IBM PowerSC
Standard Edition

バージョン 1.1.3

PowerSC Standard Edition

IBM PowerSC
Standard Edition

バージョン 1.1.3

PowerSC Standard Edition

お願い

本書および本書で紹介する製品をご使用になる前に、 51 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM PowerSC バージョン 1.1.3、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： IBM PowerSC
Standard Edition
Version 1.1.3
PowerSC Standard Edition

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

第1刷 2013.10

目次

本書について

本書は、ファイル、システム、およびネットワーク・セキュリティーに関する詳細な情報をシステム管理者に提供します。

強調表示

本書では、以下の強調表示規則を使用します。

太字	コマンド、サブルーチン、キーワード、ファイル、構造体、ディレクトリー、およびシステムによって名前が事前に定義されているその他の項目を示します。また、ユーザーが選択するボタン、ラベル、およびアイコンなどのグラフィカル・オブジェクトも示します。
イタリック	実際の名前または値をユーザーが指定する必要があるパラメーターを示します。
モノスペース	特定のデータ値の例、画面に表示されるものと同様のテキスト例、プログラマーが作成するものと同様のプログラム・コード部分の例、システムからのメッセージ、実際に入力する必要がある情報などを示します。

AIX® でのケース・センシティブ

AIX オペレーティング・システムでは、すべてケース・センシティブとなっています。これは、英大文字と小文字を区別するということです。例えば、**ls** コマンドを使用するとファイルをリスト表示できます。`LS` と入力すると、システムはそのコマンドが「`not found` (見つからない)」と応答します。同様に、`FILEA`、`FiLea`、および `filea` は、同じディレクトリーにある場合でも、3 つの異なるファイル名です。 予期しない処理が実行されないように、常に正しい大/小文字を使用するようにしてください。

ISO 9000

当製品の開発および製造には、ISO 9000 登録品質システムが使用されました。

IBM PowerSC Standard Edition 1.1.3

IBM® PowerSC™ Standard Edition には、トラステッド・ブート、トラステッド・ファイアウォール、トラステッド・ロギング、トラステッド・ネットワーク接続およびパッチ管理、ならびにセキュリティーおよびコンプライアンス自動化のフィーチャーが含まれています。

PowerSC Standard Edition 1.1.3 での新着情報

PowerSC Standard Edition バージョン 1.1.3 のトピック集の新規情報または大幅に変更された情報について説明します。

この PDF ファイルでは、新規情報および変更情報の左端にリビジョン・バー (|) が付いている場合があります。

2013 年 12 月

- 2 ページの『PowerSC Standard Edition 1.1.3 の概念』のシステム要件を更新。
- 5 ページの『トラステッド・ブートの前提条件』で、AIX オペレーティング・システムの再インストール時に置換が必要なトラステッド・ブート・ファイルを特定。
- 14 ページの『トラステッド・ファイアウォール・モニター』に、トラステッド・ファイアウォール・モニター機能に関する情報を追加。
- 15 ページの『トラステッド・ファイアウォール・ロギング』に、トラステッド・ファイアウォール・ロギング機能に関する情報を追加。
- トピック 21 ページの『トラステッド・ロギングのインストール』を追加。
- 27 ページの『パッチ管理サーバーの構成』に、トラステッド・ネットワーク接続のための暫定修正更新に関する情報を追加。
- 33 ページの『TNC サーバーのレポート作成』に、トラステッド・ネットワーク接続のサーバー・レポートに関する情報を追加。
- 7 ページの『ベリファイヤーのインストール』に、トラステッド・ネットワーク接続のベリファイヤーのインストールに関する情報を追加。
- 35 ページの『PowerSC Standard Edition コマンド入力』に、トラステッド・ファイアウォールのコマンドを追加。
- **tscpmconsole** コマンドを **pmconf** コマンドに名前変更し、その情報を 39 ページの『pmconf コマンド』に追加。
- **tscconsole** コマンドを **psconf** コマンドに名前変更し、その情報を 43 ページの『psconf コマンド』に追加。
- 49 ページの『vlantfw コマンド』の、**vlantfw** コマンドのオプションに関する情報を更新。

2012 年 11 月

23 ページの『トラステッド・ネットワーク接続およびパッチ管理』トピックの情報を更新。

2012 年 5 月

11 ページの『トラステッド・ファイアウォール』に新しいフィーチャーの資料を追加。

PowerSC Standard Edition 1.1.3 の概念

この PowerSC Standard Edition の概要では、フィーチャー、コンポーネント、および PowerSC Standard Edition フィーチャーに関連するハードウェア・サポートについて説明します。

PowerSC Standard Edition は、クラウドまたは仮想化データ・センターで稼働するシステムの強力なセキュリティーと制御を実現し、エンタープライズ・ビューと管理機能を提供します。PowerSC Standard Edition は、セキュリティーおよびコンプライアンス自動化、トラステッド・ブート、トラステッド・ファイアウォール、トラステッド・ロギング、トラステッド・ネットワーク接続およびパッチ管理を含むフィーチャー・スイートです。仮想化層に採用されているセキュリティー・テクノロジーは、スタンドアロン・システムのセキュリティーを強化します。

次の表に、エディション、エディションに含まれるフィーチャー、コンポーネント、および各コンポーネントを使用できるプロセッサー・ベース・ハードウェアに関する詳細を示します。

表 1. PowerSC Standard Edition のコンポーネント、説明、オペレーティング・システム・サポート、およびハードウェア・サポート

コンポーネント	説明	サポートされるオペレーティング・システム	サポートされるハードウェア
セキュリティーおよびコンプライアンス自動化	以下の規格について、セキュリティーおよびコンプライアンス構成の設定、モニター、および監査を自動化します。 • Payment Card Industry Data Security Standard (PCI DSS) • Sarbanes-Oxley 法令および COBIT への準拠 (SOX/COBIT) • U.S. 米国国防総省 (DoD) STIG • 医療保険の積算と責任に関する法律 (HIPAA) (Health Insurance Portability and Accountability Act (HIPAA))	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6® • POWER7®
トラステッド・ブート	ブート・イメージ、オペレーティング・システム、およびアプリケーションを計測し、仮想トラステッド・プラットフォーム・モジュール (TPM) テクノロジーを使用してそれらの信頼性を認証します。	• AIX 6 (6100-07 適用) 以降 • AIX 7 (7100-01 適用) 以降	POWER7 ファームウェア eFW7.4 以降
トラステッド・ファイアウォール	同じ 仮想 I/O サーバー が制御する指定された仮想 LAN (VLAN) の間で直接ルーティングを使用可能にすることで、時間とリソースを節約します。	• AIX 6.1 • AIX 7.1 • VIOS バージョン 2.2.1.4 以降	• POWER6 • POWER7 • 仮想 I/O サーバー バージョン 6.1S 以降
トラステッド・ロギング	AIX のログは、リアルタイムで仮想入出力サーバー (VIOS) に集中的に配置されます。このフィーチャーは、改ざん防止機能を備えたロギングと、便利なログ・バックアップおよび管理を提供します。	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6 • POWER7

表 1. PowerSC Standard Edition のコンポーネント、説明、オペレーティング・システム・サポート、およびハードウェア・サポート (続き)

コンポーネント	説明	サポートされるオペレーティング・システム	サポートされるハードウェア
トラステッド・ネットワーク接続およびパッチ管理	仮想環境のすべての AIX システムが指定のソフトウェアおよびパッチ・レベルであることを検査して、すべての AIX システムが指定のソフトウェア・レベルであることを確認するための管理ツールを提供します。ダウン・レベルの仮想システムがネットワークに追加された場合や、システムに影響を与えるセキュリティー・パッチが発行された場合にアラートを提供します。	• AIX 5.3 • AIX 6.1 • AIX 7.1 トラステッド・ネットワーク接続クライアントには、次のいずれかのコンポーネントが必要です。 • AIX 6.1 (6100-06 適用) 以降 • パッチ管理のために、SUMA 環境に AIX バージョン 7.1 サービス更新管理アシスタント (SUMA) コンソール・システム	• POWER5 • POWER6 • POWER7

PowerSC Standard Edition 1.1.3 のインストール

PowerSC Standard Edition の特定の機能ごとに、ファイルセットを 1 つインストールする必要があります。

PowerSC Standard Edition では以下のファイルセットを使用できます。

- `powerscExp.ice`: PowerSC Standard Edition のセキュリティーおよびコンプライアンスの自動化フィーチャーを必要とする AIX システムにインストールされます。
- `powerscStd.vtpm`: PowerSC Standard Edition のトラステッド・ブート・フィーチャーを必要とする AIX システムにインストールされます。
- `powerscStd.vlog`: PowerSC Standard Edition のトラステッド・ロギング・フィーチャーを必要とする AIX システムにインストールされます。
- `powerscStd.tnc_pm`: AIX バージョン 6.1 (6100-06 テクノロジー・レベル適用) またはそれ以上のバージョン、あるいは SUMA 環境の AIX バージョン 7.1 サービス更新管理アシスタント (SUMA) コンソール・システムにパッチ管理のためにインストールされます。
- `powerscStd.svm`: PowerSC Standard Edition のルーティング・フィーチャーから利益を得る可能性がある AIX システムにインストールされます。

以下のいずれかのインターフェースを使用して、PowerSC Standard Edition をインストールします。

- コマンド行インターフェース (CLI) の **installp** コマンド
- SMIT インターフェース

SMIT インターフェースを使用して PowerSC Standard Edition をインストールするには、以下のステップを実行します。

1. 次のコマンドを実行する。

   ```
   % smitty installp
   ```

2. 「**ソフトウェアのインストール**」オプションを選択します。

3. ソフトウェアの入力デバイスまたはディレクトリーを選択して、IBM Compliance Expert インストール・イメージの場所とインストール・ファイルを指定します。例えば、インストール・イメージのディレクトリー・パスとファイル名が /usr/sys/inst.images/powerscStd.vtpm である場合は、「**入力**」フィールドにファイル・パスを指定する必要があります。
4. ご使用条件を表示し、受け入れます。下矢印を使用して「**新規ご使用条件に同意する**」を選択し、Tab キーを押して値を「**はい**」に変更し、ご使用条件を受け入れます。
5. **Enter** キーを押して、インストールを開始します。
6. インストールの完了後、コマンド状況が「**OK**」であることを確認します。

ソフトウェア・ライセンスの表示

ソフトウェア・ライセンスは、CLI で次のコマンドを使用して表示できます。

```
% installp -lE -d path/filename
```

ここで、*path/filename* は、PowerSC Standard Edition インストール・イメージを指定します。

例えば、PowerSC Standard Edition に関連するライセンス情報を指定するために、CLI をして以下のコマンドを入力することができます。

```
% installp -lE -d  /usr/sys/inst.images/powerscStd.vtpm
```

関連概念:

2 ページの『PowerSC Standard Edition 1.1.3 の概念』
この PowerSC Standard Edition の概要では、フィーチャー、コンポーネント、および PowerSC Standard Edition フィーチャーに関連するハードウェア・サポートについて説明します。

7 ページの『トラステッド・ブートのインストール』
トラステッド・ブートをインストールするには、ハードウェアおよびソフトウェアの構成がいくつか必要です。

25 ページの『トラステッド・ネットワーク接続のインストール』
トラステッド・ネットワーク接続 (TNC) のコンポーネントをインストールするには、特定のステップを実行する必要があります。

関連タスク:

13 ページの『トラステッド・ファイアウォールのインストール』
PowerSC トラステッド・ファイアウォールのインストールは、他の PowerSC フィーチャーのインストールと同様です。

21 ページの『トラステッド・ロギングのインストール』
コマンド・ライン・インターフェースまたは SMIT ツールを使用して、PowerSC トラステッド・ロギング・フィーチャーをインストールすることができます。

トラステッド・ブート

トラステッド・ブート・フィーチャーは、Trusted Computing Group の TPM の仮想インスタンスである仮想トラステッド・プラットフォーム・モジュール (VTPM) を使用します。 VTPM は、システム・ブートの計測値を将来の検証のために安全に保管する目的で使用されます。

トラステッド・ブートの概念

ブート・プロセスの保全性、およびブートをトラステッド・ブートまたは非トラステッド・ブートとして分類する方法を理解することは、重要です。

ハードウェア管理コンソール (HMC) を使用して、物理システムごとに最大 60 の VTPM 対応ロジカル・パーティション (LPAR) を構成できます。構成された VTPM は、LPAR ごとに固有のものになります。VTPM は、AIX トラステッド実行テクノロジーと一緒に使用されると、以下のパーティションに対してセキュリティーと保証を提供します。

- ディスク上のブート・イメージ
- オペレーティング・システム全体
- アプリケーション層

管理者は、AIX 拡張パックで入手可能な **openpts** ベリファイヤーと一緒にインストールされる中央コンソールから、トラステッド・システムと非トラステッド・システムを表示できます。**openpts** コンソールは、1 台以上の Power Systems™ サーバーを管理して、データ・センター内の AIX システムのトラステッド状態をモニターまたは認証します。認証は、コレクターがトラステッド・ブートを実行したかどうかをベリファイヤーが判別 (または認証) するプロセスです。

トラステッド・ブート状況

コレクターの保全性をベリファイヤーが正常に認証した場合、パーティションはトラステッドであると言えます。ベリファイヤーは、コレクターがトラステッド・ブートを実行したかどうかを判別するリモート・パーティションです。コレクターは、仮想トラステッド・プラットフォーム・モジュール (VTPM) が接続され、Trusted Software Stack (TSS) がインストールされた AIX のパーティションです。これは、VTPM 内で記録された計測値がベリファイヤーによって保持されている参照セットと一致することを示しています。トラステッド・ブート状態は、パーティションが信頼できる方法でブートされたかどうかを示します。この記述は、システムのブート・プロセスの保全性に関するものであり、システムの現在または持続的なセキュリティー・レベルを示すものではありません。

非トラステッド・ブート状況

ベリファイヤーがブート・プロセスの保全性を正常に認証できない場合、パーティションは非トラステッド状態になります。非トラステッド状態は、ブート・プロセスの何らかの側面がベリファイヤーによって保持されている参照情報と矛盾していることを示します。認証の失敗の考えられる原因として、別のブート・デバイスからのブート、別のカーネル・イメージのブート、および既存のブート・イメージの変更が挙げられます。

関連概念:

9 ページの『トラステッド・ブートのトラブルシューティング』
トラステッド・ブートの使用時における認証失敗の理由を特定するには、一般的なシナリオと修復手順がいくつか必要です。

トラステッド・ブートの計画

トラステッド・ブートをインストールするために必要なハードウェアおよびソフトウェアの構成について説明します。

トラステッド・ブートの前提条件

トラステッド・ブートをインストールするには、コレクターとベリファイヤーを構成する必要があります。

| トラステッド・ブートをインストール済みのシステムに AIX オペレーティング・システムを再インストー
| ルする際は、事前に `/var/tss/lib/tpm/system.data` ファイルをコピーし、再インストールの完了後にその

| ファイルで同じ場所にあるファイルを上書きする必要があります。このファイルをコピーしない場合は、管
| 理コンソールから仮想トラステッド・プラットフォーム・モジュールを取り外して、パーティションに再イ
| ンストールする必要があります。

コレクター

コレクターをインストールするための構成要件には、以下の前提条件が含まれます。

- POWER7 ハードウェアが 740 ファームウェア・リリースで稼働している。
- IBM AIX 6 (テクノロジー・レベル 7 適用) または IBM AIX 7 (テクノロジー・レベル 1 適用) をインストールする。
- ハードウェア管理コンソール (HMC) バージョン 7.4 以降をインストールする。
- VTPM と最小 1 GB のメモリーを使用してパーティションを構成する。
- セキュア・シェル (SSH)、特に OpenSSH またはこれと同等のものをインストールする。

ベリファイヤー

openpts ベリファイヤーには、コマンド行インターフェース、および幅広いプラットフォームで実行されるように設計されたグラフィカル・ユーザー・インターフェースからアクセスできます。OpenPTS ベリファイヤーの AIX バージョンは、AIX 拡張パックで入手できます。Linux およびその他のプラットフォーム向けの OpenPTS ベリファイヤーのバージョンは、Web ダウンロードで入手できます。構成要件には、以下の前提条件が含まれます。

- SSH、特に OpenSSH またはこれと同等のものをインストールする。
- コレクターへのネットワーク接続を (SSH を介して) 確立する。
- グラフィカル・インターフェースから **openpts** コンソールにアクセスするために Java™ 1.6 以降をインストールする。

修復の準備

ここで説明するトラステッド・ブートに関する情報は、修正が必要な場合があるシチュエーションを識別するためのガイドとして役立ちます。ブート・プロセスに影響はありません。

認証の失敗を引き起こす状況は数多くあり、発生する可能性がある状況を予測するのは困難です。状況に応じて適切なアクションを決定する必要があります。ただし、いくつかの重大なシナリオに備えて準備し、そのような問題に対処する上で役立つポリシーまたはワークフローを用意しておくことをお勧めします。修復とは、認証により、1 つ以上のコレクターがトラステッドでないことが報告される場合に実行する必要がある修正処置です。

例えば、ブート・イメージがベリファイヤーの参照と異なることが原因で、認証の失敗が起こった場合、以下の質問に対する回答を検討してください。

- 脅威が確かであることをどのようにして検証できますか?
- 計画的保守または AIX のアップグレードが行われたか、新しいハードウェアが最近取り付けられましたか?
- この情報にアクセスできる管理者に連絡できますか?
- システムが最後にトラステッド状態でブートされたのはいつですか?
- セキュリティー脅威が確かであると思われる場合、どのようなアクションを実行する必要がありますか? (監査ログの収集、ネットワークからのシステムの切断、システムの電源遮断、およびユーザーへのアラートなどが推奨されます。)
- チェックする必要のある、信用性に欠けるシステムが他にありますか?

