IBM PowerSC

Standard Edition

Versão 1.1.4

PowerSC Standard Edition

IBM PowerSC

Standard Edition

Versão 1.1.4

PowerSC Standard Edition

Nota
Antes de usar esta informação e o produto que elas suportam, leia as informações em “Avisos” na página 167.

Esta edição se aplica ao IBM PowerSC Standard Edition Versão 1.1.4 e a todas as liberações e modificações subsequentes, até que seja indicado de outra maneira em novas edições.

Índice

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.

O que há de novo no PowerSC Standard Edition 1.1.4

Leia sobre informações novas ou significativamente mudadas para a coleção de tópico do PowerSC Standard Edition Versão 1.1.4.

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

Dezembro de 2015

- Informações incluídas sobre perfis de conformidade nos tópicos a seguir:
  - "Conformidade da North American Electric Reliability Corporation" na página 100
  - "Conformidade do Payment Card Industry - Data Security Standard" na página 79
  - "Conformidade de STIG do Departamento de Defesa" na página 10
  - "Conformidade de Lei Sarbanes Oxley e COBIT" na página 94
  - "Health Insurance Portability and Accountability Act (HIPAA)" na página 95
- Informações incluídas sobre a função Real Time Compliance no tópico "PowerSC Real Time Compliance" na página 111.
- Incluídas as operações **clientData** e **default_policy** e as sinalizações **-l** e **-g** no comando **psconf**.
- Atualizadas as sinalizações **-a**, **-c**, **-l** e **-n** no comando **pscxpert**.
- Atualizadas as sinalizações **-i** e **-x** no comando **pmconf**.

Notas sobre a liberação do PowerSC Standard Edition Versão 1.1.4

As notas sobre a liberação contêm informações sobre as mudanças no PowerSC Standard Edition Versão 1.1.4 que foram identificadas depois que a documentação foi concluída.

Mudanças de conjunto de arquivos do PowerSC Standard Edition

O PowerSC Express Edition não está mais disponível para compra na IBM®. O PowerSC Standard Edition 1.1.4, ou mais recente, inclui a função e os recursos a seguir que estavam disponíveis anteriormente no PowerSC Express Edition:

- Conformidade de STIG do Departamento de Defesa
- Conformidade de Lei Sarbanes Oxley e COBIT
- Conformidade de Health Insurance Portability and Accountability Act (HIPAA)
- Real-Time Compliance

A tabela a seguir exibe o nome dos conjuntos de arquivos do PowerSC Express Edition que foram mesclados com os conjuntos de arquivos do PowerSC Standard Edition versão 1.1.4, ou mais recente:

Tabela 1. Conjuntos de arquivos do PowerSC Standard Edition 1.1.4, ou mais recente

Conjuntos de arquivos do PowerSC Express Edition	Conjuntos de arquivos do PowerSC Standard Edition
powerscExp.rtc	powerscStd.rtc
powerscExp.msg.<LANG>	powerscStd.msg.<LANG>
powerscExp.license	powerscStd.license
powerscExp.ice	powerscStd.ice

Leia estas informações antes de instalar o PowerSC Standard Edition

Para visualizar a versão mais atual das Notas sobre a liberação, veja as Notas sobre a liberação on-line no IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSTQK9_1.1.4/com.ibm.powersc114.se/powersc_se_rn.htm).

PowerSC Standard Edition é um programa licenciado e não está incluído com o sistema operacional AIX.

Nota: Esse software pode conter erros que poderiam resultar em um impacto crítico no negócio. Instale as correções mais recentes disponíveis antes de usar esse software.

Informações de instalação, migração, upgrade e configuração

Para obter informações sobre como instalar o PowerSC Standard Edition, veja Instalando o PowerSC Standard Edition Versão 1.1.4.

Para obter informações o sobre hardware e as versões do sistema operacional AIX que são suportadas para o PowerSC Standard Edition, veja Conceitos do PowerSC Standard Edition 1.1.4.

Requisito de conjunto de arquivos adicional para executar o Trusted Network Connect

Para executar o Trusted Network Connect, deve-se instalar o conjunto de arquivos `powerscStd.tnc_commands` que está disponível em seu DVD do IBM PowerSC Standard Edition. Instale o conjunto de arquivos em seu sistema AIX usando o comando **installp**. Esse conjunto de arquivos fornece a função dos comandos **psconf** e **pmconf**.

Nota: Se você estiver usando a função Referente de IP do Trusted Network Connect, deve-se também instalar o conjunto de arquivos `powerscStd.tnc_commands` em seu sistema VIOS.

Mudanças de comandos

Os comandos a seguir mudaram:

- No IBM AIX 6 com Tecnologia Nível 8, ou mais recente, é possível usar o comando **tncconsole** para relatar e gerenciar o servidor trusted network connect (TNC), o cliente TNC, o Referente de IP (IPRef) do TNC e o Service Update Management Assistant (SUMA). No entanto, o comando **tncconsole** possui funções limitadas. Para usar a função integral do comando **tncconsole**, deve-se instalar o PowerSC Standard Edition. No PowerSC Standard Edition, o nome do comando **tncconsole** foi mudado para o comando **psconf**.
- A sinalização **-o** foi removida do comando **pscxpert**.

Conceitos do PowerSC Standard Edition 1.1.4

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 2. 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 • POWER8
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 • POWER8 • 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 • POWER8

Tabela 2. 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 • POWER8

Instalando o PowerSC Standard Edition 1.1.4

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:

- `powerscStd.ice`: Instalado em sistemas AIX que requerem o recurso Security and Compliance Automation 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 mais recente, ou no AIX Versão 7.1, ou mais recente, sistema de console Service Update Management Assistant (SUMA) no ambiente SUMA para gerenciamento de correção.
- `powerscStd.svm`: Instalado nos sistemas AIX que podem se beneficiar do recurso de roteamento de PowerSC Standard Edition.
- `powerscStd.rtc`: Instalado em sistemas AIX que requerem o recurso Real Time Compliance do PowerSC Standard Edition.

É possível instalar 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 1.1.4” na página 5
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 115
Existem algumas configurações de hardware e de software que são necessárias para instalar a Inicialização Confiável.

"Instalando o Trusted Network Connect" na página 135
Instalar os componentes do Trusted Network Connect (TNC) requer que você conclua certas etapas.

Tarefas relacionadas:

"Instalando o Firewall Confiável" na página 123
Instalar o PowerSC Trusted Firewall é semelhante à instalar outros recursos PowerSC.

"Instalando a Criação de Log Confiável" na página 130
É possível instalar o recurso PowerSC Trusted Logging usando a interface de linha de comandos ou a ferramenta SMIT.

Security and Compliance Automation

O AIX Profile Manager gerencia perfis predefinidos para a segurança e conformidade. O PowerSC Real Time Compliance monitora continuamente os sistemas AIX ativados para assegurar-se de que eles sejam configurados continuamente e de modo seguro.

Os perfis XML automatizam a configuração do sistema AIX recomendada da IBM para ficarem consistentes com o Payment Card Data Security Standard, a Lei Sarbanes-Oxley ou com o Security Technical Implementation Guide do UNIX do Departamento de Defesa e Health Insurance Portability and Accountability Act (HIPAA). As organizações que estão em conformidade com os padrões de segurança devem usar as configurações de segurança do sistema pré-definidas.

O AIX Profile Manager opera como um plug-in do IBM Systems Director que simplifica a aplicação de configurações de segurança, o monitoramento das configurações de segurança e a auditoria de configurações de segurança para o sistema operacional AIX e sistemas Virtual I/O Server (VIOS). Para usar o recurso de conformidade de segurança, o aplicativo PowerSC deve ser instalado nos sistemas gerenciados AIX que estão em conformidade com os padrões de conformidade. O recurso Security and Compliance Automation é incluído no PowerSC Standard Edition.

O pacote de instalação do PowerSC Standard Edition, 5765-PSE, deve ser instalado nos sistemas gerenciados AIX. O pacote de instalação instala o conjunto de arquivos `powerscStd.ice` que pode ser implementado no sistema usando o AIX Profile Manager ou o comando **pscxpert**. O PowerSC com a conformidade do IBM Compliance Expert Express (ICEE) está ativado para gerenciar e melhorar os perfis XML. Os perfis XML são gerenciados pelo AIX Profile Manager.

Nota: Instale todos os aplicativos no sistema antes de aplicar um perfil de segurança.

Conceitos de Security and Compliance Automation

O recurso de segurança e conformidade do PowerSC é um método automatizado para configurar e auditar os sistemas AIX de acordo com o U.S. Department of Defense (DoD) Security Technical Implementation Guide (STIG), o Payment Card Industry (PCI) data security standard (DSS), a lei Sarbanes-Oxley, a conformidade de COBIT (SOX/COBIT) e o Health Insurance Portability and Accountability Act (HIPAA).

O PowerSC ajuda a automatizar a configuração e o monitoramento de sistemas que devem ser compatíveis com o Payment Card Industry (PCI) data security standard (DSS) versão 1.2, 2.0 ou 3.0. Portanto, o recurso PowerSC Security and Compliance é um método preciso e completo de automação de configuração de segurança usado para atender os requisitos de conformidade de TI do STIG do UNIX do DoD, do PCI DSS, de Lei Sarbanes Oxley, conformidade de COBIT (SOX/COBIT) e do Health Insurance Portability and Accountability Act (HIPAA).

Nota: O PowerSC Security and Compliance atualiza os perfis XML existentes usados pela edição do IBM Compliance Expert express (ICEE). É possível usar os perfis XML do PowerSC Standard Edition com o comando **pscxpert**, de modo semelhante a ICEE.

Os perfis de conformidade pré-configurados entregues com o PowerSC Standard Edition reduzem a carga de trabalho administrativa de interpretar a documentação de conformidade e implementar as normas como parâmetros de configuração específicos do sistema. Essa tecnologia reduz o custo de configuração de conformidade e auditoria automatizando os processos. O IBMPowerSC Standard Edition é projetado para ajudar a gerenciar efetivamente o requisito do sistema associado à conformidade padrão externa que pode reduzir potencialmente os custos e melhorar a conformidade.

Conformidade de STIG do Departamento de Defesa

O Departamento de Defesa (DoD) dos Estados Unidos requer sistemas de computador altamente seguros. Este nível de segurança e qualidade definidos pelo DoD atende com a qualidade e a base de clientes do AIX no servidor Power Systems.

Um sistema operacional seguro, como o AIX, deve ser configurado precisamente para atingir os objetivos de segurança especificados. O DoD reconheceu a necessidade para configurações de segurança de todos os sistemas operacionais na Diretiva 8500.1. Essa diretiva estabeleceu a política e designou a responsabilidade à Defense Information Security Agency (DISA) dos EUA para fornecer orientação de configuração de segurança.

A DISA desenvolveu os princípios e as diretrizes no UNIX Security Technical Implementation Guide (STIG), que fornece um ambiente que atende ou excede os requisitos de segurança de sistemas DoD que estão operando no nível sensível de Mission Assurance Category (MAC) II, que contém informações confidenciais. O DoD dos EUA possui requisitos de segurança de TI limitados e enumerou os detalhes das definições de configuração necessárias para assegurar que o sistema opere de uma maneira segura. É possível alavancar a orientação de especialista necessária. O PowerSC Standard Edition ajuda a automatizar o processo de configurar as definições, conforme definido por DoD.

Nota: Todos os arquivos de script customizados fornecidos para manter a conformidade do DoD estão no diretório `/etc/security/pscexpert/dodv2`.

O PowerSC Standard Edition suporta os requisitos da versão 1 liberação 2 do AIX DoD STIG. Um resumo dos requisitos e como assegurar essa conformidade é fornecido nas tabelas a seguir.

