OpenLDAP クライアント設定ガイド

OSSTech 株式会社

更新日 2026-07-17

目次

1. はじめに 1
  1.1 構成概要 1
  1.2 前提条件 1
    1.2.1 LDAPディレクトリ構造の前提 1
  1.3 クライアントへのパッケージのインストール 2
  1.4 TLS証明書の設定 2
    1.4.1 公的認証局の証明書を使用する場合 2
    1.4.2 公的認証局発行のサーバー証明書以外の場合 3
  1.5 SSSD の設定 4
    1.5.1 自己署名証明書を使用する場合 5
    1.5.2 設定ファイルのパーミッション設定と SSSD の起動 5
  1.6 バインドパスワードの平文保存を避ける方法 6
    1.6.1 方法1: 匿名バインドの使用 6
    1.6.2 方法2: sss_obfuscate によるパスワードの難読化 6
  1.7 authselect による NSS/PAM の設定 7
  1.8 ホームディレクトリの自動作成 8
  1.9 動作確認 8
    1.9.1 1. ユーザー情報の取得 9
    1.9.2 2. グループ情報の取得 9
    1.9.3 3. ユーザーのグループ確認 9
    1.9.4 4. LDAP 接続の直接確認 9
    1.9.5 5. SSH ログインのテスト 10
  1.10 トラブルシューティング 10
    1.10.1 SSSD のログを確認する 10
    1.10.2 よくある問題と対処法 11
  1.11 付録: OpenLDAP サーバー側の確認事項 12
    1.11.1 posixAccount エントリの必須属性 12
    1.11.2 posixGroup エントリの必須属性 13
    1.11.3 バインド DN に必要な ACL 13

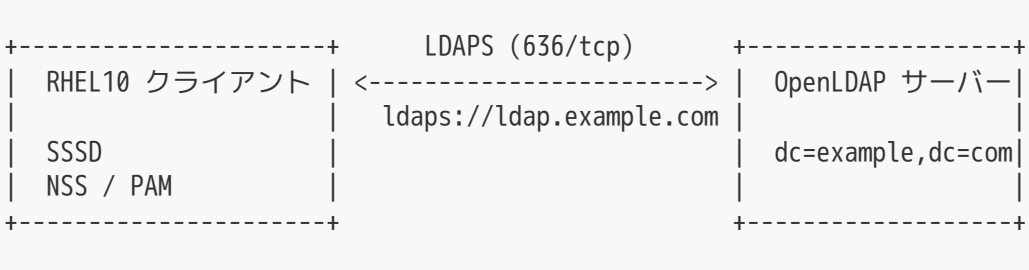
© 2026 OSSTech 株式会社

1. はじめに

本ドキュメントは、LDAPに登録されたユーザー・グループをOS(RHEL10)のユーザー・グループとして利用するための設定手順を説明します。

1.1 構成概要

本ドキュメントは以下の構成のシステムを前提にRHEL10クライアントでLDAPサーバーのユーザー・グループの情報を利用するための設定手順を説明します。



役割	ホスト名	備考
OpenLDAP サーバー	`ldap.example.com`	環境に合わせて読み替えること
RHEL10 クライアント	`client.example.com`	本手順の設定対象
ベース DN	`dc=example,dc=com`	環境に合わせて読み替えること
バインド DN	`cn=readonly,dc=example,dc=com`	読み取り専用アカウント推奨

1.2 前提条件

- RHEL 10 がインストール済みであること
- OpenLDAP サーバーが稼働しており、ユーザーおよびグループエントリが登録済みであること
- クライアントから OpenLDAP サーバーへの636/tcpポートへのネットワーク疎通ができること
- `root` 権限またはそれに相当する `sudo` 権限があること

© 2026 OSSTech 株式会社

1.2.1 LDAPディレクトリ構造の前提

本ドキュメントでは、LDAPサーバーのディレクトリ構成が次の命名規則で利用可能であることを前提としています。

```
dc=example,dc=com
 ├──── ou=People        ← ユーザーエントリ（objectClass: posixAccount）
 │     ├──── uid=alice
 │     └──── uid=bob
 └──── ou=Group         ← グループエントリ（objectClass: posixGroup）
       ├──── cn=developers
       └──── cn=admins
```

