



Red Hat Satellite 5.8

クライアント設定ガイド

Red Hat Satellite との Red Hat Enterprise Linux クライアントの設定、登録、更新

Red Hat Satellite 5.8 クライアント設定ガイド

Red Hat Satellite との Red Hat Enterprise Linux クライアントの設定、登録、更新

Red Hat Satellite Documentation Team
satellite-doc-list@redhat.com

法律上の通知

Copyright © 2017 Red Hat.

This document is licensed by Red Hat under the [Creative Commons Attribution-ShareAlike 3.0 Unported License](https://creativecommons.org/licenses/by-sa/3.0/). If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

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, 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 Software Collections 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

本ガイドは、Red Hat Enterprise Linux システムを適切に設定して Red Hat Satellite に登録し、またそこから更新をダウンロードする方法を解説します。登録方法や最新パッケージの導入方法、サーバーとクライアントの同期に関するその他のトピックが説明されています。詳細情報に関しては、Red Hat Satellite スタートガイドおよび Red Hat Satellite インストールガイドを参照してください。

目次

第1章 はじめに	3
第2章 クライアントアプリケーションの設定	4
2.1. クライアントを RED HAT SATELLITE SERVER に登録	5
2.2. アクティベーションキーを使ってクライアントを RED HAT SATELLITE に登録	5
2.3. 手作業による設定ファイルの更新	6
2.4. サーバーフェイルオーバーの実装	6
2.5. ステージングコンテンツの有効化	7
第3章 SSL インフラストラクチャー	9
3.1. SSL の概要	9
3.2. RED HAT SATELLITE SSL MAINTENANCE TOOL	10
3.3. 認証機関の SSL パブリック証明書のクライアントへの配備	14
3.4. 証明書を使用するクライアントシステムの設定	14
第4章 ソフトウェアの障害レポート	16
4.1. ソフトウェア障害レポートツールのインストール	16
4.2. ソフトウェア障害レポートツールの使用	16
4.3. 手動でのソフトウェア障害レポート	16
4.4. テスト用のソフトウェア障害の作成	17
付録A 改訂履歴	18

第1章 はじめに

本書は、Red Hat Satellite および Red Hat Satellite Proxy をご利用のお客様がクライアントシステムを構成する際に手助けとなるガイドです。

デフォルトでは、Red Hat Network クライアントのアプリケーションはすべて Red Hat Network の中央サーバーと通信するよう設定されています。そうではなく、クライアントが Red Hat Satellite または Red Hat Proxy に接続すると、デフォルト設定は変更されます。本ガイドでは、数百または数千台のシステムを有する大規模な企業環境向けに、そのデフォルト設定変更に役立つシステムの大規模な再設定の手順を紹介しています。

この作業は複雑となるため、お客様はフィールドが入力済みのスクリプトを活用して Satellite や Satellite Proxy サーバーへのアクセスに必要な多くの作業を自動化することができます。詳細は『スタートガイド』を参照してください。実際に自動で何が行われるのかを理解しておくに役立ち、初めの章ではこうした自動化で行われる再設定を手作業で行う場合の手順について説明しています。状況に応じて理想的なソリューションを決める際にお役立てください。

このガイドに記載されているコマンドの多くは表示通りに適用できる場合もありますが、さまざまな企業で採用されているネットワーク構成すべてをここで予想することは不可能となります。このため Red Hat では、それぞれの使用環境に応じた設定を考慮に入れコマンドは参照として利用されることをお勧めします。

第2章 クライアントアプリケーションの設定

Red Hat Satellite への登録など Red Hat Network のエンタープライズクラスの機能を活用するには、最新のクライアントアプリケーションの設定が必要になります。ところがクライアントを Red Hat Network に登録する前にこうしたアプリケーションを取得するのは困難です。この矛盾は、特に旧式のシステムを大量に Red Hat Network へ移行する場合に問題となります。本章ではこの問題を解決する技術をみていきます。



重要

Red Hat では、Red Hat Proxy Server もしくは Red Hat Satellite Server に接続しているクライアントが Red Hat Enterprise Linux 最新アップデートを実行して適切な接続を確保することを強く推奨しています。

また、クライアントにファイアウォールを設定している場合は Red Hat Network と正しく動作させるためにポート 80 と 443 を開いておいてください。

組織内で全員が Red Hat Satellite または Red Hat Proxy への接続の安全性を確保したり、カスタムパッケージの GPG キーのビルドや配備を行う必要はありませんが、Red Hat Satellite や Red Hat Proxy を使用する各ユーザーは以下を再設定する必要があります。

