



Red Hat Network Satellite 5.5

Proxy インストールガイド

Red Hat Network Satellite

エディション 3

Red Hat Network Satellite 5.5 Proxy インストールガイド

Red Hat Network Satellite

エディション 3

Red Hat Documentation Team

法律上の通知

Copyright © 2010 Red Hat, Inc.

This document is licensed by Red Hat under the [Creative Commons Attribution-ShareAlike 3.0 Unported License](#). 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

RHN Proxy インストールガイドへようこそ

目次

第1章 はじめに	3
1.1. RED HAT NETWORK	3
1.2. よく使われる用語	3
1.3. RHN PROXY SERVER	4
1.4. PROXY の動作のしくみ	5
第2章 要件	7
2.1. ソフトウェア要件	7
2.2. ハードウェア要件	8
2.3. ディスク領域に関する要件	8
2.4. その他の要件	8
第3章 トポロジーの例	11
3.1. 単一のプロキシトポロジー	11
3.2. 複数のプロキシを水平に結んだトポロジー	11
3.3. 複数のプロキシを垂直に結んだトポロジー	12
3.4. RHN SATELLITE SERVER とプロキシの併用	13
第4章 インストール	14
4.1. ベースインストール	14
4.2. RHN PROXY SERVER のインストール手順	14
4.2.1. 回答ファイル	18
第5章 RHN PACKAGE MANAGER およびローカルパッケージの提供	19
5.1. プライベートチャンネルの作成	20
5.2. パッケージをアップロードする	21
第6章 インストールのアップグレード	23
6.1. 前提条件	23
6.2. インストールアップグレードの手順	23
第7章 トラブルシューティング	25
7.1. プロキシサービスの維持管理	25
7.2. ログファイル	25
7.3. 質問と回答	26
7.4. 全般的な問題	26
7.5. ホストが見つかりませんでした / 完全修飾ドメイン名を確定できませんでした	27
7.6. 接続エラー	28
7.7. キャッシュ関連の問題	28
7.8. RED HAT によるプロキシのデバッグ	29
付録A RHN PROXY SERVER 設定ファイルのサンプル	31
付録B 改訂履歴	32
索引	33

第1章 はじめに

1.1. RED HAT NETWORK

Red Hat Network (RHN) は Red Hat システムおよびシステムのネットワークをシステムレベルでサポート、管理するための環境です。Red Hat Network はシステムのパフォーマンス、安全性、信頼性を最大限に高めるために必要なツール、サービス、情報リポジトリを集約しています。RHN を使用するには、システム管理者が Red Hat Network でクライアントシステムのシステムプロファイルを登録します。これには、システムのソフトウェアおよびハードウェアのプロファイルが含まれています。クライアントシステムがパッケージの更新を要求すると、そのクライアントに適用できるパッケージのみが返されます (RHN サーバーに格納されているソフトウェアプロファイルに応じて)。

Red Hat Network を使用する利点

- スケーラビリティ – 1人のシステム管理者が Red Hat Network を使用せずに1つのシステム管理を行うのに比べて、Red Hat Network を使用すると数百数千の Red Hat システムの設定管理が管理者1人で簡単、迅速、かつ正確に行うことができます。
- 標準プロトコル – セキュリティーの維持と機能向上のため標準プロトコルが使用されています。例えば、XML-RPC により Red Hat Network は単にファイルをダウンロードする以上のことができます。
- セキュリティー – 登録されたシステムと Red Hat Network 間の通信はすべてセキュアなインターネット接続を介して行われます。
- エラータ警告の表示 – 1つのウェブサイトですべてのクライアントシステムのエラータ警告を簡単に表示します。
- スケジュール済みの動作 – エラータ更新、パッケージのインストール、ソフトウェアプロファイルの更新など、動作のスケジュールにウェブサイトを使用します。
- 簡素化 – Red Hat システムの維持が単純な自動プロセスとなります。

1.2. よく使われる用語

RHN Proxy Server を理解する前に、以下の Red Hat Network 関連用語を知っておくことが重要になります。

チャンネル

チャンネルとはソフトウェアパッケージの一覧です。チャンネルには、ベースチャンネルと子チャンネルの2種類があります。ベースチャンネルは特定のアーキテクチャーと Red Hat リリースに基づくパッケージ一覧で構成されています。子チャンネルはベースチャンネルに関連するチャンネルで、エクストラパッケージが入っています。

組織管理者

組織管理者とは、組織の Red Hat Network アカウント全体にわたる最上位レベルのコントロールを備えるユーザーロールです。このロールを持つメンバーは他のユーザー、他のシステム、システムグループを組織に追加したり削除したりすることができます。Red Hat Network の組織には少なくとも1人の組織管理者が必要です。

チャンネル管理者

チャンネル管理者とは、チャンネル管理に関する機能すべてにアクセスできるユーザーロールになります。このロールを持つユーザーは、チャンネルの作成とチャンネルへのパッケージの割り当て

ができます。このロールの割り当てができるのは組織管理者で、Red Hat Network web サイトの **ユーザー** タブから行います。

Red Hat Update Agent

Red Hat Update Agent は Red Hat Network のクライアントアプリケーション (**up2date** または **yum**) です。このアプリケーションが稼働しているクライアントシステムでは、ユーザーがこのアプリケーションを使ってシステム用の更新パッケージや新しいパッケージの取得やインストールを行うことができます。

トレースバック

トレースバックには「どこが間違っていたのか」が詳細に記載されています。RHN Proxy Server のトラブルシューティングに役立ちます。重大なエラーが発生するとトレースバックが自動的に生成され、RHN Proxy Server の設定ファイルで指定されたユーザーにメールでこのトレースバックが送信されます。

これらの用語についての詳細説明は、<http://www.redhat.com/docs/manuals/satellite/>にある『Red Hat Network リファレンスガイド』と Satellite Web ユーザーインターフェースの **ヘルプ (Help)** ページを参照してください。

1.3. RHN PROXY SERVER

RHN Proxy Server はパッケージキャッシングのメカニズムで、RHN の帯域幅要件を低減し、カスタムパッケージの導入を可能にします。Proxy カスタマーは、Red Hat からのエラー更新などの RPM やユーザー組織の中央に配置したサーバーで内部生成されたカスタム RPM をキャッシュします。クライアントシステムはその後、個別にインターネットにアクセスするのではなく、Proxy からそれらの更新を受け取ります。

パッケージは Proxy が管理しますが、クライアントのシステムプロファイルとユーザー情報は安全な中央 RHN サーバー [1] に格納されます。このサーバーは RHN Web サイト (rhn.redhat.com) も提供しています。Proxy はクライアントシステムと Red Hat Network (または RHN Satellite Server) を仲介する役目を果たします。RHN Proxy Server に格納されるのはパッケージファイルのみになります。すべてのトランザクションは認証され、Red Hat Update Agent によりローカルの RHN Proxy Server から取り込まれた各パッケージの GPG 署名がチェックされます。

正式な Red Hat パッケージの格納の他、RHN Package Manager を使用して、組織独自のカスタム RPM パッケージをプライベートな RHN チャンネルから配信するよう RHN Proxy Server を設定することもできます。例えば、組織独自のソフトウェアを開発し、RPM でパッケージ化、独自の GPG 署名で署名してから、ローカル RHN Proxy Server を利用してネットワーク内の全個別システムをこのカスタムソフトウェアの最新バージョンに更新させることができます。

RHN Proxy Server を使用する利点として、以下を挙げることができます。

- スケーラビリティ – 1 組織内に複数のローカル RHN Proxy Servers を配備することが可能です。
- セキュリティ – クライアントシステムからローカルの RHN Proxy Server や Red Hat Network Server にいたるまで、エンドツーエンドの安全な接続を維持します。
- 時間節約 – インターネット経由に比べて、パッケージの配信がローカルエリアネットワークにより大幅に高速化されます。
- 帯域幅の節減 – 各クライアントシステムに対して各パッケージのダウンロードを行わず、RHN から一度に複数のパッケージをダウンロードします (ローカル Proxy サーバーのキャッシングメカニズムあたり)。

- 更新のカスタマイズ—カスタムソフトウェアパッケージの完全な自動パッケージ配信システムを作成するほか、クライアントシステムに必要とされる正式な Red Hat パッケージの配信も自動化します。プライベート RHN チャンネルをカスタマイズして、組織で社内パッケージの配信を自動化することもできます。
- 設定のカスタマイズ—特定のアーキテクチャーや OS バージョンに対して更新を制限したり許可したりします。
- 複数のインターネット接続は不要—クライアントはインターネットではなく、RHN Proxy Server のみに接続するため、Proxy に接続するローカルエリアネットワークだけが必要になります。RHN サーバーと通信するために RHN Proxy Server のみがインターネット接続を必要とします。ただし、RHN Proxy Server が RHN Satellite Server を使用している場合は、RHN Satellite Server のみがインターネット接続を必要とします。

1.4. PROXY の動作のしくみ

クライアントシステムの Red Hat Update Agent または Package Updater は Red Hat Network Server と直接は通信しません。クライアント (またはクライアント群) は RHN Proxy Server に接続し、この RHN Proxy Server が Red Hat Network Server または RHN Satellite Server に接続します。したがって、クライアントシステムはインターネットへの直接アクセスが不要です。クライアントシステムが必要なのは RHN Proxy Server へのアクセスのみです。



重要

Red Hat は、RHN Proxy Server に接続しているクライアント群が Red Hat Enterprise Linux の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ます。

RHN に直接アクセスするクライアントは、RHN サーバーが認証します。RHN Proxy Server にアクセスするクライアントも RHN が認証しますが、この場合、Proxy が RHN に認証とルート情報の両方を提供します。認証が成功すると、Red Hat Network Server は RHN Proxy Server にそのクライアントに対する特定動作の実行が許可されたことを伝えます。RHN Proxy Server は更新されたパッケージすべてをダウンロードして (キャッシュにない場合)、クライアントシステムに配信します。

