Red Hat Directory Server 12

Red Hat Directory Server 12 リリースノート

Red Hat Directory Server 12 (12.4) に関連する注目すべき機能と更新

Last Updated: 2024-08-02

Red Hat Directory Server 12 Red Hat Directory Server 12 リリースノート

Red Hat Directory Server 12 (12.4) に関連する注目すべき機能と更新

法律上の通知

概要

Red Hat Directory Server 12 で実装された改良点および追加機能について説明します。これには、主なバグ修正、既知の問題、テクノロジープレビュー、非推奨になった機能、およびこのリリースに関するその他の詳細が含まれます。

目次

RED HAT DIRECTORY SERVER に関するフィードバックの提供

Red Hat のドキュメントおよび製品に関するご意見をお待ちしております。ドキュメントの改善点があればお知らせください。これを行うには、以下を行います。

- Jira を通じて Red Hat Directory Server ドキュメントに関するフィードバックを送信する場合 (アカウントが必要):
  1. Red Hat Issue Tracker にアクセスしてください。
  2. **Summary** フィールドにわかりやすいタイトルを入力します。
  3. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも追加してください。
  4. ダイアログの下部にある **Create** をクリックします。
- Jira を通じて Red Hat Directory Server 製品に関するフィードバックを送信する場合 (アカウントが必要):
  1. Red Hat Issue Tracker にアクセスしてください。
  2. **Create Issue** ページで、**Next** をクリックします。
  3. **Summary** フィールドに入力します。
  4. **Component** フィールドでコンポーネントを選択します。
  5. **Description** フィールドに以下の内容を入力します。
     a. 選択したコンポーネントのバージョン番号。
     b. 問題を再現するための手順、または改善のための提案。
  6. **Create** をクリックします。

第1章 全般情報

マイナーバージョンに関係なく、Red Hat Directory Server 12 に関する一般的な情報について説明します。

1.1. DIRECTORY SERVER のサポートポリシーとライフサイクル

詳細は Red Hat Directory Server のエラータサポートポリシー を参照してください。

1.2. ソフトウェアの競合

Red Hat Enterprise Linux Identity Management (IdM) サーバーがインストールされているシステムに Directory Server をインストールすることはできません。同様に、Directory Server インスタンスを持つシステムには Red Hat Enterprise Linux IdM サーバーをインストールできません。

1.3. DIRECTORY SERVER 12 への移行

- Directory Server 11 を Directory Server 12 に移行する手順は、Directory Server 11 から Directory Server 12 への移行 の章を参照してください。
- Directory Server 10 を Directory Server 12 に移行する手順は、Directory Server 10 から Directory Server 12 への移行 の章を参照してください。

1.4. DIRECTORY SERVER 12 への移行に関する注意事項

Directory Server 12 のデフォルトのパスワードストレージスキームは PBKDF2-SHA512です。

Directory Server 12 は、デフォルトのパスワードストレージスキームとして **PBKDF2-SHA512** スキームを使用します。これは、**SSHA**、**SSHA512**、およびその他のスキームよりも安全です。したがって、**freeradius** などの一部のアプリケーションが **PBKDF2-SHA512** スキームをサポートしておらず、強度の弱いパスワード保存スキームを設定し直す必要がある場合は、アプリケーションがユーザーエントリーを追加または変更したときだけでなく、バインド操作が成功したときも、Directory Server がユーザーパスワードを更新する点に注意してください。ただし、**cn=config** エントリーの **nsslapd-enable-upgrade-hash** パラメーターを **off** に設定すると、バインド操作で更新を無効にできます。

Directory Server 11 を起動する新しいコマンドラインユーティリティー

バージョン 11 以降、Directory Server には、サーバーインスタンスとユーザーを管理するための新しいコマンドラインユーティリティーが用意されています。これらのユーティリティーは、Directory Server 10 およびそれ以前のバージョンで管理タスクに使用される Perl スクリプトに代わるものです。

以前のバージョンのコマンドと、Directory Server 12 における代替コマンドは、**Red Hat Directory Server インストールガイド**の付録 Red Hat Directory Server 11 で置き換えられたコマンドラインユーティリティー を参照してください。

重要

Directory Server 10 以前のバージョンの管理タスクに使用される Perl スクリプトは、**389-ds-base-legacy-tools** パッケージで引き続き利用できます。ただし、Red Hat は、新しいコマンドラインユーティリティーの **dsconf**、**dsctl**、**dscreate**、および **dsidm** のみをサポートします。

第2章 ハードウェア要件

ハードウェア要件は、次の前提条件で実行されたテストに基づいています。

- サーバーはデフォルトのインデックスを使用します。
- 各 LDAP エントリーのサイズは 1.5 KB で、30 以上の属性があります。

ディスク領域

次の表に、エントリー数に基づいた Directory Server の推奨ディスク容量のガイドラインを示します。

表2.1 必要なディスク容量

エントリー数	データベースのサイズ	データベースキャッシュ	サーバーとログ	総ディスク容量
10,000 - 500,000	2 GB	2 GB	4 GB	**8 GB**
500,000 - 1,000,000	5 GB	2 GB	4 GB	**11 GB**
1,000,000 - 5,000,000	21 GB	2 GB	4 GB	**27 GB**
5,000,000 - 10,000,000	42 GB	2 GB	4 GB	**48 GB**

総ディスク容量には、バックアップおよびレプリケーションメタデータ用の容量は含まれません。レプリケーションを有効にすると、そのメタデータは合計ディスク容量の最大 10% を必要とする場合があります。

100 万の変更があるレプリケーション changelog では、合計ディスク容量要件に少なくとも 315 MB が追加される可能性があります。

/dev/shm/ にマウントされた一時ファイルシステム (tmpfs) には、RHDS 一時ファイルを格納するために少なくとも 4 GB の空き容量が必要です。

