( printer-name )  
MAY ( sun-printer-bsdaddr $ sun-printer-kvp ) )
```

LDAP 用の汎用ディレクトリサーバーの要件

LDAP クライアントをサポートするには、すべてのサーバーが LDAP v3 プロトコルと複合ネーミングおよび補助オブジェクトクラスをサポートしている必要があります。また、次の制御を 1 つ以上サポートする必要があります:

- 単純ページモード (RFC 2696)
- 仮想リスト表示制御

サーバーは、次の認証方式を 1 つ以上サポートする必要があります。

```
anonymous
simple
sasl/cram-MD5
sasl/digest-MD5
sasl/GSSAPI
```

LDAP クライアントが `pam_unix *` モジュールを使用している場合、サーバーは UNIX crypt 形式でのパスワードの格納をサポートしている必要があります。

LDAP クライアントが TLS を使用している場合、サーバーは SSL または TLS をサポートしている必要があります。

LDAP クライアントが `sasl/GSSAPI` を使用している場合、サーバーは SASL、GSSAPI、Kerberos 5 認証をサポートしている必要があります。ネットワーク上の GSS 暗号化のサポートは、オプションです。

LDAP ネームサービスで使用されるデフォルトフィルタ

SSD を使用して個々のサービスにパラメータを手動で指定しないと、デフォルトフィルタが使用されます。特定のサービスのデフォルトフィルタを表示するには、`-v` オプションを指定して `ldaplist` を実行してください。

次の例では、`filter=(amp;objectclass=iphost)(cn=abcde)` によってデフォルトフィルタが定義されます。

```
database=hosts
filter=(amp;objectclass=iphost)(cn=abcde)
user data=(amp;s) (cn=abcde))
```

ldaplist は、次に示す一連のデフォルトフィルタを生成します (%s は文字列を意味し、%d は数値を意味する)。