- **Red Hat Update Agent** - Red Hat チャンネルの更新メカニズムです。Update Agent の使用は、オペレーティングシステムによって異なります。
 - Red Hat Enterprise Linux 5、6、および 7 の場合: **yum** プラグイン (**yum-rhn-plugin**) として使用。
 - Red Hat Enterprise Linux 3 および 4: スタンドアロンアプリケーション (**up2date**) として使用。
- **Red Hat Network Registration Client (rhn_register)** - クライアントを登録するメカニズムです。デフォルトでは、**rhn_register** はメインの Red Hat Network サーバーに対して登録します。Red Hat Satellite または Red Hat Proxy に対して登録するには、クライアントシステムを再設定する必要があります。



重要

デフォルトでは、Red Hat Enterprise Linux 5、6 および 7 での **yum** コマンドはリモートのリポジトリとの通信に SSL を使用します。このため、ファイアウォールがポート 443 での接続を許可するようにする必要があります。

SSL を迂回させる場合は **/etc/sysconfig/rhn/up2date** ファイルで **serverURL** の値を **https** から **http** に変更します。同様に、Red Hat Network のモニタリング機能や Red Hat Network のモニタリングデーモンを必要とするプローブを使用するには、クライアントシステムがポート 4545 (**sshd** 使用の場合はポート 22) での接続を許可する必要があります。

Red Hat Update Agent の最新バージョンは複数の Red Hat Satellite サーバーに対応するよう設定できるため、プライマリサーバーがアクセス不能になった場合にフェイルオーバーによって保護されます。この機能を有効にする方法については「[サーバーフェイルオーバーの実装](#)」を参照してください。

次のセクションでは、クライアントシステムが Red Hat Satellite または Proxy にアクセスする設定方法について説明しています。設定コマンドをスクリプト化する方法については Red Hat Satellite 『スタートガイド』を参照してください。

2.1. クライアントを RED HAT SATELLITE SERVER に登録

以下の手順では、**rhn_register** コマンドを使って Red Hat Satellite にシステムを登録する方法を解説します。例にあるホスト名とドメイン名は、実際の設定に適用されるものに置き換えてください。

手順2.1 rhn_register を使ってシステムを Red Hat Satellite に登録する方法:

1. **/usr/share/rhn/** ディレクトリーに切り替え、SSL 証明書をクライアントにダウンロードします。

```
# cd /usr/share/rhn/  
# wget http://satellite.example.com/pub/RHN-ORG-TRUSTED-SSL-CERT
```

2. **/etc/sysconfig/rhn/up2date** ファイルを編集し、以下のエントリーがあることを確認します。

```
serverURL=https://satellite.example.com/XMLRPC  
noSSLServerURL=http://satellite.example.com/XMLRPC  
sslCACert=/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT
```

3. **rhn_register** コマンドを使用してマシンを登録します。

```
# rhn_register
```

2.2. アクティベーションキーを使ってクライアントを RED HAT SATELLITE に登録

Red Hat では、Red Hat Proxy または Red Hat Satellite にアクセスするクライアントシステムの登録および設定にアクティベーションキーを使用することを推奨しています。アクティベーションキーを使うと、1 回の作業で複数のシステムの登録、エンタイトルメント、サブスクリプションが実行できます。アクティベーションキーの詳細については、Red Hat Satellite 『スタートガイド』を参照してください。

手順2.2 アクティベーションキーを使ってシステムを Red Hat Satellite に登録する方法:

1. アクティベーションキーを生成します。Red Hat Satellite 『スタートガイド』の「アクティベーションキーの使用」を参照してください。
2. カスタムの GPG キーをインポートします。
3. Red Hat Proxy または Red Hat Satellite の **/pub/** ディレクトリーから SSL 証明書の RPM をダウンロードしてインストールします。以下のようになります (URL をご使用の環境に合わせてください)。

```
# rpm -Uvh http://satellite.example.com/pub/rhn-org-trusted-ssl-  
cert-1.0-1.noarch.rpm
```

4. システムを Red Hat Proxy または Red Hat Satellite に登録します。

```
# rhnreg_ks --activationkey mykey --serverUrl  
https://satellite.example.com/XMLRPC --sslCACert=/usr/share/rhn/RHN-  
ORG-TRUSTED-SSL-CERT
```

この代わりに、Satellite が生成するブートストラップスクリプト (**bootstrap.sh**) を使用することもできます。Red Hat Satellite Server と Red Hat Proxy Server の両方で使用できるブートストラップスクリプトはこのようなスクリプトです。スクリプトの生成に関する詳細は、『Getting Started Guide』の『4.1.1. Using Red Hat Network Bootstrap to Register a System』に記載されています。