Tabela 3. Requisitos gerais do DoD

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
AIX00020	2	O software de Base de Computação Confiável do AIX deve ser implementado.	**Local** `/etc/security/pscexpert/dodv2/trust` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
AIX00040	2	O comando **securetcpip** deve ser usado.	**Local** `/etc/security/pscexpert/dodv2/dodsecuretcpip` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
AIX00060	2	O sistema deve ser verificado semanalmente quanto a arquivos `setuid` desautorizados e quanto à modificação desautorizada para arquivos `setuid` autorizados.	**Local** `/etc/security/pscexpert/dodv2/trust` **Ação de conformidade** Verifica semanalmente para identificar mudanças nos arquivos especificados.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
AIX00080	1	O atributo `SYSTEM` não deve ser configurado como *none* para nenhuma conta.	**Local** `/etc/security/pscexpert/dodv2/SYSattr` **Ação de conformidade** Assegura que o atributo especificado seja configurado para um valor diferente de *none*. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
AIX00200	2	O sistema não deve permitir transmissões direcionadas para mover-se pelo gateway.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Configura o valor da opção de rede `direct_broadcast` como *0*.
AIX00210	2	O sistema deve fornecer proteção com relação a ataques de Internet Control Message Protocol (ICMP) em conexões TCP.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Configura o valor da opção de rede `tcp_icmpsecure` como *1*.
AIX00220	2	O sistema deve fornecer proteção para a pilha TCP com relação a reconfigurações de conexão, sincronização (SYN) e ataques de injeção de dados.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Assegura que o valor para a opção de rede `tcp_tcpsecure` seja configurado como *7*.
AIX00230	2	O sistema deve fornecer proteção com relação a ataques de fragmentação de IP.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Configura o valor da opção de rede `ip_nfrag` como *200*.
AIX00300	1,2,3	O sistema não deve ter o serviço `bootp` ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa o serviço especificado.
AIX00310	2	Os arquivos `/etc/ftpaccess.ctl` devem existir.	**Local** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Ação de conformidade** Assegura que o arquivo exista.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN000020	2	O sistema deve requerer autenticação quando iniciar no modo de usuário único.	**Local** `/etc/security/pscexpert/dodv2/rootpasswd_home` **Ação de conformidade** Assegura que a conta raiz para quaisquer partições inicializáveis tenha uma senha no arquivo `/etc/security/passwd`. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN000100	1	O sistema operacional deve ser uma liberação suportada.	**Local** `/etc/security/pscexpert/dodv2/dodv2cat1` **Ação de conformidade** Exibe os resultados dos testes de regras especificados
GEN000120	2	As correções e atualizações de segurança do sistema mais atuais devem ser instaladas.	**Local** `/usr/sbin/instfix -i` `/etc/security/pscexpert/dodv2/dodv2cat1` **Ação de conformidade** Configure isso usando o recurso Trusted Network Connect.
GEN000140	2	O sistema deve ser verificado semanalmente quanto a arquivos `setuid` desautorizados e quanto à modificação desautorizada para arquivos `setuid` autorizados.	**Local** `/etc/security/pscexpert/dodv2/trust` **Ação de conformidade** Verifica semanalmente para identificar mudanças nos arquivos especificados.
GEN000220	2	O sistema deve ser verificado semanalmente quanto a arquivos `setuid` desautorizados e quanto à modificação desautorizada para arquivos `setuid` autorizados.	**Local** `/etc/security/pscexpert/dodv2/trust` **Ação de conformidade** Verifica semanalmente para identificar mudanças nos arquivos especificados.
GEN000240	2	O relógio do sistema deve ser sincronizado para uma origem de tempo oficial do Department of Defense (DoD).	**Local** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Ação de conformidade** Assegura que o relógio do sistema seja compatível.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN000241	2	O relógio do sistema deve ser sincronizado continuamente ou pelo menos diariamente.	**Local** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Ação de conformidade** Assegura que o relógio do sistema seja compatível.
GEN000242	2	O sistema deve usar pelo menos duas origens de tempo para sincronização do clock.	**Local** `/etc/security/pscexpert/dodv2/dodv2netrules` **Ação de conformidade** Assegura que mais de uma origem de tempo seja usada para sincronizar o clock.
GEN000280	2	Logins diretos para os tipos de contas a seguir não devem ser permitidos: • aplicativo • padrão • compartilhado • utilitário	**Local** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Ação de conformidade** Evita logins diretos para as contas especificadas.
GEN000290	2	O sistema não deve ter contas desnecessárias.	**Local** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Ação de conformidade** Assegura que não existam contas não usadas.
GEN000300 (relacionado a GEN000320, GEN000380, GEN000880)	2	Todas as contas no sistema devem ter nomes de usuário o conta exclusivos e senhas de usuário ou conta exclusivas.	**Local** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Ação de conformidade** Assegura que todas as contas atendam aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN000320 (relacionado a GEN000300, GEN000380, GEN000880)	2	Todas as contas no sistema devem ter nomes de usuário o conta exclusivos e senhas de usuário ou conta exclusivas.	**Local** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Ação de conformidade** Assegura que todas as contas atendam aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN000340	2	IDs de usuário (UIDs) e IDs de grupo (GIDs) que são reservados para contas do sistema não devem ser designados a contas não do sistema ou grupos não do sistema.	**Local** `/etc/security/pscexpert/dodv2/account` **Ação de conformidade** Essa configuração é ativada automaticamente para impingir essa regra.
GEN000360	2	UIDs e GIDs que são reservados para contas do sistema não devem ser designados a contas não do sistema ou grupos não do sistema.	**Local** `/etc/security/pscexpert/dodv2/account` **Ação de conformidade** Essa configuração é ativada automaticamente para impingir essa regra.
GEN000380 (relacionado a GEN000300, GEN000320, GEN000880)	2	Todas as contas no sistema devem ter nomes de usuário o conta exclusivos e senhas de usuário ou conta exclusivas.	**Local** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Ação de conformidade** Assegura que todas as contas atendam aos requisitos especificados.
GEN000400	2	O banner de login do Department of Defense (DoD) deve ser exibido imediatamente antes, ou como parte, de prompts de login do console.	**Local** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Ação de conformidade** Exibe o banner necessário.
GEN000402	2	O banner de login do DoD deve ser exibido imediatamente antes, ou como parte, de prompts de login do ambiente gráfico de área de trabalho.	**Local** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Ação de conformidade** O banner de login é configurado para o banner do Departamento de Defesa.
GEN000410	2	O serviço Protocolo de Transferência de Arquivos sobre SSL (FTPS) ou Protocolo de Transferência de Arquivos (FTP) no sistema deve ser configurado com o banner de login do DoD.	**Local** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Ação de conformidade** Exibe o banner ao usar FTP.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN000440	2	Tentativas bem-sucedidas e malsucedidas para efetuar login e logout devem ser registradas.	**Local** `/etc/security/pscexpert/dodv2/loginout` **Ação de conformidade** Ativa a criação de log necessária.
GEN000452	2	O sistema deve exibir a data e hora do último login de conta bem-sucedido no momento de cada login.	**Local** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Ação de conformidade** Exibe as informações necessárias.
GEN000460	2	Essa regra desativa uma conta após três tentativas de logon com falha consecutivas.	**Local** `/etc/security/pscexpert/dodv2/chusrattrdod` **Ação de conformidade** Configura o limite de tentativas de login para o valor especificado.
GEN000480	2	Essa regra configura o tempo de atraso de login para 4 segundos.	**Local** `/etc/security/pscexpert/dodv2/chdefstanzadod` **Ação de conformidade** Configura o tempo de atraso de login para o valor necessário.
GEN000540	2	Essa regra assegura que os arquivos de configuração de senha global do sistema sejam configurados de acordo com os requisitos de senha.	**Local** `/etc/security/pscexpert/dodv2/chusrattrdod` **Ação de conformidade** Configura as definições de senha necessárias.
GEN000560	1	Todas as contas no sistema devem ter senhas válidas.	**Local** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Ação de conformidade** Assegura que as contas possuam senhas.
GEN000580	2	Esta regra assegura que todas as senhas contenham um mínimo de 14 caracteres.	**Local** `/etc/security/pscexpert/dodv2/chusrattrdod` **Ação de conformidade** Configura o comprimento mínimo da senha para 14 caracteres.
GEN000585	2	O sistema deve usar um algoritmo hash criptográfico aprovado pelo Federal Information Processing Standards (FIPS) 140-2 para gerar hashes de senha de conta.	**Local** `/etc/security/pscexpert/dodv2/fipspasswd` **Ação de conformidade** Assegura que os hashes de senha usem um algoritmo hash aprovado.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN000590	2	O sistema deve usar um algoritmo hash criptográfico aprovado pelo FIPS 140-2 para gerar hashes de senha de conta.	**Local** `/etc/security/pscexpert/dodv2/fipspasswd` **Ação de conformidade** Assegura que os hashes de senha usem um algoritmo hash aprovado.
GEN000595	2	Use um algoritmo hash criptográfico aprovado pelo FIPS 140-2 ao gerar os hashes de senha que estão armazenados no sistema.	**Local** `/etc/security/pscexpert/dodv2/fipspasswd` **Ação de conformidade** Assegura que os hashes de senha usem um algoritmo hash aprovado.
GEN000640	2	Essa regra requer um mínimo de um caractere não alfabético em uma senha	**Local** `/etc/security/pscexpert/dodv2/chusrattrdod` **Ação de conformidade** Configura o número mínimo de caracteres não alfabéticos em uma senha para 1.
GEN000680	2	Essa regra assegura que as senhas contenham não mais que três caracteres de repetição consecutivos	**Local** `/etc/security/pscexpert/dodv2/chusrattrdod` **Ação de conformidade** Configura o número máximo de caracteres de repetição em uma senha para 3.
GEN000700	2	Essa regra assegura que os arquivos de configuração de senha global do sistema sejam configurados de acordo com os requisitos de senha.	**Local** `/etc/security/pscexpert/dodv2/chusrattrdod` **Ação de conformidade** Assegura que os arquivos de configuração de senha atendam aos requisitos.
GEN000740	2	Todas as senhas de conta de processamento automatizado e não interativo devem ser bloqueadas (GEN000280). Logins diretos não devem ser permitidos para contas compartilhadas ou padrão ou de aplicativo ou utilitário. (GEN002640) As contas do sistema padrão devem ser desativadas ou removidas.	**Local** `/etc/security/pscexpert/dodv2/loginout` `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Ação de conformidade** Essa configuração é ativada automaticamente.
GEN000740	2	Todas as senhas de conta de processamento automatizado e não interativo devem ser mudadas pelo menos uma vez por ano ou devem ser bloqueadas.	**Local** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Ação de conformidade** Assegura que as senhas especificadas sejam mudadas anualmente ou bloqueadas.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN000750	2	Essa regra requer que novas senhas contenham um mínimo de 4 caracteres que não estavam na senha antiga.	**Local** `/etc/security/pscexpert/dodv2/chusrattrdod` **Ação de conformidade** Configura o número mínimo de caracteres novos que são necessários em uma nova senha para 4.
GEN000760	2	As contas devem ser bloqueadas após 35 dias de inatividade.	**Local** `/etc/security/pscexpert/dodv2/disableacctdod` **Ação de conformidade** Bloqueia as contas após 35 dias de inatividade.
GEN000790	2	O sistema deve evitar o uso de palavras de dicionário para senhas.	**Local** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Ação de conformidade** Assegura que a senha padrão que estiver sendo configurada não seja fraca.
GEN000800	2	Essa regra assegura que as últimas cinco senhas não sejam reutilizadas.	**Local** `/etc/security/pscexpert/dodv2/chusrattrdod` **Ação de conformidade** Assegura que a nova senha não seja a mesma que qualquer uma das últimas 5 senhas.
GEN000880 (relacionado a GEN000300, GEN000320, GEN000380)	2	Todas as contas no sistema devem ter nomes de usuário ou conta exclusivos e senhas de usuário ou conta exclusivas.	**Local** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Ação de conformidade** Assegura que todas as contas atendam aos requisitos especificados.
GEN000900	3	O diretório inicial do usuário raiz não deve ser o diretório-raiz (/).	**Local** `/etc/security/pscexpert/dodv2/rootpasswd_home` **Ação de conformidade** Assegura que o sistema atenda ao requisito especificado. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN000940	2	O caminho da procura de executável da conta raiz deve ser o padrão do fornecedor e deve conter somente caminhos absolutos.	**Local** `/etc/security/pscexpert/dodv2/fixpathvars` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN000945	2	O caminho da procura de biblioteca da conta raiz deve ser o padrão do sistema e deve conter somente caminhos absolutos.	**Local** `/etc/security/pscexpert/dodv2/fixpathvars` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN000950	2	A lista de bibliotecas pré-carregadas da conta raiz deve estar vazia.	**Local** `/etc/security/pscexpert/dodv2/fixpathvars` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN000960 (relacionado a GEN003000, GEN003020, GEN003160, GEN003360, GEN003380)	2	A conta raiz não deve ter diretórios livremente graváveis em seu caminho da procura de executável.	**Local** `/etc/security/pscexpert/dodv2/rmwwpaths` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN000980	2	O sistema deve evitar que a conta raiz efetue login diretamente, exceto a partir do console do sistema.	**Local** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN001000	2	Os consoles remotos devem ser desativados ou protegidos contra o acesso não autorizado.	**Local** `/etc/security/pscexpert/dodv2/remoteconsole` **Ação de conformidade** Assegura que os consoles especificados sejam desativados.
GEN001020	2	A conta raiz não deve ser usada para login direto.	**Local** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Ação de conformidade** Desativa a conta raiz de efetuar login diretamente.
GEN001060	2	O sistema deve registrar tentativas bem-sucedidas e malsucedidas para acessar a conta raiz.	**Local** `/etc/security/pscexpert/dodv2/loginout` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN001100	1	As senhas raiz nunca devem ser passadas por uma rede no formulário de texto.	**Local** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN001120	2	O sistema não deve permitir o login raiz usando o protocolo `SSH`.	**Local** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Ação de conformidade** Desativa o login raiz para `SSH`.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN001440	3	Todos os usuários interativos devem ser designados a um diretório inicial no arquivo `/etc/passwd`.	**Local** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Ação de conformidade** Assegura que todos os usuários interativos possuam o diretório especificado.
GEN001475	2	O arquivo `/etc/group` não deve conter nenhum hash de senha de grupo.	**Local** `/etc/security/pscexpert/dodv2/passwdhash` **Ação de conformidade** Assegura que não existam hashes de senha de grupo no arquivo especificado. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001600	2	Os caminhos da procura de executável de scripts de controle de execução devem conter somente caminhos absolutos.	**Local** `/etc/security/pscexpert/dodv2/fixpathvars` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001605	2	Os caminhos da procura de biblioteca de scripts de controle de execução devem conter somente caminhos absolutos.	**Local** `/etc/security/pscexpert/dodv2/fixpathvars` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN001610	2	As listas de bibliotecas pré-carregadas de scripts de controle de execução devem conter somente caminhos absolutos.	**Local** `/etc/security/pscexpert/dodv2/fixpathvars` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001840	2	Todos os caminhos da procura de executável de arquivos de inicialização globais devem conter somente caminhos absolutos.	**Local** `/etc/security/pscexpert/dodv2/fixpathvars` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001845	2	Todos os caminhos da procura de biblioteca de arquivos de inicialização globais devem conter somente caminhos absolutos.	**Local** `/etc/security/pscexpert/dodv2/fixpathvars` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN001850	2	Todas as listas de bibliotecas pré-carregadas de arquivos de inicialização globais devem conter somente caminhos absolutos.	**Local** `/etc/security/pscexpert/dodv2/fixpathvars` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001900	2	Todos os caminhos da procura de executável de arquivos de inicialização locais devem conter somente caminhos absolutos.	**Local** `/etc/security/pscexpert/dodv2/fixpathvars` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001901	2	Todos os caminhos da procura de biblioteca de arquivos de inicialização locais devem conter somente caminhos absolutos.	**Local** `/etc/security/pscexpert/dodv2/fixpathvars` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN001902	2	Todas as listas de bibliotecas pré-carregadas de arquivos de inicialização locais devem conter somente caminhos absolutos.	**Local** `/etc/security/pscexpert/dodv2/fixpathvars` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001940	2	Os arquivos de inicialização do usuário não devem executar programas livremente graváveis.	**Local** `/etc/security/pscexpert/dodv2/rmwwpaths` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN001980	2	Os arquivos `.rhosts`, `.shosts`, `hosts.equiv`, `shosts.equiv`, `/etc/passwd`, `/etc/shadow` ou `/etc/group` não devem conter um sinal de mais (+) sem definir as entradas para NIS+ netgroups.	**Local** `/etc/security/pscexpert/dodv2/dodv2netrules` **Ação de conformidade** Assegura que os arquivos especificados atendem aos requisitos especificados.
GEN002000	2	Não deve haver arquivos `.netrc` no sistema.	**Local** `/etc/security/pscexpert/dodv2/dodv2netrules` **Ação de conformidade** Assegura que exista nenhum dos arquivos especificados no sistema. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN002020	2	Todos os arquivos `.rhosts`, `.shosts` ou `hosts.equiv` devem conter somente pares de host-usuário confiáveis.	**Local** `/etc/security/pscexpert/dodv2/dodv2netrules` **Ação de conformidade** Assegura que os arquivos especificados se adequem a esse requisito.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN002040	1	Essa regra desativa os arquivos `.rhosts`, `.shosts` e `hosts.equiv` ou arquivos `shosts.equiv`.	**Local** `/etc/security/pscexpert/dodv2/mvhostsfilesdod` **Ação de conformidade** Desativa os arquivos especificados.
GEN002120	1,2	Essa regra verifica e configura shells do usuário.	**Local** `/etc/security/pscexpert/dodv2/usershells` **Ação de conformidade** Cria os shells necessários. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN002140	1,2	Todos os shells que são referenciados na lista `/etc/passwd` devem ser listados no arquivo `/etc/shells`, exceto quaisquer shells especificados para evitar logins.	**Local** `/etc/security/pscexpert/dodv2/usershells` **Ação de conformidade** Assegura que os shells estejam listadas nos arquivos corretos. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN002280	2	Os arquivos e diretórios do dispositivo devem ser graváveis somente por usuários com uma conta do sistema ou quando o sistema for configurado pelo fornecedor.	**Local** `/etc/security/pscexpert/dodv2/wwdevfiles` **Ação de conformidade** Exibe arquivos de dispositivo livremente graváveis, diretórios e quaisquer outros arquivos no sistema que estiverem em diretórios não públicos.
GEN002300	2	Os arquivos de dispositivo que são usados para backup devem ser legíveis, graváveis, ou ambos, somente pelo usuário raiz ou pelo usuário do backup.	**Local** `/etc/security/pscexpert/dodv2/wwdevfiles` **Ação de conformidade** Exibe arquivos de dispositivo, diretórios e quaisquer outros arquivos livremente graváveis no sistema que estão em diretórios não públicos.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN002400	2	O sistema deve ser verificado semanalmente quanto a arquivos `setuid` desautorizados e quanto à modificação desautorizada para arquivos `setuid` autorizados.	**Local** `/etc/security/pscexpert/dodv2/trust` **Ação de conformidade** Verifica semanalmente para identificar mudanças nos arquivos especificados. **Nota:** Compare os dois logs semanais mais recentes que são criados no diretório `/var/security/pscexpert` para verificar se não houve atividade desautorizada.
GEN002420	2	Mídia removível, sistemas de arquivos remotos e qualquer sistema de arquivos que não contenha arquivos `setuid` aprovados devem ser montados usando a opção *nosuid*.	**Local** `/etc/security/pscexpert/dodv2/fsmntoptions` **Ação de conformidade** Assegura que os sistemas de arquivos montados remotamente tenham as opções especificadas. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN002430	2	Mídia removível, sistemas de arquivos remotos e qualquer sistema de arquivos que não contenha arquivos de dispositivo aprovados devem ser montados usando a opção *nodev*.	**Local** `/etc/security/pscexpert/dodv2/fsmntoptions` **Ação de conformidade** Assegura que os sistemas de arquivos montados remotamente tenham as opções especificadas. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN002480	2	Os diretórios públicos devem ser os únicos diretórios livremente graváveis e os arquivos livremente graváveis devem estar localizados somente em diretórios públicos.	**Local** `/etc/security/pscexpert/dodv2/wwdevfiles` `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Relata quando os arquivos livremente graváveis não estão em diretórios públicos.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN002640	2	As contas do sistema padrão devem ser desativadas ou removidas.	**Local** `/etc/security/pscexpert/dodv2/lockacc_rlogin` `/etc/security/pscexpert/dodv2/loginout` **Ação de conformidade** Desativa as contas do sistema padrão.
GEN002660	2	A auditoria deve ser ativada.	**Local** `/etc/security/pscexpert/dodv2/dodaudit` **Ação de conformidade** Ativa o comando `dodaudit`, que ativa a auditoria.
GEN002720	2	O sistema de auditoria deve ser configurado para auditar tentativas com falha de acessar arquivos e programas.	**Local** `/etc/security/pscexpert/dodv2/dodaudit` **Ação de conformidade** Ativa automaticamente a auditoria especificada.
GEN002740	2	O sistema de auditoria deve ser configurado para auditar exclusões de arquivo.	**Local** `/etc/security/pscexpert/dodv2/dodaudit` **Ação de conformidade** Ativa automaticamente a auditoria especificada.
GEN002750	3	O sistema de auditoria deve ser configurado para auditar criação de conta.	**Local** `/etc/security/pscexpert/dodv2/dodaudit` **Ação de conformidade** Ativa automaticamente a auditoria especificada.
GEN002751	3	O sistema de auditoria deve ser configurado para auditar modificação de conta.	**Local** `/etc/security/pscexpert/dodv2/dodaudit` **Ação de conformidade** Ativa automaticamente a auditoria especificada.
GEN002752	3	O sistema de auditoria deve ser configurado para auditar contas que estão desativadas.	**Local** `/etc/security/pscexpert/dodv2/dodaudit` **Ação de conformidade** Ativa automaticamente a auditoria especificada.
GEN002753	3	O sistema de auditoria deve ser configurado para auditar finalização de conta.	**Local** `/etc/security/pscexpert/dodv2/dodaudit` **Ação de conformidade** Ativa automaticamente a auditoria especificada.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN002760	2	O sistema de auditoria deve ser configurado para auditar todas as ações administrativas, privilegiadas e de segurança.	**Local** `/etc/security/pscexpert/dodv2/dodaudit` **Ação de conformidade** Ativa automaticamente a auditoria especificada.
GEN002800	2	O sistema de auditoria deve ser configurado para auditar login, logout e iniciação de sessão.	**Local** `/etc/security/pscexpert/dodv2/dodaudit` **Ação de conformidade** Ativa automaticamente a auditoria especificada.
GEN002820	2	O sistema de auditoria deve ser configurado para auditar todas as modificações de permissão de controle de acesso discricionário.	**Local** `/etc/security/pscexpert/dodv2/dodaudit` **Ação de conformidade** Ativa automaticamente a auditoria especificada.
GEN002825	2	O sistema de auditoria deve ser configurado para auditar o carregamento e descarregamento de módulos do kernel dinâmico.	**Local** `/etc/security/pscexpert/dodv2/dodaudit` **Ação de conformidade** Ativa automaticamente a auditoria especificada.
GEN002860	2	Os logs de auditoria devem ser girados diariamente.	**Local** `/etc/security/pscexpert/dodv2/rotateauditdod` **Ação de conformidade** Assegura que os logs de auditoria sejam girados.
GEN002960	2	O acesso ao utilitário `cron` deve ser controlado usando o arquivo `cron.allow` ou o arquivo `cron.deny`, ou ambos.	**Local** `/etc/security/pscexpert/dodv2/limitsysacc` **Ação de conformidade** Assegura que os limites de conformidade estejam ativados.
GEN003000 (relacionado a GEN000960, GEN003020, GEN003160, GEN003360, GEN003380)	2	O `Cron` não deve executar programas graváveis pelo grupo ou livremente graváveis.	**Local** `/etc/security/pscexpert/dodv2/rmwwpaths` **Ação de conformidade** Assegura que os limites de conformidade estejam ativados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN003020 (relacionado a GEN000960, GEN003000, GEN003160, GEN003360, GEN003380)	2	O `Cron` não deve executar programas em, ou subordinados a, diretórios livremente graváveis.	**Local** `/etc/security/pscexpert/dodv2/rmwwpaths` **Ação de conformidade** Remove a permissão de livremente gravável dos diretórios do programa `cron`. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN003060	2	As contas do sistema padrão (exceto para raiz) não devem ser listadas no arquivo `cron.allow`, ou devem ser incluídas no arquivo `cron.deny` se o arquivo `cron.allow` não existir.	**Local** `cron.allow` ou `cron.deny` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN003160 (relacionado a GEN000960, GEN003000, GEN003020, GEN003360, GEN003380)	2	A criação de log do `Cron` deve estar em execução.	**Local** `/etc/security/pscexpert/dodv2/rmwwpaths` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN003280	2	O acesso ao utilitário `at` deve ser controlado usando os arquivos `at.allow` e `at.deny`.	**Local** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN003300	2	O arquivo `at.deny` não deve estar vazio, se ele existir.	**Local** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN003320	2	As contas do sistema padrão que não são raiz não devem ser listadas no arquivo `at.allow`, ou devem ser incluídas no arquivo `at.deny` se o arquivo `at.allow` não existir.	**Local** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN003360 (relacionado a GEN000960, GEN003000, GEN003020, GEN003160, GEN003380)	2	O daemon `at` não deve executar programas graváveis pelo grupo ou livremente graváveis.	**Local** `/etc/security/pscexpert/dodv2/rmwwpaths` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN003380 (relacionado a GEN000960, GEN003000, GEN003020, GEN003160, GEN003360)	2	O daemon `at` não deve executar programas em, ou subordinados a, diretórios livremente graváveis.	**Local** `/etc/security/pscexpert/dodv2/rmwwpaths` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN003510	2	Os core dumps do kernel devem ser desativados a menos que sejam necessários.	**Local** `/etc/security/pscexpert/dodv2/coredumpdev` **Ação de conformidade** Desativa os core dumps do kernel.
