Red Hat Single Sign-On 7.5

リリースノート

Red Hat Single Sign-On 7.5 向け

Last Updated: 2021-09-27

Red Hat Single Sign-On 7.5 リリースノート

Red Hat Single Sign-On 7.5 向け

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

概要

本ガイドは、Red Hat Single Sign-On のリリースノートとして作成されています。

目次

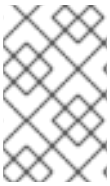
多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、弊社 の CTO、Chris Wright のメッセージを参照してください。

第1章 RED HAT SINGLE SIGN-ON 7.5.0.GA

1.1. 概要

Red Hat は、Red Hat Single Sign-On (RH-SSO) のバージョン 7.5 のリリースを発表します。RH-SSO は Keycloak プロジェクトをベースとしており、OpenID Connect、OAuth 2.0、SAML 2.0 などの一般的な標準仕様に基づいて Web SSO 機能を提供することで、Web アプリケーションのセキュリティーを保護します。RH-SSO サーバーは OpenID Connect または SAML ベースの ID プロバイダー (IdP)として機能し、エンタープライズユーザーディレクトリーまたはサードパーティー IdP が標準仕様ベースのセキュリティートークンを使用してアプリケーションを保護できるようにします。



注記

IBM Z および IBM Power Systems 向けの Red Hat Single Sign-On は、OpenShift 環境でのみサポートされます。IBM Z および IBM Power Systems でのベアメタルインストールはサポートされていません。

以下の注記は RH-SSO 7.5 リリースに適用されます。

1.2. 新機能または改善された機能

1.2.1. financial-grade API、FAPI CIBA、および Open Banking Brasil

Red Hat Single Sign-On サーバーは、Financial-grade API (FAPI) のサポートを提供します。Red Hat Single Sign-On は、OpenID Connect Client Initiated Backchannel Authentication (CIBA) および OpenBanking Brasil に準拠しています。CIBA ping モードにも対応しています。

Red Hat Single Sign-On サーバーがクライアントに対してよりセキュアで FAPI に準拠するように検証するには、FAPI クライアントポリシーを設定します。これらのポリシーにより、クライアントの SSL 要件やリダイレクト URI をセキュアにするセキュリティーのベストプラクティスが確保されます。詳細は、『Securing Applications and Services Guide』の「FAPI」セクションを参照してください。

1.2.2. 新規のアカウントコンソール

これまで User Account Service と呼ばれる Account Console が修正され、Red Hat Single Sign-On のデフォルトのアカウントコンソールになりました。ただし、ユーザーアカウントサービスのカスタムテーマがある場合は、コンソールは本リリースのデフォルトコンソールのままになります。そのため、新しいアカウントコンソールにカスタムのテーマを更新することができます。

新規コンソールは GZip を使用してアーティファクトのダウンロードを最適化します。

1.2.3. ログインテーマを PatternFly 4 にアップグレードします。

Red Hat Single Sign-On ログイン用のテーマのコンポーネントは PatternFly 4 にアップグレードされました。PatternFly 3 は新規バージョンと同時に実行されるため、PatternFly 3 コンポーネントは共存できます。

また、ログインテーマによりユーザーエクスペリエンスが向上します。また、カスタムアイデンティティープロバイダーのアイコンを定義できます。詳細は、『サーバー開発者ガイド』を参照してください。

1.2.4. ユーザーは独自のアカウントを削除できます。

指定のレルムのユーザーは、アカウントコンソールを介して独自のアカウントを削除できます。この機能は、管理コンソールの **Delete Account** アクションによって有効になります。

1.2.5. ID のブローカー同期モード

Identity Brokering Sync Mode では、ユーザープロファイルが初回ログイン時に、または外部 ID プロバイダーからのすべてのログインで更新されるかどうかを制御できます。この動作は、個別のマッパーでも上書きできます。

1.2.6. OpenID Connect / OAuth 2.0 用クライアントセッションタイムアウト

通常、SSO セッションは日数または月間続きますが、個々のクライアントセッションははるかに短くする必要があります。レルム内のすべてのクライアントに対して、個別のクライアントに個別のタイムアウトを設定できるようになりました。