関連概念:

9 ページの『トラステッド・ブートのトラブルシューティング』
トラステッド・ブートの使用時における認証失敗の理由を特定するには、一般的なシナリオと修復手順がいくつか必要です。

マイグレーションに関する考慮事項

仮想トラステッド・プラットフォーム・モジュール (VTPM) に対して使用可能にされたパーティションのマイグレーションを行う前に、以下の前提条件について考慮してください。

物理 TPM よりも VTPM の方が優れている点は、VTPM を保持しながらシステム間でパーティションを移動できることです。ロジカル・パーティションを安全にマイグレーションするために、ファームウェアは VTPM データを送信前に暗号化します。確実に安全なマイグレーションを行うには、マイグレーションの前に、以下のセキュリティー対策を実装する必要があります。

- マイグレーションを実行する 仮想 I/O サーバー (VIOS) 間で IPSEC を使用可能にします。
- マイグレーション後に VTPM データを暗号化解除できる管理対象システムを制御するために、ハードウェア管理コンソール (HMC) を使用してトラステッド・システムの鍵を設定します。データを正常にマイグレーションするには、マイグレーションの宛先システムにソース・システムと同じ鍵が必要です。

関連情報:

HMC の使用

VIOS のマイグレーション

トラステッド・ブートのインストール

トラステッド・ブートをインストールするには、ハードウェアおよびソフトウェアの構成がいくつか必要です。

関連情報:

3 ページの『PowerSC Standard Edition 1.1.3 のインストール』
PowerSC Standard Edition の特定の機能ごとに、ファイルセットを 1 つインストールする必要があります。

コレクターのインストール

AIX の基本 CD からファイルセットを使用してコレクターをインストールする必要があります。

コレクターをインストールするには、**smit** または **installp** コマンドを使用して、基本 CD にある `powerscStd.vtpm` および `openpts.collector` パッケージをインストールします。

ベリファイヤーのインストール

OpenPTS ベリファイヤー・コンポーネントは、AIX オペレーティング・システムおよびその他のプラットフォーム上で稼働します。

| ベリファイヤーの AIX バージョンは、AIX 拡張パックを使用してファイルセットからインストールできます。AIX オペレーティング・システムにベリファイヤーをインストールするには、**smit** または **installp** コマンドを使用して、AIX 拡張パックから `openpts.verifier` パッケージをインストールします。このインストールにより、ベリファイヤーのコマンド行とグラフィカル・インターフェースの両方のバージョンがインストールされます。

| その他のオペレーティング・システム用の OpenPTS ベリファイヤーは、Download Linux OpenPTS
| Verifier For Use With AIX Trusted Boot からダウンロードできます。

関連情報:

Download Linux OpenPTS Verifier For Use With AIX Trusted Boot

トラステッド・ブートの構成

システムを登録して、トラステッド・ブートでシステムを認証する手順について説明します。

システムの登録

システムをベリファイヤーに登録する手順について説明します。

システムの登録は、ベリファイヤーに一連の初期計測値を提供するプロセスであり、後続の認証要求の基礎となります。コマンド行からシステムを登録するには、ベリファイヤーから以下のコマンドを使用します。

```
openpts -i <hostname>
```

登録されたパーティションに関する情報は、$HOME/.openpts ディレクトリーに置かれます。新しい各パーティションは、登録プロセス中に固有 ID を割り当てられ、登録されたパーティションに関する情報は固有 ID に対応するディレクトリーに保管されます。

グラフィカル・インターフェースからシステムを登録するには、以下のステップを実行します。

1. **/opt/ibm/openpts_gui/openpts_GUI.sh** コマンドを使用してグラフィカル・インターフェースを起動します。
2. ナビゲーション・メニューから「**登録 (Enroll)**」を選択します。
3. システムのホスト名および SSH 資格情報を入力します。
4. 「**登録 (Enroll)**」をクリックします。

関連概念:

『システムの認証』
コマンド行およびグラフィカル・インターフェースを使用してシステムを認証する手順について説明します。

システムの認証

コマンド行およびグラフィカル・インターフェースを使用してシステムを認証する手順について説明します。

システム・ブートの保全性を照会するには、ベリファイヤーから次のコマンドを使用します。

```
openpts <hostname>
```

グラフィカル・インターフェースからシステムを認証するには、以下のステップを実行します。

1. ナビゲーション・メニューからカテゴリーを選択します。
2. 認証する 1 つ以上のシステムを選択します。
3. 「**認証 (Attest)**」をクリックします。

パスワードを使用しないシステムの登録と認証

認証要求は セキュア・シェル (SSH) を介して送信されます。パスワードを使用せずに SSH 接続を許可するには、ベリファイヤーの証明書をコレクターにインストールします。

ベリファイヤーの証明書をコレクターのシステムでセットアップするには、以下のステップを実行します。

- ベリファイヤーで、次のコマンドを実行します。

```
ssh-keygen    # No passphrase
scp ~/.ssh/id_rsa.pub <collector>:/tmp
```

- コレクターで、次のコマンドを実行します。

```
cat /tmp/id_rsa.pub >> ~/.ssh/authorized_keys
```

トラステッド・ブートの管理

トラステッド・ブートの認証結果を管理する手順について説明します。

認証結果の解釈

認証結果を表示して理解する手順について説明します。

認証の結果は、次のいずれかの状態になります。

1. 認証要求の失敗: 認証要求は正常に完了しませんでした。失敗の考えられる原因を理解するには、トラブルシューティングのセクションを参照してください。
2. システム保全性が有効: 認証が正常に完了して、システム・ブートがベリファイヤーによって保持されている参照情報と一致しています。これは、正常なトラステッド・ブートを示しています。
3. システム保全性が無効: 認証要求は完了しましたが、システム・ブート時に収集された情報とベリファイヤーによって保持されている参照情報との間に不一致が検出されました。これは、非トラステッド・ブートを示しています。

認証では、以下のメッセージが使用されて、コレクターに更新が適用されたかどうかも報告されます。

システム更新が使用可能: このメッセージは、更新がコレクターに適用され、次回のブートから有効になる一連の更新済み参照情報が使用可能であることを示しています。ベリファイヤーで更新を受け入れるか、拒否するかのプロンプトがユーザーに対して出されます。例えば、ユーザーは、コレクターで保守が行われていることを認識している場合に、これらの更新を受け入れることを選択できます。

グラフィカル・インターフェースを使用して認証の失敗を調査するには、以下のステップを実行します。

1. ナビゲーション・メニューからカテゴリーを選択します。
2. 調査するシステムを選択します。
3. システムに対応するエントリーをダブルクリックします。「プロパティー」ウィンドウが表示されます。このウィンドウには、失敗した認証に関するログ情報が含まれています。

システムの削除

ベリファイヤーのデータベースからシステムを削除する手順について説明します。

ベリファイヤーのデータベースからシステムを削除するには、次のコマンドを実行します。

```
openpts -r <hostname>
```

トラステッド・ブートのトラブルシューティング

トラステッド・ブートの使用時における認証失敗の理由を特定するには、一般的なシナリオと修復手順がいくつか必要です。

システムの現行のブート状態がベリファイヤーで保持されている参照情報と一致しない場合、**openpts** コマンドはシステムを無効として宣言します。**openpts** コマンドは、保全性が無効になった理由として考えられるものを判別します。完全な AIX のブートにはいくつかの変数があり、認証が失敗した場合は、失敗の原因を判別するために分析する必要があります。

次の表に、失敗の理由を特定するための一般的なシナリオと修復手順をリストします。

表 2. 一般的な失敗のシナリオのトラブルシューティング

失敗の理由	失敗の考えられる原因	推奨される修復手順

認証が完了しなかった。	• ホスト名が誤っています。
	• ソースと宛先の間にネットワーク経路がありません。
	• セキュリティー資格情報が誤っています。
		次のコマンドを使用して、セキュア・シェル (SSH) 接続を検査します。
		`ssh ptsc@hostname`
		SSH 接続が正常である場合は、認証失敗の以下の理由について確認します。
		• 認証対象のシステムが **tcsd** デーモンを実行していません。
		• 認証対象のシステムが、**ptsc** コマンドによって初期化されていません。このプロセスは、システム始動時に自動的に行われるはずですが、コレクター上に `/var/ptsc/` ディレクトリーが存在していることを確認してください。`/var/ptsc/` ディレクトリーが存在しない場合、コレクターで次のコマンドを実行します。
		`ptsc -i`

CEC ファームウェアが変更された。	• ファームウェア・アップグレードが適用されました。 • LPAR は、別のバージョンのファームウェアを実行していたシステムからマイグレーションされました。	LPAR をホスティングしているシステムのファームウェア・レベルを確認します。
LPAR に割り当てられているリソースが変更された。	LPAR に割り当てられている CPU またはメモリーが変更されました。	HMC のパーティション・プロファイルを確認します。
LPAR で使用可能なアダプターのファームウェアが変更された。	LPAR でハードウェア・デバイスの追加または取り外しが行われました。	HMC のパーティション・プロファイルを確認します。
LPAR に接続されているデバイスのリストが変更された。	LPAR でハードウェア・デバイスの追加または取り外しが行われました。	HMC のパーティション・プロファイルを確認します。
オペレーティング・システム・カーネルを含むブート・イメージが変更された。	• AIX の更新が適用されましたが、ベリファイヤーが更新を認識しませんでした。 • **bosboot** コマンドが実行されました。	• コレクターの管理者に、最後のリブート操作の前に保守作業が行われたかどうかを確認します。 • コレクターのログで、保守アクティビティーが行われたかどうかを確認します。
LPAR が別のデバイスからブートされた。	• ネットワーク・インストールの直後に登録が行われました。 • システムが保守デバイスからブートされました。	ブート・デバイスおよびフラグは、**bootinfo** コマンドを使用して検査できます。ネットワーク・インストール管理 (NIM) のインストールの直後、リブート操作が行われるまでの間に登録が実行された場合、登録された詳細はネットワーク・インストールに関連しており、次回のディスク・ブートには関連していません。登録を削除してロジカル・パーティションを再登録することにより、この登録を修復できます。

表 2. 一般的な失敗のシナリオのトラブルシューティング (続き)

失敗の理由	失敗の考えられる原因	推奨される修復手順
対話式のシステム管理サービス (SMS) ブート・メニューが呼び出された。		システムがトラステッドとなるためには、ユーザー対話なしに中断されることなくブート・プロセスが実行される必要があります。SMS ブート・メニューに入ると、ブートは無効になります。
トラステッド実行 (TE) データベースが変更された。	• TE データベースでバイナリー・ファイルが追加されたか、削除されました。 • データベース内のバイナリー・ファイルが更新されました。	**trustchk** コマンドを実行して、データベースを検査します。

関連概念:

6 ページの『修復の準備』
ここで説明するトラステッド・ブートに関する情報は、修正が必要な場合があるシチュエーションを識別するためのガイドとして役立ちます。ブート・プロセスに影響はありません。

4 ページの『トラステッド・ブートの概念』
ブート・プロセスの保全性、およびブートをトラステッド・ブートまたは非トラステッド・ブートとして分類する方法を理解することは、重要です。

関連情報:

HMC の使用

トラステッド・ファイアウォール

トラステッド・ファイアウォール・フィーチャーは、同一の Power Systems サーバー上の異なる仮想 LAN (VLAN) セキュリティー・ゾーン間で通信する際のパフォーマンスとリソース効率を向上する、仮想化層のセキュリティーを提供します。指定されたルールに合致するファイアウォール・パケットのフィルタリング機能を仮想化層に移動することにより、トラステッド・ファイアウォールによって外部ネットワークでの負荷が減少します。このフィルタリング機能は容易に定義できるネットワーク・フィルター・ルールによって処理されます。これにより、仮想環境のままで、トラステッド・ネットワーク・トラフィックが VLAN セキュリティー・ゾーン間を移動することが許可されます。トラステッド・ファイアウォールは、AIX、IBM i、および Linux オペレーティング・システムの間の内部ネットワーク・トラフィックを保護し、ルーティングします。

トラステッド・ファイアウォールの概念

トラステッド・ファイアウォールを使用する際には、基本的な概念をいくつか理解する必要があります。

Power Systems ハードウェアは、複数の仮想 LAN (VLAN) セキュリティー・ゾーンを使用して構成することができます。トラステッド・ファイアウォールのフィルター・ルールとして作成されたユーザー構成ポリシーによって、いくつかのトラステッド・ネットワーク・トラフィックが、複数の VLAN セキュリティー・ゾーン間を移動し、仮想化層の内部にとどまることが許可されます。これは、ネットワーク接続された物理的ファイアウォールを仮想化環境に導入するのと類似しており、ファイアウォール機能を実装するためのパフォーマンス効率が高い方式を、仮想化データ・センターに提供します。

トラステッド・ファイアウォールを使用すると、他のタイプのトラフィックを制限して高水準のセキュリティーを維持したまま、仮想 I/O サーバー (VIOS) 上のある VLAN から、同じ VIOS 上にある別の VLAN

に直接転送するための特定のタイプのトラフィックを許可するルールを構成することができます。これは、Power Systems サーバーの仮想化層内の構成可能なファイアウォールです。

図 1 の例では、情報をセキュアかつ効率的に VLAN 200 上の LPAR1 および VLAN 100 上の LPAR2 から転送できるようになることが目標です。トラステッド・ファイアウォールがない場合、LPAR1 から LPAR2 を宛先とした情報は内部ネットワークの外部のルーターに送信され、このルーターが情報を LPAR2 に経路指定します。

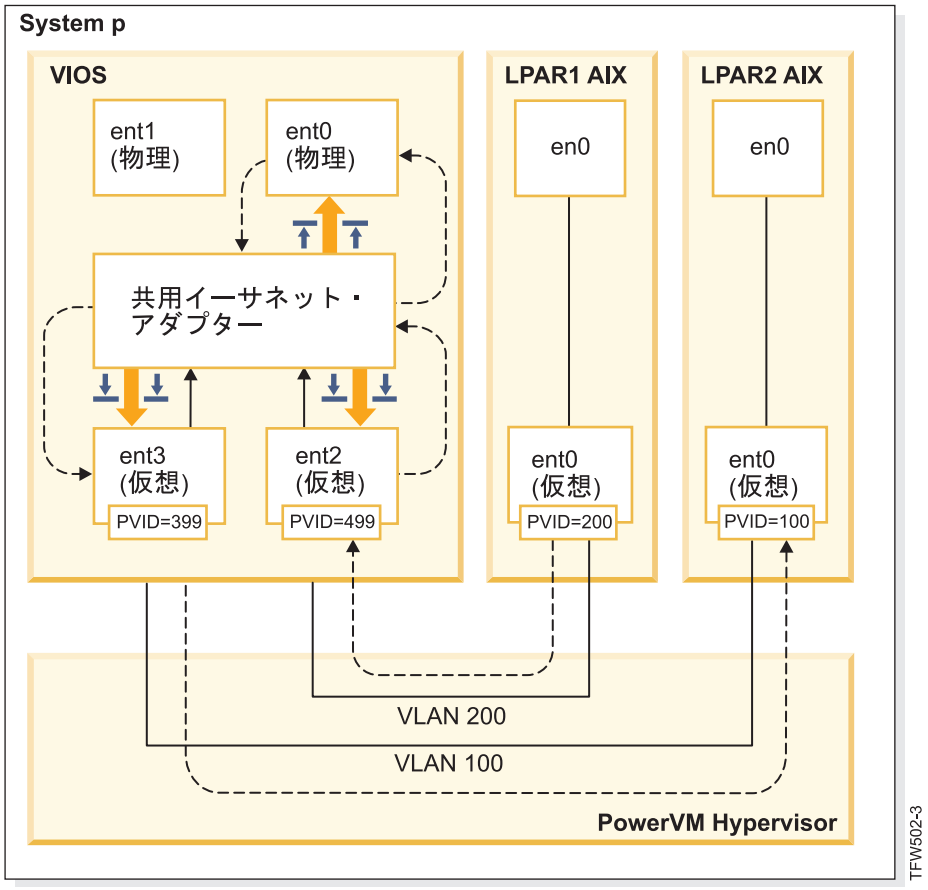

図 1. トラステッド・ファイアウォールを使用しない、VLAN 間の情報転送の例

トラステッド・ファイアウォールを使用して、情報が内部ネットワークの外部に出ずに LPAR1 から LPAR2 にパスされるのを許可するルールを構成することができます。このパスは、 13 ページの図 2 に示されています。