GEN003540	2	O sistema deve usar pilhas de programas não executáveis.	**Local** `/etc/security/pscexpert/dodv2/sedconfigdod` **Ação de conformidade** Impinge o uso de pilhas de programas não executáveis.
GEN003600	2	O sistema não deve encaminhar pacotes roteados pela origem IPv4.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Configura o valor da opção de rede `ipsrcforward` para *0*.
GEN003601	2	Os tamanhos das filas de listas não processadas TCP devem ser configurados adequadamente.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Configura o valor da opção de rede `clean_partial_conns` para *1*.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN003603	2	O sistema não deve responder a ecos do Internet Control Message Protocol versão 4 (ICMPv4) que são enviados a um endereço de transmissão.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Configura o valor da opção de rede `bcastping` para *0*.
GEN003604	2	O sistema não deve responder a solicitações de registro de data e hora do ICMP que são enviados a um endereço de transmissão.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Configura o valor da opção de rede `bcastping` para *0*.
GEN003605	2	O sistema não deve aplicar roteamento de origem invertido a respostas TCP.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Configura o valor da opção de rede `nonlocsrcroute` para *0*.
GEN003606	2	O sistema deve evitar que aplicativos locais gerem pacotes roteados pela origem.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Configura o valor da opção de rede `ipsrcroutesend` para *0*.
GEN003607	2	O sistema não deve aceitar pacotes IPv4 roteados pela origem.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Desativa a capacidade de aceitar pacotes IPv4 de rotas de origem.
GEN003609	2	O sistema deve ignorar mensagens de redirecionamento de IPv4 ICMP.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Configura o valor da opção de rede `ipignoreredirects` para *1*.
GEN003610	2	O sistema não deve enviar mensagens de redirecionamento de IPv4 ICMP.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Configura o valor da opção de rede `ipsendredirects` para *0*.
GEN003612	2	O sistema deve ser configurado para usar syncookies TCP quando ocorre uma sobrecarga de TCP SYN.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Configura o valor da opção de rede `clean_partial_conns` para *1*.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN003640	2	O sistema de arquivos raiz deve usar registro no diário ou outro método para assegurar consistência do sistema de arquivos.	**Local** `/etc/security/pscexpert/dodv2/chkjournal` **Ação de conformidade** Ativa o registro no diário no sistema de arquivos raiz.
GEN003660	2	O sistema deve registrar dados informativos de autenticação.	**Local** `/etc/security/pscexpert/dodv2/chsyslogdod` **Ação de conformidade** Ativa a criação de log de dados `auth` e `info`.
GEN003700	2	O `inetd` e `xinetd` devem ser desativados ou removidos se não estiverem sendo usados por nenhum serviço de rede.	**Local** `/etc/security/pscexpert/dodv2/dodv2services` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN003810	2	Os serviços `portmap` ou `rpcbind` não devem estar em execução a menos que sejam necessários.	**Local** `/etc/security/pscexpert/dodv2/dodv2services` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN003815	2	Os serviços `portmap` ou `rpcbind` não devem ser instalados a menos que estejam sendo usados.	**Local** `/etc/security/pscexpert/dodv2/dodv2services` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN003820-3860	1,2,3	Os daemons `rsh`, `rexexec` e `telnet` e o serviço `rlogind` não devem estar em execução.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN003865	2	As ferramentas de análise de rede não devem ser instaladas.	**Local** `/etc/security/pscexpert/dodv2/dodv2services` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN003900	2	O arquivo `hosts.lpd` (ou equivalente) não deve conter um sinal de adição (+).	**Local** `/etc/security/pscexpert/dodv2/printers` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN004220	1	As contas administrativas não devem executar um navegador da web, exceto conforme necessário para administração de serviço local.	**Local** `/etc/security/pscexpert/dodv2/dodv2cat1` **Ação de conformidade** Exibe os resultados dos testes de regras especificados
GEN004460	2	Essa regra registra dados `auth` e `info`.	**Local** `/etc/security/pscexpert/dodv2/chsyslogdod` **Ação de conformidade** Ativa a criação de log de dados `auth` e `info`.
GEN004540	2	Essa regra desativa o comando de ajuda `sendmail`.	**Local** `/etc/security/pscexpert/dodv2/sendmailhelp` `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Ação de conformidade** Desativa o comando especificado.
GEN004580	2	O sistema não deve usar arquivos `.forward`.	**Local** `/etc/security/pscexpert/dodv2/forward` **Ação de conformidade** Desativa os arquivos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN004600	1	O serviço `SMTP` deve ser a versão mais atual.	**Local** `/etc/security/pscexpert/dodv2/SMTP_ver` **Ação de conformidade** Assegura que a versão mais recente do serviço especificado esteja em execução. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN004620	2	O servidor `sendmail` deve ter o recurso de depuração desativado.	**Local** `/etc/security/pscexpert/dodv2/SMTP_ver` **Ação de conformidade** Desativa o recurso de depuração `sendmail`.
GEN004640	1	O serviço `SMTP` não deve ter um alias `uudecode` ativo.	**Local** `/etc/security/pscexpert/dodv2/SMTPuucode` **Ação de conformidade** Desativa o alias `uudecode`.
GEN004710	2	A retransmissão de e-mail deve ser restrita.	**Local** `/etc/security/pscexpert/dodv2/sendmaildod` **Ação de conformidade** Restringe a retransmissão de e-mail.
GEN004800	1,2,3	FTP decriptografado não deve ser usado no sistema.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN004820	2	O FTP anônimo não deve estar ativo no sistema a menos que ele seja autorizado.	**Local** `/etc/security/pscexpert/dodv2/anonuser` **Ação de conformidade** Desativa o FTP anônimo no sistema. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN004840	2	Se o sistema for um servidor FTP anônimo, ele deve ser isolado para a rede de Zona Desmilitarizada (DMZ).	**Local** `/etc/security/pscexpert/dodv2/anonuser` **Ação de conformidade** Assegura que um FTP anônimo no sistema esteja na rede DMZ.
GEN004880	2	O arquivo `ftpusers` deve existir.	**Local** `/etc/security/pscexpert/dodv2/chdodftpusers` **Ação de conformidade** Assegura que o arquivo especificado esteja no sistema.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN004900	2	O arquivo `ftpusers` deve conter os nomes das contas que não são permitidos usar o protocolo FTP.	**Local** `/etc/security/pscexpert/dodv2/chdodftpusers` **Ação de conformidade** Assegura que o arquivo contenha os nomes das contas necessários.
GEN005000	1	As contas de FTP anônimo não devem ter um shell funcional.	**Local** `/etc/security/pscexpert/dodv2/usershells` **Ação de conformidade** Remove shells de contas de FTP anônimo. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN005080	1	O daemon `TFTP` deve operar no modo seguro, que fornece acesso somente a um único diretório no sistema de arquivos de host.	**Local** `/etc/security/pscexpert/dodv2/tftpdod` **Ação de conformidade** Assegura que o daemon atenda aos requisitos especificados.
GEN005120	2	O daemon TFTP deve ser configurado para as especificações do fornecedor, incluindo uma conta do usuário TFTP dedicada, um shell sem login, como `/bin/false`, e um diretório inicial que é de propriedade do usuário TFTP.	**Local** `/etc/security/pscexpert/dodv2/tftpdod` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005140	1,2,3	Qualquer daemon TFTP ativo deve estar autorizado e aprovado no pacote de credenciamento do sistema.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Assegura que o daemon esteja autorizado.
GEN005160	1,2	Qualquer host X Window System deve gravar arquivos `.Xauthority`.	**Local** `/etc/security/pscexpert/dodv2/dodv2disableX` **Ação de conformidade** Assegura que o host tenha gravado os arquivos especificados.
GEN005200	1,2	Quaisquer exibições do X Window System não podem ser exportadas publicamente.	**Local** `/etc/security/pscexpert/dodv2/dodv2disableX` **Ação de conformidade** Desativa a disseminação dos programas especificados.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN005220	1,2	Os arquivos `.Xauthority` ou `X*.hosts` (ou equivalente) devem ser usados para restringir o acesso ao servidor X Window System.	**Local** `/etc/security/pscexpert/dodv2/dodv2disableX` **Ação de conformidade** Assegura que os arquivos especificados estejam disponíveis para restringir o acesso ao servidor.
GEN005240	1,2	O utilitário .Xauthority deve permitir acesso somente a hosts autorizados.	**Local** `/etc/security/pscexpert/dodv2/dodv2disableX` **Ação de conformidade** Assegura que o acesso seja limitado a hosts autorizados.
GEN005260	2	Essa regra desativa as conexões do X Window System e o gerenciador de login do XServer.	**Local** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Ação de conformidade** Desativa as conexões necessárias e o gerenciador de login.
GEN005280	1,2,3	O sistema não deve ter o serviço `UUCP` ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN005300	2	As comunidades SNMP devem ser mudadas a partir das configurações padrão.	**Local** `/etc/security/pscexpert/dodv2/chsnmp` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005305	2	O serviço SNMP deve usar somente SNMPv3 ou uma versão mais recente.	**Local** `/etc/security/pscexpert/dodv2/chsnmp` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005306	2	O serviço SNMP deve requerer o uso de um FIPS 140-2.	**Local** `/etc/security/pscexpert/dodv2/chsnmp` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005440	2	O sistema deve usar um servidor syslog remoto (host do log).	**Local** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Ação de conformidade** Assegura que o sistema esteja usando um servidor syslog remoto.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN005450	2	O sistema deve usar um servidor syslog remoto (host do log).	**Local** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Ação de conformidade** Assegura que o sistema esteja usando um servidor syslog remoto.
GEN005460	2	O sistema deve usar um servidor syslog remoto (host do log).	**Local** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Ação de conformidade** Assegura que o sistema esteja usando um servidor syslog remoto.
GEN005480	2	O sistema deve usar um servidor syslog remoto (host do log).	**Local** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Ação de conformidade** Assegura que o sistema esteja usando um servidor syslog remoto.
GEN005500	2	O daemon `SSH` deve ser configurado para usar somente o protocolo Secure Shell version 2 (SSHv2).	**Local** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005501	2	O cliente `SSH` deve ser configurado para usar somente o protocolo SSHv2.	**Local** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005504	2	O daemon `SSH` deve atender somente em endereços de rede de gerenciamento, a menos que esteja autorizado para usos diferentes de gerenciamento.	**Local** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005505	2	O daemon `SSH` deve ser configurado para usar somente cifras que se adequem aos padrões de Federal Information Processing Standards (FIPS) 140-2.	**Local** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005506	2	O daemon `SSH` deve ser configurado para usar somente cifras que se adequem aos padrões de FIPS 140-2.	**Local** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN005507	2	O daemon SSH deve ser configurado para usar somente Códigos de Autenticação de Mensagem (MACs) com algoritmos hash criptográficos que se adequem aos padrões de FIPS 140-2.	**Local** /etc/security/pscexpert/dodv2/sshDoDconfig **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005510	2	O cliente SSH deve ser configurado para usar somente MACs com cifras que se adequem aos padrões de FIPS 140-2.	**Local** /etc/security/pscexpert/dodv2/sshDoDconfig **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005511	2	O cliente SSH deve ser configurado para usar somente MACs com cifras que se adequem aos padrões de FIPS 140-2.	**Local** /etc/security/pscexpert/dodv2/sshDoDconfig **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005512	2	O daemon SSH deve ser configurado para usar somente MACs com algoritmos hash criptográficos que se adequem aos padrões de FIPS 140-2.	**Local** /etc/security/pscexpert/dodv2/sshDoDconfig **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005521	2	O daemon SSH deve restringir o login a usuários específicos, grupos, ou ambos.	**Local** /etc/security/pscexpert/dodv2/sshDoDconfig **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005536	2	O daemon SSH deve executar a verificação de modo estrito dos arquivos de configuração do configuração do diretório.	**Local** /etc/security/pscexpert/dodv2/sshDoDconfig **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005537	2	O daemon SSH deve usar a separação de privilégio.	**Local** /etc/security/pscexpert/dodv2/sshDoDconfig **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005538	2	O daemon SSH não deve permitir que rhosts autentique usando o cryptosystem Rivest-Shamir-Adleman (RSA).	**Local** /etc/security/pscexpert/dodv2/sshDoDconfig **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005539	2	O daemon SSH não deve permitir compactação ou deve permitir compactação somente após uma autenticação bem-sucedida.	**Local** /etc/security/pscexpert/dodv2/sshDoDconfig **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN005550	2	O daemon SSH deve ser configurado com o banner de logon do DoD.	**Local** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005560	2	Determine se há um gateway padrão que esteja configurado para IPv4.	**Local** `/etc/security/pscexpert/dodv2/chkgtway` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração. **Nota:** Se o seu sistema estiver executando o protocolo IPv6, assegure-se de que a configuração *ipv6_enabled* no arquivo `/etc/security/pscexpert/ipv6.conf` esteja configurada para o valor de `yes`. Se o sistema não estiver usando IPv6, assegure-se de que o valor *ipv6_enabled* esteja configurado para `no`.
GEN005570	2	Determine se há um gateway padrão que esteja configurado para IPv6.	**Local** `/etc/security/pscexpert/dodv2/chkgtway` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração. **Nota:** Se o seu sistema estiver executando o protocolo IPv6, assegure-se de que a configuração *ipv6_enabled* no arquivo `/etc/security/pscexpert/ipv6.conf` esteja configurada para o valor de `yes`. Se o sistema não estiver usando IPv6, assegure-se de que o valor *ipv6_enabled* esteja configurado para `no`.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN005590	2	O sistema não deve estar executando nenhum daemon de protocolo de roteamento, a menos que o sistema seja um roteador.	**Local** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005590	2	O sistema não deve estar executando nenhum daemon de protocolo de roteamento, a menos que o sistema seja um roteador.	**Local** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN005600	2	O encaminhamento de IP para IPv4 não deve ser ativado a menos que o sistema seja um roteador.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Configura o valor da opção de rede `ipforwarding` para *0*.
GEN005610	2	O sistema não deve ter o encaminhamento de IP para IPv6 ativado a menos que o sistema seja um roteador de IPv6.	**Local** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Ação de conformidade** Configura o valor da opção de rede `ip6forwarding` para *1*.
GEN005820	2	O UID e o GID anônimos do NFS devem ser configurados para valores sem permissões.	**Local** `/etc/security/pscexpert/dodv2/nfsoptions` **Ação de conformidade** Assegura que os IDs especificados não tenham permissões.
GEN005840	2	O servidor NFS deve ser configurado para restringir o acesso de sistema de arquivos para hosts locais.	**Local** `/etc/security/pscexpert/dodv2/nfsoptions` **Ação de conformidade** Configura o servidor NFS para restringir o acesso a hosts locais.
GEN005880	2	O servidor NFS não deve permitir o acesso raiz remoto.	**Local** `/etc/security/pscexpert/dodv2/nfsoptions` **Ação de conformidade** Desativa o acesso raiz remoto no servidor NFS.
GEN005900	2	A opção *nosuid* deve ser ativada nas montagens do cliente NFS.	**Local** `/etc/security/pscexpert/dodv2/nosuid` **Ação de conformidade** Ativa a opção *nosuid* em todas as montagens de cliente NFS.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN006060	2	O sistema não deve executar Samba a menos que seja necessário.	**Local** `/etc/security/pscexpert/dodv2/dodv2services` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN006380	1	O sistema não deve usar UDP para NIS ou NIS+.	**Local** `/etc/security/pscexpert/dodv2/dodv2cat1` **Ação de conformidade** Exibe os resultados dos testes de regras especificados
GEN006400	2	O protocolo Network Information System (NIS) não deve ser usado.	**Local** `/etc/security/pscexpert/dodv2/nisplus` **Ação de conformidade** Desativa o protocolo especificado. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN006420	2	Os mapas NIS devem ser protegidos usando nomes de domínio difíceis.	**Local** `/etc/security/pscexpert/dodv2/nisplus` **Ação de conformidade** Assegura que os nomes de domínio não sejam fáceis de determinar.
GEN006460	2	Qualquer servidor NIS+ deve estar operando no nível de segurança 2.	**Local** `/etc/security/pscexpert/dodv2/nisplus` **Ação de conformidade** Assegura que o servidor esteja no nível de segurança mínimo especificado. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN006480	2	O sistema deve ser verificado semanalmente quanto a arquivos `setuid` desautorizados e quanto à modificação desautorizada para arquivos `setuid` autorizados.	**Local** `/etc/security/pscexpert/dodv2/trust` **Ação de conformidade** Verifica semanalmente para identificar mudanças nos arquivos especificados.
GEN006560	2	O sistema deve ser verificado semanalmente quanto a arquivos `setuid` desautorizados e quanto à modificação desautorizada para arquivos `setuid` autorizados.	**Local** `/etc/security/pscexpert/dodv2/trust` **Ação de conformidade** Verifica semanalmente para identificar mudanças nos arquivos especificados.
GEN006580	2	O sistema deve usar um programa de controle de acesso.	**Local** `/etc/security/pscexpert/dodv2/checktcpd` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN006600	2	O programa de controle de acesso do sistema deve registrar cada tentativa de acesso de sistema.	**Local** `/etc/security/pscexpert/dodv2/chsyslogdod` **Ação de conformidade** Assegura que as tentativas de acesso sejam registradas.
GEN006620	2	O programa de controle de acesso do sistema deve ser configurado para conceder ou negar acesso de sistema a hosts específicos.	**Local** `/etc/security/pscexpert/dodv2/chetchostsdod` **Ação de conformidade** Configura os arquivos `hosts.deny` e `hosts.allow` para as configurações necessárias.
GEN007020	2	O Stream Control Transmission Protocol (SCTP) deve ser desativado.	**Local** `/etc/security/pscexpert/dodv2/dodv2netrules` **Ação de conformidade** Desativa o protocolo especificado.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN007700	2	O manipulador de protocolos IPv6 não deve ser ligado à pilha de rede a menos que seja necessário.	**Local** `/etc/security/pscexpert/dodv2/rminet6` **Ação de conformidade** Desativa o manipulador de protocolos IPv6 da pilha de rede, a menos que o manipulador seja especificado no arquivo `/etc/ipv6.conf`. **Nota:** Se o seu sistema estiver executando o protocolo IPv6, assegure-se de que a configuração *ipv6_enabled* no arquivo `/etc/security/pscexpert/ipv6.conf` esteja configurada para o valor de `yes`. Se o sistema não estiver usando IPv6, assegure-se de que o valor *ipv6_enabled* esteja configurado para `no`.
GEN007780	2	O sistema não deve ter túneis `6to4` ativados.	**Local** `/etc/security/pscexpert/dodv2/rmiface` **Ação de conformidade** Desativa os túneis especificados. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN007820	2	O sistema não deve ter túneis de IP configurados.	**Local** `/etc/security/pscexpert/dodv2/rmtunnel` **Ação de conformidade** Desativa túneis de IP. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN007840	2	O cliente `DHCP` deve ser desativado se ele não for usado.	**Local** `/etc/security/pscexpert/dodv2/dodv2services` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN007850	2	O cliente DHCP não deve enviar atualizações de DNS dinâmico.	**Local** /etc/security/pscexpert/dodv2/dodv2services **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN007860	2	O sistema deve ignorar mensagens de redirecionamento de IPv6 ICMP.	**Local** /etc/security/pscexpert/dodv2/ntwkoptsdod **Ação de conformidade** Configura o valor da opção de rede ipignoreredirects para *1*.
GEN007880	2	O sistema não deve enviar redirecionamentos de IPv6 ICMP.	**Local** /etc/security/pscexpert/dodv2/ntwkoptsdod **Ação de conformidade** Configura o valor da opção de rede ipsendredirects para *0*.
GEN007900	2	O sistema deve usar um filtro de caminho reverso apropriado para tráfego de rede IPv6, se o sistema usar IPv6.	**Local** /etc/security/pscexpert/dodv2/chuserstanzadod **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN007920	2	O sistema não deve encaminhar pacotes roteados pela origem IPv6.	**Local** /etc/security/pscexpert/dodv2/ntwkoptsdod **Ação de conformidade** Configura o valor da opção de rede ip6srcrouteforward para *0*.
GEN007940: GEN003607	2	O sistema não deve aceitar pacotes IPv4 ou IPv6 roteados pela origem.	**Local** /etc/security/pscexpert/dodv2/ntwkoptsdod **Ação de conformidade** Configura o valor da opção de rede ipsrcrouterecv para *0*.
GEN007950	2	O sistema não deve responder a solicitações de repetição de ICMPv6 que são enviadas a um endereço de transmissão.	**Local** /etc/security/pscexpert/dodv2/ntwkoptsdod **Ação de conformidade** Configura o valor da opção de rede bcastping para *0*.
GEN008000	2	Se o sistema estiver usando o Lightweight Directory Access Protocol (LDAP) para autenticação ou dados da conta, os certificados usados para autenticar no servidor LDAP deverão ser fornecidos a partir do PKI do DoD ou de um método aprovado pelo DoD.	**Local** /etc/security/pscexpert/dodv2/ldap_config **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN008020	2	Se o sistema estiver usando LDAP para autenticação ou dados da conta, a conexão de Segurança da Camada de Transporte (TLS) LDAP deverá requerer que o servidor forneça um certificado com um caminho confiável válido.	**Local** `/etc/security/pscexpert/dodv2/ldap_config` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN008050	2	Se o sistema estiver usando LDAP para autenticação ou dados da conta, o arquivo `/etc/ldap.conf` (ou equivalente) não deverá conter senhas.	**Local** `/etc/security/pscexpert/dodv2/ldap_config` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN008380	2	O sistema deve ser verificado semanalmente quanto a arquivos `setuid` desautorizados e quanto à modificação desautorizada para arquivos `setuid` autorizados.	**Local** `/etc/security/pscexpert/dodv2/trust` **Ação de conformidade** Verifica semanalmente para identificar mudanças nos arquivos especificados.
GEN008520	2	O sistema deve empregar um firewall local que guarde o host com relação a varreduras de portas. O firewall deve evitar portas vulneráveis por 5 minutos para guardar o host com relação a varreduras de portas.	**Local** `/etc/security/pscexpert/dodv2/ipsecshunports` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados.
GEN008540	2	O firewall local do sistema deve implementar uma política *deny-all, allow-by-exception*.	**Local** `/etc/security/pscexpert/dodv2/ipsecshunhosthls` **Ação de conformidade** Assegura que o sistema atenda aos requisitos especificados. **Nota:** É possível inserir regras de filtragem adicionais no arquivo `/etc/security/aixpert/bin/filter.txt`. Essas regras são integradas pelo script `ipsecshunhosthls.sh` ao aplicar o perfil. As entradas devem estar no formato a seguir: *`port_number`*`:`*`ip_address`*`:` *`action`* em que os valores possíveis para *action* são `Allow` ou `Deny`.
GEN008600	1	O sistema deve ser configurado para iniciar somente a partir da configuração de inicialização do sistema.	**Local** `/etc/security/pscexpert/dodv2/dodv2cat1` **Ação de conformidade** Assegura que o início do sistema use somente a configuração de inicialização do sistema.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN008640	1	O sistema não deve usar mídia removível como o carregador de inicialização.	**Local** `/etc/security/pscexpert/dodv2/dodv2cat1` **Ação de conformidade** Assegura que o sistema não inicialize a partir de uma unidade removível.
GEN009140	1,2,3	O sistema não deve ter o serviço `chargen` ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009160	1,2,3	O sistema não deve ter o serviço `Calendar Management Service Daemon` (CMSD) ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009180	1,2,3	O sistema não deve ter o serviço `tool-talk database server` (ttdbserver) ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009190	1,2,3	O sistema não deve ter o serviço `comsat` ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009200-9330	1,2,3	O sistema não pode ter outros serviços e daemons ativos.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009210	2	O sistema não deve ter o serviço `discard` ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN009220	2	O sistema não deve ter o serviço `dtspc` ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009230	2	O sistema não deve ter o serviço `echo` ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009240	2	O sistema não deve ter o serviço `Internet Message Access Protocol (IMAP)` ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009250	2	O sistema não deve ter o serviço `PostOffice Protocol (POP3)` ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009260	2	O sistema não deve ter os serviços talk ou `ntalk` ativos.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009270	2	O sistema não deve ter o serviço `netstat` ativo no processo InetD.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009280	2	O sistema não deve ter o serviço `PCNFS` ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.

