IBM PowerSC

Standard Edition

Versão 1.1.3

PowerSC Standard Edition

IBM PowerSC

Standard Edition

Versão 1.1.3

PowerSC Standard Edition

Nota
Antes de utilizar estas informações e o produto suportado por elas, leia as informações no “Avisos” na página 47.

Esta edição se aplica ao IBM PowerSC Versão 1.1.3 e a todas as liberações e modificações subsequentes até que seja indicado de maneira diferente em novas edições.

© Copyright IBM Corporation 2012, 2013.

Índice

Sobre este documento v

IBM PowerSC Standard Edition 1.1.3 . . 1

O que há de novo em PowerSC Standard Edition 1.1.3 1
Conceitos do PowerSC Standard Edition 1.1.3 . . . 2
Instalando o PowerSC Standard Edition 1.1.3 . . . 3
Inicialização Confiável 4
Conceitos de Inicialização Confiável 4
Planejamento para Inicialização Confiável . . . 5
Instalando a Inicialização Confiável. 6
Configurando a Inicialização Confiável 7
Gerenciando a Inicialização Confiável 8
Resolvendo Problemas de Inicialização Confiável 9
Firewall Confiável 10
Conceitos de Firewall Confiável 10
Instalando o Firewall Confiável. 12
Configurando o Firewall Confiável 13
Criação de Log Confiável. 17
Logs Virtuais 17
Detectando os Dispositivos de Log Virtual . . . 18
Instalando a Criação de Log Confiável 18
Configurando a Criação de Log Confiável . . . 19
Trusted Network Connect e Gerenciamento de Correção 20
Conceitos do Trusted Network Connect 20
Instalando o Trusted Network Connect 23
Configurando Trusted Network Connect e Gerenciamento de Correção 23
Gerenciando Trusted Network Connect e Gerenciamento de Correção 27
TNC Server Reporting. 30
Resolução de Problemas no Trusted Network Connect e Gerenciamento de Correção 30
Comandos do PowerSC Standard Edition 31
Comando chvfilt. 31
Comando genvfilt 33
Comando lsvfilt 34
Comando mkvfilt 35
Comando pmconf 35
Comando psconf 39
Comando rmvfilt 44
Comando vlantfw 45

Avisos 47
Considerações sobre Política de Privacidade . . . 49
Marcas Registradas 49

Índice Remissivo 51

© Copyright IBM Corp. 2012, 2013

Sobre este documento

Este documento fornece aos administradores do sistema as informações completas sobre o arquivo, o sistema e a segurança de rede.

Destaque

As convenções de destaque a seguir são utilizadas neste documento:

Negrito	Identifica comandos, sub-rotinas, palavras-chave, arquivos, estruturas, diretórios e outros itens cujos nomes são predefinidos pelo sistema. Também identifica objetos gráficos como botões, etiquetas e rótulos que o usuário seleciona.
Itálico	Identifica os parâmetros cujos nomes ou valores reais devem ser fornecidos pelo usuário.
`Espaço Simples`	Identifica exemplos de valores de dados específicos, exemplos de textos semelhantes aos que são exibidos, exemplos de partes de código do programa semelhantes ao que você pode gravar como um programador, mensagens do sistema ou informações que devem realmente ser inseridas.

Diferenciação entre maiúsculas e minúsculas no AIX

Tudo no sistema operacional do AIX funciona com distinção entre maiúsculas e minúsculas, o que significa que ele identifica uso de letras maiúsculas e minúsculas. Por exemplo, é possível utilizar o comando **ls** para listar arquivos. Se você digitar `LS`, o sistema responderá que o comando `não foi localizado`. Da mesma forma, `FILEA`, `FiLea` e `filea` são três nomes de arquivos distintos, mesmo se eles residirem no mesmo diretório. Para evitar causar a execução de ações indesejáveis, sempre assegure-se de usar maiúsculas e minúsculas corretamente.

ISO 9000

Os sistemas de qualidade registrados ISO 9000 foram utilizados no desenvolvimento e fabricação deste produto.

© Copyright IBM Corp. 2012, 2013

IBM PowerSC Standard Edition 1.1.3

O IBM® PowerSC Standard Edition inclui recursos de Inicialização Confiável, Firewall Confiável, Criação de Log Confiável, Conexão de Rede Confiável e Gerenciamento de Correção e Segurança e Automação de Conformidade.

O que há de novo em PowerSC Standard Edition 1.1.3

Leia sobre informações novas ou significantes alteradas para a coleção de tópicos do PowerSC Standard Edition Versão 1.1.3.

Nesse arquivo PDF, é possível ver barras de revisão (|) na margem esquerda que identificam as informações novas e alteradas.

Dezembro de 2013

- Atualizados os requisitos do sistema em "Conceitos do PowerSC Standard Edition 1.1.3" na página 2.
- Identificada uma substituição de arquivo de Inicialização Confiável necessária ao reinstalar o sistema operacional AIX em "Pré-requisito de Inicialização Confiável" na página 5.
- Informações incluídas sobre a função de monitoramento de Firewall Confiável em "Monitoramento de Firewall Confiável" na página 13.
- Informações incluídas sobre a função de criação de log do Firewall Confiável em "Criação de Log de Firewall Confiável" na página 13.
- Incluído o tópico "Instalando a Criação de Log Confiável" na página 18.
- Informações incluídas sobre as atualizações provisórias de correção para Trusted Network Connect em "Configurando o Servidor do Gerenciamento de Correção" na página 24.
- Informações incluídas sobre o relatório do servidor Trusted Network Connect em "TNC Server Reporting" na página 30.
- Informações incluídas sobre a instalação do verificador Trusted Network Connect em "Instalando o Verificador" na página 7.
- Incluídos os comandos do Firewall Confiável em "Comandos do PowerSC Standard Edition" na página 31.
- Renomeado o comando **tscpmconsole** para o comando **pmconf**e incluídas suas informações em "Comando pmconf" na página 35.
- Renomeado o comando **tscconsole** para o comando **psconf** e incluídas suas informações em "Comando psconf" na página 39.
- Informações atualizadas sobre as opções para o comando **vlantfw** em "Comando vlantfw" na página 45.

Novembro de 2012

Atualizadas as informações no tópico "Trusted Network Connect e Gerenciamento de Correção" na página 20.

Maio de 2012

Incluída a documentação para o novo recurso para "Firewall Confiável" na página 10.

© Copyright IBM Corp. 2012, 2013

Conceitos do PowerSC Standard Edition 1.1.3

Esta visão geral do PowerSC Standard Edition explica os recursos, componentes e suporte de hardware relacionados ao recurso PowerSC Standard Edition.

O PowerSC Standard Edition fornece segurança e controle dos sistemas operacionais em uma nuvem ou em centros de dados virtualizados e fornece uma visualização corporativa e capacidades de gerenciamento. O PowerSC Standard Edition é um conjunto de recursos que inclui Segurança e Automação de Conformidade, Inicialização Confiável, Firewall Confiável, Criação de Log Confiável e Conexão de Rede Confiável e Gerenciamento de Correção. A tecnologia de segurança que é colocada na camada de virtualização fornece segurança adicional para sistemas independentes.

A tabela a seguir fornece detalhes sobre as edições, os recursos incluídos nas edições, os componentes e o hardware baseado em processador nos quais cada componente fica disponível.

Tabela 1. Componentes PowerSC Standard Edition, Descrição, Suporte do Sistema Operacional e Suporte de Hardware

Componentes	Descrição	Sistema Operacional Suportado	Hardware Suportado
Segurança e Automação de Conformidade	Automatiza a configuração, o monitoramento e a auditoria de segurança e configuração de conformidade dos padrões a seguir: • Payment Card Industry Data Security Standard (PCI DSS) • Sarbanes-Oxley Act and COBIT compliance (SOX/COBIT) • U.S. Department of Defense (DoD) STIG • Health Insurance Portability and Accountability Act (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6 • POWER7
Inicialização Confiável	Mede a imagem de inicialização, sistema operacional e os aplicativos e atesta suas confianças usando a tecnologia virtual Trusted Platform Module (TPM).	• AIX 6 com 6100-07 ou mais recente • AIX 7 com 7100-01 ou mais recente	POWER7 firmware eFW7.4 ou mais recente
Firewall Confiável	Economiza tempo e recursos ativando o roteamento direto nas Virtual LANs (VLANs) especificadas que são controladas pelo mesmo Virtual I/O Server.	• AIX 6.1 • AIX 7.1 • VIOS Versão 2.2.1.4 ou mais recente	• POWER6 • POWER7 • Virtual I/O Server Versão 6.1S, ou mais recente
Criação de Log Confiável	Os logs de AIX estão localizados centralmente no Virtual I/O Server (VIOS) em tempo real. Este recurso fornece criação de log à prova de violação e conveniente backup de log e gerenciamento.	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6 • POWER7

Tabela 1. Componentes PowerSC Standard Edition, Descrição, Suporte do Sistema Operacional e Suporte de Hardware (continuação)

Componentes	Descrição	Sistema Operacional Suportado	Hardware Suportado
Trusted Network Connect e Gerenciamento de Correção	Verifica se todos os sistemas AIX no ambiente virtual estão no software especificado e nível da correção e fornece ferramentas de gerenciamento para assegurar que todos os sistemas AIX estejam no nível de software especificado. Fornece alertas se um sistema virtual de nível inferior for incluído na rede ou se for emitida a correção de segurança que afeta os sistemas.	• AIX 5.3 • AIX 6.1 • AIX 7.1 O cliente Trusted Network Connect requer um dos componentes a seguir: • AIX 6.1 com 6100-06 ou mais recente • O sistema de console AIX versão 7.1 Service Update Management Assistant (SUMA) no ambiente SUMA para o gerenciamento de correção	• POWER5 • POWER6 • POWER7

Instalando o PowerSC Standard Edition 1.1.3

Você deve instalar um conjunto de arquivos para cada função específica do PowerSC Standard Edition.

Os conjuntos de arquivos a seguir estão disponíveis para PowerSC Standard Edition:

- `powerscExp.ice`: Instalado em sistemas AIX que requerem o recurso de Segurança e Automação de Conformidade do PowerSC Standard Edition.
- `powerscStd.vtpm`: Instalado em sistemas AIX que requerem o recurso de Inicialização Confiável do PowerSC Standard Edition.
- `powerscStd.vlog`: Instalado em sistemas AIX que requerem o recurso de Criação de Log Confiável do PowerSC Standard Edition.
- `powerscStd.tnc_pm`: Instalado no AIX Versão 6.1 com o Nível de Tecnologia 6100-06, ou superior, ou no sistema de console AIX Versão 7.1 Service Update Management Assistant (SUMA) no ambiente SUMA para o gerenciamento de correção.
- `powerscStd.svm`: Instalado nos sistemas AIX que podem se beneficiar do recurso de roteamento de PowerSC Standard Edition.

Instale o PowerSC Standard Edition usando uma das interfaces a seguir:

- O comando **installp** a partir da interface da linha de comandos (CLI)
- A interface SMIT

Para instalar o PowerSC Standard Edition usando a interface SMIT, conclua as etapas a seguir:

1. Execute o comando a seguir:
   ```
   % smitty installp
   ```
2. Selecione a opção **Instalar Software**.
3. Selecione o dispositivo de entrada ou o diretório para o software especificar o local ou o arquivo de instalação da imagem de instalação IBM Compliance Expert. Por exemplo, se a imagem de instalação tiver o caminho do diretório e o nome do arquivo `/usr/sys/inst.images/powerscStd.vtpm`, você deve especificar o caminho do diretório no campo **INPUT**.
4. Visualize e aceite o contrato de licença. Aceite o contrato de licença usando a seta para baixo para selecionar **Novos Contratos de Licença ACCEPT** e pressione a tecla tab para alterar o valor para **Sim**.
5. Pressione **Enter** para iniciar a instalação.
6. Verifique se o status de comando é **OK** depois que a instalação é concluída.

Visualizando a Licença da Software

A licença de software pode ser visualizada na CLI usando o comando a seguir:

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

Em que *path/filename* especifica a imagem de instalação PowerSC Standard Edition.

Por exemplo, você pode inserir o comando a seguir usando a CLI para especificar as informações sobre licença relacionadas ao PowerSC Standard Edition:

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

Conceitos relacionados:

"Conceitos do PowerSC Standard Edition 1.1.3" na página 2
Esta visão geral do PowerSC Standard Edition explica os recursos, componentes e suporte de hardware relacionados ao recurso PowerSC Standard Edition.

"Instalando a Inicialização Confiável" na página 6
Existem algumas configurações de hardware e de software que são necessárias para instalar a Inicialização Confiável.

"Instalando o Trusted Network Connect" na página 23
Instalar os componentes do Trusted Network Connect (TNC) requer que você conclua certas etapas.

Tarefas relacionadas:

"Instalando o Firewall Confiável" na página 12
Instalar o PowerSC Trusted Firewall é semelhante à instalar outros recursos PowerSC.

"Instalando a Criação de Log Confiável" na página 18
É possível instalar o recurso PowerSC Trusted Logging usando a interface de linha de comandos ou a ferramenta SMIT.

Inicialização Confiável

O recurso Inicialização Confiável usa o Virtual Trusted Platform Module (VTPM), que é uma instância virtual do TMP do Trusted Computing Group. O VTPM é usado para armazenar com segurança as medições de inicialização do sistema para futura verificação.

Conceitos de Inicialização Confiável

É importante entender a integridade do processo de inicialização e como classificar a inicialização de uma inicialização confiável ou uma inicialização não confiável.

É possível configurar um máximo de 60 partições lógicas ativadas por VTPM (LPAR) para cada sistema físico usando o Hardware Management Console (HMC). Quando configurado, o VTPM é exclusivo para cada LPAR. Quando usado com a tecnologia AIX Trusted Execution, o VTPM fornecerá a segurança e a garantia para as partições a seguir:

- A imagem de inicialização no disco
- O sistema operacional inteiro
- As camadas de aplicativo

Um administrador pode visualizar os sistemas confiáveis e não confiáveis a partir de um console central que é instalado com o verificador **openpts** disponível no pacote de expansão AIX. O console **openpts** gerencia um ou mais servidores Power Systems e monitora ou atesta o estado confiável dos sistemas AIX em todo o datacenter. O atestado é o processo no qual o verificador determina (ou atesta) se um coletor executou uma inicialização confiável.

Status de Inicialização Confiável

Uma partição é considerada confiável, se o verificador atestar com êxito a integridade do coletor. O verificador é a partição remota que determina se um coletor executou uma inicialização confiável. O coletor é a partição AIX que possui um Virtual Trusted Platform Module (VTPM) anexado e o Trusted Software Stack (TSS) instalado. Ele indica que as medições registradas no VTPM correspondem a um conjunto de referência retido pelo verificador. Um estado de inicialização confiável indica se a partição foi inicializada de uma maneira confiável. Essa instrução é sobre a integridade do processo de inicialização do sistema e não indica o nível atual ou contínuo da segurança do sistema.

Status de Inicialização Não Confiável

Uma partição entra em um estado não confiável se o verificador não puder atestar com êxito a integridade do processo de inicialização. O estado não confiável indica que alguns aspectos do processo de inicialização são inconsistentes com as informações de referência retidas pelo verificador. As causas possíveis para um atestado com falha incluem a inicialização de um dispositivo de inicialização diferente, inicializando uma imagem de kernel diferente e alterando a imagem de inicialização existente.