```
hosts
(&(objectclass=iphost)(cn=%s))
-----
passwd
(&(objectclass=posixaccount)(uid=%s))
-----
services
(&(objectclass=ipservice)(cn=%s))
-----
group
(&(objectclass=posixgroup)(cn=%s))
-----
netgroup
(&(objectclass=nisnetgroup)(cn=%s))
-----
networks
(&(objectclass=ipnetwork)(ipnetworknumber=%s))
-----
netmasks
(&(objectclass=ipnetwork)(ipnetworknumber=%s))
-----
rpc
(&(objectclass=oncrpc)(cn=%s))
-----
protocols
(&(objectclass=ipprotocol)(cn=%s))
-----
bootparams
(&(objectclass=bootableDevice)(cn=%s))
-----
ethers
(&(objectclass=ieee802Device)(cn=%s))
-----
publickey
(&(objectclass=niskeyobject)(cn=%s))
or
(&(objectclass=niskeyobject)(uidnumber=%d))
-----
aliases
(&(objectclass=mailGroup)(cn=%s))
-----
```

表 7-1 getxbyy 呼び出しで使用される LDAP フィルタ

フィルタ	定義
bootparamByName	(&(objectClass=bootableDevice)(cn=%s))
etherByHost	(&(objectClass=ieee802Device)(cn=%s))
etherByEther	(&(objectClass=ieee802Device)(macAddress=%s))

フィルタ	定義
groupByName	(&(objectClass=posixGroup)(cn=%s))
groupByGID	(&(objectClass=posixGroup)(gidNumber=%ld))
groupByMember	(&(objectClass=posixGroup)(memberUid=%s))
hostsByName	(&(objectClass=ipHost)(cn=%s))
hostsByAddr	(&(objectClass=ipHost)(ipHostNumber=%s))
keyByUID	(&(objectClass=nisKeyObject)(uidNumber=%s))
keyByHost	(&(objectClass=nisKeyObject)(cn=%s))
netByName	(&(objectClass=ipNetwork)(cn=%s))
netByAddr	(&(objectClass=ipNetwork)(ipNetworkNumber=%s))
nisgroupMember	(membernisnetgroup=%s)
maskByNet	(&(objectClass=ipNetwork)(ipNetworkNumber=%s))
printerByName	(&(objectClass=sunPrinter)((printer-name=%s)(printer-aliases=%s)))
projectByName	(&(objectClass=SolarisProject)(SolarisProjectName=%s))
projectByID	(&(objectClass=SolarisProject)(SolarisProjectID=%ld))
protoByName	(&(objectClass=ipProtocol)(cn=%s))
protoByNumber	(&(objectClass=ipProtocol)(ipProtocolNumber=%d))
passwordByName	(&(objectClass=posixAccount)(uid=%s))
passwordByNumber	(&(objectClass=posixAccount)(uidNumber=%ld))
rpcByName	(&(objectClass=oncRpc)(cn=%s))
rpcByNumber	(&(objectClass=oncRpc)(oncRpcNumber=%d))
serverByName	(&(objectClass=ipService)(cn=%s))
serverByPort	(&(objectClass=ipService)(ipServicePort=%ld))
serverByNameAndProto	(&(objectClass=ipService)(cn=%s)(ipServiceProtocol=%s))
specialByNameserver	(ipServiceProtocol=%s)
ByPortAndProto	(&(objectClass=shadowAccount)(uid=%s))
netgroupByTriple	(&(objectClass=nisNetGroup)(cn=%s))
netgroupByMember	(&(objectClass=nisNetGroup)(cn=%s))
authName	(&(objectClass=SolarisAuthAttr)(cn=%s))
auditUserByName	(&(objectClass=SolarisAuditUser)(uid=%s))
execByName	(&(objectClass=SolarisExecAttr)(cn=%s)(SolarisKernelSecurityPolicy=%s)(SolarisProfileType=%s))

フィルタ	定義
execByPolicy	(&(objectClass=SolarisExecAttr)(SolarisProfileId=%s) (SolarisKernel SecurityPolicy=%s)(SolarisProfileType=%s))
profileByName	(&(objectClass=SolarisProfAttr)(cn=%s))
userByName	(&(objectClass=SolarisUserAttr)(uid=%s))

次の表に getent 属性フィルタの一覧を示します。

表 7-2 getent 属性フィルタ

フィルタ	定義
aliases	(objectClass=rfc822MailGroup)
auth_attr	(objectClass=SolarisAuthAttr)
audit_user	(objectClass=SolarisAuditUser)
exec_attr	(objectClass=SolarisExecAttr)
group	(objectClass=posixGroup)
hosts	(objectClass=ipHost)
networks	(objectClass=ipNetwork)
prof_attr	(objectClass=SolarisProfAttr)
protocols	(objectClass=ipProtocol)
passwd	(objectClass=posixAccount)
printers	(objectClass=sunPrinter)
rpc	(objectClass=oncRpc)
services	(objectClass=ipService)
shadow	(objectClass=shadowAccount)
project	(objectClass=SolarisProject)
usr_attr	(objectClass=SolarisUserAttr)

◆◆◆ 第 8 章

NIS+ から LDAP への移行

この章では、LDAP ディレクトリに格納されたネーム情報を使用する NIS クライアントの、サポートを有効にする方法について説明します。この章の手順に従うことで、NIS ネームサービスから LDAP ネームサービスへ移行できます。

LDAP への移行の利点を判定する場合は、[10 ページの「LDAP ネームサービスの概要」](#)を参照してください。

この章で扱う内容は、次のとおりです。

- [113 ページの「NIS から LDAP への移行サービスの概要」](#)
- [119 ページの「NIS から LDAP への移行 \(タスクマップ\)」](#)
- [120 ページの「NIS から LDAP への移行のための前提条件」](#)
- [121 ページの「NIS から LDAP への移行サービスの設定」](#)
- [129 ページの「Oracle Directory Server Enterprise Edition での NIS から LDAP への移行のベストプラクティス」](#)
- [132 ページの「NIS から LDAP への移行に関する制限」](#)
- [132 ページの「NIS から LDAP への移行のトラブルシューティング」](#)
- [138 ページの「NIS に戻す方法」](#)

NIS から LDAP への移行サービスの概要

NIS から LDAP への移行サービス (*N2L サービス*) は、NIS マスターサーバー上の既存の NIS デーモンを NIS から LDAP への移行用デーモンに置き換えます。また、N2L サービスでは、そのサーバー上に NIS から LDAP へのマッピングファイルも作成されます。マッピングファイルでは、NIS マップエントリと、LDAP での同等なディレクトリ情報ツリー (DIT) との間のマッピングを指定します。この移行を完了した NIS マスターサーバーは、「N2L サーバー」と呼ばれま

す。スレーブサーバーには、NISLDAPmapping ファイルはありません。したがって、引き続きそのまま動作します。スレーブサーバーのデータは、N2L サーバーから、通常の NIS マスターからと同様に、定期的に更新されます。

N2L サービスの動作は、ypserv および NISLDAPmapping 構成ファイルによって制御されます。スクリプト inityp2l は、これらの構成ファイルの作成を支援します。いったん N2L サーバーが確立されたあとは、構成ファイルを直接編集して N2L を管理できます。

N2L サービスは、次の操作をサポートします。

- LDAP ディレクトリ情報ツリー (DIT) 内に NIS マップをインポートする
- NIS の速度および拡張性を維持しつつ、クライアントから DIT 情報にアクセスする

あらゆるネームシステムで、1 つのソースの情報だけが正規のソースになります。従来の NIS では、正規の情報は NIS ソースです。N2L サービスを使用する場合、LDAP ディレクトリが正規のデータソースになります。このディレクトリは、[第1章「LDAP ネームサービスの概要」](#)で説明されているディレクトリ管理ツールを使用して管理されます。

NIS ソースは、緊急時のバックアップまたはバックアウト (LDAP に移行するのではなく、NIS の使用をやめる) にのみ使用します。N2L サービスを使用したあとは、NIS クライアントを段階的に廃止する必要があります。最終的には、すべての NIS クライアントを LDAP ネームサービスクライアントで置き換えるようにしてください。

以降のセクションでは、さらに概要情報を説明します。

- [115 ページの「NIS から LDAP への移行の対象読者」](#)
- [115 ページの「NIS から LDAP への移行サービスを使用しない場合」](#)
- [116 ページの「NIS から LDAP への移行サービスがユーザーに与える影響」](#)
- [117 ページの「NIS から LDAP への移行に関する用語」](#)
- [117 ページの「NIS から LDAP への移行コマンド、ファイル、およびマップ」](#)
- [118 ページの「サポートされる標準マッピング」](#)

NIS から LDAP への移行用ツールとサービス管理機能

NIS と LDAP のサービスはサービス管理機能によって管理されます。svcadm コマンドを使用すると、これらのサービスに対する管理アクション (有効化、無効化、再起動など) を実行でき

ます。svcs コマンドを使用してサービスのステータスを照会できます。LDAP および NIS での SMF の使用の詳細は、68 ページの「LDAP とサービス管理機能」および『Oracle Solaris 11.2 ディレクトリサービスとネームサービスでの作業: DNS と NIS』の「NIS とサービス管理機能」を参照してください。SMF については、『Oracle Solaris 11.2 でのシステムサービスの管理』を参照してください。また、詳細については `svcadm(1M)` および `svcs(1)` のマニュアルページも参照してください。

NIS から LDAP への移行の対象読者

この章の手順を実行するには、NIS および LDAP の概念、用語、および ID を理解する必要があります。NIS および LDAP のネームサービスについての詳細は、次のセクションを参照してください。

- NIS の概要については、『Oracle Solaris 11.2 ディレクトリサービスとネームサービスでの作業: DNS と NIS』の第 5 章「ネットワーク情報サービスについて」
- LDAP の概要については、第 1 章「LDAP ネームサービスの概要」

NIS から LDAP への移行サービスを使用しない場合

N2L サービスの目的は、NIS の使用から LDAP の使用への移行ツールとして機能することにあります。次の状況では、N2L サービスを使用しないでください。

- NIS と LDAP ネームサービスクライアント間でデータを共有する予定がない環境
このような環境では、N2L サーバーは、過度に複雑な NIS マスターサーバーとして機能しません。
- NIS ソースファイルを変更するツール (`yppasswd` 以外のツール) で NIS マップを管理している環境。
DIT マップから NIS ソースを再生成するタスクは、必ずしも正確ではないため、生成されたマップを手動で確認する必要があります。いったん N2L サービスを使用し始めたあとは、NIS ソースの再生成は NIS をバックアウトするため、または NIS に戻すためにだけ提供されます。
- NIS クライアントのない環境。
このような環境では、LDAP ネームサービスクライアントとそれに対応するツールを使用してください。

NIS から LDAP への移行サービスがユーザーに与える影響

N2L サービスに関連したファイルを単純にインストールしても、NIS サーバーのデフォルトの動作は変更されません。インストール時に、サーバー上の NIS のマニュアルページの一部が変更され、N2L のヘルパースクリプト `inityp2l` および `yppmap2src` が追加されます。ただし、NIS サーバー上で `inityp2l` を実行したり、N2L 構成ファイルを手動で作成したりしないと、NIS コンポーネントは従来の NIS モードで起動し、通常どおりに機能します。

`inityp2l` の実行後に、サーバーとクライアントの動作が少し変更されます。次の表に、NIS および LDAP のユーザータイプと、N2L サービスの配備後に各タイプのユーザーが注意しなければならない部分の説明を示します。

ユーザータイプ	N2L サービスの影響
NIS マスターサーバー管理者	NIS マスターサーバーは、N2L サーバーに変換される。 <code>NISLDAPmapping</code> および <code>ypserv</code> 構成ファイルが、N2L サーバーにインストールされます。N2L サーバーの確立後は、LDAP コマンドを使用してネーム情報を管理できる
NIS スレーブサーバー管理者	N2L の変換後も、NIS スレーブサーバーは NIS を通常の方法で動作する。 <code>yppmake</code> によって <code>yppush</code> が呼び出されると、N2L サーバーは、更新された NIS マップをスレーブサーバーに転送する。 yppmake(1M) のマニュアルページを参照してください。
NIS クライアント	NIS の読み取り動作は、従来の NIS と同様。LDAP ネームサービスクライアントが DIT 内の情報を変更すると、その情報が NIS マップにコピーされます。コピー操作は、構成可能なタイムアウトの期限が切れると完了する。このような動作は、クライアントが NIS スレーブサーバーに接続された場合の通常の NIS クライアントの動作と同じです。 N2L サーバーが読み取りのために LDAP サーバーにバインドできない場合、N2L サーバーはローカルにキャッシュされたコピーから情報を返す。また、N2L サーバーは内部サーバーエラーを返す場合もある。N2L サーバーの構成によって、どちらの方法で応答することも可能。詳細は、 ypserv(1M) のマニュアルページを参照してください。
すべてのユーザー	NIS クライアントがパスワードの変更を要求すると、N2L マスターサーバーとネイティブの LDAP クライアントに変更がただちに反映される NIS クライアントでのパスワードの変更を試みて、LDAP サーバーが利用できない場合は、変更は拒絶され N2L サーバーは内部サーバーエラーを返す。この動作によって、キャッシュに誤った情報が書き込まれることを防止する

NIS から LDAP への移行に関する用語

N2L サービスの実装に関連する用語を次に示します。

表 8-1 N2L の移行の関連用語

用語	説明
N2L 構成ファイル	<code>/var/yp/NISLDAPmapping</code> および <code>/var/yp/ypserv</code> ファイル。 <code>ypserv</code> デーモンが N2L モードでマスターサーバーを起動するために使用する。詳細は、 <code>NISLDAPmapping(4)</code> および <code>ypserv(4)</code> のマニュアルページを参照
マップ	N2L サービスでは、「マップ」は、次の 2 とおりの意味で使用される。 <ul style="list-style-type: none"> ■ NIS が特定の種類の情報を格納するデータベースファイル ■ LDAP DIT との間の NIS 情報のマッピングプロセス
マッピング	LDAP DIT エントリとの間の NIS エントリの変換プロセス
マッピングファイル	<code>NISLDAPmapping</code> ファイル。NIS と LDAP のファイル間のエントリのマッピング方法を確立する
標準マップ	通常使用される NIS マップ。マッピングファイルへの手動修正が不要で、N2L サービスによってサポートされる。サポートされる標準マップのリストは、 118 ページの「サポートされる標準マッピング」 を参照
非標準マップ	標準の NIS マップであるが、RFC 2307 やその後継で指定されたマッピング以外の、NIS と LDAP DIT 間のマッピングを使用するようにカスタマイズされたマップ
カスタムマップ	標準のマップではないマップ。したがって、NIS から LDAP への移行時にはマッピングファイルの手動修正が必要
LDAP クライアント	従来の LDAP クライアント。LDAP サーバーとの間で読み書きを行う。従来の LDAP クライアントは、任意の LDAP サーバーに対して読み取りおよび書き込みを行うシステム。LDAP ネームサービスクライアントは、ネーミング情報のカスタマイズされたサブセットを処理します。
LDAP ネームサービスクライアント	ネーミング情報のカスタマイズされたサブセットを処理する LDAP クライアント。
N2L サーバー	N2L サービスを使用して、N2L サーバーとして再構成された NIS マスターサーバー。再構成には、NIS デーモンの置き換えと新しい構成ファイルの追加が含まれる。

NIS から LDAP への移行コマンド、ファイル、およびマップ

2 つのユーティリティ、2 つの構成ファイル、および 1 つのマッピングが N2L の移行に関連付けられています。

表 8-2 N2L のコマンド、ファイル、およびマップの説明

コマンド/ファイル/マップ	説明
/usr/lib/netsvc/yp/ inityp2l	NISLDAPmapping および ypserv 構成ファイルの作成を支援するユーティリティ。このユーティリティは、これらのファイルを管理するための汎用ツールではない。熟練したユーザーであれば、inityp2l の出力をテキストエディタを使って検証したりカスタマイズしたりすることで、N2L 構成ファイルの管理や、カスタムマッピングの作成を行うことも可能。 inityp2l(1M) のマニュアルページを参照してください。
/usr/lib/netsvc/yp/ ypmap2src	標準の NIS マップをほぼ同等の NIS ソースファイルに変換するユーティリティ。ypmap2src の主要な用途は、N2L の移行サーバーから従来の NIS への変換。 ypmap2src(1M) のマニュアルページを参照してください。
/var/yp/NISLDAPmapping	NIS マップエントリと、LDAP 内の同等のディレクトリ情報ツリー (DIT) エントリ間のマッピングを指定する構成ファイル。 NISLDAPmapping(4) のマニュアルページを参照してください。
/var/yp/ypserv	NIS から LDAP への移行用デーモンの構成情報を指定するファイル。 ypserv(4) のマニュアルページを参照してください。
ageing.byname	NIS から LDAP への移行の実行時に、DIT でのパスワード有効期限情報の読み取りおよび書き込みのために yppasswdd によって使用されるマッピング

サポートされる標準マッピング

デフォルトでは、N2L サービスで下記のマップリストと、RFC 2307、RFC 2307bis、およびその後継の LDAP エントリとのマッピングがサポートされています。これらの標準マップでは、マッピングファイルへの手動修正は不要です。システム上でリストにないマップは、カスタムマップと見なされ、マッピングファイルの手動修正が必要です。

また、N2L サービスは、`auto.*` マップの自動マッピングもサポートします。ただし、ほとんどの `auto.*` ファイル名とそのコンテンツは、各ネットワーク構成に固有なので、このリストではこれらのファイルは指定していません。例外として、標準マップとしてサポートされる `auto.home` および `auto.master` マップがあります。

標準マップは次のとおりです。

```
audit_user
auth_attr
auto.home
auto.master
bootparams
ethers.byaddr ethers.byname
exec_attr
```