Tabela 3. Requisitos gerais do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Categoria da regra do STIG	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN009290	2	O sistema não deve ter o serviço `systat` ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009300	2	O serviço `inetd time` não deve estar ativo no sistema no daemon `inetd`.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009310	2	O sistema não deve ter o serviço `rusersd` ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009320	2	O sistema não deve ter o serviço `sprayd` ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009330	2	O sistema não deve ter o serviço `rstatd` ativo.	**Local** `/etc/security/pscexpert/dodv2/inetdservices` **Ação de conformidade** Desativa os daemons e serviços necessários comentando as entradas no arquivo `/etc/inetd.conf`.
GEN009340	2	Os gerenciadores de login do servidor X não devem estar em execução a menos que sejam necessários para o gerenciamento de sessões X1.	**Local** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Ação de conformidade** Essa regra desativa as conexões do X Window System e o gerenciador de login do XServer.

Tabela 4. Requisitos de propriedade do DoD

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
AIX00085	O arquivo `/etc/netsvc.conf` deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
AIX00090	O arquivo `/etc/netsvc.conf` deve ser de propriedade de grupo de bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, sys ou sistema.
AIX00320	O arquivo `/etc/ftpaccess.ctl` deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
AIX00330	O arquivo `/etc/ftpaccess.ctl` deve ser de propriedade de grupo de bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, sys ou sistema.
GEN000250	O arquivo de configuração de sincronização de horário (como `/etc/ntp.conf`) deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN000251	O arquivo de configuração de sincronização de horário (como `/etc/ntp.conf`) deve ser de propriedade de grupo de bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, sys ou sistema.
GEN001160	Todos os arquivos e diretórios devem ter um proprietário válido.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que todos os arquivos e diretórios possuam um proprietário válido.
GEN001170	Todos os arquivos e diretórios devem ter um proprietário do grupo válido.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que todos os arquivos e diretórios possuam um proprietário válido.
GEN001220	Todos os arquivos de sistema, programas e diretórios devem ser de propriedade de uma conta do sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos de sistema, programas e diretórios sejam de propriedade de uma conta do sistema.

Tabela 4. Requisitos de propriedade do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN001240	Os arquivos de sistema, programas e diretórios devem ser de propriedade de grupo de um grupo do sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Todos os arquivos de sistema, programas e diretórios são de propriedade de grupo de um grupo do sistema.
GEN001320	Os arquivos de Network Information Systems (NIS)/NIS+/yp devem ser de propriedade de raiz, sys ou bin.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos especificados sejam de propriedade de raiz, sys ou bin.
GEN001340	Os arquivos NIS/NIS+/yp devem ser de propriedade de grupo de sys, bin, outro ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos especificados sejam de propriedade de sys, bin, outro ou sistema.
GEN001362	O arquivo `/etc/resolv.conf` deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN001363	O arquivo `/etc/resolv.conf` deve ser de propriedade de grupo de bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, sys ou sistema.
GEN001366	O arquivo `/etc/hosts` deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN001367	O arquivo `/etc/hoststpaccess.ctl` deve ser de propriedade de grupo de bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, sys ou sistema.
GEN001371	O arquivo `/etc/nsswitch.conf` deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.

Tabela 4. Requisitos de propriedade do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN001372	O arquivo `/etc/nsswitch.conf` deve ser de propriedade de grupo de raiz, bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de raiz, bin, sys ou sistema.
GEN001378	O arquivo `/etc/passwd` deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN001379	O arquivo `/etc/passwd` deve ser de propriedade de grupo de bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, segurança, sys ou sistema.
GEN001391	O arquivo `/etc/group` deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN001392	O arquivo `/etc/group` deve ser de propriedade de grupo de bin, segurança, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, segurança, sys ou sistema.
GEN001400	O arquivo `/etc/security/passwd` deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN001410	O arquivo `/etc/security/passwd` deve ser de propriedade de grupo de bin, segurança, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, segurança, sys ou sistema.
GEN001500	Os diretórios iniciais de todos os usuários interativos devem ser de propriedade de seus respectivos usuários.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os diretórios iniciais de todos os usuários interativos devem ser de propriedade de seus respectivos usuários.