必要な RAM

データベース全体をキャッシュに保持するのに十分な RAM がシステムにあることを確認してください。サーバーの設定と使用パターンによっては、必要な RAM サイズが推奨サイズよりも大きくなる場合があります。

表2.2 必要な RAM サイズ

エントリー数	エントリーキャッシュ	レプリケーション付きエントリーキャッシュ [a]	データベースキャッシュ	DN キャッシュ	NDN キャッシュ	合計 RAM サイズ [b]
10,000 - 500,000	4 GB	5 GB	1.5 GB	45 MB	160 MB	**7 GB**
500,000 - 1,000,000	8 GB	10 GB	1.5 GB	90 MB	320 MB	**12 GB**
1,000,000 - 5,000,000	40 GB	50 GB	1.5 GB	450 MB	1.6 GB	**54 GB**
5,000,000 - 10,000,000	80 GB	100 GB	1.5 GB	900 MB	3.2 GB	**106 GB**

[a] レプリケーション付きエントリーキャッシュには、エントリーのレプリケーション状態とメタデータが含まれます。

[b] 合計 RAM サイズは、レプリケーションが有効になっていることを前提としています。

第3章 ソフトウェア要件

Directory Server でサポートされるプラットフォーム

Red Hat は、以下のプラットフォームで実行される場合、Red Hat Directory Server をサポートします。

- Red Hat Enterprise Linux 9.4 上で実行される Red Hat Directory Server 12.4。
- Red Hat Enterprise Linux 9.3 上で実行される Red Hat Directory Server 12.3。
- Red Hat Enterprise Linux 9.2 上で実行される Red Hat Directory Server 12.2。
- Red Hat Enterprise Linux 9.1 上で実行される Red Hat Directory Server 12.1。
- Red Hat Enterprise Linux 9.0 上で実行される Red Hat Directory Server 12.0。
- Red Hat Enterprise Linux は、**AMD64** および **Intel 64** アーキテクチャー向けに構築されています。
- 認定済みのハイパーバイザー上で実行される Red Hat Enterprise Linux 仮想ゲスト。詳細は、ナレッジベースソリューション Red Hat Enterprise Linux の実行が認定されているハイパーバイザー を参照してください。

Web コンソールの Directory Server ユーザーインターフェイスでサポートされているプラットフォーム

Red Hat は、以下の環境の Web コンソールでブラウザーベースの Directory Server ユーザーインターフェイスをサポートします。

オペレーティングシステム	ブラウザー
Red Hat Enterprise Linux 9.4	• Mozilla Firefox 115 以降 • Chrome 88 以降
Windows Server 2016 および 2019:	• Mozilla Firefox 115 以降 • Chrome 88 以降
Windows 10	• Mozilla Firefox 115 以降 • Microsoft Edge 88 以降 • Chrome 88 以降

Windows Synchronization ユーティリティーでサポートされるプラットフォーム

Red Hat は、以下で実行される Active Directory 用の Windows 同期ユーティリティーをサポートしています。

- Microsoft Windows Server 2019

- Microsoft Windows Server 2016

第4章 RED HAT DIRECTORY SERVER 12.4

Directory Server 12.4 に実装された重要な更新と新機能、既知の問題、バグ修正について説明します。

4.1. 389-DS-BASE パッケージの重要な更新と新機能

389-ds-base パッケージに含まれる Red Hat Directory Server 12.4 の重要な更新は、Red Hat Enterprise Linux 9.4 リリースノートに記載されています。

- **389-ds-base** がバージョン 2.4.5 にリベース
- **ns-slapd** プロセスでは、Transparent Huge Pages がデフォルトで無効になりました
- 新しい **lastLoginHistSize** 設定属性が Account Policy プラグインで利用できるようになりました
- MFA バインドを識別する、アクセスログ内の新しい **notes=M** メッセージ
- 新しい **inchainMatch** マッチングルールが利用可能になる
- HAProxy プロトコルが **389-ds-base** パッケージでサポートされるようになる

4.2. バグ修正

Red Hat Directory Server 12.4 で修正された、ユーザーに重大な影響を与えるバグについて説明します。

Directory Server はエントリーキャッシュをフラッシュする頻度を減らしている

以前は、Directory Server は必要のない場合でもエントリーキャッシュをフラッシュしていました。その結果、特定の状況では、Directory Server が応答しなくなり、パフォーマンスが低下しました。この更新により、Directory Server は必要な場合にのみエントリーキャッシュをフラッシュするようになりました。

(BZ#2234613)

attributeTypes が追加されても、Web コンソールで属性名が小文字に変更されなくなる

以前は、Web コンソールを使用してオブジェクトクラスに属性を追加すると、属性名の大文字が小文字に変更されていました。この更新により、属性名の大文字と小文字は変更されなくなりました。

(BZ#2236181)

389-ds-base パッケージに含まれている Directory Server 12.4 バグ修正は、Red Hat Enterprise Linux 9.4 リリースノートに記載されています。

- ページ結果検索を中止した後に Directory Server が失敗しなくなりました
- **nsslapd-numlisteners** 属性値が 2 より大きい場合、Directory Server は失敗しなくなる
- 自動バインド操作が、他の接続で実行される操作に影響を与えなくなる

4.3. 既知の問題

Directory Server 12.4 の既知の問題と、該当する場合は回避策について説明します。

Directory Server Web コンソールは、Web コンソール外で変更された設定を自動的に更新しません。

Red Hat Enterprise Linux 8 Web コンソールの Directory Server モジュールの設計により、コンソールのウィンドウの外部で設定を変更しても、Web コンソールには自動的に最新の設定が表示されません。たとえば、Web コンソールが開いている間にコマンドラインを使用して設定を変更すると、Web コンソールで新しい設定が自動的に更新されません。これは、別のコンピューターの Web コンソールを使用して設定を変更する場合でも当てはまります。

