



OpenLDAP



オープンソースで安全・安心のLDAPサーバー製品

Linux・Windows・macOS・各種アプリケーションの
ユーザー情報と認証の統合管理を実現

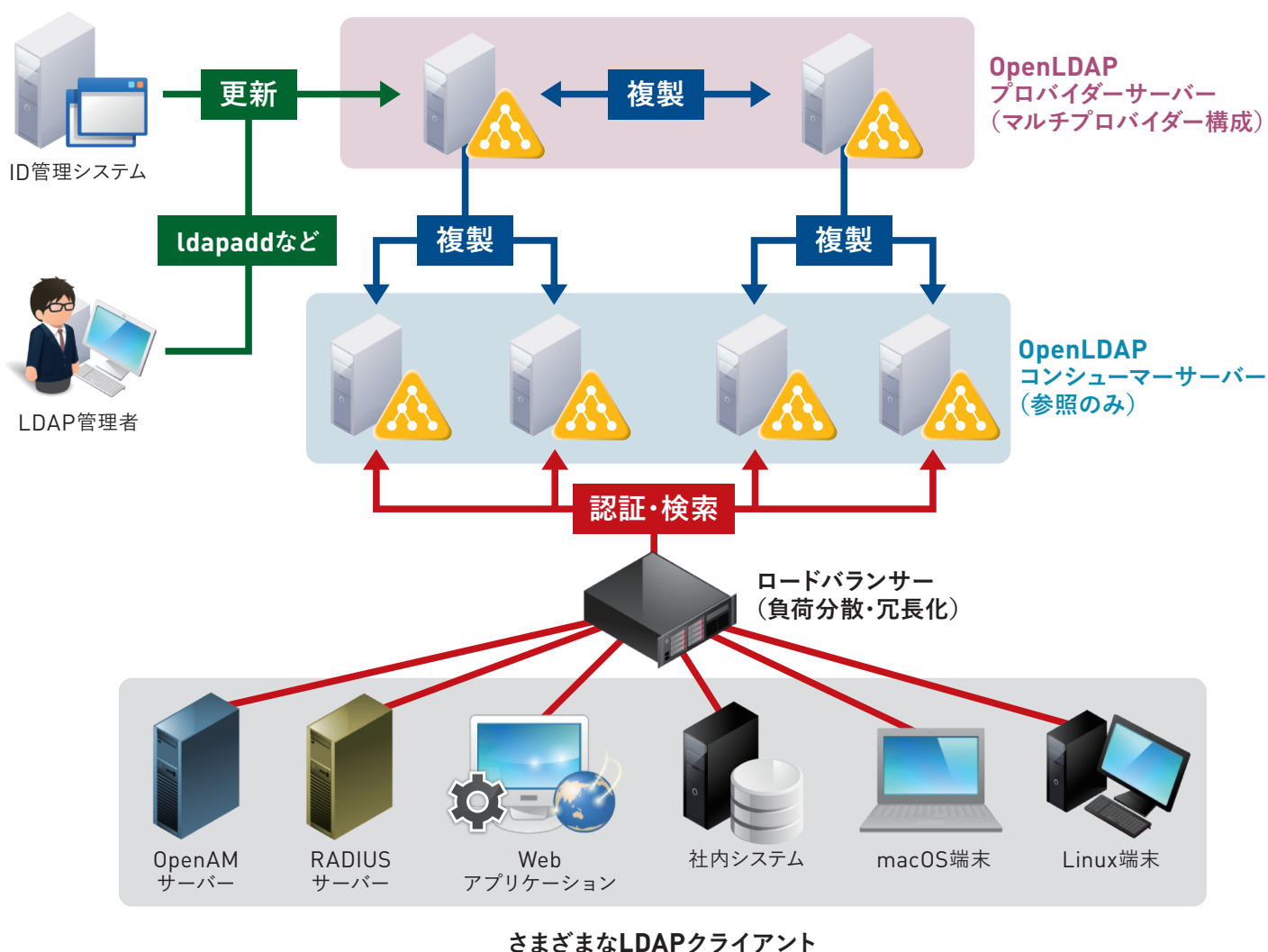
OpenLDAP とは？

- LDAPサーバーソフトウェアとして最も普及し、安定性に優れた長年の動作実績
- LDAPv3に準拠し、各種LDAP対応製品との接続において、豊富な接続情報・接続実績を提供
- プロバイダーサーバーを冗長構成として高い可用性を提供
- コンシューマーサーバーを追加することで、認証・検索処理の負荷分散、スケールアウトが可能