Tabela 4. Requisitos de propriedade do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN001520	Os diretórios iniciais de todos os usuários interativos devem ser de propriedade de grupo do grupo primário do proprietário do diretório inicial.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os diretórios iniciais de todos os usuários interativos sejam de propriedade de grupo do grupo primário do proprietário do diretório inicial.
GEN001540	Todos os arquivos e diretórios contidos nos diretórios iniciais do usuário interativo devem ser de propriedade do proprietário do diretório inicial.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que todos os arquivos e diretórios contidos nos diretórios iniciais do usuário interativo sejam de propriedade do proprietário do diretório inicial.
GEN001550	Todos os arquivos e diretórios contidos nos diretórios iniciais do usuário devem ser de propriedade de grupo de um grupo no qual o proprietário do diretório inicial é um membro.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que todos os arquivos e diretórios contidos nos diretórios iniciais do usuário sejam de propriedade de grupo de um grupo no qual o proprietário do diretório inicial é um membro.
GEN001660	Todos os arquivos de início do sistema devem ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos especificados sejam de propriedade de raiz.
GEN001680	Todos os arquivos de início do sistema devem ser de propriedade de grupo de sys, bin, outro ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos especificados sejam de propriedade de grupo de sys, bin, outro ou sistema.
GEN001740	Todos os arquivos de inicialização globais devem ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos especificados sejam de propriedade de raiz.
GEN001760	Todos os arquivos de inicialização globais devem ser de propriedade de grupo de sys, bin, sistema ou segurança.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos especificados sejam de propriedade de grupo de sys, bin, sistema ou segurança.

Tabela 4. Requisitos de propriedade do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN001820	Todos os arquivos e diretórios de estrutura básica (geralmente em `/etc/skel`) devem ser de propriedade de raiz ou bin.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos e diretórios especificados sejam de propriedade de raiz ou bin.
GEN001830	Todos os arquivos de estrutura básica (geralmente em `/etc/skel`) devem ser de propriedade de grupo de segurança.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos especificados sejam de propriedade de grupo de segurança.
GEN001860	Todos os arquivos de inicialização locais devem ser de propriedade de usuário ou raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos especificados sejam de propriedade do usuário ou raiz.
GEN001870	Os arquivos de inicialização locais devem ser de propriedade de grupo do grupo primário do usuário ou raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos de inicialização locais sejam de propriedade de grupo do grupo primário do usuário ou raiz.
GEN002060	Todos os arquivos `.rhosts`, `.shosts`, `.netrc` ou `hosts.equiv` devem ser acessíveis somente por raiz ou pelo proprietário.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que somente a raiz ou o proprietário pode acessar os arquivos especificados.
GEN002100	O arquivo `.rhosts` não deve ser suportado pelo Pluggable Authentication Module (PAM).	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado não esteja disponível usando o PAM.
GEN002200	Todos os arquivos de shell devem ser de propriedade de raiz ou bin.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos especificados sejam de propriedade de raiz ou bin.
GEN002210	Todos os arquivos de shell devem ser de propriedade de grupo de raiz, bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos especificados sejam de propriedade de grupo de raiz, bin, sys ou sistema.

Tabela 4. Requisitos de propriedade do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN002340	Os dispositivos de áudio devem ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que todos os dispositivos de áudio sejam de propriedade de raiz.
GEN002360	Todos os dispositivos de áudio devem ser de propriedade de grupo de raiz, sys, bin ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que todos os dispositivos de áudio sejam de propriedade de grupo de raiz, sys, bin ou sistema.
GEN002520	Todos os diretórios públicos devem ser de propriedade de raiz ou uma conta de aplicativo.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que todos os diretórios públicos sejam de propriedade de raiz ou uma conta de aplicativo.
GEN002540	Todos os diretórios públicos devem ser de propriedade de grupo de sistema ou um grupo de aplicativos.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que todos os diretórios públicos sejam de propriedade de sistema ou um grupo de aplicativos.
GEN002680	Os logs de auditoria do sistema devem ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos especificados sejam de propriedade de raiz.
GEN002690	Os logs de auditoria do sistema devem ser de propriedade de grupo de bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos especificados sejam de propriedade de grupo de bin, sys ou sistema.
GEN003020	O `Cron` não deve executar programas em, ou subordinados a, diretórios livremente graváveis.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Evita que `cron` execute programas em, ou subordinados a, diretórios livremente graváveis.
GEN003040	`Crontabs` deve ser de propriedade de raiz ou do criador de crontab.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que crontabs sejam de propriedade de raiz ou do criador de crontab.

Tabela 4. Requisitos de propriedade do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN003050	Os arquivos `Crontab` devem ser de propriedade de grupo de sistema, de cron ou do grupo primário do criador de crontab.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos `crontab` sejam de propriedade de grupo de sistema, cron ou do grupo primário do criador de crontab.
GEN003110	Os diretórios `Cron` e `crontab` não devem ter listas de controle de acesso estendido.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os diretórios especificados não tenham listas de controle de acesso estendido.
GEN003120	Os diretórios `Cron` e `crontab` devem ser de propriedade de raiz ou bin.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os diretórios cron e crontab sejam de propriedade de raiz ou bin.
GEN003140	Os diretórios `Cron` e `crontab` devem ser de propriedade de grupo de sistema, sys, bin ou cron.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os diretórios especificados sejam de propriedade de grupo de sistema, sys, bin ou cron.
GEN003160	A criação de log de Cron deve ser implementada.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que a criação de log de cron seja implementada.
GEN003240	O arquivo `cron.allow` deve ser de propriedade de raiz, bin ou sys.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz, bin ou sys.
GEN003250	O arquivo `cron.allow` deve ser de propriedade de grupo de sistema, bin, sys ou cron.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de sistema, bin, sys ou cron.
GEN003260	O arquivo `cron.deny` deve ser de propriedade de raiz, bin ou sys.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz, bin ou sys.

Tabela 4. Requisitos de propriedade do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN003270	O arquivo `cron.deny` deve ser de propriedade de grupo de sistema, bin, sys ou cron.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de sistema, bin, sys ou cron.
GEN003420	O diretório `at` deve ser de propriedade de raiz, bin, sys, daemon ou cron.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o diretório especificado seja de propriedade de raiz, sys, daemon ou cron.
GEN003430	O diretório `at` deve ser de propriedade de grupo de sistema, bin, sys ou cron.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o diretório especificado seja de propriedade de grupo de sistema, bin, sys ou cron.
GEN003460	O arquivo `at.allow` deve ser de propriedade de raiz, bin ou sys.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz, bin ou sys.
GEN003470	O arquivo `at.allow` deve ser de propriedade de grupo de sistema, bin, sys ou cron.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de sistema, bin, sys ou cron.
GEN003480	O arquivo `at.deny` deve ser de propriedade de raiz, bin ou sys.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz, bin ou sys.
GEN003490	O arquivo `at.deny` deve ser de propriedade de grupo de sistema, bin, sys ou cron.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de sistema, bin, sys ou cron.
GEN003720	O arquivo `inetd.conf`, o arquivo `xinetd.conf` e o diretório `xinetd.d` devem ser de propriedade de raiz ou bin.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos e o diretório especificados sejam de propriedade de raiz ou bin.

Tabela 4. Requisitos de propriedade do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN003730	O arquivo `inetd.conf`, o arquivo `xinetd.conf` e o diretório `xinetd.d` devem ser de propriedade de grupo de bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos e o diretório especificados sejam de propriedade de grupo de bin, sys ou sistema.
GEN003760	O arquivo `services` deve ser de propriedade de raiz ou bin.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz ou bin.
GEN003770	O arquivo `services` deve ser de propriedade de grupo de bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, sys ou sistema.
GEN003920	O arquivo `hosts.lpd` (ou equivalente) deve ser de propriedade de raiz, bin, sys ou lp.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz, bin, sys ou lp.
GEN003930	O arquivo `hosts.lpd` (ou equivalente) deve ser de propriedade de grupo de bin, sys ou systema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, sys ou sistema.
GEN003960	O proprietário do comando **traceroute** deve ser raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o proprietário do comando seja raiz.
GEN003980	O comando **traceroute** deve ser de propriedade de grupo de sys, bin ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o comando seja de propriedade de grupo de sys, bin ou sistema.
GEN004360	O arquivo `alias` deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN004370	O arquivo `aliases` deve ser de propriedade de grupo de sys, bin ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de sys, bin ou sistema.

Tabela 4. Requisitos de propriedade do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN004400	Os arquivos que são executados por meio de um arquivo `aliases` de e-mail devem ser de propriedade de raiz e devem estar localizados em um diretório que seja de propriedade e gravável somente por raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos que são executados por meio de um arquivo `aliases` de e-mail sejam de propriedade de raiz e estejam localizados em um diretório que seja de propriedade e gravável somente por raiz.
GEN004410	Os arquivos que são executados por meio de um arquivo `aliases` de e-mail devem ser de propriedade de grupo de raiz, bin, sys ou outro. Eles também deve estar localizados em um diretório que seja de propriedade de grupo de raiz, bin, sys ou outro.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos que são executados por meio de um arquivo `aliases` de e-mail sejam de propriedade de grupo de raiz, bin, sys ou outro. Assegura também que estejam localizados em um diretório que seja de propriedade de grupo de raiz, bin, sys ou outro.
GEN004480	O arquivo de log de serviço SMTP deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN004920	O arquivo `ftpusers` deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN004930	O arquivo `ftpusers` deve ser de propriedade de grupo de bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, sys ou sistema.
GEN005360	O arquivo `snmpd.conf` deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN005365	O arquivo `snmpd.conf` deve ser de propriedade de grupo de bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, sys ou sistema.
GEN005400	O arquivo `/etc/syslog.confd` deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.

Tabela 4. Requisitos de propriedade do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN005420	O arquivo `/etc/syslog.conf` deve ser de propriedade de grupo de bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, sys ou sistema.
GEN005610	O sistema não deve ter o encaminhamento de IP para IPv6 ativado, a menos que o sistema seja um roteador de IPv6.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o encaminhamento de IP para IPv6 não esteja ativado a menos que o sistema esteja sendo usado como um roteador de IPv6.
GEN005740	O arquivo de configuração de exportação do NFS deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN005750	O arquivo de configuração de exportação do NFS deverá ser de propriedade de grupo de raiz, bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de raiz, bin, sys ou sistema.
GEN005800	Todos os arquivos de sistema e diretórios do sistema exportados pelo NFS devem ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN005810	Todos os arquivos de sistema e diretórios do sistema exportados pelo NFS devem ser de propriedade de grupo de raiz, bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos e diretórios especificados sejam de propriedade de grupo de raiz, bin, sys ou sistema.
GEN006100	O arquivo `/usr/lib/smb.conf` deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN006120	O arquivo `/usr/lib/smb.conf` deve ser de propriedade de grupo de bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, sys ou sistema.

Tabela 4. Requisitos de propriedade do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN006160	O arquivo `/var/private/smbpasswd` deve ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN006180	O arquivo `/var/private/smbpasswd` deve ser de propriedade de grupo de sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de sys ou sistema.
GEN006340	Os arquivos no diretório `/etc/news` devem ser de propriedade de raiz ou notícias.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o diretório especificado seja de propriedade de raiz ou notícias.
GEN006360	O arquivos em `/etc/news` devem ser de propriedade de grupo de sistema ou notícias.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que os arquivos especificados sejam de propriedade de grupo de sistema ou notícias.
GEN008080	Se o sistema estiver usando LDAP para autenticação ou dados da conta, o arquivo `/etc/ldap.conf` (ou equivalente) deverá ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN008100	Se o sistema estiver usando LDAP para autenticação ou dados da conta, o arquivo `/etc/ldap.conf` (ou equivalente) deverá ser de propriedade de grupo de segurança, bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, sys ou sistema.
GEN008140	Se o sistema estiver usando LDAP para autenticação ou dados da conta, o arquivo ou diretório de autoridade de certificação TLS deverá ser de propriedade de raiz.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de raiz.
GEN008160	Se o sistema estiver usando LDAP para autenticação ou dados da conta, o arquivo ou diretório de autoridade de certificação TLS deverá ser de propriedade de grupo de raiz, bin, sys ou sistema.	**Local** `/etc/security/pscexpert/dodv2/chowndodfiles` **Ação de conformidade** Assegura que o arquivo especificado seja de propriedade de grupo de bin, sys ou sistema.

Tabela 5. Padrões do DoD para permissões de arquivo

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
AIX00100	O arquivo `/etc/netsvc.conf` deve ter o modo 0644 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
AIX00340	O arquivo `/etc/ftpaccess.ctl` deve ter o modo 0640 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN000252	O arquivo de configuração de sincronização de horário (como `/etc/ntp.conf`) deve ter o modo 0640 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN000920	O diretório inicial da conta raiz (diferente de /) deve ter o modo 0700.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o diretório seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001140	Os arquivos e diretórios de sistema não devem ter permissões de acesso irregulares.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que as permissões de acesso sejam consistentes.
GEN001180	Todos os arquivos de daemon de serviços de rede devem ter o modo 0755 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001200	Todos os arquivos de comando do sistema devem ter o modo 0755 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.

Tabela 5. Padrões do DoD para permissões de arquivo (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN001260	Os arquivos de log do sistema devem ter o modo 0640 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001280	Os arquivos de página do manual devem ter o modo 0644 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001300	Os arquivos de biblioteca devem ter o modo 0755 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001360	Os arquivos NIS/NIS+/yp devem ter o modo 0755 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001364	O arquivo `/etc/resolv.conf` deve ter o modo 0644 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001368	O arquivo `/etc/hosts` deve ter o modo 0644 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001373	O arquivo `/etc/nsswitch.conf` deve ter o modo 0644 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.

Tabela 5. Padrões do DoD para permissões de arquivo (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN001380	O arquivo `/etc/passwd` deve ter o modo 0644 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001393	O arquivo `/etc/group` deve ter o modo 0644 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001420	O arquivo `/etc/security/passwd` deve ter o modo 0400.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001480	Todos os diretórios iniciais de um usuário devem ter um modo de 0750 ou menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001560	Todos os arquivos e diretórios contidos nos diretórios iniciais de um usuário devem ter o modo 0750 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001580	Todos os scripts de controle de execução devem ter o modo 0755 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001640	Os scripts de controle de execução não devem executar programas ou scripts livremente graváveis.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Verifica programas, como `cron`, quanto a programas ou scripts livremente graváveis.

Tabela 5. Padrões do DoD para permissões de arquivo (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN001720	Todos os arquivos de inicialização globais devem ter o modo 0644 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001800	Todos os arquivos de estrutura básica (por exemplo, arquivos em `/etc/skel`) deve ter o modo 0644 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN001880	Todos os arquivos de inicialização locais devem ter o modo 0740 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN002220	Todos os arquivos de shel devem ter o modo 0755 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN002320	Os dispositivos de áudio devem ter o modo 0660 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os dispositivos de áudio sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN002560	O padrão do sistema e usuário **umask** deve ser 077.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que as configurações especificadas sejam *077*.
GEN002700	Os logs de auditoria do sistema devem ter o modo 0640 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.

Tabela 5. Padrões do DoD para permissões de arquivo (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN002717	Os arquivos executáveis da ferramenta de auditoria do sistema devem ter o modo 0750 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN002980	O arquivo `cron.allow` deve ter o modo 0600 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN003080	Os arquivos Crontab devem ter o modo 0600 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN003090	Os arquivos `Crontab` não devem ter listas de controle de acesso estendido (ACLs).	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos especificados não tenham ACLs estendidas.
GEN003100	Os diretórios Cron e crontab devem ter o modo 0755 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os diretórios especificados sejam configurados para o modo de permissões especificado, ou para um que seja menos permissivo.
GEN003180	O arquivo `cronlog` deve ter o modo 0600 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN003200	O arquivo `cron.deny` deve ter o modo 0600 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.

Tabela 5. Padrões do DoD para permissões de arquivo (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN003252	O arquivo `at.deny` deve ter o modo 0640 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN003340	O arquivo `at.allow` deve ter o modo 0600 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN003400	O diretório `at` deve ter o modo 0755 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o diretório seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN003440	As tarefas `At` não devem configurar o parâmetro **`umask`** para um valor menos restritivo que 077.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o parâmetro seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN003740	Os arquivos `inetd.conf` e `xinetd.conf` devem ter o modo 0440 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN003780	O arquivo `services` deve ter o modo 0444 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN003940	O arquivo `hosts.lpd` (ou equivalente) deve ter o modo 0644 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.

Tabela 5. Padrões do DoD para permissões de arquivo (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN004000	O arquivo `traceroute` deve ter o modo 0700 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN004380	O arquivo `alias` deve ter o modo 0644 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN004420	Os arquivos que são executados por meio do arquivo `aliases` de e-mail devem ter o modo 0755 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN004500	O arquivo de log de serviço SMTP deve ter o modo 0644 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN004940	O arquivo `ftpusers` deve ter o modo 0640 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN005040	Todos os usuários do FTP devem ter uma configuração **`umask`** padrão de 077.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que a configuração esteja correta.
GEN005100	O daemon `TFTP` deve ter o modo 0755 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o daemon seja configurado para o modo especificado, ou para um que seja menos permissivo.