この問題を回避するには、コンソールのウィンドウ外部で設定が変更された場合は、ブラウザーで Web コンソールを手動で更新します。

(BZ#1654281) (BZ#1751047)

Directory Server は、/var/lib/dirsrv/slapd-instance_name/ldif/ からのみ LDIF ファイルをインポート可能

RHEL 8.3 以降、Red Hat Directory Server (RHDS) は独自のプライベートディレクトリーを使用し、LDAP サービスに対して **PrivateTmp** systemd ディレクティブがデフォルトで有効になっています。その結果、RHDS は、**/var/lib/dirsrv/slapd-instance_name/ldif/** ディレクトリーからのみ LDIF ファイルをインポートできます。LDIF ファイルが **/var/tmp**、**/tmp**、**/root** などの別のディレクトリーに保存されている場合、インポートは次のようなエラーで失敗します。

```
Could not open LDIF file "/tmp/example.ldif", errno 2 (No such file or directory)
```

この問題を回避するには、以下の手順を実行します。

1. LDIF ファイルを **/var/lib/dirsrv/slapd-instance_name/ldif/** ディレクトリーに移動します。

   ```
   # mv /tmp/example.ldif /var/lib/dirsrv/slapd-instance_name__/ldif/
   ```

2. **dirsrv** ユーザーがファイルを読み取れるようにする権限を設定します。

   ```
   # chown dirsrv /var/lib/dirsrv/slapd-instance_name/ldif/example.ldif
   ```

3. SELinux コンテキストを復元します。

   ```
   # restorecon -Rv /var/lib/dirsrv/slapd-instance_name/ldif/
   ```

詳細については、ソリューション記事 LDAP サービスがホストの /tmp および /var/tmp ディレクトリーにあるファイルにアクセスできない を参照してください。

(BZ#2075525)

389-ds-base パッケージの既知の問題

389-ds-base packages に影響する Red Hat Directory Server 12.4 の既知の問題は、Red Hat Enterprise Linux 9.4 リリースノートに記載されています。

- オンラインバックアップとオンライン自動メンバーシップ再ビルドタスクは、2 つのロックを取得し、デッドロックを引き起こす可能性があります。

第5章 RED HAT DIRECTORY SERVER 12.3

Directory Server 12.3 に実装された新しいシステム要件、主な更新および新機能、既知の問題、および非推奨の機能について説明します。

5.1. 重要な更新および新機能

Red Hat Directory Server 12.3 の新機能と重要な更新について説明します。

Directory Server は、設定ファイル、証明書データベース、カスタムスキーマファイルをバックアップするように

以前は、Directory Server はデータベースのみをバックアップしていました。この更新により、**dsconf backup create** または **dsctl db2bak** コマンドを実行すると、Directory Server は **/etc/dirsrv/slapd-instance_name/** に保存されている設定ファイル、証明書データベース、およびカスタムスキーマファイルも、バックアップのデフォルトディレクトリー **/var/lib/dirsrv/slapd-instance_name/bak/config_files/** にバックアップします。

Web コンソールを使用してバックアップを実行する場合も、Directory Server はこれらのファイルをバックアップします。

(BZ#2147446)

Alias Entries プラグインが Directory Server で使用できるように

Alias Entries プラグインを有効にした場合、エントリーを検索すると、エイリアス化エントリーとして設定したエントリーが返されます。たとえば、Example 社の従業員である Barbara Jensen が結婚し、姓が変わったとします。彼女の古いエントリー **uid=bjensen,ou=people,dc=example,dc=com** には、新しいエントリー **uid=bsmith,ou=people,dc=example,dc=com** へのエイリアスが含まれています。プラグインが有効になっている場合、エントリー **uid=bjensen,ou=people,dc=example,dc=com** を検索すると、エントリー **uid=bsmith,ou=people,dc=example,dc=com** の情報が返されます。

エイリアスを持つエントリーを取得するには、**ldapsearch** コマンドの **-a find** パラメーターを使用します。

現在、**Alias Entries** プラグインは **ベース** レベルの検索のみをサポートしています。

詳細は、Alias Entries プラグイン の説明を参照してください。

(BZ#2203173)

checkAllStateAttrs 設定オプションが利用可能に

checkAllStateAttrs 設定を使用してユーザーの認証時に、アカウントのステータス (アクティブかどうか)、またパスワードの有効期限の両方を適用できます。このパラメーターを有効にすると、主な状態属性をチェックし、アカウント情報が正しい場合は、別の状態属性を確認します。

(BZ#2174161)

Directory Server Web コンソールを使用して、レプリケーションレポートの認証情報とエイリアスを保存できるように

以前は、Web コンソールを使用してレプリケーション監視レポートの認証情報とエイリアスを設定した場合、Web コンソールをリロードするとこれらの設定は消えていました。この機能拡張により、レプリケーションレポートの認証情報とエイリアスを設定すると、Directory Server は新しい設定を **.dsrc** ファイルに保存し、Web コンソールはリロード後に、保存された設定をアップロードします。

(BZ#2030884)

389-ds-base パッケージの重要な更新と新機能

389-ds-base パッケージに含まれている Directory Server 12.3 機能は、Red Hat Enterprise Linux 9.3 リリースノートに記載されています。

- RHEL 9.3 は 389-ds-base 2.3.4 を提供する
- **bind** 操作が失敗した場合、Directory Server がクライアント接続を閉じることができるようになる
- Automembership プラグインの改善。デフォルトではグループをクリーンアップしなくなる
- 新しい **passwordAdminSkipInfoUpdate: on/off** 設定オプションが利用可能になる
- 新しい **slapi_memberof()** プラグイン関数が Directory Server プラグインおよびクライアントアプリケーションで使用できるようになる
- Directory Server は、仮想属性 **nsRole** を、マネージドロールとフィルターされたロールのインデックス付き属性に置き換えるようになる
- 新しい **nsslapd-numlisteners** 設定オプションが利用可能になる

