Red Hat Certificate System 10

リリースノート

Red Hat Certificate System 10 に関連する主な機能および更新

Last Updated: 2024-09-08

Red Hat Certificate System 10 リリースノート

Red Hat Certificate System 10 に関連する主な機能および更新

法律上の通知

概要

これらのリリースノートには、システム要件、インストールノート、重要な変更、現在の問題など、Red Hat Certificate System 10 に関連する重要な情報が含まれています。Red Hat Certificate System 10 をデプロイする前に、これらのリリースノート全体をお読みください。

目次

第1章 RED HAT CERTIFICATE SYSTEM 10

このセクションには、Red Hat Certificate System 10 に関する一般的な情報 (サポートされているプラットフォームとシステム要件、インストールに関する注意事項、非推奨事項など) が含まれています。

重要

Red Hat Certificate System 10 のパッケージとその依存関係は、Red Hat Enterprise Linux 8 では **redhat-pki** モジュールを介して提供されます。

1.1. 前提条件

Red Hat Certificate System 10 をインストールするには、Red Hat Enterprise Linux 8 が必要です。Red Hat Enterprise Linux 8 のインストール方法の詳細は、標準的な RHEL インストールの実行 を参照してください。

1.2. ハードウェアの要件

このセクションでは、Red Hat Certificate System 10 の最小および推奨されるハードウェアを説明します。環境によっては、より多くのリソースが必要になる可能性があることに注意してください。

1.2.1. 最低要件

- CPU: 2 スレッド
- RAM: 2 GB
- ディスク容量: 20 GB

この最小要件は、Red Hat Enterprise Linux 8 の最小要件に基づいています。詳細は、Red Hat Enterprise Linux テクノロジーの機能と制限を参照してください。

1.2.2. 推奨される要件

- CPU: 4 つ以上のスレッド、AES-NI サポート
- RAM: 4 GB 以上
- ディスク容量: 80 GB 以上

1.3. サポート対象のプラットフォーム

このセクションでは、Red Hat Certificate System 10 でサポートされているさまざまなサーバープラットフォーム、ハードウェア、トークン、およびソフトウェアを説明します。

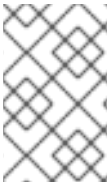
1.3.1. サーバーサポート

Red Hat Certificate System 10 の認証局 (CA)、Key Recovery Authority (KRA)、オンライン証明書ステータスプロトコル (OCSP)、トークンキーサービス (TKS)、およびトークン処理システム (TPS) サブシステムの実行は、Red Hat Enterprise Linux 8 でサポートされています。各 Red Hat Certificate System 10 マイナーリリースは、特定の Red Hat Enterprise Linux 8 マイナーバージョンでテストされ、

リリースされます。さらに、Red Hat Certificate System の各マイナーバージョンは、Red Hat Directory Server の特定のバージョンに対してもテストされます。次の表は、Red Hat Certificate System でテストされ、サポートされているマイナーバージョンを示しています。

表1.1 Red Hat Certificate System 10.x バージョンでサポートおよびテストされている Red Hat Enterprise Linux および Red Hat Directory Server のバージョン

Red Hat Certificate System のバージョン	Red Hat Enterprise Linux のバージョン	Red Hat Directory Server のバージョン
10.0	8.2	11.1
10.1	8.3	11.2
10.2	8.4	11.3
10.3	8.5	11.4
10.4	8.6	11.5



注記

Red Hat Certificate System 10 は、認定済みのハイパーバイザーの Red Hat Enterprise Linux 8 仮想ゲストでの実行に対応します。詳細は、Which hypervisors are certified to run RHEL? ソリューション記事を参照してください。

1.3.2. クライアントサポート

Enterprise Security Client (ESC) は以下でサポートされます。

- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 6 および 7 の最新版
  これらのプラットフォームは Red Hat Certificate System 10 をサポートしませんが、このクライアントは Red Hat Certificate System 10 の Token Management System (TMS) システムで使用できます。

1.3.3. サポートされる Web ブラウザー

Red Hat Certificate System 10 は、以下のブラウザーに対応しています。

表1.2 プラットフォームでサポートされる Web ブラウザー

プラットフォーム	エージェントサービス	エンドユーザーページ
Red Hat Enterprise Linux	Firefox 60 以降[a]	Firefox 60 以降

[a] この Firefox バージョンは、ブラウザーからキーの生成およびアーカイブに使用される暗号化 Web オブジェクトに対応しなくなりました。そのため、この分野では機能が限定されるはずです。

注記

HTML ベースのインスタンス設定に完全に対応するブラウザーは Mozilla Firefox のみです。

1.3.4. 対応するスマートカード

Enterprise Security Client (ESC) は、Global Platform 2.01 準拠のスマートカードおよび JavaCard 2.1 以降をサポートします。

Certificate System サブシステムは、以下のトークンを使用してテスト済みです。

- Gemalto TOP IM FIPS CY2 64K トークン (SCP01)
- Giesecke & Devrient (G&D) SmartCafe Expert 7.0 (SCP03)
- SafeNet Assured Technologies SC-650 (SCP01)

Certificate System でサポートされている唯一のカードマネージャーアプレットは、Red Hat Certificate System の pki-tps パッケージに含まれる **CoolKey** アプレットです。

1.3.5. サポート対象のハードウェアセキュリティーモジュール

以下の表は、Red Hat Certificate System がサポートする Hardware Security Modules (HSM) を示しています。

HSM	ファームウェア	アプライアンスソフトウェア	クライアントソフトウェア
nCipher nShield Connect XC (High)	nShield_HSM_Firmware-12.72.1	12.71.0	SecWorld_Lin64-12.71.0
Thales TCT Luna Network HSM Luna-T7	lunafw_update-7.11.1-4	7.11.0-25	610-500244-001_LunaClient-7.11.1-5

1.4. RHCS サブシステムをインストールするためのクイックスタート

The following procedure describes the prerequisites and the basic installation process for {RHCS} 10.

