



Red Hat Network Satellite 5.4

Proxy インストールガイド

Red Hat Network Satellite

エディション 1

Last Updated: 2017-10-06

Red Hat Network Satellite 5.4 Proxy インストールガイド

Red Hat Network Satellite

エディション 1

Landmann

rlandmann@redhat.com

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

ようこそ RHN Proxy インストールガイドへ

目次

第1章 はじめに	3
1.1. RED HAT NETWORK	3
1.2. RHN PROXY SERVER	3
1.3. 知っておくべき用語	4
1.4. どのように動作するのか	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. 補足要件	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	17
第5章 RHN PACKAGE MANAGER	19
5.1. プライベートチャンネルを作成する	19
5.2. パッケージをアップロードする	19
5.3. コマンドラインオプション	20
第6章 トラブルシューティング	23
6.1. プロキシサービスの保守	23
6.2. ログファイル	23
6.3. 質問とその答え	23
6.4. 全般的な問題	24
6.5. ホストが見つかりません / FQDN を確定できませんでした	25
6.6. 接続エラー	25
6.7. キャッシュ関連の問題	26
6.8. RED HAT によるプロキシのデバッグ	27
付録A SATELLITE の WEB サイトを利用した RHN PROXY SERVER のインストール	29
付録B RHN PROXY SERVER 設定ファイルの例	38
付録C 改訂履歴	39
索引	40

第1章 はじめに

1.1. RED HAT NETWORK

Red Hat Network (RHN) は Red Hat システム群及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 はシステム群のパフォーマンス、安全性、信頼性を最大限に高めるために必要なツールやサービス、情報リポジトリなどがすべて集約されたものとなります。RHN を使用するには、システムプロファイルと呼ばれるクライアントシステム群のソフトウェアとハードウェアのプロファイルをシステム管理者の方により Red Hat Network に登録していただきます。クライアントシステムによってパッケージの更新が要求されると、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 を使用する上での長所

- スケーラビリティ – Red Hat Network を使用せずに 1 台のシステムの管理を行うより、Red Hat Network を使用して同じ 1 人のシステム管理者により数百数千の Red Hat システム群の設定や管理を行う方がより簡単、迅速、且つ正確に行うことができます。
- 標準プロトコル – 安全性の維持と機能性向上のため標準プロトコルが使用されます。例えば、XML-RPC により Red Hat Network はファイルをダウンロードするだけでなくさまざまなことを行えるようになります。
- セキュリティ – 登録したシステムと 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 Web 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 Web サイトを使用します。
- 簡素化 – Red Hat システム群の保守が簡単な自動プロセスになります。

1.2. RHN PROXY SERVER

RHN Proxy Server は RHN のバンド幅要求を低減してカスタムパッケージの配備を可能にするパッケージキャッシングのメカニズムです。Proxy を使用する場合は、Red Hat からのエラータ更新などの RPM や独自に生成したカスタムの RPM などを中央に配置した内部サーバーでキャッシュします。クライアントシステム群は個別にインターネットにアクセスすることなく Proxy から更新を受け取ることができます。

パッケージは Proxy で管理されますが、クライアントのシステムプロファイルや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) も提供します。Proxy はクライアントシステム群と 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 上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が認証され、ローカルの RHN Proxy Server から取り込まれる各パッケージの GPG 署名は Red Hat Update Agent によりチェックされます。

正式な Red Hat パッケージを格納する他、RHN Package Manager を使用して企業や組織独自のカスタム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、独自ソフトウェアを開発して RPM にパッケージ化し、独自の GPG 署名で署名します。次に、ローカルの RHN Proxy Server を利用してネットワーク内の個別システム群をすべて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 を使用する利点には以下のようなものがあります。

- スケーラビリティ – 1 企業または組織内に複数のローカル RHN Proxy Server 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群からローカルの RHN Proxy Server や Red Hat Network サーバーへのエンドツーエンドの安全な接続を維持します。
- 時間節約 – ローカルエリアネットワークによるパッケージの配信はインターネット経由に比べ大幅に高速化されます。
- バンド幅の節減 – 各クライアントシステムごとに各パッケージのダウンロードを行うのではなく、RHN から複数のパッケージを一度だけダウンロードします (ローカルの Proxy サーバーのキャッシングメカニズム単位)。
- 更新のカスタマイズ – カスタムのソフトウェアパッケージの配信を完全に自動化する他、クライアントシステム群に必要とされる Red Hat の正式パッケージの配信も自動化します。カスタムのプライベート RHN チャンネルで社内用パッケージの配信を自動化することができます。
- 設定のカスタマイズ – 特定のアーキテクチャや OS のバージョンへの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 – クライアントシステム群はインターネットではなく RHN Proxy Server に接続するため、クライアント群に必要とされるのはローカルエリアネットワークへの接続のみです。RHN サーバーと通信するためにインターネット接続を必要とするのは RHN Proxy Server のみです。但し、RHN Proxy Server が RHN Satellite Server を使用している場合は、インターネット接続を必要とするのは RHN Satellite Server になります。

1.3. 知っておくべき用語

RHN Proxy Server を理解する前に、次のような Red Hat Network 関連の用語を知っておくことが重要になります。

Channel

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と Red Hat リリースに対応するパッケージ一覧から成ります。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すがエクストラパッケージが入っています。

Organization Administrator

Organization Administrator とは企業や組織の Red Hat Network アカウント全体を管理する最上位レベルのユーザーロールになります。このロールを持つメンバーは他のユーザー、他のシステム群、システムグループなどを追加したり削除したりすることができます。Red Hat Network の企業や組織には少なくとも 1 人の Organization Administrator が必要です。

Channel Administrator

Channel Administrator とはチャンネルの管理機能に対して完全なアクセス権を有するユーザーロールになります。このロールを有するユーザーはチャンネルを作成したりチャンネルにパッケージを割り当てることができます。このロールは RHN Web サイトのユーザー タブで Organization Administrator により割り当てることができます。

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**) であり、このアプリケーションが実行されるクライアントシステム用の新しいパッケージや更新パッケージをユーザーが取得してインストールできるようになります。

Traceback

トレースバックは「何が悪かったのか」という詳細を示し、RHN Proxy Server の問題解決を行う上で役に立ちます。トレースバックは重大なエラーが発生すると自動的に生成され、RHN Proxy Server の設定ファイル内で指定された宛先にメールが送信されます。

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』および Satellite Web ユーザーインターフェースにあるヘルプページを参照してください。

1.4. どのように動作するのか

クライアントシステムの Red Hat Update Agent またはパッケージアップデーターは Red Hat Network サーバーと直接には通信しません。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 サーバーまたは 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に直接アクセスする必要はありません。クライアントシステムは RHN Proxy Server にのみアクセスする必要があります。



重要

Red Hat は、適切な接続を確保できるようにクライアント群が接続している RHN Proxy Server には Red Hat Enterprise Linux の最新の更新を稼働させ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 サーバーにより認証されます。RHN Proxy Server にアクセスするクライアントの認証も RHN により行われますが、この場合、Proxy が RHN に対して認証およびルートを提供することになります。認証が成功すると、Red Hat Network サーバーは RHN Proxy Server にそのクライアントに対して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群の Red Hat Update Agent またはパッケージアップデーターによる要求はサーバー側で認証されますが、そのパッケージは HTTP Proxy Caching Server または RHN Proxy Server (ローカルパッケージの場合) にキャッシュされるためパッケージの配信が大幅に高速化されます。RHN Proxy Server とクライアントシステムが LAN 経由で接続されるため、速度はローカルネットワークによってのみ影響されます。

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 サーバーに到達するまで1つまたは複数の RHN Proxy Server を経由して行きます。
2. Red Hat Network サーバー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。この署名と有効期限を持つ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 サーバー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 で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 サーバーとの違いは見られません。Red Hat Network サーバー側から見ると、RHN Proxy Server は RHN クライアントの特殊タイプとなります。したがってクライアント群は、Red Hat Network サーバーに到達するために要求が通るルートによる影響を受けません。こうした論理が RHN Proxy Server 及び Red Hat Network サーバーに実施されます。

オプションで RHN Package Manager をインストールしてその企業専用に特別に作成されたカスタムパッケージを配信するよう設定することができます。こうしたカスタムパッケージを含む Red Hat パッケージ以外の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) からのみ配信が可能です。プライベートの RHN チャンネルを作成したら RHN サーバー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、これにより RHN がパッケージのインストールを自動化することができるようになります。実際のカスタム RPM パッケージは RHN Proxy Server 上に格納し、企業組織のローカルエリアネットワーク内でクライアントシステム群に送信します。

RHN Proxy Server を利用するようコンピュータネットワークを設定するのは簡単です。クライアントシステム群の Red Hat Network アプリケーションが Red Hat Network サーバーではなく RHN Proxy Server に接続されるよう設定する必要があります。詳細については『RHN クライアント設定ガイド』を参照してください。プロキシ側でチェーン内の次のプロキシを指定する必要があります (最終的に Red Hat Network サーバーに到着)。RHN Package Manager を使用する場合はクライアントシステム群をプライベート RHN チャンネルにサブスクライブさせなければなりません。

[1] 本ガイドでは、「RHN」は RHN の Hosted サイト (<http://rhn.redhat.com>) または RHN Satellite Server のいずれかを指します。

第2章 要件

インストールを行う前に次の要件が満たされていることを確認してください。 **Satellite** 自体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 5.1** をインストールする場合は **Satellite** のバージョンが **5.1** またはそれ以降でなければならず、**5.0** またはそれ以前のバージョンではインストールを行えません。

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利用可能でなければなりません。

- ベースとなるオペレーティングシステム – **RHN Proxy Server** は **Red Hat Enterprise Linux 5** に対応しています。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、キックスタートなどからインストールできます。または **Red Hat** でサポートしているインストール方法ならいつでも行うことができます。