基本機能

- LDAPv3に準拠したディレクトリサービスを提供
- TLSによる通信経路の暗号化
- IPアドレスやグループ属性によるアクセス権の管理
- パスワードポリシーによるパスワードの保護強化
- カスタムスキーマによる任意の属性の登録
- マルチプロバイダー/プロバイダー・コンシューマ機能による冗長構成、スケールアウト、負荷分散

システム構成例



OSSTech OpenLDAP の機能・特長

各種LDAPサーバーからの移行に対応

OSSTech版 OpenLDAP 2.4、およびその他の OpenLDAP環境や商用LDAPサーバー製品からの移行に対応可能。

多様なパスワードハッシュ方式の対応

パスワードのハッシュアルゴリズムとして、CRYPT、Argon2、PBKDF2などを利用可能とし、既存環境からの移行に対応し、パスワード漏洩に対する保護を強化します。

各種オーバーレイの同梱

OpenLDAPで利用可能な各種オーバーレイを設定のみで利用できる状態でパッケージ済みです。

運用管理の強化

日次バックアップ機能とログローテート機能をパッケージに組み込み済みで、障害時のリカバリや操作ログの監査が実施できます。

Active Directoryとのパスワード双方向同期

OSSTech OpenLDAPの機能のみでWindows ADとOpenLDAPのパスワード双方向同期が可能です。また、Windows ADサーバーに追加モジュールの導入が不要です。

運用支援コマンドの追加

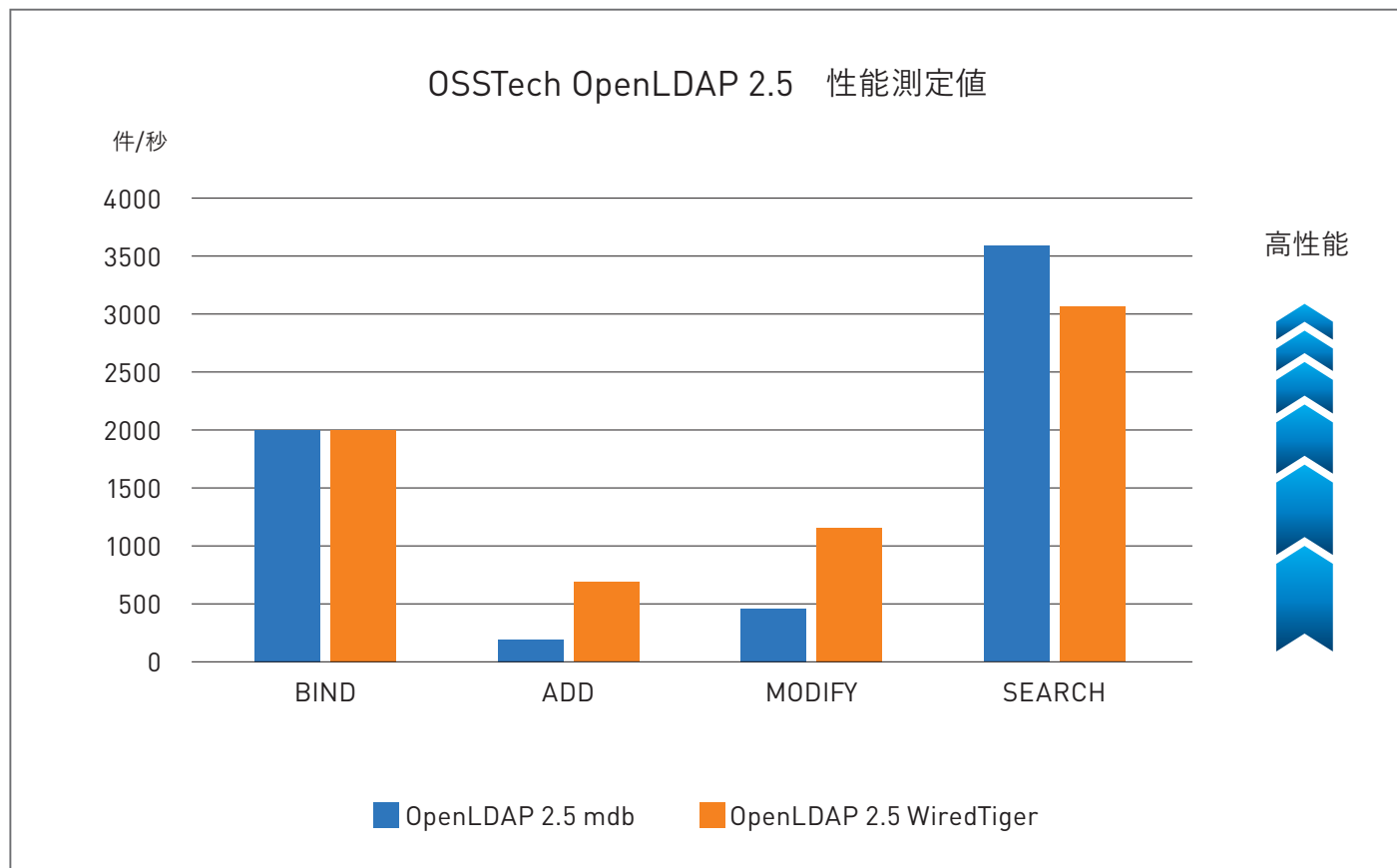
LDIFの比較コマンドや、LDIFのソートコマンドなど、運用時にLDAPのデータを簡単に操作するためのコマンド群を提供します。