5.2. バグ修正

Red Hat Directory Server 12.3 で修正された、ユーザーに重大な影響を与えるバグについて説明します。

cockpit-389-ds パッケージのアップグレードにより、389-ds-base および python3-lib389 パッケージが更新されるように

以前は、**cockpit-389-ds** パッケージは、依存する **389-ds-base** パッケージのバージョンを指定していませんでした。その結果、**cockpit-389-ds** パッケージをアップグレードするだけでは **389-ds-base** および **python3-lib389** パッケージが更新されず、パッケージ間の不整合や互換性の問題が発生する可能性がありました。この更新により、**cockpit-389-ds** パッケージは **389-ds-base** の特定のバージョンに依存するようになり、**cockpit-389-ds** パッケージの更新により **389-ds-base** および **python3-lib389** パッケージもアップグレードされるようになりました。

(BZ#2240021)

コンシューマーでレプリケーションを無効にしてもサーバーがクラッシュしなくなる

以前は、コンシューマーサーバーでレプリケーションを無効にすると、Directory Server はコンシューマー上で存在しない変更ログを削除しようとしていました。その結果、サーバーは次のエラーで予期せず終了していました。

```
Error: -1 - Can't contact LDAP server - []
```

この更新により、コンシューマーでのレプリケーションの無効化が期待どおりに機能するようになりました。

(BZ#2184599)

非 root インスタンスの作成後に起動に失敗しなくなる

以前は、非 root インスタンスのテンプレートで Rust プラグインが誤って無効になり、デフォルトのパ

スワードスキームが Rust ベースの hasher に移動していました。その結果、非 root インスタンスを作成できませんでした。この更新により、非 root インスタンスが Rust プラグインをサポートし、PBKDF2-SHA512 デフォルトパスワードスキームを使用してインスタンスを作成できるようになりました。

(BZ#2151864)

dsconf ユーティリティーが、ハブまたは consumer ロールを設定するときに replica-id として値 65535 のみを受け入れるように

以前は、ハブまたは consumer ロールを設定するときに、**dsconf** ユーティリティーは **65535** 以外の値の **replica-id** オプションも受け入れていました。この更新により、**dsconf** ユーティリティーは、ハブまたは consumer ロールの **replica-id** 値として **65535** のみを受け入れます。**dsconf** コマンドでこの値を指定しない場合、Directory Server は **replica-id** 値として **65535** を自動的に割り当てます。

(BZ#1987373)

dscreate ds-root コマンドでパスが正規化されるように

以前は、非 root ユーザーの下でインスタンスを作成し、末尾にスラッシュを含む **bin_dir** 引数値を指定すると、**dscreate ds-root** は **$PATH** 変数で **bin_dir** 値を見つけることができませんでした。その結果、非 root ユーザーのインスタンスは作成されませんでした。今回の更新により、**dscreate ds-root** コマンドでパスが正規化され、インスタンスが期待どおりに作成されるようになりました。

(BZ#2151868)

dsconf ユーティリティーに、entryUUID プラグインの修正タスクを作成するための fixup オプションが追加される

以前は、**dsconf** ユーティリティーでは、**entryUUID** プラグインの修正タスクを作成するオプションを提供していませんでした。その結果、管理者は **dsconf** を使用して、**entryUUID** 属性を既存のエントリーに自動的に追加するタスクを作成することができませんでした。この更新により、**dsconf** ユーティリティーで **fixup** オプションを使用して、**entryUUID** プラグインの修正タスクを作成できるようになりました。たとえば、**dn=example,dc=com** エントリーの下の、**uid** 属性を含むすべてのエントリーを修正するには、次のように入力します。

```
# dsconf instance_name plugin entryuuid fixup -f “(uid=*)” “dn=example,dc=com"
```

(BZ#2047175)

FIPS モードで Directory Server をインストールする際に、アクセスログにエラーメッセージが表示されなくなる

以前は、Directory Server を FIPS モードでインストールすると、アクセスログファイルに次のエラーメッセージが表示されていました。

```
[time_stamp]
- WARN - slapd_do_all_nss_ssl_init - ERROR: TLS is not enabled, and the
machine is in FIPS mode. Some functionality won’t work correctly (for
example, users with PBKDF2_SHA256 password scheme won’t be able to log
in). It’s highly advisable to enable TLS on this instance.
```

今回の更新でこの問題は修正され、アクセスログにエラーメッセージが表示されなくなりました。

(BZ#2153668)

389-ds-base パッケージに含まれている Directory Server 12.3 バグ修正は、Red Hat Enterprise Linux 9.3 リリースノートに記載されています。

- 通常のユーザーによるページ検索はパフォーマンスに影響を与えなくなる
- LMDB インポートがより高速に動作するようになる
- スキーマのレプリケーションが Directory Server で正しく機能するようになる
- Directory Server で referral モードが正しく動作するようになる
- 再起動後に **dirsrv** サービスが正しく開始されるようになる
- セキュリティーパラメーターの変更が正しく機能するようになる

5.3. 既知の問題

Directory Server 12.3 の既知の問題と、該当する場合は回避策について説明します。

Directory Server は、/var/lib/dirsrv/slapd-instance_name/ldif/ からのみ LDIF ファイルをインポート可能

RHEL 8.3 以降、Red Hat Directory Server (RHDS) は独自のプライベートディレクトリーを使用し、LDAP サービスに対して **PrivateTmp** systemd ディレクティブがデフォルトで有効になっています。その結果、RHDS は、**/var/lib/dirsrv/slapd-instance_name/ldif/** ディレクトリーからのみ LDIF ファイルをインポートできます。LDIF ファイルが **/var/tmp**、**/tmp**、**/root** などの別のディレクトリーに保存されている場合、インポートは次のようなエラーで失敗します。

```
Could not open LDIF file "/tmp/example.ldif", errno 2 (No such file or directory)
```