RHN Proxy Server は **Xen**、**KVM**、**VMware** など **Red Hat** がサポートしている仮想環境内の **Red Hat Enterprise Linux 5** 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、競合を避けるため **RHN Proxy Server** は物理的なハードウェアを基礎として実行する単一アプリケーションとして配備することを推奨します。また、仮想化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している場合のパフォーマンスと常に同等になるとは限らないため、仮想環境の選択および調整に関するガイドラインには十分な注意が必要な場合があります。



注記

ご購入頂いた **RHN Proxy** には、1 **Proxy** につき 1 インスタンス分の **Red Hat Enterprise Linux Server** サポートが含まれています。 **RHN Proxy** は、**Enterprise Linux** の新規のインストール上にインストールする必要があり、この **RHN Proxy** がオペレーティングシステムで提供される唯一のサービスでありアプリケーションでなければなりません。その環境内で他のデーモンやアプリケーション、サービスなどの実行に **RHN Proxy** に同梱されている **Red Hat Enterprise Linux** オペレーティングシステムを使用してもサポートされません。

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。パッケージを追加するとインストール時にエラーが発生する可能性があります。したがって、**Red Hat** は次の方法で目的の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。

- ご利用の **RHN Satellite Server** アカウント内で使用できる **RHN Proxy Server** エンタイトルメント
- ご利用の **RHN Satellite Server** アカウント内で使用できる **Provisioning** エンタイトルメント (ご利用の **RHN Proxy Server** エンタイトルメントに同梱されているはずです)

- 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 **spacewalk-proxy-installer** パッケージが含まれ、このパッケージに 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があります。
- Proxy 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)
- プロキシにインストールする RHN Hosted ユーザー用の **rhns-certs-tools** パッケージ (RHN Tools チャンネルより)、または RHN Satellite Server ユーザーに親サーバーの証明書を生成する際に使用する SSL CA 証明パスワード
- 旧式の Web UI によるインストール方法を使用する場合、リモートコマンド群及び Red Hat Network 経由による設定管理を受け付けるシステム構成。詳細は「[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 5 GB の記憶容量
- ディストリビューション/チャンネルごとに 25 GB 以上の記憶容量

Apache Web server に対する負荷は、クライアントシステム群が 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群の `/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を大幅に増大することになります。



注記

RHN Proxy Server は、マルチホームのネットワークポロジではキックスタートによるプロビジョニングに対応していません。複数のネットワークインターフェースを持つ Proxy サーバーではキックスタートは正しく機能しません。

2.3. ディスク領域に関する要件

RHN Proxy Server で使用されるキャッシングのメカニズムはクライアント群の帯域幅を大幅に節約することができる Squid HTTP プロキシになります。利用可能な領域が十分にあるはずで、キャッシュされたパッケージは `/var/spool/squid` に格納されます。ディストリビューションまたはチャンネルごとに 6 GB の空き領域の配分が必要となります。

RHN Proxy Server でカスタムのパッケージやローカルのパッケージを配信するよう設定を行う場合は、ローカルの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全カスタムパッケージの格納に十分なディスク領域があることを必ず確認してください。カスタムパッケージは `/var/spool/rhn-proxy` 内に格納されることとなります。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するカスタムパッケージの数により異なります。

2.4. 補足要件

次の補足要件を満たしていない限り RHN Proxy Server のインストールが完了したとはいえません。

完全なアクセス

クライアントシステム群には RHN Proxy Server のサービスおよびポートへの完全なネットワークアクセスが必要になります。

ファイアウォールのルール

RHN では RHN Proxy Server の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を強く推奨します。ただし、RHN Proxy Server の実装に応じて各種の TCP ポートを Proxy 上で開く必要があります。

表2.1 Proxy で開くポート

ポート	方向	理由
80	アウトバウンド	Proxy はこのポートを使用して rhn.redhat.com 、 xmlrpc.rhn.redhat.com 、Satellite URL に接続します (RHN Hosted と Satellite Server のどちらと RHN Proxy が通信するのかにより異なる)。
80	インバウンド	クライアントの要求は http か https 経由で着信します。
443	インバウンド	クライアントの要求は http か https 経由で着信します。
443	アウトバウンド	Proxy はこのポートを使用して rhn.redhat.com 、 xmlrpc.rhn.redhat.com 、Satellite URL に接続します (RHN Hosted と Satellite Server のどちらと RHN Proxy が通信するのかにより異なる)。
4545	アウトバウンド	Proxy が RHN Satellite Server に接続されている場合、Monitoring が有効でプローブが登録済みシステム群に対して設定されていると、Monitoring がこの TCP ポート経由でクライアントシステム上で実行中の <code>rhnmmd</code> への接続を確立します。
5222	インバウンド	RHN Push テクノロジーを使用している場合、このポートを開くと <code>osad</code> クライアントから Proxy 上の <code>jabberd</code> デーモンへの接続が許可されます。
5269	アウトバウンド	Proxy が RHN Satellite Server に接続されている場合、RHN Push テクノロジーの <code>jabberd</code> 経由サーバーツーカーサーバー接続を許可するためにこのポートを開いておく必要があります。

システム時間の同期

SSL を実行している Web サーバーに接続する際には時間が非常に重要になります。SSL 証明が使用

中または使用前に期限切れにならないよう、クライアント群とサーバーで設定する時間は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をお勧めします。

完全修飾ドメイン名 (FQDN)

RHN Proxy Server がインストールされ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 のアカウント

増分更新を受信するため中央 Red Hat Network サーバーに接続する場合は Red Hat Network のアカウントが必要になります。アカウントのセットアップについてはご購入時に担当セールスがお手伝いさせていただきます。

ログイン情報のバックアップ

主要なログイン情報についてはすべてお客様側で記録を保持して頂かなければなりません。RHN Proxy Server の場合、SSL 証明書の生成および Organization Administrator アカウントのユーザー名とパスワードなどになります。Red Hat ではこの情報を別々のフロッピー 2 枚にそれぞれコピーし、またハードコピーとして印刷して耐火性金庫などに保存することを強くお勧めします。

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、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)は `/var/www/html/pub/` などプロキシ上の転送が行われない場所に置くよう注意してください。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はパブリックにはアクセスできないようにすることをお勧めします。こうしたマシンへのシェルアクセスはシステム管理者に限り、ユーザーにはアクセスを持たせないようにしてください。不必要なサービスはすべて無効にしてください。`ntsysv` や `chkconfig` を使用するとサービスを無効にすることができます。

最後に、各ガイドは次のような順序でお読みになるとよいでしょう。

1. 『RHN Proxy Server インストールガイド』 - 現在お読みになられているガイドでは、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』 - このガイドでは、RHN Proxy Server または RHN Satellite Server により管理されるシステム群の設定方法を説明しています。(また、このガイドをお読み頂く上で『RHN リファレンスガイド』も参照して頂く必要がある場合があります。RHN リファレンスガイドはシステム群の登録と更新について記載されています。)
3. 『RHN チャンネル管理ガイド』 - 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、システム群の登録及び更新を行う方法、RHN Web 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つでしょう。

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。次のような要素に応じて構成方法を選択してください。

1. RHN Proxy Server によってサービスを提供するクライアントシステムの合計数。
2. RHN Proxy Server に **同時接続** が予測されるクライアント群の最大数
3. RHN Proxy Server によって管理されるカスタムパッケージとチャンネルの数
4. その環境で使用する RHN Proxy Server の数

本章では考えられる構成とその利点について説明していきます。

3.1. 単一のプロキシトポロジー

単一の RHN Proxy Server を使用してネットワーク全体を供給するのが最もシンプルな構成になります。この構成は小規模サイズのクライアントグループとネットワークを提供するのに適しています。Red Hat の RPM をキャッシュし、またカスタムパッケージをローカルサーバーに格納できる点などが長所となります。

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点が単一の RHN Proxy Server を使用する上での短所です。

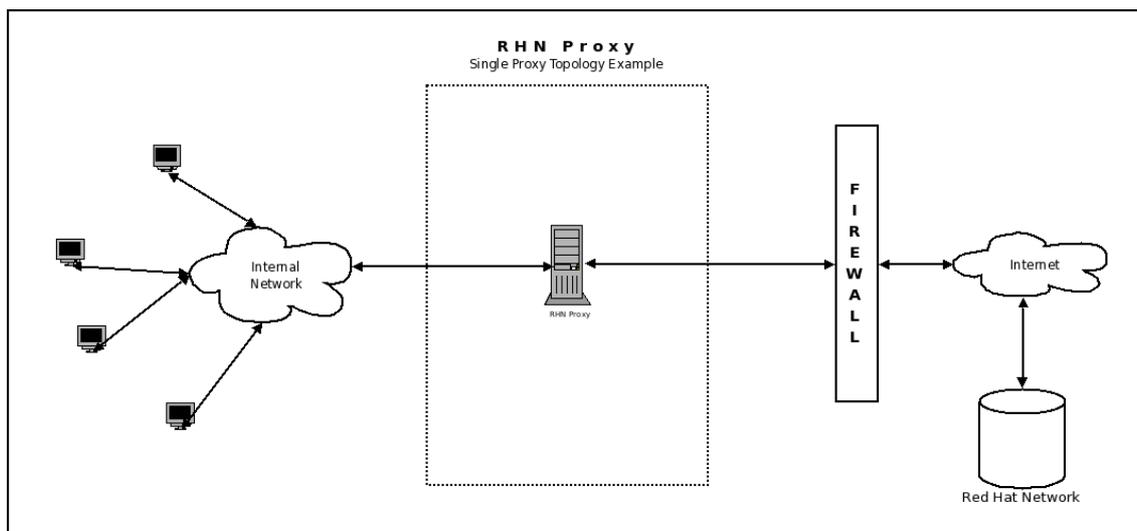


図3.1 単一のプロキシトポロジー

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 に接続するなどのより分散型の方法が必要になる場合があります。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 Proxy** 間でパッケージを同期化するファイル転送プログラムを使用します。
- NFS 共有を Proxy とカスタムチャンネルのレポジトリ間に作成します。