LDAPロードバランサー機能の提供

OpenLDAPが提供するLDAPロードバランサー(lload)により、複数台のLDAPコンシューマーサーバーの負荷分散と冗長化を実現可能です。

OSSTech OpenLDAP のバックエンドデータベース

WiredTigerバックエンドとMDBバックエンドに対応



【測定環境】RHEL9 / OSSTech OpenLDAP 2.5.12 / AWS EC2 t3.small / ストレージ io1

※ 本測定結果はLDAPサーバー環境の選定材料とするための参考値です。

システムの要求性能に合わせてスケールアップ、スケールアウトを組み合わせて構成してください。

OSSTech OpenLDAP 機能一覧

- LDAPv3 に準拠し、LDAPサービスを提供
- カスタムスキーマの定義により任意の属性の登録が可能
- エントリに対して、ユーザー、グループ、IPアドレスなどによるアクセス制限が可能
- LDAP接続時にシンプル認証・SASL認証が可能
- LDAP通信をTLSにより暗号化可能
- LDAPサービスの接続ユーザー、接続元IPアドレス、操作内容をログに記録
- パスワード格納時のハッシュ化アルゴリズムとして、CRYPT、PBKDF2、Argon2などに対応
- パスワードポリシーとして有効期限、パスワードの最小・最大文字数、複雑性、アカウントロックなどの制約を設定可能
- データ格納先のバックエンドとして、WiredTiger、MDBに対応
- 設定方式として、slapd.confによる設定ファイル方式と、configバックエンドによるLDAPデータベース方式に対応
- 複数のLDAPツリーを1つのLDAPサービス内で管理可能
- Windows Active Directoryとのパスワード双方向同期が可能

OpenLDAPパッケージ同梱オーバーレイ

モジュール名	用途
syncprov	LDAP複製機能
ppolicy	パスワードポリシー
pw-sha2	SHA-2 形式パスワード
pw-pbkdf2	PBKDF2 形式パスワード
auditlog	変更履歴の記録
dynlist	グループメンバー情報の自動反映
unique	属性値の一意制約
valsort	検索結果のソート機能
lastbind	認証成功時刻の記録
psync	ADとのパスワード双方向同期
smbk5pwd	Sambaパスワードの自動同期

OSSTech OpenLDAP 製品

- 稼働ノードに対するノードライセンス体系
- RPM形式で提供
- 導入時の各種設定内容をインストールガイドにて説明
- 運用に役立つバックアップ設定などを初期設定済み

OpenLDAP 年間サポート

- OpenLDAP運用・障害に関する問い合わせ対応
- アップデートパッケージ提供
- 対応時間：平日 9時 - 17時
- システム単位の年間サポート
- 長期間サポートを提供

OpenLDAP 導入・移行 技術支援サービス

- LDAPサービス導入案件の営業支援
- OpenLDAP 設計・導入作業の実施
- OpenLDAP 設計・導入作業のメールによる技術支援
- OpenLDAP スキーマのカスタマイズ対応
- 旧OpenLDAP環境からのLDAPデータ移行
- 商用LDAP環境からOpenLDAPへの移行

OpenLDAPの開発・導入に長年携わってきた
LDAPのスペシャリストによる支援をご活用ください!

ハードウェア要件

- Intel または AMD の x86-64互換CPU
- メモリ 4GB以上
- ディスク 20GB以上(OS領域含む)

対応OS

- Red Hat Enterprise Linux 9 / 8 (x86-64)
- Rocky Linux 9 / 8 (x86-64)
- AlmaLinux 9 / 8 (x86-64)
- Amazon Linux 2023 (x86-64)

※ 対応OSの最新情報はOSSTech製品ページを参照してください