クライアントシステムの Red Hat Update Agent または Package Updater による要求はサーバー側で認証されますが、パッケージが HTTP Proxy Caching Server または RHN Proxy Server (ローカルパッケージの場合) でキャッシュされるためパッケージ配信が大幅に速くなります。RHN Proxy Server とクライアントシステムが LAN 経由で接続されるので、影響を与えるのはローカルネットワークの速度のみです。

認証は次の順序で行われます。

1. クライアントはクライアントセッションの冒頭でログイン動作を行います。このログインが Red Hat Network Server に到達するまで1つまたは複数の RHN Proxy Server を経由します。
2. Red Hat Network Server はこのクライアントの認証を試みます。認証が成功すると、サーバーは RHN Proxy Server のチェーンを介してセッショントークンを返してきます。署名と有効期限を持つこのトークンには、チャンネルサブスクリプション、ユーザー名などのユーザー情報が含まれています。
3. 各 RHN Proxy Server はこのトークンを `/var/cache/rhn/` 内のローカルファイルシステムにキャッシュします。キャッシングにより Red Hat Network Server との認証で発生するオーバーヘッドを減少させ、Red Hat Network のパフォーマンスを大幅に向上させます。
4. このセッショントークンはクライアントマシンに返され、Red Hat Network の次の動作で使用されます。

クライアント側からは、RHN Proxy Server と Red Hat Network Server との違いは見られません。Red Hat Network Server 側から見ると、RHN Proxy Server は特殊な RHN クライアントとなります。したがってクライアントは、Red Hat Network Server に到達するために要求が通るルートに影響されません。これらの論理すべてが RHN Proxy Server および Red Hat Network Server に実装されています。

オプションで RHN Package Manager をインストールして、カスタムパッケージを実施する設定にすることができます。組織用に特別に書かれたカスタムパッケージを含む、Red Hat パッケージでないすべてのパッケージは、プライベートソフトウェアチャンネル（別名：カスタムソフトウェアチャンネル）からのみ配信できます。プライベート RHN チャンネルを作成した後に、RHN Server にパッケージヘッダーをアップロードして、カスタム RPM パッケージをそのプライベートチャンネルに関連付けます。アップロードするのはヘッダーのみで、実際のパッケージファイルはアップロードしません。ヘッダーにはソフトウェアの依存性など重要な RPM 情報が含まれるためアップロードが必要となり、これで RHN によるパッケージのインストール自動化が可能になります。実際のカスタム RPM パッケージは RHN Proxy Server 上に格納され、組織のローカルエリアネットワーク内からクライアントシステムに送信されます。

コンピュータネットワークが RHN Proxy Server を利用するように設定するのは簡単です。クライアントシステムの Red Hat Network アプリケーションが Red Hat Network Server ではなく RHN Proxy Server に接続するよう設定されている必要があります。詳細については『RHN クライアント設定ガイド (RHN Client Configuration Guide)』を参照してください。Proxy 側では、チェーン内の次の Proxy を指定する必要があります（最終的には Red Hat Network Server で終わる）。RHN Package Manager を使用する場合、クライアントシステムはプライベート RHN チャンネルをサブスクライブしている必要があります。

[1] 本ガイド上の「RHN」は RHN Hosted のサイト (<http://rh.redhat.com>) または RHN Satellite Server を指します。

第2章 要件

本章は、RHN Proxy Server のインストール前に満たす必要のある要件にフォーカスしています。Satellite のバージョンがインストールしようとしている Proxy のバージョンと同等またはそれ以降でなければなりません。たとえば、RHN Proxy Server 5.4 をインストールする場合、Satellite のバージョンは 5.4 またはそれ以降でなければなりません。5.3 またはそれ以前のバージョンは使用しないでください。

2.1. ソフトウェア要件

インストールを行うには、次のソフトウェア関連のコンポーネントが必要になります。

- ベースオペレーティングシステム – RHN Proxy Server は Red Hat Enterprise Linux 5 および 6 で対応しています。オペレーティングシステムはディスク、ローカルの ISO イメージ、キックスタート、または Red Hat でサポートしているいずれの方法でもインストールすることができます。

RHN Proxy Server は、Xen、KVM、Mware など Red Hat が対応している仮想化環境下の Red Hat Enterprise Linux 5 および 6 にインストールすることができます。

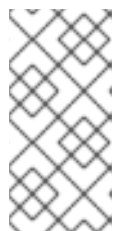
実稼働環境に導入する場合、RHN Proxy Server は基礎となる物理的なハードウェアで実行される唯一のアプリケーションとして導入し、競合を避けることが推奨されます。また、仮想化した環境の機能的なサポートは物理的なハードウェアで実行する場合のパフォーマンスと常と同じとは限らないため、仮想化環境の選択や推奨されるガイドラインの微調整を注意して考慮してください。



注記

購入いただいた RHN Proxy 製品にはそれぞれ、1 インスタンスの Red Hat Enterprise Linux Server サポートが含まれています。RHN Proxy は、新規インストールした Enterprise Linux にインストールして、RHN Proxy がオペレーティングシステムで提供される唯一のアプリケーションおよびサービスとしてください。ご使用の環境内で他のデーモン、アプリケーション、サービスなどの実行に RHN Proxy に含まれる Red Hat Enterprise Linux OS を使用することは、サポート対象外となります。

Red Hat Enterprise Linux の各バージョンは、RHN Proxy Server をサポートするために特定のパッケージセットを必要とします。パッケージをさらに追加すると、インストール時にエラーが発生する場合があります。したがって、Red Hat は次の方法で希望するパッケージを取得することをお勧めします。



注記

キックスタートの場合は、パッケージグループ @ **Base** を指定します。

CD または ISO イメージを使用して Red Hat Enterprise Linux をインストールする場合は、パッケージグループ **Minimal** を選択します。

- RHN Satellite Server アカウント内で利用可能な RHN Proxy Server エンタイトルメント。
- RHN Satellite Server アカウント内で利用可能な Provisioning エンタイトルメント (RHN Proxy Server エンタイトルメントとパッケージ化されています)。
- インストールした Red Hat Enterprise Linux バージョン用の Red Hat Network Tools チャンネ

ルへのアクセス。このチャンネルには RHN Proxy Server のインストールに必要な `configure-proxy.sh` インストールプログラムを収納している `spacewalk-proxy-installer` パッケージが含まれています。

- プロキシにインストールするすべての `rhncfg*` パッケージ (RHN ツールチャンネルから)。
- RHN Hosted ユーザーの場合は、プロキシに (RHN Tools チャンネルから) インストールする `spacewalk-certs-tools` パッケージ、または RHN Satellite Server ユーザーの場合は親サーバーの証明書生成に使用する SSL (secure sockets layer) CA 証明パスワード。
- 推奨されていない Web UI インストールの方法を使用する場合は、Red Hat Network から設定管理やりもットコマンドを受信するためのシステム構成。詳細については「[RHN Proxy Server のインストール手順](#)」を参照してください。

2.2. ハードウェア要件

RHN Proxy Server には次のハードウェア構成が必要となります。

- Pentium IV Processor または同等のプロセッサ
- 512 MB メモリ
- Red Hat Enterprise Linux のベースインストール用に最小 5 GB のストレージ
- ディストリビューション/チャンネルごとに 6 GB のストレージ

Apache Web サーバーに対する負荷は、クライアントシステムが Proxy に接続する頻度に直接関連してきます。クライアントシステムの `/etc/sysconfig/rhn/rhnsd` 設定ファイル内に設定された 4 時間 (または 240 分) のデフォルト間隔を短くすると、このコンポーネントに対する負荷は大幅に増大します。

2.3. ディスク領域に関する要件

RHN Proxy Server が使用するキャッシングのメカニズムは Squid HTTP プロキシになり、クライアント群の帯域幅を大幅に節約します。これには適度な領域が必要となります。キャッシュされたパッケージは `/var/spool/squid` に格納されます。空き領域の割り当ては、ディストリビューション/チャンネルごとに 6 GB のストレージが必要となります。

RHN Proxy Server がカスタムパッケージまたはローカルパッケージを配信するように設定する場合には、ローカルパッケージを格納するシステムの `/var` マウントポイントにカスタムパッケージすべてを保持するのに十分なディスク領域があることを確認します。これらカスタムパッケージは `/var/spool/rhn-proxy` 内に格納されています。ローカルパッケージ用に必要となるディスク領域は、配信されるカスタムパッケージの数によって異なります。

2.4. その他の要件

RHN Proxy Server のインストールが完了したとみなす前に、次の補足要件を満たす必要があります。

完全なアクセス

クライアントシステムは、RHN Proxy Server サービスとポートに完全なネットワークアクセスが必要となります。

ファイアウォールのルール

RHN では、RHN Proxy Server ソリューションをファイアウォールでインターネットから保護することが強く推奨されます。しかし、ご使用の RHN Proxy Server の実装に応じて各種の TCP ポートが Proxy で開いている必要があります。