いずれかのソリューションによりいずれの RHN Proxy Server のいずれのクライアントにもすべてのカスタムパッケージが配信されることとなります。

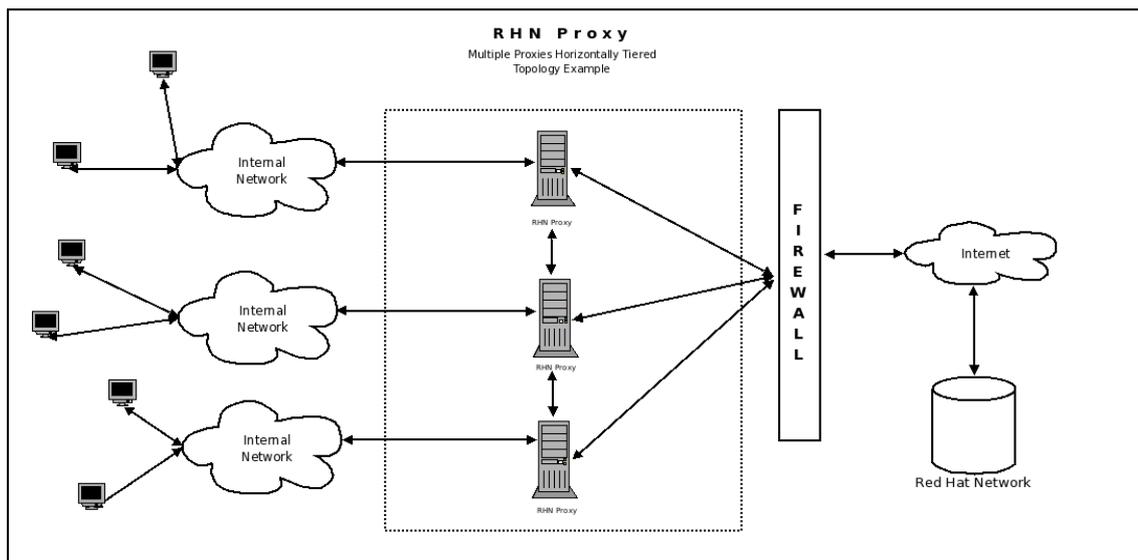


図3.2 複数のプロキシを水平に結んだトポロジー

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 の代替方法として、第1プロキシを定めて他のプロキシは Red Hat Network の RPM やローカルに作成されたカスタムパッケージを取得するためにこのプロキシに接続させます。基本的には、第2プロキシ群は第1プロキシのクライアント群として動作します。各プロキシは製品固有の **up2date** 機能を使用するため RHN Proxy Server 間で同期を行う必要性が緩和されます。

水平に結んだ構成と同様、垂直方法によりいずれの RHN Proxy Server のいずれのクライアントにもすべてのカスタムパッケージを配信することができます。Proxy は単にファイルシステムにパッケージがあるかどうかその Proxy のリポジトリを検索するだけです。パッケージが見つからないと上位のレベルで検索を試行します。

垂直に結んだ構成では、第2 Proxy 群が RHN からの更新やカスタムパッケージを必ず第1 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第1 Proxy にのみ配置しなければなりません。最後に、第2 Proxy の設定ファイルは Red Hat Network を直接ポイントするのではなく、第1 Proxy をポイントしている必要があります。

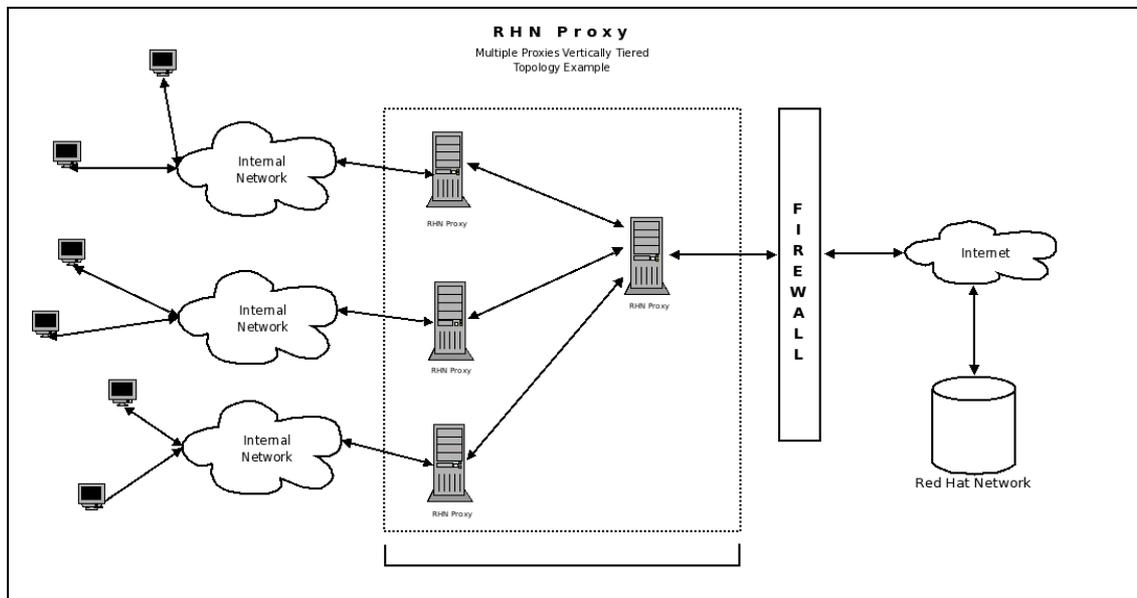


図3.3 複数のプロキシを垂直に結んだトポロジー

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以外にも、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、サテライトは大規模なクライアントシステム群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 (RHN Client Configuration Guide)』に説明があります。両者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 (RHN Channel Management Guide)』を参照してください。

第4章 インストール

本章では、はじめての RHN Proxy Server 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。RHN Proxy Server の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及びインストール後は、次の点を必ず確認してください。

- 前述したハードウェア要件に従い、パッケージの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` になり、カスタムパッケージは `/var/spool/rhn-proxy` に置かれます。



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上にある使用可能な容量を自動的に計算し、その空き容量の最大 60 パーセントを RHN Proxy Server の使用に割り当てます。

- RHN Proxy Server に必要な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 のインストールが失敗する原因となります。

Red Hat Enterprise Linux の各バージョンに必要とされる適切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 のインストール手順を以下に説明します。

1. コマンド `rhn_register` を使用して RHN Proxy Server エンタイトルメントを持つ企業または組織のアカウントで Red Hat Network (中央 RHN サーバーまたは 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。
2. インストールを実行するには以下のコマンドを入力します。

```
configure-proxy.sh
```

インストールオプションや SSL 証明書の生成など、RHN Proxy Server のインストールおよび初期設定に関する詳細についてはコマンドラインのインストールプログラムにより求められる一連のプロンプトで進められていきます。インストールプロセスを以下に示します。



注記

プロンプトで何も入力せずに **Enter** キーを押すと、RHN Proxy Server 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。

また、ユーザーに入力をまったくさせずデフォルトの答えを使用したい場合は、すべてデフォルトの応答を使用する **--non-interactive** オプションを使います。

- 最初のプロンプトセットはインストールに関するサイト固有の詳細について聞いてきます。

```
Proxy version to activate [5.3]:
```

Proxy version ではインストールする RHN Proxy Server のバージョン確認を求めてきます。

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

RHN Parent は Proxy にサービスを提供するシステムのドメイン名またはアドレスです。RHN Hosted サーバー (xmlrpc.rhn.redhat.com)、RHN Satellite Server 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電子メールアドレスであり、通常は Proxy 管理者の電子メールです。このプロンプトで複数の電子メールアドレスを入力する場合はカンマで区切ります。

- 次のプロンプトセットは SSL 証明書を生成するための詳細設定に関する事項です。RHN Proxy Server との通信の安全性を確保するため SSL を使用することを推奨します。

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

Use SSL プロンプトで **y** を入力すると RHN Proxy Server が SSL に対応するよう設定されます。

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

CA Chain プロンプトでは、**Enter** キーを押すと認証局 (CA) チェーンのデフォルトパスを使用するようになります。RHN Proxy が RHN Satellite と通信している場合には、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 `/usr/share/rhn/RHNS-CA-CERT` ファイルとなります。

```
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** などのようにプロキシホスト名とポート番号を入力します。

```
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]:
```

適切な SSL サーバー証明書を作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。

5. コマンドラインインストールプログラムでは、RHN Proxy Server に監視機能のサポートをインストールするかどうか聞いてきます。また、今後の RHN Proxy Server インストール用の設定チャンネルを作成してデータを入力することができます。このプログラムによって SSL 設定が完了され、RHN Proxy Server インストールプログラムを実行した結果として設定を変更したすべてのサービスデーモンが再起動されます。

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

Proxy サーバーに監視機能の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
```

configure-proxy.sh プログラムによって SSL が設定されます。まず認証局のパスワードの作成とその確認が求められ、次に SSL のキーとパブリック証明書が生成されます。

```
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

```

インストーラは **configure-proxy.sh** の実行中に作成された設定ファイルに応じて設定チャンネルを作成するかどうか聞いてきます。RHN Proxy Server をインストールし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 の設定チャンネルが作成され、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**、**jabberd** などのサーバーファイルが収集されます。