```

group.bygid group.byname group.adjunct.byname
hosts.byaddr hosts.byname
ipnodes.byaddr ipnodes.byname
mail.byaddr mail.aliases
netgroup netgroup.byprojid netgroup.byuser netgroup.byhost
netid.byname
netmasks.byaddr
networks.byaddr networks.byname
passwd.byname passwd.byuid passwd.adjunct.byname
prof_attr
project.byname project.byprojectid
protocols.byname protocols.bynumber
publickey.byname
rpc.bynumber
services.byname services.byservicename
timezone.byname
user_attr

```

NIS から LDAP への移行時に、`yppasswdd` デーモンは、N2L 固有のマッピング `ageing.byname` を使用して、DIT でのパスワード有効期限情報の読み取りと書き込みを行います。パスワード有効期限を使用していない場合は、`ageing.byname` マッピングは無視されます。

NIS から LDAP への移行 (タスクマップ)

次の表に、NIS から LDAP への標準およびカスタムのマッピングで N2L サービスをインストールして管理するために必要な手順を示します。

タスク	説明	手順
すべての前提条件を完了する。	NIS サーバーおよび Oracle Directory Server Enterprise Edition (LDAP サーバー) が適切に構成されていることを確認する。	120 ページの「NIS から LDAP への移行のための前提条件」
N2L サービスの設定	NIS マスターサーバーで、 <code>inityp2l</code> を実行して、次のいずれかのマッピングを設定する 標準マッピング カスタムまたは非標準マッピング	122 ページの「標準マッピングを使用して N2L サービスを設定する方法」 124 ページの「カスタムマッピングまたは非標準マッピングを使用して N2L サービスを設定する方法」
マップをカスタマイズする。	N2L の移行のためのカスタムマップの作成方法の例を参照する	127 ページの「カスタムマップの例」

タスク	説明	手順
Oracle Directory Server Enterprise Edition に N2L を構成する。	N2L 移行のために Oracle Directory Server Enterprise Edition を LDAP サーバーとして構成する。	129 ページの「Oracle Directory Server Enterprise Edition での NIS から LDAP への移行のベストプラクティス」
システムをトラブルシューティングする。	一般的な N2L の問題を特定し解決する	132 ページの「NIS から LDAP への移行のトラブルシューティング」
NIS に戻す。	次のいずれか適切なマップを使用して NIS に戻す 以前の NIS ソースファイルに基づくマップ 現在の DIT に基づくマップ	138 ページの「以前のソースファイルに基づくマップに戻す方法」 139 ページの「現在の DIT 内容に基づくマップに戻す方法」

NIS から LDAP への移行のための前提条件

N2L サービスを実装する前に、次の項目を確認または完了する必要があります。

- `inityp2l` スクリプトを実行して N2L モードを有効にする前に、システムが従来の NIS サーバーで動作するように設定されていること
- システムで LDAP ディレクトリサーバーを構成していること

NIS から LDAP への移行ツールは、Oracle Directory Server Enterprise Edition および Oracle で提供される互換性のあるバージョンのディレクトリサーバーに対応しています。Oracle Directory Server Enterprise Edition を使用している場合は、N2L サービスを設定する前に、`idsconfig` コマンドを使用してサーバーを構成します。`idsconfig` についての詳細は、[第4章「Oracle Directory Server Enterprise Edition への LDAP クライアントの設定」](#)および `idsconfig(1M)` のマニュアルページを参照してください。

その他のサードパーティー製 LDAP サーバーも N2L サービスで動作する可能性がありますが、Oracle ではサポートされません。Oracle Directory Server Enterprise Edition または互換性のある Oracle サーバー以外の LDAP サーバーを使用している場合は、N2L サービスを設定する前に、RFC 2307bis、RFC 4876、またはその後継のスキーマをサポートするようにサーバーを手動で構成する必要があります。

- `config/host` プロパティでは、`dns` の前に `files` を使用します。
- N2L マスターサーバーと LDAP サーバーのアドレスが N2L マスターサーバー上の `hosts` ファイル内に存在することを確認してください。

代わりに、`ypserv` 内にホスト名ではなく、LDAP サーバーアドレスをリストする方法もあります。LDAP サーバーのアドレスが別の場所にもリストされているため、LDAP サーバーと N2L マスターサーバーのどちらかのアドレスを変更するには、別のファイルの修正も必要です。

NIS から LDAP への移行サービスの設定

このセクションの手順に示すように、標準のマッピングとカスタムマッピングのどちらかを使用すると、N2L サービスを設定できます。

NIS から LDAP への変換の一部として、`inityp2l` コマンドを実行する必要があります。このコマンドは、対話型で、構成情報を入力するスクリプトを実行します。入力する必要がある情報のタイプについては、[ypserv\(1M\)](#) のマニュアルページを参照してください。

- 作成する構成ファイルの名前 (デフォルト = `/etc/default/ypserv`)
- LDAP の構成情報を格納する DN (デフォルト = `ypserv`)
- LDAP との間でデータをマッピングするための優先サーバーリスト
- LDAP との間でデータをマッピングするための認証方式
- LDAP との間でデータをマッピングするための TLS (Transport Layer Security)
- LDAP との間でデータを読み書きするためのプロキシのユーザーバインド DN
- LDAP との間でデータを読み書きするためのプロキシのユーザーパスワード
- LDAP バインド動作のタイムアウト値 (秒単位)
- LDAP 検索動作のタイムアウト値 (秒単位)
- LDAP 変更動作のタイムアウト値 (秒単位)
- LDAP 追加動作のタイムアウト値 (秒単位)
- LDAP 削除動作のタイムアウト値 (秒単位)
- LDAP サーバーでの検索動作の制限時間 (秒単位)
- LDAP サーバーでの検索動作の制限サイズ (バイト単位)
- N2L が LDAP 照会に従うかどうか
- LDAP 検索のエラー処理、検索試行回数、および各試行間のタイムアウト (秒単位)
- 格納のエラー処理、検索試行回数、および各試行間のタイムアウト (秒単位)
- マッピングファイル名

- auto_direct マップのマッピング情報を生成するかどうか
スクリプトは、マッピングファイル内の適切な位置にカスタムマップについての情報を配置します。
- ネーミングコンテキスト
- パスワードの変更を有効にするかどうか
- 任意のマップのデフォルトの TTL 値を変更するかどうか

注記 - sasl/cram-md5 認証は、Oracle Directory Server Enterprise Edition を含むほとんどの LDAP サーバーではサポートされません。

▼ 標準マッピングを使用して N2L サービスを設定する方法

118 ページの「[サポートされる標準マッピング](#)」にリストされているマップを移行する場合は、この手順に従います。カスタムマップまたは非標準マップを使用している場合は、124 ページの「[カスタムマッピングまたは非標準マッピングを使用して N2L サービスを設定する方法](#)」を参照してください。

LDAP サーバーの設定が終わったら、inityp2l スクリプトを実行して、プロンプトに従って構成情報を入力します。inityp2l は構成を行い、標準および auto.* マップのためのマッピングファイルを設定します。

1. [120 ページの「NIS から LDAP への移行のための前提条件」](#)にリストされた前提条件の手順を完了します。
2. NIS マスターサーバー上の管理者になります。
詳細は、『Oracle Solaris 11.2 でのユーザーとプロセスのセキュリティー保護』の「[割り当てられている管理権利の使用](#)」を参照してください。

3. NIS マスターサーバーを N2L サーバーに変換します。

inityp2l

NIS マスターサーバーで inityp2l スクリプトを実行して、プロンプトに従います。指定が必要な情報のリストは、121 ページの「[NIS から LDAP への移行サービスの設定](#)」を参照してください。

詳細は、[inityp2l\(1M\)](#) のマニュアルページを参照してください。

4. LDAP ディレクトリ情報ツリー (DIT) が完全に初期化されているかどうかを判定します。

NISLDAPmapping ファイルにリストされたすべてのマップの配備に必要な情報がすでに DIT 内に存在する場合、DIT は完全に初期化されています。

DIT が完全に初期化されている場合は、手順 5 をスキップして、[ステップ 6](#) に進んでください。

5. NIS ソースファイルから移行するため、DIT を初期化します。

この手順は、DIT が完全に初期化されていない場合にのみ実行します。

a. 以前の NIS マップが最新の状態になっていることを確認してください。

```
# cd /var/yp
# make
```

詳細は、[ypmake\(1M\)](#) のマニュアルページを参照してください。

b. NIS サービスを停止します。

```
# svcadm disable network/nis/server:default
```

c. 以前のマップを DIT にコピーしてから、マップ用の N2L サポートを初期化します。

```
# ypserv -IR
```

ypserv が終了するまで待ちます。

ヒント - 元の NIS dbm ファイルは上書きされません。必要に応じて、これらのファイルを回復できます。

d. DNS および NIS サービスを起動して、これらのサービスが新しいマップを使用していることを確認します。

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

これで、N2L サービスが標準マップを使用して設定されました。手順 6 を行う必要はありません。

6. NIS マップを初期化します。

DIT が完全に初期化され、手順 5 をスキップした場合に限って、次の手順を実行してください。

- a. NIS サービスを停止します。

```
# svcadm disable network/nis/server:default
```

- b. DIT 内の情報に従って NIS マップを初期化します。

```
# ypserv -r
```

ypserv が終了するまで待ちます。

ヒント - 元の NIS dbm ファイルは上書きされません。必要に応じて、これらのファイルを回復できます。

- c. DNS および NIS サービスを起動して、これらのサービスが新しいマップを使用していることを確認します。

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

▼ カスタムマッピングまたは非標準マッピングを使用して N2L サービスを設定する方法

次の状況に適合する場合、この手順を実行してください。

- [118 ページの「サポートされる標準マッピング」](#)にリストされていないマップがある
- RFC 2307 とは異なるマッピングで LDAP にマップしたい標準の NIS マップがある

1. [120 ページの「NIS から LDAP への移行のための前提条件」](#)にリストされた前提条件の手順を完了します。

2. NIS マスターサーバー上の管理者になります。

詳細は、『[Oracle Solaris 11.2 でのユーザーとプロセスのセキュリティ保護](#)』の「[割り当てられている管理権利の使用](#)」を参照してください。

役割には、認証と特権コマンドが含まれます。役割の詳細については、『[Oracle Solaris 11.2 でのユーザーとプロセスのセキュリティ保護](#)』の第 3 章「[Oracle Solaris での権利の割り当て](#)」を参照してください。

3. NIS マスターサーバーを N2L サーバーに構成します。

```
# inityp2l
```

NIS マスターサーバーで `inityp2l` スクリプトを実行して、プロンプトに従います。指定が必要な情報のリストは、[121 ページの「NIS から LDAP への移行サービスの設定」](#)を参照してください。

詳細は、[inityp2l\(1M\)](#) のマニュアルページを参照してください。

4. `/var/yp/NISLDAPmapping` ファイルを修正します。

マッピングファイルの修正方法の例は、[127 ページの「カスタムマップの例」](#)を参照してください。

5. LDAP ディレクトリ情報ツリー (DIT) が完全に初期化されているかどうかを判定します。

`NISLDAPmapping` ファイルにリストされたすべてのマップの配備に必要な情報がすでに DIT 内に存在する場合、DIT は完全に初期化されています。

■ DIT が完全に初期化されている場合は、手順 6 をスキップします。

6. NIS ソースファイルから移行するため、DIT を初期化します。

a. 以前の NIS マップが最新の状態になっていることを確認してください。