ブートストラップスクリプトを取得するには、次のコマンドを実行します。

```
wget http://satellite.example.com/pub/bootstrap/bootstrap.sh
```



重要

Satellite サーバー上でブートストラップスクリプトが生成された後、そのスクリプトを手作業で編集する必要があります。編集されていないブートストラップスクリプトを最初に実行すると、手作業による編集が必要であることを伝えるメッセージが表示されます。スクリプトをクライアントにダウンロードする前に、指示にしたがって Satellite サーバーでブートストラップスクリプトを編集します。

2.3. 手作業による設定ファイルの更新

前のセクションで説明した GUI インターフェースによる設定の代替方法として、アプリケーションの設定ファイルを編集することで **Red Hat Update Agent** の再設定を行うこともできます。

Red Hat Proxy Satellite に接続しているクライアントシステム上の **Update Agent** を設定するには、**/etc/sysconfig/rhn/up2date** 設定ファイル内の **serverURL** と **noSSLServerURL** の値を (root で) 編集します。デフォルトの Red Hat Network URL を Proxy または Satellite の完全修飾ドメイン名 (FQDN) に置き換えてください。例えば、以下のようになります。

```
serverURL[comment]=Remote server URL
serverURL=https://your_primary.your_domain.com/XMLRPC

noSSLServerURL[comment]=Remote server URL without SSL
noSSLServerURL=http://your_primary.your_domain.com/XMLRPC
```



警告

/etc/sysconfig/rhn/up2date 内の **httpProxy** 設定では Red Hat Proxy は参照されません。この値は、オプションとなるクライアント用 HTTP プロキシを設定する場合に使用されます。Red Hat Proxy が適切に設定されている場合、**httpProxy** の値は空白にしておいてください (値を設定しない)。

2.4. サーバーフェイルオーバーの実装

手順2.3 サーバーのフェイルオーバーを実装する方法:

1. Red Hat Enterprise Linux 5、6、または 7 を稼働していること確認します。Red Hat Enterprise Linux 3 または 4 の場合、最新バージョンの **up2date** を使用します。
2. セカンダリサーバーを **/etc/sysconfig/rhn/up2date** 設定ファイルの **serverURL** と

noSSLServerURL に (root になって) 手作業で追加します。

3. Red Hat Proxy または Red Hat Satellite の完全修飾ドメイン名 (FQDN) をプライマリサーバーの直後にセミコロン (;) で分けて追加します。ご使用のクライアントは、ここで示された順番にこれらのサーバーへの接続を試みます。必要な数のサーバーを含めてください。例えば、以下ようになります。

```
serverURL[comment]=Remote server URL
serverURL=https://satellite.example.com/XMLRPC;
https://your_secondary.your_domain.com/XMLRPC;

noSSLServerURL[comment]=Remote server URL without SSL
noSSLServerURL=http://satellite.example.com/XMLRPC;
http://your_secondary.your_domain.com/XMLRPC;
```

2.5. ステージングコンテンツの有効化

ステージングコンテンツは、予定されたインストールを行う前にクライアントシステムでパッケージまたはエラータの配備をステージングする機能です。予定された配備の 24 時間前以内にクライアントは RPM の内容をシステムのローカルディスクに事前ダウンロードします。その後、予定されたアクションを実行するときに特定のパッケージおよびエラータはクライアント上でキャッシュされます。これにより、以下が実現されます。

- ステージングコンテンツがない場合よりも迅速にインストールを行えます。
- クライアントのリクエストを Satellite サーバーに分散できます。
- クライアントパッケージのインストールおよびアップグレードに必要な時間が短縮されます。

前提条件

Red Hat Enterprise Linux 5.6 以上または Red Hat Enterprise Linux 6.1 以上がクライアント側に必要になります。

この機能は、Satellite 上ではデフォルトで無効になっています。クライアントのデフォルト設定ファイルは有効になっています。ステージングコンテンツを使用するには、使用する各組織のクライアントシステム上と Satellite サーバー内で有効にする必要があります。

Satellite サーバー上のステージングコンテンツを有効にするには、**管理** → **組織** と選択し、対象の企業または組織をクリックした後、**設定** タブで **ステージングコンテンツの有効化** オプションを選択します。

クライアント上でステージングコンテンツを有効にするには、テキストエディターで **/etc/sysconfig/rhn/up2date** ファイルを開き、以下の行が含まれるように編集します。

```
stagingContent[comment]=Retrieve content of future actions in advance
stagingContent=1

...

stagingContentWindow[comment]=How much forward we should look for future
actions. In hours
stagingContentWindow=24
```