- 最後にインストーラは RHN Proxy Server 関連のすべてのサービスの起動と再起動を行い、これらが完了するとインストーラは終了します。

```

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

システムに RHN Proxy Server をインストールするプロセスの一部を自動化したい場合は **configure-proxy.sh** プログラムを使用すると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した応答を含む **回答ファイル** を作成することができます。

以下にサンプルファイルを示します。バージョン番号、親サーバーとして機能する RHN Satellite Server サーバー、SSL、および他の設定パラメータに関して指定した回答が含まれています。回答

ファイルの作成方法と使い方については、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=5.2
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 で回答ファイルを使用するには以下のコマンドを入力します (例では **answers.txt** という名前)。

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

第5章 RHN PACKAGE MANAGER

コマンドラインツールの RHN Package Manager を使用すると、プライベート RHN チャンネルに関連付けられたローカルパッケージを RHN Proxy Server 経由で提供することができるようになります。RHN Proxy Server が Red Hat パッケージしか更新しない場合は RHN Package Manager をインストールしないようにしてください。

RHN Package Manager を使用する場合は `rhns-proxy-package-manager` パッケージとその依存パッケージをインストールします。

RHN サーバーにはパッケージのヘッダー情報のみをアップロードします。RHN がクライアントシステム群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、`/etc/rhn/rhn.conf` 設定ファイルで定義されているプロキシと同じ設定を使用します。

5.1. プライベートチャンネルを作成する

RHN Proxy Server からローカルパッケージを供給する前に、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** 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、このユーザーにチャンネル編集に関するパーミッションセットがあるかどう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** 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** 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** 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が推奨されているフィールドです。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** 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 **Organization Administrator** になる必要があります。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を作成したら、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から RHN Proxy Broker Server にそのパッケージをコピーします。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、コマンドラインで次のように入力します。

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

pkg-list はアップロードするパッケージの一覧です。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は存在し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指定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とパッケージはどのチャンネルにも追加されません。こうしたパッケージは Red Hat Network Web 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。この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、RHN Web インターフェースを使うと直ちに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**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**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**サブタブをクリックすると、各 RPM が一覧表示されるはずですが。

コマンドラインでは、ローカルディレクトリが RHN サーバーのチャンネルイメージと同期しているかどうかを確認することもできます。

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

-s オプションを付けると不足しているパッケージがすべて表示されます (RHN サーバーにアップロードされているのにローカルディレクトリにないパッケージ)。このコマンドを使用するには **Organization Administrator** になる必要があります。このスクリプトでは RHN のユーザー名とパスワードの入力が求められます。その他コマンドラインオプションについては [表 5.1 「rhn_package_manager オプション」](#) を参照してください。

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 Web サイトに行く必要があります。

5.3. コマンドラインオプション

RHN Package Manager (**rhn_package_manager**) の全コマンドラインオプションの概要を示します。

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	DIR ディレクトリのパッケージを処理します。

オプション	詳細
<code>-cCHANNEL</code> 、 <code>--channel=CHANNEL</code>	指定したチャンネルを管理します - 複数表記が可能です。
<code>-nNUMBER</code> 、 <code>--count=NUMBER</code>	呼び出し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。
<code>-l</code> 、 <code>--list</code>	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。
<code>-s</code> 、 <code>--sync</code>	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。
<code>-p</code> 、 <code>--printconf</code>	現在の設定を表示して終了します。
<code>-XPATTERN</code> 、 <code>--exclude=PATTERN</code>	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。
<code>--newest</code>	指定チャンネル用にサーバーに既にプッシュしたパッケージよりも新しいパッケージのみプッシュを行います。
<code>--stdin</code>	<code>stdin</code> からパッケージ名を読み取ります。
<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しかプッシュを試行しません。
<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>-?</code> 、 <code>--usage</code>	オプションの簡潔な説明を表示します。
<code>--copyonly</code>	引数内に指定した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のパッケージを1つだけ紛失してしまったが、そのチャンネルの全パッケージの再インポートは行いたくない場合に便利です。例、 <code>rhn_package_manager -cCHANNEL --copyonly/PATH/TO/MISSING/FILE</code>

オプション	詳細
-h、--help	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 `rhncp` の `man` ページでも説明されています (`man rhncp`)。

第6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要因の判定方法と解決方法のヒントについて記載しています。本章以外にヘルプが必要な場合には、<https://rh.redhat.com/help/contact.pxt> の Red Hat Network サポートまでご連絡ください。全オプションの一覧はサテライトのエンタイトルメントを有するアカウントを使ってログインするとご覧頂けます。

6.1. プロキシサービスの保守

RHN Proxy Server は多数の個別コンポーネントから構成されるため、Red Hat は **rhn-proxy** というスクリプトを提供しています。このスクリプトを使用すると、Proxy の停止、起動、状態の取得などができます。

```
/usr/sbin/rhn-proxy start
/usr/sbin/rhn-proxy stop
/usr/sbin/rhn-proxy restart
/usr/sbin/rhn-proxy status
```

RHN Proxy Server 全体をシャットダウンしてから起動して、その全サービスの状態メッセージを一度に取得するには **rhn-proxy** コマンドを使用します。

6.2. ログファイル

トラブルシューティングの手順とは実際には関連するログファイル、ときには複数のログファイルを調査することからスタートします。こうしたファイルはデバイス上やアプリケーション内で起きていたアクティビティに関する貴重な情報を提供してくれるため、パフォーマンスを監視して適切な設定を確保することができます。関連ログファイルのパスについては表6.1「ログファイル」をご覧ください。

表6.1 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>

6.3. 質問とその答え

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方法及び設定方法に関してよくある質問と答えを記載しています。

問： RHN Package Manager の設定後に、ローカルの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のようにしたら確認できますか？

答: コマンド `rhnpkgmgr -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 Web インターフェースに行くことができます。

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させたら、登録システムで `up2date -l --showall` コマンドを実行してプライベート RHN チャンネルからのパッケージを表示させることもできます。

問: Proxy Server の DNS 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: クライアントシステムで `up2date -u` コマンドを実行して名前の変更を反映させます。

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: Squid サーバーに対する接続はすべて `/var/log/squid/access.log` ファイルに記録されます。

問: クライアントシステム群の Red Hat Update Agent が RHN Proxy Server 経由で接続しません。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 経由で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 の機能拡張になります。ログファイルの場所については [表6.1「ログファイル」](#) をご覧ください。

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6.1「ログファイル」](#) にあります。

6.4. 全般的な問題

全般的な問題の調査と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またはファイル群を調べます。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。次に、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てみます。

よくある問題としてディスク領域が満杯というのがあります。この問題の最も明確な兆候として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、ディスクが満杯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率 (Use%) の欄にある割合を確認します。

■

```
df -h
```

ログファイル以外にも、各種コンポーネントの状態を回収して貴重な情報を取得することができます。Apache Web server 及び Squid に対して行うことができます。

Apache Web server の状態を取得するには、次のコマンドを実行します。

```
service httpd status
```

Squid の状態を取得するには、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、`/etc/rhn/rhn.conf` の `traceback_mail` に正しい電子メールアドレスが設定されているか確認します。

6.5. ホストが見つかりません / FQDN 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) にのみ完全に依存しているため、主要なアプリケーションが RHN Proxy Server の名前を IP アドレスに解決できなければなりません。Red Hat Update Agent、Red Hat Network Registration Client、Apache Web server は特にこれに関する問題が発生しやすく、起動に失敗すると RHN アプリケーションでは "host not found (ホストが見つかりません)" のエラーが発生し Web サーバーでは "Could not determine the server's fully qualified domain name (完全修飾ドメイン名を確定できませんでした)" というメッセージが出力されます。

この問題は一般的に `/etc/hosts` ファイルに起因します。解決されるドメイン名の順序と方法を定義している `/etc/nsswitch.conf` を調べるとこれを確認することができます。通常、`/etc/hosts` ファイルがまず最初に確認され、次に NIS を使用していれば NIS そして DNS の順序で確認されます。Apache Web server が起動して RHN クライアントアプリケーション群が動作するためには、これらのいずれかが成功しなければなりません。

この問題を解決するには、次に示すような `/etc/hosts` ファイルの内容を確認します。

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

まず、次のようにテキストエディタで問題となっているマシン情報を削除します。

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

次に、この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。まだ失敗する場合は、次のようにファイル内のプロキシの 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
```

上記の値は実際のプロキシの 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が。特定の IP アドレスを定める場合は、マシンが新しいアドレスを取得した際にこのファイルの更新が必要になりますので忘れないようにしてください。

6.6. 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には、次の手順で確認します。

- 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 上には上記のパッケージがインストールされ、全クライアントシステム群には該当の `rhn-org-trusted-ssl-cert-*.noarch.rpm` または生の CA SSL パブリック (クライアント) 証明書が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群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。
- RHN Proxy Server を1つまたは複数使用する場合、各プロキシの SSL 証明書が正しく設定されているか確認します。RHN Proxy Server を RHN Satellite Server と併用する場合、Proxy はサーバーとクライアント両方の役割を果たすため、Proxy サーバーとしての 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。これについては『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は指定している URL が有効であるか確認してください。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を含ませることはできません。`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だけを含ませるようにしてください。
- 「補足要件」で説明されているように、必要となるポートをブロックしてしまうファイアウォールをクライアントシステム群が使用していないか確認します。

6.7. キャッシュ関連の問題

パッケージ配信が失敗したりオブジェクトが破損しているような見えるけれど接続関連のエラーではない場合はキャッシュのクリアを考慮してください。RHN Proxy Server には接続する必要があるキャッシュが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/` にあります。これをクリアにする場合は、Apache Web server と Squid を停止してからこのディレクトリの内容を削除した後、両方のサービスを再度起動します。次の順序でコマンドを発行します。

```
service httpd stop
service squid stop
rm -fv /var/spool/squid/*
service squid start
service httpd start
```

ディレクトリをクリアにして squid を再起動すると同じ作業が手早く行えますが、RHN トレースバックのメッセージをいくつか受け取る可能性があります。

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 のリリースで非推奨となり、前述の内部認証キャッシングのメカニズムに変更されましたが、このデーモンがご使用のプロキシでまだ実行している場合があります。これをオフにするには、次の順序で個別のコマンド群を発行します。