Conceitos relacionados:

"Resolvendo Problemas de Inicialização Confiável" na página 9
Existem alguns cenários comuns e etapas corretivas que são necessários para ajudar a identificar a razão para a falha de atestado ao usar a Inicialização Confiável.

Planejamento para Inicialização Confiável

Aprenda sobre as configurações de hardware e de software que são necessárias para instalar a Inicialização Confiável.

Pré-requisito de Inicialização Confiável

A instalação da Inicialização Confiável envolve configurar o coletor e o verificador.

Ao preparar para reinstalar o sistema operacional AIX em um sistema com a Inicialização Confiável já instalada, você deve copiar o arquivo `/var/tss/lib/tpm/system.data` e usá-lo para substituir o arquivo no mesmo local depois que a reinstalação for concluída. Se você não copiar este arquivo, você deve remover o Módulo da Plataforma Confiável virtualizado do console de gerenciamento e reinstalá-lo na partição.

Coletor

Os requisitos de configuração para instalar um coletor envolvem os pré-requisitos a seguir:

- O hardware POWER7 que está sendo executado em uma liberação de firmware 740.
- Instale o IBM AIX 6 com Tecnologia Nível 7 ou instale o IBM AIX 7 com Tecnologia Nível 1.
- Instale o Hardware Management Console (HMC) versão 7.4 ou mais recente.
- Configure a partição com VTPM e um mínimo de 1 GB de memória.
- Instale o Secure Shell (SSH), especificamente OpenSSH ou equivalente.

Verificador

O verificador **openpts** pode ser acessado a partir da interface da linha de comandos e da interface gráfica com o usuário que foi projetada para execução em um intervalo de plataformas. A versão AIX do verificador OpenPTS está disponível no pacote de expansão AIX. As versões do verificador OpenPTS para Linux e outras plataformas estão disponíveis através de um download da web. Os requisitos de configuração incluem os pré-requisitos a seguir:

- Instale o SSH, especificamente OpenSSH ou equivalente.
- Estabeleça a conectividade de rede (através SSH) para o coletor.

- Instale o Java™ 1.6 ou posterior para acessar o console **openpts** a partir da interface gráfica.

Preparando para Correção

As informações de Inicialização Confiável que estão descritas aqui servem como guia para identificar as situações que podem precisar de correção. Não afeta o processo de inicialização.

Existem várias circunstâncias que podem fazer com que o atestado falhe e é difícil prever a circunstância que você pode encontrar. Você deve decidir sobre a ação apropriada dependendo da circunstância. No entanto, é uma boa prática preparar alguns dos cenários graves e fazer com quem uma política ou um fluxo de trabalho ajude a manipular esses incidentes. A correção é uma ação corretiva que deve ser executada quando o atestado relatar um ou mais coletores não confiáveis.

Por exemplo, se ocorreu uma falha de atestado devido à imagem de inicialização diferente da referência do verificador, considere ter respostas para as perguntas a seguir:

- Como você pode verificar se a ameaça é crível?
- Ocorreu alguma manutenção planejada que tenha sido executada, um upgrade AIX ou novo hardware que tenha sido instalado recentemente.
- Você pode contatar o administrador que possui acesso a essas informações?
- Quando o sistema foi inicializado pela última vez em um estado confiável?
- Se a ameaça de segurança parece legítima, qual ação você deve executar? (As sugestões incluem a coleta de logs de auditoria, desconectando o sistema da rede, desligando o sistema e alertando os usuários).
- Havia algum outro sistema comprometido que deveria ser verificado?

Conceitos relacionados:

"Resolvendo Problemas de Inicialização Confiável" na página 9
Existem alguns cenários comuns e etapas corretivas que são necessários para ajudar a identificar a razão para a falha de atestado ao usar a Inicialização Confiável.

Considerações de Migração

Considere esses pré-requisitos antes de migrar uma partição que esteja ativada para Virtual Trusted Platform Module (VTPM).

Uma vantagem de um VTPM sobre um TPM físico que permite que a partição mova entre os sistemas enquanto retém o VTPM. Para migrar com segurança a partição lógica, o firmware criptografa os dados VTPM antes da transmissão. Para assegurar uma migração segura, as medidas de segurança a seguir devem ser implementadas antes da migração:

- Ative IPSEC entre o Virtual I/O Server (VIOS) que está executando a migração.
- Configure a chave do sistema confiável através do Hardware Management Console (HMC) para controlar os sistemas gerenciados que são capazes de descriptografar os dados VTPM após a migração. O sistema de destino de migração deve ter a mesma chave que o sistema de origem para migrar com êxito os dados.

Informações relacionadas:

Usando o HMC

Migração VIOS

Instalando a Inicialização Confiável

Existem algumas configurações de hardware e de software que são necessárias para instalar a Inicialização Confiável.

Informações relacionadas:

"Instalando o PowerSC Standard Edition 1.1.3" na página 3
Você deve instalar um conjunto de arquivos para cada função específica do PowerSC Standard Edition.

Instalando o Coletor

Você deve instalar o coletor usando o conjunto de arquivos a partir do CD base AIX.

Para instalar o coletor, instale os pacotes `powerscStd.vtpm` e `openpts.collector` que estão no CD base, usando o comando **smit** ou **installp**.

Instalando o Verificador

O componente do verificador OpenPTS é executado no sistema operacional AIX e em outras plataformas.

A versão AIX do verificador pode ser instalada a partir do conjunto de arquivos usando o pacote de expansão AIX. Para instalar o verificador no sistema operacional AIX, instale o pacote `openpts.verifier` a partir do pacote de expansão AIX, usando o comando **smit** ou **installp**. Isso instala ambas as versões da interface gráfica e linha de comandos do verificador.

O verificador OpenPTS para outros sistemas operacionais pode ser transferido por download a partir do `Download Linux OpenPTS Verifier For Use With AIX Trusted Boot`.

Informações relacionadas:

Download do Verificador Linux OpenPTS para Uso com Inicialização Confiável AIX

Configurando a Inicialização Confiável

Aprenda o procedimento para inscrever um sistema e atestar um sistema para Inicialização Confiável.

Inscrevendo um Sistema

Aprenda o procedimento para inscrever um sistema com o verificador.

Inscrever um sistema é o processo de fornecer um conjunto inicial de medidas ao verificador, que forma a base para as solicitações de atestado subsequente. Para inscrever um sistema a partir da linha de comandos, use o comando a seguir a partir do verificador:

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

As informações sobre a partição inscrita estão localizadas no diretório `$HOME/.openpts`. Cada nova partição é designada a um identificador exclusivo durante o processo de inscrição e as informações relacionadas às partições inscritas ficam armazenadas no diretório correspondente ao ID exclusivo.

Para inscrever um sistema a partir da interface gráfica, conclua as etapas a seguir:

1. Ative a interface gráfica usando o comando **/opt/ibm/openpts_gui/openpts_GUI.sh**.
2. Selecione **Inscrever** no menu de navegação.
3. Insira o nome do host e as credenciais SSH do sistema.
4. Clique em **Inscrever**.

Conceitos relacionados:

"Atestando um Sistema"
Aprenda o procedimento para atestar um sistema a partir da linha de comandos e usando a interface gráfica.

Atestando um Sistema

Aprenda o procedimento para atestar um sistema a partir da linha de comandos e usando a interface gráfica.

Para consultar a integridade de uma inicialização do sistema, use o comando a seguir a partir do verificador:

```
openpts <hostname>
```

Para atestar um sistema a partir da interface gráfica, conclua as etapas a seguir:

1. Selecione uma categoria a partir do menu de navegação.
2. Selecione um ou mais sistemas a serem atestado.
3. Clique em **Atestar**.

Inscrevendo e Atestando um Sistema sem uma Senha

A solicitação de atestado é enviada através do Shell Seguro (SSH). Instale o certificado do verificador no coletor para permitir as conexões SSH sem uma senha.

Para configurar o certificado do verificador no sistema do coletor, conclua as etapas a seguir:

- No verificador, execute os comandos a seguir:

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

- No coletor, execute o comando a seguir:

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

Gerenciando a Inicialização Confiável

Aprenda o procedimento para gerenciar os resultados de atestado de Inicialização Confiável.

Interpretando Resultados de Atestado

Aprenda o procedimento para visualizar e entender os resultados de atestado.

Um atestado pode resultar em um dos estados a seguir:

1. A solicitação de atestado falhou: A solicitação de atestado não foi concluída com êxito. Consulte a seção Resolução de Problemas para entender as possíveis causas para a falha.
2. Validade da integridade do sistema: O atestado foi concluído com êxito e a inicialização do sistema corresponde às informações de referência que são retidas pelo verificador. Isso indica uma Inicialização Confiável bem-sucedida.
3. Integridade do sistema inválida: A solicitação de atestado foi concluída, mas foi detectada uma discrepância entre as informações que são coletadas durante a inicialização do sistema e as informações de referência que são retidas pelo verificador. Isso indica uma inicialização não confiável.

O atestado também relata se uma atualização foi aplicada no coletor usando a mensagem a seguir:

Atualização do sistema disponível: Esta mensagem indica que uma atualização foi aplicada no coletor e um conjunto de informações de referência atualizada está disponível, o que é efetivo para a próxima inicialização. O usuário é solicitado no verificador a aceitar ou rejeitar as atualizações. Por exemplo, o usuário pode optar por aceitar essas atualizações, se o usuário estiver ciente da manutenção que ocorre no coletor.

Para investigar uma falha de atestado usando uma interface gráfica, conclua as etapas a seguir:

1. Selecione uma categoria a partir do menu de navegação.
2. Selecione um sistema a ser investigado.
3. Clique duas vezes na entrada correspondente ao sistema. Uma janela propriedades é exibida. Essa janela contém informação de log sobre o atestado com falha.

Excluindo os Sistemas

Aprenda o procedimento para excluir um sistema do banco de dados do verificador.

Para remover um sistema a partir do banco de dados do verificador, execute o comando:

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

Resolvendo Problemas de Inicialização Confiável

Existem alguns cenários comuns e etapas corretivas que são necessários para ajudar a identificar a razão para a falha de atestado ao usar a Inicialização Confiável.

O comando **openpts** declara um sistema como inválido se o estado de inicialização atual do sistema não corresponder às informações de referência retidas no verificador. O comando **openpts** determina o possível motivo para que a integridade seja inválida. Existem diversas variáveis em uma inicialização AIX integral e um atestado com falha requer análise para determinar a causa da falha.

A tabela a seguir lista alguns dos cenários comuns e etapas reparatórias para identificar o motivo para a falha:

Tabela 2. Resolução de Problemas de Alguns dos Cenários Comuns para a Falha

Motivo para a Falha	**Possíveis Causas da Falha**	**Correção Sugerida**

Atestado não concluído.	• Nome do host incorreto.
	• Nenhuma rota de rede entre a origem e o destino.
	• Credenciais de segurança incorretas.
		Verifique a conexão Secure Shell (SSH) usando o comando a seguir:
		`ssh ptsc@hostname`
		
		Se a conexão SSH for bem-sucedida, verifique os motivos a seguir para falha de atestado:
		• O sistema que está sendo atestado não está executando o daemon **tcsd**.
		• O sistema que está sendo atestado não foi inicializado pelo comando **ptsc**. Este processo deve ocorrer automaticamente durante a inicialização do sistema, mas verifique a presença de um diretório `/var/ptsc/` no coletor. Se o diretório `/var/ptsc/` não existir, execute o comando a seguir no coletor:
		`ptsc -i`

O firmware CEC foi alterado.	• O upgrade de firmware foi aplicado. • O LPAR foi migrado para um sistema que estava executando uma versão diferente do firmware.	Verifique o nível de firmware do sistema que está hospedando o LPAR.
Os recursos alocados para o LPAR foram alterados.	A CPU ou a memória alocada para LPAR foi alterada.	Verifique o perfil de partição no HMC.
O firmware alterado para os adaptadores que estão disponíveis no LPAR.	O dispositivo de hardware foi incluído ou removido do LPAR.	Verifique o perfil de partição no HMC.
A lista de dispositivos anexados ao LPAR foi alterada.	O dispositivo de hardware foi incluído ou removido do LPAR.	Verifique o perfil de partição no HMC.

Tabela 2. Resolução de Problemas de Alguns dos Cenários Comuns para a Falha (continuação)

Motivo para a Falha	Possíveis Causas da Falha	Correção Sugerida
Foi alterada a imagem de inicialização, que inclui o kernel do sistema operacional.	• Uma atualização AIX foi aplicada e o verificador não reconheceu a atualização. • O comando **bosboot** foi executado.	• Confirme com o administrador do coletor se alguma manutenção foi executada antes da mais recente operação de reinicialização. • Verifique os logs no coletor para atividade de manutenção.
O LPAR é inicializado de um dispositivo diferente.	• A inscrição foi executada imediatamente após a instalação de rede. • O sistema é inicializado a partir de um dispositivo de manutenção.	O dispositivo de inicialização e os sinalizadores podem ser verificados usando o comando **bootinfo**. Se a inscrição foi executada imediatamente após a instalação Network Installation Management (NIM) e antes da operação de reinicialização, os detalhes inscritos pertencem à instalação de rede e não à próxima inicialização de disco. Esta inscrição pode ser reparada removendo a inscrição e reinscrevendo a partição lógica.
O menu de inicialização System Management Services (SMS) interativa foi chamado.		O processo de inicialização deve ser executado de maneira ininterrupta sem que a interação do usuário seja confiável. Inserir o menu de inicialização SMS faz com que a inicialização seja inválida.
O banco de dados de execução confiável (TE) foi alterado.	• Os arquivos binários foram incluídos ou removidos do banco de dados TE. • Os arquivos binários no banco de dados foram atualizados.	Execute o comando **trustchk** para verificar o banco de dados.

Conceitos relacionados:

"Preparando para Correção" na página 6
As informações de Inicialização Confiável que estão descritas aqui servem como guia para identificar as situações que podem precisar de correção. Não afeta o processo de inicialização.

"Conceitos de Inicialização Confiável" na página 4
É importante entender a integridade do processo de inicialização e como classificar a inicialização de uma inicialização confiável ou uma inicialização não confiável.

Informações relacionadas:

Usando o HMC

Firewall Confiável

O recurso Firewall Confiável fornece segurança da camada de virtualização que melhora o desempenho e a eficiência de recurso ao se comunicar entre diferentes zonas de segurança Virtual LAN (VLAN) no mesmo servidor Power Systems. O Firewall Confiável diminui a carga na rede externa, movendo a capacidade de filtragem dos pacotes de firewall que atendem regras especificadas para a camada de virtualização. Esta capacidade de filtragem é controlada pelas regras de filtragem de rede anteriormente definidas, que permitem que o tráfego de rede confiável cruze entre as zonas de segurança VLAN sem sair do ambiente virtual. O Firewall Confiável protege e roteia tráfego de rede interna entre os sistemas operacionais AIX, IBM i e Linux.

Conceitos de Firewall Confiável

Existem alguns conceitos básicos a serem entendidos ao usar o Firewall Confiável.

O hardware Power Systems pode ser configurado com múltiplas zonas de segurança Virtual LAN (VLAN). Uma política configurada pelo usuário, criada como uma regra de filtragem do Firewall Confiável, permite que algum tráfego de rede confiável cruze as zonas de segurança VLAN e

permaneçam internos na camada de virtualização. Isso é semelhante a introduzir um firewall físico anexado à rede no ambiente virtualizado, que fornece um método mais eficiente em desempenho de implementar os recursos de firewall para os datacenters virtualizados.