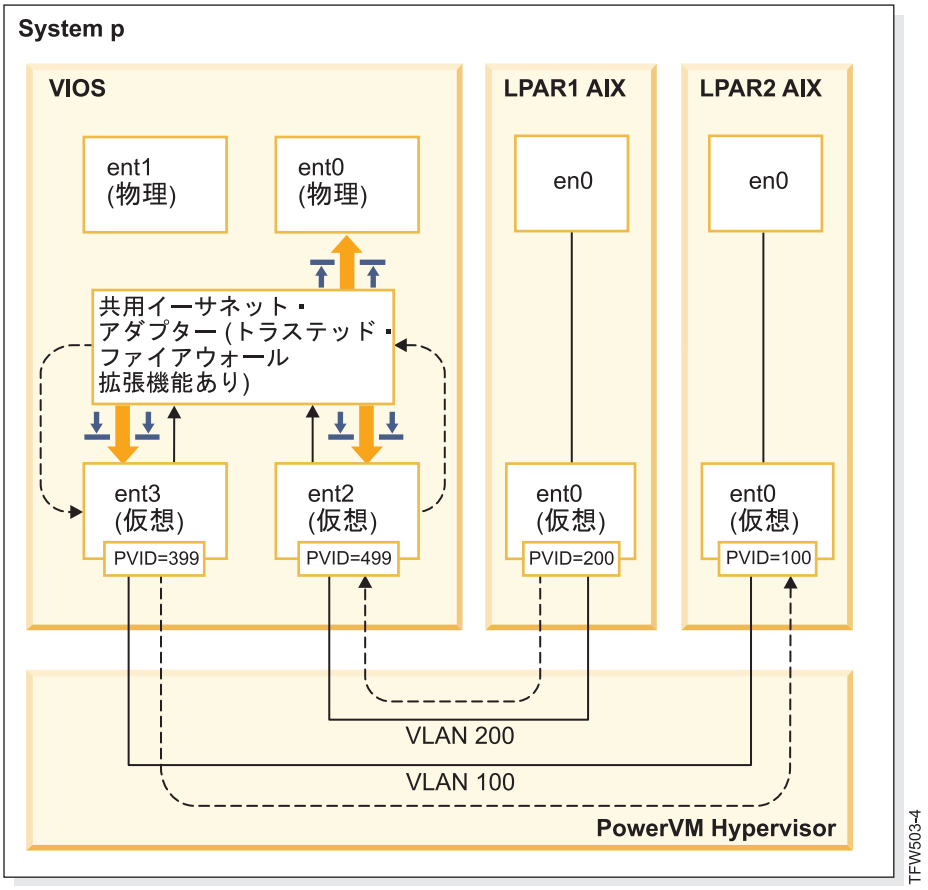

図 2. トラステッド・ファイアウォールを使用した、VLAN 間の情報転送の例

特定の情報が VLAN 間をセキュアにパスすることを許可する構成ルールによって、宛先へのパスが短くなります。トラステッド・ファイアウォールでは、共用イーサネット・アダプター (SEA) および Security Virtual Machine (SVM) カーネル・エクステンションを使用して、通信が可能になります。

共用イーサネット・アダプター

SEA は、経路指定の開始点および終着点です。SVM が登録されると、SEA はパケットを受け取り、それを SVM に転送します。パケットの宛先が同一の Power Systems サーバー上の LPAR であると SVM が判断した場合、SVM はパケットの層 2 のヘッダーを更新します。パケットは、システム内部または外部ネットワーク上の最終の宛先に転送するために、SEA に戻されます。

Security Virtual Machine

SVM は、フィルター・ルールの適用地点です。フィルター・ルールは、内部ネットワークのセキュリティーを維持するために必要です。 SVM を SEA に登録すると、パケットは外部ネットワークに送信される前に SVM に転送されます。パケットが内部ネットワークにとどまるか、または外部ネットワークに移動するかを、SVM がアクティブなフィルター・ルールに基づいて判別します。

トラステッド・ファイアウォールのインストール

PowerSC トラステッド・ファイアウォールのインストールは、他の PowerSC フィーチャーのインストールと同様です。

前提条件:

- 1.1.1.0 より前の PowerSC バージョンには、トラステッド・ファイアウォールをインストールするために必要なファイルセットがありませんでした。バージョン 1.1.1.0 以降の PowerSC インストール CD を必ず準備してください。
- トラステッド・ファイアウォールを利用するには、仮想 LAN (VLAN) を構成するためにハードウェア管理コンソール (HMC) または 仮想 I/O サーバー (VIOS) を既に使用したことがなければなりません。

トラステッド・ファイアウォールは、PowerSC Standard Edition のインストール CD で、追加のファイルセットとして提供されています。ファイル名は `powerscStd.svm.rte` です。トラステッド・ファイアウォールは、PowerSC バージョン 1.1.0.0 以降の既存のインスタンスに追加することも、PowerSC バージョン 1.1.1.0 以降の新規インストールの一環としてインストールすることも可能です。

トラステッド・ファイアウォール機能を既存の PowerSC インスタンスに追加するには、以下のようにします。

1. VIOS バージョン 2.2.1.4 以降を実行していることを確認します。
2. バージョン 1.1.1.0 の PowerSC インストール CD を挿入するか、インストール CD のイメージをダウンロードします。
3. ルート・アクセスに **oem_setup_env** コマンドを使用します。
4. **installp** コマンドまたは SMIT ツールを使用して、`PowerscStd.svm.rte` ファイルセットをインストールします。

関連情報:

3 ページの『PowerSC Standard Edition 1.1.3 のインストール』
PowerSC Standard Edition の特定の機能ごとに、ファイルセットを 1 つインストールする必要があります。

トラステッド・ファイアウォールの構成

トラステッド・ファイアウォール・フィーチャーをインストールしたら、追加の構成設定が必要です。

トラステッド・ファイアウォール・モニター

トラステッド・ファイアウォール・モニターは、さまざまなロジカル・パーティション (LPAR) からのシステム・トラフィックを分析し、トラステッド・ファイアウォールの実行により、システム・パフォーマンスが向上するかどうか判断するのに役立つ情報を提供します。

トラステッド・ファイアウォールのモニター機能が、同一の中央電子処理装置上のさまざまな仮想 LAN (VLAN) から大量のトラフィックを記録する場合は、トラステッド・ファイアウォールを使用可能化することが、ご使用のシステムにメリットをもたらします。

トラステッド・ファイアウォール・モニターを使用可能にするには、次のコマンドを入力します。

```
vlantfw -m
```

トラステッド・ファイアウォール・モニターの結果を表示するには、次のコマンドを入力します。

```
vlantfw -D
```

トラステッド・ファイアウォール・モニターを使用不可にするには、次のコマンドを入力します。

```
vlantfw -M
```

トラステッド・ファイアウォール・ロギング

トラステッド・ファイアウォール・ロギングは、中央電子処理装置内のネットワーク・トラフィック・パスのリストをコンパイルします。このリストは、トラステッド・ファイアウォールがトラフィックのルーティングに使用するフィルターを示します。

トラステッド・ファイアウォール・モニターが、トラフィックのルーティングにより内部的に効率性が改善されたと判断した場合、トラステッド・ファイアウォール・ロギングは `svm.log` ファイル内にパスのリストを保持します。`svm.log` ファイルのサイズの制限は 16 MB です。エントリーが 16 MB の制限を超えると、最も古いエントリーがログ・ファイルから削除されます。

トラステッド・ファイアウォール・ロギングを開始するには、以下のコマンドを入力します。

```
vlantfw -l
```

トラステッド・ファイアウォール・ロギングを停止するには、以下のコマンドを入力します。

```
vlantfw -L
```

このログ・ファイルの場所は、`/home/padmin/svm/svm.log` です。

複数の共用イーサネット・アダプター

複数の共用イーサネット・アダプターを使用するシステム上で、トラステッド・ファイアウォールを構成することができます。

一部の構成では、同一の 仮想 I/O サーバー (VIOS) 上で複数の共用イーサネット・アダプターが使用されます。複数の SEA によって、フェイルオーバー保護およびリソース平準化という利点が実現します。トラステッド・ファイアウォールは複数の SEA が同一の VIOS 上にある場合、複数の SEA 全体のルーティングをサポートします。

16 ページの図 3 では、複数の SEA を使用した環境を示します。

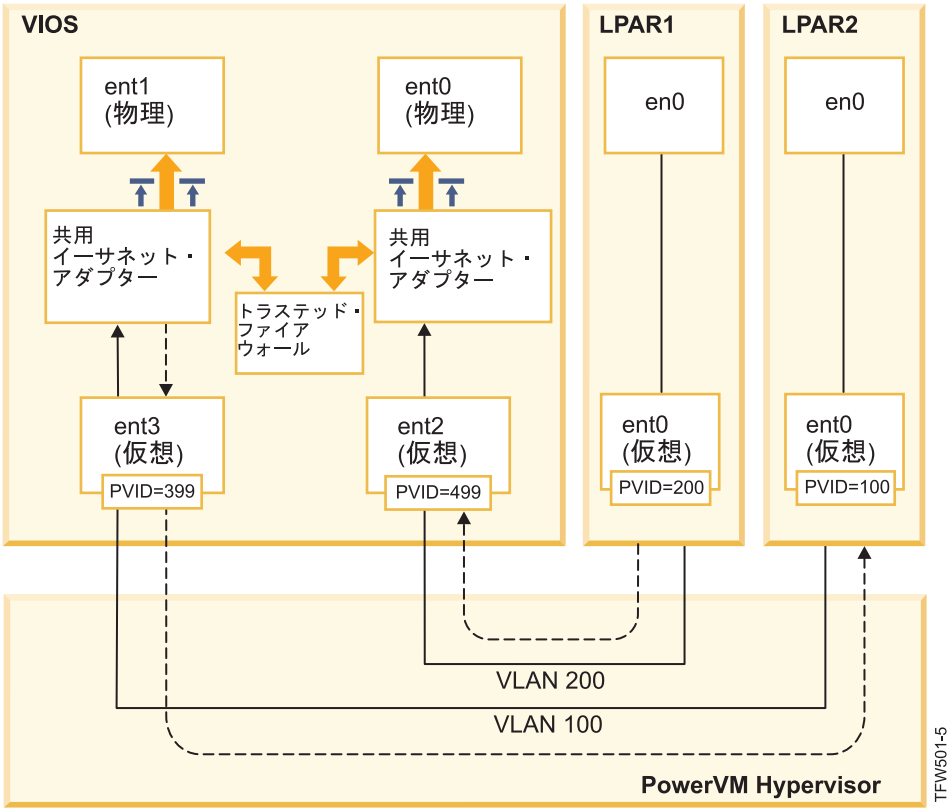

図 3. 単一の VIOS 上で複数の共用イーサネット・アダプターを使用する構成

トラステッド・ファイアウォールによってサポートされる複数の SEA 構成の例は、以下のとおりです。

- 同一の Power® ハイパーバイザー仮想スイッチ上で、トランク・アダプターを使用して SEA が構成される。この構成がサポートされるのは、各 SEA が異なる VLAN ID を使用してネットワーク・トラフィックを受信するためです。
- 複数の異なる Power ハイパーバイザー仮想スイッチ上で、トランク・アダプターを使用して SEA が構成され、各トランク・アダプターは異なる VLAN ID 上にある。この構成でも、各 SEA は異なる VLAN ID を使用してネットワーク・トラフィックを受信します。
- 複数の異なる Power ハイパーバイザー仮想スイッチ上で、トランク・アダプターを使用して SEA が構成され、この仮想スイッチ上では同一の VLAN ID が再利用される。この場合、両方の SEA に対するトラフィックでは同じ VLAN ID が使用されます。

  この構成の例としては、仮想スイッチ 10 の VLAN200 で LPAR2 が使用され、仮想スイッチ 20 の VLAN200 で LPAR3 が使用されます。両方の LPAR およびそれに対応する SEA では、同一の VLAN ID (VLAN200) が使用され、両方の SEA はその VLAN ID のパケットにアクセスすることができます。

複数の VIOS でブリッジングを使用可能にすることはできません。これが理由で、以下の複数の SEA の構成はトラステッド・ファイアウォールによってサポートされません。

- 複数の VIOS および複数の SEA ドライバー。
- 冗長 SEA ロード共有。VLAN 間のルーティング用に構成されたトランク・アダプターは、VIOS サーバーの間で分割することができません。

共用イーサネット・アダプターの除去

共用イーサネット・アダプター装置をシステムから除去する手順は、特定の順序で実行する必要があります。

ご使用のシステムから共用イーサネット・アダプターを除去するには、以下のステップを実行します。

1. 以下のコマンドを入力して、SEA に関連付けられている Security Virtual Machine を除去します。

   ```
   rmdev -dev svm
   ```

2. 以下のコマンドを入力して、SEA を除去します。

   ```
   rmdev -dev shared ethernet adapter ID
   ```

注: SVM を除去する前に SEA を除去すると、システム障害が発生する可能性があります。

ルールの作成

トラステッド・ファイアウォールの VLAN 間ルーティングを使用可能にするためのルールを作成することができます。

トラステッド・ファイアウォールのルーティング機能を使用可能にするために、許可される通信を指定するルールを作成する必要があります。セキュリティーを強化するために、システム上にあるすべての VLAN 間での通信を許可するという単一のルールはありません。アクティブ化された各ルールは、指定されたエンドポイントに対して双方向の通信を許可しますが、許可された接続にはそれぞれ独自のルールが必要です。

ルールの作成は 仮想 I/O サーバー (VIOS) インターフェースで行われるため、コマンドに関する追加情報は、Power Systems ハードウェア・インフォメーション・センターの VIOS トピックの集合で入手可能です。

ルールを作成するには、以下のステップを実行します。

1. VIOS コマンド行インターフェースを開きます。
2. 以下のコマンドを入力して、SVM ドライバーを開始します。

   ```
   mksvm
   ```

3. 以下の開始コマンドを入力して、トラステッド・ファイアウォールを開始します。

   ```
   vlantfw -s
   ```

4. 既知のすべての LPAR IP および MAC アドレスを表示するには、以下のコマンドを入力します。

   ```
   vlantfw -d
   ```

   作成するルールの対象となるロジカル・パーティション (LPAR) の IP アドレスと MAC アドレスが必要になります。

5. 以下のいずれかのコマンドを入力して、2 つの LPAR (LPAR1 および LPAR2) の間で通信を許可するフィルター・ルールを作成します。
   - `genvfilt -v4 -a P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress]`
   - `genvfilt -v4 -a P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress]-o any -p 0 -O gt -P 23`

   注: 一方のフィルター・ルールでは、ポートおよびプロトコルの入力に応じて、デフォルトで双方向の通信が許可されます。例えば、以下のコマンドを実行して、LPAR1 から LPAR2 の Telnet を使用可能にすることができます。

   ```
   genvfilt -v4 -a-P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress] -o
   any -p 0 -O eq -P 23
   ```