■

```
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
```

Red Hat では非推奨となりサポートされない **RHN Authentication Daemon** を維持しなければならない場合には、冗長なログ機能が原因でパフォーマンスに悪影響を及ぼす可能性がある点に注意してください。こういう理由でこのログ機能はデフォルトでオフになっています (`/var/log/rhn/rhn_auth_cache.log`)。このデーモンをあえて実行しログを行いたい場合は、プロキシの `/etc/rhn/rhn.conf` ファイルに次の行を追加してログ機能をオンにします。

```
auth_cache.debug = 2
```

6.8. RED HAT によるプロキシのデバッグ

こうしたトラブルシューティングには手を尽くしたが解決できない、または問題を **Red Hat Network** の技術者に委ねたい場合は、**RHN Proxy Server** に付属する信頼度の高いサポートを利用することをお勧めします。

こうしたサポートのひとつが **Red Hat ナレッジベース** です。Red Hat ナレッジベースでは、ユーザーが直面した最も一般的な問題のソリューションを提供し、発生した **Proxy** の問題に対して適切な解答を見つけ出すことができる堅牢な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> でご覧いただくことができます。

また、Red Hat は **SoS Report** と呼ばれるコマンドラインツールも提供しています。一般的には `sosreport` のコマンドで知られています。このツールは **Proxy** の設定パラメータ、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。

RHN Satellite Server 情報にこのツールを使用する場合は `sos` パッケージをインストールしておく必要があります。Satellite サーバーで `root` になり `sosreport -o rhn` と入力してレポートを作成します。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.
```

ファーストネーム (名) のイニシャルとラストネーム (姓)、そしてサポートケース番号 (Issue Tracker 番号とも呼ばれる) の入力が必要です。

レポートが生成され圧縮ファイルにアーカイブされるまでに数分かかる場合があります。完了したら、迅速な診断が行えるよう `/tmp/` ディレクトリにできた新しいファイルを Red Hat の担当者にメールで送信してください。

付録A SATELLITE の WEB サイトを利用した RHN PROXY SERVER のインストール

「[RHN Proxy Server のインストール手順](#)」に記載されているインストール方法以外にも、RHN Satellite Server の Web サイトから RHN Proxy Server をインストールすることができます。



警告

このインストール方法は非推奨になっているため、RHN Satellite Server の今後のバージョンでは削除される可能性があります。推奨されるインストール方法については「[RHN Proxy Server のインストール手順](#)」に記載されています。

1. `rhncfg-register` コマンドを使用して、RHN Proxy Server エンタイトルメントを持つ組織のアカウントを使い新しくインストールした Red Hat Enterprise Linux AS システムを Red Hat Network (中央 RHN サーバーまたは RHN Satellite Server) に登録します。
2. システムに Provisioning エンタイトルメントを与えます。RHN Web サイト (または Proxy を提供している Satellite の完全修飾ドメイン名) にアクセスし、Organization Administrator としてログインしてから **ユーザーの RHN => サブスクリプションの管理** ページに移動します。RHN Proxy Server をインストールするシステムのチェックボックスを選択し、ドロップダウンボックスから Provisioning を選択して **エンタイトルメントの追加** ボタンをクリックします。
3. システムの名前をクリックし、**システム => システムの詳細** ページに移動してベースとなるオペレーティングシステム用の Red Hat Network Tools チャンネルにシステムをサブスクライブさせていることを確認します。サブスクライブされているチャンネル セクションで Tools チャンネルに一覧表示されているチャンネルを確認します。このチャンネルにサブスクライブされていない場合は **チャンネルサブスクリプションの変更** リンクをクリックし、ツールチャンネルの隣にあるチェックボックスを選択して **サブスクリプションの変更** ボタンをクリックし、その選択を確認します。
4. まず、システム (System) => システムの詳細 (System Details) => ソフトウェア (Software) => パッケージ (Packages) => インストール (Install) サブタブに移動して `rhncfg-actions` パッケージをインストールします (依存パッケージとして `rhncfg` パッケージと `rhncfg-client` パッケージもインストールされます)。次に **パッケージ名によるフィルタ (Filter by Package Name)** のテキスト検索ボックスを使用して `rhncfg-actions` を検索します。結果一覧で `rhncfg-actions` パッケージを選択しインストールします。
5. Proxy で SSL 暗号化を有効にし、中央 RHN サーバーに接続する場合は同じ Red Hat Network Tools チャンネルから `rhns-certs-tools` パッケージをインストールし、RHN SSL Maintenance Tool を使用して後で必要となる tar ファイルを生成します。手順については、『RHN クライアント設定ガイド (RHN Client Configuration Guide)』の「SSL 証明書」の章を参照してください。

Proxy で SSL の暗号化を有効にして RHN Satellite Server または別の RHN Proxy Server に SSL を使用して接続する場合は、この親システムに対して使用する CA 証明書のパスワードも必要になります。

- ターミナルから `root` としてシステムにログインし、`rhn_check` コマンドを実行してスケジュールされているパッケージのインストールを直ちに開始します。
- パッケージがインストールされたら (システムの詳細 => イベント (Events) タブで確認)、以下のコマンドを使用してシステムがリモートのコマンドと設定管理を受け入れるよう準備を整えます。