Com o Firewall Confiável, é possível configurar as regras para permitir que certos tipos de tráfego sejam transferidos diretamente de uma VLAN em um Virtual I/O Server (VIOS) para outra VLAN no mesmo VIOS, enquanto ainda mantém um alto nível de segurança limitando outros tipos de tráfego. É um firewall configurável na camada de virtualização dos servidores Power Systems.

Usando o exemplo em Figura 1, o objetivo é conseguir transferir as informações com segurança e eficiência do LPAR1 no VLAN 200 e do LPAR2 no VLAN 100. Sem o Firewall Confiável, as informações de destino para LPAR2 de LPAR1 são enviadas da rede interna para o roteador, que roteia as informações de volta para LPAR2.

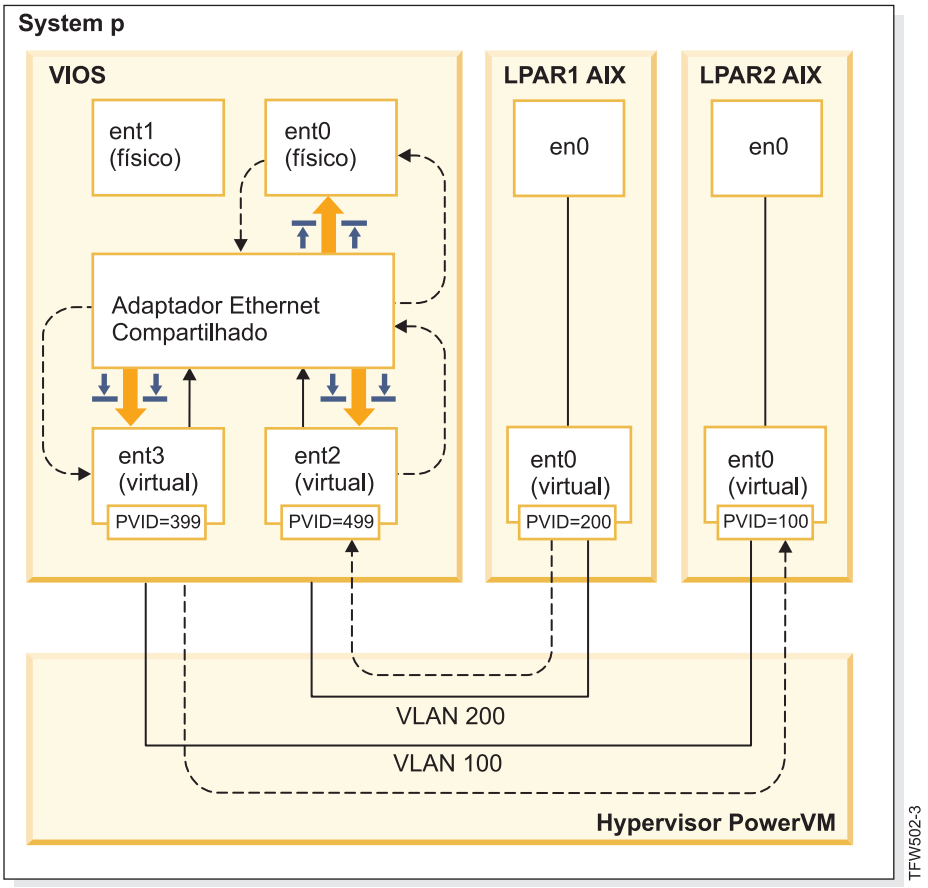

Figura 1. Exemplo de transferência de informações de LAN cruzada sem o Firewall Confiável

Usando o Firewall Confiável, é possível configurar as regras para permitir que as informações passem de LPAR1 para LPAR2 sem sair da rede interna. Este caminho é mostrado em Figura 2 na página 12.

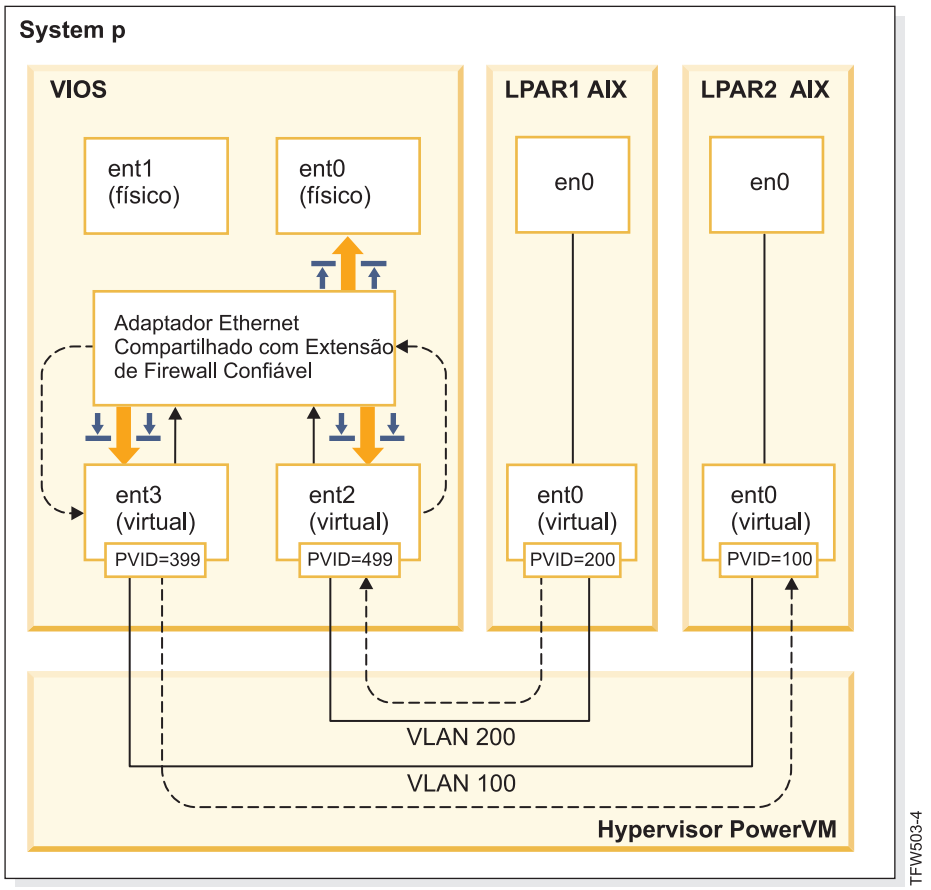

Figura 2. Exemplo de Transferência de Informações de VLAN Cruzada com Firewall Confiável

As regras de configuração que permitem que certas informações passem com segurança nas VLANs encurtam o caminho até seu destino. O Firewall Confiável usa a extensão kernel Shared Ethernet Adapter (SEA) e Security Virtual Machine (SVM) para ativar a comunicação.

Adaptador Ethernet Compartilhado
O SEA é onde o roteamento inicia e termina. Quando o SVM é registrado, o SEA recebe os pacotes e os encaminha para o SVM. Se o SVM determinar que o pacote é para um LPAR no mesmo servidor Power Systems, ele atualiza o cabeçalho da camada 2 do pacote. O pacote é retornado ao SEA para encaminhamento para o destino final no sistema ou na rede externa.

Máquina Virtual de Segurança
O SVM fica onde as regras de filtragem são aplicadas. As regras de filtragem são necessárias para manter a segurança na rede interna. Depois de registrar o SVM com o SEA, os pacotes são encaminhados para o SVM antes de serem enviados para a rede externa. Com base nas regras do filtro ativo, o SVM determina se um pacote permanece na rede interna ou move para a rede externa.

Instalando o Firewall Confiável

Instalar o PowerSC Trusted Firewall é semelhante à instalar outros recursos PowerSC.

Pré-requisitos:

- As versões do PowerSC anteriores à 1.1.1.0 não tinham o conjunto de arquivos necessários para instalar o Firewall Confiável. Assegure-se de ter o CD de instalação PowerSC para a versão 1.1.1.0, ou mais recente.

- Para tirar proveito do Firewall Confiável, você já deve ter usado o Hardware Management Console (HMC) ou Virtual I/O Server (VIOS) para configurar suas Virtual LANs (VLANs).

O Firewall Confiável é fornecido como um conjunto de arquivos adicionais no CD de instalação do PowerSC Standard Edition. O nome do arquivo é `powerscStd.svm.rte`. É possível incluir o Firewall Confiável em uma instância existente de PowerSC Versão 1.1.0.0, ou mais recente, ou instalá-lo como parte de uma nova instalação de PowerSC Versão 1.1.1.0, ou mais recente.

Para incluir a função de Firewall Confiável em uma instância PowerSC existente:

1. Assegure-se de que esteja executando o VIOS Versão 2.2.1.4, ou mais recente.
2. Insira o CD de instalação PowerSC para versão 1.1.1.0 ou faça download da imagem do CD de instalação.
3. Use o comando **oem_setup_env** para acesso raiz.
4. Use o comando **installp** ou a ferramenta SMIT para instalar o conjunto de arquivos `PowerscStd.svm.rte`.

Informações relacionadas:

"Instalando o PowerSC Standard Edition 1.1.3" na página 3
Você deve instalar um conjunto de arquivos para cada função específica do PowerSC Standard Edition.

Configurando o Firewall Confiável

As definições de configuração adicionais são necessárias para o recurso de Firewall Confiável depois que ele for instalado.

Monitoramento de Firewall Confiável

O monitoramento de Firewall Confiável analisa o tráfego do sistema de diferentes partições lógicas (LPARs) para fornecer informações úteis para determinar se executar o Firewall Confiável melhora o desempenho do sistema.

Se a função de monitoramento do Firewall Confiável registrar uma quantia significativa de tráfego de diferentes Virtual LANs (VLANs) que estejam no mesmo complexo central de eletrônica, ativar o Firewall Confiável deve beneficiar o seu sistema.

Para ativar o monitoramento Firewall Confiável, insira o comando a seguir:

```
vlantfw -m
```

Para exibir os resultados do monitoramento de Firewall Confiável, insira o comando a seguir:

```
vlantfw -D
```

Para desativar o monitoramento Firewall Confiável, insira o comando a seguir:

```
vlantfw -M
```

Criação de Log de Firewall Confiável

A criação de log de Firewall Confiável compila uma lista de caminhos de tráfego de rede no complexo central de eletrônica. A lista mostra os filtros que o Firewall Confiável usa para rotear o tráfego.

Quando o monitoramento de Firewall Confiável determinar que rotear o tráfego internamente melhora a eficiência, a criação de log de Firewall Confiável manterá uma lista de caminhos no arquivo `svm.log`. O limite de tamanho do arquivo `svm.log` é 16 MB. Se as entradas excederem o limite de 16 MB, as entradas mais antigas serão removidas do arquivo de log.

Para iniciar a criação de log do Firewall Confiável, insira o comando a seguir:

```
vlantfw -l
```

| Para parar a criação de log do Firewall Confiável, insira o comando a seguir:
| `vlantfw -L`

| É possível visualizar o arquivo de log no local a seguir: `/home/padmin/svm/svm.log`.

Múltiplos Adaptadores Ethernet Compartilhados

Você pode configurar o Firewall Confiável em sistemas que usam múltiplos Adaptadores Ethernet Compartilhados.

Algumas configurações usam os Shared Ethernet Adapters (SEAs) no mesmo Virtual I/O Server (VIOS). Múltiplos SEAs podem fornecer benefícios de proteção contra failover e nivelamento de recursos. O Firewall Confiável suporta o roteamento em múltiplos SEAs, contanto que estejam no mesmo VIOS.

Figura 3 mostra um ambiente usando múltiplos SEAs.

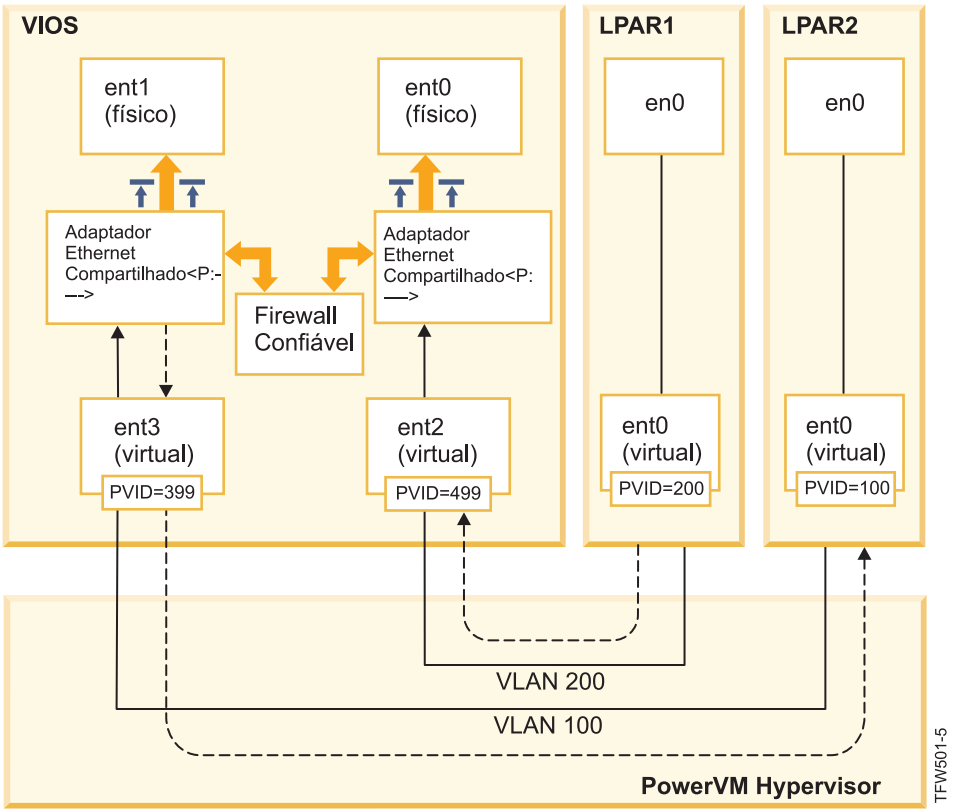

Figura 3. Configuração usando múltiplos Adaptadores Ethernet Compartilhados em um único VIOS

A seguir estão os exemplos de múltiplas configurações SEA que são suportadas pelo Firewall Confiável:

- Os SEAs são configurados com adaptadores de tronco no mesmo comutador virtual hypervisor Power. Esta configuração é suportada porque cada SEA recebe o tráfego de rede com diferentes VLAN IDs.
- Os SEAs são configurados com adaptadores de tronco em diferentes comutadores virtuais do hypervisor Power e cada adaptador de tronco fica em um ID VLAN diferente. Nesta configuração, cada SEA ainda recebe o tráfego de rede usando diferentes IDs VLAN.
- Os SEAs são configurados com adaptadores de tronco em diferentes comutadores virtuais do hypervisor Power e os mesmos IDs VLAN são reutilizados nos comutadores virtuais. Neste caso, o tráfego para ambos os SEAs possui os mesmos IDs VLAN.

Um exemplo desta configuração é ter LPAR2 no VLAN200 com o comutador virtual 10 e LPAR3 em VLAN200 com comutador virtual 20. Como ambos os LPARs e seus SEAs correspondentes usam o mesmo ID de VLAN (VLAN200), ambos os SEAs possuem acesso aos pacotes com esse ID de VLAN.

Não é possível ativar a ponte em mais de um VIOS. Por este motivo, as múltiplas configurações SEA a seguir não são suportadas pelo Firewall Confiável:

- Múltiplos VIOS e múltiplos drivers SEA.
- Compartilhamento de carga SEA redundante: Os adaptadores de tronco que são configurados para roteamento entre VLAN não podem ser divididos entre os servidores VIOS.