前提条件

- 最新の Red Hat Enterprise Linux 8 バージョンがアクティブなネットワーク接続でインストールされている。最新の ISO イメージについては、Download Red Hat Enterprise Linux を参照してください。

手順

1. Red Hat Subscription Manager (RHSM) を使用してカスタマーポータルアカウントにシステムを登録してから、登録済みのシステムに対して、このアカウントで利用可能なサブスクリプションの一覧を表示します。

```
$ subscription-manager register
$ subscription-manager list --available --all
```

2. 前の手順で取得した対応するプール ID を使用して、Red Hat Enterprise Linux Server および Red Hat Certificate System に必要なサブスクリプションを割り当てます。

```
$ subscription-manager attach --pool=POOL_ID_RHEL_SERVER
$ subscription-manager attach --pool=POOL_ID_CERT_SYSTEM
```

3. Red Hat Enterprise Linux に最新の更新が適用されていることを確認してください。

```
$ dnf update
```

4. Directory Server モジュールをインストールします。

```
& dnf module enable 389-ds:1.4 && dnf install 389-ds-base
```

5. 実際のドメイン名が **/etc/resolv.conf** に指定されていること、またホスト名が **/etc/hosts** に設定されていることを確認します。

6. Directory Server インタラクティブインストーラーを実行し、必要に応じてカスタマイズします。

```
$ dscreate interactive
```

詳細またはその他のインストール方法は、Red Hat Directory Server インストールガイド を参照してください。

7. Certificate System のパッケージと依存関係をインストールします。

```
$ dnf module enable redhat-pki:10 && dnf install redhat-pki
```

8. **pkispawn** スクリプトを実行して、サブシステムインスタンスを作成および設定します。他のタイプのサブシステムを設定する前に、少なくとも 1 つの CA サブシステムをインストールして完全に設定する必要があります。詳細は、**pkispawn** の man ページを参照してください。オプションが指定されていない場合には、pkispawn はインタラクティブモードで実行され、インストールに必要な基本情報をユーザーに求めます。

```
$ pkispawn
```

9. 適切に設定されたローカルまたはリモートの Mozilla Firefox Web ブラウザーを使用して、さまざまな Red Hat Certificate System サブシステムのエージェントインターフェイスにアクセスします。

Red Hat Certificate System サブシステムのインストールと設定の詳細は、計画、インストールおよびデプロイメントガイド を参照してください。

関連情報

- Red Hat Enterprise Linux のダウンロード
- 標準的な RHEL インストールの実行

- Red Hat Directory Server インストールガイド
- 計画、インストール、およびデプロイメントのガイド

1.5. 非推奨の機能

このセクションでは、Red Hat Certificate System 10 で非推奨になった機能を説明します。

Certificate System の SCP01 サポートが非推奨に

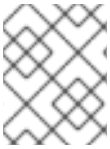
Secure Channel Protocol 01 (SCP01) のサポートは Certificate System 10 で非推奨になり、削除される可能性があります。Red Hat は、SCP03 をサポートするスマートカードの使用を推奨します。

pkiconsole ツールが非推奨に

Certificate System 10 では、**pkiconsole** ツールが非推奨になります。

第2章 RED HAT ENTERPRISE LINUX 8.6 上の RED HAT CERTIFICATE SYSTEM 10.4

このセクションでは、注目すべき更新と新機能、重要なバグ修正、ユーザーが知っておくべき現在の既知の問題など、RHEL 8.6 上の Red Hat Certificate System 10.4 の重要な変更を説明します。



注記

Red Hat Certificate System を以前のマイナーバージョンにダウングレードすることはサポートされていません。

2.1. CS10.4 の更新と新機能

このセクションでは、Red Hat Certificate System 10.4 の新機能および重要な更新を説明します。

pki-core パッケージの更新と新機能:

Certificate System パッケージがバージョン 10.13.0 にリベース

pki-core、**redhat-pki**、**redhat-pki-theme**、および **pki-console** パッケージがアップストリームバージョン 10.13.0 にアップグレードされ、以前のバージョンに対するバグ修正や機能強化が数多く追加されました。

2.2. テクノロジープレビュー

テクノロジープレビュー機能として RHCS で ACME がサポートされるように

Automated Certificate Management Environment (ACME) レスポンダーを介したサーバー証明書の発行は、Red Hat Certificate System (RHCS) で利用できます。ACME レスポンダーは ACME v2 プロトコル (RFC 8555) をサポートします。

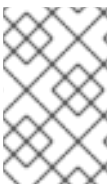
以前は、ユーザーは認証局 (CA) の独自の証明書署名要求 (CSR) 送信ルーチンを使用する必要がありました。ルーチンでは、要求を手動で確認して証明書を発行するために、認証局 (CA) エージェントが必要になる場合がありました。

RHCS ACME レスポンダーは、CA エージェントを使用せずに、サーバー証明書の自動発行とライフサイクル管理のための標準メカニズムを提供するようになりました。この機能により、RHCS CA を既存の証明書発行インフラストラクチャーと統合して、デプロイメント用のパブリック CA と開発用の内部 CA をターゲットにすることができます。

このテクノロジープレビューには、ACME サーバーのサポートのみが含まれていることに注意してください。ACME クライアントが、このリリースに同梱されているわけではありません。さらに、この ACME プレビューは、発行データを保持したり、ユーザー登録を処理したりしません。

今後、Red Hat Enterprise Linux が更新されることで、ACME のインストールで問題が発生する可能性があることに注意してください。

詳細は、IETF definition of ACME を参照してください。



注記

この機能はテクノロジープレビューとして提供され、今後の製品機能への早期アクセスを提供し、サブスクリプション契約ではまだ完全にはサポートされていないことに注意してください。