```
/usr/bin/rhn-actions-control --enable-all
```

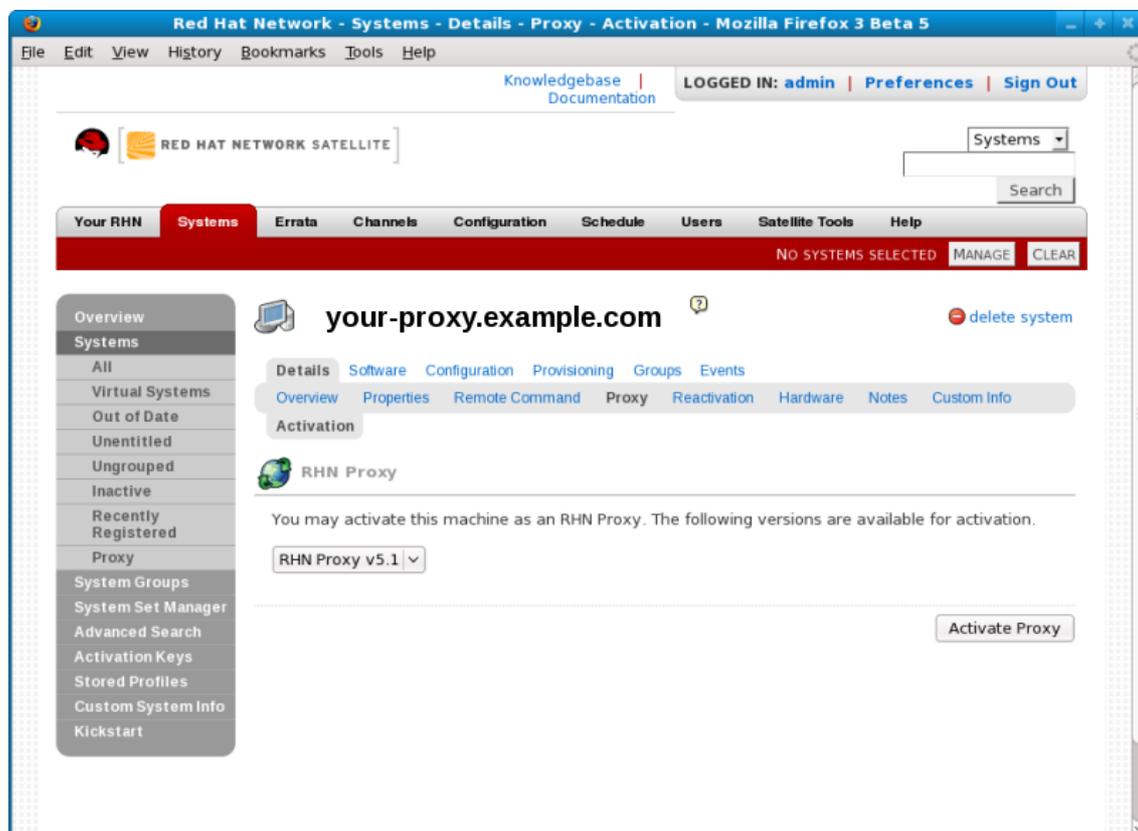
- RHN Web サイト内でシステムの詳細 => 詳細 => プロキシ サブタブに移動します。



警告

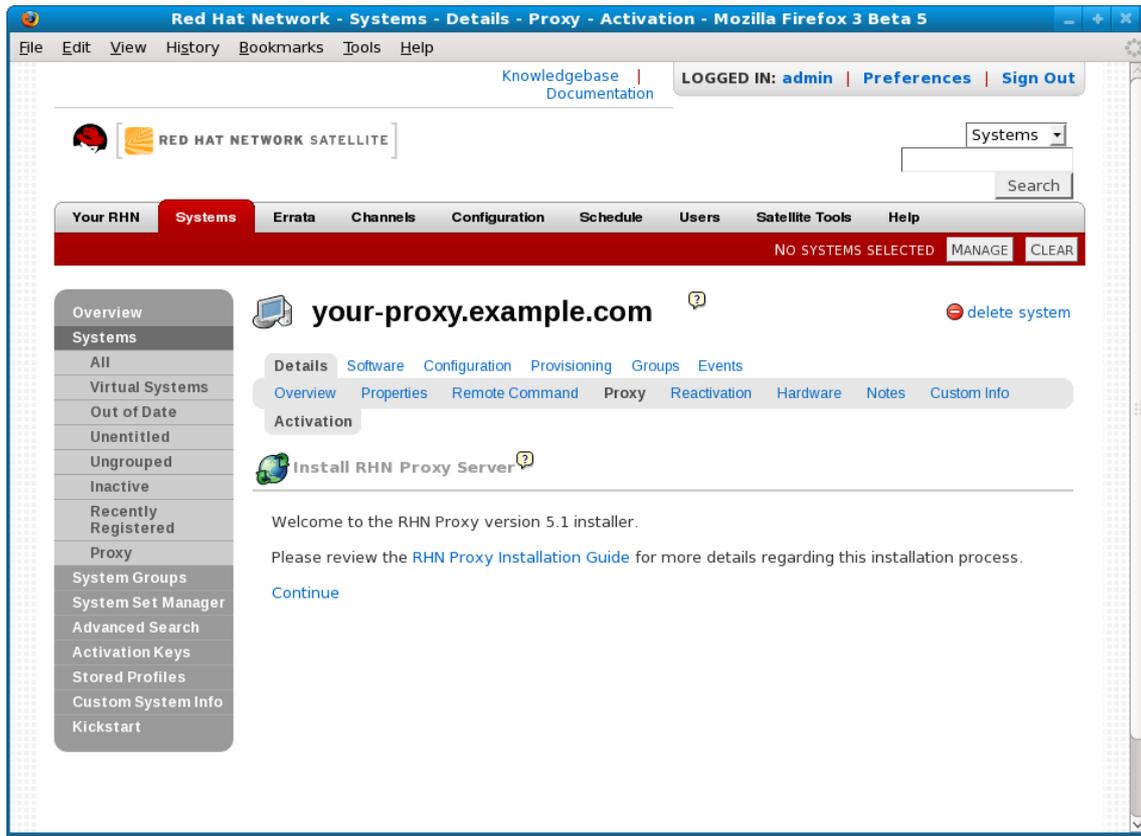
システムの登録が完了したら、**Proxy** タブを表示させるにはこのシステムをデフォルトの RHEL ベースチャンネルに登録する必要があります。システムをカスタムのチャンネルやクローン作成したチャンネルに登録している場合、プロキシタブは表示されません。

また、RHN Proxy Server のインストールにより今後のアップグレードを容易にするためシステム上の設定ファイル `squid.conf` と `httpd.conf` が置き換えられることがあります。これらのファイルが編集済みであり内容を保持したい場合、ファイルはローテーションされるのでインストール後に取得できます。



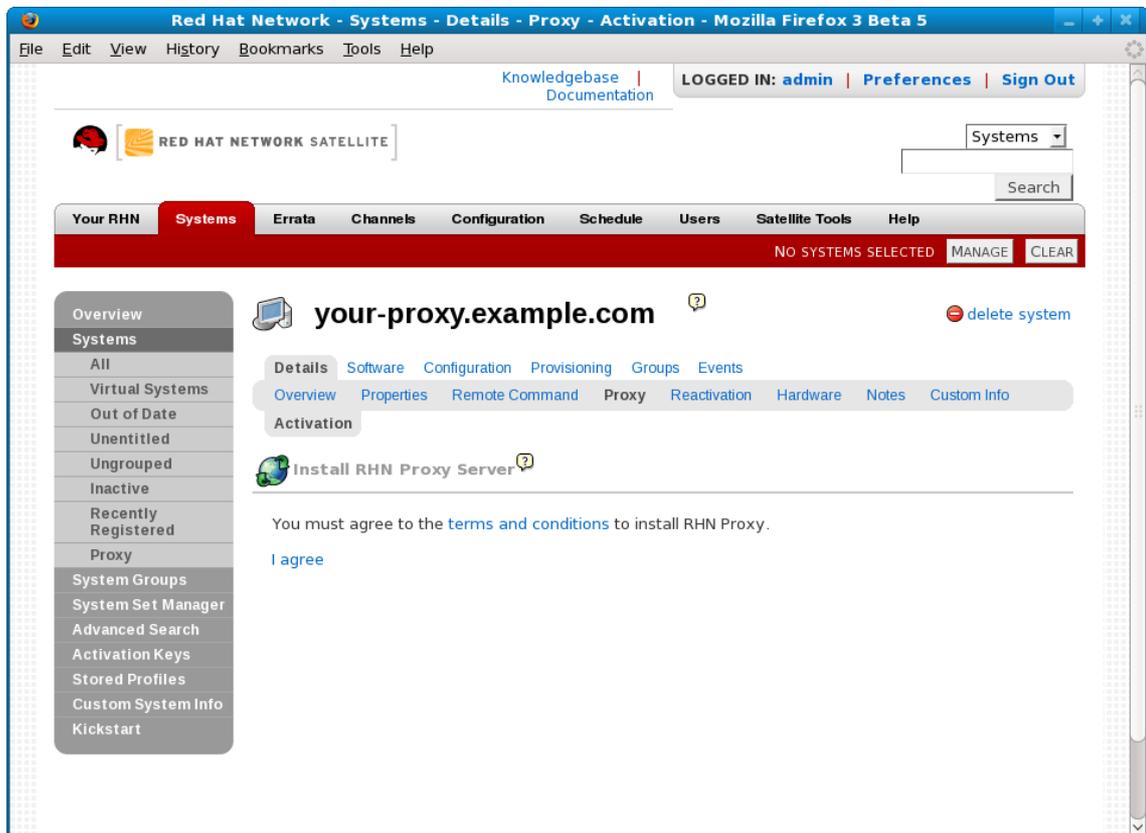
図A.1 システムの詳細 (System Details) => プロキシ (Proxy)

9. システムの詳細 => 詳細 => プロキシ サブタブ内にあるプルダウンメニューはシステムを RHN Proxy Server として有効化できるかどうかを示しているはずです。正しいバージョンが選択されていることを確認し、**プロキシの有効化 (Activate Proxy)** ボタンをクリックします。インストールのようこそ (**Welcome**) ページが表示されます。



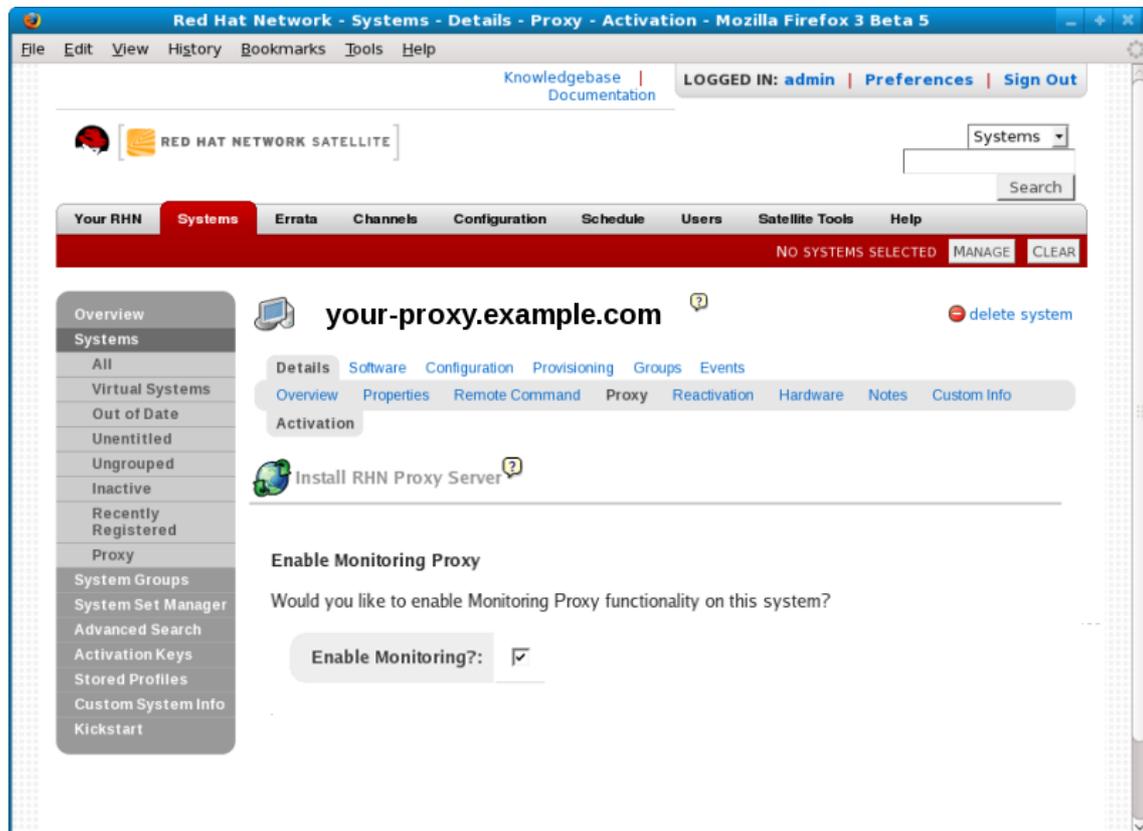
図A.2 ようこそ

10. ようこそ (**Welcome**) ページにはシステムで満たされていない要件が表示されます。システムの準備が整うと **続行** リンクが表示されます。このリンクをクリックすると**使用に関する条件** ページに移動します。



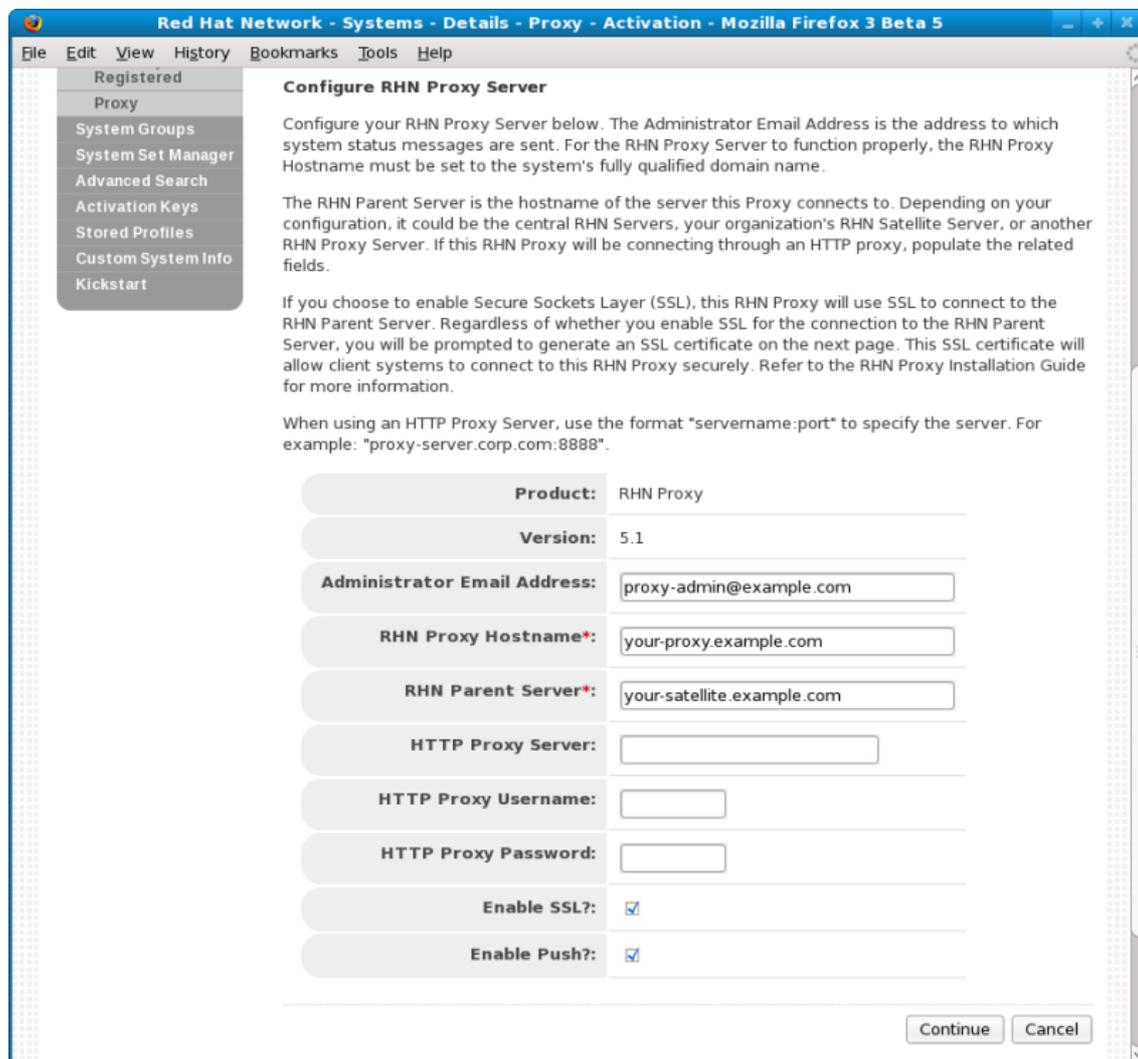
図A.3 使用条件

11. **使用に関する条件** ページで**使用に関する条件** リンクをクリックし、RHN Proxy Server の使用許諾契約書を参照します。同意する場合は**同意 (I agree)** リンクをクリックします。インストールを続行する場合は同意が必要になります。Proxy が Satellite に登録され監視機能が有効になっている場合は、**Monitoring を有効にする** のページが表示されます。



図A.4 監視の有効化

12. **Monitoring** を有効にする ページで Proxy が提供しているシステムの監視をその Proxy を使用して行うかどうかを決定する必要があります。これを行うには RHN Proxy Server が [2章要件](#) で指定された要件を満たし、RHN Satellite Server (または Satellite に接続している別の Proxy) に接続している必要があります。Proxy で監視を有効にする場合は、そのチェックボックスを選択して **続行** をクリックします。RHN Proxy Server の設定 (**Configure RHN Proxy Server**) ページが表示されます。



図A.5 RHN Proxy Server の設定

13. **RHN Proxy Server の設定 (Configure RHN Proxy Server)** ページで必須となるフィールドはすべて入力します。管理者の電子メールアドレスには **Proxy** によって生成されるすべてのメール (場合によっては大量のエラー関連のトレースバックを含む) が届きます。こうしたエラー関連のトレースバックなどの受信については、件名が「**RHN TRACEBACK from hostname**」のメッセージをキャプチャするメールフィルタなどを作成して対処することができます。複数の管理者を指定する場合は、電子メールアドレスをコンマで区切って入力します。

RHN Proxy Hostname は RHN Proxy Server の完全修飾ドメイン名 (FQDN) です。RHN Parent Server は Proxy にサービスを提供するサーバーのドメイン名です。中央 RHN サーバー、別の RHN Proxy Server、または RHN Satellite Server のいずれかになります。中央 RHN サーバーに接続する場合は `xmlrpc.rhn.redhat.com` の値を含めます。Satellite または別の Proxy に接続する場合は親となるシステムの FQDN を入力します。

HTTP プロキシ経由で RHN Proxy Server を接続する場合は、関連するフィールドを使用して設定を行います。HTTP Proxy Server フィールドに `http://` や `https://` などのプロトコルを含めないようにしてください。 `your-gateway.example.com:3128` などのように `hostname:port` の形式でホスト名とポートのみを入力します。



注記

インストールプロセスで変更されるのは Proxy 設定ファイルの `/etc/rhn/rhn.conf` のみです。Red Hat Update Agent (`up2date`) の設定ファイルとなる `/etc/sysconfig/rhn/up2date` については、RHN Satellite Server などの別のサーバーからのアップデートを受信できるよう手動で更新する必要があります。