1.3 クライアントへのパッケージのインストール

RHEL10クライアントがLDAPサーバーのユーザー情報を参照するために必要となるsssdおよび関連パッケージのインストールを行います。

```
# dnf install -y \
  sssd \
  sssd-ldap \
  openldap-clients \
  oddjob \
  oddjob-mkhomedir \
  authselect
```

パッケージ	用途
`sssd`	System Security Services Daemon 本体
`sssd-ldap`	SSSD の LDAP プロバイダー
`openldap-clients`	`ldapsearch` などの動作確認コマンド
`oddjob` / `oddjob-mkhomedir`	ログイン時のホームディレクトリ自動作成
`authselect`	NSS / PAM プロファイル管理ツール

1.4 TLS証明書の設定

LDAPサーバーとの通信を安全に行うため、本手順ではLDAPS接続の設定をします。 LDAPS 接続では、サーバー証明書の種類によって設定方法が一部異なります。

1.4.1 公的認証局の証明書を使用する場合

LDAPサーバー側が UPKI、Let's Encrypt、DigiCert、GlobalSign などの公的認証局（CA）が発行した証明書を使用している場合、RHEL10 にはデフォルトで主要な公的 CA のルート証明書が含まれているため、RHEL10クライアントに追加の証明書配置は不要です。

クライアントからLDAPサーバーに接続できるか事前に確認します。

```
$ openssl s_client -connect ldap.example.com:636 </dev/null
```

出力の末尾に以下が含まれれば、クライアントにおいてLDAPサーバーの証明書は信頼されており、追加の証明書配置などの設定は不要です。

```
Verify return code: 0 (ok)
```

1.4.2 公的認証局発行のサーバー証明書以外の場合

- 自己署名証明書の場合
  - LDAPサーバーの証明書が自己署名の場合はLDAPサーバーに設置されているサーバー証明書をクライアントの信頼ストアに追加します。
- プライベートCA発行のサーバー証明書の場合
  - サーバー証明書発行元のプライベートCA証明書をクライアントの信頼ストアに追加します。

証明書の配置と信頼ストアへの登録

RHEL10クライアントでプライベートCA証明書や自己署名証明書を信頼するために、入手した証明書を次のコマンドでOSの信頼ストアに登録します。

(1) CA 証明書をシステムの信頼ストア用ディレクトリに配置しパーミッションを設定します。

```
# install -o root -g root -m 644  /path/to/ldap-ca.crt /etc/pki/ca-
trust/source/anchors/ldap-ca.crt
```

© 2026 OSSTech 株式会社

(2) OSの証明書情報に反映します。

```
# update-ca-trust extract
```

証明書が信頼されているか確認

次のコマンドでLDAPサーバーの証明書が信頼されているか確認します。

```
# openssl s_client -connect ldap.example.com:636 </dev/null
```

出力の末尾が以下になれば証明書が信頼された状態です。

```
Verify return code: 0 (ok)
```

エラーが出る場合は取得した証明書のSubjectや有効期限が想定通りであるか次のコマンドで確認します。

```
# openssl x509 -in /etc/pki/ca-trust/source/anchors/ldap-ca.crt -text -noout | \
  grep -E "Subject:|Issuer:|Not After"
```