Removendo os Adaptadores Ethernet Compartilhados

As etapas para remover os dispositivos de Adaptadores Ethernet Compartilhados do sistema devem ser executadas em uma ordem específica.

Para remover um Shared Ethernet Adapter (SEA) do seu sistema, conclua as etapas a seguir:

1. Remova a Máquina Virtual de Segurança associada ao SEA, inserindo o comando a seguir:
   ```
   rmdev -dev svm
   ```
2. Remova o SEA inserindo o comando a seguir:
   ```
   rmdev -dev shared ethernet adapter ID
   ```

Nota: Remover o SEA antes de remover o SVM pode resultar em falha do sistema.

Criando Regras

É possível criar regras para ativar o roteamento de VLAN cruzada de Firewall Confiável.

Para ativar os recursos de roteamento de Firewall Confiável, você deve criar regras especificando quais comunicações são permitidas. Para segurança aprimorada, não há regra única que permita a comunicação entre todas as VLANs no sistema. Cada conexão permitida requer sua própria regra, embora cada regra ativada permita comunicação em ambas as direções para seus terminais especificados.

Como a criação de regra é criada na interface Virtual I/O Server (VIOS), as informações adicionais sobre os comandos ficam disponíveis na coleção de tópico VIOS no Centro de Informações Power Systems Hardware.

Para criar uma regra, conclua as etapas a seguir:

1. Abra a interface da linha de comandos VIOS.
2. Inicialize o driver SVM inserindo o comando a seguir:
   ```
   mksvm
   ```
3. Inicie o Firewall Confiável inserindo o comando inicial:
   ```
   vlantfw -s
   ```
4. Para exibir todos os endereços LPAR IP e MAC conhecidos, insira o comando a seguir:
   ```
   vlantfw -d
   ```

   Você precisará de endereços IP e MAC das partições lógicas (LPARs) para as quais você esteja criando regras.
5. Crie a regra de filtragem para permitir a comunicação entre dois LPARs (LPAR1 e LPAR2) inserindo um dos comandos a seguir:
   - `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`

Nota: Uma regra de filtragem permite a comunicação em ambas as direções, por padrão, dependendo da porta e entradas de protocolo. Por exemplo, você pode ativar o Telnet para LPAR1 para LPAR2, executando o comando a seguir:

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

6. Ative todas as regras de filtragem no kernel, inserindo os comandos a seguir:

```
mkvfilt -u
```

Nota: Este procedimento ativa esta regra e quaisquer outras regras de filtragem que existam no sistema.

Exemplos Adicionais

Os exemplos a seguir mostram algumas outras regras de filtragem que você pode criar usando o Firewall Confiável.

- Para permitir a comunicação de Shell Seguro do LPAR no VLAN 100 para LPAR no VLAN 200, insira o comando a seguir:

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

- Para permitir o tráfego entre todas as portas de 0 a 499, insira o comando a seguir:

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

- Para permitir todo o tráfego TCP entre os LPARs, insira o comando a seguir:

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

  Se você não especificar qualquer porta ou operações de porta, o tráfego poderá usar todas as portas.

- Para permitir o sistema de mensagens Internet Control Message Protocol entre LPARs, insira o comando a seguir:

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

Conceitos relacionados:

"Desativando Regras"
É possível desativar as regras que permitem o roteamento de VLAN cruzada no recurso Firewall Confiável.

Referências relacionadas:

"Comando genvfilt" na página 33

"Comando mkvfilt" na página 35

"Comando vlantfw" na página 45

Informações relacionadas:

Servidor de E/S Virtual (VIOS)

Desativando Regras

É possível desativar as regras que permitem o roteamento de VLAN cruzada no recurso Firewall Confiável.

Como as regras são desativadas na interface Virtual I/O Server (VIOS), as informações adicionais sobre os comandos e o processo ficam disponíveis na coleção de tópico VIOS no Centro de Informações de Hardware Power Systems.

Para desativar uma regra, conclua as etapas a seguir:

1. Abra a interface da linha de comandos VIOS.
2. Para exibir todas as regras de filtro ativo, insira o comando a seguir:

```
lsvfilt -a
```

É possível omitir o sinalizador **-a** para exibir todas as regras de filtragem armazenadas no Gerenciador de Dados do Objeto.

3. Observe o número de identificação para a regra de filtragem que você está desativando. Para este exemplo, o número de identificação da regra de filtragem é 23.
4. Desative a regra de filtragem 23 quando estiver ativada no kernel, inserindo o comando a seguir:

   ```
   rmvfilt -n 23
   ```

   Para desativar todas as regras de filtragem no kernel, insira o comando a seguir:

   ```
   rmvfilt -n all
   ```

Conceitos relacionados:

"Criando Regras" na página 15
É possível criar regras para ativar o roteamento de VLAN cruzada de Firewall Confiável.

Referências relacionadas:

"Comando lsvfilt" na página 34

"Comando rmvfilt" na página 44

Criação de Log Confiável

A Criação de Log ConfiávelPowerVM permite que os AIX LPARs gravem nos arquivos de log que são armazenados em um Virtual I/O Server (VIOS) anexado. Os dados são transmitidos para o VIOS diretamente através do hypervisor e a conectividade de rede não é necessária entre o cliente LPAR e o VIOS.

Logs Virtuais

O administrador Virtual I/O Server (VIOS) cria e gerencia os arquivos de log e eles são apresentados ao sistema operacional AIX como dispositivo de log virtual no diretório `/dev`, semelhante aos discos virtuais ou mídia ótica virtual.

Armazenar os arquivos de log como logs virtuais aumenta o nível de confiança nos registros porque eles não podem ser alterados por um usuário com privilégios raiz no cliente LPAR em que eles foram gerados. Múltiplos dispositivos de log virtual podem ser anexados ao mesmo cliente LPAR e cada log é um arquivo diferente no diretório `/dev`.

A Criação de Log Confiável permite que os dados de vários LPARs do cliente sejam consolidados em um único sistema de arquivos, que fica acessível no VIOS. Portanto, o VIOS fornece um único local no sistema para análise de log e arquivamento. O administrador LPAR cliente pode configurar os aplicativos e o sistema operacional AIX para gravar os dados para os dispositivos de log virtual, que são semelhantes a gravar dados para os arquivos locais. O subsistema de Auditoria AIX pode ser configurado para direcionar os registros de auditoria para os logs virtuais e outros serviços AIX, como syslog, trabalham com suas configurações existentes para direcionar os dados para os logs virtuais.

Para configurar o log virtual, o administrador VIOS deve especificar um nome para o log virtual, que possui os componentes separados a seguir:

- Nome do Cliente
- Nome do Log

Os nomes dos dois componentes podem ser configurados pelo administrador VIOS para qualquer valor, mas o nome do cliente geralmente é o mesmo para todos os logs virtuais que são conectados a um determinado LPAR (por exemplo, o nome do host do LPAR). O nome do log é usado para identificar o propósito do log (por exemplo, auditoria ou syslog).

Em um AIX LPAR, cada dispositivo de log virtual fica presente como dois arquivos funcionalmente equivalentes no sistema de arquivos `/dev`. O primeiro arquivo é nomeado após o dispositivo, por

exemplo, /dev/vlog0, e o segundo arquivo é nomeado concatenando um prefixo vl com o nome de log e o número do dispositivo. Por exemplo, se o dispositivo de log virtual vlog0 tiver audit como o nome de log, ele ficará presente no sistema de arquivos /dev como vlog0 e vlaudit0.

Informações relacionadas:

Criando os Logs Virtuais

Detectando os Dispositivos de Log Virtual

Depois que um administrador VIOS tiver criado dispositivos de log virtual e os tiver conectado a um cliente LPAR, a configuração de dispositivo do cliente LPAR deve ser atualizada para que os dispositivos fiquem visíveis.

O administrador LPAR de cliente atualiza as configurações usando um dos métodos a seguir:

- Reinicializando o LPAR de cliente
- Executando o comando **cfgmgr**

Execute o comando **lsdev** para exibir os dispositivos de log virtual. Os dispositivos são prefixados com vlog, por padrão. Um exemplo da saída de comando **lsdev** em um AIX LPAR em que dois dispositivos de logs virtuais estejam presentes é o seguinte:

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

Inspecione as propriedades de um dispositivo de log virtual individual usando o comando lsattr –El *<device name>*, que produz saída semelhante ao seguinte:

```
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
```

Esta saída exibe o nome do cliente, o nome do dispositivo e a quantia de dados de log que o VIOS pode armazenar.

O log virtual armazena dois tipos de dados de log, que são:

- Dados do log: Os dados de log bruto gerados pelos aplicativos no AIX LPAR.
- Dados de estado: As informações sobre quando os dispositivos foram configurados, abertos, fechados e outras operações que são usadas para analisar a atividade de log.

O administrador VIOS especifica a quantia de **dados de log** e **dados de estado** que podem ser armazenados para cada log virtual e a quantia é indicada pelos atributos max_log_size e max_state_size. Quando a quantia de dados armazenados exceder o limite especificado, os dados de log mais antigos serão sobrescritos. O administrador VIOS deve assegurar que os dados de log sejam coletados e arquivados frequentemente para preservar os logs.

Instalando a Criação de Log Confiável

É possível instalar o recurso PowerSC Trusted Logging usando a interface de linha de comandos ou a ferramenta SMIT.

Os pré-requisitos para instalar o Trusted Logging são VIOS 2.2.1.0, ou mais recente e IBM AIX 6 com Tecnologia Nível 7 ou IBM AIX 7 com Tecnologia Nível 1.

| O nome do arquivo para instalar o recurso Trusted Logging é `powerscStd.vlog`, que está incluído no CD
| de instalação do PowerSC Standard Edition.

| Para instalar a função Trusted Logging:

| 1. Assegure-se de que esteja executando o VIOS Versão 2.2.1.0, ou mais recente.
| 2. Insira o CD de instalação PowerSC ou faça download da imagem do CD de instalação.
| 3. Use o comando **installp** ou a ferramenta SMIT para instalar o conjunto de arquivos `powerscStd.vlog`.

| **Informações relacionadas**:

| “Instalando o PowerSC Standard Edition 1.1.3” na página 3
| Você deve instalar um conjunto de arquivos para cada função específica do PowerSC Standard Edition.

Configurando a Criação de Log Confiável

Aprenda o procedimento para configurar a Criação de Log Confiável no subsistema de Auditoria AIX e syslog.

Configurando o Subsistema de Auditoria AIX

O subsistema de Auditoria AIX pode ser configurado para gravar dados binários para um dispositivo de log virtual além de gravar os logs para o sistema de arquivos local.

Nota: Antes de configurar o subsistema de Auditoria AIX, você deve concluir o procedimento em “Detectando os Dispositivos de Log Virtual” na página 18.

Para configurar o subsistema de Auditoria AIX, conclua as etapas a seguir:

1. Configure o subsistema de Auditoria AIX para registrar os dados no modo binário (`auditbin`).
2. Ative a Criação de Log Confiável para a auditoria AIX, editando o arquivo de configuração `/etc/security/audit/config`.
3. Inclua um parâmetro `virtual_log = /dev/vlog0` para a sub-rotina `bin:`.

   Nota: A instrução será válida se o administrador LPAR desejar que os dados `auditbin` sejam gravados para o `/dev/vlog0`.
4. Reinicie o subsistema de Auditoria AIX na sequência a seguir:

```
audit shutdown
audit start
```

Os registros de auditoria são gravados para Virtual I/O Server (VIOS) através do dispositivo de log virtual especificado além de gravar os logs para o sistema de arquivos local. Os logs são armazenados sob o controle de parâmetros `bin1` e `bin2` na sub-rotina `bin:` do arquivo de configuração `/etc/security/audit/config`.

Informações relacionadas:

Subsistema de Auditoria

Configurando o syslog

O syslog pode ser configurado para gravar as mensagens nos logs virtuais, incluindo as regras no arquivo `/etc/syslog.conf`.

Nota: Antes de configurar o arquivo `/etc/syslog.conf`, você deve concluir o procedimento em “Detectando os Dispositivos de Log Virtual” na página 18.

É possível editar o arquivo `/etc/syslog.conf` para corresponder as mensagens de log, que são baseadas nos critérios a seguir:

- Instalação
- Nível de prioridade

Para usar os logs virtuais para as mensagens syslog, o arquivo `/etc/syslog.conf` deve ser configurado com regras para gravar as mensagens desejadas para o log virtual apropriado no diretório `/dev`.

Por exemplo, para enviar as mensagens de nível de depuração que são geradas por qualquer instalação para o log virtual `vlog0`, inclua a linha a seguir no arquivo `/etc/syslog.conf`:

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

Nota: Não use as instalações de rotação de log disponíveis no daemon `syslogd` para qualquer comando que grave os dados nos logs virtuais. Os arquivos no sistema de arquivos `/dev` não são arquivos regulares e não podem ser renomeados e movidos. O administrador VIOS deve configurar a rotação de log virtual no VIOS.

O daemon `syslogd` deve ser reiniciado após a configuração usando o comando a seguir:

```
refresh -s syslogd
```

Informações relacionadas:

Daemon syslogd

Gravando os Dados para os Dispositivos de Log Virtual

Os dados arbitrários são gravados em um dispositivo de log virtual abrindo o arquivo apropriado no diretório `/dev` e gravando os dados no arquivo. Um log virtual pode ser aberto por um processo por vez.

Por exemplo:

Para gravar as mensagens para os dispositivos de log virtuais usando o comando **echo**, insira o comando a seguir:

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

Para armazenar os arquivos nos dispositivos de log usando o comando **cat**, insira o comando a seguir:

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

O tamanho máximo de gravação individual é limitado a 32 KB e os programas que tentam gravar mais dados em uma única operação de gravação recebem um erro de E/S (EIO). Os utilitários da interface da linha de comandos (CLI), como o comando **cat**, dividem automaticamente as transferências em operações de gravação de 32 KB.

Trusted Network Connect e Gerenciamento de Correção

Trusted Network Connect (TNC) faz parte do grupo de computação confiável (TCG) que fornece especificações para verificar a integridade de terminal. TNC definiu a arquitetura de solução aberta que ajuda os administradores a forçarem as políticas a controlarem efetivamente o acesso à infraestrutura de rede.

Conceitos do Trusted Network Connect

Aprenda sobre os componentes, configurando a comunicação segura e o sistema de gerenciamento de correção do Trusted Network Connect (TNC).

Componentes Trusted Network Connect

Aprenda sobre os componentes da estrutura Trusted Network Connect (TNC).

O modelo TNC consiste nos componentes a seguir:

Servidor Trusted Network Connect:

O servidor Trusted Network Connect (TNC) identifica os clientes que são incluídos na rede e inicia uma verificação neles.

O cliente TNC fornece as informações de nível do conjunto de arquivos necessárias para o servidor para verificação. O servidor determina se o cliente está no nível configurado pelo administrador. Se o cliente não for compatível, o servidor TNC notificará o administrador sobre a correção necessária.

O servidor TNC inicia as verificações nos clientes que estão tentando acessar a rede. O servidor TNC carrega um conjunto de Integrity Measurement Verifiers (IMVs) que pode solicitar medições de integridade a partir dos clientes e verificá-las. O AIX possui um IMV padrão, que verifica o conjunto de arquivos e o nível de caminho de segurança dos sistemas. O servidor TNC é uma estrutura que carrega e gerencia múltiplos módulos IMV. Para verificar um cliente, ele depende das IMVs para solicitar as informações dos clientes e verifica os clientes.