```
# cd /var/yp
# make
```

詳細は、[ypmake\(1M\)](#) のマニュアルページを参照してください。

b. NIS デーモンを停止します。

```
# svcadm disable network/nis/server:default
```

c. 以前のマップを DIT にコピーしてから、マップ用の N2L サポートを初期化します。

```
# ypserv -Ir
```

`ypserv` が終了するまで待ちます。

ヒント - 元の NIS `dbm` ファイルは上書きされません。必要に応じて、これらのファイルを回復できます。

d. DNS および NIS サービスを起動して、これらのサービスが新しいマップを使用していることを確認します。

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

e. 手順 7 をスキップして、[ステップ 8](#) から続行します。

7. NIS マップを初期化します。

DIT が完全に初期化されている場合に限って、この手順を実行します。

a. NIS デーモンを停止します。

```
# svcadm disable network/nis/server:default
```

b. DIT 内の情報に従って NIS マップを初期化します。

```
# ypserv -r
```

ypserv が終了するまで待ちます。

ヒント - 元の NIS dbm ファイルは上書きされません。必要に応じて、これらのファイルを回復できます。

c. DNS および NIS サービスを起動して、これらのサービスが新しいマップを使用していることを確認します。

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

8. LDAP エントリが正しいことを確認します。

エントリが間違っている場合、LDAP ネームサービスクライアントからはそのエントリを見つけられません。

```
# ldapsearch -h server -s sub -b "ou=servdates, dc=..." \ "objectclass=servDates"
```

9. LDAP マップの内容を確認します。

次の出力例は、makedm コマンドを使用して hosts.byaddr マップの内容を確認する方法を示しています。

```
# makedbm -u LDAP_servdate.bynumber
plato: 1/3/2001
johnson: 2/4/2003,1/3/2001
yeats: 4/4/2002
poe: 3/3/2002,3/4/2000
```

出力結果が期待どおりの内容であれば、NIS から LDAP への移行は成功です。

元の NIS dbm ファイルは上書きされないことに注意してください。したがって、いつでもこれらのファイルは回復できます。詳細については、[138 ページの「NIS に戻す方法」](#)を参照してください。

カスタムマップの例

このセクションの例では、マップをカスタマイズする方法を示します。必要に応じて、任意のテキストエディタを使用して、`/var/yp/NISLDAPmapping` ファイルを修正します。ファイル属性と構文の詳細は、[NISLDAPmapping\(4\)](#) のマニュアルページ、および [第1章「LDAP ネームサービスの概要」](#)にある LDAP ネームサービス情報を参照してください。

例 8-1 ホストエントリの移動

この例では、DIT でデフォルトの位置から別の (非標準の) 位置にホストエントリを移動する方法を示します。

NISLDAPmapping ファイル内の `nisLDAPobjectDN` 属性を新しいベース LDAP 識別名 (DN) に変更します。この例では、LDAP オブジェクトの内部構造は変更されません。したがって、`objectClass` エントリは変更されません。

変更前:

```
nisLDAPobjectDN hosts: \  
ou=hosts,?one?, \  
objectClass=device, \  
objectClass=ipHost
```

変更後:

```
nisLDAPobjectDN hosts: \  
ou=newHosts,?one?, \  
objectClass=device, \  
objectClass=ipHost
```

この変更によって、エントリは次のようにマッピングされます。

```
dn: ou=newHosts, dom=domain1, dc=sun, dc=com
```

元は、次のようでした。

```
dn: ou=hosts, dom=domain1, dc=sun, dc=com.
```

例 8-2 カスタムマップの実装

この例では、カスタムマップの実装方法を示します。

仮想のマップ「servdate.bynumber」には、システムのサービス日付についての情報が含まれます。このマップには、マシンのシリアル番号でインデックスが付けられます。この例では、123 です。各エントリは、マシンの所有者名、コロン、およびサービス日付のコンマ区切りのリストで構成されます。たとえば、John Smith:1/3/2001,4/5/2003 のようになります。

古いマップ構造は、次の形式の LDAP エントリにマップされます。

```
dn: number=123,ou=servdates,dc=... \
number: 123 \
userName: John Smith \
date: 1/3/2001 \
date: 4/5/2003 \
.
.
.
objectClass: servDates
```

NISLDAPmapping ファイルを調べると、必要なパターンに最も近いマッピングが group であることがわかります。カスタムマッピングは group マッピングを参考にできます。マップは 1 つだけなので、nisLDAPdatabaseIdMapping 属性は不要です。NISLDAPmapping に追加される属性は、次のとおりです。

```
nisLDAPentryTtl servdate.bynumber:1800:5400:3600

nisLDAPnameFields servdate.bynumber: \
("%s:%s", uname, dates)

nisLDAPobjectDN servdate.bynumber: \
ou=servdates, ?one? \
objectClass=servDates:

nisLDAPattributeFromField servdate.bynumber: \
dn=("number=%s", rf_key), \
number=rf_key, \
userName=uname, \
(date)=(dates, ",")

nisLDAPfieldFromAttribute servdate.bynumber: \
rf_key=number, \
uname=userName, \
dates=("%s", (date), ",")
```

Oracle Directory Server Enterprise Edition での NIS から LDAP への移行のベストプラクティス

N2L サービスは、Oracle Directory Server Enterprise Edition に対応しています。その他のサードパーティー製 LDAP サーバーも N2L サービスで動作する可能性があります。Oracle ではサポートされません。Oracle Directory Server Enterprise Edition サーバーまたは互換性のある Oracle サーバー以外の LDAP サーバーを使用している場合は、RFC 2307、RFC 2307bis、および RFC 4876、またはその後継のスキーマをサポートするようにサーバーを手動で構成する必要があります。

Oracle Directory Server Enterprise Edition を使用すれば、ディレクトリサーバーを強化してパフォーマンスを改善できます。これらの強化を行うには、Oracle Directory Server Enterprise Edition 上に LDAP の管理者権限が必要です。また、ディレクトリサーバーのリポートが必要な場合があります。リポートは、サーバーの LDAP クライアントとの間で調整が必要なタスクです。Oracle Directory Server Enterprise Edition のドキュメントは、[Sun Java System Directory Server Enterprise Edition 6.2](#) の Web サイトで入手できます。(お気に入りの検索エンジンを使用して、"oracle.com: sun java system directory server enterprise edition" を検索します。)

Oracle Directory Server Enterprise Edition での仮想リスト表示 (VLV) インデックスの作成

大規模なマップでは、LDAP の仮想リスト表示 (VLV) インデックスを使用して、LDAP の検索から正しい結果が得られることを保証しなければなりません。Oracle Directory Server Enterprise Edition での VLV インデックスの設定については、[Sun Java System Directory Server Enterprise Edition 6.2](#) のドキュメントを参照してください。

VLV の検索結果では、固定ページサイズ 50000 を使用します。Oracle Directory Server Enterprise Edition で VLV を使用する場合は、LDAP サーバーと N2L サーバーの両方が、このサイズの転送を処理できる必要があります。すべてのマップがこの制限より小規模であることが明らかな場合は、VLV インデックスを使用する必要はありません。ただし、マップがこのサイズ制限より大きい場合、またはすべてのマップのサイズが明確な場合以外には、VLV インデックスを使用して、結果が不完全となることを防止しなければなりません。

VLV インデックスを使用している場合は、次のように適切なサイズ制限を設定します。

- Oracle Directory Server Enterprise Edition では、`nsslapd-sizelimit` 属性を 50000 以上、または -1 に設定する必要があります。[idsconfig\(1M\)](#) のマニュアルページを参照してください。
- N2L サーバーでは、`nisLDAPsearchSizelimit` 属性を 50000 以上、または 0 に設定する必要があります。詳細は、[NISLDAPmapping\(4\)](#) のマニュアルページを参照してください。

VLV インデックスが作成されたら、Oracle Directory Server Enterprise Edition サーバーで `vlvindex` オプションを付けて `dsadm` を実行して、VLV インデックスをアクティブにします。詳細は、[dsadm\(1M\)](#) のマニュアルページを参照してください。

標準マップ用 VLV

次の状況に適合する場合、Oracle Directory Server Enterprise Edition の `idsconfig` コマンドを使用して、VLV を設定してください。

- Oracle Directory Server Enterprise Edition を使用している。
- 標準マップを RFC 2307bis LDAP エントリにマップしている。

VLV はドメイン固有です。よって、`idsconfig` を実行するたびに、1 つの NIS ドメインに VLV が作成されます。そのため、NIS から LDAP への移行中、`NISLDAPmapping` ファイルに含まれている各 `nisLDAPdomainContext` 属性に対して 1 回 `idsconfig` を実行する必要があります。

カスタムマップおよび非標準マップ用 VLV

次の状況に適合する場合、マップ用の新しい Oracle Directory Server Enterprise Edition VLV を手動で作成するか、既存の VLV インデックスをコピーして変更する必要があります。

- Oracle Directory Server Enterprise Edition を使用している。
- 大規模なカスタムマップがあるか、非標準の DIT 位置にマップされる標準のマップがある場合

既存の VLV 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。

```
% ldapsearch -h hostname -s sub -b "cn=ldbm database,cn=plugins,cn=config"  
"objectclass=vlvSearch"
```

Oracle Directory Server Enterprise Edition でのサーバータイムアウトの回避

N2L サーバーがマップをリフレッシュすると、その結果、大規模な LDAP ディレクトリアクセスが行われる場合があります。Oracle Directory Server Enterprise Edition が正しく構成されていない場合、リフレッシュ動作は完了前にタイムアウトになることがあります。ディレクトリサーバーのタイムアウトを防止するには、Oracle Directory Server Enterprise Edition 属性を手動で、または `idsconfig` コマンドを実行して変更する必要があります。

たとえば、サーバーでの検索リクエストの実行にかかる最小時間を秒単位で増やすには、次の属性を修正します。

