



Red Hat Single Sign-On 7.3

リリースノート

Red Hat Single Sign-On 7.3 向け

Red Hat Single Sign-On 7.3 リリースノート

Red Hat Single Sign-On 7.3 向け

法律上の通知

Copyright © 2023 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

概要

このガイドは、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

第1章 RED HAT SINGLE SIGN-ON 7.3	3
1.1. 概要	3
1.2. 新機能または改善機能	3
1.3. 修正された問題	7
1.4. 既知の問題	7
1.5. サポート対象の設定	8
1.6. コンポーネントのバージョン	8

第1章 RED HAT SINGLE SIGN-ON 7.3

1.1. 概要

Red Hat は、Red Hat Single Sign-On (RH-SSO)のバージョン 7.3 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。

以下の注記は RH-SSO 7.3 リリースに適用されます。

1.2. 新機能または改善機能

このリリースの新機能の一部はテクノロジープレビューの機能です。つまり、これらは利用可能ですが、完全にサポートされていません。これらはテストに使用できますが、テクノロジープレビューのマークが付いた機能は実稼働環境での使用はサポートされません。これらは、この一覧およびドキュメントでテクノロジープレビューとしてマークされています。これらは実稼働環境での使用を完全にサポートしていないため、テクノロジープレビュー機能はデフォルトで無効になっていますが、機能を試す場合は有効にすることができます。テクノロジープレビュー機能に関するフィードバックをお寄せいただくため、テクノロジープレビュー機能のコメントがある場合は、サポートチケットのログを作成してください。テクノロジープレビューから実稼働に移行すると、API と機能はメジャーバージョンのライフサイクルの間修正されるため、テクノロジープレビュー期間中のコメントは必要な方法で機能に影響を与えるために重要です。

本リリースでは、テクノロジープレビュー機能のままにされている既存の機能は次のとおりです。

- トークンの交換
- 詳細な認可パーミッション
- Authorization Services におけるルール(Drools)ベースのポリシー

1.2.1. 認証サービス

Authorization Services は、RH-SSO 7.1 リリースでテクノロジープレビュー機能として導入されました。7.3 では完全にサポートされるようになりました。ただし、Drools を使用して実装したカスタムルールに関連する小規模なサブコンポーネントは、テクニカルプレビューのままとなっています。

認可サービスは、新しい User Managed Access 2.0 (UMA 2.0)仕様に基いてアップグレードされました。以前のリリースでは、UMA 1.0 バージョンに依存していました。アップグレードすると、ユーザーはリソースを管理し、関連するパーミッション、アクセス要求の承認、アカウント管理コンソールを介して他のユーザーとの共有を行う機能が導入されました。

また、多くの小さな改善と追加が行われました。

- リソース属性 - パーミッションを評価するときにポリシーによって使用されるために、リソースの属性を定義できるようになりました。
- アダプターの改善 - 認可サービスの NodeJS アダプターサポートが追加されました。
- 評価 API の改善 - ユーザーロール、グループ、属性の確認など、現在のレルムからのアクセス情報。特定のパーミッションの適用方法に関する追加情報を提供するために、任意の要求をリソースサーバーにプッシュします。

- 非同期承認フロー：クライアントアプリケーションは、承認リクエストを開始するかどうかを選択し、リソースの所有者の承認を要求できるようになりました。この機能を使用すると、アプリケーションが別のユーザーの代わりにリソースの所有者の承認を要求することができます。
- ユーザー管理のパーミッション API - リソースサーバーは、特定のユーザーが所有するリソースに追加のポリシーを関連付けることができます。新しい API は、ロール、グループ、ユーザー、クライアント、または JavaScript を使用して条件を使用してこれらのパーミッションを管理する操作を提供します。
- プッシュされた要求 - クライアントアプリケーションは、これらの要求に基づいてパーミッションを評価するために、承認要求と共に任意の要求を Keycloak に送信できます。これは、特定のトランザクションの範囲で、またはランタイムに関する情報に基づいてアクセスを付与（または拒否）する必要がある場合に便利です。
- ポリシーエンフォーサー：ポリシーエンフォーサーは通常のアクセストークンを受け入れるようになり、リソースサーバーによって保護されているリソースにアクセスするために、(UMA を使用しない場合に)リソースサーバーによって保護されているリソースにアクセスするために、RPT でアクセストークンを交換する必要がなくなりました。ポリシーエンフォーサーがリソースサーバー側でどのように設定されているかによって、ベアラートークンとしての通常のアクセストークンを利用できます。
- 追加の変更：特定のアプリケーションのニーズに応じて、さらなるパフォーマンスプロファイリングを行うための追加の設定オプションを使用したパフォーマンスの改善と最適化。