Gerenciamento de Correções:

O servidor Trusted Network Connect (TNC) se integra ao SUMA para fornecer uma solução de gerenciamento de correção.

O AIX SUMA que faz download dos service packs mais recentes e correções de segurança disponíveis no IBM ECC e Fix Central. O TNC e o daemon de gerenciamento de correção envia por push as mais recentes informações atualizadas para o servidor TNC, que serve como um conjunto de arquivos de linha de base para verificar os clientes.

O daemon **tncpmd** deve ser configurado para gerenciar os downloads Service Update Management Assistant (SUMA) e para enviar por push informações do conjunto de arquivos para o servidor TNC. Este daemon deve ser hospedado em um sistema que é conectado à Internet para conseguir fazer download das atualizações automaticamente. Para usar o servidor de gerenciamento de correção TNC sem conectá-lo à Internet, você pode registrar um repositório de correção definido pelo usuário com o servidor de gerenciamento de correção TNC.

Nota: O servidor TNC e o daemon **tncpmd** podem ser hospedados no mesmo sistema.

Cliente Trusted Network Connect:

O cliente Trusted Network Connect (TNC) fornece as informações necessárias pelo servidor TNC para verificação.

O servidor determina se o cliente está no nível configurado pelo administrador. Se o cliente não for compatível, o servidor TNC notificará o administrador sobre as atualizações necessárias.

O cliente TNC carrega os IMCs na inicialização e usa os IMCs para reunir as informações necessárias.

Referenciador IP Trusted Network Connect:

O servidor Trusted Network Connect (TNC) pode iniciar automaticamente a verificação nos clientes que fazem parte da rede. O referenciador IP sendo executando na partição Virtual I/O Server (VIOS) detecta os novos clientes que são atendidos pelo VIOS e envia os seus endereços IP no servidor TNC. O servidor TNC verifica o cliente a respeito da política que é definida.

Comunicação Segura Trusted Network Connect

Os daemons Trusted Network Connect (TNC) se comunicam sobre os canais criptografados que são ativados por Transport Layer Security (TLS) ou Secure Sockets Layer (SSL).

A comunicação segura deve assegurar que os dados e os comandos que fluem na rede sejam autenticados e seguros. Cada sistema deve ter sua própria chave e certificado, que são gerados quando o comando de inicialização para os componente for executado. Esse processo é completamente transparente para o administrador e requer menos envolvimento do administrador.

Para verificar um novo cliente, o certificado do cliente deve ser importado no banco de dados do servidor. O certificado é marcado como não confiável inicialmente e o administrador usa o comando **psconf** para visualizar e marcar os certificados como confiáveis inserindo o comando a seguir:

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

Para usar uma chave e certificado diferentes, o comando **psconf** fornece a opção para importar o certificado.

Para importar o certificado a partir do servidor, insira o comando a seguir:

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

Para importar o certificado a partir do cliente, insira o comando a seguir:

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

Protocolo Trusted Network Connect

O protocolo Trusted Network Connect (CNC) é usado com a estrutura TNC para manter a integridade da rede.

O TNC fornece especificações para verificar a integridade do ponto de extremidade. Os terminais que solicitam acesso são avaliados com base nas medidas de integridade de componentes críticos que podem afetar seu ambiente operacional. A estrutura TNC permite que os administradores monitorem a integridade dos sistemas na rede. O TNC é integrado com a infraestrutura de distribuição da correção AIX para construir uma solução de gerenciamento de correção completa.

As especificações TNC devem atender os requisitos da arquitetura do sistema AIX e Família POWER. Os componentes de TNC são projetadas para fornecer uma solução de gerenciamento de correção completa no sistema operacional AIX. Esta configuração permite que os administradores gerenciem eficientemente a configuração de software nas implementações AIX. Ela fornece ferramentas para verificar os níveis de correção dos sistemas e gerar um relatórios sobre os clientes que não são compatíveis. Além disso, o gerenciamento de correção simplifica o processo de download das correções e as instala.

Módulos IMC e IMV

O servidor ou o cliente Trusted Network Connect (TNC) usam internamente os módulos Integrity Measurement Collector (IMC) e Integrity Measurement Verifier (IMV) para a verificação do servidor.

Esta estrutura permite carregar múltiplos módulos IMC e IMV no servidor e clientes. O módulo que executa a verificação do sistema operacional (OS) e do nível do conjunto de arquivos é fornecido com o sistema operacional AIX, por padrão. Para acessar os módulos que são enviados com o sistema operacional AIX, use um dos caminhos a seguir:

- `/usr/lib/security/tnc/libfileset_imc.a`: Coleta o nível de SO e as informações sobre o conjunto de arquivos que é instalado a partir do sistema do cliente e o envia para o IMV (servidor TNC) para verificação.
- `/usr/lib/security/tnc/libfileset_imv.a`: Solicita o nível do S.O. e as informações do conjunto de arquivos a partir do cliente e o compara com as informações da linha de base. Também atualiza o status do cliente no banco de dados do servidor TNC. Para visualizar o status, insira o comando a seguir:

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

Referências relacionadas:

"Comando psconf" na página 39

Instalando o Trusted Network Connect

Instalar os componentes do Trusted Network Connect (TNC) requer que você conclua certas etapas.

Para definir a configuração para usar os componentes do TNC, conclua as etapas a seguir:

1. Identifique os endereços IP dos sistemas para configurar o servidor TNC, o servidor Trusted Network Connect and Patch Management (TNCPM) e o referente TNC IP para Virtual I/O Server (VIOS).

   Nota: O servidor TNC não pode ser configurado como um cliente TNC.
2. Configure o servidor Network Installation Management (NIM). O sistema que é configurado como um servidor é o NIM master e os conjuntos de arquivos `sets:bos.sysmgt.nim.master` devem ser instalados no sistema do cliente.
3. Configure o servidor TNCPM. Esta configuração pode ser configurada no sistema NIM. O servidor TNCPM usa o SUMA para fazer o download das correções dos websites IBM Fix Central e ECC. Para fazer download das atualizações, o sistema deve ser conectado à Internet. Insira o comando a seguir para configurar o servidor TNCPM:

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

   Por exemplo:

   ```
   pmconf mktncpm pmport=20000 tncserver=1.1.1.1:10000
   ```
4. Configure as políticas no servidor TNC. Para criar as políticas para verificar os clientes, consulte "Criando Políticas para o Cliente Trusted Network Connect" na página 27.
5. Configure o referenciador TNC IP no VIOS. Esta configuração no VIOS aciona a verificação nos clientes que estão se conectando a rede. Insira o comando a seguir para configurar o referenciador:

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

   Por exemplo:

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

   Nota: O valor da porta do servidor e a porta TNC, que é uma porta cliente, devem ser iguais:
6. Configure os clientes usando o comando a seguir:

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

   Por exemplo:

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

Referências relacionadas:

"Comando psconf" na página 39

Informações relacionadas:

"Instalando o PowerSC Standard Edition 1.1.3" na página 3
Você deve instalar um conjunto de arquivos para cada função específica do PowerSC Standard Edition.

Instalando com NIM

IBM Fix Central

Centro de Ajuda Online Passport Advantage

Configurando Trusted Network Connect e Gerenciamento de Correção

Você deve configurar Trusted Network Connect (TNC) como um daemon de gerenciamento de correção. O servidor TNC é integrado ao SUMA para fornecer uma solução de gerenciamento de correção abrangente.

Configurando o Servidor Trusted Network Connect

Aprenda as etapas para configurar o servidor TNC.

Para configurar o servidor TNC, o arquivo `/etc/tnccs.conf` deve ter um valor semelhante ao seguinte:

```
component = SERVER
```

Para configurar um sistema como um servidor, insira o comando a seguir:

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

Por exemplo:

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

Nota: A porta `tncport` e a porta `pmserver` devem ser configuradas para diferentes valores e se o valor do parâmetro `recheck_interval` não for fornecido, um valor padrão de 1440 minutos será usado.

O valor de porta padrão de 42830 minutos é usado para a porta `tncport` e o valor de porta de 38240 minutos é usado para a porta `pmserver`.

Referências relacionadas:

"Comando psconf" na página 39

Configurando o Cliente Trusted Network Connect

Aprenda as etapas para configurar o cliente Trusted Network Connect (TNC) e as definições de configuração necessárias para a configuração.

Para configurar o cliente TNC, o arquivo `/etc/tnccs.conf` deve ter um valor semelhante ao seguinte:

```
component = CLIENT
```

Para configurar um sistema como um cliente, insira o comando a seguir:

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

Por exemplo:

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

Nota: O valor da porta do servidor e o `tncport`, que é uma porta cliente devem ser iguais.

Referências relacionadas:

"Comando psconf" na página 39

Configurando o Servidor do Gerenciamento de Correção

Aprenda as etapas para configurar um sistema como um servidor do gerenciamento de correção.

O servidor do gerenciamento de correção Trusted Network Connect (TNC) deve ser configurado no servidor Network Installation Management (NIM) de modo que os clientes TNC possam ser atualizados.

Para inicializar os repositórios de correção para gerenciamento de correção TNC, insira o comando a seguir:

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

Um exemplo do comando **pmconf** a seguir:

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

O comando **init** faz download do service pack mais recente para cada nível de tecnologia, e torna isso disponível para o servidor TNC. Os service packs atualizados permitem que o servidor TNC execute uma

verificação de cliente TNC da linha de base e para o servidor de gerenciamento de correção TNC para instalar as atualizações de cliente TNC. Especifique o sinalizador **-A** para aceitar todos os contratos de licença ao executar as atualizações de cliente. Por exemplo, os repositórios de correção que são transferidos pelo download pelo servidor de gerenciamento de correção TNC no arquivo `/var/tnc/tncpm/fix_repository`. Use o sinalizador **-P** para especificar um diretório diferente.

Para ativar o IBM Security Advisory automático e downloads de correção provisória, é possível especificar um intervalo de correção provisória. Esse recurso fornece a notificação automática de correções provisórias de segurança recém-publicadas e identificadores Common Vulnerabilities and Exposures (CVE) associados. Todas as recomendações de segurança e correções provisórias são verificadas antes do registro com TNC. A chave pública de vulnerabilidade IBM AIX, que é necessário para fazer o download das correções temporárias automaticamente, é disponível no website IBM AIX Security. O service pack automático e os downloads de correção provisória são desativados, configurando o intervalo de download e intervalo de correção provisória para 0.

Também é possível atualizar o service pack e o registro de correção provisória manualmente. Para registrar manualmente um IBM Security Advisory juntamente com suas correções provisórias correspondentes, insira o comando a seguir:

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

Para registrar manualmente uma correção provisória independente, insira o comando a seguir:

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

Para registrar um novo nível de tecnologia e fazer o download de seu service pack mais recente, insira o comando a seguir:

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

Para fazer o download de um service pack que não seja a versão mais atual, ou para fazer o download de um nível de tecnologia a ser usado para verificação e atualizações de cliente, insira o comando a seguir:

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

Para registrar um service pack ou repositório de correção de nível de tecnologia que exista no sistema, insira o comando a seguir:

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

Para configurar um sistema para servir como um servidor de gerenciamento de correção, insira o comando a seguir:

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

Um exemplo desse comando a seguir:

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

O servidor de gerenciamento de correção TNC sempre suporta o gerenciamento de Authorized Problem Analysis Reports (APARs) de segurança. Insira o comando a seguir para configurar o gerenciamento de correção TNC para gerenciar outros tipos de APARs:

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

No exemplo anterior, <APAR_type_list> é uma lista separada por vírgula que contém os tipos a seguir de APARs:

- HIPER
- PE

- Aprimoramento

O servidor de gerenciamento de correção TNC suporta **syslog** para download do service pack, nível de tecnologia e atualizações de cliente. A instalação é `user` e a prioridade é `info`. Um exemplo disso é `user.info`.

O servidor de gerenciamento de correção TNC também mantém um log com todas as atualizações de cliente no diretório `/var/tnc/tncpm/log/update/<ip>/<timestamp>`.

Referências relacionadas:

"Comando psconf" na página 39

Informações relacionadas:

IBM AIX Security

Configurando a Notificação de Email do Servidor Trusted Network Connect

Aprenda o procedimento para configurar a notificação por email para o servidor Trusted Network Connect (TNC).

O servidor TNC visualiza o nível de correção do cliente se o servidor TNC achar que o cliente não é compatível, ele envia um email para o administrador com o resultado e a correção necessária.

| Para configurar o endereço de email do administrador, insira o comando:

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

| Por exemplo:

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

| No exemplo anterior, o email para o grupo de IPs *vayugrp1* e *vayugrp2* é enviado para o endereço de email abc@ibm.com.

| Para enviar um email para um endereço de email global para o grupo de IP que não possui um endereço de email designado, insira o comando a seguir:

```
psconf add –e <mailaddress>
```

| Por exemplo:

```
psconf add –e abc@ibm.com
```

| No exemplo anterior, se um grupo de IPs não tiver um endereço de email designado, o correio será enviado ao endereço de email abc@ibm.com. Ele atua como um endereço de email global.

Referências relacionadas:

"Comando psconf" na página 39

Configurando o Referenciador IP no VIOS

Aprenda a configurar o referenciador IP no Virtual I/O Server (VIOS) para iniciar automaticamente a verificação.

Nota: Você deve configurar a extensão kernel SVM no Virtual I/O Server (VIOS) antes de configurar o referenciador IP.

Para configurar o Referenciador TNC IP, o arquivo de configuração `/etc/tnccs.conf` deve ter uma configuração semelhante ao seguinte `component = IPREF`.

| É possível configurar um sistema como um cliente, inserindo o comando a seguir:

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

| Por exemplo:

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

| O valor da porta `tncserver` e `tncport`, que é a porta cliente devem ser iguais.

Referências relacionadas:

"Comando psconf" na página 39

Gerenciando Trusted Network Connect e Gerenciamento de Correção

Aprenda a gerenciar o Trusted Network Connect (TNC) para implementar as tarefas, como incluir os clientes, políticas, logs, resultados de verificação, clientes de atualização e certificados relacionados ao TNC.

Visualizando os Logs do Servidor Trusted Network Connect

Aprenda a visualizar os logs do servidor Trusted Network Connect (TNC).

| O servidor TNC registra os resultados de verificação de todos os clientes. Para visualizar o log, execute o
| comando **psconf**:

```
psconf list –H –i <ip |ALL>
```

| **Referências relacionadas**:

"Comando psconf" na página 39

Criando Políticas para o Cliente Trusted Network Connect

Aprenda a configurar as políticas relacionadas ao cliente Trusted Network Connect (TNC).

| O console `psconf` fornece a interface necessária para gerenciar as políticas TNC. Cada cliente ou um
| grupo de clientes pode estar associado a uma política.

As políticas a seguir podem ser criadas:

- Um grupo de Internet Protocol (IP) contém vários endereços IP de cliente.
- Cada IP de cliente pode pertencer a apenas um grupo.
- O grupo de IPs é associado a um grupo de políticas.
- Um grupo de política contém diferentes tipos de políticas. Por exemplo, a política do conjunto de arquivos que especifica qual deve ser o nível do sistema operacional do cliente (ou seja, liberação, nível de tecnologia e service pack). Pode haver várias políticas do conjunto de arquivos em um grupo de políticas e o cliente que se refere a essa política deve estar no nível especificado por uma das políticas do conjunto de arquivos.