表2.1 Proxy で開くポート

ポート	方向	理由
80	送信	Proxy はこのポートを使用して rhn.redhat.com 、 xmlrpc.rhn.redhat.com 、Satellite の URL (RHN Proxy が RHN Hosted または Satellite Server と通信している場合で異なる) に到達します。
80	受信	クライアントの要求は http か https 経由で到着します。
443	受信	クライアントの要求は http か https 経由で到着します。
443	送信	Proxy はこのポートを使用して rhn.redhat.com 、 xmlrpc.rhn.redhat.com 、Satellite の URL (RHN Proxy が RHN Hosted または Satellite Server と通信している場合で異なる) に到達します。
4545	送信	ご使用の Proxy が RHN Satellite Server に接続されている場合、Monitoring が有効になっており、プローブが登録済みシステムに設定されているなら、Monitoring は、この TCP ポートを経由してクライアントシステム上で実行している <code>rhnmd</code> へ接続します。
5222	受信	RHN Push 技術を使用している時にこのポートを開くと、Proxy 上の <code>jabberd</code> デーモンへの <code>osad</code> クライアントの接続を許可します。
5269	送信	ご使用の Proxy が RHN Satellite Server に接続されている場合、RHN Push Technology での <code>jabberd</code> 経由のサーバー対サーバー接続を可能にするため、ポートを開いておく必要があります。

同期システム時間

SSL (Secure Sockets Layer) を実行している Web サーバーに接続する際は、時間が非常に重要になります。SSL 証明書が使用前または使用中に期限切れにならないよう、クライアントとサーバーの時間設定がかなり近い時間でなければなりません。NTP (Network Time Protocol) を使用して時計を同期することが推奨されます。

完全修飾ドメイン名 (FQDN)

RHN Proxy Server をインストールするシステムは、自身の完全修飾ドメイン名を正しく解決できなければなりません。

Red Hat Network アカウント

インクリメンタル (増分) 更新を受信するために中央 Red Hat Network Server に接続するお客様は、Red Hat Network アカウントが必要になります。このアカウントのセットアップについてはご購入時に担当者がお手伝いします。

ログイン情報のバックアップ

主要なログイン情報はすべて、お客様に記録を保持していただく必要があります。RHN Proxy Server の場合、組織管理者アカウントのユーザー名とパスワード、SSL 証明の生成などがこれに該当します。Red Hat は、これらの情報を別々のディスク 2 枚 (CD/DVD/リムーバブルハードディスク) にそれぞれコピーし、またハードコピーに印刷して、安全な場所で保管することを強く推奨します。

ディストリビューションの場所

プロキシは事実上、すべてのローカル HTTP 要求を中央 RHN サーバーに転送するため、プロキシ上の転送が行われない場所にディストリビューション行きのファイル(キックスタートインストールツリー内など)を置くよう注意してください: `/var/www/html/pub/`。このディレクトリに配置されたファイルはプロキシから直接ダウンロードすることができます。特に GPG キーの配信やキックスタート用のインストールツリーの作成時に便利です。

また、Red Hat はコードを実行しているシステムが一般からアクセスできないようにすることを推奨します。システム管理者以外のユーザーがこれらのマシンへのシェルアクセスを持たないようにしてください。不要なサービスはすべて無効にしてください。サービスを無効にするには、`ntsysv` または `chkconfig` を使用します。

最後に、およそ次の順序でテクニカルドキュメントを手元に用意してください。

1. 『RHN Proxy Server インストールガイド』 – 現在ご覧になっている本ガイドは、RHN Proxy Server を設定して稼働するために必要な基本ステップを説明しています。
2. 『RHN クライアント設定ガイド (The RHN Client Configuration Guide)』 – このガイドでは、RHN Proxy Server または RHN Satellite Server で管理するシステムの設定方法を説明しています。(このガイドの利用にあたっては、『RHN リファレンスガイド』への参照が必要な場合があります。RHN リファレンスガイドではシステムの登録と更新の手順が説明されています。)
3. 『RHN チャンネル管理ガイド (The RHN Channel Management Guide)』 – このガイドでは、カスタムパッケージの構築方法、カスタムチャンネルの作成方法、プライベートエラータの管理方法に関して推奨される方法を詳細に説明しています。
4. 『RHN リファレンスガイド』 – このガイドでは、RHN アカウントの作成方法、システムの登録および更新を行う方法、RHN ウェブサイトのさまざまな使用方法などについて説明しています。インストールから設定のプロセスまで全体を通してこのガイドが役に立ちます。

第3章 トポロジーの例

RHN Proxy Server はさまざまな方法で構成することができます。次の要素に応じて、構成方法を選択してください。

1. RHN Proxy Server が管理するクライアントシステムの総数
2. RHN Proxy Server に同時に接続する可能性のあるクライアントの最大数
3. RHN Proxy Server が管理するカスタムパッケージとチャンネルの数
4. お客様の環境で使用する RHN Proxy Server の数

本章では可能な構成とそれらの利点について説明します。

3.1. 単一のプロキシトポロジー

最もシンプルな構成は、単一の RHN Proxy Server を使用してネットワーク全体に接続することです。この構成は小規模なクライアントグループとネットワークを接続するのに適切で、その利点は Red Hat RPM をキャッシュしてカスタムパッケージをローカルサーバーに格納する点です。

単一の RHN Proxy Server を使用する短所は、パッケージを要求するクライアント数が増えるにつれてパフォーマンスが低下することです。

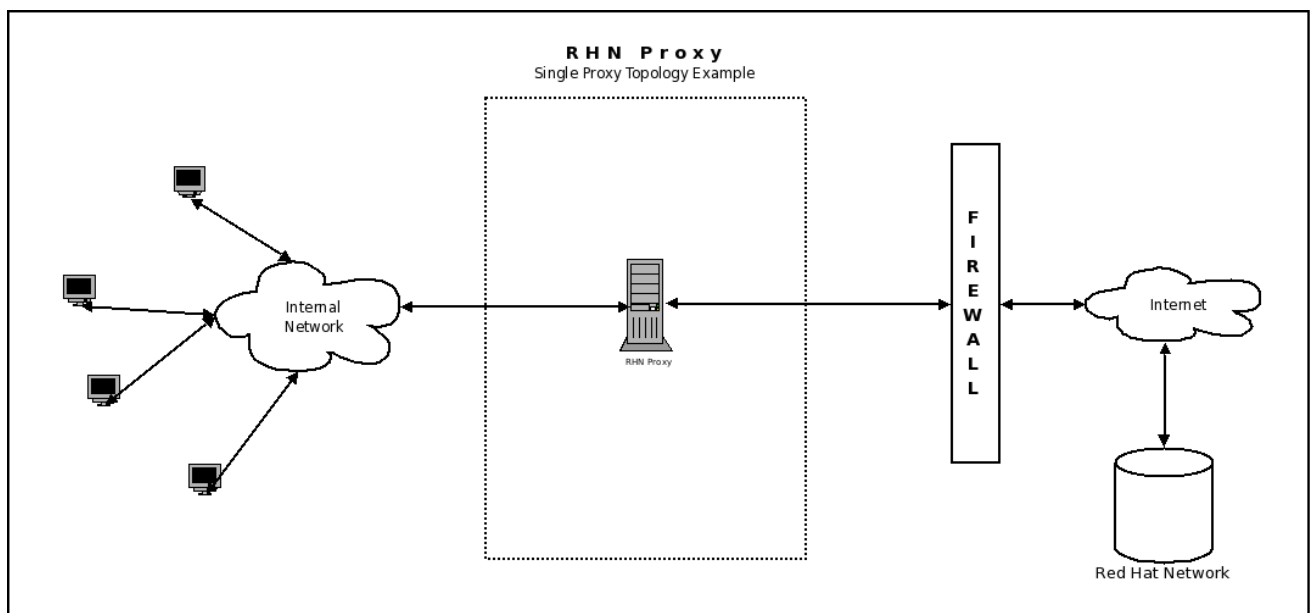


図3.1 単一のプロキシトポロジー

3.2. 複数のプロキシを水平に結んだトポロジー

大規模なネットワークには、複数の RHN Proxy Server をすべて個別に Red Hat Network に接続するなどしたより分散型の方法が必要になる場合があります。この水平に結んだ構成は、各プロキシが RHN と同時に同期できるようにする一方、クライアント要求の負荷を分散します。

この水平構成の短所は、個別のプロキシにロードされたカスタムパッケージがその仲間となるサーバーに配信されなければならない点です。こうした状況は次のいずれかで対処することができます。