1.2.1.1. 承認サービスのルールベースのポリシーはテクノロジープレビューです。

テクノロジープレビューの Drools 機能を使用して実装されたカスタムルールに関連する Authorization Services のサブコンポーネントのままです。

テクノロジープレビューのマークが付いた機能は、実稼働環境での使用はサポートされません。

1.2.2. OpenShift との統合

Red Hat Single Sign-On を使用して OpenShift 3.11 を完全に保護できるようになりました。これには、サービスアカウントを OAuth クライアントとして Red Hat Single Sign-On に自動的に公開する機能が含まれます。この機能は現在テクノロジープレビューとして提供されています。

テクノロジープレビューのマークが付いた機能は、実稼働環境での使用はサポートされません。

1.2.3. クライアントアダプターの新しい機能

- Fuse 7 - Fuse アダプターが最新の Fuse 7 リリースと整合しました。
- Sprint Boot 2 のサポート
- JavaScript -
 - ネイティブ Promise サポート：JavaScript アダプターはネイティブの promise をサポートするようになりました。古いスタイルの promise のサポートも維持されます。いずれも交換可能なものとして使用できます。
 - JavaScript - Cordova モードでは、ログインおよび JavaScript アダプターの他のメソッドに Cordova 固有のオプションを渡すことができるようになりました。また、Cordova の JavaScript アダプターに、ブラウザータブとユニバーサルリンクを使用するサポートも追

加されました。これにより、複数のアプリケーション間の SSO が可能になり、セキュリティが向上します。

- SAML アダプターのマルチテナンシーサポート : OpenID Connect アダプターですでに可能なような複数の Keycloak レalm との統合を可能にします。

1.2.4. 新規の署名アルゴリズム

RH-SSO サーバーは、RS256、RS384、RS512、ES256、ES384、ES512、HS256、HS384、および HS512 をサポートするようになりました。

Elliptic Curve Digital Signature Algorithm (ES256/384/512) がサポートされるようになりました。また、RSA 署名と同様のセキュリティプロパティを提供するようになりましたが、使用する CPU が大幅に少なくなります。

HMAC (HS256/384/512) がサポートされ、アプリケーションが署名自体を検証しようとするのを防ぐことができるようになりました。これらは対称署名であるため、Keycloak のみが署名を検証できるため、アプリケーションはトークンイントロスペクションエンドポイントを使用してトークンを検証する必要があります。

RH-SSO アダプターは追加の署名アルゴリズムに対応しておらず、現在 RS256 のみをサポートしています。

1.2.5. ホスト名の処理

RH-SSO のホスト名を設定するためのより柔軟な方法を導入しました。これにより、クラウド関連の環境にデプロイする際の柔軟性が向上します。リクエストヘッダーに基づいて判断するか、固定ホスト名として設定できます。後者は、有効なホスト名のみを使用し、内部アプリケーションが代替 URL を介して RH-SSO を呼び出すことを許可します。

1.2.6. X509 Client Authenticator

新しく追加された Client Authenticator は X509 Client Certificates および Mutual TLS を使用してクライアントからの接続を保護します。さらに、RH-SSO Server は、クライアントの証明書のサブジェクト DN フィールドを検証します。

1.2.7. クライアントスコープ

Client Templates に代わるクライアントスコープのサポートを追加しました。クライアントスコープはより柔軟なアプローチであり、OAuth スコープパラメーターのサポートも改善します。

クライアントスコープと同意画面に関連する変更があります。これで、consent 画面の一覧は、プロトコルマッパーおよびロールではなくクライアントスコープにリンクされるようになりました。

詳細は、ドキュメントおよび移行ガイドを参照してください。

1.2.7.1. OpenID Connect クライアントのオーディエンスサポートの強化

OpenID Connect クライアントに発行されたトークンでオーディエンスを指定できるようになりました。アダプター側でのオーディエンスの検証もサポートされています。

1.2.8. OAuth 2 Certificate Bound Access Token

仕様 OAuth 2.0 Mutual TLS Client Authentication および Certificate Bound Access Tokens を部分的に

実装しました。具体的には、Certificate Bound Access Tokens のサポートを利用できるようになりました。機密クライアントが双方向 SSL を使用できる場合、RH-SSO はクライアント証明書のハッシュをクライアントに発行したトークンに追加できます。現時点では、トークンのハッシュ（更新トークン要求時など）を検証する RH-SSO 自体になります。アダプターにもサポートを追加する予定です。また、相互 TLS クライアント認証のサポートを追加する予定です。テーマおよびテーマリソース

