OpenJDK 17

FIPS を使用した RHEL での OpenJDK 17 の設定

ガイド

Last Updated: 2022-05-14

OpenJDK 17 FIPS を使用した RHEL での OpenJDK 17 の設定

ガイド

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

OpenJDK は、Red Hat Enterprise Linux プラットフォーム上の Red Hat 製品です。『FIPS を使用した RHEL での OpenJDK 17 の設定』では、FIPS の概要と、FIPS で OpenJDK を有効化および設定する方法を説明します。

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。

RED HAT ドキュメントへのフィードバック

弊社のドキュメントに関するご意見やご感想をお寄せください。フィードバックをお寄せいただくには、ドキュメントのテキストを強調表示し、コメントを追加できます。

本セクションでは、フィードバックの送信方法を説明します。

前提条件

- Red Hat カスタマーポータルにログインしている。
- Red Hat カスタマーポータルで、**マルチページ HTML** 形式でドキュメントを表示します。

手順

フィードバックを提供するには、以下の手順を実施します。

1. ドキュメントの右上隅にある **フィードバック** ボタンをクリックして、既存のフィードバックを確認します。

注記

フィードバック機能は、**マルチページ HTML** 形式でのみ有効です。

2. フィードバックを提供するドキュメントのセクションを強調表示します。
3. ハイライトされたテキスト近くに表示される **Add Feedback** ポップアップをクリックします。ページの右側のフィードバックセクションにテキストボックスが表示されます。
4. テキストボックスにフィードバックを入力し、**Submit** をクリックします。ドキュメントに関する問題が作成されます。
5. 問題を表示するには、フィードバックビューで問題トラッカーリンクをクリックします。

第1章 FIPS (FEDERAL INFORMATION PROCESSING STANDARD) の概要

FIPS (Federal Information Processing Standards) は、コンピューターシステムやネットワーク間のセキュリティーおよび相互運用性を強化するためのガイドラインと要件を提供します。FIPS 140-2 および 140-3 シリーズは、ハードウェアおよびソフトウェアの両レベルで暗号化モジュールに適用されます。アメリカ国立標準技術研究所 は、進行中の暗号モジュールと承認済みの暗号モジュールの両方の検索可能なリストとともに暗号化モジュール検証プログラムを実装しています。

Red Hat Enterprise Linux (RHEL) は、FIPS 140-2 コンプライアンスシステム全体を有効にする統合フレームワークを提供します。FIPS モードで操作する場合、暗号化ライブラリーを使用するソフトウェアパッケージはグローバルポリシーに従って自己設定されます。ほとんどのパッケージでは、互換性やその他のニーズにおいて、デフォルトの調整動作を変更する手段を提供します。

OpenJDK 17 は、FIPS ポリシー対応パッケージです。

関連情報

- 暗号モジュール検証プログラムの詳細は、**National Institute of Standards and Technology** Web サイトの Cryptographic Module Validation Program CMVP を参照してください。
- FIPS モードを有効にして RHEL をインストールする方法は、「FIPS モードが有効になっている RHEL 8 システムのインストール」を参照してください。
- RHEL をインストールした後に FIPS モードを有効にする方法は、「FIPS モードへのシステムの切り替え」を参照してください。
- RHEL の FIPS モードで OpenJDK を実行する方法の詳細「Running OpenJDK in FIPS mode on RHEL」を参照してください。
- Government 標準による Red Hat コンプライアンスについての詳細は、「Goverment Standards」を参照してください。

第2章 FIPS モードでの OPENJDK 17 の設定

OpenJDK 17 は、起動時に FIPS モードがシステムで有効になっているかどうかを確認します。yes の場合、グローバルポリシーに従って FIPS を自己設定します。これは、RHEL 8.3 以降のデフォルトの動作です。以前の RHEL 8 リリースでは、**com.redhat.fips** システムプロパティーを JVM 引数として **true** に設定する必要があります。例: **-Dcom.redhat.fips=true**

注記

JVM インスタンスの実行中に FIPS モードがシステムで有効になっている場合は、変更を有効にするためにインスタンスを再起動する必要があります。

OpenJDK 17 を設定して、グローバル FIPS 調整をバイパスできます。たとえば、OpenJDK が提供するスキームではなく、Hardware Security Module (HSM) で FIPS コンプライアンスを有効にする場合があります。