これらのエントリーが含まれていないと、クライアント内のステージングコンテンツはデフォルトで無効になり、時間帯は 24 時間前になります。

```
stagingContent=0  
stagingContentWindow=24
```

第3章 SSL インフラストラクチャー

Red Hat Satellite を使用するお客様にとって安全性は最重要の関心事となります。Red Hat Satellite の長所の 1 つは各要求をすべて SSL (Secure Sockets Layer) プロトコルを使用して処理できる点にあります。このレベルでの安全性を維持するために、独自のインフラストラクチャー内に Red Hat Satellite をインストールしている場合は、カスタムの SSL キーと証明書を作成する必要があります。

SSL キーと証明書を手作業で作成し配備する作業はかなり複雑になる可能性があります。Red Hat Proxy Server と Red Hat Satellite Server はいずれも、インストール時に独自のプライベート認証機関 (CA) に基づく SSL キーと証明書を作成することができます。また、これらの作業のための **Red Hat Satellite SSL Maintenance Tool** という別のコマンドラインユーティリティもあります。いずれにしても、管理しているインフラストラクチャー内の全システムにこれらのキーと証明書を配備する必要があります。多くの場合、こうした SSL キーと証明書の導入は自動化されています。本章ではこうした作業を行う上で効率的な方法について説明していきます。



注記

本章では SSL については詳しく説明していません。Red Hat Satellite **SSL Maintenance Tool** は、このパブリックキーのインフラストラクチャー (PKI) のセットアップや保守に関連する複雑な部分を表示しないように設計されています。詳細については Red Hat Enterprise Linux 『導入ガイド』の関連セクションを参照してください。

3.1. SSL の概要

SSL は、クライアントとサーバーのアプリケーションが安全に情報を受け渡しできるようにするプロトコルです。SSL ではパブリックキーとプライベートキーの組み合わせ方式を使用してクライアントとサーバー間で行われる通信を暗号化します。パブリック証明書はアクセス可能な場所に配置しますが、プライベートキーは安全な場所に保管しておく必要があります。プライベートキーとそのペアとなるパブリック証明書との厳密な関係 (デジタル署名) によってこのシステムが動作します。この関係により、信頼できる接続が確立されます。



注記

本書内の SSL プライベートキーとパブリック証明書は、プライベートキーとパブリックキーというようにいずれもキーと表現されていることがあります。しかし、SSL についての説明では、慣例的に SSL キーペア (またはキーセット) のペアとなるパブリックキーを SSL パブリック証明書と呼んでいます。

組織の SSL インフラストラクチャは一般的に以下に挙げる SSL キーと証明書で構成されています。

- 認証機関 (CA) の SSL プライベートキーとパブリック証明書: 通常、1 組織に対して 1 組しか生成されません。パブリック証明書はそのプライベートキーによってデジタル署名されます。パブリック証明書はすべてのシステムに配布されます。
- Web サーバーの SSL プライベートキーとパブリック証明書: アプリケーションサーバー 1 台に対して 1 組になります。パブリック証明書はそのプライベートキーと認証機関 (CA) の SSL プライベートキーの両方によってデジタル署名されます。中間的な SSL 証明書の要求が発生するため、Web サーバーのキー セット とよく呼ばれます。この使用目的の詳細はここでは重要ではありません。Web サーバーの SSL プライベートキー、パブリック証明書、そして認証機関 (CA) の SSL プライベートキーの 3 つすべてを Red Hat Satellite サーバーに配備します。

以下のシナリオで概念をわかりやすく視覚化してみます。例えば、Red Hat Satellite Server 1 台、Red Hat Proxy Server 5 台を備えた企業では、認証機関の SSL キーペア 1 組と Web サーバーの SSL キー 6 セットを生成する必要があります。認証機関の SSL パブリック証明書は全システムに配信さ

れ、すべてのクライアントによって各アップストリームサーバーへの接続を確立するため使用されます。各サーバーにはサーバー独自の SSL キーセットがあり、このキーセットはサーバーのホスト名に明確に関連付けられ、そのサーバーの SSL プライベートキーと認証局の SSL プライベートキーの組み合わせを使って生成されます。これにより Web サーバーの SSL パブリック証明書と認証機関の SSL キーペア、サーバーのプライベートキーとの間でデジタル的に検証可能な関連付けが確立されます。Web サーバーのキーセットは他の Web サーバーとは共有できません。