6. 以下のコマンドを入力して、カーネル内のすべてのフィルター・ルールをアクティブにします。

```
mkvfilt -u
```

注: この手順では、このルールおよびシステム内に存在する他のすべてのフィルター・ルールがアクティブにされます。

追加の例

以下の例では、トラステッド・ファイアウォールを使用して作成することができる他のフィルター・ルールを示しています。

- VLAN 100 上の LPAR から VLAN 200 上の LPAR へのセキュア・シェル通信を許可するには、以下のコマンドを入力します。

  ```
  genvfilt -v4 -a P -z 100 -Z 200 -o any -p 0 -O eq -P 22 -c tcp
  ```

- 0 から 499 のすべてのポート間でのトラフィックを許可するには、以下のコマンドを入力します。

  ```
  genvfilt -v4 -a P -z 100 -z 200 -o lt -p 500 -O lt -P 500 -c tcp
  ```

- LPAR 間でのすべての TCP トラフィックを許可するには、以下のコマンドを入力します。

  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c tcp
  ```

  ポート、またはポート操作を指定しない場合、トラフィックではすべてのポートが使用されます。

- LPAR 間での Internet Control Message Protocol メッセージングを許可するには、以下のコマンドを入力します。

  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c icmp
  ```

関連概念:

『ルールの非アクティブ化』
トラステッド・ファイアウォール・フィーチャーで、VLAN 間ルーティングを使用可能にするルールを非アクティブにすることができます。

関連資料:

36 ページの『genvfilt コマンド』
38 ページの『mkvfilt コマンド』
49 ページの『vlantfw コマンド』

関連情報:

仮想入出力サーバー (VIOS)

ルールの非アクティブ化

トラステッド・ファイアウォール・フィーチャーで、VLAN 間ルーティングを使用可能にするルールを非アクティブにすることができます。

ルールの非アクティブ化は 仮想 I/O サーバー (VIOS) インターフェースで行われるため、コマンドおよび処理に関する追加情報は、Power Systems ハードウェア・インフォメーション・センターの VIOS トピックの集合で入手可能です。

ルールを非アクティブにするには、以下のステップを実行します。

1. VIOS コマンド行インターフェースを開きます。
2. アクティブなすべてのフィルター・ルールを表示するには、以下のコマンドを入力します。

   ```
   lsvfilt -a
   ```

オブジェクト・データ・マネージャーに保管されているすべてのフィルター・ルールを表示する場合、**-a** フラグを省略することができます。

3. 非アクティブにするフィルター・ルールの識別番号をメモしてください。この例では、フィルター・ルールの識別番号は 23 です。
4. 以下のコマンドを入力して、フィルター・ルール 23 がカーネル内でアクティブである場合に、このルールを非アクティブにします。

   ```
   rmvfilt -n 23
   ```

   カーネル内のすべてのフィルター・ルールを非アクティブにするには、以下のコマンドを入力します。

   ```
   rmvfilt -n all
   ```

関連概念:

17 ページの『ルールの作成』
トラステッド・ファイアウォールの VLAN 間ルーティングを使用可能にするためのルールを作成することができます。

関連資料:

38 ページの『lsvfilt コマンド』

48 ページの『rmvfilt コマンド』

トラステッド・ロギング

PowerVM® のトラステッド・ロギングにより、AIX LPAR は、接続された 仮想 I/O サーバー (VIOS) に保管されているログ・ファイルに書き込むことができます。データはハイパーバイザーを使用して VIOS に直接送信され、クライアント LPAR と VIOS の間にネットワーク接続は必要ありません。

仮想ログ

仮想 I/O サーバー (VIOS) の管理者はログ・ファイルを作成して管理します。これらのファイルは、仮想ディスクまたは仮想光メディアと同様に /dev ディレクトリー内の仮想ログ・デバイスとして AIX オペレーティング・システムに提示されます。

ログ・ファイルを仮想ログとして保管すると、それらが生成されたクライアント LPAR で root 権限を持つユーザーがそれらのファイルを変更できないため、記録の信頼性のレベルが向上します。複数の仮想ログ・デバイスを同じクライアント LPAR に接続することができます。各ログは、/dev ディレクトリー内の別個のファイルになります。

トラステッド・ロギングにより、複数のクライアント LPAR のログ・データを VIOS からアクセス可能な単一のファイルシステムに統合できます。そのため、VIOS は、ログの分析およびアーカイブのためのシステム上の単一の場所を提供します。クライアント LPAR の管理者は、データを仮想ログ・デバイスに書き込むようにアプリケーションおよび AIX オペレーティング・システムを構成できます。これは、ローカル・ファイルにデータを書き込むのと似ています。監査記録を仮想ログに送信するように AIX 監査サブシステムを構成できます。syslog などのその他の AIX サービスは既存の構成と連動して、データを仮想ログに送信します。

仮想ログを構成するために、VIOS の管理者は、次の個別のコンポーネントで構成される、仮想ログの名前を指定する必要があります。

- クライアント名
- ログ名

これらの 2 つのコンポーネントの名前は、VIOS 管理者によって任意の値に設定できます。ただし、クライアント名は、通常は特定の LPAR に接続されたすべての仮想ログで同じです (例えば、LPAR のホスト名)。ログ名は、ログの目的 (監査または syslog など) を識別するために使用されます。

AIX LPAR では、それぞれの仮想ログ・デバイスは /dev ファイルシステム内の 2 つの機能的に同等なファイルとして存在します。最初のファイルの名前にはデバイスの名前が使用され (例えば、/dev/vlog0)、2 番目のファイルには、vl プレフィックスをログ名およびデバイス番号と連結した名前が付けられます。例えば、仮想ログ・デバイス vlog0 のログ名が audit である場合、その仮想ログ・デバイスは、/dev ファイルシステム内で vlog0 および vlaudit0 の両方として存在します。

関連情報:

仮想ログの作成

仮想ログ・デバイスの検出

VIOS の管理者が仮想ログ・デバイスを作成してクライアント LPAR に接続した後、そのデバイスが認識されるには、クライアント LPAR のデバイス構成をリフレッシュする必要があります。

クライアント LPAR の管理者は、以下のいずれかの方法を使用して設定をリフレッシュします。

- クライアント LPAR のリブート
- **cfgmgr** コマンドの実行

lsdev コマンドを実行して、仮想ログ・デバイスを表示します。デバイスには、デフォルトで vlog のプレフィックスが付けられています。次に、2 つの仮想ログ・デバイスが存在する AIX LPAR での **lsdev** コマンド出力の例を示します。

```
lsdev
vlog0  Virtual Log Device
vlog1  Virtual Log Device
```

lsattr –El *<device name>* コマンドを使用して、個々の仮想ログ・デバイスのプロパティーを検査します。このコマンドにより、次のような出力が生成されます。

```
lsattr -El vlog0
PCM                         Path Control Module            False
client_name    dev-lpar-05 Client Name                    False
device_name    vlsyslog0   Device Name                    False
log_name       syslog      Log Name                       False
max_log_size   4194304     Maximum Size of Log Data File  False
max_state_size 2097152     Maximum Size of Log State File False
pvid           none        Physical Volume Identifier     False
```

この出力には、クライアント名、デバイス名、および VIOS が保管できるログ・データの量が表示されます。

仮想ログは、次の 2 つのタイプのログ・データを保管します。

- ログ・データ: AIX LPAR のアプリケーションによって生成された生のログ・データ。
- 状態データ: デバイスの構成、オープン、クローズ、およびログ・アクティビティーの分析に使用されるその他の操作の実行時に関する情報。

VIOS の管理者は、各仮想ログに保管できる**ログ・データ**および**状態データ**の量を指定します。これらの量は、max_log_size 属性および max_state_size 属性によって示されます。保管されているデータの量が指定の制限を超える場合、最も古いログ・データが上書きされます。VIOS の管理者は、ログを保存するためにログ・データの収集とアーカイブが頻繁に行われるようにする必要があります。

トラステッド・ロギングのインストール

コマンド・ライン・インターフェースまたは SMIT ツールを使用して、PowerSC トラステッド・ロギング・フィーチャーをインストールすることができます。

トラステッド・ロギングをインストールするための前提条件は、VIOS 2.2.1.0 以降、および IBM AIX 6 (テクノロジー・レベル 7 適用) または IBM AIX 7 (テクノロジー・レベル 1 適用) です。

トラステッド・ロギング・フィーチャーをインストールするためのファイル名は `powerscStd.vlog` で、これは PowerSC Standard Edition のインストール CD に含まれています。

トラステッド・ロギングの機能をインストールするには、次のようにします。

1. VIOS バージョン 2.2.1.0 以降を実行していることを確認します。
2. PowerSC インストール CD を挿入するか、インストール CD のイメージをダウンロードします。
3. **installp** コマンドまたは SMIT ツールを使用して、`powerscStd.vlog` ファイルセットをインストールします。

関連情報:

3 ページの『PowerSC Standard Edition 1.1.3 のインストール』

PowerSC Standard Edition の特定の機能ごとに、ファイルセットを 1 つインストールする必要があります。

トラステッド・ロギングの構成

AIX 監査サブシステムのトラステッド・ロギングおよび syslog を構成する手順について説明します。

AIX 監査サブシステムの構成

ローカル・ファイルシステムにログを書き込むほか、仮想ログ・デバイスにバイナリー・データを書き込むために、AIX 監査サブシステムを構成することができます。

注: AIX 監査サブシステムを構成する前に、20 ページの『仮想ログ・デバイスの検出』の手順を完了しておく必要があります。

AIX 監査サブシステムを構成するには、以下のステップを実行します。

1. バイナリー (`auditbin`) モードでデータをログに記録するように AIX 監査サブシステムを構成します。
2. `/etc/security/audit/config` 構成ファイルを編集して、AIX の監査のためにトラステッド・ロギングを活動化します。
3. `bin:` スタンザに `virtual_log = /dev/vlog0` パラメーターを追加します。

   注: LPAR の管理者が `auditbin` データを `/dev/vlog0` に書き込みたい場合、この指示は有効です。
4. 次の順序で AIX 監査サブシステムを再始動します。

```
audit shutdown
audit start
```

ローカル・ファイルシステムへのログの書き込みに加えて、監査レコードが、指定された仮想ログ・デバイスを介して 仮想 I/O サーバー (VIOS) に書き込まれます。ログは、`/etc/security/audit/config` 構成ファイルの `bin:` スタンザの既存の `bin1` および `bin2` パラメーターの制御下で保管されます。

関連情報:

監査サブシステム

syslog の構成

/etc/syslog.conf ファイルにルールを追加することによって、メッセージを仮想ログに書き込むように syslog を構成できます。

注: /etc/syslog.conf ファイルを構成する前に、20 ページの『仮想ログ・デバイスの検出』の手順を完了しておく必要があります。

/etc/syslog.conf ファイルを編集し、以下の基準に基づいてログ・メッセージを突き合わせることができます。

- 機能
- 優先順位レベル

syslog メッセージのために仮想ログを使用するには、目的のメッセージを /dev ディレクトリーの適切な仮想ログに書き込むルールを指定して /etc/syslog.conf ファイルを構成する必要があります。

例えば、何らかの機能によって生成されたデバッグ・レベル・メッセージを vlog0 仮想ログに送信するには、以下の行を /etc/syslog.conf ファイルに追加します。

```
*.debug /dev/vlog0
```

注: データを仮想ログに書き込むコマンドに対して、syslogd デーモンで使用可能なログのローテーション機能を使用しないでください。/dev ファイルシステム内のファイルは正規ファイルではなく、名前変更したり、移動したりすることはできません。 VIOS 管理者は、VIOS 内の仮想ログのローテーションを構成する必要があります。

構成の後、次のコマンドを使用して syslogd デーモンを再開する必要があります。

```
refresh -s syslogd
```

関連情報:

syslogd デーモン

仮想ログ・デバイスへのデータの書き込み

/dev ディレクトリーの適切なファイルを開き、そのファイルにデータを書き込むことによって、任意のデータが仮想ログ・デバイスに書き込まれます。仮想ログを開くことができるプロセスは一度に 1 つのみです。

例えば、次のように入力します。

echo コマンドを使用して仮想ログ・デバイスにメッセージを書き込むには、次のコマンドを入力します。

```
 echo "Log Message" > /dev/vlog0
```

cat コマンドを使用して仮想ログ・デバイスにファイルを保管するには、次のコマンドを入力します。

```
cat /etc/passwd > /dev/vlog0
```

個別の最大書き込みサイズは 32 KB に制限されており、さらに多くのデータを 1 回の書き込み操作で書き込もうとするプログラムは入出力 (EIO) エラーを受け取ります。**cat** コマンドなどのコマンド行インターフェース (CLI) ユーティリティーは自動的に転送を 32 KB の書き込み操作に分割します。

トラステッド・ネットワーク接続およびパッチ管理

トラステッド・ネットワーク接続 (TNC) は、エンドポイントの保全性を検証するための規格を規定する Trusted Computing Group (TCG) の一部を成しています。 TNC は、管理者がポリシーを適用してネットワーク・インフラストラクチャーへのアクセスを効果的に制御する上で役立つオープン・ソリューション・アーキテクチャーを定義しています。

トラステッド・ネットワーク接続の概念

トラステッド・ネットワーク接続 (TNC) のコンポーネント、セキュア通信の構成、およびパッチ管理システムについて説明します。

トラステッド・ネットワーク接続のコンポーネント

トラステッド・ネットワーク接続 (TNC) フレームワークのコンポーネントについて説明します。

TNC モデルは、以下のコンポーネントで構成されます。

トラステッド・ネットワーク接続サーバー:

トラステッド・ネットワーク接続 (TNC) サーバーは、ネットワークに追加されたクライアントを識別して、それらに対する検証を開始します。

TNC クライアントは、検証のために必要なファイルセット・レベルの情報をサーバーに提供します。サーバーは、クライアントが管理者によって構成されたレベルであるかどうかを判別します。クライアントが準拠していない場合、TNC サーバーは、管理者に必要な修復処置について通知します。

TNC サーバーは、ネットワークへのアクセスを試行しているクライアントに対する検証を開始します。TNC サーバーは、クライアントから保全性計測値を要求して検証することができる一連の保全性計測ベリファイヤー (IMV) をロードします。AIX には、システムのファイルセットおよびセキュリティー・パッチ・レベルを検証するデフォルトの IMV があります。TNC サーバーは、複数の IMV モジュールをロードして管理するフレームワークです。クライアントを検証する際、クライアントからの情報を要求するために IMV を使用して、クライアントを検証します。

パッチ管理:

トラステッド・ネットワーク接続 (TNC) サーバーは、SUMA と統合して、パッチ管理ソリューションを提供します。

AIX SUMA は、IBM ECC および Fix Central で入手可能な最新の Service Pack およびセキュリティー・フィックスをダウンロードします。TNC およびパッチ管理デーモンは、最新の更新済み情報を TNC サーバーにプッシュします。この情報は、クライアントを検証するための基本的なファイルセットとして機能します。

サービス更新管理アシスタント (SUMA) のダウンロードを管理して、ファイルセット情報を TNC サーバーにプッシュするには、**tncpmd** デーモンを構成する必要があります。更新を自動的にダウンロードできるようにするには、このデーモンが、インターネットに接続されたシステムでホストされている必要があります。TNC パッチ管理サーバーをインターネットに接続せずに使用する場合、ユーザー定義のフィックス・リポジトリーを TNC パッチ管理サーバーに登録することができます。

注: TNC サーバーおよび **tncpmd** デーモンを同じシステムでホストすることができます。

トラステッド・ネットワーク接続クライアント:

トラステッド・ネットワーク接続 (TNC) クライアントは、検証のために TNC サーバーで必要となる情報を提供します。

サーバーは、クライアントが管理者によって構成されたレベルであるかどうかを判別します。クライアントが準拠していない場合、TNC サーバーは、管理者に必要な更新について通知します。

TNC クライアントは、始動時に IMC をロードし、IMC を使用して必要な情報を収集します。

トラステッド・ネットワーク接続の IP リファラー:

トラステッド・ネットワーク接続 (TNC) サーバーは、ネットワークの一部であるクライアントに対する検証を自動的に開始できます。仮想 I/O サーバー (VIOS) パーティションで実行される IP リファラーは、VIOS によってサービス提供されている新規クライアントを検出して、それらの IP アドレスを TNC サーバーに送信します。TNC サーバーは、定義されているポリシーに関してクライアントを検証します。