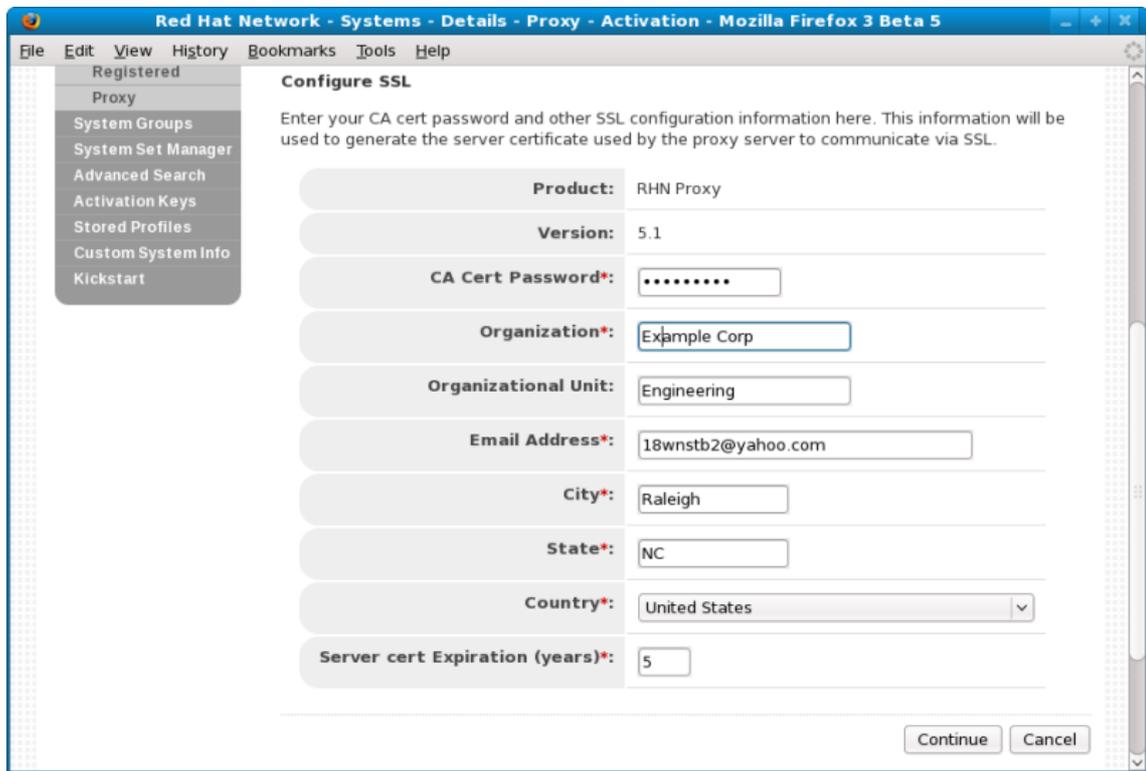
最後に最下部のチェックボックスをチェックして SSL を有効化するかどうかを決定する必要があります。Red Hat は RHN Proxy Server を経由するすべてのトラフィックに対してこのレベルの暗号化を導入することを強く推奨します。ただし、この場合は RHN サーバー (デフォルトで SSL が有効化された) または SSL を有効化した RHN Satellite Server や RHN Proxy Server に接続する必要があります。中央 RHN サーバーへの接続には、前述した証明書 tar ファイルのアップロードが必要です。SSL を使用して Satellite または別の Proxy に接続するには、親システムで SSL を有効化するときを使用した CA 証明書のパスワードが必要です。



注記

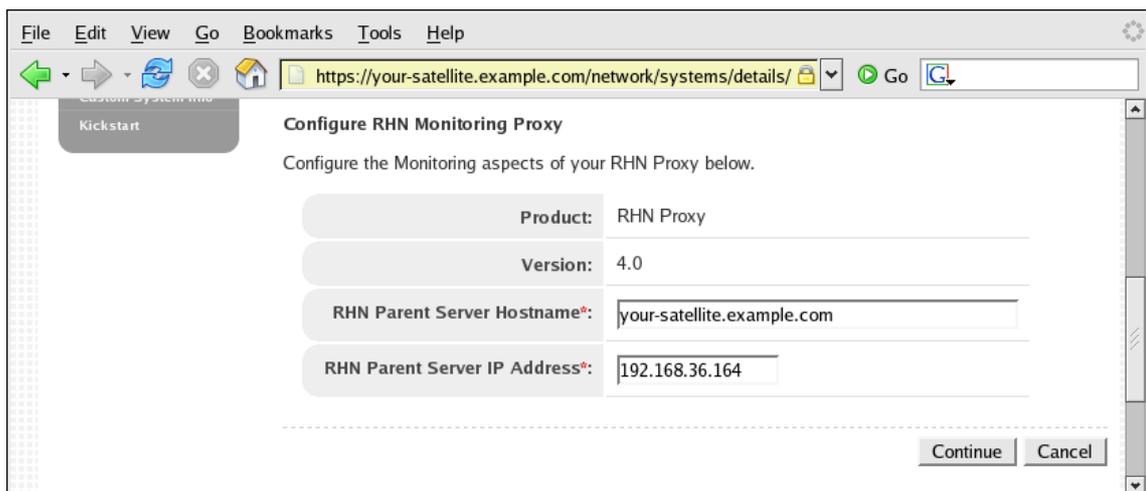
SSL を使用して安全な RHN Proxy Server インフラストラクチャを構成する方法については、『Red Hat Network クライアント設定ガイド』の「SSL インフラストラクチャ」の章を参照してください。

インストール時に SSL を有効にしない場合はこのチェックボックスを未選択のままにしておきます。インストール後にこのレベルのセキュリティを取得する方法について『RHN クライアント設定ガイド』の SSL 証明書の章を参照しておいてください。完了したら**続行**をクリックします。SSL を有効にする選択をして Satellite に接続すると、**SSL の設定 (Configure SSL)** ページが表示されます。SSL を有効にする選択をして別の Proxy または中央 RHN サーバーに接続すると、**SSL のアップロード (Upload SSL)** ページが表示されます。SSL は有効にせず Monitoring を有効にしている場合は、**Monitoring の設定 (Configure Monitoring)** ページの説明に移動します。SSL または Monitoring を有効にしていない場合は、インストールの**進捗状況 (Install Progress)** ページの説明に移動します。



図A.6 SSLの設定

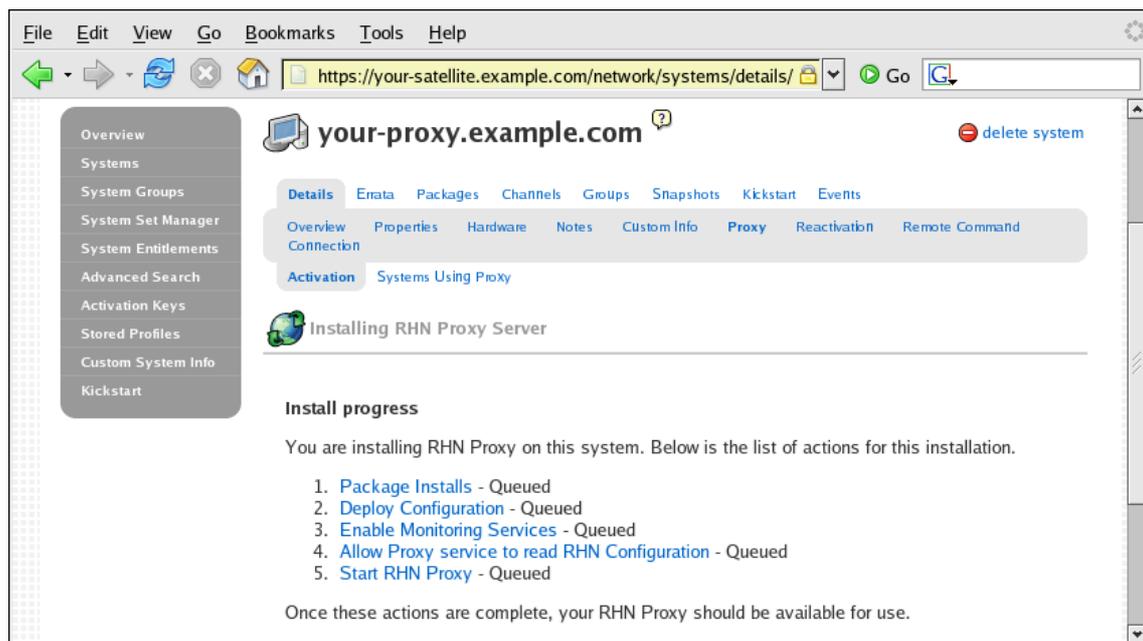
14. **SSL の設定 (Configure SSL)** ページで(有効にしている SSL で Proxy を RHN Satellite Server に接続する場合にのみ適用可)、サーバー証明書の生成に必要な情報を入力します。最も重要な項目は CA 証明書のパスワードです。親サーバーで SSL を有効化したときに使用したパスワードと一致していなければなりません。残りのフィールドは親サーバーの値と一致することもあります。地理的に異なる場所を反映させる場合など RHN Proxy Server の役割によって異なることもあります。同様に、Email アドレスは Proxy 管理者の Email アドレスとして入力したものと同じでも構いませんが、特定の証明書管理者に送信することもできます。証明書の期限を設定することができます。ここに入力した値は 2章要件で説明しているように必ずバックアップ情報内に存在するようにしてください。完了したら **続行** をクリックします。



図A.7 Monitoringの設定

15. **Monitoring の設定 (Configure Monitoring)** ページで RHN Proxy Server に接続させる親サーバーのホスト名と IP アドレスを入力するか、既に入力がある場合はそれを確認します。親サーバーは RHN Satellite Server または Satellite に接続する別の Proxy のいずれかでな

ければなりません。中央 RHN サーバーを経由した **Monitoring** は行えません。完了したら **続行** をクリックします。インストールの進捗状況 (**Install Progress**) ページが表示されます。



図A.8 インストールの進捗度

16. インストールの進捗状況 (**Install Progress**) ページでは、実行中のインストールのステップを監視することができます。ステップのリンクをクリックするとその **アクションの詳細** ページに移動します。動作が開始されると、状態が **キュー待ち** から **開始** に変わり最後に **完了** になります。前述のパッケージのインストールと同様、これらのステップはシステムのターミナルで `root` として `rhn_check` コマンドを実行すると直ちに実行させることができます。完了するとインストールの進捗状況 (**Install Progress**) ページに **インストールが完了しました (The installation is complete)** というメッセージが表示されます。これで RHN Proxy Server によってサービスが提供されるシステムの登録を開始することができるようになりました。『RHN クライアント設定ガイド』を参照してください。
17. インストールの進捗状況 (**Install Progress**) ページ上の項目がすべて **完了** になったら Proxy の使用準備が整ったこととなります。これでシステムを Proxy 経由で RHN に登録できるようになりました。

付録B RHN PROXY SERVER 設定ファイルの例

RHN Proxy Server の `/etc/rhn/rhn.conf` 設定ファイルではキーの設定を行う手段を提供しています。ただし、ファイル内に書き込みエラーがあるとプロキシに障害が発生する可能性がありますので注意してください。設定の変更を行う際は十分に注意してください。