クライアントのオフラインセッションタイムアウトを設定することもできます。これにより、オフラインのトークンの期限が切れ、無効化するまでの最大時間を決定します。

1.2.7. OAuth 2.0 Token Revocation (RFC 7009)

Red Hat Single Sign-On を OAuth 2.0 の承認サーバーとして使用するアプリケーションでは、トークン失効エンドポイントを使用して更新トークンを取り消すことができるようになりました。

1.2.8. OAuth 2.0 Device Authorization Grant (RFC 8628)

OAuth 2.0 Device Authorization Grant (認可グラント) のサポートが利用できるようになりました。

1.2.9. OpenID Connect のバックチャネルログアウト

OpenID Connect Back-Channel Logout のサポートが利用できるようになりました。

1.2.10. オフラインセッションの改善

オフラインセッションのプリロードが改善され、パフォーマンスが向上します。

1.2.11. その他の改善

1.2.11.1. AccessTokenResponse のカスタム要求

カスタムクレームを AccessTokenResponse に追加できるようになりました。これは一般的な拡張機能ですが、米国の規制が含まれるヘルスケアプロバイダー標準をサポートします。

1.2.11.2. アイデンティティーブローカー向け PKCE のサポート

Red Hat Single Sign-On は、外部 OpenID Connect Identity Provider にブローカーを使用する場合に PKCE を活用できるようになりました。

1.2.11.3. User Profile SPI の改良と宣言型設定のサポート

ユーザープロファイルの管理をより容易にするために、ユーザープロファイル SPI が改善されました。これらの改善には、管理コンソールを使用したユーザープロファイルの設定サポートが含まれます。詳細は、『サーバー管理ガイド』を参照してください。

1.2.11.4. クライアント通信へのサーバーの SAML アーティファクトバインディング

Red Hat Single Sign-On は、**SAML アーティファクト** バインディングを使用したクライアントとの通信をサポートするようになりました。クライアント設定で新しい **Force Artifact Binding** オプションが利用できます。アーティファクトメッセージを使用してクライアントとの通信を強制します。詳細は、『サーバー管理ガイド』を参照してください。このバージョンでは、Red Hat Single Sign-On SAML クライアントアダプターはアーティファクトバインディングをサポートしません。

1.2.11.5. デフォルトのロール処理の向上

デフォルトロールは、一般的に **default-roles-<realmName>** という名前が付けられ、新しい複合ロールとして内部に保存されるようになりました。以前のバージョンでは、レルムロールおよびクライアントのデフォルトロールは、Identity Brokering を介してインポートされた新規ユーザーと、ユーザーに直接割り当てられました。ただし、複合ロールはそれらに割り当てられ、他のデフォルトロールは有効なロールとして割り当てられます。この変更により、特に多数のクライアントを使用して、デフォルトのロール処理のパフォーマンスが向上します。すべてのクライアントを経由する必要がなくなりました。

1.2.11.6. メールパスワードポリシーなし

Not Email ポリシーを使用して、メールアドレスと同じパスワードを禁止することができます。

1.2.11.7. http://127.0.0.1 のあるすべてのポートの redirect-uri のサポート

http://localhost は、HTTP サーバーがランダムなポートで起動する際にコールバックとして使用されます。ベストプラクティスは、ローカルホストの代わりに http://127.0.0.1 を使用します。