2.3. CS 10.4 のバグ修正

この箇所では、ユーザーに重大な影響を及ぼしていて、Red Hat Certificate System 10.4 で修正されたバグを説明します。

TPS が tps-cert-find のトークンプロファイル分離を適切に適用するように

今回の修正により、**tps-cert-find** コマンドは、**tps-token-find** コマンドと同様に、ユーザープロファイルに従って、トークン ID、ユーザー ID、ステータス、日付などのエントリーを適切に制限するようになりました。

トークンが TPS Web UI に正しく表示されるように

以前は、**tpsclient** ツールを使用してトークンをフォーマットおよび登録したり、Web UI を介してトークンを追加したりすると、デバッグログにエントリーが正常に記録されたことが示されていても、TPS Web UI にトークンは表示されませんでした。今回の修正により、Web UI はすべてのトークンを適切に一覧表示するようになりました。

pki-core パッケージでのバグ修正

pki-server ca-cert-request-show がファイルへの書き込み時に失敗しない

以前のリリースでは、**pki-server ca-cert-request-show <request_id> -i <instance> --output-file <output_file>** コマンドが **ERROR: a bytes-like object is required, not 'str'** のエラーで失敗しました。今回の修正により、ファイルに書き込む前に証明書要求がバイトとしてエンコードされるようになり、このコマンドで正常に証明書がエクスポートされるはずです。

2.4. CS 10.4 の既知の問題

この箇所では、Red Hat Certificate System 10.4 でユーザーが知っておくべき既知の問題と、該当する場合は回避策を説明します。

TPS では匿名バインドの ACI アクセスの追加が必要

以前のバージョンでは、匿名バインド ACI はデフォルトで許可されていましたが、LDAP では無効になっています。これにより、TPS スマートカードの登録またはフォーマットができなくなります。

この問題が修正されるまでの回避策として、Directory Server で匿名バインド ACI を手動で追加する必要があります。

```
$ ldapmodify -D "cn=Directory Manager" -W -x -p 3389 -h hostname -x <<EOF
dn: dc=example,dc=org
changetype: modify
add: aci
aci: (targetattr!="userPassword || aci")(version 3.0; acl "Enable anonymous access"; allow (read,
search, compare) userdn="ldap:///anyone";)
EOF
```

pki-core パッケージの既知の問題:

auditSigningCert に属性がないため、HSM を使用した KRA のクローン作成が失敗する

HSM を使用して KRA のクローンを作成する場合に、**auditSigningCert** の信頼属性 **u,u,Pu** がマスターとクローンのエイリアス DB の間で暗黙的に同期されるはずですが、クローンのエイリアス DB での複製に失敗するようになりました。結果として、HSM を使用した KRA のクローン作成は、**auditSigningCert cert-topology-02-KRA KRA is invalid: Invalid certificate: (-8101) Certificate type not approved for application** というエラーで失敗します。

この問題を回避するには、**auditSigningCert** の **u,u,Pu** 信頼属性をクローン KRA のエイリアス DB に明示的に追加し、インスタンスを再起動する必要があります。以下に例を示します。

- 回避策の前:

```
# certutil -vv -V -d /var/lib/pki/clone-KRA/alias/ -h nfast -n 'token:auditSigningCert cert-topology-02-KRA KRA' -u J
  Enter Password or Pin for "token":
  certutil: certificate is invalid: Certificate type not approved for application.
```

- 回避策の後:

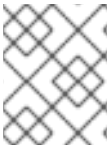
```
# certutil -M -d /var/lib/pki/clone-KRA/alias/ -n 'token:auditSigningCert cert-topology-02-KRA KRA' -t u,u,Pu
# certutil -vv -V -d /var/lib/pki/clone-KRA/alias/ -h nfast -n 'token:auditSigningCert cert-topology-02-KRA KRA' -u J
  Enter Password or Pin for "token":
  certutil: certificate is valid
```

--agent-uid pkidbuser オプションを指定して cert-fix ユーティリティーを使用すると Certificate System が破損

--agent-uid pkidbuser オプションを指定して **cert-fix** ユーティリティーを使用すると、Certificate System の LDAP 設定が破損します。したがって、Certificate System は不安定になり、システムの復元に手動の操作が必要になる可能性があります。

第3章 RED HAT ENTERPRISE LINUX 8.5 上の RED HAT CERTIFICATE SYSTEM 10.3

このセクションでは、注目すべき更新と新機能、重要なバグ修正、ユーザーが知っておくべき現在の既知の問題など、RHEL 8.5 上の Red Hat Certificate System 10.3 の重要な変更を説明します。



注記

Red Hat Certificate System を以前のマイナーバージョンにダウングレードすることはサポートされていません。

3.1. CS 10.3 の更新と新機能

このセクションでは、Red Hat Certificate System 10.3 の新機能および重要な更新を説明します。

pki-core パッケージの更新と新機能:

Certificate System パッケージがバージョン 10.12.4 にリベース

pki-core、**redhat-pki**、**redhat-pki-theme**、および **pki-console** パッケージがアップストリームバージョン 10.12.4 にアップグレードされ、以前のバージョンに対するバグ修正や機能強化が数多く追加されました。

3.2. テクノロジープレビュー

テクノロジープレビュー機能として RHCS で ACME がサポートされるように

Automated Certificate Management Environment (ACME) レスポンダーを介したサーバー証明書の発行は、Red Hat Certificate System (RHCS) で利用できます。ACME レスポンダーは ACME v2 プロトコル (RFC 8555) をサポートします。

以前は、ユーザーは認証局 (CA) の独自の証明書署名要求 (CSR) 送信ルーチンを使用する必要がありました。ルーチンでは、要求を手動で確認して証明書を発行するために、認証局 (CA) エージェントが必要になる場合がありました。

RHCS ACME レスポンダーは、CA エージェントを使用せずに、サーバー証明書の自動発行とライフサイクル管理のための標準メカニズムを提供するようになりました。この機能により、RHCS CA を既存の証明書発行インフラストラクチャーと統合して、デプロイメント用のパブリック CA と開発用の内部 CA をターゲットにすることができます。