Tabela 5. Padrões do DoD para permissões de arquivo (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN005180	Todos os arquivos `.Xauthority` devem ter o modo 0600 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN005320	O arquivo `snmpd.conf` deve ter o modo 0600 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN005340	Os arquivos Management Information Base (MIB) devem ter o modo 0640 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN005390	O arquivo `/etc/syslog.conf` deve ter o modo 0640 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN005522	Os arquivos-chave do host públicos SSH devem ter o modo 0644 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN005523	Os arquivos-chave do host privados SSH devem ter o modo 0600 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que os arquivos sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN006140	O arquivo `/usr/lib/smb.conf` deve ter o modo 0644 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.

Tabela 5. Padrões do DoD para permissões de arquivo (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN006200	O arquivo `var/private/smbpasswdallow` deve ter o modo 0600 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN006260	O arquivo `/etc/news/hosts.nntp` (ou equivalente) deve ter o modo 0600 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN006280	O arquivo `/etc/news/hosts.nntp.nolimit` (ou equivalente) deve ter o modo 0600 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN006300	O arquivo `/etc/news/nnrp.accessnews/hosts.nntp` (ou equivalente) deve ter o modo 0600 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN006320	O arquivo `/etc/news/passwd.nntp` (ou equivalente) deve ter o modo 0600 ou um modo que seja menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN008060	Se o sistema estiver usando LDAP para autenticação ou dados da conta, o arquivo `/etc/ldap.conf` (ou equivalente) deverá ter o modo 0644 ou ser menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo seja configurado para o modo de permissão especificado, ou para um que seja menos permissivo.
GEN008180	Se o sistema estiver usando LDAP para autenticação ou dados da conta, o arquivo ou diretório de autoridade de certificação TLS, ou ambos, deverá ter o modo 0644 (0755 para diretórios) ou ser menos permissivo.	**Local** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Ação de conformidade** Assegura que o arquivo, os diretórios, ou ambos, sejam configurados para o modo de permissão especificado, ou para um que seja menos permissivo.

Tabela 6. Requisitos de lista de controle de acesso (ACL) do DoD

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
AIX00110	O arquivo `/etc/netsvc.conf` não deve ter uma lista de controle de acesso estendida (ACL).	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
AIX00350	O arquivo `/etc/ftpaccess.ctl` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN000253	O arquivo de configuração de sincronização de horário (como `/etc/ntp.conf`) não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN000930	O diretório inicial da conta raiz não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001190	Todos os arquivos de daemon de serviços de rede não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 6. Requisitos de lista de controle de acesso (ACL) do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN001210	Todos os arquivos de comando do sistema não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001270	Os arquivos de log do Sistema não devem ter ACLs estendidas, exceto conforme necessário para suportar software autorizado.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001310	Todos os arquivos de biblioteca não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001361	Os arquivos de comando NIS/NIS+/yp não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001365	O arquivo `/etc/resolv.conf` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 6. Requisitos de lista de controle de acesso (ACL) do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN001369	O arquivo `/etc/hosts` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001374	O arquivo `/etc/nsswitch.conf` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001390	O arquivo `/etc/passwd` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001394	O arquivo `/etc/group` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001430	O arquivo `/etc/security/passwd` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 6. Requisitos de lista de controle de acesso (ACL) do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN001570	Todos os arquivos e diretórios contidos em diretórios iniciais do usuário não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001590	Todos os scripts de controle de execução não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001730	Todos os arquivos de inicialização globais não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001810	Os arquivos de estrutura básica não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN001890	Os arquivos de inicialização locais não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 6. Requisitos de lista de controle de acesso (ACL) do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN002230	Todos os arquivos de shell não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN002330	Os dispositivos de áudio não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN002710	Todos os arquivos de auditoria do sistema não devem ter ACLs estendidas	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN002990	As ACLs estendidas devem ser desativadas para os arquivos `cron.allow` e `cron.deny`.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN003090	Os arquivos Crontab não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 6. Requisitos de lista de controle de acesso (ACL) do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN003110	Os diretórios Cron e crontab não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN003190	Os arquivos de log cron não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN003210	O arquivo `cron.deny` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN003245	O arquivo `at.allow` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN003255	O arquivo `at.denyeny` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 6. Requisitos de lista de controle de acesso (ACL) do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN003410	O diretório `at` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN003745	Os arquivos `inetd.conf` e `xinetd.conf` não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN003790	O arquivo de serviços não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN003950	O arquivo `hosts.lpd` (ou equivalente) não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN004010	O arquivo `traceroute` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 6. Requisitos de lista de controle de acesso (ACL) do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN004390	O arquivo `alias` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN004430	Os arquivos que são executados por meio de um arquivo `aliases` de e-mail não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN004510	O arquivo de log de serviço SMTP não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN004950	O arquivo `ftpusers` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN005190	Os arquivos `.Xauthority` não devem ter ACLS estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 6. Requisitos de lista de controle de acesso (ACL) do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN005350	Os arquivos Management Information Base (MIB) não devem ter ACLs estendidas.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN005375	O arquivo `snmpd.conf` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN005395	O arquivo `/etc/syslog.conf` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN006150	O arquivo `/usr/lib/smb.conf` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN006210	O arquivo `/var/private/smbpasswd` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 6. Requisitos de lista de controle de acesso (ACL) do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN006270	O arquivo `/etc/news/hosts.nntp` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN006290	O arquivo `/etc/news/hosts.nntp.nolimit` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN006310	O arquivo `/etc/news/nnrp.access` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN006330	O arquivo `/etc/news/passwd.nntp` não deve ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Desativa a ACL estendida especificada. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.
GEN008120	Se o sistema estiver usando LDAP para autenticação ou dados da conta, o arquivo `/etc/ldap.conf` (ou equivalente) não deverá ter uma lista de controle de acesso estendido (ACL).	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Assegura que os arquivos especificados não tenham uma ACL estendida. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Tabela 6. Requisitos de lista de controle de acesso (ACL) do DoD (continuação)

ID de ponto de verificação do STIG do Departamento de Defesa	Descrição	Local do script no qual a ação é definida e os resultados da ação que ativa a conformidade
GEN008200	Se o sistema estiver usando LDAP para autenticação ou dados da conta, o arquivo ou diretório de autoridade de certificação LDAP TLS (conforme apropriado) não deverá ter uma ACL estendida.	**Local** `/etc/security/pscexpert/dodv2/acldodfiles` **Ação de conformidade** Assegura que o diretório ou arquivo especificado não tenha uma ACL estendida. **Nota:** Essa configuração não é mudada automaticamente quando a política é reconfigurada para a política padrão do AIX usando o arquivo `DoDv2_to_AIXDefault.xml`. Deve-se mudar manualmente essa configuração.

Informações relacionadas:

Conformidade de STIG do Departamento de Defesa

Conformidade do Payment Card Industry - Data Security Standard

O Payment Card Industry – Data Security Standard (PCI – DSS) categoriza a segurança de TI em 12 seções que são chamadas de 12 procedimentos de avaliação de requisitos e segurança.

Os 12 procedimentos de avaliação de requisitos e segurança de segurança de TI definidos por PCI - DSS incluem os itens a seguir:

Requisito 1: Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão. Lista documentada de serviços e portas necessários para os negócios. Esse requisito é implementado desativando serviços desnecessários e inseguros.

Requisito 2: Não usar padrões oferecidos pelo fornecedor para senhas do sistema e outros parâmetros de segurança.
Sempre mude os padrões fornecidos pelo fornecedor antes de instalar um sistema na rede. Esse requisito é implementado desativando o daemon Protocolo Simples de Gerenciamento de Rede (SNMP).

Requisito 3: Proteger os dados armazenados do titular do cartão.
Esse requisito é implementado ativando o recurso Encrypted File System (EFS) fornecido com o sistema operacional AIX.

Requisito 4: Criptografar os dados do titular do cartão ao transmitir os dados através de redes públicas abertas.
Esse requisito é implementado ativando o recurso IP Security (IPSEC) que é fornecido com o sistema operacional AIX.

Requisito 5: Usar e atualizar regularmente programas de software de antivírus.
Esse requisito é implementado usando o programa da política de Execução Confiável. Execução Confiável é o software de antivírus recomendado e é nativo ao sistema operacional AIX. O PCI requer que você capture os logs do programa Execução Confiável, permitindo que o gerenciamento de informações e evento de segurança (SIEM) monitorem os alertas. Executando o programa de Execução Confiável no modo somente log, não pare as verificações, quando um erro for causado por uma incompatibilidade de hash.

Requisito 6: Desenvolver e manter sistemas e aplicativos seguros.
Para implementar este requisito, você deve instalar as correções necessárias em seu sistema manualmente. Se você comprou o PowerSC Standard Edition, será possível usar o recurso Connect Network Trusted (CNC).

Requisito 7: Restringir o acesso aos dados do titular do cartão, pela necessidade de negócios a ser conhecida.

É possível implementar medidas fortes de controle de acesso usando o recurso RBAC para ativar regras e funções. O RBAC não pode ser automatizado, porque ele requer a entrada de um administrador para ser ativado.

O `RbacEnablement` verifica o sistema para determinar se as propriedades isso, so, e sa para as funções existem no sistema. Se essas propriedades não existirem, o script as criará. Esse script também é executado como parte das verificações de pscexpert que ele conclui quando está executando comandos, como o comando `pscxpert -c`.

Requisito 8: Designar um ID exclusivo para cada usuário que tenha acesso ao computador.

É possível implementar esse requisito ativando os perfis PCI. As regras a seguir aplicam-se ao perfil PCI:

- Altere as senhas do usuário pelo menos a cada 90 dias.
- Requeira um comprimento mínimo de senha de 7.
- Use uma senha que contenha numerais e caracteres alfabéticos.
- Não permita que um indivíduo envie uma nova senha que seja a mesma que as quatro senhas anteriores que foram usadas.
- Limite as tentativas de acesso repetidas bloqueando o ID do usuário após seis tentativas malsucedidas.
- Configure a duração do bloqueio de acesso para 30 minutos ou até que um administrador ative novamente o ID do usuário.
- Requeira que um usuário insira novamente uma senha para reativar um terminal depois que ele ficar inativo por 15 minutos ou mais.

Requisito 9: Restrinja o acesso físico aos dados do dono do cartão.

Repositórios de armazenamento que contêm dados sensitivos do dono do cartão em um espaço de acesso restrito.

Requisito 10: Rastrear e monitorar todo o acesso a recursos da rede e aos dados do dono do cartão.

Esse requisito é implementado registrando o acesso aos componentes do sistema, ativando os logs automáticos nos componentes do sistema.

Requisito 11: Testar regularmente os sistemas e processos de segurança.

Esse requisito é implementado usando o recurso Real-Time Compliance.

Requisito 12: Manter uma política de segurança que inclui segurança de informações para funcionários e contratados.

Ativação de modems para fornecedores somente quando necessário pelos fornecedores, com desativação imediata após o uso. Esse requisito é implementado desativando o login de raiz remoto, ativando em uma base necessária por um administrador do sistema e, em seguida, desativando quando não for mais necessário.

O PowerSC Standard Edition reduz o gerenciamento de configuração que é necessário para atender às diretrizes definidas pelo PCI DSS versão 2.0 e PCI DSS versão 3.0. No entanto, o processo inteiro não pode ser automatizado.

Por exemplo, o acesso restrito aos dados do dono do cartão com base no requisito de negócios não pode ser automatizado. O sistema operacional AIX fornece tecnologias de segurança forte, como o Role Based Access Control (RBAC); no entanto, o PowerSC Standard Edition não pode automatizar essa configuração, porque ele não pode determinar os indivíduos que requerem acesso e os indivíduos que não requerem. O IBM Compliance Expert pode automatizar a configuração de outras configurações de segurança consistentes com os requisitos de PCI.

Quando o perfil PCI é aplicado a um ambiente de banco de dados, várias portas TCP e UDP usadas pela pilha de software são desativadas por restrições. Devem-se ativar essas portas e desativar a função

Trusted Execution para executar o aplicativo e a carga de trabalho. Execute os comandos a seguir para remover as restrições nas portas e desativar a função Trusted Execution:

```
trustchk -p TE=OFF
tcptr -delete 9091 65535
tcptr -delete 9090 9090
tcptr -delete 112 9089
tcptr -add 9091 65535 1024 1
```

Nota: Todos os arquivos de script customizados fornecidos para manter a conformidade de PCI - DSS estão no diretório `/etc/security/pscexpert/bin`.

A tabela a seguir mostra como o PowerSC Standard Edition direciona os requisitos da norma PCI DSS usando as funções do utilitário AIX Security Expert:

Tabela 7. Configurações relacionadas às normas de conformidade do PCI DSS versão 2.0 e versão 3.0

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do script que modifica o valor
2.1	Sempre altere os padrões fornecidos pelo fornecedor antes de instalar um sistema na rede. Por exemplo, inclua senhas, sequências de Protocolo Simples de Gerenciamento de Rede e elimine contas desnecessárias.	Configura o número mínimo de semanas que devem passar antes de poder mudar um senha para 0 semanas, configurando o parâmetro **minage** para o valor de 0.	`/etc/security/pscexpert/bin/chusrattr`
PCI versão 2 8.5.9 **PCI versão 3** 8.2.4	Altere as senhas do usuário pelo menos a cada 90 dias.	Configura o número máximo de semanas que uma senha é válida para 13 semanas, configurando o parâmetro **maxage** para um valor de 13.	`/etc/security/pscexpert/bin/chusrattr`
2.1	Sempre altere os padrões fornecidos pelo fornecedor antes de instalar um sistema na rede. Por exemplo, inclua senhas, sequências de Protocolo Simples de Gerenciamento de Rede e elimine contas desnecessárias.	Configura o número de semanas que uma conta com uma senha expirada permanece no sistema para 8 semanas, configurando o parâmetro **maxexpired** para um valor de 8.	`/etc/security/pscexpert/bin/chusrattr`
PCI versão 2 8.5.10 **PCI versão 3** 8.2.3	Requer um comprimento mínimo da senha de pelo menos 7 caracteres.	Configura o comprimento mínimo de senha para 7 caracteres, configurando o parâmetro **minlen** para um valor de 7.	`/etc/security/pscexpert/bin/chusrattr`
PCI versão 2 8.5.11 **PCI versão 3** 8.2.3	Use as senhas que contêm os caracteres numéricos e alfabéticos.	Configura o número mínimo de caracteres alfabéticos que são necessários em uma senha para 1. Essa configuração assegura que a senha contenha caracteres alfabéticos, configurando o parâmetro **minalpha** para um valor de 1.	`/etc/security/pscexpert/bin/chusrattr`
PCI versão 2 8.5.11 **PCI versão 3** 8.2.3	Use as senhas que contêm os caracteres numéricos e alfabéticos.	Configura o número mínimo de caracteres não alfabéticos que são necessários em uma senha para 1. Essa configuração assegura que a senha contenha caracteres não alfabéticos, configurando o parâmetro **minother** para um valor de 1.	`/etc/security/pscexpert/bin/chusrattr`

Tabela 7. Configurações relacionadas às normas de conformidade do PCI DSS versão 2.0 e versão 3.0 (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do script que modifica o valor
PCI versão 2 2.1 **PCI versão 3** 8.2.2	Sempre altere os padrões fornecidos pelo fornecedor antes de instalar um sistema na rede. Por exemplo, inclua senhas, sequências de Protocolo Simples de Gerenciamento de Rede e elimine contas desnecessárias.	Configura o número máximo de vezes que um caractere pode ser repetido em uma senha para 8, configurando o parâmetro **maxrepeats** para um valor de 8. Essa configuração indica que um caractere em uma senha pode ser repetido um número ilimitado de vezes quando se adequar às outras limitações de senha.	/etc/security/pscexpert/bin/chusrattr
PCI versão 2 8.5.12 **PCI versão 3** 8.2.5	Não permita que um indivíduo envie uma nova senha que é a mesma que qualquer uma das últimas quatro senhas que foram usadas.	Configura o número de semanas antes que uma senha possa ser reutilizada para 52, configurando o parâmetro **histexpire** para um valor de 52.	/etc/security/pscexpert/bin/chusrattr
PCI versão 2 8.5.12 **PCI versão 3** 8.2.5	Não permita que um indivíduo envie uma nova senha que é a mesma que qualquer uma das últimas quatro senhas que foram usadas.	Configura o número de senhas anteriores que não podem ser reutilizadas para 4, configurando o parâmetro **histsize** para um valor de 4.	/etc/security/pscexpert/bin/chusrattr
PCI versão 2 8.5.13 **PCI versão 3** 10.2.4	Limite as tentativas de acesso repetidas bloqueando o ID do usuário após não mais do que seis tentativas.	Configura o número de tentativas de login malsucedidas consecutivas que desativa uma conta para 6 tentativas para cada conta não raiz, configurando o parâmetro **loginentries** para um valor de 6.	/etc/security/pscexpert/bin/chusrattr
PCI versão 2 8.5.13 **PCI versão 3** 10.2.4	Limite as tentativas de acesso repetidas bloqueando o ID do usuário após não mais do que seis tentativas.	Configura o número de tentativas de login malsucedidas consecutivas que desativa uma porta para 6 tentativas, configurando o parâmetro **logindisable** para um valor de 6.	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg
PCI versão 2 8.5.14 **PCI versão 3** 10.2.4	Configure a duração de bloqueio para um mínimo de 30 minutos ou até que o administrador ative o ID do usuário.	Configura a duração de tempo que uma porta fica bloqueada após ser desativada pelo atributo *logindisable* para 30 minutos, configurando o parâmetro **loginreenable** para um valor de 30.	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg
12.3.9	Ativação de tecnologias de acesso remoto para os fornecedores e parceiros de negócios apenas quando necessário por fornecedores e parceiros de negócios, com a desativação imediata após o uso.	Desativa a função de login raiz remoto configurando seu valor como false. O administrador do sistema pode ativar a função de login remoto conforme necessário e, em seguida, desativar quando a tarefa for concluída.	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user