Os comandos a seguir mostram como criar um grupo de IPs, grupo de políticas e políticas do conjunto de arquivos.

| Para criar um grupo de IPs, insira o comando a seguir:

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

| Por exemplo:

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

| **Nota:** Para obter um grupo, pelo menos um IP deve ser fornecido. Múltiplos IPs devem ser separados
| por uma vírgula.

| Para criar uma política do conjunto de arquivos, insira o comando a seguir:

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

| Por exemplo:

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

| **Nota:** As informações de construção devem estar no formato `<rel00-TL-sp>`.

| Para criar uma política e designar um grupo de IPs, insira o comando a seguir:
| `psconf add –P <policyname> ipgroup=[±] <ipgrp1, ipgrp2 ...]`

| Por exemplo:
| `psconf add –P mypol ipgroup=myipgrp,myipgrp1`

Para designar a política do conjunto de arquivos a uma política, insira o comando a seguir:
`psconf add –P <policyname> fspolicy=[±]<fspol1, fspol2 ...>`

Por exemplo:
`psconf add –P mypol fspolicy=myfspol,myfspol1`

Nota: Se múltiplas políticas do conjunto de arquivos forem fornecidas, o sistema forçará a melhor política correspondente no cliente. Por exemplo, se o cliente estiver em `6100-02-01` e você mencionar a política do conjunto de arquivos como `7100-03-04` e `6100-02-03`, então `6100-02-03` será reforçado no cliente.

Referências relacionadas:

"Comando psconf" na página 39

Iniciando a Verificação para o Cliente Trusted Network Connect

Aprenda a verificar o cliente Trusted Network Connect (TNC).

Use um dos métodos a seguir para verificação do cliente:

- O daemon do referenciador IP no Virtual I/O Server (VIOS) encaminha o IP do cliente para o servidor TNC: O cliente LPAR adquire o IP e tenta acessar a rede. O daemon do referenciador IP no VIOS detecta o novo endereço IP e o encaminha para o servidor TNC: O servidor TNC inicia a verificação ao receber o novo endereço IP.
- O servidor TNC verifica o cliente periodicamente: O administrador pode incluir os IPs do cliente que devem ser verificados no banco de dados da política TNC. O servidor TNC verifica os clientes que estão no banco de dados. A nova verificação acontece automaticamente em intervalos regulares com referência ao valor de atributo `recheck_interval` especificado no arquivo de configuração `/etc/tnccs.conf`.
- O administrador inicia a verificação de cliente manualmente: O administrador pode iniciar a verificação manualmente para verificar se um cliente é incluído na rede executando o comando a seguir:
  `tncconsole verify -i <ip>`

Nota: Para recursos que não estejam conectados a um VIOS, os clientes podem ser verificados e atualizados quando são incluídos manualmente para o servidor TNC.

Referências relacionadas:

"Comando psconf" na página 39

Visualizando os Resultados da Verificação do Trusted Network Connect

Aprenda o procedimento para visualizar os resultados de verificação do cliente Trusted Network Connect (TNC).

| Para visualizar os resultados de verificação dos clientes na rede, insira o comando a seguir:
| `psconf list -s ALL -i ALL`

| Este comando exibe todos os clientes que possuem um status **IGNORED**, **COMPLIANT** ou **FAILED**.

| • **IGNORED**: O IP do cliente é ignorado na lista IP (ou seja, o cliente pode estar isento da verificação).
| • **COMPLIANT**: O cliente passou na verificação (ou seja, o cliente é compatível com a política).
| • **FAILED**: O cliente falhou na verificação (ou seja, o cliente não é compatível com a política e a ação de
| administração é necessária).

| Para determinar o motivo para a falha, execute o comando **psconf** com o IP do cliente que falhou:

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

Referências relacionadas:

"Comando psconf" na página 39

Atualizando o Cliente Trusted Network Connect

O servidor Trusted Network Connect (TNC) verifica um cliente e atualiza o banco de dados com o status do cliente e o resultado de verificação. O administrador pode visualizar os resultados e executar a ação para atualizar o cliente.

| Para atualizar um cliente que esteja em um nível anterior, insira o comando a seguir:

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

| Por exemplo:

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

O comando **psconf** atualiza o cliente com a construção e as instalações APAR, se elas não estiverem instaladas.

Referências relacionadas:

"Comando psconf" na página 39

Gerenciando Políticas de Gerenciamento de Correção

| O comando **pmconf** é usado para configurar as políticas de gerenciamento de correção.

As políticas de gerenciamento de correção fornecem informações, como o endereço IP do servidor TNC e o intervalo de tempo para iniciar uma atualização SUMA.

| Para gerenciar a política de gerenciamento de correção, insira o comando a seguir:

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

| Por exemplo:

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

Nota: As portas `pmport` e `tncserver` devem ser diferentes.

Referências relacionadas:

"Comando pmconf" na página 35

Importando os Certificados Trusted Network Connect

Aprenda o procedimento para importar um certificado e para transmitir com segurança os dados na rede.

| Os daemons Trusted Network Connect (TNC) se comunicam nos canais criptografados usando o
| protocolo Transport Layer Security (TLS) ou Secure Sockets Layer (SSL). 1Esse daemon assegura que os
| dados e os comandos que são transportados na rede sejam autenticados e seguros. Cada sistema possui
| sua própria chave e certificado, que são gerados quando o comando de inicialização para os componente
| for executado. Esse processo é transparente para o administrador e requer menos envolvimento do
| administrador. Quando um cliente estiver sendo verificado pela primeira vez, seu certificado será

| importado para o banco de dados do servidor. O certificado é marcado como não confiável inicialmente e
| o administrador usa o comando **psconf** para visualizar e marcar os certificados como confiáveis,
| inserindo o comando a seguir:

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

| Se o administrador quiser usar uma chave e certificado diferentes, o comando **psconf** fornecerá o recurso
| para importar a chave e o certificado.

| Para importar o certificado a partir de um servidor, insira o comando a seguir:

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

| Para importar o certificado a partir de um cliente, insira o comando a seguir:

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

Referências relacionadas:

"Comando psconf" na página 39

| TNC Server Reporting

| O servidor Trusted Network Connect (TNC) suporta o formato comma-separated values (CSV) e o
| formato de saída de texto para suas Common Vulnerabilities and Exposures (CVE), IBM Security
| Advisory, políticas de servidor TNC, correção de segurança do cliente TNC e service packs registrados e
| relatórios de correção provisória.

| O relatório CVE exibe todas as exposições e vulnerabilidades comuns para os service packs registrados.
| Para exibir os resultados deste relatório, insira o comando a seguir:

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

| O relatório IBM Security Advisory exibe as vulnerabilidades de segurança conhecidas no software IBM
| instalado. Para exibir os resultados deste relatório, insira o comando a seguir:

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

| O relatório de políticas do servidor TNC exibe as políticas de segurança que são forçadas no servidor
| TNC. Para exibir os resultados deste relatório, insira o comando a seguir:

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

| O relatório de correção do cliente TNC exibe as correções provisórias instaladas e ausentes para o cliente
| TNC. Para exibir os resultados deste relatório, insira o comando a seguir:

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

| Também é possível executar um relatório que gera uma lista de service packs registrados e os Authorized
| Program Analysis Reports (APARs) relacionados e as correções provisórias. Para exibir os resultados deste
| relatório, insira o comando a seguir:

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

| **Referências relacionadas**:

| "Comando psconf" na página 39

Resolução de Problemas no Trusted Network Connect e Gerenciamento de Correção

Aprenda as causas possíveis para a falha e as etapas para solucionar problemas no TNC e no sistema de gerenciamento de correção.

Para solucionar problemas do TNC e o sistema de gerenciamento de correção, verifique as definições de configuração listadas na tabela seguir.

Tabela 3. Resolução de problemas nas definições de configuração para TNC e sistema de gerenciamento de Correção

Problema	Solução
O servidor TNC não está sendo iniciado ou respondendo	Conclua o procedimento a seguir: 1. Determine se o daemon do servidor TNC está sendo executado, executando o comando: `ps –eaf | grep tnccsd` 2. Se não estiver em execução, exclua o arquivo `/var/tnc/.tncsock`. 3. Reinicie o servidor. Se isso não resolver o problema, verifique o arquivo de configuração `/etc/tnccs.conf` para a entrada `component = SERVER` no servidor TNC.
O servidor de gerenciamento de correção TNC não está iniciando ou respondendo	• Determine se o daemon do servidor de gerenciamento de correção TNC está sendo executado, inserindo o comando a seguir: `ps –eaf | grep tncpmd` • Verifique o arquivo de configuração `/etc/tnccs.conf` para a entrada `component = TNCPM` no servidor de gerenciamento de correção TNC.
O cliente TNC não está iniciando ou respondendo	• Determine se o daemon do cliente TNC está sendo executado, inserindo o comando a seguir: `ps –eaf | grep tnccsd` • Verifique o arquivo de configuração `/etc/tnccs.conf` para a entrada `component = CLIENT` no cliente TNC.
O referenciador TNC IP não está em execução no Virtual I/O Server (VIOS)	• Determine se o daemon do referenciador TNC está sendo executado, inserindo o comando a seguir: `ps –eaf | grep tnccsd` • Verifique o arquivo de configuração `/etc/tnccs.conf` para a entrada `component = IPREF` no VIOS.
Não foi possível configurar um sistema como um servidor ou cliente TNC	O servidor e o cliente TNC não podem ser executados simultaneamente no mesmo sistema.
Os daemons estão em execução, mas a verificação não acontece	Ative as mensagens de log para os daemons. Configure o log `level=info` no arquivo `/etc/tnccs.conf`. É possível analisar as mensagens de log.

Comandos do PowerSC Standard Edition

O PowerSC Standard Edition fornece comandos que permitem a comunicação com o componente Trusted Firewall e o componente Trusted Network Connect usando a linha de comandos.

Comando chvfilt

Propósito

Altera os valores para a regra de filtragem cruzado de LAN virtual existente.

Sintaxe

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>]

Descrição

O comando **chvfilt** é usado para alterar a definição de uma regra de filtro cruzado de LAN virtual na tabela da regra de filtro.

Sinalizadores

-a Especifica a ação. Valores válidos a seguir:
- D (Negar): Bloqueia o tráfego
- P (Permitir): Permite o tráfego

-c Especifica diferentes protocolos aos quais a regra de filtragem é aplicável. Valores válidos a seguir:
- udp
- icmp
- icmpv6
- tcp
- qualquer

-d Especifica o endereço de destino no formato IPv4 ou IPv6.

-m Especifica a máscara de endereço de origem.

-M Especifica a máscara de endereço de destino.

-n Especifica o ID do filtro da regra de filtragem que deve ser modificada.

-o Especifica a porta de origem ou a operação do tipo Internet Control Message Protocol (ICMP). Valores válidos a seguir:
- lt
- gt
- eq
- qualquer

-O Especifica a porta de destino ou a operação do código ICMP. Valores válidos a seguir:
- lt
- gt
- eq
- qualquer

-p Especifica a porta de origem ou o tipo ICMP.

-P Especifica a porta de destino ou o código ICMP.

-s Especifica o endereço de origem no formato v4 ou v6.

-v Especifica a versão IP da tabela da regra de filtragem. Os valores válidos são 4 e 6.

-z Especifica o ID de LAN virtual da partição lógica de origem.

-Z Especifica o ID de LAN virtual da partição lógica de destino.

Status de Saída

Este comando retorna os valores de saída a seguir:

0 Conclusão bem-sucedida.

>0 Ocorreu um erro.

Exemplos

1. Para alterar uma regra de filtro válido que existe no kernel, digite o comando da seguinte maneira:

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

2. Quando uma regra de filtragem (n=2) não existir no kernel, a saída será a seguinte:

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

   O sistema exibe a saída da seguinte maneira:

   ```
   ioctl(QUERY_FILTER) failed no filter rule err=2
   Não é possível alterar a regra de filtragem.
   ```

Comando genvfilt

Propósito

Inclui uma regra de filtragem para o cruzamento Virtual LAN (VLAN) entre as partições lógicas no mesmo servidor IBM Power Systems.

Sintaxe

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**>]

Descrição

O comando **genvfilt** inclui uma regra de filtragem para o cruzamento Virtual LAN (VLAN) entre as partições lógicas (LPARs) no mesmo servidor IBM Power Systems.

Sinalizadores

-a Especifica a ação. Valores válidos a seguir:
- D (Negar): Bloqueia o tráfego
- P (Permitir): Permite o tráfego

-c Especifica diferentes protocolos aos quais a regra de filtragem é aplicável. Valores válidos a seguir:
- udp
- icmp
- icmpv6
- tcp
- qualquer

-d Especifica o endereço de destino no formato v4 ou v6.

-m Especifica a máscara do endereço de origem

-M Especifica a máscara de endereço de destino.

-o Especifica a porta de origem ou a operação do tipo Internet Control Message Protocol (ICMP). Valores válidos a seguir:
- lt
- gt
- eq
- qualquer

-O Especifica a porta de destino ou a operação do código ICMP. Valores válidos a seguir:
- lt
- gt

- eq
- qualquer

-p Especifica a porta de origem ou o tipo ICMP.

-P Especifica a porta de destino ou o código ICMP.

-s Especifica o endereço de origem no formato IPv4 ou IPv6.

-v Especifica a versão IP da tabela da regra de filtragem. Os valores válidos são 4 e 6.

-z Especifica o ID de LAN virtual do LPAR de origem. O ID de LAN virtual deve estar no intervalo de 1 a 4096.

-Z Especifica o ID de LAN virtual do LPAR de destino. O ID de LAN virtual deve estar no intervalo de 1 a 4096.

Status de Saída

Este comando retorna os valores de saída a seguir:

0 Conclusão bem-sucedida.

>0 Ocorreu um erro.

Exemplos

1. Para incluir uma regra de filtragem para permitir dados TCP a partir de um ID VLAN de origem de 100 para um ID VLAN de destino de 200 em portas específicas, digite o comando a seguinte maneira:

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

Referências relacionadas:

"Comando mkvfilt" na página 35

"Comando vlantfw" na página 45

Comando lsvfilt

Propósito

Lista regras de filtragem de cruzamento de LAN virtual a partir da tabela de filtro.

Sintaxe

lsvfilt [**-a**]

Descrição

O comando **lsvfilt** é usado para listar as regras de filtragem de cruzamento de LAN virtual e seus status.

Sinalizadores

-a Lista apenas as regras de filtragem ativas.

Status de Saída

Este comando retorna os valores de saída a seguir:

0 Conclusão bem-sucedida.

>0 Ocorreu um erro.

Exemplos

1. Para listar todas as regras de filtro ativo no kernel, digite o comando da seguinte maneira:

```
lsvfilt -a
```

Conceitos relacionados:

"Desativando Regras" na página 16
É possível desativar as regras que permitem o roteamento de VLAN cruzada no recurso Firewall Confiável.

Comando mkvfilt
Propósito

Ativa as regras de filtragem de cruzamento de LAN virtual definidas pelo comando **genvfilt**.

Sintaxe

mkvfilt -u

Descrição

O comando **mkvfilt** ativa as regras de filtro de cruzamento de LAN virtual definidas pelo comando **genvfilt**.

Sinalizadores

-u Ativa as regras de filtragem na tabela da regra de filtragem.

Status de Saída

Este comando retorna os valores de saída a seguir:

0 Conclusão bem-sucedida.

>0 Ocorreu um erro.