このテクノロジープレビューには、ACME サーバーのサポートのみが含まれていることに注意してください。ACME クライアントが、このリリースに同梱されているわけではありません。さらに、この ACME プレビューは、発行データを保持したり、ユーザー登録を処理したりしません。

今後、Red Hat Enterprise Linux が更新されることで、ACME のインストールで問題が発生する可能性があることに注意してください。

詳細は、IETF definition of ACME を参照してください。

注記

この機能はテクノロジープレビューとして提供され、今後の製品機能への早期アクセスを提供し、サブスクリプション契約ではまだ完全にはサポートされていないことに注意してください。

3.3. CS 10.3 のバグ修正

この箇所では、ユーザーに重大な影響を及ぼしていて、Red Hat Certificate System 10.3 で修正されたバグを説明します。

pki-core パッケージでのバグ修正

pcsc-lite、pcsc-lite-ccid および esc が追加され、特定の SCP03 および SCP01 トークンを使用したセキュアなチャネルの完了が失敗しなくなる

Red Hat Certificate System 10.2 のリリース時点で、**pcsc-lite**、**pcsc-lite-ccid**、および **esc** パッケージの問題により、特定の SCP03 および SCP01 トークンを使用してセキュリティー保護されたチャネルを完了できませんでした。これは、その後のバッチ更新で修正されています。

SubCA 署名証明書の検証中に SubCA の 2 段階インストールが失敗することはなくなった

以前のリリースでは、FIPS が有効になっている HSM 環境で、2 段階の方法を使用して SubCA をインストールすると失敗しました。RSA または ECC オプションのいずれかで、SubCA 署名証明書を検証しようとすると、エラーが返されました。今回の修正により、pki cli コマンドが **nss-import-cert** から **client-import-cert** と **--cert `to `--ca-cert** に変更されました。その結果、CA 署名証明書は信頼できる状態で nssdb に適切にインポートされます。さらに、pkispawn が **pki-server subsystem-cert-validate** 呼び出しに失敗した場合、このパッチを使用すると、**pkispawn** を完了させながら、失敗の詳細を提供できます。これにより、管理者は CA 署名証明書を手動で追加できますが、前述の修正により、問題の発生を防ぐことができます。

3.4. CS 10.3 の既知の問題

このパートでは、Red Hat Certificate System 10.3 でユーザーが知っておくべき既知の問題と、該当する場合は回避策を説明します。

TPS では匿名バインドの ACI アクセスの追加が必要

以前のバージョンでは、匿名バインド ACI はデフォルトで許可されていましたが、LDAP では無効になっています。これにより、TPS スマートカードの登録またはフォーマットができなくなります。

この問題が修正されるまでの回避策として、Directory Server で匿名バインド ACI を手動で追加する必要があります。

```
$ ldapmodify -D "cn=Directory Manager" -W -x -p 3389 -h hostname -x <<EOF
dn: dc=example,dc=org
changetype: modify
add: aci
aci: (targetattr!="userPassword || aci")(version 3.0; acl "Enable anonymous access"; allow (read,
search, compare) userdn="ldap:///anyone";)
EOF
```

トークンは TPS Web UI に表示されない

tpsclient ツールを使用してトークンをフォーマットおよび登録する場合、または Web UI を介してトークンを追加する場合、デバッグログにはエントリーが正常に記録されていることが示されますが、TPS Web UI にはトークンは表示されません。

この問題が修正されるまでの回避策として、次の例のように **tps-token-find** コマンドを使用してトークンを一覧表示します。

```
# pki -d /opt/pki/certdb/ -c SECret.123 -p 25443 -n 'PKI TPS Administrator for Example.Org'
tps-token-find
```

pki-core パッケージの既知の問題:

auditSigningCert に属性がないため、HSM を使用した KRA のクローン作成が失敗する

HSM を使用して KRA のクローンを作成する場合に、**auditSigningCert** の信頼属性 **u,u,Pu** がマスターとクローンのエイリアス DB の間で暗黙的に同期されるはずですが、クローンのエイリアス DB での複製に失敗するようになりました。結果として、HSM を使用した KRA のクローン作成は、**auditSigningCert cert-topology-02-KRA KRA is invalid: Invalid certificate: (-8101) Certificate type not approved for application** というエラーで失敗します。

この問題を回避するには、**auditSigningCert** の **u,u,Pu** 信頼属性をクローン KRA のエイリアス DB に明示的に追加し、インスタンスを再起動する必要があります。以下に例を示します。

- 回避策の前:

```
# certutil -vv -V -d /var/lib/pki/clone-KRA/alias/ -h nfast -n 'token:auditSigningCert cert-
topology-02-KRA KRA' -u J
  Enter Password or Pin for "token":
  certutil: certificate is invalid: Certificate type not approved for application.
```

- 回避策の後:

```
# certutil -M -d /var/lib/pki/clone-KRA/alias/ -n 'token:auditSigningCert cert-topology-
02-KRA KRA' -t u,u,Pu
# certutil -vv -V -d /var/lib/pki/clone-KRA/alias/ -h nfast -n 'token:auditSigningCert cert-
topology-02-KRA KRA' -u J
  Enter Password or Pin for "token":
  certutil: certificate is valid
```

--agent-uid pkidbuser オプションを指定して cert-fix ユーティリティーを使用すると Certificate System が破損

--agent-uid pkidbuser オプションを指定して **cert-fix** ユーティリティーを使用すると、Certificate System の LDAP 設定が破損します。したがって、Certificate System は不安定になり、システムの復元に手動の操作が必要になる可能性があります。

第4章 RED HAT ENTERPRISE LINUX 8.4 上の RED HAT CERTIFICATE SYSTEM 10.2

このセクションでは、注目すべき更新と新機能、重要なバグ修正、ユーザーが知っておくべき現在の既知の問題など、RHEL 8.4 上の Red Hat Certificate System 10.2 の重要な変更を説明します。