トラステッド・ネットワーク接続のセキュア通信

トラステッド・ネットワーク接続 (TNC) デーモンは、トランスポート層セキュリティー (TLS) または Secure Sockets Layer (SSL) によって使用可能になる暗号化チャネルを介して通信します。

セキュア通信とは、ネットワークを行き来するデータとコマンドが確実に認証され、安全であるようにすることです。各システムには独自の鍵と証明書が必要です。これらは、コンポーネントに対する初期化コマンドが実行されるときに生成されます。このプロセスは管理者に対して完全に透過的であるため、管理者が介入する必要性が減ります。

新規クライアントを検証するには、そのクライアントの証明書をサーバーのデータベースにインポートする必要があります。最初に証明書には非トラステッドのマークが付けられます。管理者は **psconf** コマンドを使用して証明書を表示し、次のコマンドを入力してその証明書にトラステッドのマークを付けます。

```
psconf certadd –i<ip> -t<TRUSTED|UNTRUSTED>
```

別の鍵と証明書を使用するために、**psconf** コマンドは、証明書をインポートするオプションを提供します。

サーバーから証明書をインポートするには、次のコマンドを入力します。

```
psconf import  -S -k<key filename> -f<key filename>
```

クライアントから証明書をインポートするには、次のコマンドを入力します。

```
psconf import -C -k<key filename> -f<key filename>
```

トラステッド・ネットワーク接続プロトコル

トラステッド・ネットワーク接続 (TNC) プロトコルは、ネットワーク保全性を維持するために、TNC フレームワークと共に使用します。

TNC は、エンドポイントの保全性を検証するための規格を提供します。アクセスを要求するエンドポイントは、稼働環境に影響を与える可能性がある重要なコンポーネントの保全性計測に基づいて評価されます。TNC フレームワークにより、管理者はネットワーク内のシステムの保全性をモニターすることができます。TNC は AIX パッチ配布インフラストラクチャーと統合され、完全なパッチ管理ソリューションを構築します。

TNC の規格は、AIX および POWER® family システム体系の要件を満たす必要があります。 TNC のコンポーネントは、AIX オペレーティング・システムで完全なパッチ管理ソリューションを提供するように設計されています。この構成により、管理者は AIX デプロイメントのソフトウェア構成を効率的に管理することができます。システムのパッチ・レベルを検査して、準拠していないクライアントに関するレポートを生成するツールが用意されています。さらに、パッチ管理は、パッチをダウンロードしてインストールするプロセスを簡素化します。

IMC および IMV モジュール

トラステッド・ネットワーク接続 (TNC) サーバーまたはクライアントは、サーバーの検証のために保全性計測コレクター (IMC) モジュールおよび保全性計測ベリファイヤー (IMV) モジュールを内部的に使用します。

このフレームワークでは、複数の IMC および IMV モジュールをサーバーとクライアントにロードすることができます。オペレーティング・システム (OS) レベルおよびファイルセット・レベルの検証を実行するモジュールは、デフォルトで AIX オペレーティング・システムに付属しています。AIX オペレーティング・システムに付属のモジュールにアクセスするには、以下のいずれかのパスを使用します。

- `/usr/lib/security/tnc/libfileset_imc.a`: クライアント・システムからインストールされた OS レベルおよびファイルセットに関する情報を収集して、検証のために IMV (TNC サーバー) に送信します。
- `/usr/lib/security/tnc/libfileset_imv.a`: クライアントから OS レベルおよびファイルセット情報を要求して、それを基本的な情報と比較します。また、TNC サーバーのデータベースでクライアントの状況を更新します。状況を表示するには、以下のコマンドを入力します。

```
psconf list -s<COMPLIANT|IGNORE|FAILED|ALL>-i<ip|ALL> [-c] [-q]
```

関連資料:

43 ページの『psconf コマンド』

トラステッド・ネットワーク接続のインストール

トラステッド・ネットワーク接続 (TNC) のコンポーネントをインストールするには、特定のステップを実行する必要があります。

TNC のコンポーネントを使用するためのセットアップを構成するには、以下のステップを実行します。

1. TNC サーバー、トラステッド・ネットワーク接続およびパッチ管理 (TNCPM) サーバー、および 仮想 I/O サーバー (VIOS) の TNC IP リファラーをセットアップするための、システムの IP アドレスを確認します。

   注: TNC サーバーを TNC クライアントとして構成することはできません。
2. ネットワーク・インストール管理 (NIM) サーバーをセットアップします。サーバーとして構成されるシステムは NIM マスターであり、`sets:bos.sysmgt.nim.master` ファイルセットがクライアント・システムにインストールされている必要があります。
3. TNCPM サーバーを構成します。この構成は、NIM システムでセットアップすることができます。TNCPM サーバーは、SUMA を使用して、IBM Fix Central および ECC Web サイトからパッチをダウンロードします。更新をダウンロードするには、システムはインターネットに接続されている必要があります。次のコマンドを入力して、TNCPM サーバーを構成します。

   ```
   pmconf mktncpm [pmport=<port>]tncserver=<host:port>
   ```

   例えば、次のように入力します。

   ```
   pmconf mktncpm pmport=20000 tncserver=1.1.1.1:10000
   ```

4. TNC サーバーでポリシーを構成します。クライアントを検証するためのポリシーを作成するには、 30 ページの『トラステッド・ネットワーク接続クライアントに関するポリシーの作成』を参照してください。
5. VIOS で TNC IP リファラーを構成します。VIOS 上のこの構成は、ネットワークに接続するクライアントに対する検証をトリガーします。次のコマンドを入力して、リファラーを構成します。

   ```
   psconf mkipref tncport=<port> tncserver=<ip:port>
   ```

   例えば、次のように入力します。

   ```
   psconf mkipref tncport=10000 tncserver=1.1.1.1:10000
   ```

   注: サーバー・ポートとクライアント・ポートの TNC ポートの値は同じでなければなりません。
6. 次のコマンドを使用して、クライアントを構成します。

   ```
   psconf mkclient tncport=<port> tncserver=<serverip>:<port>
   ```

   例えば、次のように入力します。

   ```
   psconf mkclient tncport=10000 tncserver=10.1.1.1:10000
   ```

関連資料:

43 ページの『psconf コマンド』

関連情報:

3 ページの『PowerSC Standard Edition 1.1.3 のインストール』
PowerSC Standard Edition の特定の機能ごとに、ファイルセットを 1 つインストールする必要があります。

NIM でのインストール

IBM Fix Central

パスポート・アドバンテージ・オンライン・ヘルプ・センター

トラステッド・ネットワーク接続およびパッチ管理の構成

トラステッド・ネットワーク接続 (TNC) を、パッチ管理デーモンとして構成する必要があります。 TNC サーバーは、SUMA と統合して包括的なパッチ管理ソリューションを提供します。

トラステッド・ネットワーク接続サーバーの構成

TNC サーバーを構成する手順について説明します。

TNC サーバーを構成するには、`/etc/tnccs.conf` ファイルに次のような値が入っている必要があります。

```
component = SERVER
```

システムをサーバーとして構成するには、次のコマンドを入力します。

```
psconf mkserver tncport=<port> pmserver=<ip|hostname[,ip2|hostname2..]:port>
[recheck_interval=<time in mins>]
```

例えば、次のように入力します。

```
psconf mkserver tncport=10000 pmserver=2.2.2.2:20000 recheck_interval=20
```

注: `tncport` ポートと `pmserver` ポートは、異なる値に設定する必要があります。`recheck_interval` パラメーターの値が指定されない場合、デフォルト値の 1440 分が使用されます。

tncport ポートに使用されるデフォルトのポート値は 42830 分で、pmserver ポートに使用されるデフォルト値は 38240 分です。

関連資料:

43 ページの『psconf コマンド』

トラステッド・ネットワーク接続クライアントの構成

トラステッド・ネットワーク接続 (TNC) クライアントを構成する手順と、セットアップに必要な構成設定について説明します。

TNC クライアントを構成するには、/etc/tnccs.conf ファイルに次のような値が入っている必要があります。

```
component = CLIENT
```

システムをクライアントとして構成するには、次のコマンドを入力します。

```
psconf mkclient tncport=<port> tncserver=<ip:port>
```

例えば、次のように入力します。

```
psconf mkclient tncport=10000 tncserver=1.1.1.1:10000
```

注: サーバー・ポートとクライアント・ポートの tncport の値は同じでなければなりません。

関連資料:

43 ページの『psconf コマンド』

パッチ管理サーバーの構成

システムをパッチ管理サーバーとして構成する手順について説明します。

TNC クライアントを更新できるように、トラステッド・ネットワーク接続 (TNC) パッチ管理サーバーをネットワーク・インストール管理 (NIM) サーバー上で構成する必要があります。

| TNC パッチ管理のフィックス・リポジトリーを初期化するには、以下のコマンドを入力します。

```
| pmconf init -i <download interval> -l <TL list> [-A] [-P <download path>][-x <ifix interval>]
| [-K <ifix key>]
```

| **pmconf** コマンドの例は、以下のとおりです。

```
| pmconf init -i 1440 -l 6100-07,7100-01
```

init コマンドでは、各テクノロジー・レベルに対して最新の Service Pack がダウンロードされ、TNC サーバー用に使用可能にされます。更新済みの Service Pack によって、TNC サーバーが基本的な TNC クライアントの検証を実行できるようになり、TNC パッチ管理サーバーで TNC クライアントの更新をインストールできるようになります。クライアントの更新を実行する際に、すべてのご使用条件に同意するには、**-A** フラグを指定します。デフォルトでは、TNC パッチ管理サーバーがダウンロードするフィックス・リポジトリーは、/var/tnc/tncpm/fix_repository ファイル内です。別のディレクトリーを指定するには、**-P** フラグを使用します。

| IBM セキュリティー・アドバイザリーおよび暫定修正の自動ダウンロードを可能にするには、暫定修正の
| 間隔を指定します。この機能により、新規に公開されるセキュリティー暫定修正および関連する Common
| Vulnerabilities and Exposures (CVE) 識別子が自動的に通知されます。セキュリティー・アドバイザリーお
| よび暫定修正はすべて、TNC に登録される前に検査されます。暫定修正を自動的にダウンロードするため

| に必須の IBM AIX ぜい弱性公開鍵は、IBM AIX セキュリティーの Web サイトで入手できます。Service
| Pack および暫定修正の自動ダウンロードは、ダウンロードの間隔と暫定修正の間隔の両方を 0 に設定する
| ことによって無効になります。

Service Pack および暫定修正の登録を手動で更新することもできます。IBM セキュリティー・アドバイザリーを対応する暫定修正とともに手動で登録するには、以下のコマンドを入力します。

```
pmconf add -y <advisory file> -v <signature file>  -e <ifix tar file>
```

| スタンドアロン暫定修正を手動で登録するには、以下のコマンドを入力します。

```
| pmconf add -p <SP> -e <ifix file>
```

新規のテクノロジー・レベルを登録し、その最新の Service Pack をダウンロードするには、以下のコマンドを入力します。

```
pmconf add -l <TL list>
```

最新ではないバージョンの Service Pack をダウンロードする場合、または検証およびクライアントの更新に使用するテクノロジー・レベルをダウンロードする場合は、以下のコマンドを入力します。

```
pmconf add -l <TL list> -d
pmconf add -s <SP List>
```

システム上に存在する Service Pack またはテクノロジー・レベルのフィックス・リポジトリーを登録するには、以下のコマンドを入力します。

```
pmconf add -s <SP> -p <user_defined_fix_repository>
pmconf add -l <TL> -p <user_defined_fix_repository>
```

システムがパッチ管理サーバーとして機能するように構成するには、次のコマンドを入力します。

```
pmconf mktncpm [pmport=<port>] tncserver=ip_list[:port]
```

このコマンドの例は、以下のとおりです。

```
pmconf mktncpm pmport=20000 tncserver=1.1.1.1:100000
```

TNC パッチ管理サーバーは、セキュリティーの Authorized Problem Analysis Reports (APAR) の管理を常にサポートします。その他のタイプの APAR を管理するように TNC パッチ管理を構成するには、以下のコマンドを入力します。

```
pmconf add -t <APAR_type_list>
```

直前の例の <APAR_type_list> は、以下のタイプの APAR を含むコンマ区切りリストです。

- HIPER
- PE
- 拡張

TNC パッチ管理サーバーは、Service Pack、テクノロジー・レベル、およびクライアント更新のダウンロードにおける **syslog** をサポートします。機能は `user` で、優先順位は `info` です。この例は `user.info` です。

また、TNC パッチ管理サーバーは、`/var/tnc/tncpm/log/update/<ip>/<timestamp>` ディレクトリーにあるすべてのクライアント更新と共にログも維持します。

関連資料:

43 ページの『psconf コマンド』

関連情報:

IBM AIX Security

トラステッド・ネットワーク接続サーバーの電子メール通知の構成

トラステッド・ネットワーク接続 (TNC) サーバーの電子メール通知を構成する手順について説明します。

TNC サーバーはクライアントのパッチ・レベルを表示します。TNC サーバーは、クライアントが準拠していないことを検出すると、結果と必要な修復処置を示す電子メールを管理者に送信します。

管理者の電子メール・アドレスを構成するには、次のコマンドを入力します。

```
psconf add –e <email_id>[ipgroup=[±]G1, G2 ..]
```

例えば、次のように入力します。

```
psconf add –e abc@ibm.com ipgroup=vayugrp1,vayugrp2
```

上記の例では、IP グループ *vayugrp1* および *vayugrp2* に関する電子メールが abc@ibm.com という電子メール・アドレスに送信されます。

電子メール・アドレスが割り当てられていない IP グループに関するメールをグローバル電子メール・アドレスに送信するには、次のコマンドを入力します。

```
psconf add –e <mailaddress>
```

例えば、次のように入力します。

```
psconf add –e abc@ibm.com
```

上記の例では、IP グループに電子メール・アドレスが割り当てられていない場合に、abc@ibm.com という電子メール・アドレスにメールが送信されます。これは、グローバル電子メール・アドレスとして機能します。

関連資料:

43 ページの『psconf コマンド』

VIOS での IP リファラーの構成

仮想 I/O サーバー (VIOS) で IP リファラーを構成して、検証を自動的に開始する方法を説明します。

注: IP リファラーを構成する前に、仮想入出力サーバー (VIOS) で SVM カーネル・エクステンションを構成する必要があります。

TNC IP リファラーを構成するには、`/etc/tnccs.conf` 構成ファイルに `component = IPREF` のような設定値がなければなりません。

次のコマンドを入力して、システムをクライアントとして構成することができます。

```
psconf mkipref tncport=<port> tncserver=<ip:port>
```

例えば、次のように入力します。

```
psconf mkipref tncport=10000 tncserver=1.1.1.1:10000
```

`tncserver` ポートと、クライアント・ポートの `tncport` の値は同じでなければなりません。

関連資料:

43 ページの『psconf コマンド』

トラステッド・ネットワーク接続およびパッチ管理の管理

トラステッド・ネットワーク接続 (TNC) を管理して、クライアント、ポリシー、ログ、検証結果の追加、クライアントおよび TNC に関連した証明書の更新といったタスクを実装します。

トラステッド・ネットワーク接続サーバーのログの表示

トラステッド・ネットワーク接続 (TNC) サーバーのログを表示する方法を説明します。

TNC サーバーは、すべてのクライアントの検証結果をログに記録します。ログを表示するには、**psconf** コマンドを実行します。

```
psconf list –H –i <ip |ALL>
```

関連資料:

43 ページの『psconf コマンド』

トラステッド・ネットワーク接続クライアントに関するポリシーの作成

トラステッド・ネットワーク接続 (TNC) クライアントに関連するポリシーをセットアップする方法を説明します。

psconf コンソールは、TNC ポリシーを管理するために必要なインターフェースを備えています。各クライアントまたはクライアント・グループをポリシーに関連付けることができます。

以下のポリシーを作成できます。

- インターネット・プロトコル (IP) グループには複数のクライアント IP アドレスが含まれます。
- 各クライアント IP は、1 つのグループのみに所属できます。
- IP グループはポリシー・グループに関連付けられます。
- ポリシー・グループには、さまざまな種類のポリシーが含まれます。例えば、クライアントに必要なオペレーティング・システム・レベル (リリース、テクノロジー・レベル、および Service Pack) を指定するファイルセット・ポリシーがあります。ポリシー・グループには複数のファイルセット・ポリシーが含まれる場合があり、このポリシーを参照するクライアントは、いずれかのファイルセット・ポリシーで指定されているレベルでなければなりません。