重要

このシステムの最も重要な部分は認証機関の SSL キーペアになります。このプライベートキーとパブリック証明書から、管理者はどの Web サーバーの SSL キーセットも再生成することができます。この認証機関の SSL キーペアは必ず安全な場所に保管してください。複数のサーバーで構成される Red Hat Satellite のインフラストラクチャー全体の設定が完了し稼働を開始したら、このツールもしくはインストーラで生成された SSL のビルドディレクトリーを別のメディアにアーカイブし、認証機関のパスワードを書き留め、このメディアとパスワードを安全な場所に保管することを強く推奨します。

3.2. RED HAT SATELLITE SSL MAINTENANCE TOOL

Red Hat Satellite では安全な組織インフラストラクチャーの管理を容易にするコマンドラインツールを提供しています。**Red Hat Satellite SSL Tool** はそのコマンドである **rhn-ssl-tool** でよく知られています。このツールは **spacewalk-certs-tools** パッケージの一部となります。最新の Red Hat Proxy Server と Red Hat Satellite Server (および Red Hat Satellite Server ISO) のソフトウェアチャンネル内にあります。**Red Hat Satellite SSL Tool** により、組織が独自の認証機関 SSL キーペアや Web サーバーの SSL キーセット (キーペアとも呼ばれる) を生成できるようになります。

このツールは単なるビルドツールで、必要なすべての SSL キーと証明書を生成します。また、全クライアントマシンへの配信やインストールを素早く行なえるよう複数のファイルを RPM 形式にパッケージ化します。ただし、配備は行いません。配備に関しては管理者が行なうことになります。多くの場合 Red Hat Satellite Server によって自動化されます。



注記

rhn-ssl-tool を収納している **spacewalk-certs-tools** は、最低限の要件を満たしている現在の Red Hat Enterprise Linux システムであれば、いずれにもインストールして実行することができます。ワークステーション、もしくは Satellite や Proxy サーバー以外の別のシステムから SSL インフラストラクチャーの管理を希望する管理者向けに提供されている機能です。

Red Hat Satellite SSL Tool は以下の状況で必要となります。

- 認証機関のパブリック証明書を更新する場合
- 中央の Red Hat Satellite Server にトップレベルサービスとして接続する Red Hat Proxy Server 3.6 またはそれ以降をインストールする場合。安全上、ホストされているサーバーは、認証機関の SSL キーと証明書のリポジトリとすることはできません。このキーペアは組織外に公開されないためです。
- 以前は SSL を使用していなかった Satellite または Proxy インフラストラクチャーを SSL を使用するよう再構成する場合
- 複数の Red Hat Satellite Server を Red Hat Satellite インフラストラクチャーに追加する場合。この作業に関しては Red Hat の担当者にお問い合わせください。

Red Hat Satellite SSL Tool は、以下の状況では **不要** となります。

- Red Hat Satellite Server のインストール中。すべての SSL 設定は、インストール中に行われます。SSL キーと証明書は自動的に作成され配備されます。
- Red Hat Satellite Server 3.6 またはそれ以降にトップレベルサービスとして接続されている場合の Red Hat Proxy Server 3.6 またはそれ以降のインストール中。Red Hat Satellite Server には、Red Hat Proxy Server の SSL キーおよび証明書の設定、作成、配備に必要なすべての SSL 情報が含まれています。

Red Hat Satellite Server と Red Hat Proxy Server のインストール手順では、各サーバーの `/pub` ディレクトリーに認証機関の SSL パブリック証明書が必ず配備されるようになっています。このパブリック証明書はクライアントシステムが Red Hat Satellite Server に接続を行う際に使用されます。詳細については「[認証機関の SSL パブリック証明書のクライアントへの配備](#)」を参照してください。

つまり、組織の Satellite もしくは Proxy インフラストラクチャーに Red Hat Satellite Server の最新バージョンをトップレベルのサービスとして導入する場合には、**Red Hat Satellite SSL Tool** を使用する必要性はほとんどありません。

3.2.1. SSL 証明書の生成

Red Hat Satellite SSL Maintenance Tool を使用する主な利点は、セキュリティ、柔軟性、移植性になります。各 Red Hat Satellite サーバーに別々の Web サーバー SSL キーと証明書を作成し、組織が作成した一組の認証機関 SSL キーペアですべてに署名を行うことにより安全性を確保しています。spacewalk-certs-tools パッケージがインストールされているマシンならどのマシンでもツールが動作できるという柔軟性があり、保管する場所を選ばずどこにでも格納でき必要なときにインストールができる構造という移植性も備えています。

組織のインフラストラクチャーのトップレベルサーバーが最新の Red Hat Satellite Server である場合、必要なことはアーカイブから **ssl-build** ツリーを `/root` ディレクトリーに復元し、Red Hat Satellite Server の Web サイト内で提供される設定ツールを利用するだけです。