RHN Satellite Server を併用している場合は、`traceback_mail` および `proxy.rhn_parent` などのパラメータに特に注意してください。詳細については設定ファイルの例とそのコメント (`#` マークが先頭に行っている行) をご覧ください。



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 が一時的にオフになります。これを行うと非常に危険な状態となります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、設定ファイルからその行自体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C 改訂履歴

改訂 1-3.400 Rebuild with publican 4.0.0	2013-10-31	Rüdiger Landmann
改訂 1-3 Rebuild for Publican 3.0	2012-07-18	Anthony Towns
改訂 1.0-0	Fri Jul 23 2010	

索引

シンボル

どのように動作するのか, [どのように動作するのか](#)

アウトバウンドのポート

[80, 443, 補足要件](#)

インストール

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

[Satellite の Web サイト](#), [Satellite の Web サイト](#) を利用した RHN Proxy Server のインストール
ベース, [ベースインストール](#)

インバウンドのポート、サテライト

[5222, 補足要件](#)

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へのサブスクリプトパッケージをアップロードする](#)

ソフトウェア要件, [ソフトウェア要件](#)

チャンネル, [知っておくべき用語](#)

[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を作成する](#)

チャンネル管理者, [知っておくべき用語](#)

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](#)

単一のプロキシ, [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, [知っておくべき用語](#)

ハードウェア要件, [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を作成する](#)

プロキシのポート, [補足要件](#)

ホストが見つかりません

[FQDN を確定できませんでした](#), [ホストが見つかりません / FQDN を確定できませんでした](#)

ポート

[443, 補足要件](#)

[5222, 補足要件](#)

[80, 補足要件](#)

ポート [443, 補足要件](#)

ポート 4545, [補足要件](#)

ポート 80, [補足要件](#)

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](#)

接続エラー, [接続エラー](#)

知っておくべき用語, [知っておくべき用語](#)

補足要件, [補足要件](#)

要件, [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](#)

補足, [補足要件](#)

認証, [どのように動作するのか](#)

認証のキャッシング

消去する, [キャッシュ関連の問題](#)

質問と答え, [質問とその答え](#)

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](#)

O

Organization Administrator, [知っておくべき用語](#)

R

Red Hat Network

はじめに, [Red Hat Network](#)

Red Hat Update Agent, [知っておくべき用語](#), [どのように動作するのか](#)

RHN Authentication Daemon, [無効にする](#)

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

RHN Package Manager, [どのように動作するのか](#), [RHN Package Manager](#)

インストールする, [RHN Package Manager](#)

コマンドラインオプション, [コマンドラインオプション](#)

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を作成する](#)

ローカルのパッケージ一覧を確認, [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を作成する](#)

設定ファイル, [RHN Package Manager](#)

rhn-proxy

サービス, [プロキシサービスの保守](#)

rhn.conf

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

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 のキャッシュ, [キャッシュ関連の問題](#)