- `rsync` ファイル転送プログラムを使用して、Proxy 間でパッケージを同期できます。

- NFS (Network File System) 共有を、Proxy とカスタムチャンネルレポジトリとの間で確立できます。

いずれかのソリューションにより、RHN Proxy Server のクライアントすべてに全部のカスタムパッケージが配信可能となります。

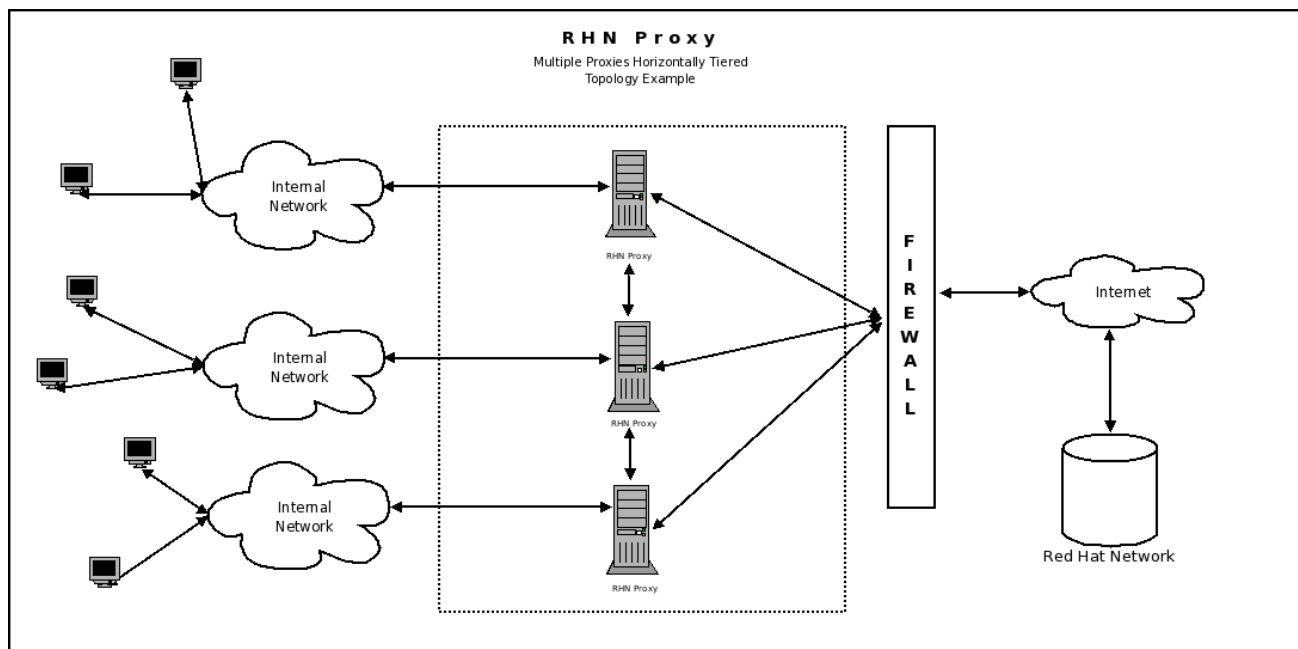


図3.2 複数のプロキシを水平に結んだトポロジー

3.3. 複数のプロキシを垂直に結んだトポロジー

複数の RHN Proxy Server の代替方法は、第一プロキシを定めて、他のプロキシは Red Hat Network の RPM やローカルで作成されたカスタムパッケージを取得するために、この第一プロキシに接続するという方法です。事実上、二次的なプロキシは第一プロキシのクライアント群として動作します。この方法では、プロキシが製品固有の **up2date** 機能を使用するため、RHN Proxy Server 間で同期を確立する必要性が軽減されます。

水平に結んだ構成と同様に、この垂直方法でも、すべての RHN Proxy Server のクライアントに全部のカスタムパッケージが配信可能となります。Proxy は単に、自己のリポジリーを検索して、自己のファイルシステムにパッケージがあるかどうかを調べます。パッケージが見つからない場合は、上位のレベルで検索を試行します。

この垂直に結んだ構成では、二次的 Proxy 群が RHN からの更新やカスタムパッケージを必ず一次 Proxy から取得するようにします。また、子 Proxy 群へ確実に配信するために、カスタムチャンネルとパッケージは一次 Proxy にのみ配置しなければなりません。最後に、二次的 Proxy の設定ファイルは Red Hat Network に直接向けるのではなく、第一 Proxy に向ける必要があります。

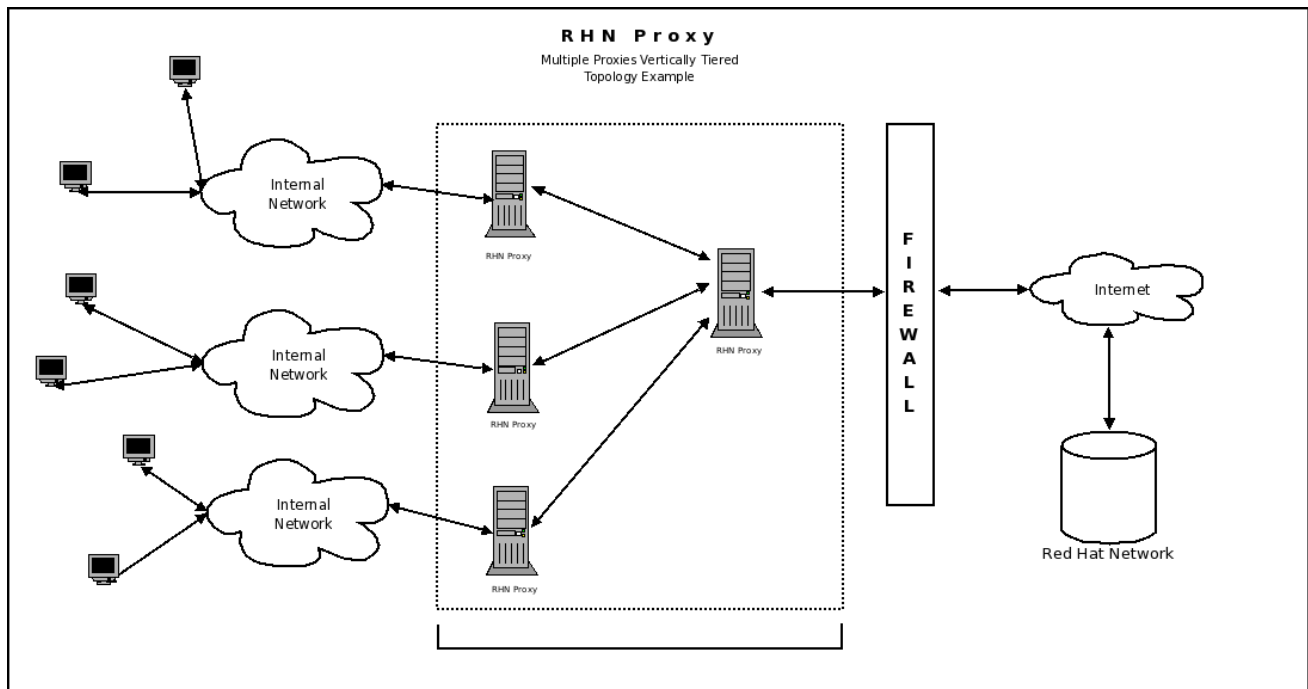


図3.3 複数のプロキシを垂直に結んだトポロジー

3.4. RHN SATELLITE SERVER とプロキシの併用

本章に記載されている方法の他に、RHN Proxy Server を RHN Satellite Server と併用するオプションもあります。この方法は、プロキシを垂直に結んだ構成と同様の働きをしますが、サテライトはより多数のクライアントシステムを管理することができるため許容量が大幅に増大します。

この組合せについての全体的な詳細は、『RHN Satellite Server インストールガイド』にあるトポロジーの範例の章を参照してください。両製品のSSL証明のリンク方法については、『RHN クライアント設定ガイド』に説明があります。両製品間でチャンネルとパッケージを共有する方法については、『RHN チャンネル管理ガイド』を参照してください。

第4章 インストール

本章では、RHN Proxy Server の初期インストールについて説明します。ここでは、[2章要件](#)に記載されている必要条件を満たしているものと仮定しています。ただし、RHN Proxy Server を新しいバージョンにアップグレードする場合は Red Hat 担当者までご連絡ください。

4.1. ベースインストール

RHN Proxy Server は Red Hat Enterprise Linux オペレーティングシステム上で稼働するよう設計されています。したがって、第1段階としてディスク、ISO イメージ、またはキックスタートなどでベースとなるオペレーティングシステムをインストールします。オペレーティングシステムのインストール中およびインストール後は、次の点を確認してください。

- 前述のハードウェア要件に従い、パッケージ格納に使用するパーティションに十分な領域を配分します。Red Hat パッケージがキャッシュされるデフォルトの場所は `/var/spool/squid` で、カスタムパッケージは `/var/spool/rhn-proxy` になります。



注記

インストールプログラムは、`/var/spool/squid` がマウントされるパーティションで利用可能な容量を自動的に計算し、RHN Proxy Server の使用に空き容量の最大 60 パーセントを割り当てます。

- RHN Proxy Server が必要とするパッケージをインストールします。



注記

ベースパッケージのみをインストールしてください。他のパッケージは RHN Proxy Server のインストール失敗の原因になります。

Red Hat Enterprise Linux の各バージョンで必要なパッケージグループを取得する方法については「[ソフトウェア要件](#)」を参照してください。

- プロキシで NTP (Network Time Protocol) を有効にしてから該当のタイムゾーンを選択します。すべてのクライアントシステムは既に `ntpd` デーモンを実行していて正しいタイムゾーンが設定されていなければなりません。
- インストール後に `ipchains` サービスと `iptables` サービスを無効にします。

4.2. RHN PROXY SERVER のインストール手順

RHN Proxy Server インストールの手順を以下に説明します。

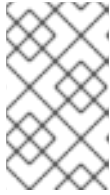
1. インストールする RHN Proxy Server システムに、`root` ユーザーとしてログインします。
2. RHN Proxy Server エンタイトルメントのある組織アカウントを使用して、コマンド `rhn_register` で Red Hat Network (中央 RHN Server または RHN Satellite Server のいずれか) に新たにインストールした Red Hat Enterprise Linux を登録します。
3. クライアントで RHN Tools チャンネルをサブスクライブします。
4. プロキシインストーラーをインストールします。



```
yum install spacewalk-proxy-installer
```

5. インストールを実行します。

```
configure-proxy.sh
```



注記

この手順を正常に実行するには、**Satellite** サーバーに **root** でアクセスする必要があります。別の方法としては、コマンドに **--force-own-ca** オプションを加えます。

コマンドラインインストールプログラムでは、インストールオプションや SSL 証明書生成などの **RHN Proxy Server** インストールおよび初期設定の詳細について一連のプロンプトが表示されます。以下の指示では、インストールプロセスを説明しています。



注記

プロンプトの表示で入力を行わずに **Enter** キーを押すと、**RHN Proxy Server** のコマンドラインインストールプログラムは括弧で囲まれたデフォルトの応答を使用します。

別の方法としては、ユーザーの対話をまったく使わずにデフォルトの答えを使用したい場合は、すべてのデフォルト応答を使用する **--non-interactive** オプションを使用します。