以下のコマンドは、IP グループ、ポリシー・グループ、およびファイルセット・ポリシーの作成方法を示しています。

IP グループを作成するには、次のコマンドを入力します。

```
psconf add –G <ipgrpname> ip=[±]<ip1,ip2,ip3 ...>
```

例えば、次のように入力します。

```
psconf add –G myipgrp ip=1.1.1.1,2.2.2.2
```

注: グループの場合、少なくとも 1 つの IP を指定する必要があります。複数の IP はコンマで区切る必要があります。

ファイルセット・ポリシーを作成するには、次のコマンドを入力します。

```
psconf add –F <fspolicyname> <rel00-TL-SP>
```

例えば、次のように入力します。

```
psconf add –F myfspol  6100-02-03 aparlist=IY0001,IY0002
```

注: ビルド情報は、<rel00-TL-sp> の形式でなければなりません。

ポリシーを作成して IP グループを割り当てるには、次のコマンドを入力します。

```
psconf add –P <policyname> ipgroup=[±] <ipgrp1, ipgrp2 ...]
```

例えば、次のように入力します。

```
psconf add –P mypol ipgroup=myipgrp,myipgrp1
```

ファイルセット・ポリシーをポリシーに割り当てるには、次のコマンドを入力します。

```
psconf add –P <policyname> fspolicy=[±]<fspol1, fspol2 ...>
```

例えば、次のように入力します。

```
psconf add –P mypol fspolicy=myfspol,myfspol1
```

注: 複数のファイルセット・ポリシーが指定される場合、システムは、クライアントに一致する最適なポリシーを適用します。例えば、クライアントが 6100-02-01 にあり、ファイルセット・ポリシー 7100-03-04 および 6100-02-03 を指定する場合、このクライアントには 6100-02-03 が適用されます。

関連資料:

43 ページの『psconf コマンド』

トラステッド・ネットワーク接続クライアントの検証の開始

トラステッド・ネットワーク接続 (TNC) クライアントを検証する方法を説明します。

クライアント検証のために以下のいずれかの方法を使用します。

- 仮想 I/O サーバー (VIOS) の IP リファラー・デーモンが、クライアント IP を TNC サーバーに転送します。クライアント LPAR は、IP を取得してネットワークへのアクセスを試行します。VIOS の IP リファラー・デーモンは、新しい IP アドレスを検出して、それを TNC サーバーに転送します。TNC サーバーは新しい IP アドレスを受信するとすぐに、検証を開始します。
- TNC サーバーが、定期的にクライアントを検証します。管理者は、検証されるクライアント IP を TNC ポリシー・データベースに追加することができます。 TNC サーバーは、データベース内のクライアントを検証します。再検証は、/etc/tnccs.conf 構成ファイルで指定されている recheck_interval 属性値を参照して定期的な間隔で自動的に行われます。
- 管理者が、クライアント検証を手動で開始します。管理者は、次のコマンドを実行することにより、検証を手動で開始して、クライアントがネットワークに追加されたかどうかを検証できます。

  ```
  tncconsole verify -i <ip>
  ```

注: VIOS に接続されないリソースの場合、クライアントが手動で TNC サーバーに追加されると、検証および更新することができます。

関連資料:

43 ページの『psconf コマンド』

トラステッド・ネットワーク接続の検証結果の表示

トラステッド・ネットワーク接続 (TNC) クライアントの検証結果を表示する手順について説明します。

ネットワーク内のクライアントの検証結果を表示するには、次のコマンドを入力します。

```
psconf list -s ALL -i ALL
```

このコマンドにより、**IGNORED**、**COMPLIANT**、または **FAILED** 状況のすべてのクライアントが表示されます。

- **IGNORED**: クライアント IP は IP リストで無視されます (つまり、クライアントの検証を免除できます)。
- **COMPLIANT**: クライアントは検証に合格しました (つまり、クライアントはポリシーに準拠しています)。
- **FAILED**: クライアントの検証は失敗しました (つまり、クライアントはポリシーに準拠しておらず、管理アクションが必要です)。

失敗の理由を判別するには、次のように、失敗したクライアント IP を指定して **psconf** コマンドを実行します。

```
psconf list -s ALL -i <ip>
```

関連資料:

43 ページの『psconf コマンド』

トラステッド・ネットワーク接続クライアントの更新

トラステッド・ネットワーク接続 (TNC) サーバーは、クライアントを検証し、クライアントの状況と検証結果を使用してデータベースを更新します。管理者は、結果を表示し、クライアントを更新するためのアクションを実行できます。

旧レベルのクライアントを更新するには、次のコマンドを入力します。

```
psconf update -i <ip> -r <buildinfo> [-a apar1,apar2...]
```

例えば、次のように入力します。

```
psconf update –i 4.4.4.4 –r 6100-02-03 –a IY0004
```

psconf コマンドは、未インストールのビルドおよび APAR をインストールしてクライアントを更新します。

関連資料:

43 ページの『psconf コマンド』

パッチ管理ポリシーの管理

パッチ管理ポリシーを構成するために、**pmconf** コマンドが使用されます。

パッチ管理ポリシーは、TNC サーバーの IP アドレスや SUMA 更新を開始する時間間隔などの情報を提供します。

パッチ管理ポリシーを管理するには、次のコマンドを入力します。

```
pmconf mktncpm [pmport=<port>] tncserver=<host:port>
```

例えば、次のように入力します。

```
pmconf mktncpm pmport=2000 tncserver=10.1.1.1:1000
```

注: `pmport` と `tncserver` は、異なるポートでなければなりません。

関連資料:

39 ページの『pmconf コマンド』

トラステッド・ネットワーク接続の証明書のインポート

証明書をインポートして、ネットワークでデータを安全に送信する手順について説明します。

トラステッド・ネットワーク接続 (TNC) デーモンは、トランスポート層セキュリティー (TLS) または Secure Sockets Layer (SSL) プロトコルによって使用可能になる暗号化チャネルを介して通信します。このデーモンは、ネットワーク上を移送されるデータとコマンドが確実に認証され、安全であるようにします。各システムには独自の鍵と証明書があります。これらは、コンポーネントに対する初期化コマンドが実行されるときに生成されます。このプロセスは管理者に対して透過的であるため、管理者が介入する必要性が減ります。クライアントが初めて検証されるとき、その証明書がサーバーのデータベースにインポートされます。最初に証明書には非トラステッドのマークが付けられます。管理者は **psconf** コマンドを使用して証明書を表示し、次のコマンドを入力してその証明書にトラステッドのマークを付けます。

```
psconf certadd –i <ip> -t <TRUSTED|UNTRUSTED>
```

管理者が別の鍵と証明書を使用する必要がある場合、**psconf** コマンドは、その鍵と証明書をインポートするための機能を提供します。

サーバーから証明書をインポートするには、次のコマンドを入力します。

```
psconf import  -S -k <key filename> -f <filename>
```

クライアントから証明書をインポートするには、次のコマンドを入力します。

```
psconf import -C -k <key filename> -f <filename>
```

関連資料:

43 ページの『psconf コマンド』

TNC サーバーのレポート作成

トラステッド・ネットワーク接続 (TNC) サーバーは、その Common Vulnerabilities and Exposures (CVE)、IBM セキュリティー・アドバイザリー、TNC サーバー・ポリシー、TNC クライアント・セキュリティー・フィックス、登録済みサービス・パックおよび暫定修正のレポート作成に、コンマ区切り値 (CSV) 形式とテキスト出力形式の両方をサポートします。

CVE レポートには、登録済みサービス・パックに共通する機密漏れの危険性およびぜい弱性がすべて表示されます。このレポートの結果を表示するには、以下のコマンドを入力します。

```
psconf report -v {CVEid|ALL} -o {TEXT|CSV}
```

IBM セキュリティー・アドバイザリー・レポートには、インストールされた IBM ソフトウェアの、セキュリティーに関する既知のぜい弱性が表示されます。このレポートの結果を表示するには、以下のコマンドを入力します。

```
psconf report -A <advisoryname>
```

TNC サーバー・ポリシー・レポートには、TNC サーバー上で実行されるセキュリティー・ポリシーが表示されます。このレポートの結果を表示するには、以下のコマンドを入力します。

```
psconf report -P {policyname|ALL} -o {TEXT|CSV}
```

TNC クライアント・フィックス・レポートには、TNC クライアントのインストール済みまたは欠落した暫定修正が表示されます。このレポートの結果を表示するには、以下のコマンドを入力します。

| `psconf report -i {ip|ALL} -o {TEXT|CSV}`

| また、登録済みサービス・パックと、関連するプログラム診断依頼書 (APAR) および暫定修正のリストを
| 生成するレポートを実行することもできます。このレポートの結果を表示するには、以下のコマンドを入力
| します。

| `psconf report -B {buildinfo|ALL} -o {TEXT|CSV}`

| **関連資料**:

| 43 ページの『psconf コマンド』

トラステッド・ネットワーク接続およびパッチ管理のトラブルシューティング

障害の考えられる原因と、TNC およびパッチ管理システムのトラブルシューティングを行う手順について説明します。

TNC およびパッチ管理システムのトラブルシューティングを行うには、次の表にリストされている構成設定を検査します。

表 3. TNC およびパッチ管理システムの構成設定のトラブルシューティング

問題	解決方法
TNC サーバーが始動しないか、応答しない	以下の手順を実行します。 1. 次のコマンドを入力して、TNC サーバー・デーモンが実行されているかどうかを判別します。 `ps -eaf | grep tnccsd` 2. 実行されていない場合は、`/var/tnc/.tncsock` ファイルを削除します。 3. サーバーを再始動します。 問題が解決されない場合には、TNC サーバーの `/etc/tnccs.conf` 構成ファイルで `component = SERVER` エントリーがあるか確認します。
TNC パッチ管理サーバーが始動しないか、応答しない	• 次のコマンドを入力して、TNC パッチ管理サーバー・デーモンが実行されているかどうかを判別します。 `ps –eaf | grep tncpmd` • TNC パッチ管理サーバーの `/etc/tnccs.conf` 構成ファイルで `component = TNCPM` エントリーがあるか確認します。
TNC クライアントが始動しないか、応答しない	• 次のコマンドを入力して、TNC クライアント・デーモンが実行されているかどうかを判別します。 `ps -eaf | grep tnccsd` • TNC クライアントの `/etc/tnccs.conf` 構成ファイルで `component = CLIENT` エントリーがあるか確認します。
TNC IP リファラーが 仮想 I/O サーバー (VIOS) で実行されていない	• 次のコマンドを入力して、TNC IP リファラー・デーモンが実行されているかどうかを判別します。 `ps -eaf | grep tnccsd` • VIOS の `/etc/tnccs.conf` 構成ファイルで `component = IPREF` エントリーがあるか確認します。
システムを TNC サーバーとクライアントの両方として構成できない	TNC サーバーとクライアントは同じシステム上で同時に稼働することはできません。

表 3. TNC およびパッチ管理システムの構成設定のトラブルシューティング (続き)

問題	解決方法
デーモンは実行されているが、検証が行われない	デーモンに対してログ・メッセージを有効にします。/etc/tnccs.conf ファイルで level=info ログを設定します。ログ・メッセージを分析することができます。

PowerSC Standard Edition コマンド入力

PowerSC Standard Edition は、コマンド・ラインを使用して、トラステッド・ファイアウォールのコンポーネントおよびトラステッド・ネットワーク接続のコンポーネントとの通信を可能にするコマンドを提供します。

chvfilt コマンド

目的

既存の仮想 LAN 間のフィルター規則の値を変更します。

構文

chvfilt [**-v <4|6>**] **-n fid** [**-a <D|P>**] [**-z <svlan>**] [**-Z <dvlan>**] [**-s <s_addr>**] [**-d <d_addr>**] [**-o <src_port_op>**] [**-p <src_port>**] [**-O <dst_port_op>**] [**-P <dst_port>**] [**-c <protocol>**]

説明

chvfilt コマンドは、仮想 LAN 間のフィルター規則 (フィルター規則テーブルにある) の定義を変更するのに使用します。

フラグ

-a アクションを指定します。有効な値は次のとおりです。

- D (拒否): トラフィックをブロックします。
- P (許可): トラフィックを許可します。

-c フィルター規則を適用できるさまざまなプロトコルを指定します。有効な値は次のとおりです。

- udp
- icmp
- icmpv6
- tcp
- any

-d 宛先アドレスを、IPv4 または IPv6 形式で指定します。

-m 送信元のアドレス・マスクを指定します。

-M 宛先のアドレス・マスクを指定します。

-n 変更する必要のあるフィルター規則のフィルター ID を指定します。

-o 送信元ポートまたは Internet Control Message Protocol (ICMP) タイプの操作を指定します。有効な値は次のとおりです。

- lt
- gt

- eq
- any

-O 宛先ポートまたは ICMP コード操作を指定します。有効な値は次のとおりです。

- lt
- gt
- eq
- any

-p 送信元ポートまたは ICMP タイプを指定します。

-P 宛先ポートまたは ICMP コードを指定します。

-s 送信元アドレスを、v4 または v6 形式で指定します。

-v フィルター規則テーブルの IP バージョンを指定します。有効な値は 4 と 6 です。

-z 送信元のロジカル・パーティションの仮想 LAN ID を指定します。

-Z 宛先のロジカル・パーティションの仮想 LAN ID を指定します。

終了状況

このコマンドは、以下の終了値を戻します。

0 正常終了。

>0 エラーが発生しました。

例

1. カーネルに存在する有効なフィルター規則を変更する場合は、次のコマンドを入力します。

   ```
   chvfilt -n 1 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

2. フィルター規則 (n=2) がカーネルに存在しない場合、出力は以下のようになります。

   ```
   chvfilt -n 2 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

   システムは次の出力を表示します。

   ```
   ioctl(QUERY_FILTER) failed no filter rule err=2
   Cannot Change the filter rule.
   ```

genvfilt コマンド

目的

同一の IBM Power Systems サーバー上のロジカル・パーティションの間にある仮想 LAN (VLAN) のフィルター規則を追加します。

構文

genvfilt -v <4|6> -a <D|P> -z <svlan> -Z <dvlan> [-s <s_addr>] [-d <d_addr>] [-o <src_port_op>] [-p <src_port>] [-O <dst_port_op>] [-P <dst_port>] [-c <protocol>]

説明

genvfiltコマンドは、同一の IBM Power Systems サーバー上のロジカル・パーティションの間にある仮想 LAN (VLAN) のフィルター規則を追加するのに使用します。

フラグ

-a アクションを指定します。有効な値は次のとおりです。

- D (拒否): トラフィックをブロックします。
- P (許可): トラフィックを許可します。

-c フィルター規則を適用できるさまざまなプロトコルを指定します。有効な値は次のとおりです。

- udp
- icmp
- icmpv6
- tcp
- any

-d 宛先アドレスを、v4 または v6 形式で指定します。

-m 送信元のアドレス・マスクを指定します。

-M 宛先のアドレス・マスクを指定します。

-o 送信元ポートまたは Internet Control Message Protocol (ICMP) タイプの操作を指定します。有効な値は次のとおりです。

- lt
- gt
- eq
- any

-O 宛先ポートまたは ICMP コード操作を指定します。有効な値は次のとおりです。

- lt
- gt
- eq
- any

-p 送信元ポートまたは ICMP タイプを指定します。

-P 宛先ポートまたは ICMP コードを指定します。

-s 送信元アドレスを、IPv4 または IPv6 形式で指定します。

-v フィルター規則テーブルの IP バージョンを指定します。有効な値は 4 と 6 です。

-z 送信元の LPAR の仮想 LAN ID を指定します。仮想 LAN ID は、1 から 4096 の範囲の値でなければなりません。

-Z 宛先の LPAR の仮想 LAN ID を指定します。仮想 LAN ID は、1 から 4096 の範囲の値でなければなりません。

終了状況

このコマンドは、以下の終了値を戻します。

0 正常終了。

>0 エラーが発生しました。

例

1. 送信元 VLAN ID 100 から、特定のポート上の宛先 VLAN ID 200 への TCP データを許可するフィルター規則を追加する場合は、次のコマンドを入力します。

```
genvfilt -v4 -a P -z 100 -Z 200  -o lt -p 345 -O lt -P 345 -c tcp
```