証明書の信頼設定が完了したら、sssdを設定します。

1.5 SSSD の設定

sssdは、OSの認証やユーザー・グループ情報の参照を様々なリソースと連携するためのサービスです。

LDAPに登録されたユーザー情報やグループ情報を参照するためにsssdからLDAPを参照するための設定をクライアント上で行います。

sssdのLDAP参照時の標準設定では、posixAccountオブジェクトクラスを持つユーザーエントリをOSから利用可能です。同様にposixGroupオブジェクトクラスを持つエントリをグループエントリとして利用可能です。

sssdの設定として、`/etc/sssd/sssd.conf` を以下の内容で作成します。

© 2026 OSSTech 株式会社

```
[sssd]
services = nss, pam
domains = LDAP
config_file_version = 2

[domain/LDAP]
id_provider = ldap
auth_provider = ldap

# OpenLDAP サーバーの URI
ldap_uri = ldaps://ldap.example.com

# ベース DN
ldap_search_base = dc=example,dc=com

# バインド DN とパスワード（匿名バインドが可能な場合は省略可）
ldap_default_bind_dn = cn=readonly,dc=example,dc=com
ldap_default_authtok_type = password
ldap_default_authtok = ********  （cn=readonlyエントリのパスワードを指定）

# ユーザー検索設定
ldap_user_search_base = ou=People,dc=example,dc=com
ldap_user_object_class = posixAccount
ldap_user_name = uid

# グループ検索設定
ldap_group_search_base = ou=Group,dc=example,dc=com
ldap_group_object_class = posixGroup
ldap_group_name = cn

# TLS 設定（公的 CA 証明書はシステムの CA バンドルを使用）
ldap_tls_reqcert = demand

# キャッシュ設定
cache_credentials = true

# UID/GID の範囲（ローカルユーザーと重複しない値を設定）
min_id = 10000
max_id = 999999

# ログインシェルとホームディレクトリのフォールバック
default_shell = /bin/bash
fallback_homedir = /home/%u

# true にすると getent passwd で全ユーザーを列挙できる（大規模環境では false 推奨）
enumerate = false
```

LDAPに登録されているユーザーエントリ、グループエントリのうち、uidNumberやgidNumberがmin_idからmax_idの範囲に収まるエントリのみが有効となります。

© 2026 OSSTech 株式会社

1.5.1 自己署名証明書を使用する場合

LDAPサーバーの証明書として自己署名証明書を利用する場合、sssd.conf のTLS設定にldap_tls_cacertパラメーターを追加します。

```
# TLS 設定（自己署名/プライベートCA 証明書を明示的に指定）
ldap_tls_cacert = /etc/pki/ca-trust/source/anchors/ldap-ca.crt
```

1.5.2 設定ファイルのパーミッション設定と SSSD の起動

sssd.confファイルはrootのみ参照可能とするため、次の権限を設定します。

```
# chmod 600 /etc/sssd/sssd.conf
# chown root:root /etc/sssd/sssd.conf
```

SSSD の起動と自動起動の有効化を行います。

```
# systemctl enable --now sssd
# systemctl status sssd
```

1.6 バインドパスワードの平文保存を避ける方法

前述の `sssd.conf` ファイルの `ldap_default_authtok` に平文パスワードを記載した場合、ファイルパーミッションが 600 であっても root 権限を持つユーザーには読み取られるリスクがあります。 以下に、平文パスワードの記載を避けるための方法を説明します。

1.6.1 方法1: 匿名バインドの使用

LDAPサーバーがposixAccountやposixGroupオブジェクトクラスの各属性に対する匿名アクセスを許可している場合、バインド DN とパスワードの設定を省略することで、パスワードの記載を回避できます。

© 2026 OSSTech 株式会社

```
[domain/LDAP]
id_provider = ldap
auth_provider = ldap
ldap_uri = ldaps://ldap.example.com
ldap_search_base = dc=example,dc=com

# ldap_default_bind_dn と ldap_default_authtok を省略する
```

匿名バインドを利用する場合、LDAPサーバー側の ACL で、匿名ユーザーが `ou=People` および `ou=Group` 配下のエントリを読み取れるよう設定されている必要があります。

> 注意: `userPassword` 属性は匿名アクセスでは読み取れないよう ACL で制限してください。

1.6.2 方法2: sss_obfuscate によるパスワードの難読化

`sss_obfuscate` コマンドを使用してパスワードを難読化できます。 設定ファイルに平文パスワードが残らなくなります。

> 注意: 難読化は暗号化ではなく可逆変換です。技術的な知識があれば元の値を復元できるため、完全なセキュリティ対策とはなりません。

手順

1. まず通常どおり `sssd.conf` に平文パスワードを設定します：

```
ldap_default_bind_dn = cn=readonly,dc=example,dc=com
ldap_default_authtok_type = password
ldap_default_authtok = ****************
```