```
dn: cn=config
nsslapd-timelimit: -1
```

テストのためには、属性値として `-1` を使用できます。この値は、制限がないことを示しています。最適な制限値が決まったら、属性値を変更します。稼働サーバーに、`-1` の属性値が設定されてはなりません。制限がないと、サーバーがサービス妨害攻撃に無防備になる場合があります。

LDAP での Oracle Directory Server Enterprise Edition の構成についての詳細は、このマニュアルの [第4章「Oracle Directory Server Enterprise Edition への LDAP クライアントの設定」](#)を参照してください。

Oracle Directory Server Enterprise Edition でのバッファオーバーランの回避

バッファオーバーランを回避するには、Oracle Directory Server Enterprise Edition 属性を手動で、または `idsconfig` コマンドを実行することで変更する必要があります。

- たとえば、クライアント検索照会に返されるエントリの最大数を増やすには、次の属性を修正します。

```
dn: cn=config
nsslapd-sizelimit: -1
```

- クライアント検索照会で確認されるエントリの最大数を増やすには、次の属性を修正します。

```
dn: cn=config, cn=ldb database, cn=plugins, cn=config
nsslapd-lookthroughlimit: -1
```

テストのためには、属性値として -1 を使用できます。この値は、制限がないことを示しています。最適な制限値が決まったら、属性値を変更します。稼働サーバーに、-1 の属性値が設定されていることはありません。制限がないと、サーバーがサービス妨害攻撃に無防備になる場合があります。

VLV が使用されている場合は、`sizelimit` 属性値を [129 ページの「Oracle Directory Server Enterprise Edition での仮想リスト表示 \(VLV\) インデックスの作成」](#) で定義されているように設定してください。VLV を使用していない場合、もっとも大きなコンテナを格納できるようにサイズ制限を設定する必要があります。

LDAP での Oracle Directory Server Enterprise Edition の構成についての詳細は、[第4章「Oracle Directory Server Enterprise Edition への LDAP クライアントの設定」](#) を参照してください。

NIS から LDAP への移行に関する制限

N2L サーバーの設定が完了すると、以降 NIS ソースファイルは使用されません。したがって、N2L サーバーで `yppmake` を実行しないでください。既存の `cron` ジョブの場合など、`yppmake` が誤って実行されても、N2L サービスは影響を受けません。ただし、`yppush` を明示的に呼び出すことを推奨する警告がログに記録されます。

NIS から LDAP への移行のトラブルシューティング

このセクションでは、トラブルシューティングの 2 つの領域を説明します。

- [133 ページの「よくある LDAP エラーメッセージ」](#)
- [134 ページの「NIS から LDAP への移行に関する問題」](#)

よくある LDAP エラーメッセージ

N2L サーバーが LDAP 内部の問題に関連するエラーをログに記録して、LDAP 関連のエラーメッセージが表示される場合があります。エラーは致命的なものではありませんが、調査すべき問題を示しています。たとえば、N2L サーバーは動作を継続していても、返される結果が古かったり、不完全になる場合があります。

このセクションでは、N2L サービスを実装するときに発生する可能性のある、よくある LDAP エラーメッセージをいくつか示します。エラーの説明、考えられる原因、およびエラーの解決も含みます。

Administrative limit exceeded

エラー番号: 11

原因: ディレクトリサーバーの `nsslapd-sizelimit` 属性で許可されているものより大きな LDAP 検索が実行されました。情報の一部だけが返されます。

対処方法: `nsslapd-sizelimit` 属性の値を増やすか、または失敗した検索のための VLV インデックスを実装します。

Invalid DN Syntax

エラー番号: 34

原因: 不正な文字を含む DN で LDAP エントリを書き込もうとする試みが行われました。N2L サーバーは、DN 内で生成される + 記号などの不正な文字のエスケープを試みます。

対処方法: LDAP サーバーのエラーログをチェックして、どの不正な DN が書き込まれたかを見つけたあと、不正な DN を生成した `NISLDAPmapping` ファイルを変更します。

Object class violation

エラー番号: 65

原因: 無効な LDAP エントリを書き込もうとする試みが行われました。一般に、このエラーは、次のいずれかの状況で起こる可能性のある `MUST` 属性の欠落のために発生します。

- 見つからない属性のエントリを作成する `NISLDAPmapping` ファイルのバグ
- 存在しないオブジェクトへの `AUXILIARY` 属性の追加の試み

たとえば、ユーザー名がまだ `passwd.byxxx` マップから作成されていない場合、そのユーザーに対する補足情報の追加の試みは失敗します。

対処方法: NISLDAPmapping ファイル内のバグの場合は、サーバーのエラーログに書き込まれた内容をチェックして問題の本質を特定します。

Can't contact LDAP server

エラー番号: 81

原因: ypserv ファイルが、間違った LDAP ディレクトリサーバーを指し示すように誤って構成されている可能性があります。または、ディレクトリサーバーが稼働していません。

対処方法: 再構成して確認します。

- ypserv ファイルを再構成して、正しい LDAP ディレクトリサーバーを指定します。
- LDAP サーバーが実行中であることを確認するには、次のように入力します。

```
% ping hostname 5 | grep "no answer" || \  
    (ldapsearch -h hostname -s base -b "" \  
    "objectclass=*" >/dev/null && echo Directory accessible)
```

サーバーが使用できない場合は、「no answer from *hostname*」というメッセージが表示されます。LDAP サーバーに問題がある場合は、「ldap_search: Can't connect to the LDAP server - Connection refused」というメッセージが表示されます。最後に、すべてが動作している場合は、「Directory accessible.」というメッセージが表示されます。

Timeout

エラー番号: 85

原因: LDAP 操作がタイムアウトしました。通常は、DIT からのマップの更新中に発生します。古い情報がマップに含まれている可能性があります。

対処方法: ypserv 構成ファイル内の nisLDAPxxxTimeout 属性の値を増やします。

NIS から LDAP への移行に関する問題

N2L サーバーの実行中に、次の問題が発生する場合があります。考えられる原因と対策を説明します。

NISLDAPmapping ファイルのデバッグ

マッピングファイル NISLDAPmapping は複雑なファイルです。多くの潜在的なエラーによって、マッピングが予期しない動作をする場合があります。次の方法を用いて、この問題を解決してください。

`ypserv -ir` (または `-Ir`) を実行するとコンソールメッセージが表示される

説明: コンソールに簡単なメッセージが表示され、サーバーが終了します (詳細な説明は `syslog` に書き込まれます)。

原因: マッピングファイルの構文が正しくない可能性があります。

対処方法: NISLDAPmapping ファイル内の構文をチェックして修正します。

起動時に NIS デーモンが終了する

説明: `ypserv` またはその他の NIS デーモンを実行すると、LDAP 関連のエラーメッセージがログに記録され、デーモンが終了します。

原因: 次のいずれかの原因が考えられます。

- LDAP サーバーと通信できない
- NIS マップまたは DIT 内のエントリが、指定されたマッピングと互換性がない
- LDAP サーバーへの読み書きの試みがエラーを返す

対処方法: LDAP サーバー上のエラーログを調べます。[133 ページの「よくある LDAP エラーメッセージ」](#)で LDAP エラーの説明を参照してください。

NIS 動作からの予期しない結果

説明: NIS 操作が予期された結果を返しません、ログにエラーは記録されていません。

原因: LDAP または NIS マップ内に正しくないエントリが存在する可能性があります。これにより、マッピングが意図したように完了しません。

対処方法: LDAP DIT および N2L バージョンの NIS マップ内のエントリをチェックして修正します。

1. LDAP DIT に正しいエントリが存在するかをチェックしてから、必要に応じてエントリを修正します。

Oracle Directory Server Enterprise Edition を使用している場合は、`dsadm startconsole` コマンドを実行して管理コンソールを起動します。

2. 新しく生成されたマップを元のマップと比較することによって、`/var/yp` ディレクトリ内の N2L バージョンの NIS マップに予期されたエントリが含まれていることを確認します。必要に応じてエントリを修正します。

```
# cd /var/yp/domainname
# makedbm -u test.byname
# makedbm -u test.byname
```

マップの出力をチェックする場合は、次のことに注意してください。

- 両方のファイルでのエントリの順序が異なる可能性
出力を比較する前に、`sort` コマンドを使用します。
- 両方のファイルでの空白の使い方が異なる可能性
出力を比較するときは `diff -b` コマンドを使用します。

NIS マップの処理順序

説明: オブジェクトクラス違反が発生しました。

原因: `ypserv -i` コマンドを実行すると、各 NIS マップが読み取られ、その内容が DIT に書き込まれます。複数のマップが、同一の DIT オブジェクトに属性を提供する場合もあります。通常、オブジェクトは、1 つのマップによってそのオブジェクトの MUST 属性のすべてを含む大部分を生成されます。ほかのマップは、ほかの MAY 属性を提供します。

マップは、`NISLDAPmapping` ファイルに定義されている `nisLDAPobjectDN` 属性と同じ順序で処理されます。MAY 属性を含むマップが MUST 属性を含むマップより先に処理されると、オブジェクトクラス違反が発生します。このエラーについての詳細は、[133 ページの「よくある LDAP エラーメッセージ」](#)のエラー 65 を参照してください。

対処方法: マップが正しい順序で処理されるように、`nisLDAPobjectDN` 属性の順序を変更します。

一時的な解決として、`ypserv -i` コマンドを何回か再実行します。コマンドが実行されるたびに、LDAP エントリは完全な状態になります。

注記 - 1 つのマップからオブジェクトのすべての MUST 属性を作成できないマッピングはサポートされていません。

N2L サーバーのタイムアウトの問題

サーバーがタイムアウトします。

原因: N2L サーバーがマップをリフレッシュした結果、大規模な LDAP ディレクトリの 1 回のアクセスが行われる場合があります。Oracle Directory Server Enterprise Edition が正しく構成されていない場合、この動作は完了前にタイムアウトになることがあります。

対処方法: ディレクトリサーバーのタイムアウトを回避するには、Oracle Directory Server Enterprise Edition 属性を手動で、または `idsconfig` コマンドを実行することで変更します。詳細は、[133 ページの「よくある LDAP エラーメッセージ」](#)および [129 ページの「Oracle Directory Server Enterprise Edition での NIS から LDAP への移行のベストプラクティス」](#)を参照してください。

N2L のロックファイルの問題

`ypserv` コマンドは起動しますが、NIS リクエストに対して応答しません。

原因: N2L サーバーのロックファイルが、NIS マップへのアクセスを正しく同期していません。このような状況が発生してはなりません。

対処方法: N2L サーバーで次のコマンドを入力して、アクションを記述します。