この問題を回避するには、以下の手順を実行します。

1. LDIF ファイルを **/var/lib/dirsrv/slapd-instance_name/ldif/** ディレクトリーに移動します。

   ```
   # mv /tmp/example.ldif /var/lib/dirsrv/slapd-instance_name__/ldif/
   ```

2. **dirsrv** ユーザーがファイルを読み取れるようにする権限を設定します。

   ```
   # chown dirsrv /var/lib/dirsrv/slapd-instance_name/ldif/example.ldif
   ```

3. SELinux コンテキストを復元します。

   ```
   # restorecon -Rv /var/lib/dirsrv/slapd-instance_name/ldif/
   ```

詳細については、ソリューション記事 LDAP サービスがホストの /tmp および /var/tmp ディレクトリーにあるファイルにアクセスできない を参照してください。

(BZ#2075525)

389-ds-base パッケージの既知の問題

389-ds-base packages に影響する Red Hat Directory Server 12.3 の既知の問題は、Red Hat Enterprise Linux 9.3 リリースノートに記載されています。

- **nsslapd-numlisteners** 属性値が 2 より大きい場合、Directory Server が失敗する

5.4. 非推奨になった機能

Red Hat Directory Server 12.3 で非推奨となった機能について説明します。

389-ds-base パッケージの非推奨機能

389-ds-base パッケージで非推奨となった Directory Server 12.3 の機能は、Red Hat Enterprise Linux 9.3 リリースノートに記載されています。

- **nsslapd-ldapimaprootdn** パラメーターが非推奨になる

5.5. 削除された機能

Red Hat Directory Server 12.3 で削除された機能について説明します。

389-ds-base パッケージの削除された機能

Red Hat Directory Server の **389-ds-base** パッケージから削除された機能は、Red Hat Enterprise Linux 9.3 リリースノートに記載されています。

- **nsslapd-conntablesize** 設定パラメーターが **389-ds-base** から削除される

第6章 RED HAT DIRECTORY SERVER 12.2

Directory Server 12.2 に実装された新しいシステム要件、主な更新および新機能、既知の問題、および非推奨の機能について説明します。

6.1. 重要な更新および新機能

Red Hat Directory Server 12.2 の新機能と重要な更新について説明します。

Directory Server 12.2 はアップストリームバージョン 2.2.7 にリベースされる

Directory Server 12.2 は、アップストリームバージョン 2.2.7 をベースとしており、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。主な変更点の包括的なリストについては、更新する前に、リリースノート https://directory.fedoraproject.org/docs/389ds/releases/release-2-2-1.html https://directory.fedoraproject.org/docs/389ds/releases/release-2-2-2.html https://directory.fedoraproject.org/docs/389ds/releases/release-2-2-3.html https://directory.fedoraproject.org/docs/389ds/releases/release-2-2-4.html https://directory.fedoraproject.org/docs/389ds/releases/release-2-2-5.html https://directory.fedoraproject.org/docs/389ds/releases/release-2-2-6.html https://directory.fedoraproject.org/docs/389ds/releases/release-2-2-7.html を参照してください。

dsconf ユーティリティーで、タスクのタイムアウトを設定できるようになりました。

以前のリリースでは、タスクが 4 分以上かかると、**dsconf** は以下のメッセージを返していました。

```
DEBUG: The backup create task has failed with the error code: (None)
...
```

今回の機能拡張により、**--timeout** オプションを使用して、タスクに必要なタイムアウトを設定できるようになりました。タイムアウトによってタスクは停止されませんが、**dsconf** ユーティリティーによるタスクの結果の待機は停止します。

(BZ#1993124)

Web コンソールを使用して、証明書をインポートおよびエクスポートできるようになりました。

以前のバージョンでは、Web コンソールを使用してサーバーファイルシステムのファイルから証明書をインポートできませんでした。今回のリリースでは、**base64**でエンコードされた証明書をコピーしてファイルをインポートすることもできます。さらに、認証局とサーバー証明書をエクスポートすることもできます。

(BZ#1751264)

389-ds-base パッケージの重要な更新と新機能

389-ds-base パッケージに含まれている Directory Server 12.2 機能は、Red Hat Enterprise Linux 9.2 リリースノートに記載されています。

- Directory Server が TLS の ECDSA 秘密キーをサポートするようになりました。
- Directory Server が検索操作の拡張ログをサポートするようになりました。
- NUNC_STANS エラーログレベルは、新しい **1048576** ログレベルに置き換えられました
- Directory Server ではセキュリティーログが導入されています。

- Directory Server でアーカイブされたログファイルを圧縮できるようになりました。
- デフォルトの動作の変更: Directory Server が、データベース追加時とまったく同じスペルの DN を返すようになりました。
- Directory Server 監査ログ用の新しい **nsslapd-auditlog-display-attrs** 設定パラメーター
- 新しい **pamModuleIsThreadSafe** 設定オプションが利用可能になりました
- Directory Server が証明書バンドルをインポートできるようになりました。

6.2. バグ修正

Red Hat Directory Server 12.2 で修正された、ユーザーに重大な影響を与えるバグについて説明します。

389-ds-base パッケージに含まれている Directory Server 12.2 バグ修正は、Red Hat Enterprise Linux 9.2 リリースノートに記載されています。

- Directory Server レプリケーションマネージャーアカウントのパスワード変更が正しく機能するようになりました
- **db_dir** パラメーターを含むカスタムパスを使用する場合は、**dscreate** ユーティリティーが正しく動作するようになりました

6.3. 既知の問題

Directory Server 12.2 の既知の問題と、該当する場合の回避策について説明します。

Directory Server は、/var/lib/dirsrv/slapd-instance_name/ldif/ からのみ LDIF ファイルをインポート可能