注記

Red Hat Certificate System を以前のマイナーバージョンにダウングレードすることはサポートされていません。

4.1. CS 10.2 の更新と新機能

このセクションでは、Red Hat Certificate System 10.2 の新機能および重要な更新を説明します。

pki-core パッケージの更新と新機能:

Certificate System パッケージがバージョン 10.10.5 にリベース

pki-core、**redhat-pki**、**redhat-pki-theme**、および **pki-console** パッケージがアップストリームバージョン 10.10.5 にアップグレードされ、以前のバージョンに対するバグ修正や機能強化が数多く追加されました。

4.2. テクノロジープレビュー

テクノロジープレビュー機能として RHCS で ACME がサポートされるように

Automated Certificate Management Environment (ACME) レスポンダーを介したサーバー証明書の発行は、Red Hat Certificate System (RHCS) で利用できます。ACME レスポンダーは ACME v2 プロトコル (RFC 8555) をサポートします。

以前は、ユーザーは認証局 (CA) の独自の証明書署名要求 (CSR) 送信ルーチンを使用する必要がありました。ルーチンでは、要求を手動で確認して証明書を発行するために、認証局 (CA) エージェントが必要になる場合がありました。

RHCS ACME レスポンダーは、CA エージェントを使用せずに、サーバー証明書の自動発行とライフサイクル管理のための標準メカニズムを提供するようになりました。この機能により、RHCS CA を既存の証明書発行インフラストラクチャーと統合して、デプロイメント用のパブリック CA と開発用の内部 CA をターゲットにすることができます。

このテクノロジープレビューには、ACME サーバーのサポートのみが含まれていることに注意してください。ACME クライアントが、このリリースに同梱されているわけではありません。さらに、この ACME プレビューは、発行データを保持したり、ユーザー登録を処理したりしません。

今後、Red Hat Enterprise Linux が更新されることで、ACME のインストールで問題が発生する可能性があることに注意してください。

詳細は、IETF definition of ACME を参照してください。

注記

この機能はテクノロジープレビューとして提供され、今後の製品機能への早期アクセスを提供し、サブスクリプション契約ではまだ完全にはサポートされていないことに注意してください。

4.3. CS 10.2 のバグ修正

この箇所では、ユーザーに重大な影響を及ぼしていて、Red Hat Certificate System 10.2 で修正されたバグを説明します。

pki-core パッケージでのバグ修正

PKI CA に接続された PKI ACME Responder が発行した証明書で OCSP 検証に失敗しなくなる

以前のバージョンでは、PKI CA が提供するデフォルトの ACME 証明書プロファイルには、実際の OCSP サービスを参照していないサンプル OCSP URL が含まれていました。これにより、PKI ACME Responder が PKI CA 発行者を使用するように設定されている場合に、この Responder が発行する証明書は OCSP 検証に失敗する可能性がありました。今回の更新で、ACME 証明書プロファイルのハードコーディングされた URL が削除され、カスタマイズしない場合にプロファイル設定ファイルを修正するアップグレードスクリプトが追加されました。

pki-tools ファイルが 1 つのフォルダーに

pki-tools パッケージの以下のファイルは、別々の **java-tools** フォルダーおよび **native-tools** フォルダーにありました。

- **/usr/share/pki/java-tools/DRMTool.cfg**
- **/usr/share/pki/java-tools/KRATool.cfg**
- **/usr/share/pki/native-tools/setpin.conf**

一貫性を保つために、以下が 1 つのフォルダーに統合されました。

- **/usr/share/pki/tools/DRMTool.cfg**
- **/usr/share/pki/tools/KRATool.cfg**
- **/usr/share/pki/tools/setpin.conf**

4.4. CS 10.2 の既知の問題

このパートでは、Red Hat Certificate System 10.2 でユーザーが知っておくべき既知の問題と、該当する場合は回避策を説明します。

pcsc-lite、pcsc-lite-ccid、および esc に関する既知の問題

Red Hat Certificate System 10.2 のリリース日時点で、現在利用できる **pcsc-lite** パッケージ、**pcsc-lite-ccid** パッケージ、および **esc** パッケージが含まれ、特定の SCP03 トークンおよび SCP01 トークンを使用したセキュアなチャネルの完了に失敗する可能性があります。RHEL 8.4 の今後のバッチ更新では、これらのパッケージの修正バージョンが提供されます。

HSM を使用した KRA のクローン作成が失敗する

HSM を使用した KRA のクローン作成が失敗し、クローンのデバッグログに **auditSigningCert cert-topology-02-KRA KRA is invalid: Invalid certificate: (-8101) Certificate type not approved for application** エラーが表示されます。

SubCA 署名証明書の検証中に SubCA の 2 段階インストールに失敗する

2 段階の方法を使用した SubCA のインストールは、FIPS が有効になっている HSM 環境では失敗します。RSA オプションまたは ECC オプションのいずれかを使用すると、SubCA 署名証明書がエラーを返します。

TPS では匿名バインドの ACI アクセスの追加が必要

以前のバージョンでは、匿名バインド ACI はデフォルトで許可されていましたが、LDAP では無効になっています。これにより、TPS スマートカードの登録またはフォーマットができなくなります。

この問題が修正されるまでの回避策として、Directory Server で匿名バインド ACI を手動で追加する必要があります。

```
$ ldapmodify -D "cn=Directory Manager" -W -x -p 3389 -h hostname -x <<EOF
dn: dc=example,dc=org
changetype: modify
add: aci
aci: (targetattr!="userPassword || aci")(version 3.0; acl "Enable anonymous access"; allow (read,
search, compare) userdn="ldap:///anyone";)
EOF
```

pki-core パッケージの既知の問題:

--agent-uid pkidbuser オプションを指定して cert-fix ユーティリティーを使用すると Certificate System が破損

--agent-uid pkidbuser オプションを指定して **cert-fix** ユーティリティーを使用すると、Certificate System の LDAP 設定が破損します。したがって、Certificate System は不安定になり、システムの復元に手動の操作が必要になる可能性があります。