Red Hat Satellite SSL Maintenance Tool を最大限に活用するために、以下の高レベルの作業を記載された順序で行ってください。各作業で必要となる細かな点については後半のセクションを参照してください。

1. 組織内のシステムに spacewalk-certs-tools パッケージをインストールします。恐らく Red Hat Satellite Server か Red Hat Proxy Server にインストールすることになると思いますが、必ずしもこれらである必要はありません。
2. 組織に対して認証機関の SSL キーペアを 1 組作成し、その RPM またはパブリック証明書をすべてのクライアントシステムにインストールします。詳細は「[認証機関の SSL キーペアの生成](#)」を参照してください。
3. 配備する各 Proxy および Satellite サーバー用に Web サーバーの SSL キーセットを作成し、その RPM ファイルを Red Hat Satellite サーバーにインストールします。
4. **httpd** サービスを再起動します。

```
# service httpd restart
```

5. SSL の **ビルドツリー** (主となるビルドディレクトリーと全サブディレクトリーおよびファイルから構成されている) を CD や DVD などのリムーバブルメディアにバックアップします (必要なディスク領域はわずかです)。

6. このアーカイブを検証してから安全な場所に格納します。例えば、Proxy や Satellite のインストールガイドの『その他の要件』セクションに記載されているバックアップ格納用の場所などです。
7. 今後のために認証機関のパスワードを記録して保管します。
8. 安全を期すため、ビルドツリーはビルドシステムから削除します。ただし、Satellite のインフラストラクチャー全体が正しく構成され設定が完了してから行なってください。



注記

追加で Web サーバー SSL キーセットが必要な場合は、**Red Hat Satellite SSL Maintenance Tool** を実行しているシステム上でビルドツリーを再生してから 3 から 7 のステップをくり返します。

3.2.2. Red Hat Satellite SSL Maintenance Tool のオプション

Red Hat Satellite SSL Maintenance Tool では、認証機関の SSL キーペアを生成したり、サーバーの SSL 証明書とキーを管理するためのコマンドラインオプションを数多く提供しています。コマンドラインのヘルプオプションは以下の通りです。

- **rhn-ssl-tool --help**: 一般的なヘルプ。
- **rhn-ssl-tool --gen-ca --help**: 認証機関のヘルプ。
- **rhn-ssl-tool --gen-server --help**: Web サーバーのヘルプ。

詳細は man ページ (**man rhn-ssl-tool**) を参照してください。

3.2.3. 認証機関の SSL キーペアの生成

Web サーバーで必要とされる SSL キーセットを作成する前に、まず認証機関の SSL キーペアを生成します。認証機関の SSL パブリック証明書は Satellite や Proxy のクライアントシステムに配付されます。**Red Hat Satellite SSL Maintenance Tool** を使用すると、必要に応じて認証機関の SSL キーペアを生成し、その後の Red Hat Satellite サーバーの導入すべてにそれを再利用することができます。

クライアントに配付するキーペアとパブリック RPM はビルドのプロセスで自動的に作成されます。認証機関の全コンポーネントはコマンドラインで指定されたビルドディレクトリー、通常は **/root/ssl-build** (旧式の Satellite や Proxy サーバーの場合は **/etc/sysconfig/rhn/ssl**) に作成されます。認証機関の SSL キーペアを生成するには次のコマンドを実行します。



重要

例で使用している値は組織に応じた値に置き換えてください。

```
# rhn-ssl-tool --gen-ca \
  --password=MY_CA_PASSWORD \
  --dir="/root/ssl-build" \
  --set-state="North Carolina" \
  --set-city="Raleigh" \
  --set-org="Example Inc." \
  --set-org-unit="SSL CA Unit"
```

このコマンドは指定されたビルドディレクトリー内に以下の関連ファイルを生成します。

- **RHN-ORG-PRIVATE-SSL-KEY**: 認証機関の SSL プライベートキー
- **RHN-ORG-TRUSTED-SSL-CERT**: 認証機関の SSL パブリック証明書
- **rhn-org-trusted-ssl-cert-VER-REL.noarch.rpm**: クライアントシステムへの配付用に準備された RPM

このファイルには (上記の) 認証機関 SSL パブリック証明書が含まれ、`/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT` としてこれをインストールします。

- **rhn-ca-openssl.cnf**: 認証機関の SSL 設定ファイル
- **latest.txt**: 関連ファイルの最新バージョン記載しているリスト

このプロセスが終了したら、RPM をクライアントシステムに配信します。詳細は「[認証機関の SSL パブリック証明書のクライアントへの配備](#)」を参照してください。