Tabela 7. Configurações relacionadas às normas de conformidade do PCI DSS versão 2.0 e versão 3.0 (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do script que modifica o valor
8.1	Designe um ID exclusivo a todos os usuários antes de permiti-los acessar os componentes do sistema ou os dados do dono do cartão.	Ativa a função que assegura que todos os usuários tenham um nome de usuário exclusivo antes que possam acessar os componentes do sistema ou os dados do dono do cartão configurando essa função como um valor de true.	• `/etc/security/pscexpert/bin/chuserstanza` • `/etc/security/user`
10.2	Ative a auditoria no sistema.	Ativa a auditoria dos arquivos binários no sistema.	`/etc/security/pscexpert/bin/pciaudit`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon `lpd`.	Para o daemon `lpd` e comenta a linha de entrada correspondente no arquivo `/etc/inittab` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/comntrows`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o Common Desktop Environment (CDE).	Desativa a função CDE quando o Layer Four Traceroute (LFT) não for configurado.	`/etc/security/pscexpert/bin/comntrows`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon `timed`.	Para o daemon `timed` e comenta a linha de entrada correspondente no arquivo `/etc/rc.tcpip` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/rctcpip`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon `NTP`.	Para o daemon `NTP` e comenta a linha de entrada correspondente no arquivo `/etc/rc.tcpip` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/rctcpip`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon `rwhod`.	Para o daemon `rwhod` e comenta a linha de entrada correspondente no arquivo `/etc/rc.tcpip` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/rctcpip`
PCI versão 2 2.1 **PCI versão 3** 2.1.1	Altere os padrões fornecidos pelo fornecedor antes de instalar um sistema na rede, que inclui desativar o daemon `SNMP`.	Para o daemon `SNMP` e comenta a linha de entrada correspondente no arquivo `/etc/rc.tcpip` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/rctcpip`
PCI versão 2 2.1 **PCI versão 3** 2.1.1	Altere padrões fornecidos pelo fornecedor antes de instalar um sistema na rede, que inclui desativar o daemon `SNMPMIBD`.	Desativa o daemon `SNMPMIBD` comentando a entrada correspondente no arquivo `/etc/rc.tcpip` que inicia automaticamente o daemon.	`/etc/security/pscexpert/bin/rctcpip`

Tabela 7. Configurações relacionadas às normas de conformidade do PCI DSS versão 2.0 e versão 3.0 (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do script que modifica o valor
2.1	Altere padrões fornecidos pelo fornecedor antes de instalar um sistema na rede, que inclui desativar o daemon AIXMIBD.	Desativa o daemon AIXMIBD comentando a entrada correspondente no arquivo /etc/rc.tcpip que inicia automaticamente o daemon.	/etc/security/pscexpert/bin/rctcpip
2.1	Altere padrões fornecidos pelo fornecedor antes de instalar um sistema na rede, que inclui desativar o daemon HOSTMIBD.	Desativa o daemon HOSTMIBD comentando a entrada correspondente no arquivo /etc/rc.tcpip que inicia automaticamente o daemon.	/etc/security/pscexpert/bin/rctcpip
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon DPID2.	Para o daemon DPID2 e comenta a linha de entrada correspondente no arquivo /etc/rc.tcpip que inicia o daemon automaticamente.	/etc/security/pscexpert/bin/rctcpip
PCI versão 2 2.1 **PCI versão 3** 2.2.2	Altere padrões fornecidos pelo fornecedor antes de instalar um sistema na rede, que inclui parar o servidor DHCP.	Desativa o servidor DHCP.	/etc/security/pscexpert/bin/rctcpip
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o agente DHCP.	Para e desativa o agente de retransmissão DHCP e comenta a linha de entrada correspondente no arquivo /etc/rc.tcpip que inicia automaticamente o agente.	/etc/security/pscexpert/bin/rctcpip
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon rshd.	Para e desativa todas as instâncias do daemon rshd e o serviço de shell e comenta as entradas correspondentes no arquivo /etc/inetd.conf que iniciam automaticamente as instâncias.	/etc/security/pscexpert/bin/cominetdconf
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon rlogind.	Para e desativa todas as instâncias do daemon rlogind e serviço rlogin. O utilitário AIX Security Expert também comenta a linha de entradas correspondentes no arquivo /etc/inetd.conf que inicia as instâncias automaticamente.	/etc/security/pscexpert/bin/cominetdconf
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon rexecd.	Para e desativa todas as instâncias do daemon rexecd. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo /etc/inetd.conf que inicia o daemon automaticamente.	/etc/security/pscexpert/bin/cominetdconf

Tabela 7. Configurações relacionadas às normas de conformidade do PCI DSS versão 2.0 e versão 3.0 (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do script que modifica o valor
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon `comsat`.	Para e desativa todas as instâncias do daemon `comsat`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon `fingerd`.	Para e desativa todas as instâncias do daemon `fingerd`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon `systat`.	Para e desativa todas as instâncias do daemon `systat`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
2.1	Altere padrões fornecidos pelo fornecedor antes de instalar um sistema na rede, que inclui desativar o comando `netstat`.	Desativa o comando `netstat` comentando a entrada correspondente no arquivo `/etc/inetd.conf`.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.3	Desative os serviços não necessários e não seguros, que incluem o daemon `tftp`.	Para e desativa todas as instâncias do daemon `tftp`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon `talkd`.	Para e desativa todas as instâncias do daemon `talkd`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon `rquotad`.	Para e desativa todas as instâncias do daemon `rquotad`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`

Tabela 7. Configurações relacionadas às normas de conformidade do PCI DSS versão 2.0 e versão 3.0 (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do script que modifica o valor
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon `rstatd`.	Para e desativa todas as instâncias do daemon `rstatd`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon `rusersd`.	Para e desativa todas as instâncias do daemon `rusersd`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon `rwalld`.	Para e desativa todas as instâncias do daemon `rwalld`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon `sprayd`.	Para e desativa todas as instâncias do daemon `sprayd`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o daemon `pcnfsd`.	Para e desativa todas as instâncias do daemon `pcnfsd`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o serviço `TCP echo`.	Para e desativa todas as instâncias do serviço `echo(tcp)`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o serviço automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o serviço `TCP discard`.	Para e desativa todas as instâncias do serviço `discard(tcp)`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o serviço automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`

Tabela 7. Configurações relacionadas às normas de conformidade do PCI DSS versão 2.0 e versão 3.0 (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do script que modifica o valor
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o serviço TCP `chargen`.	Para e desativa todas as instâncias do serviço `chargen(tcp)`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o serviço automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o serviço TCP `daytime`.	Para e desativa todas as instâncias do serviço `daytime(tcp)`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o serviço automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o serviço TCP `time`.	Para e desativa todas as instâncias do serviço `timed(tcp)`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o serviço automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o serviço UDP `echo`.	Para e desativa todas as instâncias do serviço `echo(udp)`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o serviço automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o serviço UDP `discard`.	Para e desativa todas as instâncias do serviço `discard(udp)`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o serviço automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o serviço UDP `chargen`.	Para e desativa todas as instâncias do serviço `chargen(udp)`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o serviço automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o serviço UDP `daytime`.	Para e desativa todas as instâncias do serviço `daytime(udp)`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o serviço automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`

Tabela 7. Configurações relacionadas às normas de conformidade do PCI DSS versão 2.0 e versão 3.0 (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do script que modifica o valor
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o serviço `UDP time`.	Para e desativa todas as instâncias do serviço `timed(udp)`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o serviço automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.3	Desative os serviços não necessários e não seguros, que incluem o serviço `FTP`.	Para e desativa todas as instâncias do daemon `ftpd`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.3	Desative os serviços não necessários e não seguros, que incluem o serviço `telnet`.	Para e desativa todas as instâncias do daemon `telnetd`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o daemon automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o `dtspc`.	Para e desativa todas as instâncias do daemon `dtspc`. O AIX Security Expert também comentará a linha de entrada correspondente no arquivo `/etc/inittab` que iniciará automaticamente o daemon quando o LFT não estiver configurado e o CDE estiver desativado no arquivo `/etc/inittab`.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o serviço `ttdbserver`.	Para e desativa todas as instâncias do serviço `ttdbserver`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o serviço automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 2.2.2	Desative os serviços não necessários e não seguros, que incluem o serviço `cmsd`.	Para e desativa todas as instâncias do serviço `cmsd`. O utilitário AIX Security Expert também comenta a linha de entrada correspondente no arquivo `/etc/inetd.conf` que inicia o serviço automaticamente.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versão 2 2.2.3 **PCI versão 3** 2.2.4	Configure os parâmetros de segurança do sistema para evitar mau uso.	Remove os comandos Set User ID (SUID) comentando a entrada correspondente no arquivo `/etc/inetd.conf` que ativa automaticamente os comandos.	`/etc/security/pscexpert/bin/rmsuidfrmrcmds`

Tabela 7. Configurações relacionadas às normas de conformidade do PCI DSS versão 2.0 e versão 3.0 (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do script que modifica o valor
PCI versão 2 2.2.3 **PCI versão 3** 2.2.4	Configure os parâmetros de segurança do sistema para evitar mau uso.	Ativa o nível de segurança mais baixo para o Gerenciador de Permissões de Arquivo.	`/etc/security/pscexpert/bin/filepermgr`
PCI versão 2 2.2.3 **PCI versão 3** 2.2.4	Configure os parâmetros de segurança do sistema para evitar mau uso.	Modifica o protocolo Network File System com configurações restritas que se adequam aos requisitos de segurança PCI. Essas configurações restritas incluem a desativação do acesso raiz remoto e acesso UID e GID anônimo.	`/etc/security/pscexpert/bin/nfsconfig`
PCI versão 2 2.2.2 **PCI versão 3** 2.2.3	Ative apenas os serviços necessários e seguros, protocolos, daemons, etc., conforme necessário para a função correta do sistema. Implemente recursos de segurança para os serviços, protocolos ou daemons necessários que são considerados inseguros.	Ativa os daemons `rlogind`, `rshd` e `tftpd`, que não são seguros.	`/etc/security/pscexpert/bin/disrmtdmns`
PCI versão 2 2.2.2 **PCI versão 3** 2.2.3	Ative apenas os serviços necessários e seguros, protocolos, daemons, etc., conforme necessário para a função correta do sistema. Implemente recursos de segurança para os serviços, protocolos ou daemons necessários que são considerados inseguros.	Ativa os daemons `rlogind`, `rshd` e `tftpd`, que não são seguros.	`/etc/security/pscexpert/bin/rmrhostsnetrc`
PCI versão 2 2.2.2 **PCI versão 3** 2.2.3	Ative apenas os serviços necessários e seguros, protocolos, daemons, etc., conforme necessário para a função correta do sistema. Implemente recursos de segurança para os serviços, protocolos ou daemons necessários que são considerados inseguros.	Desativa os daemons `logind`, `rshd` e `tftpdpci_rmetchostsequiv`, que não são seguros.	`/etc/security/pscexpert/bin/rmetchostsequiv`
PCI versão 2 1.3.6 **PCI versão 3** 2.2.3	Implemente a inspeção stateful ou a filtragem de pacotes em que apenas as conexões estabelecidas são permitidas na rede.	Ativa a opção **`clean_partial_conns`** de rede configurando seu valor como 1.	`/etc/security/pscexpert/bin/ntwkopts`

Tabela 7. Configurações relacionadas às normas de conformidade do PCI DSS versão 2.0 e versão 3.0 (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do script que modifica o valor
PCI versão 2 2.2.2 **PCI versão 3** 2.2.3	Implemente a inspeção stateful ou a filtragem de pacotes em que apenas as conexões estabelecidas são permitidas na rede.	Ativa a segurança de TCP configurando a opção **tcp_tcpsecure** de rede como um valor de 7. Essa configuração fornece proteção com relação aos dados, reconfiguração (RST) e ataques de solicitação de conexão TCP (SYN).	`/etc/security/pscexpert/bin/ntwkopts`
1.2	Proteja o acesso não autorizado a portas não usadas.	Configura o sistema para evitar os hosts por 5 minutos para evitar que outros sistemas acessem portas não usadas.	`/etc/security/pscexpert/bin/ipsecshunhosthls` **Nota:** É possível inserir regras de filtragem adicionais no arquivo `/etc/security/aixpert/bin/filter.txt`. Essas regras são integradas pelo script `ipsecshunhosthls.sh` ao aplicar o perfil. As entradas devem estar no formato a seguir: *port_number*:*ip_address*:*action* em que os valores possíveis para *action* são `Allow` ou `Deny`.
1.2	Proteja o host a partir de varreduras de porta.	Configura o sistema para evitar portas vulneráveis por 5 minutos, que evita varreduras de porta.	`/etc/security/pscexpert/bin/ipsecshunports` **Nota:** É possível inserir regras de filtragem adicionais no arquivo `/etc/security/aixpert/bin/filter.txt`. Essas regras são integradas pelo script `ipsecshunhosthls.sh` ao aplicar o perfil. As entradas devem estar no formato a seguir: *port_number*:*ip_address*:*action* em que os valores possíveis para *action* são `Allow` ou `Deny`.
1.2	Limite as permissões de criação de objeto.	Configura as permissões de criação de objeto padrão para 22, configurando o parâmetro **umask** para um valor de 22.	`/etc/security/pscexpert/bin/chusrattr`
1.2	Limite o acesso de sistema.	Assegura que o ID raiz seja o único listado no arquivo `cron.allow` e remove o arquivo `cron.deny` do sistema.	`/etc/security/pscexpert/bin/limitsysacc`
6.5.8	Remova o ponto da raiz do caminho.	Remove os pontos da variável de ambiente PATH nos arquivos a seguir localizados no diretório inicial raiz: • .cshrc • .kshrc • .login • .profile	`/etc/security/pscexpert/bin/rmdotfrmpathroot`

Tabela 7. Configurações relacionadas às normas de conformidade do PCI DSS versão 2.0 e versão 3.0 (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do script que modifica o valor
6.5.8	Remova o ponto do caminho não raiz:	Remove os pontos da variável de ambiente *PATH* nos arquivos a seguir no diretório inicial do usuário: • .cshrc • .kshrc • .login • .profile	`/etc/security/pscexpert/bin/rmdotfrmpathnroot`
2.2.3	Limite o acesso de sistema.	Inclui o recurso de usuário raiz e o nome de usuário no arquivo `/etc/ftpusers`.	`/etc/security/pscexpert/bin/chetcftpusers`
2.1	Remova a conta guest.	Remove a conta guest e seus arquivos.	`/etc/security/pscexpert/bin/execmds`
6.5.2	Evite programas de ativação na área de conteúdo.	Ativa o recurso Stack Execution Disable (SED).	`/etc/security/pscexpert/bin/sedconfig`
8.2	Assegure-se de que a senha para a raiz não seja fraca.	Inicia uma verificação de integridade de senha raiz com relação à senha raiz, desse modo, assegurando uma senha raiz forte.	`/etc/security/pscexpert/bin/chuserstanza`
PCI versão 2 8.5.15 **PCI versão 3** 8.1.8	Limite o acesso de sistema, configurando o tempo inativo de sessão.	Configura o limite de tempo inativo para 15 minutos. Se a sessão estiver inativa por mais de 15 minutos você deverá inserir novamente a senha.	`/etc/security/pscexpert/bin/autologoff`
1.3.5	Limite o tráfego de acesso para informações do dono do cartão.	Configura o regulamento de tráfego TCP para sua configuração alta, que impinge a mitigação da negação de serviço em portas.	`/etc/security/pscexpert/bin/tcptr_pscexpert`
1.3.5	Mantenha uma conexão segura ao migrar dados.	Ativa a criação do túnel IP Security (IPSec) automatizada entre Servidores de E/S Virtuais durante a migração da partição ativa.	`/etc/security/pscexpert/bin/cfgsecmig`
1.3.5	Limite os pacotes a partir de origens desconhecidas.	Ativa os pacotes do Hardware Management Console.	`/etc/security/pscexpert/bin/ipsecpermithostorport`
5.1.1	Mantenha o software antivírus.	Mantém a integridade do sistema detectando, removendo e a protegendo com relação aos tipos conhecidos de software malicioso.	`/etc/security/pscexpert/bin/manageITsecurity`
PCI versão 2 Seção 7 **PCI versão 3** Seção 7	Mantenha o acesso em uma base, conforme necessário.	Ative o Role Based Access Control (RBAC) criando o operador do sistema, o administrador do sistema e as funções de usuário executivo de segurança do sistema de informações com as permissões necessárias.	`/etc/security/pscexpert/bin/EnableRbac`