2. `sss_obfuscate` コマンドで難読化を行います

sssd-toolsパッケージを追加インストールします。

```
# dnf install -y sssd-tools
```

© 2026 OSSTech 株式会社

sss_obfuscateコマンドにsssd.confのLDAPのパスワードが指定されているドメイン(本ドキュメントの場合はLDAP)を指定して実行します。

```
# sss_obfuscate --domain LDAP
Enter password: ********     (cn=readonlyのパスワードを入力)
Re-enter password: ********  (cn=readonlyのパスワードを再入力)
```

コマンド実行後、`sssd.conf` の該当箇所が難読化された値に自動で書き換えられます：

```
ldap_default_bind_dn = cn=readonly,dc=example,dc=com
ldap_default_authtok_type = obfuscated_password
ldap_default_authtok = AAAQABagVAjf7XXXXXXXXXXXXXXXXXXXXXXXXXXX==
```

以上の設定変更完了後、sssdサービスを再起動してください。

```
# systemctl restart sssd
```

1.7 authselect による NSS/PAM の設定

sssdの設定が完了後、`authselect` コマンドを使用して、sssd を NSS および PAM に組み込み、OSから利用可能に変更します。

authselectコマンドに「with-mkhomedir」オプションを指定することで、ユーザーの初回ログイン時にホームディレクトリの自動生成を有効化できます。

```
# authselect select sssd with-mkhomedir
```

設定内容を確認します。

```
# authselect current
```

次の結果が表示されることを確認します。

```
Profile ID: sssd
Enabled features:
- with-mkhomedir
```

`/etc/nsswitch.conf` ファイルの passwd、groupの行に `sss` が追加されていることを確認します。

```
# grep -E '^(passwd|group)' /etc/nsswitch.conf
```

次の結果が表示されることを確認します。

```
passwd:     files sss systemd
group:      files [SUCCESS=merge] sss [SUCCESS=merge] systemd
```

1.8 ホームディレクトリの自動作成

`oddjob-mkhomedir` サービスを有効化します。

```
# systemctl enable --now oddjobd
# systemctl status oddjobd
```

本サービスによりLDAP ユーザーがクライアントに初めてログインした際に ホームディレクトリが自動的に作成されます。

1.9 動作確認

次の手順でLDAPに登録されたユーザー・グループ情報を利用できることを確認します。

1.9.1 1. ユーザー情報の取得

```
# getent passwd alice
```

© 2026 OSSTech 株式会社

期待される出力例:

```
alice:*:10001:10001:Alice Smith:/home/alice:/bin/bash
```

1.9.2 2. グループ情報の取得

```
# getent group developers
```

期待される出力例:

```
developers:*:20001:alice,bob
```

1.9.3 3. ユーザーのグループ確認

```
# id alice
```

期待される出力例:

```
uid=10001(alice) gid=10001(alice) groups=10001(alice),20001(developers)
```

1.9.4 4. LDAP 接続の直接確認

```
## 公的 CA 証明書の場合

# ldapsearch -x -H ldaps://ldap.example.com -W \
  -D "cn=readonly,dc=example,dc=com" \
  -b "ou=People,dc=example,dc=com" \
  "(uid=alice)"

Enter Password: *********  (cn=readonlyの接続パスワードを指定)


## 自己署名/プライベートCA発行 証明書の場合

環境変数で LDAPサーバーの自己署名/プライベートCA 証明書を指定します。

# LDAPTLS_CACERT=/etc/pki/ca-trust/source/anchors/ldap-ca.crt \
  ldapsearch -x -H ldaps://ldap.example.com -W \
  -D "cn=readonly,dc=example,dc=com" \
  -b "ou=People,dc=example,dc=com" \
  "(uid=alice)"
```