3.2.4. Web サーバー SSL キーセットの生成

この時点で認証機関の SSL キーペアは既に生成されています。Web サーバーの SSL キーセットについては、特に Proxy や Satellite を複数配備する場合、より頻繁に生成される可能性があります。それぞれ異なる Satellite もしくは Proxy サーバーのホスト名に対して、SSL キーと証明書の各セットは別々に生成しインストールする必要があります。このため、`--set-hostname` の値はサーバーごとに異なります。

サーバー証明書のビルドプロセスは、以下の 1 点を除いて認証機関の SSL キーペアの生成と同様になります。つまり、サーバーの全コンポーネントは、ビルドディレクトリー内のサブディレクトリーに格納されるという点です。これらのサブディレクトリーは、`/root/ssl-build/MACHINE_NAME` などのビルドシステムのマシン名を反映します。サーバー証明書を生成するには、以下のコマンドを実行します。



重要

例で使用している値は組織に応じた値に置き換えてください。

以下のコマンドは単一行のコマンドです。すべてを一行で入力するようにしてください。

```
# rhn-ssl-tool --gen-server \
  --password=MY_CA_PASSWORD \
  --dir="/root/ssl-build" \
  --set-state="MY_STATE" \
  --set-city="MY_CITY" \
  --set-org="Example Inc." \
  --set-org-unit="MY_ORG_UNIT" \
  --set-email="admin@example.com" \
  --set-hostname="machinename.example.com"
```

このコマンドは、マシン特定のビルドディレクトリー内のサブディレクトリーに以下の関連ファイルを生成します。

- **server.key**: Web サーバーの SSL プライベートサーバーキー
- **server.csr**: Web サーバーの SSL 証明書リクエスト

- **server.crt**: Web サーバーの SSL パブリック証明書
- **rhn-org-httpd-ssl-key-pair-MACHINE_NAME-VER-REL.noarch.rpm**: Satellite および Proxy サーバーへの配付用に準備された RPM。関連の **src.rpm** ファイルも生成されます。

この RPM ファイルには **server.key**、**server.csr**、**server.crt** ファイルが含まれます。これらのファイルは、以下のディレクトリーにインストールされます。

- **/etc/httpd/conf/ssl.key/server.key**
- **/etc/httpd/conf/ssl.csr/server.csr**
- **/etc/httpd/conf/ssl.crt/server.crt**

- **rhn-server-openssl.cnf**: Web サーバーの SSL 設定ファイル
- **latest.txt**: 関連ファイルの最新バージョン記載しているリスト

このプロセスが終了したら、RPM ファイルをそれぞれの Satellite もしくは Proxy Server 配布、インストールして、**httpd** サービスを再起動させます。

```
# service httpd restart
```

3.3. 認証機関の SSL パブリック証明書のクライアントへの配備

Red Hat Satellite Proxy Server および Red Hat Satellite Server のインストールプロセスでは、認証機関の SSL パブリック証明書が生成され、RPM ファイルにパッケージ化されます。このインストールプロセスにより、認証機関の SSL パブリック証明書と RPM ファイルのいずれかまたは両方のコピーが Satellite もしくは Proxy サーバーの **/var/www/html/pub/** ディレクトリーに配置され公開されます。

Web ブラウザーを使用すると、<http://proxy-or-sat.example.com/pub/> ディレクトリーのコンテンツを確認できます。**wget** または **curl** コマンドを使用すると、認証機関の SSL パブリック証明書をクライアントシステムにダウンロードすることができます。



重要

これらのコマンドを実行する前に、証明書や RPM ファイルの名前を確認してください。

```
# curl -O http://proxy-or-sat.example.com/pub/RHN-ORG-TRUSTED-SSL-CERT
# wget http://proxy-or-sat.example.com/pub/RHN-ORG-TRUSTED-SSL-CERT
```

また、認証機関の SSL パブリック証明書の RPM ファイルが **/pub** ディレクトリーにあれば、**rpm** コマンドを使ってパッケージをインストールすることもできます。例を以下に示します。

```
# rpm -Uvh http://proxy-or-sat.example.com/pub/rhn-org-trusted-ssl-cert-VER-REL.noarch.rpm
```

3.4. 証明書を使用するクライアントシステムの設定

RPM ファイルまたは証明書をクライアントシステムに配備したら、新たな 認証機関の SSL パブリック証明書ファイルを使用するように必要に応じて **Red Hat Update Agent** および **Red Hat Satellite Registration Client** の設定ファイルを編集する必要があります。また、設定を更新して、適切な

Red Hat Proxy Server または Red Hat Satellite Server に接続するようにする必要もあります。`/usr/share/rhn` ディレクトリーが一般的に受け入れられている認証機関の SSL パブリック証明書の格納場所となります。