Exemplos

1. Para ativar as regras de filtragem no kernel, digite o comando da seguinte maneira:

```
mkvfilt -u
```

Referências relacionadas:

"Comando genvfilt" na página 33

Comando pmconf
Propósito

Relata e gerencia o servidor Trusted Network Connect Patch Management (TNCPM) confiável registrando os níveis de tecnologia e servidores TNC para as mais recentes correções e gerando relatórios no status TNCPM.

Nota: O servidor TNCPM deve ser executado apenas no AIX Versão 7.1 com Nível de Tecnologia 7100-02 para permitir o download do metadados do service pack.

Sintaxe

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*

Descrição

As funções do comando **pmconf** são as seguintes:

Gerenciamento do repositório de correção
Registra ou remove o registro dos níveis de tecnologia; remove os registros dos servidores TNC. O TNCPM cria um repositório de correção para cada nível de tecnologia que contém as mais recentes correções, informações **lslpp** (por exemplo, informações sobre os conjuntos de arquivos instalados ou atualizações do conjunto de arquivos) e informações da correção de segurança para esse nível de tecnologia.

Relatório
Gera relatórios no status de TNCPM.

As operações a seguir podem ser executadas usando o comando **pmconf**:

Item	Descrição
add	Registra um novo nível de tecnologia usando o TNCPM.
chtncpm	Altera os atributos no arquivo tnccs.conf. Um comando **start** explícito é necessário para que as mudanças entrem em vigor no servidor TNCPM.
delete	Cancela o registro de um nível de tecnologia usando TNCPM.
history	Exibe a atualização e o histórico de download.
listar	Exibe as informações sobre TNCPM.
log	Configura o nível de log para os componentes TNC.
mktncpm	Cria o servidor TNCPM.
modify	Modifica os atributos tncpm.conf.
rmtncpm	Remove o servidor TNCPM.
start	Inicia o servidor TNCPM.
stop	Para o servidor TNCPM.

Sinalizadores

Item	Descrição
-A	Aceita todos os contratos de licença ao executar as atualizações de cliente.
-a <advisory file>	Especifica o arquivo consultivo que corresponde ao parâmetro **ifix**. Se o arquivo consultivo não for fornecido, o parâmetro **ifix** não será visualizado como um endereço Common Vulnerabilities and Exposures (CVE) da correção provisória.
-e <ifix file>	Especifica as correções provisórias incluídas no TNCPM.
-i *download_interval*	Especifica o intervalo que o TNCPM verifica para um novo service pack para os níveis de tecnologia registrados. O intervalo é um valor de número inteiro que representa os minutos ou no formato a seguir: **d** (nº de dias): **h** (horas): **m** (minutos).
-K <ifix key>	Especifica a chave pública do IBM AIX Product Security Incident Response Tool (PSIRT) que é usada para autenticar os consultores transferidos por download e as correções provisórias. Esta chave pública pode ser transferida por download a partir de um servidor de chave pública PGP usando o ID **0x28BFAA12**.
-p *SP_list*	Especifica uma lista de service packs a ser transferida por download. A lista é uma lista separada por vírgula no formato, REL00-TL-SP (por exemplo, `6100-01-04` representa o service pack 04 para o nível de tecnologia 01 e versão 6.1). Ao usar o sinalizador -U, especifique apenas um SP.
-t *APAR_type_list*	Especifica os tipos APAR que o TNCPM suporta para a atualização de cliente e atendimento do servidor TNC. Os APARs de segurança são sempre suportados. APAR_type_list é uma lista separada por vírgula dos tipos a seguir: HIPER, FileNet Process Engine, Enhancement.
-P *fix_repository_path*	Especifica o diretório de download para os repositórios de correção que serão transferidos por download por TNCPM. O diretório padrão é **/var/tnc/tncpm/fix_repository**.
-U *user_defined_fix_repository*	Especifica o caminho até o repositório de correção definido pelo usuário. Especifique a liberação, o nível de tecnologia e o service pack que estão associados ao repositório de correção que é usado para verificação e atualizações de clientes.
-s	Gera um relatório de service packs registrados.
-l *SP*	Gera um relatório de informações **lslpp** para o service pack. *SP* está no formato, REL00-TL-SP (por exemplo, `6100-01-04` representa o service pack 04 para o nível de tecnologia 01 e versão 6.1).
-u	Gera um relatório do histórico de atualização de cliente.
-d	Gera um relatório do histórico de download do service pack.
-C	Gera um relatório para o certificado do servidor.

Item	Descrição
-a *SP*	Gera um relatório de informações Authorized Program Analysis Report (APAR) de segurança para o service pack. *SP* está no formato, REL00-TL-SP (por exemplo, `6100-01-04` representa o service pack 04 para o nível de tecnologia 01 e versão 6.1).
-f *filename*	Especifica o nome do arquivo de certificado.
-k *key_filename*	Especifica o arquivo do qual a chave do certificado deve ser lido no caso de uma operação de importação.

-c	Exibe os atributos do usuário nos registros separados por dois pontos, da seguinte maneira:
	`# name: attribute1: attribute2: ...`
	`policy: value1: value2: ...`

-v <*signature file*>	Especifica o arquivo de assinaturas para o consultor de vulnerabilidade IBM AIX.
-y <*advisory file*>	Especifica um arquivo do consultor de vulnerabilidade IBM AIX.
-q	Suprime as informações do cabeçalho.
-x <*ifix interval*>	Especifica o intervalo em minutos para o qual verificar e fazer o download de novas correções provisórias. Se este valor estiver configurado como 0, a notificação e o download de correção provisória automático serão desativados. O intervalo padrão é a cada 24 horas.

Status de Saída

Este comando retorna os valores de saída a seguir:

Item	Descrição
0	O comando foi executado com êxito e todas as mudanças solicitadas são feitas.
>0	Ocorreu um erro. A mensagem de erro impressa inclui mais detalhes sobre o tipo de falha.

Exemplos

1. Para inicializar TNCPM, insira o comando a seguir:
   ```
   pmconf init -f 10080 -l 5300-11,6100-00
   ```
2. Para criar o daemon TNCPM, insira o comando a seguir:
   ```
   mktncpm pmport=55777 tncserver=11.11.11.11:77555
   ```
3. Para iniciar o servidor, insira o comando a seguir:
   ```
   pmconf start
   ```
4. Para parar o servidor, insira o comando a seguir:
   ```
   pmconf stop
   ```
5. Para registrar um novo nível de tecnologia usando TNCPM, insira o comando a seguir:
   ```
   pmconf add -l 6100-01
   ```
6. Para cancelar registro de um nível de tecnologia de TNCPM, insira o comando a seguir:
   ```
   pmconf delete -l 6100-01
   ```
7. Para cancelar registro de um servidor TNC que possui um endereço IP 11.11.11.11 de TNCPM, insira o comando a seguir:
   ```
   pmconf delete -t 11.11.11.11
   ```
8. Para registrar uma versão mais recente de um service pack mais antigo para TNCPM, insira o comando a seguir:
   ```
   pmconf add -s 6100-01-04
   ```
9. Para cancelar registro de um service pack mais antigo do TNCPM, insira o comando a seguir:
   ```
   pmconf delete -s 6100-01-04
   ```
10. Para gerar um relatório de repositórios de correção para cada nível de tecnologia registrado, insira o comando a seguir:
    ```
    pmconf list -s
    ```
11. Para gerar um relatório de informações **lslpp** de um nível de tecnologia registrado, insira o comando a seguir:
    ```
    pmconf list -l 6100-01-02
    ```
12. Para gerar um relatório a partir do histórico de atualização, insira o comando a seguir:

```
pmconf hist -u
```

13. Para gerar um relatório a partir do histórico de download, insira o comando a seguir:
```
pmconf hist -d
```
14. Para gerar um relatório do certificado do servidor, insira o comando a seguir:
```
pmconf list -C
```
15. Para gerar um relatório de informações APAR de segurança do service pack, insira o comando a seguir:
```
pmconf list -a 6100-01-02
```
16. Para importar um certificado do servidor, insira o comando a seguir:
```
pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt
```
17. Para exportar o certificado do servidor, insira o comando a seguir:
```
pmconf export -f /tmp/server.txt
```

Comando psconf

Propósito

Relata e gerencia o servidor Trusted Network Connect (TNC), o cliente TNC, o TNC IP Referrer (IPRef) e Service Update Management Assistant (SUMA). Gerencia o conjunto de arquivos e as políticas de gerenciamento de correção a respeito da integridade do terminal (servidor e cliente) ou após a conexão de rede para proteger a rede das ameaças e ataques.

Sintaxe

Operações do servidor TNC:

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>**

| Operações do cliente TNC:

| **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>*

| Operações TNC IPRef:

| **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

Descrição

A tecnologia TNC é uma arquitetura baseada em padrão aberta para autenticação de terminal, medição de integridade de plataforma e integração de sistemas de segurança. A arquitetura TNC inspeciona os terminais (clientes e servidores de rede) para conformidade com as políticas de segurança antes de permiti-las na rede protegida. O TNC IPRef notifica o servidor TNC sobre quaisquer novos IPs que forem detectados no Virtual I/O Server (VIOS).

O SUMA ajuda a mover os administradores de sistema para longe da tarefa de recuperar manualmente as atualizações de manutenção da web. Ele oferece opções flexíveis que permitem que o administrador do sistema configure uma interface automatizada para fazer o download de correções de um website de distribuição de correção para seus sistemas.

O comando **psconf** gerencia o servidor de rede e os clientes incluindo ou excluindo as políticas de segurança, validando os clientes como confiáveis ou não confiáveis, gerando relatórios e atualizando o servidor e o cliente.

As operações a seguir podem ser executadas usando o comando **psconf**:

Item	Descrição
add	Inclui uma política, um cliente ou informações de email no servidor TNC.
apargrp	Especifica os nomes do grupo APAR como parte da política do conjunto de arquivos que são usados para verificação de clientes TNC.
aparlist	Especifica a lista de APARs que fazem parte do grupo APAR.
certadd	Marca o certificado como confiável ou não confiável.
certdel	Exclui as informações do cliente.
chclient	Altera os atributos no arquivo `tnccs.conf`. Um comando **start** explícito é necessário para que as mudanças ocorram no cliente TNC. A sintaxe de attribute=value será igual a do **mkclient**.
chipref	Altera os atributos no arquivo `tnccs.conf`. Um comando **start** explícito é necessário para que as mudanças entrem em vigor em IPRef. A sintaxe de attribute=value é igual à do **mkipref**.
chserver	Altera os atributos no arquivo `tnccs.conf`. Um comando **start** explícito é necessário para que as mudanças entrem em vigor no servidor TNC. A sintaxe de attribute=value é igual à do **mkserver**. **Nota:** O atributo **dbpath** não pode ser alterado usando o comando **chserver**. Ele pode ser configurado apenas ao executar o **mkserver**.
dbpath	Especifica o local do banco de dados TNC. O valor padrão é `/var/tnc`.
delete	Exclui uma política ou as informações do cliente.
export	Exporta o certificado do cliente ou do servidor, ou o banco de dados no servidor TNC.
fspolicy	Especifica a política do conjunto de arquivos na liberação, nível de tecnologia e service pack que são usados para verificação de Clientes TNC.
import	Importa um certificado no cliente ou servidor, ou banco de dados no servidor TNC.
ipgroup	Especifica o grupo Internet Protocol (IP) que contém múltiplos endereços IP do cliente ou nomes de host.
listar	Exibe informações sobre o servidor TNC, o cliente TNC ou o SUMA.
log	Configura o nível de log para os componentes TNC.
mkclient	Configura o cliente TNC.
mkipref	Configura o TNC IPRef.
mkserver	Configura o servidor TNC.
pmport	Especifica o número da porta no qual o **pmserver** atende. O valor padrão é 38240.
pmserver	Especifica o nome do host ou o endereço IP do comando **suma** que faz download dos service packs mais recentes e correções de segurança disponíveis no website IBM® ECC e website IBM Fix Central.
recheck_interval	Especifica o intervalo em minutos ou formato d (days) : h (hours) : m (minutes) para o servidor TNC verificar os clientes TNC. **Nota:** Um valor **recheck_interval=0** significa que o planejador não inicia a verificação dos clientes em intervalos regulares e os clientes registrados são automaticamente verificados durante a inicialização. Nesses casos, o cliente pode ser manualmente verificado.
relatório	Gera um relatório que possui uma extensão de arquivo .txt ou .csv.

Item	Descrição
restart	Reinicia o cliente TNC, o servidor TNC ou o TNC IPRef.
rmclient	Remove a configuração do cliente TNC.
rmipref	Remove a configuração do TNC IPRef.
rmserver	Remove a configuração do servidor TNC.
start	Inicia o cliente TNC, o servidor TNC ou o TNC IPRef.
status	Mostra o status da configuração TNC.
stop	Para o cliente TNC, o servidor TNC ou o TNC IPRef.
tncport	Especifica o número da porta no qual o servidor TNC atende. O valor padrão é 42830.
tncserver	Especifica o servidor TNC que verifica ou atualiza os clientes TNC.
tssserver	Especifica o IP ou o nome do host do servidor Trusted Surveyor.
update	Instala as correções no cliente.
verificar	Inicia uma verificação manual do cliente.

Sinalizadores

Item	Descrição
-A <advisoryName>	Especifica o nome do consultor para o relatório.
-B <buildinfo>	Especifica as informações de construção para preparar um relatório de correção.

-c	Exibe os atributos do usuário nos registros separados por dois pontos da seguinte maneira:
	`# name: attribute1: attribute2: ...`
	`policy: value1: value2: ...`

-C	Especifica que a operação é para o componente do cliente.
Caminho dir/local do arquivo de banco de dados **-d** *do banco de dados*	Especifica o local do caminho do arquivo para importação do banco de dados/especifica o local do caminho do diretório para exportação do banco de dados.
-D *yyyy-mm-dd*	Especifica a data para uma determinada entrada do cliente no histórico de log, em que *yyyy* é o ano, *mm* é o mês e *dd* é o dia.
-e *emailid* **ipgroup=[±]***g1, g2...*	Especifica o Id do email seguido por uma lista de nomes do grupo de IPs separados por vírgula.
-E | FAIL | COMPLIANT | ALL |	Especifica o evento para o qual os emails precisam ser enviados para o Id do email configurado. FAIL- Os correios são enviados quando o status de verificação do cliente for FAILED. COMPLIANT- Os correios são enviados quando o status de verificação do cliente for COMPLAINT. ALL - Os correios são enviados para todos os statuses da verificação do cliente.
-f *filename*	Especifica o arquivo do qual o certificado deve ler no caso de uma operação de importação ou especifica o local para o qual o certificado deve ser gravado no caso de uma operação de exportação.
-F *fspolicy buildinfo*	Especifica o nome da política do sistema de arquivos, seguido pelas informações de construção. As informações de construção podem ser fornecidas no formato a seguir: `6100-04-01`, em que `6100` representa a versão 6.1, `04` é o nível de manutenção e `01` é o service pack.
-G *ipgroupname* **ip=[±]***ip1, ip2...*	Especifica o nome do grupo de IPs seguido por uma lista de IPs separados por vírgula.
-H	Lista o log do histórico.
-i *host*	Especifica o endereço IP ou o nome do host.
-I ip=[±]*ip1, ip2...* | [±] host1,host2...	Especifica o IP/nome do host que deve ser ignorando durante a verificação.
-k *filename*	Especifica o arquivo do qual a chave do certificado deve ser lido no caso de uma operação de importação.
-p	Visualiza a atualização de cliente TNC.
-P <policyName>	Especifica o nome da política para preparar um relatório de política do cliente.
-q	Suprime as informações do cabeçalho.
-r *buildinfo*	Gera o relatório baseado nas informações de construção. As informações de construção podem ser fornecidas no formato a seguir: `6100-04-01`, em que `6100` representa a versão 6.1, `04` é o nível de manutenção e `01` é o service pack.
-R	Especifica que a operação é para o componente IPRef.