6. 最初の一連のプロンプトはインストールに関するサイト固有の詳細です。

```
Proxy version to activate [5.4]:
```

Proxy version のプロンプトでは、インストールする **RHN Proxy Server** のバージョンを確認するよう求められます。

```
RHN Parent [satserver.example.com]:
```

RHN Parent は **Proxy** を処理するシステムのドメイン名またはアドレスであり、**RHN Hosted** サーバー (`xmlrpc.rhn.redhat.com`) または **Satellite** サーバーなどになります。

```
Traceback email []:
```

Traceback email はエラー関連のトレースバックメッセージが送信される E メールアドレスで、通常は **Proxy** 管理者の E メールです。このプロンプトで複数の E メールアドレスを入力する場合はカンマで区切ります。

7. 次の一連のプロンプトは SSL 証明書生成の詳細設定に関するものです。この設定は **RHN Proxy Server** と行き来するトラフィックの安全確保のために推奨されます。

```
Use SSL [Y/n]: y
```

Use SSL プロンプトで **y** と入力して、SSL に対応するよう **RHN Proxy Server** を設定します。

CA Chain [/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT]:

認証局 (CA) チェーンのデフォルトのパスを使用する場合は **CA Chain** プロンプトで **Enter** キーを押します。RHN Proxy が RHN Satellite と通信している場合、この値は通常 **/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT** になります。RHN Hosted と通信している場合は通常 **/usr/share/rhn/RHNS-CA-CERT** ファイルになります。カスタムの SSL 証明書は **/usr/share/rhn/** ディレクトリに配置してください。

HTTP Proxy []:

RHN Proxy Server が HTTP プロキシを使用して接続する場合は、**corporate.proxy.example.com:3128** のように、プロキシホスト名とポート番号を入力します。

適切な SSL サーバー証明書を生成するのに必要な詳細 (**Organization** 名、**Organization Unit (Engineering** など)、**Common Name** (ドメイン名) と市、県、国の詳細を含む) を入力します。最後に SSL 証明書を担当する管理者または技術担当者の電子メールを入力します。

```
Regardless of whether you enabled SSL for the connection to the
Proxy Parent
Server, you will be prompted to generate an SSL certificate.
This SSL certificate will allow client systems to connect to this
Spacewalk Proxy
securely. Refer to the Spacewalk Proxy Installation Guide for more
information.
Organization: Example Company
Organization Unit [proxy1.example.com]:
Common Name: proxy1.example.com
City: New York
State: New York
Country code: US
Email [admin@example.com]:
```

8. RHN Proxy Server インストールプログラムを実行することで、コマンドラインインストールプログラムは以下を行います。

- RHN Proxy Server へのモニタリングサポートのインストールを要求します。
- 今後の RHN Proxy Server インストール用に、組織が設定チャンネルを作成、追加できるようにします。
- SSL 設定を完了します。
- 設定を修正したすべてのサービスデーモンを再起動します。

```
You do not have monitoring installed. Do you want to install it?
Will run 'yum install spacewalk-proxy-monitoring'. [Y/n]:n
```

Proxy サーバーに監視サポートをインストールするかどうかを確認します。

```
Generating CA key and public certificate:
CA password:
CA password confirmation:
Copying CA public certificate to /var/www/html/pub for distribution
```

```

to clients:
Generating SSL key and public certificate:
CA password:
Backup made: 'rhn-ca-openssl.cnf' --> 'rhn-ca-openssl.cnf.1'
Rotated: rhn-ca-openssl.cnf --> rhn-ca-openssl.cnf.1
Installing SSL certificate for Apache and Jabberd:
Preparing packages for installation...
rhn-org-httpd-ssl-key-pair-proxy1.example-1.0-1

```

次に **configure-proxy.sh** プログラムによって SSL を設定します。この場合、SSL キーと公開証明書を生成する前に証明書認証局のパスワードを作成するよう求められます。

```

Create and populate configuration channel
rhn_proxy_config_1000010000? [Y]:
Using server name satserver.example.com
Red Hat Network username: admin
Password:
Creating config channel rhn_proxy_config_1000010000
Config channel rhn_proxy_config_1000010000 created
using server name satserver.example.com
Pushing to channel rhn_proxy_config_1000010000:
Local file /etc/httpd/conf.d/ssl.conf -> remote file
/etc/httpd/conf.d/ssl.conf
Local file /etc/rhn/rhn.conf -> remote file /etc/rhn/rhn.conf
Local file /etc/rhn/cluster.ini -> remote file /etc/rhn/cluster.ini
Local file /etc/squid/squid.conf -> remote file
/etc/squid/squid.conf
Local file /etc/httpd/conf.d/cobbler-proxy.conf -> remote file
/etc/httpd/conf.d/cobbler-proxy.conf
Local file /etc/httpd/conf.d/rhn_proxy.conf -> remote file
/etc/httpd/conf.d/rhn_proxy.conf
Local file /etc/httpd/conf.d/rhn_broker.conf -> remote file
/etc/httpd/conf.d/rhn_broker.conf
Local file /etc/httpd/conf.d/rhn_redirect.conf -> remote file
/etc/httpd/conf.d/rhn_redirect.conf
Local file /etc/jabberd/c2s.xml -> remote file /etc/jabberd/c2s.xml
Local file /etc/jabberd/sm.xml -> remote file /etc/jabberd/sm.xml

```

次にインストーラーは **configure-proxy.sh** の実行中に作成された設定ファイルに基づいて設定チャンネルを作成するかどうかを尋ね、RHN Proxy Server がインストールされたクライアントシステムの名前 (上記の例では sysID は 1000010000) に基づいて RHN Satellite Server 設定チャンネルを作成し、Proxy サーバーの設定チャンネルを構成するさまざまな **httpd**、**SSL**、**squid**、および **jabberd** のサーバーファイルを収集します。

- 最後にインストーラーは RHN Proxy Server 関連のすべてのサービスを起動してから再起動し、これが完了すると終了します。

```

Enabling Satellite Proxy
Shutting down rhn-proxy...
Shutting down Jabber router: [ OK
]
Stopping httpd: [ OK
]
Stopping squid: [ OK
]

```

```

Done.
Starting rhn-proxy...
init_cache_dir /var/spool/squid... Starting squid: .      [ OK ]
Starting httpd:                                          [ OK ]
]
Starting Jabber services                                [ OK ]
]
Done.

```

4.2.1. 回答ファイル

システムで RHN Proxy Server のインストールプロセスの一部を自動化したい場合、管理者は **configure-proxy.sh** プログラムを使用してインストールプログラムのプロンプトに対して事前に指定された応答を含む回答ファイル (*answer files*) を作成できます。

以下は、バージョン番号、親サーバーとして機能する RHN Satellite Server、SSL、および他の設定パラメーターに関する事前指定の回答を含む回答ファイルの例です。回答ファイルの作成と使用の詳細については、シェルスクリプトで **man configure-proxy.sh** を入力して **configure-proxy.sh** の **man** ページを参照してください。

```

# example of answer file for configure-proxy.sh
# for full list of possible option see
# man configure-proxy.sh

VERSION=5.4
RHN_PARENT=rhn-satellite.example.com
TRACEBACK_EMAIL=jsmith@example.com
USE_SSL=1
SSL_ORG="Red Hat"
SSL_ORGUNIT="Spacewalk"
SSL_CITY=Raleigh
SSL_STATE=NC
SSL_COUNTRY=US
INSTALL_MONITORING=N
ENABLE_SCOUT=N
CA_CHAIN=/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT
POPULATE_CONFIG_CHANNEL=Y

```

configure-proxy.sh で回答ファイル (例では **answers.txt** と呼ばれる) を使用するには以下のコマンドを入力します。

```
configure-proxy.sh --answer-file=answers.txt
```

第5章 RHN PACKAGE MANAGER およびローカルパッケージの提供

RHN Package Manager はコマンドラインツールで、これを使用すると組織は RHN Proxy Server 経由でプライベートの RHN チャンネル関連のローカルパッケージを提供することができます。RHN Proxy Server 用の Red Hat 公式パッケージのみを更新する場合は、RHN Package Manager をインストールしないでください。

RHN Package Manager を使用するには、**spacewalk-proxy-package-manager** パッケージとそれに依存するパッケージをインストールします。

パッケージのヘッダー情報のみを RHN Server にアップロードします。RHN がクライアントシステムのパッケージ依存を解決するには、このヘッダーが必要になります。実際のパッケージファイル (*.rpm) は RHN Proxy Server に格納されます。

RHN Package Manager はプロキシと同じ設定である、**/etc/rhn/rhn.conf** 設定ファイルでの定義を使用します。

RHN Package Manager のコマンドライン **rhn_package_manager** の全オプションの概要は以下のとおりです。

表5.1 rhn_package_manager オプション

オプション	詳細
-v、--verbose	冗長性を高めます。
-dDIR、--dir=DIR	ディレクトリ <i>DIR</i> のパッケージを処理します。
-cCHANNEL、--channel=CHANNEL	指定したチャンネルを管理します – 複数表記が可能です。
-nNUMBER、--count=NUMBER	コールごとに指定したヘッダー数を処理します – デフォルトのヘッダー数は 32 です。
-l、--list	指定したチャンネル内の各パッケージ名、バージョン番号、リリース番号、アーキテクチャを一覧表示します。
-s、--sync	ローカルディレクトリがサーバーと同期中であるかどうか確認します。
-p、--printconf	現在の設定を表示して終了します。
-XPATTERN、--exclude=PATTERN	指定した表現と一致するファイルを除外します – 複数使用が可能です。
--newest	指定したチャンネル用にサーバーに対して既にプッシュされたパッケージより新しいパッケージのみプッシュします。
--stdin	stdin からパッケージ名を読み取ります。