```
# svcadm disable network/nis/server:default
# rm /var/run/yp_maplock /var/run/yp_mapupdate
# svcadm enable network/nis/server:default
```

N2L のデッドロックの問題

N2L サーバーがデッドロックします。

原因: N2L マスターサーバーと LDAP サーバーのアドレスが `hosts`、`ipnodes`、または `ypserv` ファイル内に正しくリストされていないと、デッドロックが発生する可能性があります。N2L の正しいアドレス構成についての詳細は、[120 ページの「NIS から LDAP への移行のための前提条件」](#)を参照してください。

デッドロックの発生する例として、次の一連の事柄を考えてみてください。

1. NIS クライアントが IP アドレスの検索を試みます。
2. N2L サーバーが、`hosts` エントリは最新ではないことを検出します。
3. N2L サーバーが LDAP からの `hosts` エントリの更新を試みます。
4. N2L サーバーは、その LDAP サーバーの名前を `ypserv` から取得したあと、`libldap` を使用して検索を実行します。

5. `libldap` は、ネームサービススイッチを呼び出して、LDAP サーバー名の IP アドレスへの変換を試みます。
6. ネームサービススイッチの設定に基づき、N2L サーバーへの NIS 呼び出しを行い、デッドロックが発生します。

対処方法: N2L マスターサーバーと LDAP サーバーのアドレスを N2L マスターサーバー上の `hosts` または `ipnodes` ファイル内にリストします。`hosts` ファイルおよび `ipnodes` ファイルがローカルホスト名を解決するためにどのようにして構成されているかに応じて、サーバーアドレスは、各ファイルに、またはその両方にリストされなければなりません。また、`svc:/network/name-service/switch` サービスの `config/hosts` プロパティの検索順序で、`files` が `nis` の前に指定されていることも確認してください。

このデッドロックの問題に対する別の解決方法として、`ypserv` ファイル内にホスト名ではなく、LDAP サーバーアドレスをリストする方法があります。LDAP サーバーのアドレスが別の場所にもリストされているため、LDAP サーバーと N2L サーバーのどちらかのアドレスを変更するには、さらに少し作業が必要となります。

NIS に戻す方法

N2L サービスを使用して NIS から LDAP に移行されたサイトでは、すべての NIS クライアントを LDAP ネームサービスクライアントに徐々に置き換えていくことが望まれます。最終的には、NIS クライアントに対するサポートは不要になります。ただし、必要に応じて、N2L サービスは、このセクションの手順に示すように、従来の NIS に復帰するための 2 種類の方法を提供します。

ヒント - 従来の NIS は、N2L バージョンの NIS マップが存在しても、それを無視します。NIS に戻したあとで、サーバー上の N2L バージョンのマップをそのままにしておいた場合でも問題を起こしません。このため、N2L マップを保持しておく、あとで N2L を再度有効にする際に役立つことがあります。ただし、マップはディスクスペースを消費することに注意してください。

▼ 以前のソースファイルに基づくマップに戻す方法

1. 管理者になります。

詳細は、『Oracle Solaris 11.2 でのユーザーとプロセスのセキュリティ保護』の「割り当てられている管理権利の使用」を参照してください。

2. NIS デーモンを停止します。

```
# svcadm disable network/nis/server:default
```

3. N2L を無効にします。

このコマンドは、N2L マッピングファイルをバックアップして、移動します。

```
# mv /var/yp/NISLDAPmapping backup-filename
```

4. NOPUSH 環境変数を設定して、ypmake によって新しいマップが転送されないようにします。

```
# NOPUSH=1
```

5. 以前のソースに基づいて、NIS マップの新しいセットを作成します。

```
# cd /var/yp  
# make
```

6. (オプション) N2L バージョンの NIS マップを削除します。

```
# rm /var/yp/domain-name/LDAP_*
```

7. DNS および NIS サービスを起動します。

```
# svcadm enable network/dns/client:default  
# svcadm enable network/nis/server:default
```

▼ 現在の DIT 内容に基づくマップに戻す方法

この手順を実行する前に、従来の NIS ソースファイルをバックアップします。

1. 管理者になります。

詳細は、『Oracle Solaris 11.2 でのユーザーとプロセスのセキュリティ保護』の「割り当てられている管理権利の使用」を参照してください。

2. NIS デーモンを停止します。

```
# svcadm disable network/nis/server:default
```

3. DIT に基づいてマップを更新します。

```
# ypserv -r
```

ypserv が終了するまで待ちます。

4. N2L を無効にします。

このコマンドは、N2L マッピングファイルをバックアップして、移動します。

```
# mv /var/yp/NISLDAPmapping backupfilename
```

5. NIS ソースファイルを再生成します。

```
# ypmap2src
```

6. 再生成された NIS ソースファイルの内容と構造が正しいことを手動でチェックしてください。

7. 再生成された NIS ソースファイルを適切なディレクトリに移動します。

8. (オプション) N2L バージョンのマッピングファイルを削除します。