OpenJDK 17 の FIPS プロパティーは次のとおりです。

- **security.useSystemPropertiesFile**
  - セキュリティープロパティー **$JAVA_HOME/lib/security/java.security** または **java.security.properties** にダイレクトされたファイルにあります。
  - デフォルトの **java.security** ファイル内の値を変更するには、特権アクセスが必要です。
  - 永続設定。
  - **false** に設定すると、グローバル FIPS と crypto-policies 調整の両方が無効になります。デフォルトでは **true** に設定されます。
- **java.security.disableSystemPropertiesFile**
  - JVM に渡されるシステムプロパティーを引数として渡すシステムプロパティー。For example, **-Djava.security.disableSystemPropertiesFile=true**.
  - 非特権アクセスで十分です。
  - 非永続的な設定。
  - **true** に設定すると、グローバル FIPS と crypto-policies アライメントの両方が無効になります。**security.useSystemPropertiesFile=false** セキュリティプロパティーと同じ効果が生成されます。いずれのプロパティーも異なる動作に設定されている場合は、**java.security.disableSystemPropertiesFile** が上書きされます。デフォルトでは **false** に設定されます。
- **com.redhat.fips**
  - JVM に渡されるシステムプロパティーを引数として渡すシステムプロパティー。例: **-Dcom.redhat.fips=false**
  - 非特権アクセスで十分です。
  - 非永続的な設定。
  - **false** に設定すると、グローバル crypto-policies を適用している間に FIPS 調整を無効にします。以前のプロパティーのいずれかが crypto-policies 調整を無効にするように設定されている場合には、このプロパティーは効果がありません。つまり、crypto-policies は FIPS

調整の前提条件です。デフォルトでは **true** に設定されます。

関連情報

- FIPS モードを有効にする方法は、「FIPS モードへのシステムの切り替え」を参照してください。

第3章 OPENJDK 17 のデフォルトの FIPS 設定

OpenJDK 17 には、FIPS 準拠設定にデフォルト設定される FIPS (Federal Information Processing Standard) 設定の概要が含まれています。

これらのデフォルト設定に変更を加える前に、以下の OpenJDK 17 のデフォルト FIPS 設定を確認してください。

3.1. セキュリティープロバイダー

グローバル java セキュリティーポリシーファイルは、OpenJDK セキュリティーポリシーを制御します。**$JRE_HOME/lib/security/java.security** に java セキュリティーポリシーファイルがあります。

FIPS モードを有効にすると、OpenJDK はインストールされたセキュリティープロバイダーを以下のものに置き換えます。これは優先度が高い順になります。

SunPKCS11-NSS-FIPS

- Network Security Services (NSS) ソフトウェアトークン (PKCS#11 バックエンド) で初期化されます。NSS ソフトウェアトークンには、以下の設定が含まれます。
  - name = NSS-FIPS
  - nssLibraryDirectory = /usr/lib64
  - nssSecmodDirectory = /etc/pki/nssdb
  - nssDbMode = readOnly
  - nssModule = fips
- NSS ライブラリーは、FIPS 準拠のソフトウェアトークンを実装します。また、RHEL で FIPS ポリシー対応も可能にします。

SUN

- X.509 証明書でサポートされるのは、X.509 証明書のみです。アプリケーションがこのプロバイダーの他の暗号化アルゴリズムを使用していないことを確認します。それ以外の場合は、セキュリティープロバイダーは **java.security.NoSuchAlgorithmException** メッセージを出力します。

SunEC

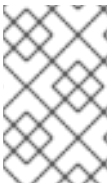
- **SunPKCS11** 補助ヘルパーの場合のみ。アプリケーションがこのプロバイダーを明示的に使用していないことを確認してください。

SunJSSE

- TLS サポートの場合、**SunJSSE** は X.509 証明書に **SUN** プロバイダーを使用し、すべての暗号化プリミティブに **SunPKCS11-NSS-FIPS** プロバイダーを使用します。

3.2. CRYPTO-POLICIES

FIPS モードを有効にすると、OpenJDK はグローバル crypto-policies から暗号化アルゴリズムの設定値を取ります。これらの値は **/etc/crypto-policies/back-ends/java.config** にあります。RHEL の **update-crypto-policies** ツールを使用すると、一貫性のある方法で crypto-policies を管理できます。



注記

暗号ポリシー承認アルゴリズムは、OpenJDK の FIPS モードでは使用できません。これは、FIPS 準拠の実装が NSS ライブラリーで利用できない場合や、OpenJDK の **SunPKCS11** セキュリティープロバイダーでサポートされない場合に発生します。

3.3. TRUST ANCHOR 証明書

OpenJDK は、FIPS モードでは、グローバル Trust Anchor 証明書リポジトリーを使用します。このリポジトリーは、**/etc/pki/java/cacerts** で確認することができます。RHEL の **update-ca-trust** ツールを使用して、一貫性のある方法で証明書を管理します。

3.4. キーストア

FIPS モードでは、OpenJDK は、鍵の読み取り専用 **PKCS#11** ストアとして NSS DB を使用します。これにより、**keystore.type** セキュリティープロパティーは **PKCS11** に設定されます。NSS DB リポジトリーは **/etc/pki/nssdb** で見つけることができます。RHEL で **modutil** ツールを使用し、NSS DB キーを管理します。

改訂日時: 2021-11-28 22:58:44 +1000