1.9.5 5. SSH ログインのテスト

クライアントに、sshでログインし、LDAPに登録されているユーザー名・パスワードでログインできることを確認します。

```
$ ssh alice@client.example.com
```

ログイン成功後に、ホームディレクトリが作成されていることを確認します。

```
$ pwd
/home/alice
```

1.10 トラブルシューティング

sshでのログインが失敗する場合、次の箇所を確認します。

1.10.1 SSSD のログを確認する

/etc/sssd/sssd.conf の [domain/LDAP] セクションにdebug_levelパラメーターを追加してデバッグレベルを上げることで、ログイン時のログが記録されます。

```
[domain/LDAP]
...
debug_level = 7
```

設定変更後、sssdサービスを再起動します。

```
# systemctl restart sssd
```

sssdのログでエラーを確認します。

```
# journalctl -u sssd -f
# tail -f /var/log/sssd/sssd_LDAP.log
```

1.10.2 よくある問題と対処法

`getent passwd` でユーザーが表示されない

SSSD キャッシュをクリアして再試行してください。

```
# sss_cache -E
# systemctl restart sssd
# getent passwd alice
```

TLS 証明書の検証エラー

自己署名証明書の場合、以下を確認します。

```
# CA 証明書でサーバー証明書を検証
openssl s_client -connect ldap.example.com:636 \
  -CAfile /etc/pki/ca-trust/source/anchors/ldap-ca.crt </dev/null
```

ca-bundle.crtの実体ファイルの更新日を確認し、update-ca-trust が実行されているか確認し、更新がされていない場合は、update-ca-trustを実行します。

```
# ls -la /etc/pki/tls/certs/ca-bundle.crt
# ls -l /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem
# update-ca-trust extract
```

配置した証明書のサブジェクト代替名（SAN）にサーバーのホスト名が含まれているか確認します。

```
# openssl x509 -in /etc/pki/ca-trust/source/anchors/ldap-ca.crt -text -noout | \
  grep -A2 "Subject Alternative Name"
```

バインドエラー（認証失敗）

sssdに指定したDNでLDAPサーバーへの接続が成功するか、ldapwhoamiコマンドで確認します。

```
# ldapwhoami -x -H ldaps://ldap.example.com \
  -D "cn=readonly,dc=example,dc=com" -W

Enter LDAP Password: ********  （cn=readonlyエントリのパスワードを入力）
```

パーミッションエラーで SSSD が起動しない

sssd.confファイルのパーミッションが600であることを確認します。

```
# ls -l /etc/sssd/sssd.conf
```

ホームディレクトリが作成されない

authselectの設定でmkhomedirオプションが有効なことと、oddjobdサービスが起動していることを確認します。

```
# systemctl status oddjobd
# authselect current | grep mkhomedir
# grep mkhomedir /etc/pam.d/system-auth
```

1.11 付録: OpenLDAP サーバー側の確認事項

1.11.1 posixAccount エントリの必須属性

属性	必須	例
`objectClass`	○	`posixAccount`, `inetOrgPerson`
`uid`	○	`alice`
`uidNumber`	○	`10001`
`gidNumber`	○	`10001`
`homeDirectory`	○	`/home/alice`
`loginShell`	-	`/bin/bash`
`userPassword`	-	`{ARGON2}...`

1.11.2 posixGroup エントリの必須属性

属性	必須	例
`objectClass`	○	`posixGroup`
`cn`	○	`developers`
`gidNumber`	○	`20001`
`memberUid`	-	`alice`, `bob`

1.11.3 バインド DN に必要な ACL

sssdからLDAPに接続する際にLDAPサーバーのcn=readonlyには以下のACLを設定し、userPassword属性にはanonymous authの権限を付与します。

© 2026 OSSTech 株式会社

```
access to *
  by dn="cn=readonly,dc=example,dc=com" read
  by * break

access to attrs=userPassword
  by self write
  by anonymous auth
  by * none
```