Item	Descrição
-s COMPLIANT | IGNORE | FAILED | ALL	Exibe o cliente por status da seguinte maneira: **COMPLIANT** Exibe os clientes ativos. **IGNORE** Exibe os clientes que são excluídos de qualquer verificação. **FAILED** Exibe os clientes que falharam na verificação segundo a política configurada. **ALL** Exibe todos os clientes independentemente de seus statuses.
-S <host>	Especifica o nome do host para preparar um relatório de correção de segurança do cliente.
-t TRUSTED | UNTRUSTED	Marca o cliente especificado como confiável ou não confiável. **Nota:** Apenas os administradores de sistema podem verificar o servidor ou o cliente como confiável ou não confiável.
-T	Especifica que o cliente pode acessar as solicitações de qualquer servidor TS que possui um certificado válido.
-u	Desinstale uma correção provisória que é instalada em um cliente TNC.
-v	Especifica uma lista de correção provisória separada por vírgula.
-V	Especifica o nome do grupo de correção provisória.

Status de Saída

Este comando retorna os valores de saída a seguir:

Item	Descrição
0	O comando foi executado com êxito e todas as mudanças solicitadas são feitas.
>0	Ocorreu um erro. A mensagem de erro impressa inclui mais detalhes sobre o tipo de falha.

Exemplos

1. Para iniciar o servidor TNC, insira o comando a seguir:
   ```
   psconf start server
   ```
2. Para incluir uma política do sistema de arquivos denominada `71D_latest` para a construção `7100-04-02`, insira o comando a seguir:
   ```
   psconf add -F 71D_latest 7100-04-02
   ```
3. Para excluir uma política do sistema de arquivos denominada `71D_old`, insira o comando a seguir:
   ```
   psconf delete -F 71D_old
   ```
4. Para validar se o cliente que possui um endereço IP de `11.11.11.11` é **trusted**, insira o comando a seguir:
   ```
   psconf certadd -i 11.11.11.11 -t TRUSTED
   ```
5. Para excluir o cliente que possui um endereço IP de `11.11.11.11` do servidor, insira o comando a seguir:
   ```
   psconf certdel -i 11.11.11.11
   ```
6. Para verificar as informações do cliente que possuem um endereço IP de `11.11.11.11`, insira o comando a seguir:
   ```
   psconf verify -i 11.11.11.11
   ```
7. Para exibir as informações do cliente que possuem um endereço IP de `11.11.11.11`, insira o comando a seguir:
   ```
   psconf list -i 11.11.11.11
   ```
8. Para gerar o relatório para os clientes que estão no status **COMPLAINT**, insira o comando a seguir:
   ```
   psconf list -s CPMPLIANT -i ALL
   ```
9. Para gerar o relatório para o `7100-04-02` de construção, insira o comando a seguir:
   ```
   psconf list -r 7100-04-02
   ```

10. Para exibir o histórico de conexão de um cliente que possui um endereço IP de 11.11.11.11, insira o comando a seguir:
    ```
    psconf list -H -i 11.11.11.11
    ```
11. Para excluir a entrada de um cliente que possui um endereço IP 11.11.11.11 do histórico de log mais antigo ou igual a 1º de fevereiro de 2009, insira o comando a seguir:
    ```
    psconf delete -H -i 11.11.11.11 -D 2009-02-01
    ```
12. Para importar o certificado de cliente de um cliente que possui o endereço IP 11.11.11.11 a partir do servidor, insira o comando a seguir:
    ```
    psconf import -C -i 11.11.11.11 -f /tmp/client.txt
    ```
13. Para exportar o certificado do servidor de um cliente, insira o comando a seguir:
    ```
    psconf export -S -f /tmp/server.txt
    ```
14. Para atualizar o cliente que possui um endereço IP de 11.11.11.11 para um nível apropriado do servidor, insira o comando a seguir:
    ```
    psconf update -i 11.11.11.11
    ```
15. Para exibir os status do cliente, insira o comando a seguir:
    ```
    psconf status
    ```
16. Para exibir o certificado de cliente, insira o comando a seguir:
    ```
    psconf list -C
    ```
17. Para iniciar o cliente, insira o seguinte comando:
    ```
    psconf start client
    ```

Segurança

Os usuários RBAC de atenção e os usuários AIX confiáveis:

Este comando pode executar operações privilegiadas. Somente usuários privilegiados podem executar essas operações. Para obter informações adicionais sobre a autorização e os privilégios, consulte Banco de Dados do Comando Privilegiado na Segurança. Para uma lista de privilégios e as autorizações associadas a esse comando, consulte o comando **lssecattr** ou o subcomando **getcmdattr**

Comando rmvfilt

Propósito

Remove as regras de filtragem de cruzamento de LAN virtual a partir da tabela de filtro.

Sintaxe

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

Descrição

O comando **rmvfilt** é usado para remover as regras de filtragem de cruzamento de LAN virtual a partir da tabela de filtro.

Sinalizadores

-n Especifica o ID da regra de filtragem que será removido. A opção **all** é usada para remover todas as regras de filtragem.

Status de Saída

Este comando retorna os valores de saída a seguir:

0 Conclusão bem-sucedida.

>0 Ocorreu um erro.

Exemplos

1. Para remover todas as regras de filtragem ou para desativar todas as regras de filtragem no kernel, digite o comando da seguinte maneira:

   ```
   rmvfilt -n all
   ```

Conceitos relacionados:

"Desativando Regras" na página 16
É possível desativar as regras que permitem o roteamento de VLAN cruzada no recurso Firewall Confiável.

Comando vlantfw

Propósito

Exibe ou limpa o IP e as informações de mapeamento Media Access Control (MAC) e controla a função de criação de log.

Sintaxe

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

Descrição

O comando **vlantfw** exibe ou limpa as entradas de mapeamento IP e MAC. Ele também fornece a capacidade de iniciar ou parar o recurso de criação de log de Firewall Confiável.

Sinalizadores

-d Exibe todas as informações de mapeamento IP.

-D Exibe os dados de conexão coletados.

-E Exibe os dados de conexão entre as partições lógicas (LPARs) em diferentes complexos do processador central.

-f Remove todas as informações de mapeamento IP.

-F Limpa o cache de dados de conexão.

-G Exibe as regras de filtragem que podem ser configuradas para rotear o tráfego internamente usando o Firewall Confiável.

-I Exibe os dados de conexão entre LPARs que estão associados com diferentes IDs de VLAN, mas compartilham os mesmos complexos do processador central.

-l Inicia o recurso de criação de log de Firewall Confiável.

-L Para o recurso de criação de log de Firewall Confiável e redireciona o conteúdo do arquivo de rastreio para o arquivo `/home/padmin/svm/svm.log`.

-m Ativa o monitoramento de Firewall Confiável.

-M Desativa o monitoramento de Firewall Confiável.

-q Consulta o status de máquina virtual segura.

-s Inicia o Firewall Confiável.

-t Para o Firewall Confiável.

Parâmetros

-N *integer*
Exibe a regra de filtragem que corresponde ao número inteiro que é especificado.

Status de Saída

Este comando retorna os valores de saída a seguir:

0 Conclusão bem-sucedida.

>0 Ocorreu um erro.

Exemplos

1. Para exibir todos os mapeamentos IP, digite o comando da seguinte maneira:
   ```
   vlantfw -d
   ```
2. Para remover todos os mapeamentos IP, digite o comando da seguinte maneira:
   ```
   vlantfw -f
   ```
3. Para iniciar a função de criação de log de Firewall Confiável, digite o comando da seguinte maneira:
   ```
   vlantfw -l
   ```
4. Para verificar o status de uma máquina virtual segura, digite o comando da seguinte maneira:
   ```
   vlantfw -q
   ```
5. Para iniciar o firewall confiável, digite o comando da seguinte maneira:
   ```
   vlantfw -s
   ```
6. Para parar o firewall confiável, digite o comando da seguinte maneira:
   ```
   vlantfw -t
   ```
7. Para exibir as regras correspondentes que podem ser usadas para gerar os filtros que roteiam o tráfego no complexo do processador central, digite o comando da seguinte maneira:
   ```
   vlantfw -G
   ```

Referências relacionadas:

"Comando genvfilt" na página 33

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇAO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira responsabilidade do Cliente.

IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

© Copyright IBM Corp. 2012, 2013

Licenciados deste programa que desejam obter informações sobre este assunto com o objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) a utilização mútua das informações trocadas, devem entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, Contrato Internacional de Licença do Programa IBM ou de qualquer outro contrato equivalente.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores.

Todas as instruções relativas à direção ou intento futuro da IBM estão sujeitas a mudanças ou retirada sem aviso e representam apenas objetivos.

Todos os preços IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a alteração sem aviso prévio. Os preços para o revendedor podem variar.

Estas informações foram projetadas apenas com o propósito de planejamento. As informações aqui contidas estão sujeitas a alterações antes que os produtos descritos estejam disponíveis.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos incluem nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com nomes e endereços utilizados por uma empresa real é mera coincidência.

LICENÇA DE COPYRIGHT:

Estas informações contêm programas de aplicativos de amostra na linguagem fonte, ilustrando as técnicas de programação em diversas plataformas operacionais. O Cliente pode copiar, modificar e distribuir estes programas de amostra sem a necessidade de pagar à IBM, com objetivos de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo para a plataforma operacional para a qual os programas de amostra são criados. Esses exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou implicar a confiabilidade, manutenção ou função destes programas. Os programas de amostra são fornecidos "NO ESTADO EM QUE SE ENCONTRAM", sem garantia de nenhum tipo. A IBM não é responsável por nenhum dano decorrente do uso dos programas de amostra.

Cada cópia ou parte destes programas de amostra ou qualquer trabalho derivado deve incluir um aviso de copyright com os dizeres:

© (nome de sua empresa) (ano). Partes deste código são derivadas dos Programas de Amostras da IBM Corp. © Copyright IBM Corp. _digite o ano ou anos_.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

Considerações sobre Política de Privacidade

Os Produtos de software IBM, incluindo soluções de software como serviço, (“Ofertas de Software”) podem usar cookies ou outras tecnologias para coletar informações de uso do produto, para ajudar a melhorar a experiência do usuário final, para customizar as interações com o usuário final ou para outros fins. Em muitos casos, nenhuma informação pessoalmente identificável é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar a coletar informações pessoalmente identificáveis. Se esta Oferta de Software usar cookies para coletar informações pessoalmente identificáveis, informações específicas sobre o uso de cookies desta oferta serão definidas abaixo.

Esta Oferta de Software não usa cookies ou outras tecnologias para coletar informações pessoalmente identificáveis.

Se as configurações implementadas para esta Oferta de Software fornecerem a você como cliente a capacidade de coletar informações pessoalmente identificáveis de usuários finais via cookies e outras tecnologias, você deve buscar seu próprio aconselhamento jurídico sobre quaisquer leis aplicáveis a tal coleta de dados, incluindo requisitos para aviso e consenso.

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para estes fins, consulte a Política de Privacidade da IBM em http://www.ibm.com/privacy e Declaração de Privacidade Online da IBM na http://www.ibm.com/privacy/details seção titulada “Cookies, Web Beacons and Other Technologies” e “IBM Software Products and Software-as-a-Service Privacy Statement” em http://www.ibm.com/software/info/product-privacy.

Marcas Registradas

IBM, o logotipo IBM e ibm.com são marcas ou marcas registradas da International Business Machines Corp., registradas em vários países no mundo todo. Outros nomes de produtos e serviços podem ser marcas registradas da IBM ou de outras empresas. Uma lista atual de marcas registradas da IBM está disponível na web em Copyright and trademark information em www.ibm.com/legal/copytrade.shtml.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.

Java e todas as marcas registradas e logotipos baseados em Java são marcas ou marcas registradas da Oracle e/ou de suas afiliadas.

Índice Remissivo

A

Atestando um Sistema 8
Atualizando o Cliente TNC 29

C

Cliente TNC 21
comando chvfilt 31
Comando genvfilt 33
Comando lsvfilt 34
Comando mkvfilt 35
Comando pmconf 35
Comando psconf 39
Comando rmvfilt 44
Comando vlantfw 45
Comandos
  chvfilt 31
  genvfilt 33
  lsvfilt 34
  mkvfilt 35
  rmvfilt 44
  vlantfw 45
Componentes 20
comunicação segura 22
conceitos 20
Conceitos de Firewall Confiável 10
Conceitos de Inicialização Confiável 4
Configurando 24
Configurando a Criação de Log Confiável 19
Configurando a Inicialização Confiável 7
Configurando o Cliente 24
Configurando o Servidor 24
Configurando o Servidor do Gerenciamento de Correção 24
Considerações de Migração 6
Criação de Log Confiável 17, 18, 20
  instalando 18

E

Excluindo os Sistemas 9

F

Firewall Confiável 10
  configurando 13
    múltiplos SEAs 14
  criando regras 15
  desativando regras 16
  instalando 12
  removendo
    SEAs 15

G

Gerenciamento de Correções 21
Gerenciando a Inicialização Confiável 8
Gerenciando políticas 29
Gerenciando TNC e gerenciamento de Correção 27
Gravando os Dados para os Dispositivos de Log Virtual 20

I

importar certificados 22
Importar certificados 29
Inicialização Confiável 4, 5, 6, 7, 8, 9
Inscrevendo um sistema 7
Instalando 3, 23
Instalando a Inicialização Confiável 7
Instalando o Coletor 7
Instalando o PowerSC Standard Edition 3
Instalando o Verificador 7
Interpretando Resultados de Atestado 8

L

logs virtuais 17

M

Módulos IMC e IMV 22

N

notificação por email 26

P

Planejando 5
Políticas do Cliente 27
PowerSC
  Criação de Log Confiável
    instalando 18
  Firewall Confiável
    configurando 13
    configurando com múltiplos SEAs 14
    criando regras 15
    desativando regras 16
    instalando 12
    removendo SEAs 15
PowerSC Standard Edition 1, 2, 3
Pré-requisitos 5
Preparando para Correção 6
Protocolo 22

R

Referenciador IP 21
Referenciador IP no VIOS 26
Relatório e ferramenta de gerenciamento para TNC, SUMA
  usando o comando psconf 39
Relatório e ferramenta de gerenciamento para TNCPM
  usando o comando pmconf 35
requisitos de hardware e software 2
resolução de problemas 9
Resolução de Problemas no TNC e Gerenciamento de
  Correção 30

© Copyright IBM Corp. 2012, 2013

S

Servidor 21
servidor Trusted Network Connect 26
Servidor Trusted Network Connect 27
Subsistema de Auditoria AIX 19
SUMA 21
syslog AIX 19

T

TNC 30
Trusted Network Connect 20, 21, 22, 23, 24, 26, 27, 28, 29
Trusted Network Connect e Gerenciamento de Correção 20

V

Verificação do Cliente 28
visão geral 2, 20
Visão Geral da Criação de Log de Firewall Confiável 17
Visualizando Dispositivos de Log Virtual 18
Visualizando Logs 27
Visualizando os Resultados de Verificação 28

Impresso no Brasil