通常のプロバイダーデプロイメントを使用して、テーマを RH-SSO にホットデプロイできるようになりました。また、テーマリソースのサポートも追加されました。これにより、テーマを作成せずにテンプレートやリソースを追加できます。これは、追加のページを認証フローに追加する必要があるカスタムオーセンティケーターに役立ちます。

また、特定のクライアントのテーマをオーバーライドするサポートも追加されました。これがニーズに十分でない場合、テーマの選択にカスタムロジックを実装できる新しい Theme Selector SPI もあります。

1.2.9. UI の改善

以下のページの設計は 7.3 リリースで更新されます。

- Welcome ページ
- ログインページ

1.2.10. 強化された Remember Me

記憶するセッションに対して異なるセッションアイドルと最大タイムアウトを指定する機能が導入されました。これにより、通常のセッションよりも長くセッションの存続が可能になります。

1.2.11. グループのページネーションサポート

以前のバージョンでは、多数のグループで管理コンソールで問題が発生しました。これは、グループのページネーションの導入によって解決されるようになりました。

1.2.12. 多数のオフラインセッションによる起動時間の向上

以前は、オフラインセッションが多数ある場合、RH-SSO の起動に長い時間がかかる可能性がありました。この起動時間が大幅に短縮されました。

1.2.13. DB2 のサポートが削除される

DB2 のサポートはしばらく非推奨になりました。このリリースでは、DB2 のサポートをすべて削除しました。

1.2.14. 若干の改善

- 最初の Idp 認証の後に、アイデンティティプロバイダーのアイデンティティを既存のアカウントに自動的にリンクするオーセンティケーター。
- 現在のロケールを OAuth2 IdP に渡すことを許可
- Content-Security-Policy-Report-Only セキュリティヘッダーのサポート
- SAML のスクリプトベースの ProtocolMapper
- Instagram を使用したログインサポートを追加しました。

- 管理コンソールのユーザー ID による検索
- **hd** パラメーターを使用した Google ログインのホスト型ドメインのサポート
- ドット(.)を持つ要求を作成するオプションが追加されました。

1.3. 修正された問題

本リリースでは、1,200 を超える問題が解決されました。

- <https://issues.redhat.com/issues/?filter=12337585>

1.4. 既知の問題

以下は、このリリースの既知の問題です。

- [KEYCLOAK-6127: ロールの](#) 管理ユーザーは、許可されたパーミッションに関係なく、一部の操作に引き続き必要となります。
- [KEYCLOAK-8043](#) - prompt=none doesn't work with default identity provider
- [KEYCLOAK-8049](#): ルートノードのグループポリシーを作成する際の nullpointer
- [KEYCLOAK-8766](#): elytron アダプターを使用すると、OIDC リクエストのある CORS が失敗する
- [KEYCLOAK-8821](#): KeycloakApplication が正常にデプロイされていない場合、server.log のコンテンツが削除されます。
- [KEYCLOAK-8867](#) - uma-policy を介してクエリーする際に、ポリシーに関連付けられたリソースを返します。
- [KEYCLOAK-8957](#) - フェデレーション ID ログインにより、ユーザーアカウントが破損します。
- [KEYCLOAK-9093](#) - False-Positive UMA ポリシー評価
- [KEYCLOAK-9095](#) - Web Origins が null の場合、AuthenticatedActionsHandler で NullPointerException が発生する
- [KEYCLOAK-9183](#) - 既存の LDAP エントリーが LDAPStorageProvider 経由でパスワードを検証すると NullPointerException が発生する
- [KEYCLOAK-9272](#) - トラストストアのパスワードがない場合の NullPointer
- [KEYCLOAK-9310](#) - 必要なカスタムアクションプロバイダーを削除すると、レルムモデルが破損する
- [KEYCLOAK-10211](#) - libunix-dbus-java がいないため、RHEL8 で SSSD 統合が機能しない
- [KEYCLOAK-10238](#): Securing Applications and Services Guide には、RHEL 8 へのアダプターのインストール手順がありません。インストールプロセスは以前のリリースと同じですが、RHEL 8 のリポジトリ名が必要です。同じリポジトリから EAP を最初にインストールしてください。
- [KEYCLOAK-10239](#): Securing Applications and Services Guide には、RPM インストールセクションのパッケージ名が廃止されています。

- [KEYCLOAK-10260](#): .installation ディレクトリーの無効なパーミッションにより、パッチのインストールができなくなります。この問題を回避するには、rhssso-7.3 ディレクトリーに移動し、`chmod 775 .installation` コマンドを実行します。

1.5. サポート対象の設定

RH-SSO Server 7.3 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。

1.6. コンポーネントのバージョン

RH-SSO 7.3 でサポートされるコンポーネント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。