第5章 RED HAT ENTERPRISE LINUX 8.3 上の RED HAT CERTIFICATE SYSTEM 10.1

このセクションでは、注目すべき更新と新機能、重要なバグ修正、ユーザーが知っておくべき現在の既知の問題など、RHEL 8.3 上の Red Hat Certificate System 10.1 の重要な変更を説明します。

注記

Red Hat Certificate System を以前のマイナーバージョンにダウングレードすることはサポートされていません。

5.1. CS 10.1 の更新と新機能

このセクションでは、Red Hat Certificate System 10.1 の新機能および重要な更新を説明します。

Certificate System パッケージがバージョン 10.9.0 にリベース

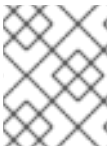
pki-core、**redhat-pki**、**redhat-pki-theme**、および **pki-console** パッケージがアップストリームバージョン 10.9.0 にアップグレードされ、以前のバージョンに対するバグ修正や機能強化が数多く追加されました。

JSS が FIPS 準拠の SSLContext を提供

以前のリリースでは、Tomcat は Java Cryptography Architecture (JCA) SSLContext クラスの SSLEngine ディレクティブを使用していました。デフォルトの SunJSSE 実装は連邦情報処理標準 (FIPS) に準拠していないため、PKI は JSS 経由で FIPS 準拠の実装を提供するようになりました。

サーバー側の Keygen 登録

多くの新しいバージョンのブラウザーでは、PKI キーを生成する機能と、キーアーカイブ用の CRMF のサポートが削除されています。この相互運用性を解決するために、Red Hat Certificate System 10.1 では、サーバー側の Keygen 登録メカニズムが導入されています。キーは KRA サーバーで生成され、PKCS#12 のクライアントに安全に転送されます。



注記

暗号化証明書にのみサーバー側 Keygen メカニズムを使用することが強く推奨されます。

主な機能

- 証明書要求キーは KRA で生成されます (注: CA と連携するには、KRA をインストールする必要があります)。
- プロファイルのデフォルトプラグイン **serverKeygenUserKeyDefaultImpl** により、キーアーカイブ (つまり **enableArchival**) を有効化または無効化できるように
- RSA 鍵と EC 鍵の両方のサポート
- 手動 (エージェント) 承認と自動承認 (ディレクトリーパスワードベースなど) の両方のサポート

CA 証明書の埋め込み署名証明書タイムスタンプを使用した CA 証明書送信

Red Hat Certificate System は、Certificate Transparency (CT) V1 サポートの基本バージョン (rfc 6962) を提供します。各デプロイメントサイトがルート CA 証明書を含めることを選択した信頼できるログか

ら、Signed Certificate Time スタンプ (SCT) が埋め込まれた証明書を発行する機能があります。複数の CT ログに対応するようにシステムを設定することもできます。この機能を使用するには、少なくとも 1 つの信頼できる CT ログが必要です。

重要

デプロイメントサイトが、信頼できる CT ログサーバーとの信頼関係を確立します。

pki-core パッケージの更新と新機能:

公開鍵基盤 (PKI) の全体的な正常性を確認できるようになる

pki-healthcheck ツールでは、公開鍵基盤 (PKI) 環境の正常性に影響を与える可能性のあるエラー状態を見つけ、報告できるチェック機能が含まれています。

PKI が、RSA PSS (Probabilistic Signature Scheme) 署名アルゴリズムに対応するようになる

今回の機能強化により、PKI は RSA PSS (Probabilistic Signature Scheme) 署名アルゴリズムに対応するようになりました。この機能を有効にするには、特定のサブシステムに対して **pkispawn** スクリプトファイルに以下の行を設定します (**pki_use_pss_rsa_signing_algorithm=True**)。

5.2. テクノロジープレビュー

テクノロジープレビュー機能として RHCS で ACME がサポートされるように

Automated Certificate Management Environment (ACME) レスポンダーを介したサーバー証明書の発行は、Red Hat Certificate System (RHCS) で利用できます。ACME レスポンダーは ACME v2 プロトコル (RFC 8555) をサポートします。

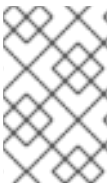
以前は、ユーザーは認証局 (CA) の独自の証明書署名要求 (CSR) 送信ルーチンを使用する必要がありました。ルーチンでは、要求を手動で確認して証明書を発行するために、認証局 (CA) エージェントが必要になる場合がありました。

RHCS ACME レスポンダーは、CA エージェントを使用せずに、サーバー証明書の自動発行とライフサイクル管理のための標準メカニズムを提供するようになりました。この機能により、RHCS CA を既存の証明書発行インフラストラクチャーと統合して、デプロイメント用のパブリック CA と開発用の内部 CA をターゲットにすることができます。

このテクノロジープレビューには、ACME サーバーのサポートのみが含まれていることに注意してください。ACME クライアントが、このリリースに同梱されているわけではありません。さらに、この ACME プレビューは、発行データを保持したり、ユーザー登録を処理したりしません。

今後、Red Hat Enterprise Linux が更新されることで、ACME のインストールで問題が発生する可能性があることに注意してください。

詳細は、IETF definition of ACME を参照してください。



注記

この機能はテクノロジープレビューとして提供され、今後の製品機能への早期アクセスを提供し、サブスクリプション契約ではまだ完全にはサポートされていないことに注意してください。

5.3. CS 10.1 のバグ修正

この箇所では、ユーザーに重大な影響を及ぼしていて、Red Hat Certificate System 10.1 で修正されたバグを説明します。

pki-core パッケージでのバグ修正

TPS インストールで Auditors グループを使用できるようになる

以前のバージョンでは、LDAP は TPS 固有の Auditor のグループエントリーを表示していました。新規インストールで、デフォルトの TPS **Auditors** グループが追加されました。このグループを使用するには、既存のインスタンスで手動の LDAP 手順を実行する必要があります。