関連資料:

『mkvfilt コマンド』

49 ページの『vlantfw コマンド』

lsvfilt コマンド

目的

仮想 LAN 間のフィルター規則を、フィルター・テーブルからリストします。

構文

lsvfilt [**-a**]

説明

lsvfilt コマンドは、仮想 LAN 間のフィルター規則およびその状況をリストするのに使用されます。

フラグ

-a アクティブなフィルター規則のみをリストします。

終了状況

このコマンドは、以下の終了値を戻します。

0 正常終了。

>0 エラーが発生しました。

例

1. カーネル内のアクティブなフィルター規則をすべてリストするには、次のコマンドを入力します。

```
lsvfilt -a
```

関連概念:

18 ページの『ルールの非アクティブ化』

トラステッド・ファイアウォール・フィーチャーで、VLAN 間ルーティングを使用可能にするルールを非アクティブにすることができます。

mkvfilt コマンド

目的

genvfilt コマンドで定義した、仮想 LAN 間のフィルター規則をアクティブにします。

構文

mkvfilt -u

説明

mkvfilt コマンドは、**genvfilt** コマンドで定義した、仮想 LAN 間のフィルター規則をアクティブにします。

フラグ

-u フィルター・ルール・テーブル内のフィルター・ルールを活動化します。

終了状況

このコマンドは、以下の終了値を戻します。

0 正常終了。

>0 エラーが発生しました。

例

1. カーネル内のフィルター規則をアクティブにするには、次のコマンドを入力します。

```
mkvfilt -u
```

関連資料:

36 ページの『genvfilt コマンド』

pmconf コマンド

目的

最新フィックスを適用するためのテクノロジー・レベルと TNC サーバーを登録し、TNCPM 状況に関するレポートを生成することにより、トラステッド・ネットワーク接続パッチ管理 (TNCPM) サーバーのレポート作成と管理を行います。

注: サービス・パック・メタデータのダウンロードを可能にするために、TNCPM サーバーは 7100-02 テクノロジー・レベルの AIX バージョン 7.1 上でのみ実行する必要があります。

構文

pmconf mktncpm [**pmport=**<*port*>] **tncserver=***ip* | hostname **:** *port*

pmconf rmtncpm

pmconf start

pmconf stop

| **pmconf init -i** <*download interval*> **-l** <*TL List*> **-A** [**-P** <*download path*>] [**-x** <*ifix interval*>] [**-K**
| <*ifix key*>]

pmconf add -l *TL_list*

pmconf add -p <*SP List*> [**-U** <*user-defined SP path*>]

| **pmconf add -p** <*SP*> **-e** <*ifix file*>

| **pmconf add -y** <*advisory file*> **-v** <*signature file*> **-e** <*ifix tar file*>

pmconf delete -l *TL_list*

pmconf delete -p *<SP List>*

pmconf delete -p *<SP>***-e** *ifix file*

pmconf list -s [**-c**] [**-q**]

pmconf list -l *SP*

pmconf list -C

pmconf list -a *SP*

pmconf hist -u

pmconf hist -d

pmconf import -f *cert_filename* **-k** *key_filename*

pmconf export -f *filename*

pmconf modify -i *< download interval>*

pmconf modify -P *<download path>*

pmconf modify -g *<yes or no to accept all licenses>*

pmconf modify -t *<APAR type list>*

pmconf modify -x *<ifix interval>*

pmconf modify -K *<ifix key>*

pmconf delete -l *<TL list>*

pmconf restart

pmconf status

pmconf log loglevel = info | error | none

pmconf chtncpm attribute = *value*

説明

pmconf コマンドの機能は次のとおりです。

フィックス・リポジトリー管理
テクノロジー・レベルの登録または登録抹消、TNC サーバーの登録抹消を行います。 TNCPM は、テクノロジー・レベルごとに、そのテクノロジー・レベルの最新フィックス、**lslpp** 情報 (例えば、インストールされているファイルセットや、ファイルセットの更新に関する情報)、およびセキュリティー・フィックス情報を含むフィックス・リポジトリーを作成します。

レポート作成
TNCPM の状況に関するレポートを生成します。

pmconf コマンドを使用して、次の操作を実行できます。

項目	説明
追加	TNCPM を使用して新しいテクノロジー・レベルを登録します。
chtncpm	tnccs.conf ファイルの属性を変更します。 TNCPM サーバーで変更を有効にするには、明示的 **start** コマンドが必要です。
delete	TNCPM を使用してテクノロジー・レベルを登録抹消します。
history	更新およびダウンロードのヒストリーを表示します。
list	TNCPM に関する情報を表示します。
log	TNC コンポーネントのログ・レベルを設定します。
mktncpm	TNCPM サーバーを作成します。
modify	tncpm.conf 属性を変更します。
rmtncpm	TNCPM サーバーを除去します。
start	TNCPM サーバーを始動します。
stop	TNCPM サーバーを停止します。

フラグ

項目	説明
-A	クライアントの更新を実行するときにすべてのご使用条件を受け入れます。
-a <advisory file>	**ifix** パラメーターに対応する勧告ファイルを指定します。勧告ファイルが提供されていない場合、**ifix** パラメーターは暫定修正の Common Vulnerabilities and Exposures (CVE) アドレスとして表示されません。
-e <ifix file>	TNCPM に追加された暫定修正を指定します。
-i *download_interval*	登録済みテクノロジー・レベル用の新しいサービス・パックがあるかどうか TNCPM が検査する間隔を指定します。間隔は、分数を表す整数値、または「**d** (日数): **h** (時間数): **m** (分数)」の形式です。
-K <ifix key>	ダウンロードされた勧告および暫定修正の認証に使用する IBM AIX Product Security Incident Response Tool (PSIRT) の公開鍵を指定します。この公開鍵は、**0x28BFAA12** ID を使用して PGP 公開鍵サーバーからダウンロードすることができます。
-p *SP_list*	ダウンロードするサービス・パックのリストを指定します。このリストは、REL00-TL-SP の形式のコンマ区切りリストです (例えば、`6100-01-04` はテクノロジー・レベル 01 およびバージョン 6.1 のサービス・パック 04 を表しています)。 -U フラグを使用する場合は、SP を 1 つだけ指定します。
-t *APAR_type_list*	TNCPM がクライアント更新および TNC サーバー・リスト作成のためにサポートする、APAR タイプを指定します。セキュリティー APAR は常にサポートされます。APAR_type_list は、HIPER、FileNet® Process Engine、Enhancement の各タイプのコンマで区切られたリストです。
-P *fix_repository_path*	TNCPM によってダウンロードされるフィックス・リポジトリー用のダウンロード・ディレクトリーを指定します。デフォルトのディレクトリーは **/var/tnc/tncpm/fix_repository** です。
-U *user_defined_fix_repository*	ユーザー定義のフィックス・リポジトリーへのパスを指定します。クライアントの検証および更新に使用されるフィックス・リポジトリーに関連付けられているリリース、テクノロジー・レベル、およびサービス・パックを指定します。
-s	登録済みサービス・パックのレポートを生成します。
-l *SP*	サービス・パックに関する **lslpp** 情報のレポートを生成します。 *SP* の形式は REL00-TL-SP です (例えば、`6100-01-04` はテクノロジー・レベル 01 およびバージョン 6.1 のサービス・パック 04 を表しています)。
-u	クライアント更新ヒストリーのレポートを生成します。
-d	サービス・パックのダウンロード・ヒストリーのレポートを生成します。
-C	サーバー証明書のレポートを生成します。
-a *SP*	サービス・パックのセキュリティーに関するプログラム診断依頼書 (APAR) 情報のレポートを生成します。*SP* の形式は REL00-TL-SP です (例えば、`6100-01-04` はテクノロジー・レベル 01 およびバージョン 6.1 のサービス・パック 04 を表しています)。
-f *filename*	証明書ファイル名を指定します。
-k *key_filename*	インポート操作の場合は、証明書鍵を読み取る元のファイルを指定します。

-c	以下のように、コロン区切りレコードでユーザー属性を表示します。
	`# name: attribute1: attribute2: ...`
	`policy: value1: value2: ...`

-v <*signature file*>	IBM AIX ぜい弱性勧告の署名ファイルを指定します。
-y <*advisory file*>	IBM AIX ぜい弱性勧告ファイルを指定します。
-q	ヘッダー情報を抑止します。
-x <*ifix interval*>	新しい暫定修正がないか検査してダウンロードする間隔を分単位で指定します。この値が 0 に設定されている場合、暫定修正の自動ダウンロードおよび通知は使用不可になっています。デフォルトの間隔は、24 時間ごとです。

終了状況

このコマンドは、以下の終了値を戻します。

項目	説明
0	コマンドが正常に実行され、要求された変更がすべて行われました。
>0	エラーが発生しました。出力されるエラー・メッセージに、障害のタイプに関する詳細情報が示されます。

例

1. TNCPM を初期化するには、以下のコマンドを入力します。

   ```
   pmconf init -f 10080 -l 5300-11,6100-00
   ```

2. TNCPM デーモンを作成するには、以下のコマンドを入力します。

   ```
   mktncpm pmport=55777 tncserver=11.11.11.11:77555
   ```

3. サーバーを始動するには、以下のコマンドを入力します。

   ```
   pmconf start
   ```

4. サーバーを停止するには、以下のコマンドを入力します。

   ```
   pmconf stop
   ```

5. TNCPM を使用して新しいテクノロジー・レベルを登録するには、以下のコマンドを入力します。

   ```
   pmconf add -l 6100-01
   ```

6. TNCPM からテクノロジー・レベルを登録抹消するには、以下のコマンドを入力します。

   ```
   pmconf delete -l 6100-01
   ```

7. IP アドレス 11.11.11.11 を持つ TNC サーバーを TNCPM から登録抹消するには、以下のコマンドを入力します。

   ```
   pmconf delete -t 11.11.11.11
   ```

8. 以前のサービス・パックの新バージョンを TNCPM に登録するには、以下のコマンドを入力します。

   ```
   pmconf add -s 6100-01-04
   ```

9. TNCPM から以前のサービス・パックを登録抹消するには、以下のコマンドを入力します。

   ```
   pmconf delete -s 6100-01-04
   ```

10. 登録済みテクノロジー・レベルごとのフィックス・リポジトリーのレポートを生成するには、以下のコマンドを入力します。

    ```
    pmconf list -s
    ```

11. 登録済みテクノロジー・レベルの **lslpp** 情報のレポートを生成するには、以下のコマンドを入力します。

    ```
    pmconf list -l 6100-01-02
    ```

12. 更新ヒストリーからレポートを生成するには、以下のコマンドを入力します。

    ```
    pmconf hist -u
    ```

13. ダウンロード・ヒストリーからレポートを生成するには、以下のコマンドを入力します。

    ```
    pmconf hist -d
    ```

14. サーバー証明書のレポートを生成するには、以下のコマンドを入力します。

    ```
    pmconf list -C
    ```

15. サービス・パック・セキュリティー APAR 情報のレポートを生成するには、以下のコマンドを入力します。

    ```
    pmconf list -a 6100-01-02
    ```

16. サーバー証明書をインポートするには、以下のコマンドを入力します。

```
pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt
```

17. サーバー証明書をエクスポートするには、以下のコマンドを入力します。

```
pmconf export -f /tmp/server.txt
```

psconf コマンド

目的

トラステッド・ネットワーク接続 (TNC) サーバー、TNC クライアント、TNC IP Referrer (IPRef)、および Service Update Management Assistant (SUMA) のレポート作成と管理を行います。このコマンドは、ネットワークを脅威やアタックから保護するために、ネットワークの接続時または接続後のエンドポイント (サーバーおよびクライアント) の保全性に関するファイルセット管理ポリシーおよびパッチ管理ポリシーを管理します。

構文

TNC サーバーの操作:

psconf mkserver [**tncport=**<*port*>] **pmserver=**<*host*:*port*> [tsserver=<host>] [**recheck_interval=**<*time_in_minutes*> | **d** (days) : **h** (hours) : **m** (minutes)] [**dbpath** = <*user-defined directory*>]

psconf { **rmserver** | **status** }

psconf { **start** | **stop** | **restart** } **server**

psconf chserver attribute = *value*

psconf add -F <*FSPolicyname*> -r <*buildinfo*> [**apargrp=** [±]<*apargrp1, apargrp2.. >*] [*ifixgrp*=[+|-]<*ifixgrp1*,*ifixgrp2...>*]

psconf add { **-G** <*ipgroupname*> **ip=**[±]<*host1, host2...>* | {**-A**<*apargrp*> [**aparlist=**[±]*apar1, apar2...* | {**-V** <*ifixgrp*> [*ifixlist*=[+|-]*ifix1*,*ifix2...*]}

psconf add -P <*policyname*> { **fspolicy=**[±]<*f1,f2...>* | **ipgroup=**[±]<*g1,g2...>* }

psconf add -e *emailid* [-E FAIL | COMPLIANT | ALL] [**ipgroup=** [±]<*g1,g2...>*]

psconf add -I ip= [±]<*host1, host2...>*

psconf delete { **-F** <*FSPolicyname*> | **-G** <*ipgroupname*> | **-P** <*policyname*> | **-A** <*apargrp*> | **-V** <*ifixgrp*>}

psconf delete -H -i <*host* | **ALL**> **-D** <*yyyy-mm-dd*>

psconf certadd -i <*host*> **-t** <**TRUSTED** | **UNTRUSTED**>

psconf certdel -i <*host*>

psconf verify -i <*host*> | **-G** <*ipgroup*>

psconf update [-p] {-i< *host* >| **-G** <*ipgroup*> [**-r** <*buildinfo*> | **-a** <*apar1, apar2...>* | [**-u**] **-v** <*ifix1, ifix2,...>*}

| **psconf log loglevel=<info | error | none>**

| **psconf import -C -i** <*host*> **-f** <*filename*> | **–d** <*import database filename*>

| **psconf** { **import -k** <*key_filename*> | **export**} **-S -f** <*filename*>

| **psconf list** { **-S** | **-G** < *ipgroupname* | **ALL** > | **-F** < *FSPolicyname* | **ALL** > | **-P** < *policyname* | **ALL** > |
| **-r** < *buildinfo* | **ALL** > | **-I -i** < *ip* | **ALL** > | **-A** < *apargrp* | **ALL** > | **-V** <*ifixgrp*>} [**-c**] [**-q**]

| **psconf list** { **-H** | **-s** <**COMPLIANT** | **IGNORE** | **FAILED** | **ALL**> } **-i** <*host* | **ALL**> [**-c**] [**-q**]

| **psconf export -d** <*path to export directory*>

| **psconf report -v <CVEid|ALL> -o <TEXT|CSV>**

| **psconf report -A <advisoryname>**

| **psconf report -P <policyname|ALL> -o <TEXT|CSV>**

| **psconf report -i <ip|ALL> -o <TEXT|CSV>**

| **psconf report -B <buildinfo|ALL> -o <TEXT|CSV>**

| TNC クライアントの操作:

| **psconf mkclient** [**tncport=**<*port*>] **tncserver=**<*host:port*>

| **psconf mkclient tncport=**<*port*> -T

| **psconf** { **rmclient** | **status** }

| **psconf** {**start** | **stop** | **restart** } **client**

| **psconf chclient** attribute = *value*

| **psconf list** { **-C** | **-S** }

| **psconf export** { **-C** | **-S** } **-f** <*filename*>

| **psconf import** { **-S** | **-C -k** <*key_filename*> } **-f** <*filename*>

| TNC IPRef の操作:

| **psconf mkipref** [**tncport=**<*port*>] **tncserver=**<host:port>

| **psconf** { **rmipref** | **status**}

| **psconf** { **start** | **stop** | **restart**} ipref

| **psconf chipref** attribute = *value*

| **psconf** { **import -k** <*key_filename*> | **export** } **-R -f** <*filename*>

| **psconf list -R**

説明

TNC テクノロジーは、エンドポイントの認証、プラットフォームの保全性の計測、およびセキュリティー・システムの統合に関する、オープンな標準に基づいたアーキテクチャーです。TNC アーキテクチャーは、保護されたネットワーク上でエンドポイント (ネットワーク・クライアントおよびサーバー) を受け入れる前に、セキュリティー・ポリシーに準拠しているかどうかエンドポイントを検査します。仮想 I/O サーバー (VIOS) 上で新しい IP が検出されると、TNC IPRef は TNC サーバーにそのことを通知します。