```
# rm /var/yp/domain-name/LDAP_*
```

9. DNS および NIS サービスを起動します。

```
# svcadm enable network/dns/client:default  
# svcadm enable network/nis/server:default
```

用語集

アプリケーションレベルのネームサービス	ファイル、メール、印刷などのサービスを提供するアプリケーションに組み込まれているネームサービスのこと。アプリケーションレベルのネームサービスは、企業レベルのネームサービスの下に位置する。企業レベルのネームサービスが提供するコンテキストの中に、アプリケーションレベルのネームサービスのコンテキストを組み込むことができる。
暗号化	データのプライバシーを保護するための手段。
暗号化鍵	「データ暗号化鍵」の項を参照。
インターネットアドレス	TCP/IPを使用してホストに割り当てられた 32 ビットアドレス。「ドット形式の 10 進表記」の項を参照。
インデックス付き名前	テーブル内のエントリを識別するために使用される命名形式。
エントリ	データベーステーブル内の 1 行のデータ (DIT 内の LDAP 要素など)。
鍵 (暗号化)	鍵の管理および配布システムの一部として、ほかの鍵を暗号化および暗号化解除するために使用される鍵。「データ暗号化鍵」の項も参照。
鍵サーバー	非公開鍵を格納する、Oracle Solaris オペレーティング環境のプロセス。
企業レベルのネットワーク	「企業レベルの」ネットワークは、ケーブル、赤外線ビーム、または無線ブロードキャスト経由で通信する単一のローカルエリアネットワーク (LAN) である場合や、ケーブルまたは直接電話接続でリンクされた 2 つ以上の LAN のクラスタである場合がある。企業レベルのネットワーク内では、DNS や X.500/LDAP などのグローバルネームサービスを使用せずに、どのマシンからでも任意のマシンにアクセスできる。
逆解決	DNS ソフトウェアを使用して、ワークステーションの IP アドレスをワークステーション名に変換するプロセス。
クライアント	(1) クライアントは、ネームサーバーにネームサービスをリクエストする主体 (マシンまたはユーザー)。 (2) ファイルシステムのクライアントサーバーモデルでは、クライアントとは、計算パワーや大きな記憶容量などの計算サーバーのリソースにリモートアクセスするマシン。

(3) クライアントサーバーモデルでは、クライアントは「サーバープロセス」からサービスにアクセスするアプリケーションのこと。このモデルでは、クライアントとサーバーを同一マシンまたは個別のマシンで実行できる。

クライアントサーバーモデル	ネットワークサービスと、これらのサービスのモデルユーザープロセス (プログラム) を説明するための一般的な方法。たとえば、「ドメインネームシステム (DNS)」のネームサーバー/ネームリゾルバパラダイムなど。「クライアント」の項も参照。
グループ ID	ユーザーのデフォルトのグループを識別する番号。
グローバルネームサービス	グローバルネームサービスは、電話、衛星、またはその他の通信システムでリンクされているこれらの世界中の企業レベルのネットワークを識別 (名前付け) する。この世界規模でリンクされたネットワークの集合は、「インターネット」と呼ばれている。グローバルネームサービスは、ネットワーク名の指定のほかに、特定のネットワーク上の個々のマシンとユーザーも識別する。
広域ネットワーク (WAN)	異なる地理的な場所に存在する複数のローカルエリアネットワーク (LAN) またはシステムを電話、光ファイバ、衛星などのリンクで接続するネットワーク。
公開鍵	数学的に生成された 1 対の番号の公開コンポーネントであり、非公開鍵と組み合わせれば DES 鍵が生成される。この DES 鍵を使用すれば、情報のエンコードとデコードを行える。公開鍵は、すべてのユーザーとマシンが使用できる。どのユーザーやマシンにも、固有の公開鍵と非公開鍵が 1 対ある。
コンテキスト	N2L サービスの場合、コンテキストは、一般に NIS ドメインがその下でマップされるもの。「baseDN」の項も参照。
サーバー	(1) NIS、DNS、および LDAP では、ネットワークにネームサービスを提供するホストマシン。 (2) ファイルシステムのクライアントサーバーモデルでは、サーバーとは計算リソース (計算サーバーとも呼ばれる) と大きな記憶容量を備えたマシン。クライアントマシンはリモートアクセスが可能であり、これらのリソースを使用できる。ウィンドウシステムのクライアントサーバーモデルでは、サーバーはウィンドウサービスをアプリケーション (クライアントプロセス) に提供するプロセスのこと。このモデルでは、クライアントとサーバーを同一マシンまたは個別のマシンで実行できる。 (3) ファイルの提供を実際に処理するデーモン。
サーバーリスト	「優先サーバーリスト」の項を参照。
サブネット	ルーティングを単純化するために、1 つの論理ネットワークをより小さな物理ネットワークに分割する実際的なスキーム。
資格情報	クライアントソフトウェアが各リクエストとともにネームサーバーに送信する認証情報。この情報によって、ユーザーまたはマシンの ID が検査される。
識別名 (DN)	識別名は、X.500 ディレクトリ情報ベース (DIB) 内のエントリであり、ルートから指定されたエントリまでつながるパスに沿った、ツリー内の各エントリから選択された属性で構成される。

スキーマ	任意の特定の LDAP DIT 内にどのような種類のデータを格納できるかを定義する一連の規則。
スレーブサーバー	NIS データベースのコピーを保持するサーバーシステム。このシステムには、ディスクと動作環境の完全なコピーが存在する。
接尾辞	LDAP では、DIT の識別名 (DN)。
ソース	NIS ソースファイル
属性	各 LDAP エントリは、いくつかの名前付き属性で構成され、各属性は 1 つまたは複数の値を持つ。 また、N2L サービスマッピングおよび構成ファイルもそれぞれ、いくつかの名前付き属性で構成される。各属性は 1 つまたは複数の値を持つ。
ディレクトリ	LDAP ディレクトリは、LDAP オブジェクトのコンテナ。(2) UNIX では、ファイルまたはサブディレクトリのコンテナのこと。
ディレクトリキャッシュ	ディレクトリオブジェクトに関連付けられたデータを格納するために使用されるローカルファイル。
ディレクトリ情報ツリー (DIT)	DIT は、特定のネットワークの分散型ディレクトリ構造。デフォルトでは、クライアントは、DIT が特定の構造を持っていると想定して情報にアクセスする。LDAP サーバーがサポートするドメインごとに、想定された構造を持つ想定されたサブツリーがある。
データ暗号化鍵	暗号化を実行するプログラムを対象としたデータを暗号化および暗号化解除するために使用される鍵。「鍵 (暗号化)」の項も参照。
データ暗号化規格 (DES)	データを暗号化および復号化するための、アメリカ商務省標準局によって開発された一般的に使用されている高度なアルゴリズム。「SUN-DES-1」の項も参照。
ドット形式の 10 進表記	32 ビット整数の構文表現であり、ピリオド (ドット) で区切られた 4 つの 10 進表記の 8 ビット数で構成される。192.168.67.20 のように、インターネットでの IP アドレスを表現するために使用される。
ドメイン	(1) インターネットでは、ネーミング階層の一部であり、通常はローカルエリアネットワーク (LAN)、広域ネットワーク (WAN)、またはこのようなネットワークの一部に対応する。構文上、インターネットドメイン名は小数点 (ドット) によって区切られた一連の名前 (ラベル) から構成される。たとえば、sales.example.com。 (2) ISO の開放型システム間相互接続 (OSI) では、「ドメイン」は、MHS プライベート管理ドメイン (PRMD) やディレクトリ管理ドメイン (DMD) などのように、複雑な分散システムの管理パーティションとして使用されるのが普通。
ドメインネームサービス (DNS)	ドメイン名やマシン名を企業の外部のアドレス (インターネット上のアドレスなど) にマップするためネーミングポリシーおよびメカニズムを提供するサービス。すなわち DNS は、ドメイン名と

	マシン名をインターネットなどの企業外部のアドレスにマッピングする場合のネーミングポリシーとメカニズムを提供する。
ドメイン名	DNS 管理ファイルを共有するローカルネットワーク上のシステムのグループに割り当てられた名前。ネットワーク情報サービスのデータベースが正常に動作するためにはドメイン名が必要。「ドメイン」の項も参照。
名前解決	ワークステーション名またはユーザー名をアドレスに変換するプロセス。
名前空間	(1) 名前空間は、ユーザー、ワークステーション、およびアプリケーションがネットワーク全体にわたって通信する必要のある情報を格納する。 (2) ネーミングシステムで使用される名前セット。
認証	サーバーがクライアントの識別情報を検証できるようにするための手段。
ネームサーバー	1 つまたは複数のネットワークネームサービスを実行するサーバー。
ネームサービス	マシン、ユーザー、ドメイン、ルータ、およびその他のネットワークの名前とアドレスを処理するネットワークサービス。
ネームサービススイッチ	ネームサービスクライアントが自身のネットワーク情報を取得できるソースを定義する <code>svc:/system/name-service/switch</code> サービス。
ネットワークパスワード	「Secure RPC パスワード」の項を参照。
ネットワークマスク	ローカルサブネットアドレスを特定のインターネットプロトコルアドレスの残りから分離するためにソフトウェアによって使用される数値。
非公開鍵	数学的に生成された 1 対の番号の非公開コンポーネントであり、公開鍵と組み合わせれば DES 鍵が生成される。この DES 鍵を使用すれば、情報のエンコードとデコードを行える。送信側の非公開鍵は、その鍵の所有者だけが使用できる。どのユーザーやマシンにも、固有の公開鍵と非公開鍵が 1 対ある。
フィールド	NIS マップエントリは、いくつかのコンポーネントと区切り文字で構成される可能性がある。N2L サービスマッピングプロセスの一部として、エントリはまず、いくつかの名前付きフィールドに分解される。
マスターサーバー	特定のドメインのネットワーク情報サービスデータベースのマスターコピーを保持するサーバー。名前空間に対する変更は、必ずマスターサーバーのネームサービスデータベース上で行う。ドメイン中に複数のマスターサーバーを作成できない。
マッピング	NIS エントリと DIT エントリの間の変換を行うプロセス。この処理は、「マッピング」ファイルにより制御される。
メール交換レコード	DNS ドメイン名とそれらに対応するメールホストの一覧が含まれているファイル。

メールホスト	サイトの電子メールのルーターおよび受信側として機能するワークステーション。
優先サーバーリスト	client_info テーブルまたは client_info ファイルのこと。優先サーバーリストには、あるクライアントマシンまたはドメインから見た優先サーバーが指定される。
リモート手続き呼び出し (RPC)	分散コンピューティングのクライアントサーバーモデルを実装するための容易で、一般的なパラダイム。与えられた引数を使用することによって、要求がリモートシステムに送信され、指定された手順が実行される。そのあと、その結果が呼び出し側に返される。
レコード	「エンTRY」の項を参照。
ローカルエリアネットワーク (LAN)	データやソフトウェアの共有および交換の目的のためにまとまって接続されている、地理的に一か所に存在する複数のシステム。
baseDN	DIT の一部のベースとなっている DN。これが NIS ドメインエントリの baseDN である場合は、コンテキストとも呼ばれる。
databaseID	N2L サービスの場合、databaseID は、同じ形式の NIS エントリを含む (LDAP への同じマッピングを持つ) マップのグループの別名。これらのマップの鍵は異なっている可能性がある。
DBM	NIS マップを格納するために当初使用されるデータベース。
DES	「データ暗号化規格 (DES)」の項を参照。
DIT	「ディレクトリ情報ツリー」の項を参照。
DN	LDAP 内の識別名。ツリー構造を持つ LDAP ディレクトリのアドレススキーム。各 LDAP エントリに一意的な名前を付与する。
DNS	「ドメインネームシステム」の項を参照。
DNS ゾーン	ネットワークドメイン内の管理境界であり、多くの場合は 1 つまたは複数のサブドメインで構成される。
DNS ゾーンファイル	DNS ソフトウェアがドメイン内の全ワークステーションの名前と IP アドレスを格納する一連のファイル。
DNS 転送	NIS サーバーは、自身で応答できないリクエストを DNS サーバーに転送する。
gid	「グループ ID」の項を参照。
IP	インターネットプロトコル。インターネットプロトコル体系の「ネットワーク層」プロトコル。
IP アドレス	ネットワーク内の各ホストを識別する一意の番号。
LDAP	Lightweight Directory Access Protocol は、LDAP ネームサービスクライアントおよびサーバーが互いに通信するために使用する、標準の拡張可能なディレクトリアクセスプロトコル。
MIS	経営情報システム (またはサービス)。

N2L サーバー	NIS-to-LDAP サーバー。N2L サービスを使用して、N2L サーバーとして再構成された NIS マスターサーバー。再構成には、NIS デーモンの置き換えと新しい構成ファイルの追加が含まれる。
NDBM	DBM の改良されたバージョン。
NIS	ネットワーク上のシステムおよびユーザーに関する重要な情報が取められている分散型ネットワーク情報サービス。NIS データベースは、「マスターサーバー」とすべての「スレーブサーバー」に格納されている。
NIS マップ	NIS によって使用されるファイルであり、ネットワーク上の全ユーザーのパスワードエントリやネットワーク上の全ホストマシンの名前など特定種類の情報を格納する。NIS サービスの一部であるプログラムはこれらのマップを参照する。「NIS」の項も参照。
RDN	相対識別名。DN の一部。
RFC 2307	標準の NIS マップから DIT エントリへの情報のマッピングを指定した RFC。デフォルトでは、N2L サービスは、更新されたバージョン RFC 2307bis で指定されたマッピングを実装している。