1. これを修正するには、**ldapmodify** ユーティリティーを実行して問題の LDAP サーバーに接続し、不足しているオブジェクトを追加します。

```
$ ldapmodify -x -D "cn=Directory Manager" -w $PASSWORD << EOF
dn: cn=Auditors,ou=Groups,{rootSuffix}
changeType: add
objectClass: top
objectClass: groupOfUniqueNames
cn: Auditors
description: People who can read the signed audit logs for TPS
EOF
```

{rootSuffix} を、TPS 設定ファイルのベース DN (**pki_ds_base_dn**) に置き換えます。(例: **dc=tks,dc=pki,dc={DOMAIN…},dc={TLD}**)

これにより、既存の TPS インストールでは、新しい TPS インストールとともに **Auditors** グループを使用できます。

5.4. CS 10.1 の既知の問題

このパートでは、Red Hat Certificate System 10.1 でユーザーが知っておくべき既知の問題と、該当する場合は回避策を説明します。

TPS では匿名バインドの ACI アクセスの追加が必要

以前のバージョンでは、匿名バインド ACI はデフォルトで許可されていましたが、LDAP では無効になっています。これにより、TPS スマートカードの登録またはフォーマットができなくなります。

この問題が修正されるまでの回避策として、Directory Server で匿名バインド ACI を手動で追加する必要があります。

```
$ ldapmodify -D "cn=Directory Manager" -W -x -p 3389 -h hostname -x <<EOF
dn: dc=example,dc=org
changetype: modify
add: aci
aci: (targetattr!="userPassword || aci")(version 3.0; acl "Enable anonymous access"; allow (read,
search, compare) userdn="ldap:///anyone";)
EOF
```

pki-core パッケージの既知の問題:

PKI CA に接続する PKI ACME Responder が発行する証明書により、OCSP の検証が失敗する可能性がある

PKI CA が提供するデフォルトの ACME 証明書プロファイルには、実際の OCSP サービスを参照しない

サンプル OCSP URL が含まれています。これにより、PKI ACME Responder が PKI CA 発行者を使用するように設定されている場合、レスポンダーが発行する証明書は OCSP 検証に失敗する可能性があります。

この問題を回避するには、**/usr/share/pki/ca/profiles/ca/acmeServerCert.cfg** 設定ファイルの **policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0** プロパティーを空の値に設定する必要があります。

1. ACME Responder 設定ファイルで **policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0=http://ocsp.example.com** を **policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0=** に変更します。

2. サービスを再起動して、証明書を再生成します。

これにより、PKI CA は、実際の OCSP サービスを参照する自動生成 OCSP URL で ACME 証明書を生成します。

--agent-uid pkidbuser オプションを指定して **cert-fix** ユーティリティーを使用すると Certificate System が破損

--agent-uid pkidbuser オプションを指定して **cert-fix** ユーティリティーを使用すると、Certificate System の LDAP 設定が破損します。したがって、Certificate System は不安定になり、システムの復元に手動の操作が必要になる可能性があります。

第6章 RED HAT ENTERPRISE LINUX 8.2 上の RED HAT CERTIFICATE SYSTEM 10.0

このセクションでは、注目すべき更新と新機能、重要なバグ修正、ユーザーが知っておくべき現在の既知の問題など、RHEL 8.2 上の Red Hat Certificate System 10.0 の重要な変更を説明します。

6.1. CS 10.0 の更新と新機能

このセクションでは、Red Hat Certificate System 10.0 の新機能および重要な更新を説明します。

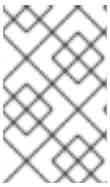
Certificate System パッケージがバージョン 10.8.3 にリベース

pki-core、**redhat-pki**、**redhat-pki-theme**、および **pki-console** パッケージがアップストリームバージョン 10.8.3 にアップグレードされ、以前のバージョンに対するバグ修正や機能強化が数多く追加されました。

pki-core パッケージの更新と新機能:

テクノロジープレビューとして、公開鍵基盤の全体的な正常性を確認できるようになる

pki-healthcheck ツールでは、公開鍵基盤 (PKI) 環境の正常性に影響を与える可能性のあるエラー状態を見つけ、報告できるチェック機能が含まれています。



注記

この機能はテクノロジープレビューとして提供され、今後の製品機能への早期アクセスを提供し、サブスクリプション契約ではまだ完全にはサポートされていないことに注意してください。

pki subsystem-cert-find コマンドおよび pki subsystem-cert-show コマンドが証明書のシリアル番号を表示

今回の機能強化により、Certificate System の **pki subsystem-cert-find** コマンドおよび **pki subsystem-cert-show** コマンドでは、出力の証明書のシリアル番号が表示されるようになりました。シリアル番号は重要な情報であり、他の複数のコマンドで必要になることがよくあります。その結果、証明書のシリアル番号を識別するのが容易になりました。

pki user コマンドおよび pki group コマンドが、Certificate System で非推奨になる

今回の更新で、Certificate System の新しい **pki <subsystem>-user** コマンドおよび **pki <subsystem>-group** コマンドが、**pki user** コマンドおよび **pki group** コマンドに置き換わりました。以前のコマンドは引き続き機能しますが、コマンドが非推奨となり、新しいコマンドを参照するようにというメッセージが表示されます。

Certificate System がシステム証明書のオフライン更新をサポートするようになる

今回の機能強化により、管理者はオフライン更新機能を使用して、Certificate System で設定されているシステム証明書を更新できます。システム証明書の期限が切れると、Certificate System が起動できなくなります。この機能強化により、管理者は期限切れのシステム証明書を置き換える必要がなくなりました。

Certificate System は、外部 CA 署名用の SKI 拡張機能を備えた CSR を作成できるようになる

この機能拡張により、Certificate System は、外部認証局 (CA) 署名用の SKI (Subject Key Identifier) 拡張機能を使用した証明書署名要求 (CSR) の作成をサポートします。特定の CA は、特定の値で、または