RHEL 8.3 以降、Red Hat Directory Server (RHDS) は独自のプライベートディレクトリーを使用し、LDAP サービスに対して **PrivateTmp** systemd ディレクティブがデフォルトで有効になっています。その結果、RHDS は、**/var/lib/dirsrv/slapd-instance_name/ldif/** ディレクトリーからのみ LDIF ファイルをインポートできます。LDIF ファイルが **/var/tmp**、**/tmp**、**/root** などの別のディレクトリーに保存されている場合、インポートは次のようなエラーで失敗します。

```
Could not open LDIF file "/tmp/example.ldif", errno 2 (No such file or directory)
```

この問題を回避するには、以下の手順を実行します。

1. LDIF ファイルを **/var/lib/dirsrv/slapd-instance_name/ldif/** ディレクトリーに移動します。

   ```
   # mv /tmp/example.ldif /var/lib/dirsrv/slapd-instance_name__/ldif/
   ```

2. **dirsrv** ユーザーがファイルを読み取れるようにする権限を設定します。

   ```
   # chown dirsrv /var/lib/dirsrv/slapd-instance_name/ldif/example.ldif
   ```

3. SELinux コンテキストを復元します。

   ```
   # restorecon -Rv /var/lib/dirsrv/slapd-instance_name/ldif/
   ```

詳細については、ソリューション記事 LDAP サービスがホストの /tmp および /var/tmp ディレクトリーにあるファイルにアクセスできない を参照してください。

(BZ#2075525)

FIPS モードでの Directory Server のインストール時にアクセスログにエラーメッセージが表示されます。

FIPS モードで Directory Server をインストールすると、アクセスログファイルに次のエラーメッセージが表示されます。

```
[time_stamp]
- WARN - slapd_do_all_nss_ssl_init - ERROR: TLS is not enabled, and the
machine is in FIPS mode. Some functionality won't work correctly (for
example, users with PBKDF2_SHA256 password scheme won't be able to log
in). It's highly advisable to enable TLS on this instance.
```

このような動作が発生するのは、Directory Server により、まず、TLS が初期化されていないことが検出され、エラーメッセージが記録されるためです。ただし、後で **dscreate** ユーティリティーが TLS の初期化を完了し、セキュリティーを有効にすると、エラーメッセージは表示されなくなります。

(BZ#2153668)

389-ds-base パッケージの既知の問題

389-ds-base パッケージ に影響する Red Hat Directory Server 12.2 の既知の問題は、Red Hat Enterprise Linux 9.2 リリースノートに記載されています。

- **dsconf** ユーティリティーには、**entryUUID** プラグインの修正タスクを作成するオプションがない。
- Directory Server で接尾辞の referral の設定に失敗する。
- referral mode で起動すると、Directory Server が予期せず終了する

6.4. 非推奨になった機能

Red Hat Directory Server 12.2 で非推奨となった機能について説明します。

389-ds-base パッケージの非推奨機能

389-ds-base パッケージで非推奨となった Directory Server 12.2 機能は、Red Hat Enterprise Linux 9.2 リリースノートに記載されています。

- **nsslapd-idlistscanlimit** パラメーターは非推奨となり、デフォルト値が変更されました

第7章 RED HAT DIRECTORY SERVER 12.1

Directory Server 12.1 に実装された新しいシステム要件、主な更新および新機能、既知の問題、および非推奨の機能について説明します。

7.1. 主な更新と新機能

このセクションでは、Directory Server 12.1 の新機能と重要な更新について説明します。

Directory Server 12.1 はアップストリームバージョン 2.1.3 にリベースされる

Directory Server 12.1 は、アップストリームバージョン 2.1.3 に基づいており、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。主な変更点の一覧については、更新前にアップストリームのリリースノートを参照してください。

- https://directory.fedoraproject.org/docs/389ds/releases/release-2-1-0.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-1-1.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-1-3.html

LDAP ブラウザーへの完全対応

この機能拡張により、Web コンソールの **LDAP Browser** タブから LDAP エントリーを管理できます。たとえば、以下を行うことができます。

- **ツリー** ビューまたは **テーブル** ビューを使用してディレクトリーを参照します。
- ユーザー、グループ、組織単位 (OU)、カスタムエントリーなどのエントリーを管理します。
- アクセス制御命令 (ACI) を管理します。
- サービス定義 (CoS) のクラスを管理します。
- エントリーを検索します。

389-ds-base パッケージで特記すべき更新と新機能

389-ds-base パッケージに含まれている Red Hat Directory Server の機能は、Red Hat Enterprise Linux 9.1 リリースノートに記載されています。

- Directory Server が **ldapdelete** 使用時の再帰的な削除操作に対応
- Directory Server インストール時における基本的な複製オプションの設定に対応
- Directory Server が Auto Membership プラグインタスクのキャンセルに対応
- Directory Server は、root 以外のユーザーによるインスタンスの作成をサポート
- Directory Server でレプリケーション changelog のトリミングがデフォルトで有効化

7.2. 既知の問題

このセクションでは、Directory Server 12.1 の既知の問題と、該当する場合の回避法について説明します。

Directory Server は、/var/lib/dirsrv/slapd-instance_name/ldif/ からのみ LDIF ファイルをインポート可能

dsconf backend import コマンドでは、インポートする LDIF ファイルへのパスを指定する必要があります。ただし、ファイルシステムと SELinux のアクセス許可、およびその他のオペレーティングシステムの制限により、Directory Server は **/var/lib/dirsrv/slapd-instance_name/ldif/** ディレクトリーからのみ LDIF ファイルをインポートできます。LDIF ファイルが別のディレクトリーに保存されている場合、インポートは次のようなエラーで失敗します。

```
Could not open LDIF file "/tmp/example.ldif", errno 2 (No such file or directory)
```

この問題を回避するには、以下を実行します。

1. ファイルを /var/lib/dirsrv/slapd-**instance_name**/ldif/ ディレクトリーに移動します。

```
# mv /tmp/example.ldif /var/lib/dirsrv/slapd-instance_name/ldif/
```