RPC	リモート手続き呼び出し (RPC) を参照。
SASL	Simple Authentication and Security Layer (簡易認証セキュリティ層)。アプリケーション層プロトコルにおける認証およびセキュリティ層の意味上の取り決め。
searchTriple	特定の属性を検索する DIT 内の場所についての説明。searchTriple は、ベース DN、スコープ、およびフィルタで構成される。これは、RFC 2255 で定義された LDAP URL 形式の一部である。
Secure RPC パスワード	Secure RPC プロトコルに必要なパスワード。非公開鍵の暗号化に使用される。このパスワードはユーザーのログインパスワードと同じでなければならない。
SSL	SSL は Secure Sockets Layer プロトコルである。LDAP セキュアなどのアプリケーションプロトコルを作成するためのトランスポート層のセキュリティメカニズムの総称。
TCP	「 <i>Transport Control Protocol (TCP)</i> 」の項を参照。
TCP/IP	Transport Control Protocol/Interface Program の略語。このプロトコル群は、最初はインターネット用に開発された。「インターネット」プロトコル群とも呼ばれる。Oracle Solaris ネットワークは、デフォルトでは TCP/IP 上で動作する。
Transport Control Protocol (TCP)	信頼性の高い、コネクション型の全二重ストリームを提供する、インターネットプロトコル群内の主要なトランスポートプロトコル。配信には IP を使用する。「TCP/IP」の項を参照。
Transport Layer	TLS は、LDAP クライアントとディレクトリサーバーの間の通信をセキュリティ保護して、プライバシーとデータの完全性の両方を提供する。TLS プロトコルは、Secure Sockets Layer (SSL) プロトコルのスーパーセットである。

**Security
(TLS)**

X.500 開放型システム間相互接続 (OSI) 規格によって定義されたグローバルレベルのディレクトリサービス。LDAP の前身。

yp Yellow Pages™。NIS コード内部で今も使用される NIS の古い名前。

索引

数字・記号

- /usr/lib/netsvc/yp/inityp2l コマンド, 116, 118
- /usr/lib/netsvc/yp/ypmap2src コマンド, 116, 118
- /var/yp/NISLDAPmapping ファイル, 118
- /var/yp/ypserv ファイル
 - N2L 移行および, 118

あ

アカウント管理

- enableShadowUpdate スイッチ, 27
- LDAP がサポートする機能, 29
- pam_ldap を使用する LDAP クライアントの場合, 61
- pam_unix_* クライアント用の LDAP サーバー, 30
- pam_unix_* モジュールを使用する LDAP クライアントの場合, 63
- PAM モジュールと LDAP, 29
- ディレクトリサーバーでの構成, 61
- アクセス制御情報, 15

暗号化

- 定義, 141

暗号化鍵

- 定義, 141

インターネットアドレス

- 定義, 141

インデックス付き名前

- 定義, 141

インデックス表示 参照 仮想リスト表示インデックス エントリ

- 定義, 141

か

鍵 (暗号化)

- 定義, 141
- 鍵サーバー
 - 定義, 141
- 仮想リスト表示インデックス, 47
- 企業レベルのネットワーク
 - 定義, 141
- 逆解決
 - 定義, 141
- クライアント
 - 定義, 141
- クライアントサーバーモデル
 - 定義, 142
- グループ ID
 - 定義, 142
- グローバルネームサービス
 - 定義, 142
- 検索記述子, 11
- 公開鍵
 - 定義, 142
- コンテキスト
 - 定義, 142

さ

- サーバー
 - 定義, 142
- サーバーリスト
 - 定義, 142
- サービス検索記述子, 41
- サブネット
 - 定義, 142
- 資格情報
 - 定義, 142
- 資格ストレージ
 - LDAP クライアント, 20
- 資格レベル

- LDAP クライアント, 18
- 識別名
 - 定義, 142
- スキーマ 参照 LDAP スキーマ
 - RFC 2307bis, 90
 - 定義, 143
 - マッピング, 40
- スレーブサーバー
 - 定義, 143
- 接尾辞
 - 定義, 143
- ソース
 - 定義, 143
- 属性
 - Internet Print Protocol, 101
 - 定義, 143

た

- ディレクトリ
 - 定義, 143
- ディレクトリキャッシュ
 - 定義, 143
- ディレクトリサーバー, 10
- ディレクトリ情報ツリー, 11
 - DIT コンテナ, 11
 - 定義, 143
- ディレクトリユーザーエージェントのスキーマ, 95
- データ暗号化鍵
 - 定義, 143
- データ暗号化規格 参照 DES
- データ移入, 40
- ドット形式の 10 進表記
 - 定義, 143
- ドメイン
 - 定義, 143
- ドメインネームシステム (DNS) 参照 DNS
- ドメイン名
 - 定義, 144
- トラブルシューティング
 - LDAP, 79

な

- 名前解決

- 定義, 144
- 名前空間
 - 定義, 144
- 認証
 - 定義, 144
- 認証方法
 - LDAP での選択, 21
 - LDAP 内のサービス, 23
 - PAM モジュール, 24
- ネームサーバー
 - 定義, 144
- ネームサービス
 - 定義, 144
- ネームサービススイッチ
 - 定義, 144
- ネットワーク情報サービススキーマ, 90
- ネットワークパスワード 参照 Secure RPC パスワード
- ネットワークマスク
 - 定義, 144

は

- パスワード
 - LDAP, および, 28
- パスワードエントリ
 - enableShadowUpdate スイッチ, 19
- パスワード管理 参照 アカウント管理
- 非公開鍵
 - 定義, 144
- フィールド
 - 定義, 144
- プラグイン可能認証モジュール, 24
- プロキシ認証, 15
- プロジェクトスキーマ
 - オブジェクトクラス, 98
 - 属性, 98
- プロファイル
 - LDAP クライアント, 69

ま

- マスターサーバー
 - 定義, 144
- マッピング
 - 定義, 144

マッピングファイル
NIS から LDAP へ, 113
メールエイリアススキーマ, 95
メール交換レコード
定義, 144
メールホスト
定義, 145

や

役割に基づく LDAP スキーマ, 99
オブジェクトクラス, 100
ユーザー別の資格情報, 19

ら

リフェラル, 49
レコード
定義, 145

A

adminDN 属性
説明, 70
adminPassword 属性
説明, 70
ageing.byname マップ
N2L 移行および, 118
anonymous 資格, 18
attributeMap 属性, 42
説明, 34
authenticationMethod 属性
pam_ldap モジュールおよび, 24
passwd-cmd サービスおよび, 28
説明, 34
複数値の例, 21

B

baseDN
定義, 145
bindTimeLimit 属性

説明, 35

C

certificatePath 属性
説明, 70
cn 属性
説明, 34
credentialLevel 属性
説明, 34

D

databaseID
定義, 145
defaultSearchBase 属性
説明, 34
defaultSearchScope 属性
説明, 34
defaultServerList 属性
説明, 34
DES
定義, 143, 145
DIT 参照 ディレクトリ情報ツリー
DN
定義, 145
DNS
定義, 145, 143
DNS ゾーン
定義, 145
DNS ゾーンファイル
定義, 145
DNS 転送
定義, 145
domainName 属性
説明, 70

E

enableShadowUpdate スイッチ, 27

F

FMRI

LDAP, 68
followReferrals 属性
説明, 35

I

inityp2l コマンド, 116, 118
IP
定義, 145
IP アドレス
定義, 145

K

Kerberos, 15
keyserv サービス
LDAP 認証および, 23

L

LAN
定義, 145
LDAP
FMRI, 68
NIS からの移行, 113
NIS に戻す方法, 138
SMF, 68
アカウント管理, 29
クライアント資格レベル, 18
構成および管理用のコマンド, 12
サポートされる PAM モジュールの比較, 25, 28
スキーマ 参照 LDAP スキーマ
その他のネームサービスとの比較, 12
ディレクトリサーバーでのアカウント管理の有効化,
61
定義, 145
データ交換フォーマット (LDIF), 11
トラブルシューティング 参照 LDAP のトラブル
シューティング
認証サービス, 10, 15
ネームサービス, 10
利点と制限, 10
LDAP から NIS に戻す方法, 138
LDAP クライアント

ローカルプロファイル属性, 69
LDAP クライアントプロファイル
属性, 33
LDAP コマンド, 12
LDAP スキーマ, 89
ディレクトリユーザーエージェント, 95
プロジェクト, 98
メールエイリアス, 95
役割に基づく属性, 99
LDAP ネットワークモデル, 35
LDAP のトラブルシューティング
ldapclient がサーバーにバインドできない, 84
LDAP ドメイン内のシステムにリモートアクセスでき
ない, 83, 83
検索が遅い, 84
未解決のホスト名, 82
ログインの失敗, 83
ldapaddent コマンド, 58
ldapclient コマンド
クライアントプロファイル属性, 69
Lightweight Directory Access Protocol 参照
LDAP

M

mail 属性, 95
mailGroup オブジェクトクラス, 95
MIS
定義, 145

N

N2L サーバー, 113, 117
N2L サービス, 113
カスタムマップの例, 127
サポートされるマッピング, 118
使用しない場合, 115
設定, 121
N2L の移行 参照 NIS から LDAP への移行
NIS
定義, 146
NIS から LDAP へ
SMF および, 114
NIS から LDAP への移行, 113, 113, 113
参照 N2L

hosts データベース, 120
idsconfig コマンドの使用, 120
LDAP エラーコード, 133
NISLDAPmapping ファイルのデバッグ, 135
NIS に戻す方法, 138
Oracle Directory Server Enterprise Edition
を使用した, 129
仮想リスト表示 (VLV) の使用, 129
構成ファイル, 117
コマンド, 117
サーバーのタイムアウト, 131
制限, 132
前提条件, 120
デッドロック, 138
トラブルシューティング, 132
ネームサービススイッチ構成, 120
バッファオーバーラン, 131
問題, 134
用語, 117
NIS マップ
定義, 146
NISLDAPmapping ファイル, 113, 118
none 認証方法
LDAP および, 21

O

objectclassMap 属性, 42
説明, 35
Oracle Directory Server Enterprise Edition
idsconfig を使用した設定, 45

P

pam_ldap
LDAP でのアカウント管理, 61
pam_ldap サービス
LDAP 認証および, 23
pam_unix_* モジュール
LDAP でのアカウント管理, 30, 63
PAM サービス, 15
PAM モジュール
LDAP, 24
認証方法, 24

passwd-cmd サービス
LDAP 認証および, 23
preferredServerList 属性
説明, 34
profileTTL 属性
説明, 35
proxy anonymous 資格情報, 19
proxy 資格情報, 18
proxyDN 属性
説明, 70
proxyPassword 属性
説明, 70

R

RFC2307bis LDAP スキーマ, 90
RFC 2307bis
属性, 90
RFC 2307
オブジェクトクラス, 92
RPC
定義, 145, 146

S

serviceAuthenticationMethod 属性, 23
pam_ldap モジュールおよび, 24
passwd-cmd サービスおよび, 28
説明, 34
SASL
定義, 146
sasl 認証方法
LDAP および, 21
searchTimeLimit 属性
説明, 35
searchTriple
定義, 146
Secure RPC パスワード
定義, 146
Secure Sockets Layer 参照 SSL
serviceSearchDescriptor 属性
説明, 34
simple 認証方法
LDAP および, 21

SMF
NIS から LDAP への移行用ツールおよび, 114
と LDAP, 68
SSD, 41
SSL
定義, 146
SSL プロトコル, 17
N2L 移行および, 118

T

TCP 参照 Transport Control Protocol
TCP/IP
定義, 146
TLS 参照 Transport Layer Security
tls 認証方法
LDAP および, 22
Transport Control Protocol
定義, 146
Transport Layer Security, 17
定義, 146

V

VLV 参照 仮想リスト表示インデックス

W

WAN
定義, 142

X

X.500
定義, 147

Y

yp
定義, 147
ypmap2src コマンド, 116, 118
ypserv ファイル