オプション	詳細
<code>--nosig</code>	署名がないパッケージをプッシュします。デフォルトでは RHN Package Manager は署名されたパッケージのみのプッシュを試行します。
<code>--username=USERNAME</code>	RHN ユーザー名を指定します。このオプションでユーザー名を指定していない場合は、ユーザー名の入力が必要です。
<code>--password=PASSWORD</code>	RHN パスワードを指定します。このオプションでパスワードを指定していない場合は、パスワードの入力が必要です。
<code>--source</code>	ソースパッケージのヘッダーをアップロードします。
<code>--dontcopy</code>	アップロード後の手順で、パッケージをパッケージツリー内の最終配置場所にコピーしません。
<code>--test</code>	プッシュされるパッケージのみを表示します。
<code>--no-ssl</code>	推奨しません - SSL をオフにします。
<code>-?, --usage</code>	オプションの簡潔な説明を表示します。
<code>--copyonly</code>	引数内に表示されているファイルを指定チャンネルにコピーします。プロキシのチャンネルがパッケージを1つ紛失してしまいそのチャンネルのパッケージすべてを再度インポートしたくない場合に便利です。例： <code>rhn_package_manager -c CHANNEL --copyonly/PATH/TO/MISSING/FILE</code>
<code>-h, --help</code>	オプション一覧とヘルプ画面を表示します。



注記

これらコマンドラインオプションは `rhn_package_manager` の man ページでも説明されています：`man rhn_package_manager`

RHN Package Manager によるローカルパッケージの提供を可能にするには、以下の手順が必要になります。

1. プライベートチャンネルを作成する
2. ローカルパッケージをそのチャンネルにアップロードする。

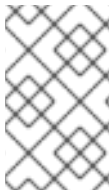
これらの手順は、次のセクションで説明します。

5.1. プライベートチャンネルの作成

RHN Proxy Server からローカルパッケージの提供を行う前に、ローカルパッケージを格納するプライベートチャンネルが必要になります。次の手順でプライベートチャンネルを作成します。

1. <https://rhn.redhat.com> の RHN ウェブインターフェースにログインします。
2. 上部ナビゲーションバーのチャンネル (**Channels**) をクリックします。左にあるナビゲーションバーに **チャンネルの管理 (Manage Channels)** オプションが表示されない場合には、このユーザーがチャンネル編集に関する権限を有しているか確認してください。上部ナビゲーションバーから **ユーザー (Users)** カテゴリにアクセスすると確認できます。
3. 左にあるナビゲーションバーで、**ソフトウェアチャンネルの管理 (Manage Software Channels)** をクリックしてからページの右上部にある**新しいチャンネルの作成 (create new channel)** ボタンをクリックします。
4. 親チャンネルとベースチャンネルのアーキテクチャを選択して、新しいプライベートチャンネルの名前、ラベル、概要、説明を入力します。チャンネルラベルは少なくとも 6 文字以上の長さで英文字で始まらなければなりません。使用できるのは小文字、数字、ダッシュ(-)、ピリオド(.)のみになります。また、チャンネルの GPG キーの URL も入力します。ただし、このフィールドは必須ではありません。セキュリティ強化のため入力推奨されるフィールドです。GPG キーの生成方法については、RHN チャンネル管理ガイド (RHN Channel Management Guide) を参照してください。
5. **チャンネルの作成 (Create Channel)** をクリックします。

5.2. パッケージをアップロードする



注記

プライベート RHN チャンネルにパッケージをアップロードするには、組織管理者である必要があります。スクリプトにより RHN ユーザー名とパスワードの入力が求められます。

プライベートチャンネルの作成後に、RHN サーバーにバイナリ RPM とソース RPM のパッケージヘッダーをアップロードして、パッケージを RHN Proxy Broker Server にコピーします。バイナリ RPM のパッケージヘッダーをアップロードするには、以下のコマンドを入力します。

```
rhn_package_manager -c "label_of_private_channel" pkg-list
```

このコマンドはパッケージのヘッダーを指定されたチャンネル名に、パッケージそのものを `/var/spool/rhn-proxy/rhn` にアップロードします。

pkg-list はアップロードするパッケージ一覧です。代わりに、**-d** オプションを使ってチャンネルに追加するパッケージを含むローカルディレクトリを指定することもできます。このディレクトリには含まれるべきパッケージ以外のファイルがないことを確認してください。RHN Package Manager は標準入力からパッケージ一覧を読み取ることもできます (**--stdin** を使用)。

ソース RPM のパッケージヘッダーをアップロードするには、

```
rhn_package_manager -c "label_of_private_channel" --source pkg-list>
```

複数のチャンネルを指定している場合 (**-c** または **--channel** を使用)、アップロードしたパッケージヘッダーは併記したチャンネルすべてにリンクされます。



注記

チャンネル名が指定されていない場合、パッケージはどのチャンネルにも追加されません。この場合、パッケージは **Red Hat Network** ウェブインターフェースを使ってチャンネルに追加することができます。インターフェースは既存のプライベートチャンネルの変更にも使用できます。

パッケージをアップロードしたら、すぐに **RHN** ウェブインターフェースを使ってパッケージがあるか確認することができます。上部ナビゲーションバーの **チャンネル (Channels)** をクリックして、左に表示されるナビゲーションバーの **ソフトウェアチャンネルの管理 (Manage Software Channels)** をクリック、カスタムチャンネルの名前をクリックします。**パッケージ (Packages)** サブタブをクリックすると、各 **RPM** が一覧表示されます。

以下のコマンドラインで、ローカルディレクトリがチャンネルの **RHN** サーバーのイメージと同期しているかどうかを確認してください。

```
rhn_package_manager -s -c "label_of_private_channel"
```

-s オプションは、欠けているパッケージすべてを一覧表示します (**RHN Server** にアップロードされたがローカルディレクトリにないもの)。このコマンドを使用するには、組織管理者である必要があります。スクリプトにより **RHN** ユーザー名とパスワードの入力が求められます。

ローカルパッケージの更新に **RHN Package Manager** を使用している場合、そのシステムをプライベートチャンネルにサブスクライブさせるには **RHN** ウェブサイトに行く必要があります。

第6章 インストールのアップグレード

本章では、RHN Proxy Server のインストールをアップグレードする方法について説明します。完全に稼働中の RHN Proxy Server とそれにもなう必要なエンタイトルメントがあることを前提としています。

6.1. 前提条件

最新バージョンの RHN Proxy Server には以下が必要になります。

- Red Hat Enterprise Linux 5 (32 ビットまたは 64 ビット) もしくは Red Hat Enterprise Linux 6 (64 ビットのみ)
- Red Hat Network Classic または親 Satellite Server から古い Proxy Server のシステムプロファイルを削除する (該当する場合)。

6.2. インストールアップグレードの手順

1. Proxy Server をバックアップします。該当する場合は、バックアップからディレクトリー `/root/ssl-build` に SSL ビルドの方向を復元します。
2. Proxy Server を Red Hat Network Classic または親 Satellite Server (該当する場合) に登録します。Proxy Server が Red Hat Enterprise Linux Server のベースチャンネルと Red Hat Network Tools の子チャンネルの両方にサブスクライブしていることを確認します。
3. Red Hat Network Tools の子チャンネルから `spacewalk-proxy-installer` パッケージをインストールします。

```
# yum install spacewalk-proxy-installer
```

4. 「[RHN Proxy Server のインストール手順](#)」にあるように、最新バージョンのプロキシをインストールします。

注記

プロキシサーバーが Red Hat Network Classic に登録されていて、かつこのプロキシサーバーが以前にカスタムチャンネルを管理していた場合、アップグレード前のバックアップからこのカスタムパスのリポジトリーを復元する必要があります。パーミッションと所有権も適切に設定する必要があります。

```
# chmod 0750 /var/spool/rhn-proxy
# chown apache:apache /var/spool/rhn-proxy
# mkdir -m 0750 -p /var/spool/rhn-proxy/list
# chown apache:apache /var/spool/rhn-proxy/list
```

デフォルトのカスタムパッケージのリポジトリーは通常、`/var/spool/rhn-proxy` です。

5. インストール後に、サーバーを最新のエラータ更新にアップデートします。

```
# yum update
```

6. RHN Proxy Server サービスを再起動して、RHN Proxy Server の機能をテストします。

```
█ # /usr/sbin/rhn-proxy restart
```

第7章 トラブルシューティング

本章では、RHN Proxy Server に関連する一般的なエラーの原因の判定方法と解決方法のヒントについて説明しています。本章以外にヘルプが必要な場合には、<https://rhn.redhat.com/help/contact.pxt> の Red Hat Network サポートまでご連絡ください。利用可能なオプション一覧を表示するには、サテライトのエンタイトルメントがあるアカウントを使ってログインしてください。

7.1. プロキシサービスの維持管理

RHN Proxy Server は多数の個別コンポーネントで構成されているため、Red Hat は **rhn-proxy** というスクリプトを提供しています。これを使用すると管理者は、Proxy を停止、起動、再起動したり、Proxy のステータスを取得することができます。

表7.1 rhn-proxy コマンド

コマンド	機能
<code>/usr/sbin/rhn-proxy start</code>	このコマンドは、RHN Proxy Server が起動していない場合、起動させます。
<code>/usr/sbin/rhn-proxy stop</code>	このコマンドは、RHN Proxy Server が停止していない場合、停止させます。
<code>/usr/sbin/rhn-proxy restart</code>	このコマンドは、現在稼働している RHN Proxy Server を停止して、再起動させます。RHN Proxy Server が停止している場合は、起動させます。
<code>/usr/sbin/rhn-proxy status</code>	このコマンドは、RHN Proxy Server の最新状況を表示させます。