CA 公開鍵から派生したこの拡張を必要とします。これにより、管理者は **pkispawn** ユーティリティーに渡される設定ファイルの **pki_req_ski** パラメーターを使用して、SKI 拡張子を持つ CSR を作成できるようになりました。

6.2. テクノロジープレビュー

テクノロジープレビュー機能として RHCS で ACME がサポートされるように

Automated Certificate Management Environment (ACME) レスポンダーを介したサーバー証明書の発行は、Red Hat Certificate System (RHCS) で利用できます。ACME レスポンダーは ACME v2 プロトコル (RFC 8555) をサポートします。

以前は、ユーザーは認証局 (CA) の独自の証明書署名要求 (CSR) 送信ルーチンを使用する必要がありました。ルーチンでは、要求を手動で確認して証明書を発行するために、認証局 (CA) エージェントが必要になる場合がありました。

RHCS ACME レスポンダーは、CA エージェントを使用せずに、サーバー証明書の自動発行とライフサイクル管理のための標準メカニズムを提供するようになりました。この機能により、RHCS CA を既存の証明書発行インフラストラクチャーと統合して、デプロイメント用のパブリック CA と開発用の内部 CA をターゲットにすることができます。

このテクノロジープレビューには、ACME サーバーのサポートのみが含まれていることに注意してください。ACME クライアントが、このリリースに同梱されているわけではありません。さらに、この ACME プレビューは、発行データを保持したり、ユーザー登録を処理したりしません。

今後、Red Hat Enterprise Linux が更新されることで、ACME のインストールで問題が発生する可能性があることに注意してください。

詳細は、IETF definition of ACME を参照してください。

注記

この機能はテクノロジープレビューとして提供され、今後の製品機能への早期アクセスを提供し、サブスクリプション契約ではまだ完全にはサポートされていないことに注意してください。

6.3. CS 10.0 のバグ修正

この箇所では、ユーザーに重大な影響を及ぼしていて、Red Hat Certificate System 10.0 で修正されたバグを説明します。

pki-core パッケージでのバグ修正

pkidestroy ユーティリティーが正しいインスタンスを選択するように

以前のリリースでは、半分削除されたインスタンスで **pkidestroy --force** コマンドを実行すると、**-i instance** オプションでインスタンス名を指定していても、デフォルトで **pki-tomcat** インスタンスが選択されていました。これにより、目的のインスタンスではなく、**pki-tomcat** インスタンスが削除され、**--remove-logs** オプションを指定しても、目的のインスタンスのログが削除されませんでした。**pkidestroy** は、正しいインスタンス名を適用し、目的のインスタンスの残り物のみを削除するようになりました。

Nuxwdog サービスは、HSM 環境で PKI サーバーの起動に失敗しなくなる

以前のリリースでは、バグにより、**keyutils** パッケージが **pki-core** パッケージの依存関係としてインストールされませんでした。さらに、**Nuxwdog** ウォッチドッグサービスでは、ハードウェアセキュリ

ティーモジュール (HSM) を使用する環境で公開鍵基盤 (PKI) サーバーを起動できませんでした。これらの問題は修正されています。その結果、必要な **keyutils** パッケージが依存関係として自動的にインストールされ、**Nuxwdog** が、HSM を使用する環境で想定通りに PKI サーバーを起動するようになりました。

Certificate System がサービスの起動時に SetAllPropertiesRule 操作の警告をログに記録しなくなる

以前は、Certificate System は、サービスの開始時に **/var/log/messages** ログファイルの **SetAllPropertiesRule** 操作で警告を記録していました。この問題は修正され、上記の警告はログに記録されなくなりました。

Certificate System がデバッグログのローテーションをサポートするように

以前は、Certificate System は、ログローテーションに対応しないカスタムのログフレームワークを使用していました。これにより、**/var/log/pki/instance_name/ca/debug** などのデバッグログが無限に増大しました。今回の更新では、Certificate System は、ログローテーションに対応する java.logging.util フレームワークを使用するようになり、**/var/lib/pki/instance_name/conf/logging.properties** ファイルでログローテーションを設定できます。

Certificate System KRA クライアントは、Key Request のレスポンスを正しく解析する

Certificate System が新しい JSON ライブラリーに切り替わりました。その結果、特定のオブジェクトのシリアライズが異なり、Python のキーリカバリー認証局 (KRA) クライアントが、**鍵要求** の応答を解析できませんでした。クライアントは、古い JSON ライブラリーと新しい JSON ライブラリーの両方を使用した応答に対応するように修正されました。これにより、Python KRA クライアントは **キー要求** 応答を正しく解析します。

6.4. CS 10.0 の既知の問題

このパートでは、Red Hat Certificate System 10.0 でユーザーが知っておくべき既知の問題と、該当する場合は回避策を説明します。

TPS では匿名バインドの ACI アクセスの追加が必要

以前のバージョンでは、匿名バインド ACI はデフォルトで許可されていましたが、LDAP では無効になっています。これにより、TPS スマートカードの登録またはフォーマットができなくなります。

この問題が修正されるまでの回避策として、Directory Server で匿名バインド ACI を手動で追加する必要があります。

```
$ ldapmodify -D "cn=Directory Manager" -W -x -p 3389 -h hostname -x <<EOF
dn: dc=example,dc=org
changetype: modify
add: aci
aci: (targetattr!="userPassword || aci")(version 3.0; acl "Enable anonymous access"; allow (read,
search, compare) userdn="ldap:///anyone";)
EOF
```

pki-core パッケージの既知の問題:

--agent-uid pkidbuser オプションを指定して cert-fix ユーティリティーを使用すると Certificate System が破損

--agent-uid pkidbuser オプションを指定して **cert-fix** ユーティリティーを使用すると、Certificate System の LDAP 設定が破損します。したがって、Certificate System は不安定になり、システムの復元に手動の操作が必要になる可能性があります。