2. **dirsrv** ユーザーがファイルを読み取れるようにする権限を設定します。

```
# chown dirsrv /var/lib/dirsrv/slapd-instance_name/ldif/example.ldif
```

3. SELinux コンテキストを復元します。

```
# restorecon -Rv /var/lib/dirsrv/slapd-instance_name/ldif/
```

(BZ#2081352)

レプリケーションマネージャーアカウントのパスワードを変更した後に Directory Server のレプリケーションに失敗する

Directory Server では、パスワード変更後に、レプリカ合意のパスワードキャッシュが適切に更新されません。そのため、レプリケーションマネージャーアカウントのパスワードを変更すると、レプリケーションが破損します。この問題を回避するには、Directory Server インスタンスを再起動します。その結果、キャッシュは起動時に再ビルドされ、レプリケーション接続は古いパスワードではなく新しいパスワードにバインドします。

(BZ#1956987)

389-ds-base パッケージの既知の問題

389-ds-base パッケージに含まれている Red Hat Directory Server の既知の問題は、Red Hat Enterprise Linux 9.1 リリースノートに記載されています。

- **dsconf** ユーティリティーには、**entryUUID** プラグインの修正タスクを作成するオプションがない。
- Directory Server で接尾辞の referral の設定に失敗する。
- referral mode で起動すると、Directory Server が予期せず終了する

389-ds-base パッケージの非推奨機能

389-ds-base パッケージから削除された Red Hat Directory Server の非推奨機能については、Red Hat Enterprise Linux 9.1 リリースノートに記載されています。

- **-h** および **-p** オプションは、OpenLDAP クライアントユーティリティーで廃止されました。

第8章 RED HAT DIRECTORY SERVER 12.0

このセクションでは、前提条件やプラットフォーム要件など、Directory Server 12.0 のインストールに関連する情報について説明します。

8.1. 主な更新と新機能

このセクションでは、Directory Server 12.0 の新機能と重要な更新について説明します。

Directory Server 12.0 は、アップストリームバージョン 2.0.14 をベースとする

Directory Server 12.0 は、アップストリームバージョン 2.0.14 をベースとしており、以前のバージョンに比べて多くのバグ修正と機能拡張が提供されています。主な変更点の一覧については、更新前にアップストリームのリリースノートを参照してください。

- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-14.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-13.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-12.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-11.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-10.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-9.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-8.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-7.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-6.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-5.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-4.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-3.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-2.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-1.html

389-ds-base パッケージで特記すべき更新と新機能

389-ds-base パッケージに含まれている Red Hat Directory Server の機能は、Red Hat Enterprise Linux 9.0 リリースノートに記載されています。

- Directory Server はグローバル changelog を使用しなくなりました
- Directory Server が、**tmpfs** ファイルシステムのデータベースのメモリーマッピングされたファイルを保存するようになりました

8.2. バグ修正

このセクションでは、Directory Server 12.0 で修正された、ユーザーに重大な影響を与えるバグについて説明します。

エントリーキャッシュ設定の手動による変更が、Web コンソールで正しく機能するようになる

デフォルトでは、Directory Server は自動キャッシュチューニングを使用します。ただし、以前は、Web コンソールで自動キャッシュ調整設定を無効にして、目的のエントリーキャッシュ設定を手動で設定することはできませんでした。この更新により問題が修正され、その結果、Web コンソールでエントリーキャッシュを手動で設定できるようになりました。

Web コンソールのさまざまな部分の誤りを修正

以前は、Web コンソールのさまざまな部分にテキストフィールドの誤りが含まれていました。その結果、誤った情報メッセージがユーザーに表示されました。この更新により問題が修正され、Web コンソールに正しいテキストメッセージが表示されるようになりました。

複数のプラグインの設定変更が、Web コンソールで正しく機能するようになる

以前は、Web コンソールを使用してプラグインの設定を変更しようとすると、誤ったエラーメッセージが表示されるか、読み込みループが消えませんでした。その結果、新しい設定を保存できなかったか、設定が正常に保存されたかどうかがわかりませんでした。次のプラグインが影響を受けていました。

- Posix Winsync プラグイン
- Referential Integrity プラグイン
- RootDN Access Control プラグイン
- Retro Changelog プラグイン

今回の更新でこの問題が修正されています。その結果、Web コンソールを使用してこれらのプラグインを期待どおりに設定できるようになりました。

Changelog のエクスポートが Web コンソールで期待どおりに機能するようになる

以前の Web コンソールでは、デバッグ目的で changelog をエクスポートするときに、**Decode Base64 changes** オプションと **Only Export CSNs** オプションの両方を選択できました。しかし、**Export CSNs** オプションしか考慮されませんでした。このリリースでは、1 つのオプションのみを選択でき、changelog は、選択したオプションに従って期待どおりにエクスポートされます。

レプリケーショントポロジーレポートのクレデンシャルと命名エイリアスの設定が、Web コンソールで正しく機能するようになる

以前は、ポップアップウィンドウの **Add Report Credentials** と **Add Report Alias** のフィールドに書き込み可能ではなかったため、Web コンソールを使用してレプリケーショントポロジーレポートのクレデンシャルまたは命名エイリアスを設定できませんでした。このリリースでは、ポップアップウィンドウのフィールドは書き込み可能であり、レポートのクレデンシャルを設定したり、期待どおりに命名エイリアスを設定したりできます。

Directory Server コンソールがログ設定値を検証するようになる

以前は、Directory Server Web コンソールは、**Logging** ページのさまざまな種類のログに対して無効な値を受け入れていました。その結果、ユーザーが設定を保存しようとしたときにエラーが発生しました。この更新により、ロギング設定値の検証が追加されます。その結果、Web コンソールは無効な入力を受け入れません。