7.2. ログファイル

ほとんどのトラブルシューティングを行う際の最初の手順は、関連するファイルまたはログファイルを調査することからスタートします。これらのファイルは、デバイス上やアプリケーション内で実行されたアクティビティーに関する貴重な情報を提供し、パフォーマンスを監視して適切な設定の確認にも使用できます。関連ログファイルのパスについては表7.2「ログファイル」を参照してください。

表7.2 ログファイル

コンポーネント	ログファイルの場所
Apache Web server	<code>/var/log/httpd/</code> ディレクトリ
Squid	<code>/var/log/squid/</code> ディレクトリ
RHN Proxy Broker Server	<code>/var/log/rhn/rhn_proxy_broker.log</code>
RHN SSL Redirect Server	<code>/var/log/rhn/rhn_proxy_redirect.log</code>
Red Hat Update Agent	<code>/var/log/yum.log</code>

7.3. 質問と回答

本セクションには、RHN Proxy Server ソリューションのインストールと設定方法に関するよくある質問とその答えを記載しています。

問： RHN Package Manager の設定後に、ローカルパッケージがプライベート RHN チャンネルに正しく追加されたかどうか、どのように確認できますか？

答： コマンド `rhn_package_manager -l -c "name_of_private_channel"` を使用して RHN サーバーに対して既知のプライベートチャンネルパッケージを一覧表示します。または、RHN ウェブインターフェースで確認します。

登録システムをプライベートチャンネルにサブスクライブしたら、登録システムでコマンド `up2date -l --showall` を実行してプライベート RHN チャンネルからパッケージを検索することもできます。

問： Proxy Server の DNS 名設定を変更したらクライアントシステムを更新できなくなりました。この障害をどのように解決すればいいでしょうか？

答： 名前の変更を反映するためにクライアントシステムで `up2date -u` コマンドを実行します。

問： クライアント群が Squid サーバーに接続しているかどうか、どうしたら確認することができますか？

答： `/var/log/squid/access.log` ファイルが Squid サーバーに対する接続をすべて記録しています。

問： クライアントシステムの Red Hat Update Agent が RHN Proxy Server に接続しません。どうしたら解決できますか？

答： Red Hat Update Agent の最新バージョンがクライアントシステムにインストールされているか確認してください。最新バージョンには、RHN Proxy Server への接続に必要な機能が含まれています。最新バージョンはコマンド `yum update yum` を `root` として実行して Red Hat Network から取得するか、<http://www.redhat.com/support/errata/> から取得できます。

RHN Proxy Server は Apache の機能拡張です。ログファイルの場所については [表7.2 「ログファイル」](#) を参照してください。

問： RHN Proxy Server 設定が動作しません。どこからトラブルシューティングを開始したらよいですか？

答： `/etc/sysconfig/rhn/systemid` がパーミッション `0640` で `root.apache` によって所有されているか確認してください。

ログファイルを調べます。一覧は [表7.2 「ログファイル」](#) をご覧ください。

7.4. 全般的な問題

全般的な問題の調査/解決を開始するには、支障が生じているコンポーネントに関連するログファイル

を調べます。すべてのログファイルに **tail** を使用して、それから **up2date --list** を実行すると役に立ちます。その後、解決の糸口となるようなものがないか新しいログのエントリをすべて調べます。

よくある問題は、ディスク領域がいっぱいになっているというものです。この問題の最も顕著な兆候はログファイルへの書き込みが停止される状況です。単語の途中など、書き込み中にログ作業が停止された場合は、ディスクがいっぱいである可能性があります。これを確認するには、次のコマンドを実行して使用% (Use%) の欄にある割合を確認します。

```
df -h
```

ログファイルの他にも、各種コンポーネントのステータスを読みだして貴重な情報を取得することができます。Apache Web server と Squid に対して行うことができます。

Apache Web server のステータスを読み出すには、次のコマンドを実行します。

```
service httpd status
```

Squid のステータスを読み出すには、次のコマンドを実行します。

```
service squid status
```

RHN Proxy Server から管理者にメールが送信されていない場合は、**/etc/rhn/rhn.conf** の **traceback_mail** に正しいメールアドレスが設定されているか確認します。

7.5. ホストが見つかりませんでした / 完全修飾ドメイン名を確定できませんでした

RHN の設定ファイルは完全修飾ドメイン名 (FQDN) に完全に頼っているため、主要アプリケーションが RHN Proxy Server の名前を IP アドレスに解決することが必須となります。Red Hat Update Agent、Red Hat Network Registration Client、Apache Web server は特に、起動に失敗すると RHN アプリケーションが "host not found (ホストが見つかりません)" のエラーを発行し、Web サーバーが "Could not determine the server's fully qualified domain name (サーバーの完全修飾ドメイン名を確定できませんでした)" を表示するこの問題を発生させる傾向があります。

この問題は通常、**/etc/hosts** ファイルが原因となっています。ドメイン名を解決する順序と方法を定義する **/etc/nsswitch.conf** ファイルを調べることで、これが確認できます。通常、**/etc/hosts** ファイルが最初にチェックされ、続いて使用されていけば NIS (Network Information Service)、DNS の順序でチェックされます。Apache Web server が起動し、RHN クライアントアプリケーションが動作するためには、これらのいずれかが成功する必要があります。

この問題を解決するには、**/etc/hosts** ファイルの内容を確認します。次のようになっています。

```
127.0.0.1 this_machine.example.com this_machine localhost.localdomain \
localhost
```

テキストエディターでマシンのホスト情報を削除します。以下のようになります。

```
127.0.0.1 localhost.localdomain.com localhost
```

次に、ファイルを保存して RHN クライアントアプリケーションまたは Apache Web server を再度実行します。失敗が続く場合は、次のようにファイル内でプロキシの IP アドレスを明示的に識別させます。

```
127.0.0.1 localhost.localdomain.com localhost
123.45.67.8 this_machine.example.com this_machine
```

上記の値を実際のプロキシの IP アドレスに置き換えてください。これで問題が解決されるはずです。特定の IP アドレスを規定する場合には、マシンが新しいアドレスを取得した時点でそのファイルを更新する必要があります。

7.6. 接続エラー

接続エラー関連と思われる問題が発生している場合は、次の手順を実行します。

- 適切なパッケージを確認します。

```
rhn-org-httpd-ssl-key-pair-MACHINE_NAME-VER-REL.noarch.rpm
```

RHN Proxy Server 上に上記のパッケージがインストールされ、対応する **rhn-org-trusted-ssl-cert-*.noarch.rpm** または Raw 形式の CA SSL パブリック (クライアント) 証明書がすべてのクライアントシステムにインストールされていることを確認します。

- クライアントシステムが適切な証明書を使用するように設定されているか確認します。
- 1つまたは複数の Red Hat Network Proxy サーバーを使用している場合は、各プロキシの SSL 証明書が正しく用意されていることを確認します。RHN Satellite Server と併用して RHN Proxy Server を使用している場合は、プロキシはサーバーとクライアントの両方の役割を担うため、自身のサーバー SSL キーペアと CA SSL パブリック (クライアント) 証明書の両方がインストールされていなければなりません。詳しい説明については『RHN クライアント設定ガイド』の SSL 証明書の章を参照してください。
- RHN Proxy Server が HTTP Proxy 経由で接続している場合、表示されている URL が有効であることを確認します。例えば、HTTP Proxy URL フィールドには、**http://** や **https://** などのプロトコルへの参照が含まれてはいけません。**your-gateway.example.com:8080** などのように、**hostname:port** の形式でホスト名とポートのみを記載します。
- 「その他の要件」にあるように、必要なポートをブロックするファイアウォールをクライアントシステム自体が使用していないか確認します。

7.7. キャッシュ関連の問題

パッケージ配信が失敗するか、オブジェクトが破損しているように見えるが接続エラー関連ではない場合は、キャッシュの消去を検討してください。RHN Proxy Server には接続するキャッシュが2つあります。1つは Squid 用で、もう1つは認証用です。

Squid キャッシュは **/var/spool/squid/** にあり、以下の手順で消去します。

1. Apache Web server を停止します: **service httpd stop**
2. Squid server を停止します: **service squid stop**
3. 当該ディレクトリーのコンテンツを消去します: **rm -fv /var/cache/rhn/***
4. 両方のサービスを再起動します:


```
service squid start
service httpd start
```

ディレクトリーをクリアにして **squid** を再起動するとこのタスクをより速く行えますが、この方法だと多数の RHN トレースバックメッセージという結果になる可能性が高くなります。

プロキシにより使用されている認証用の内部キャッシングのメカニズムにもキャッシュのクリアが必要になる場合があります。これを行うには、次のコマンドを発行します。

```
rm -fv /var/cache/rhn/*
```

RHN Authentication Daemon は **RHN Proxy Server 3.2.2** のリリースで廃止され前述の内部認証キャッシングメカニズムに変更されましたが、そのデーモンがまだプロキシで実行している場合があります。これをオフにするには、次の順序でコマンドを発行します。

```
chkconfig --level 2345 rhn_auth_cache off service rhn_auth_cache stop
```

キャッシュをクリアするには、次を発行します。

```
rm /var/up2date/rhn_auth_cache
```

RHN Authentication Daemon の維持については、**Red Hat** は推奨しておらず、サポートもしていませんが、もしこれが必要な場合は、冗長なログ作業によりパフォーマンスに悪影響を与える可能性があるので留意してください。この理由で、デフォルトではログ作業がオフになっています (**/var/log/rhn/rhn_auth_cache.log** への)。このデーモンを実行してログを行う場合は、プロキシの **/etc/rhn/rhn.conf** ファイルに次の行を追加してログ作業をオンにします。

```
auth_cache.debug = 2
```