SUMA を使用すると、システム管理者が Web からメンテナンス更新を手動で取得する作業が不要になります。システム管理者がフィックスをフィックス配布 Web サイトから各システムにダウンロードするための自動化インターフェースをセットアップできるようにする柔軟なオプションが提供されます。

psconf コマンドは、セキュリティー・ポリシーの追加または削除、トラステッドまたは非トラステッドとしてのクライアントの検証、レポートの生成、およびサーバーとクライアントの更新によって、ネットワーク・サーバーおよびクライアントを管理します。

psconf コマンドを使用して、次の操作を実行できます。

項目	説明
追加	ポリシー、クライアント、または E メール情報を TNC サーバーに追加します。
apargrp	TNC クライアントの検証に使用されるファイルセット・ポリシーの一部として APAR グループ名を指定します。
aparlist	APAR グループの一部である APAR のリストを指定します。
certadd	証明書にトラステッドまたは非トラステッドのマークを付けます。
certdel	クライアント情報を削除します。
chclient	`tnccs.conf` ファイルの属性を変更します。 TNC クライアントで変更を有効にするには、明示的 **start** コマンドが必要です。attribute=value の構文は、**mkclient** の構文と同じです。
chipref	`tnccs.conf` ファイルの属性を変更します。 IPRef で変更を有効にするには、明示的 **start** コマンドが必要です。attribute=value の構文は、**mkipref** の構文と同じです。
chserver	`tnccs.conf` ファイルの属性を変更します。 TNC サーバーで変更を有効にするには、明示的 **start** コマンドが必要です。attribute=value の構文は、**mkserver** の構文と同じです。 **注: dbpath** 属性は、**chserver** コマンドを使用して変更することはできません。この属性は、**mkserver** の実行中にのみ設定できます。
dbpath	TNC データベースの位置を指定します。デフォルト値は `/var/tnc` です。
delete	ポリシーまたはクライアント情報を削除します。
export	クライアントまたはサーバーの証明書、あるいは TNC サーバー上のデータベースをエクスポートします。
fspolicy	TNC クライアントの検証に使用される、リリース、テクノロジー・レベル、およびサービス・パックのファイルセット・ポリシーを指定します。
import	クライアントまたはサーバー上の証明書、あるいは TNC サーバー上のデータベースをインポートします。
ipgroup	複数の IP アドレスまたはホスト名を含むインターネット・プロトコル (IP) グループを指定します。
list	TNC サーバー、TNC クライアント、または SUMA に関する情報を表示します。
log	TNC コンポーネントのログ・レベルを設定します。
mkclient	TNC クライアントを構成します。
mkipref	TNC IPRef を構成します。
mkserver	TNC サーバーを構成します。
pmport	**pmserver** が listen するポート番号を指定します。デフォルト値は 38240 です。
pmserver	IBM® ECC Web サイトおよび IBM Fix Central Web サイトから入手可能な最新のサービス・パックとセキュリティー・フィックスをダウンロードする **suma** コマンドのホスト名または IP アドレスを指定します。
recheck_interval	TNC クライアントを検証する TNC サーバーの間隔を分単位または「d (日) : h (時間) : m (分)」のフォーマットで指定します。 **お願い: recheck_interval=0** の値は、スケジューラーがクライアントの検証を定期的に開始するのではなく、登録されたクライアントが始動時に自動的に検証されることを意味します。そのような場合、クライアントは手動で検証できます。

項目	説明
report	.txt または .csv ファイル拡張子を持つレポートを生成します。
restart	TNC クライアント、TNC サーバー、または TNC IPRef を再始動します。
rmclient	TNC クライアントを構成解除します。
rmipref	TNC IPRef を構成解除します。
rmserver	TNC サーバーを構成解除します。
start	TNC クライアント、TNC サーバー、または TNC IPRef を開始します。
status	TNC 構成の状況を表示します。
stop	TNC クライアント、TNC サーバー、または TNC IPRef を停止します。
tncport	TNC サーバーが listen するポート番号を指定します。デフォルト値は 42830 です。
tncserver	TNC クライアントを検証または更新する TNC サーバーを指定します。
tssserver	Trusted Surveyor サーバーの IP またはホスト名を指定します。
update	クライアントにパッチをインストールします。
verify	クライアントの手動検証を開始します。

フラグ

項目	説明
-A <advisoryName>	レポートの勧告的な名前を指定します。
-B <buildinfo>	パッチ・レポートを作成するための構築情報を指定します。

-c	以下のように、コロン区切りレコードでユーザー属性を表示します。
	`# name: attribute1: attribute2: ...`
	`policy: value1: value2: ...`

-C	操作の対象がクライアント・コンポーネントであることを指定します。
-d *database file location/dir path of database*	データベースのインポート用のファイル・パス・ロケーションを指定するか、またはデータベースのエクスポート用のディレクトリー・パス・ロケーションを指定します。
-D *yyyy-mm-dd*	ログ・ヒストリー内の特定のクライアント・エントリーに対して日付を指定します。ここで、*yyyy* は年、*mm* は月、*dd* は日です。
-e *emailid* **ipgroup=[±]***g1, g2...*	E メール ID とコンマ区切りの IP グループ名リストを続けて指定します。
-E | FAIL | COMPLIANT | ALL |	E メールを構成済み E メール ID に送信する必要がある場合のイベントを指定します。 FAIL - クライアントの検証状況が FAILED の場合にメールが送信されます。 COMPLIANT - クライアントの検証状況が COMPLIANT の場合にメールが送信されます。 ALL - メールはクライアント検証のすべての状況に対して送信されます。
-f *filename*	インポート操作の場合は証明書を読み取る元のファイルを指定し、エクスポート操作の場合は証明書を書き込む先の場所を指定します。
-F *fspolicy buildinfo*	ファイルシステム・ポリシー名とビルド情報を続けて指定します。ビルド情報は、次の形式で指定できます。 `6100-04-01` (ここで、`6100` はバージョン 6.1 を表し、`04` はメンテナンス・レベル、`01` はサービス・パックです)
-G *ipgroupname* **ip=[±]***ip1, ip2...*	IP グループ名と、コンマ区切りの IP リストを続けて指定します。
-H	ヒストリー・ログをリストします。
-i *host*	IP アドレスまたはホスト名を指定します。
-I ip=[±]*ip1, ip2...* | [±]host1,host2...	検証時に無視する必要がある IP/ホスト名を指定します。
-k *filename*	インポート操作の場合は、証明書鍵を読み取る元のファイルを指定します。
-p	TNC クライアントの更新をプレビューします。
-P <policyName>	クライアント・ポリシー・レポートを作成するためのポリシー名を指定します。
-q	ヘッダー情報を抑止します。

項目	説明
-r *buildinfo*	ビルド情報に基づいてレポートを生成します。ビルド情報は、次の形式で指定できます。 6100-04-01 (ここで、6100 はバージョン 6.1 を表し、04 はメンテナンス・レベル、01 はサービス・パックです)
-R	操作の対象が IPRef コンポーネントであることを指定します。
-s COMPLIANT | IGNORE | FAILED | ALL	次のように、クライアントを状況別に表示します。 **COMPLIANT** アクティブ・クライアントを表示します。 **IGNORE** いずれかの検証対象から除外されたクライアントを表示します。 **FAILED** 構成ポリシーに基づく検証に失敗したクライアントを表示します。 **ALL** 状況に関係なく、すべてのクライアントを表示します。
-S <host>	クライアント・セキュリティー・フィックス・レポートを作成するためのホスト名を指定します。
-t TRUSTED | UNTRUSTED	指定したクライアントにトラステッドまたは非トラステッドのマークを付けます。 **注:** サーバーまたはクライアントがトラステッドまたは非トラステッドであることの確認は、システム管理者のみが行うことができます。
-T	有効な証明書を持っている TS サーバーからの要求をクライアントが受け入れることができることを指定します。
-u	TNC クライアントにインストールした暫定修正をアンインストールします。
-v	コンマで区切られた暫定修正リストを指定します。
-V	暫定修正グループ名を指定します。

終了状況

このコマンドは、以下の終了値を戻します。

項目	説明
0	コマンドが正常に実行され、要求された変更がすべて行われました。
>0	エラーが発生しました。出力されるエラー・メッセージに、障害のタイプに関する詳細情報が示されます。

例

1. TNC サーバーを開始するには、以下のコマンドを入力します。

   ```
   psconf start server
   ```

2. ビルド 7100-04-02 に対してファイルシステム・ポリシー 71D_latest を追加するには、以下のコマンドを入力します。

   ```
   psconf add -F 71D_latest 7100-04-02
   ```

3. ファイルシステム・ポリシー 71D_old を削除するには、以下のコマンドを入力します。

   ```
   psconf delete -F 71D_old
   ```

4. IP アドレス 11.11.11.11 を持つクライアントが**トラステッド**であることを確認するには、以下のコマンドを入力します。

   ```
   psconf certadd -i 11.11.11.11 -t TRUSTED
   ```

5. IP アドレス 11.11.11.11 を持つクライアントをサーバーから削除するには、以下のコマンドを入力します。

   ```
   psconf certdel -i 11.11.11.11
   ```

6. IP アドレス 11.11.11.11 を持つクライアントの情報を検証するには、以下のコマンドを入力します。

   ```
   psconf verify -i 11.11.11.11
   ```

7. IP アドレス 11.11.11.11 を持つクライアントの情報を表示するには、以下のコマンドを入力します。

```
psconf list -i 11.11.11.11
```

8. **COMPLAINT** 状況にあるクライアントに関するレポートを生成するには、以下のコマンドを入力します。

   ```
   psconf list -s CPMPLIANT -i ALL
   ```

9. ビルド 7100-04-02 に関するレポートを生成するには、以下のコマンドを入力します。

   ```
   psconf list -r 7100-04-02
   ```

10. IP アドレス 11.11.11.11 を持つクライアントの接続ヒストリーを表示するには、以下のコマンドを入力します。

    ```
    psconf list -H -i 11.11.11.11
    ```

11. 2009 年 2 月 1 日またはそれより古い、IP アドレス 11.11.11.11 を持つクライアントのエントリーをログ・ヒストリーから削除するには、以下のコマンドを入力します。

    ```
    psconf delete -H -i 11.11.11.11 -D 2009-02-01
    ```

12. IP アドレス 11.11.11.11 を持つクライアントのクライアント証明書をサーバーからインポートするには、以下のコマンドを入力します。

    ```
    psconf import -C -i 11.11.11.11 -f /tmp/client.txt
    ```

13. クライアントからサーバー証明書をエクスポートするには、以下のコマンドを入力します。

    ```
    psconf export -S -f /tmp/server.txt
    ```

14. IP アドレス 11.11.11.11 を持つクライアントをサーバーからの適切なレベルに更新するには、以下のコマンドを入力します。

    ```
    psconf update -i 11.11.11.11
    ```

15. クライアントの状況を表示するには、以下のコマンドを入力します。

    ```
    psconf status
    ```

16. クライアント証明書を表示するには、以下のコマンドを入力します。

    ```
    psconf list -C
    ```

17. クライアントを開始するには、以下のコマンドを入力します。

    ```
    psconf start client
    ```

セキュリティー

RBAC ユーザーと Trusted AIX ユーザーへの注意:

このコマンドは特権命令を実行できます。特権命令を実行できるのは特権ユーザーのみです。許可と特権の詳細については、「セキュリティー」の『特権コマンド・データベース』を参照してください。このコマンドに関連する特権と許可のリストについては、**lssecattr** コマンドまたは **getcmdattr** サブコマンドを参照してください。

rmvfilt コマンド

目的

仮想 LAN 間のフィルター規則を、フィルター・テーブルから削除します。

構文

rmvfilt -n [**fid|all>**]

説明

rmvfilt コマンドは、仮想 LAN 間のフィルター規則を、フィルター・テーブルから削除するのに使用されます。

フラグ

-n 削除するフィルター規則の ID を指定します。**all** オプションは、すべてのフィルター規則を削除する場合に使用します。

終了状況

このコマンドは、以下の終了値を戻します。

0 正常終了。

>0 エラーが発生しました。

例

1. すべてのフィルター規則を削除する場合、またはカーネル内のすべてのフィルター規則を非アクティブにする場合は、次のコマンドを入力します。

   ```
   rmvfilt -n all
   ```

関連概念:

18 ページの『ルールの非アクティブ化』
トラステッド・ファイアウォール・フィーチャーで、VLAN 間ルーティングを使用可能にするルールを非アクティブにすることができます。

vlantfw コマンド

目的

IP およびメディア・アクセス制御 (MAC) マッピング情報を表示または消去し、ロギング機能を制御します。

構文

vlantfw -h | -s | -t | -d | -f | -G | -q | -D | -E | -F | -i | -l | -L | -m | -M | -N *integer*

説明

vlantfw コマンドは、IP および MAC マッピング・エントリーを表示または消去します。また、このコマンドにより、トラステッド・ファイアウォールのロギング機能を開始または停止することもできます。

フラグ

-d IP マッピング情報をすべて表示します。

-D 収集した接続データを表示します。

-E さまざまな中央処理装置上のロジカル・パーティション (LPAR) 間の接続データを表示します。

-f IP マッピング情報をすべて削除します。

-F 接続データのキャッシュをクリアします。

-G トラステッド・ファイアウォールを使用して、トラフィックを内部的にルーティングするために構成できるフィルター規則を表示します。

-I 異なる VLAN ID に関連付けられているが、同一の中央処理装置を共有する LPAR 間の接続データを表示します。

-l トラステッド・ファイアウォールのロギング機能を開始します。

-L トラステッド・ファイアウォールのロギング機能を停止し、トレース・ファイルの内容を /home/padmin/svm/svm.log ファイルにリダイレクトします。

-m トラステッド・ファイアウォール・モニターを使用可能にします。

-M トラステッド・ファイアウォール・モニターを使用不可にします。

-q セキュアな仮想マシンの状況を照会します。

-s トラステッド・ファイアウォールを開始します。

-t トラステッド・ファイアウォールを停止します。

パラメーター

-N *integer*
指定された整数に対応するフィルター規則を表示します。

終了状況

このコマンドは、以下の終了値を戻します。

0 正常終了。

>0 エラーが発生しました。

例

1. すべての IP マッピングを表示するには、次のコマンドを入力します。
   ```
   vlantfw -d
   ```
2. すべての IP マッピングを除去するには、次のコマンドを入力します。
   ```
   vlantfw -f
   ```
3. トラステッド・ファイアウォールのロギング機能を開始するには、次のコマンドを入力します。
   ```
   vlantfw -l
   ```
4. セキュアな仮想マシンの状況を検査するには、次のコマンドを入力します。
   ```
   vlantfw -q
   ```
5. トラステッド・ファイアウォールを開始するには、次のコマンドを入力します。
   ```
   vlantfw -s
   ```
6. トラステッド・ファイアウォールを停止するには、次のコマンドを入力します。
   ```
   vlantfw -t
   ```
7. 中央処理装置内のトラフィックをルーティングするフィルターの生成に使用可能な、対応する規則を表示するには、次のコマンドを入力します。
   ```
   vlantfw -G
   ```

関連資料:

36 ページの『genvfilt コマンド』

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。 日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。 本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。 これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。 本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。 実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。 国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。 本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。 それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Dept. LRAS/Bldg. 903
11501 Burnet Road

Austin, TX 78758-3400
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。 そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。 実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。 IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、 現行価格であり、通知なしに変更されるものです。 卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。 記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。 より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。 このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。 従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。サンプル・プログラムは、いかなる種類の保証なしに、現存するままの状態で提供されます。 IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. _年を入れる_.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

プライバシー・ポリシーに関する考慮事項

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。 IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらのCookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。

この「ソフトウェア・オファリング」は、Cookie もしくはその他のテクノロジーを使用して個人情報を収集することはありません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie などの各種テクノロジーの使用について詳しくは、『IBM オンラインでのプライバシー・ステートメントのハイライト』(http://www.ibm.com/privacy/jp/ja/)、『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』というタイトルのセクション、および『IBM Software Products and Software-as-a-Service Privacy Statement』(http://www.ibm.com/software/info/product-privacy) を参照してください。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corp. の商標です。 他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。 現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml の「Copyright and trademark information」をご覧ください。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

Java およびすべての Java 関連の商標およびロゴは、Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

[ナ行]

[ハ行]

[マ行]

[ラ行]

A

C

G

I

L

M

P

R

S

T

V

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21