検索機能を使用した後、Schema ページの属性を編集できなくなる

以前は、Directory Server Web コンソールの **Schema** ページで属性を検索した後、カスケードスタイルシート (CSS) の設定ミスにより、属性が編集可能でした。今回の更新により、編集機能が無効になりました。

DNA プラグインの有効化が失敗しなくなる

以前は、Directory Server Web コンソールで Distributed Numeric Assignment (DNA) プラグインを有効にしようとして失敗し、ブラウザーエラーが発生していました。この更新では、DNA プラグインの有効化が期待どおりに機能します。

アカウントポリシープラグインに設定エントリーを追加しても失敗しなくなる

以前は、アカウントポリシープラグインに設定エントリーを追加しようとすると、エラーが発生して失敗することがありました。この問題を修正するために、この更新では、**Shared Config DN** 値が指定されていない場合は、**Create Config** ボタンが無効になります。

レプリケーションメタデータを含む LDIF ファイルからのインポートが正しく機能するようになる

以前は、レプリケーションメタデータを含む LDIF ファイルをインポートすると、特定の場合にレプリケーションが失敗する可能性がありました。

最初のケースでは、インポートされた LDIF ファイルの接尾辞エントリーの前に配置されたレプリケーション更新ベクトル (RUV) エントリーは無視されました。その結果、ジェネレーション ID の不一致が原因で、インポートされたレプリカを使用したレプリケーションが失敗しました。この更新により、Directory Server はインポートの最後にスキップされた RUV エントリーを確実に書き込みます。

2 番目のケースでは、RUV の不一致後に再初期化された changelog に、開始変更シーケンス番号 (CSN) が含まれていませんでした。その結果、changelog に CSN がないため、インポートされたレプリカを使用したレプリケーションが失敗しました。この更新により、changelog を再初期化するときに、Directory Server が RUV **maxcsn** エントリーを確実に作成します。

その結果、この更新により、管理者は、レプリケーションメタデータを含む LDIF ファイルからインポートした後にレプリケーションを再初期化する必要がなくなります。

389-ds-base パッケージのバグ修正

389-ds-base パッケージに含まれている Red Hat Directory Server のバグ修正は、Red Hat Enterprise Linux 9.0 リリースノートに記載されています。

- PBKDF2 アルゴリズムでハッシュされたパスワードを使用した FIPS モードでの Directory Server への認証が期待どおりに機能するようになる

8.3. テクノロジープレビュー

このセクションでは、Directory Server 12.0 でサポートされていないテクノロジープレビューについて説明します。

Directory Server Web コンソールは、テクノロジープレビューとして LDAP ブラウザーを提供

LDAP ブラウザーが Directory Server Web コンソールに追加されました。Web コンソールの **LDAP Browser** タブを使用すると、次のことができます。

- ディレクトリーを参照する
- ユーザー、グループ、組織単位 (OU)、カスタムエントリーなどのエントリーを管理する
- ACI を管理する

Red Hat は、この機能をサポート対象外のテクノロジープレビューとして提供していることに注意してください。

8.4. 既知の問題

このセクションでは、Directory Server 12.0 の既知の問題と、該当する場合の回避法について説明します。

Directory Server は、/var/lib/dirsrv/slapd-instance_name/ldif/ からのみ LDIF ファイルをインポート可能

dsconf backend import コマンドでは、インポートする LDIF ファイルへのパスを指定する必要があります。ただし、ファイルシステムと SELinux のアクセス許可、およびその他のオペレーティングシステムの制限により、Directory Server は **/var/lib/dirsrv/slapd-instance_name/ldif/** ディレクトリーからのみ LDIF ファイルをインポートできます。LDIF ファイルが別のディレクトリーに保存されている場合、インポートは次のようなエラーで失敗します。

```
Could not open LDIF file "/tmp/example.ldif", errno 2 (No such file or directory)
```

この問題を回避するには、以下を実行します。

1. ファイルを /var/lib/dirsrv/slapd-**instance_name**/ldif/ ディレクトリーに移動します。

```
# mv /tmp/example.ldif /var/lib/dirsrv/slapd-instance_name/ldif/
```

2. **dirsrv** ユーザーがファイルを読み取れるようにする権限を設定します。

```
# chown dirsrv /var/lib/dirsrv/slapd-instance_name/ldif/example.ldif
```

3. SELinux コンテキストを復元します。

```
# restorecon -Rv /var/lib/dirsrv/slapd-instance_name/ldif/
```

レプリケーションマネージャーアカウントのパスワードを変更した後に Directory Server のレプリケーションに失敗する

Directory Server では、パスワード変更後に、レプリカ合意のパスワードキャッシュが適切に更新されません。そのため、レプリケーションマネージャーアカウントのパスワードを変更すると、レプリケーションが破損します。この問題を回避するには、Directory Server インスタンスを再起動します。その結果、キャッシュは起動時に再ビルドされ、レプリケーション接続は古いパスワードではなく新しいパスワードにバインドします。

389-ds-base パッケージの既知の問題

389-ds-base パッケージに含まれている Red Hat Directory Server の既知の問題は、Red Hat Enterprise Linux 9.0 リリースノートに記載されています。

- **dsconf** ユーティリティーには、**entryUUID** プラグインの修正タスクを作成するオプションがない。
- Directory Server で接尾辞の referral の設定に失敗する。
- referral mode で起動すると、Directory Server が予期せず終了する。

8.5. 削除された機能

このセクションでは、Directory Server 12.0 で削除された機能について説明します。

nsslapd-subtree-rename-switch パラメーターが削除される

管理者は以前、データベース内のサブツリー間でエントリーが移動しないように Directory Server を設定できました。安定性の問題により、この機能は削除され、その結果、**nsslapd-subtree-rename-switch** パラメーターは存在しなくなりました。その結果、サブツリー間でのエントリーの移動を無効にすることはできなくなりました。別の方法として、この機能が必要な場合は、アクセス制御命令 (ACI) を作成します。