7.8. RED HAT によるプロキシのデバッグ

上記のトラブルシューティングすべてを試しても問題が解決できない場合、あるいは **Red Hat Network** の技術者に問題の解決を任せたい場合には、**RHN Proxy Server** で提供されている信頼性の高いサポートの利用をお勧めします。

専門知識にアクセスする方法の一つは **Red Hat ナレッジベース** です。ユーザーがよく遭遇する一般的な問題に対するソリューションを提供し、**Proxy** 関連の問題に適切な答えを見つけ出すことができる堅牢なブラウジングと検索インターフェースを備えています。**Red Hat ナレッジベース** は <http://kbase.redhat.com> からアクセスできます。

また、**Red Hat** は **SoS Report** と呼ばれるコマンドラインツールを提供しており、そのコマンドである **sosreport** として知られています。このツールは **Proxy** の設定パラメーター、ログファイル、データベース情報を収集し、**Red Hat** に直接送信します。

このツールを **RHN Satellite Server** の情報に使用する場合は **sos** パッケージをインストールしておく必要があります。レポートを作成するには、**Satellite** サーバー上で **root** になり **sosreport -o rhn** と入力します。たとえば、

```
[root@satserver ~]# sosreport -o rhn
sosreport (version 1.7)
```

```
This utility will collect some detailed information about the hardware and setup of your Red Hat Enterprise Linux system. The information is collected and an archive is packaged under /tmp, which you can send to a support representative. Red Hat will use this information for diagnostic purposes ONLY and it will be considered confidential information.
```

```
This process may take a while to complete. No changes will be made to your system.
```

```
Press ENTER to continue, or CTRL-C to quit.
```

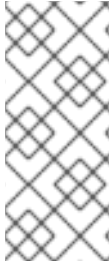
すると、名前のイニシャルとラストネーム (姓)、サポートケース番号の入力が求められます。

ファイルの生成および圧縮ファイルへのアーカイブには数分かかる場合があります。完了後は、迅速な診断を行うために **/tmp/** ディレクトリーにできた新しいファイルを **Red Hat** 担当者にメール送信してください。

付録A RHN PROXY SERVER 設定ファイルのサンプル

RHN Proxy Server の `/etc/rhn/rhn.conf` 設定ファイルを使用すると、管理者はキー構成を確立することができます。ただし、このファイルにエラーがあるとプロキシの障害が発生する可能性があるので注意してください。設定変更は十分に注意して行ってください。

RHN Satellite Server も併用している場合は、`traceback_mail` および `proxy.rhn_parent` などのパラメーターに特に注意してください。詳細については以下の設定ファイルの例とそのコメント (# マークで始まる行)を確認してください。



注記

テスト目的の場合に限り、`use_ssl` 設定を `rhn.conf` に追加することができます。値を `0` に設定するとプロキシとそれより上位のサーバ間の SSL を一時的にオフにします。これを行うとセキュリティーが大いに脅かされる状態となるので注意してください。デフォルト値の `1` に設定を戻して SSL を再度有効にするか、単に設定ファイルからその行を削除してください。

```
# Automatically generated RHN Management Proxy Server configuration file.
# -----
# -----

# SSL CA certificate location
proxy.ca_chain = /usr/share/rhn/RHNS-CA-CERT

# Corporate HTTP proxy, format: corp_gateway.example.com:8080
proxy.http_proxy =

# Password for that corporate HTTP proxy
proxy.http_proxy_password =

# Username for that corporate HTTP proxy
proxy.http_proxy_username =

# Location of locally built, custom packages
proxy.pkg_dir = /var/spool/rhn-proxy

# Hostname of RHN Server or RHN Satellite
proxy.rhn_parent = rhn.redhat.com

# Destination of all tracebacks, etc.
traceback_mail = user0@domain.com, user1@domain.com
```

付録B 改訂履歴

改訂 3-5.2.400 Rebuild with publican 4.0.0	2013-10-31	Rüdiger Landmann
改訂 3-5.2 翻訳ファイル完成	Mon Apr 22 2013	Kenzo Moriguchi
改訂 3-5.1 翻訳ファイルを XML ソースバージョン 3-5 と同期	Thu Mar 21 2013	Noriko Mizumoto
改訂 3-5 5.5 向け最終パッケージ	Wed Sept 19 2012	Dan Macpherson
改訂 3-4 5.5 リリース用に準備 テクニカルレビューによる変更を適用 BZ#491007 インストールのアップデートの章を追加	Wed Jul 4 2012	Athene Chan
改訂 3-0 5.5 リリース用に準備 テクニカルレビューによる変更を適用 BZ#491007 インストールのアップデートの章を追加	Wed Jul 4 2012	Athene Chan
改訂 2-5 BZ#682996 - 「インストール」の章で指示を更新 BZ#705755 - 「Package manager」の章に追加情報 BZ#722193 - 「要件」の章でエラーを修正 BZ#729617 - 「インストール」の章でエラーを修正 BZ#729663 - 「インストール」の章で警告を追加	Thu Jan 5 2012	Lana Brindley
改訂 2-4 z-stream リリースの変更を y-stream に適用	Mon Aug 15 2011	Lana Brindley
改訂 2-3 BZ#713527 - RHEL 6 の参照を追加	Wed Jun 22 2011	Lana Brindley
改訂 2-2 翻訳用の準備	Wed Jun 15 2011	Lana Brindley
改訂 2-1 翻訳者からの修正	Fri May 27 2011	Lana Brindley
改訂 2-0 翻訳の準備	Fri May 6 2011	Lana Brindley
改訂 1-9 BZ#653844 - QE レビュー	Wed April 27 2011	Lana Brindley
改訂 1-8 BZ#646176 - インストール	Mon Feb 7 2011	Lana Brindley

索引

シンボル

その他の要件, [その他の要件](#)

よく使われる用語, [よく使われる用語](#)

インストール

[RHN Proxy Server の, RHN Proxy Server のインストール手順](#)

[ベース, ベースインストール](#)

キャッシュ関連の問題, [キャッシュ関連の問題](#)

クライアント設定

[プライベートチャンネルにサブスクライブ, パッケージをアップロードする](#)

ソフトウェアに関する要件, [ソフトウェア要件](#)

チャンネル, [よく使われる用語](#)

[プライベートチャンネルを作成する, プライベートチャンネルの作成](#)

チャンネル管理者, [よく使われる用語](#)

ディスク領域に関する要件, [ディスク領域に関する要件](#)

トポロジー, [トポロジーの例](#)

[RHN Satellite Server とプロキシの併用, RHN Satellite Server とプロキシの併用](#)

[単一の Proxy, 単一のプロキシトポロジー](#)

[複数のプロキシを垂直に結んだトポロジー, 複数のプロキシを垂直に結んだトポロジー](#)

[複数のプロキシを水平に結んだトポロジー, 複数のプロキシを水平に結んだトポロジー](#)

トラブルシューティング, [トラブルシューティング](#)

トレースバック, [よく使われる用語](#)

ハードウェアに関する要件, [ハードウェア要件](#)

プライベートチャンネル, [プライベートチャンネルの作成](#)

ホストが見つかりませんのエラー

[完全修飾ドメイン名を確定できませんでした, ホストが見つかりませんでした / 完全修飾ドメイン名を確定できませんでした](#)

ポート

[443, その他の要件](#)

[5222, その他の要件](#)

[80, その他の要件](#)

ポート [443, その他の要件](#)

ポート [4545, その他の要件](#)

ポート [80, その他の要件](#)

ログファイル, [ログファイル](#)

全般的な問題, [全般的な問題](#)

利点, [RHN Proxy Server](#)

受信用ポート、 [Satellite](#)

[5222](#), [その他の要件](#)

接続エラー, [接続エラー](#)

組織管理者, [よく使われる用語](#)

要件, [要件](#)

その他, [その他の要件](#)

ソフトウェア, [ソフトウェア要件](#)

ディスク領域, [ディスク領域に関する要件](#)

ハードウェア, [ハードウェア要件](#)

認証, [Proxy の動作のしくみ](#)

認証キャッシング

消去する, [キャッシュ関連の問題](#)

質問と回答, [質問と回答](#)

送信用ポート

[80](#), [443](#), [その他の要件](#)

H

HTTP Proxy Caching Server

ディスク領域に関する要件, [ディスク領域に関する要件](#)

P

Proxy の動作のしくみ, [Proxy の動作のしくみ](#)

Proxy ポート, [その他の要件](#)

R

Red Hat Network

はじめに, [Red Hat Network](#)

Red Hat Update Agent, [よく使われる用語](#), [Proxy の動作のしくみ](#)

RHN Authentication Daemon、無効化

[rhn_auth_cache](#)、停止する, [キャッシュ関連の問題](#)

RHN Package Manager, [Proxy の動作のしくみ](#), [RHN Package Manager およびローカルパッケージの提供](#)

インストールする, [RHN Package Manager およびローカルパッケージの提供](#)

コマンドラインオプション, [RHN Package Manager およびローカルパッケージの提供](#)

チャンネル、指定する, [パッケージをアップロードする](#)

パッケージヘッダーのアップロード, [パッケージをアップロードする](#)

プライベートチャンネルの作成, [プライベートチャンネルの作成](#)

ローカルのパッケージ一覧の確認, [パッケージをアップロードする](#)

設定する, [プライベートチャンネルの作成](#)

設定ファイル, [RHN Package Manager](#) およびローカルパッケージの提供

rhn-proxy

サービス, [プロキシサービスの維持管理](#)

rhn.conf

サンプルファイル, [RHN Proxy Server](#) 設定ファイルのサンプル

rhn_package_manager , [パッケージをアップロードする](#) (参照 [RHN Package Manager](#))

S

satellite-debug, [Red Hat](#) によるプロキシのデバッグ

squid キャッシング, [キャッシュ関連の問題](#)