Red Hat Proxy Server と Red Hat Satellite Server はいずれもデフォルトで **Red Hat Satellite Bootstrap** がインストールされています。これにより繰り返しの手順が大幅に減り、クライアントシステムの登録と設定のプロセスが簡略化されます。詳細は『Red Hat Satellite スタートガイド』を参照してください。

第4章 ソフトウェアの障害レポート

Red Hat Satellite のソフトウェア障害レポート機能と 自動バグ報告ツール (ABRT) を利用して、システムの全般的なレポート作成機能を拡張することができます。この拡張機能により、クライアントは ABRT が捕捉した障害を Satellite サーバーに自動的にレポートし、この捕捉された障害を集中的な方法で処理することができます。これらの障害レポートの処理には、Web UI または API のいずれかを使用することができます。

4.1. ソフトウェア障害レポートツールのインストール

以下での手順では、クライアントに ABRT 用の Red Hat Satellite ツールをインストールする方法について説明します。

手順4.1 ソフトウェア障害レポート機能の使用方法

1. **root** ユーザーでクライアントシステムにログインします。
2. クライアントシステムに `spacewalk-abrt` パッケージをインストールします。このパッケージは `abrt` パッケージを依存関係としてインストールします。

```
# yum install spacewalk-abrt
```



注記

`abrt` パッケージも `spacewalk-abrt` パッケージも Red Hat Enterprise Linux 5 では利用できません。

4.2. ソフトウェア障害レポートツールの使用

`spacewalk-abrt` パッケージには 2 つの重要なコンポーネントがあります。

- ABRT 用の設定ファイル: `/etc/libreport/events.d/spacewalk.conf`
- `spacewalk-abrt` ユーティリティー: `/usr/bin/spacewalk-abrt`

設定ファイルは `abrt` デーモンに `/usr/bin/spacewalk-abrt` ユーティリティーを使って、システム上で発生したソフトウェア障害すべてを Satellite サーバーに自動的にレポートするように指示します。このプロセスは完全自動化されており、通常はユーザーが作業する必要はありません。

Red Hat Satellite の Web UI を使ってクライアントからのソフトウェア障害レポートを表示します。詳細は『Red Hat Satellite ユーザーガイド』を参照してください。

4.3. 手動でのソフトウェア障害レポート

`spacewalk-abrt` ユーティリティーを使って手動でソフトウェア障害を Satellite サーバーにレポートします。以下の手順では、ソフトウェア障害レポートを手動で送信する方法を説明しています。

手順4.2 手動でソフトウェア障害をレポートする方法

1. `abrt-cli list` パラメーターを使って既存の障害レポート一覧を表示します。

```
# abrt-cli list
```

```
@0
Directory: /var/tmp/abrt/ccpp-2013-02-28-15:48:50-8820
count: 2
executable: /usr/bin/python2.7
package: python-2.7.3-13.fc16
time: Thu 28 Feb 2013 03:48:50 PM CET
uid: 0

@1
Directory: /var/tmp/abrt/oops-2013-02-27-14:16:03-8107-1
count: 3
package: kernel
time: Wed 27 Feb 2013 02:16:03 PM CET
```

2. レポートする障害を特定したら、**--report** オプションを使ってレポートを Satellite サーバーに送信します。

```
# spacewalk-abrt --report /var/tmp/abrt/ccpp-2013-02-28-15:48:50-8820
```

3. システム上で発生したすべてのソフトウェア障害を手動でレポートするには、**--sync** オプションを使用します。

```
# spacewalk-abrt --sync
```

4.4. テスト用のソフトウェア障害の作成

レポート設定が正常に機能するかどうかを検証するためにソフトウェア障害を強制的に発生させることができます。以下の例では、**kill** コマンドを使ってシグナル **11** 引数（セグメンテーション障害）をプロセスに送信する例を示しています。

```
# abrt-cli list
# sleep 600 &
[1] 17564
# kill -11 17564
#
[1]+  Segmentation fault          (core dumped) sleep 600
#
# abrt-cli list
@0
Directory:      /var/spool/abrt/ccpp-2013-05-14-04:56:17-17564
count:          1
executable:     /bin/sleep
package:        coreutils-8.4-19.el6
time:           Tue 14 May 2013 04:56:17 EDT
uid:            0
#
```

付録A 改訂履歴

改訂 1.1-0.1

Mon Sep 18 2017

Red Hat

翻訳ファイルを XML ソースバージョン 1.1-0 と同期

改訂 1.1-0

Wed Feb 1 2017

Satellite Documentation Team

Red Hat Satellite 5.8 リリース向けの初版。