1.2.12. その他の改善点

- Red Hat Single Sign-On JavaScript アダプターにアプリケーションイニシエーターを呼び出すサポートが追加されました。
- 署名および暗号化された ID トークンに使用される AES 192 および AES 256 アルゴリズムのサポート。
- ユーザーセッションではなく、更新トークンなしで OAuth2 クライアント認証情報の付与をサポートします。
- OAuth2 Revocation エンドポイントにアクセストークンを送信するサポート。
- アクティブな認証セッションの最大数を設定するサポート。デフォルト値は、ブラウザーセッションごとに 300 認証セッション (ブラウザータブ) に設定されます。
- LDAPv3 パスワードの変更操作をサポートするため、管理コンソールは設定された LDAP サーバーからメタデータを要求する機能を含む、LDAPv3 パスワード変更操作をサポートします。
- LDAP グループマッパーの namespace サポート。Red Hat Single Sign-On グループツリーの指定のブランチ (namespace) で、LDAP からグループをマッピングできます。以前、LDAP からのグループは常に Red Hat Single Sign-On の最上位グループとして追加されました。
- SAML アイデンティティープロバイダーが発行する認証要求の AuthnContext セクションの仕様のサポートが追加されました。
- 評価時のリソースおよびポリシーの取得によるパフォーマンスの向上

- 新規のアイデンティティープロバイダー **マッパー、OIDC Advanced 属性をロールマッパー** に対応として、SAML マッパーの Advanced Claim (Advanced Claim) に追加されました。新しいマッパーは、属性値と複数の属性値の正規表現をサポートします。

1.3. 既存のテクノロジープレビュー機能

以下の機能は引き続きテクノロジープレビューのステータスになります。

- クロスサイトデータレプリケーション
- RH-SSO Operator
- トークンの交換
- 詳細な承認パーミッション
- W3C Web 認証 (WebAuthn)

1.4. 削除済みまたは非推奨の機能

これらの機能のステータスが変更になりました。

- RH-SSO 7.5 は、Red Hat Enterprise Linux 6 (RHEL 6) へのインストールをサポートしません。RHEL 6 では、2020 年 11 月 30 日にライフサイクルの ELS フェーズに入りました。お客様は、RHEL 7 または 8 バージョンに RH-SSO 7.5 のアップグレードをデプロイする必要があります。
- RPM からのインストールは非推奨になりました。RH-SSO は、引き続き 7.x 製品の有効期間用の RPM の提供を行いますが、次のメジャーバージョンでは RPM は配信されません。製品は、引き続き ZIP ファイルからのインストールと、OpenShift でのインストールを引き続きサポートします。
- Authorization Services Drools Policy は RH-SSO 7.4 で削除されました。
- 管理 REST エンドポイントおよびコンソールを使用したスクリプトのアップロードが非推奨となりました。これは今後のリリースで削除されます。

1.5. 修正された問題

3 を超える場合、700 の問題は RH-SSO 7.4 と 7.5.0 の間で修正されました。詳細は「RHSSO 7.5.0 Fixed Issues」を参照してください。

1.6. 既知の問題

本リリースには、以下の既知の問題が含まれています。

- KEYCLOAK-18115: RHSSO 7.4.6 で拒否された属性の編集を試行
- KEYCLOAK-18338: 設定された SSSD でユーザーアカウントの更新を試みると Internal Server Error が発生する
- KEYCLOAK-18994: deleteExpiredClientSessions が MariaDB で非常に遅い

1.7. サポートされる構成

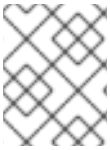
RH-SSO Server 7.5 でサポートされる機能および設定の一覧は、カスタマーポータルで確認できます。

1.8. コンポーネントのバージョン

RH-SSO 7.5 でサポートされるコンポーネントのバージョンの一覧は、カスタマーポータルで確認できます。

1.9. RED HAT OPENSHIFT の RED HAT SINGLE SIGN-ON メータリングラベル

メータリングラベルを Red Hat Single Sign-On に追加し、OpenShift Metering Operator を使用して Red Hat サブスクリプションの詳細を確認できます。



注記

メータリングラベルは、Operator がデプロイおよび管理する Pod に追加しないでください。

Red Hat Single Sign-On では、以下のメータリングラベルを使用できます。

- **com.redhat.component-name: Red Hat Single Sign-On**
- **com.redhat.component-type: application**
- **com.redhat.component-version: 7.5**
- **com.redhat.product-name: "Red_Hat_Runtimes"**
- **com.redhat.product-version: 2020/Q2**

関連資料

- OpenShift Container Platform でのメータリングの設定および使用