Tabela 7. Configurações relacionadas às normas de conformidade do PCI DSS versão 2.0 e versão 3.0 (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do script que modifica o valor
PCI versão 2 Não incluído no perfil da versão 2, incluído na versão 3. **PCI versão 3** 2.3	Implemente mais recursos de segurança para quaisquer serviços, protocolos ou daemons necessários que forem considerados não seguros.	Usa tecnologias asseguradas, como Shell Seguro (SSH), SSH File Transfer Protocol (S-FTP), Secure Sockets Layer (SSL) ou Internet Protocol Security Virtual Private Network (IPsec VPN) para proteger serviços não seguros, como NetBIOS, compartilhamento de arquivo, Telnet e FTP. Também configura o daemon SSH para usar somente o protocolo SSHv2.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versão 2 Não incluído no perfil da versão 2, incluído na versão 3. **PCI versão 3** 2.3	O Cliente SSH deve ser configurado para usar somente o protocolo SSHv2.	Configura o cliente SSH para usar o protocolo SSHv2.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versão 2 Não incluído no perfil da versão 2, incluído na versão 3. **PCI versão 3** 2.3	O daemon SSH deve atender somente em endereços de rede de gerenciamento, a menos que esteja autorizado para usos diferentes de gerenciamento.	Assegura que o daemon SSH esteja configurado somente para atender.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versão 2 Não incluído no perfil da versão 2, incluído na versão 3. **PCI versão 3** 2.3	O daemon SSH deve ser configurado para usar somente cifras aprovadas pelo FIPS 140-2	Assegura que o daemon SSH use somente as cifras FIPS 140-2.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versão 2 Não incluído no perfil da versão 2, incluído na versão 3. **PCI versão 3** 2.3	O daemon SSH deve ser configurado para usar somente Códigos de Autenticação de Mensagem (MACs) que empregam algoritmos hash criptográficos aprovados pelo FIPS 140-2.	Assegura que os MACs estejam executando os algoritmos aprovados.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versão 2 Não incluído no perfil da versão 2, incluído na versão 3. **PCI versão 3** 2.3	O daemon SSH deve restringir a capacidade de login a usuários ou grupos específicos.	Restringe o login no sistema a usuários e grupos específicos.	`/etc/security/pscexpert/bin/sshPCIconfig`

Tabela 7. Configurações relacionadas às normas de conformidade do PCI DSS versão 2.0 e versão 3.0 (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do script que modifica o valor
PCI versão 2 Não incluído no perfil da versão 2, incluído na versão 3. **PCI versão 3** 2.3	O sistema deve exibir a data e hora do último login de conta bem-sucedido após o login.	Mantém as informações do último login bem-sucedido e as exibe após o próximo login bem-sucedido.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versão 2 Não incluído no perfil da versão 2, incluído na versão 3. **PCI versão 3** 2.3	O daemon SSH deve concluir a verificação de modo estrito dos arquivos de configuração do diretório inicial.	Assegura que os arquivos de configuração do diretório inicial estejam configuradas para os modos corretos.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versão 2 Não incluído no perfil da versão 2, incluído na versão 3. **PCI versão 3** 2.3	O daemon SSH deve usar a separação de privilégio.	Assegura que o daemon SSH tenha a quantia correta de separação de seus privilégios.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versão 2 Não incluído no perfil da versão 2, incluído na versão 3. **PCI versão 3** 2.3	O daemon SSH não deve permitir que rhosts tenham autenticação RSA.	Desativa a autenticação RSA para rhosts quando você está usando o daemon SSH.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versão 2 Não incluído no perfil da versão 2, incluído na versão 3. **PCI versão 3** 2.3	Restrinja o número máximo de sessões de login para 2 por usuário.	Configura o número máximo de sessões de login para 2 por usuário.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versão 2 1.1.5 2.2.2 **PCI versão 3** 10.4	Examine os padrões e processos de configuração para verificar se a tecnologia de sincronização de tempo é implementada e mantida atual conforme o PCI DSS Requirements 6.1 e 6.2.	Ativa o daemon ntp.	`/etc/security/pscexpert/bin/rctcpip`

Tabela 7. Configurações relacionadas às normas de conformidade do PCI DSS versão 2.0 e versão 3.0 (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do script que modifica o valor
PCI versão 2 Não incluído no perfil da versão 2, incluído na versão 3. **PCI versão 3** 8.1.5	Desative uma conta do usuário quando não estiver em uso.	Desativa as contas do usuário após 35 dias de inatividade.	`/etc/security/pscexpert/bin/disableacctpci`
PCI versão 2 Não incluído no perfil da versão 2, incluído na versão 3. **PCI versão 3** 8.2	Restrinja o número máximo de sessões de login para 2 por usuário.	Configura o número máximo de sessões ativas para o conjunto de usuários para 2, configurando o parâmetro **`maxulogs`** para um valor de 2.	`/etc/security/pscexpert/bin/chusrattr`

Conformidade de Lei Sarbanes Oxley e COBIT

A Lei Sarbanes-Oxley (SOX) de 2002 com base no 107⌂ congresso dos Estados Unidos da América supervisiona a auditoria de empresas públicas sujeitas às leis de segurança e questões relacionadas, para proteger os interesses dos investidores.

O SOX Seção 404 instrui a avaliação de gerenciamento sobre controles internos. Para a maioria das organizações, os controles internos abrangem os sistemas de tecnologia da informação, que processam e relatam os dados financeiros da empresa. A Lei SOX fornece detalhes específicos sobre TI e segurança de TI. Muitos auditores SOX se baseiam em padrões, como COBIT como um método para medir e auditar o controle de TI adequado. A opção de configuração XML SOX/COBIT do PowerSC Standard Edition fornece a configuração de segurança do AIX e Virtual I/O Server (sistemas VIOS necessários para atender às diretrizes de conformidade de COBIT.

O IBM Compliance Expert Express Edition é executado na versão a seguir do sistema operacional AIX:

- AIX 6.1
- AIX 7.1
- AIX 7.2

A conformidade com normas externas é uma responsabilidade de uma carga de trabalho do administrador de sistema AIX. O IBM Compliance Expert Express Edition é projetado para simplificar o gerenciamento de configurações do sistema operacional e os relatórios necessários para conformidades padrão.

Os perfis de conformidade pré-configurados entregues com o IBM Compliance Expert Express Edition reduzem a carga de trabalho administrativa de interpretar a documentação de conformidade e implementar essas normas, conforme parâmetros de configuração do sistema específico.

Os recursos do IBM Compliance Expert Express Edition são projetados para ajudar os clientes a gerenciar efetivamente os requisitos do sistema, que são associados à conformidade padrão externa que pode reduzir potencialmente os custos ao melhorar a conformidade. Todos os padrões de segurança externos incluem outros aspectos do que as definições de configuração do sistema. O uso do IBM Compliance Expert Express Edition não pode assegurar as conformidades padrão. O Expert Compliance foi projetado

para simplificar o gerenciamento de definição de configuração dos sistemas que ajuda os administradores a focar em outros aspectos de conformidades padrão.

Informações relacionadas:

Conformidade de COBIT

Health Insurance Portability and Accountability Act (HIPAA)

A Health Insurance Portability and Accountability Act (HIPAA) é um perfil de segurança que focaliza na proteção de Electronically Protected Health Information (EPHI).

A Regra de Segurança HIPAA focaliza especificamente na defesa de EPHI e apenas um subconjunto de agências estão sujeitas à Regra de Segurança HIPAA com base em suas funções e uso de EPHI.

Todas as entidades cobertas pela HIPAA, semelhantes a algumas das agências federais, devem estar em conformidade com as regras de Segurança HIPAA.

A Regra de Segurança HIPAA foca na proteção da confidencialidade, da integridade e da disponibilidade de EPHI, conforme definido na Regra de Segurança.

O EPHI que uma entidade coberta cria, recebe, mantém ou transmite deve ser protegido com relação a ameaças razoavelmente antecipadas, riscos e usos e divulgações inadmissíveis.

Os requisitos, padrões e especificações de implementação da Regra de Segurança HIPAA aplicam-se às entidades cobertas a seguir:

- Provedores de assistência médica
- Planos de saúde
- clearinghouses de assistência médica
- Patrocinadores de cartão de medicamento e de receitas da Medicare

Os detalhes da tabela a seguir sobre várias seções da Regra de Segurança HIPAA e cada seção inclui várias normas e especificações de implementação.

Nota: Todos os arquivos de script customizados fornecidos para manter a conformidade de HIPAA estão no diretório `/etc/security/pscexpert/bin`.

Tabela 8. Detalhes de Regras e Implementação de HIPAA

Seções de Regras de Segurança de HIPAA	Especificação de implementação	A implementação do aixpert	Comandos e valores de retorno
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 164.312 (b)	Implementa os procedimentos para revisar regularmente os registros da atividade do sistema de informações, como logs de auditoria, relatórios de acesso e relatórios de incidente de segurança.	Determina se a auditoria está ativada no sistema.	**Comando**: **#audit query**. **Valor de retorno**: se bem-sucedido, esse comando sairá com um valor de 0. Se malsucedido, o comando sairá com um valor de 1.

Tabela 8. Detalhes de Regras e Implementação de HIPAA (continuação)

Seções de Regras de Segurança de HIPAA	Especificação de implementação	A implementação do aixpert	Comandos e valores de retorno
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 166.312 (b)	Implementa os procedimentos para revisar regularmente os registros da atividade do sistema de informações, como logs de auditoria, relatórios de acesso e relatórios de incidente de segurança.	Ativa a auditoria no sistema. Além disso, configura os eventos a serem capturados.	**Comando**: **# audit start >/dev/null 2>&1**. **Valor de retorno**: se bem-sucedido, esse comando sairá com um valor de 0. Se malsucedido, o comando sairá com um valor de 1. Os eventos a seguir são auditados: **FILE_Mknod, FILE_Open, FS_Mkdir, PROC_Execute, DEV_Create, FILE_Acl, FILE_Chpriv, FILE_Fchpriv, FILE_Mode, INIT_Start, PASSWORD_Change, PASSWORD_Check, PROC_Adjtime, PROC_Kill, PROC_Privilege, PROC_Setpgid, USER_SU, USER_Change, USER_Create, USER_Login, USER_Logout, USER_Reboot, USER_Remove, USER_SetEnv, USER_SU, FILE_Acl,FILE_Fchmod,FILE_Fchown**
164.312 (a) (2) (iV)	Criptografia e Decriptografia (A):Implementa um mecanismo para criptografar e decriptografar o EPHI.	Determina se o Sistema de Arquivos com Criptografia (EFS) está ativado no sistema.	**Comando**: **# efskeymgr -V >/dev/null 2>&1**. **Valor de retorno**: Se EFS já estiver ativado, esse comando sairá com um valor de 0. Se EFS não estiver ativado, esse comando sairá com um valor de 1.
164.312 (a) (2) (iii)	Logoff Automático (A): Implementa os processos eletrônicos para encerrar uma sessão eletrônica após um intervalo predefinido de inatividade.	Configura o sistema para efetuar logout de processos interativos após 15 minutes minutos de inatividade.	**Comando**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1** **echo "TMOUT=900 ; TIMEOUT=900; export TMOUT TIMEOUT**. **Valor de retorno**: Se o comando falhar ao localizar o valor **TMOUT=15**, o script sairá com um valor de 1. Caso contrário, o comando sairá com um valor de 0.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Assegura que todas as senhas contenham um mínimo de 14 caracteres.	**Comando**: **chsec -f /etc/security/user -s user -a minlen=8**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o script sairá com um código de erro de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Assegura que todas as senhas incluam pelo menos dois caracteres alfabéticos, um dos quais deve ser alterado para letras maiúsculas.	**Comando**: **chsec -f /etc/security/user -s user –a minalpha=4**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o comando sairá com um código de erro de 1.

Tabela 8. Detalhes de Regras e Implementação de HIPAA (continuação)

Seções de Regras de Segurança de HIPAA	Especificação de implementação	A implementação do aixpert	Comandos e valores de retorno
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Especifica o número mínimo de caracteres não alfabéticos em uma senha como 2.	**Comando**: **#chsec –f /etc/security/user –s user –a minother=2**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o comando sairá com um código de erro de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Assegure-se de que todas as senhas não contenham nenhum caractere repetitivo.	**Comando**: **#chsec –f /etc/security/user –s user –a maxrepeats=1**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o comando sairá com um código de erro de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Assegure-se de que uma senha não seja reutilizada dentro das últimas cinco mudanças.	**Comando**: **#chsec –f /etc/security/user –s user –a histsize=5**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o comando sairá com um código de erro de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Especifica o número máximo de semanas como 13 semanas, para que a senha permaneça válida.	**Comando**: **#chsec –f /etc/security/user –s user –a maxage=8**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o comando sairá com um código de erro de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Remove qualquer número mínimo de requisitos da semana antes que uma senha possa ser alterada.	**Comando**: **#chsec –f /etc/security/user –s user –a minage=2**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o comando sairá com um código de erro de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Especifica o número máximo de semanas como 4 semanas, para alterar uma senha expirada, após o valor do parâmetro **maxage** configurado pelo usuário expirar.	**Comando**: **#chsec –f /etc/security/user –s user –a maxexpired=4**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o comando sairá com um código de erro de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Especifica que o número mínimo de caracteres que não podem ser repetidos da senha antiga é de 4 caracteres.	**Comando**: **#chsec –f /etc/security/user –s user –a mindiff=4**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o comando sairá com um código de erro de 1.

Tabela 8. Detalhes de Regras e Implementação de HIPAA (continuação)

Seções de Regras de Segurança de HIPAA	Especificação de implementação	A implementação do aixpert	Comandos e valores de retorno
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Especifica que o número de dias é 5 a ser aguardado antes que o sistema emita um aviso que uma mudança de senha é necessária.	**Comando**: **#chsec –f /etc/security/user –s user –a pwdwarntime = 5**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o comando sairá com um código de erro de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Verifica a exatidão de definições do usuário e corrige os erros.	**Comando**: **/usr/bin/usrck -y ALL** **/usr/bin/usrck –n ALL**. **Valor de retorno**: O comando não retorna um valor. O comando verifica e corrige os erros, se houver.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Bloqueia a conta após três tentativas de login consecutivas com falha.	**Comando**: **#chsec –f /etc/security/user –s user –a loginretries=3**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o comando sairá com um código de erro de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Especifica o atraso entre um login sem sucesso para o outro como 5 segundos.	**Comando**: **chsec -f /etc/security/login.cfg -s default -a logindelay=5**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o comando sairá com um código de erro de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Especifica o número de tentativas de login sem sucesso em uma porta, antes que a porta seja bloqueada como 10.	**Comando**: **chsec -f /etc/security/lastlog -s username -a \ unsuccessful_login_count=10**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o comando sairá com um código de erro de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Especifica o intervalo de tempo em uma porta para as tentativas de login sem sucesso antes que a porta seja desativada como 60 segundos.	**Comando**: **#chsec -f /etc/security/lastlog -s user –a time_last_unsuccessful_login=60**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o comando sairá com um código de erro de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Especifica o intervalo de tempo após o qual uma porta é desbloqueada e após ser desativada, como 30 minutos.	**Comando**: **#chsec -f /etc/security/login.cfg -s default -a loginreenable = 30**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o comando sairá com um código de erro de 1.

Tabela 8. Detalhes de Regras e Implementação de HIPAA (continuação)

Seções de Regras de Segurança de HIPAA	Especificação de implementação	A implementação do aixpert	Comandos e valores de retorno
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Especifica o intervalo de tempo para digitar uma senha como 30 segundos.	**Comando**: **chsec -f /etc/security/login.cfg -s usw -a logintimeout=30**. **Valor de retorno**: se bem-sucedido, esse script sairá com um valor de 0. Se malsucedido, o comando sairá com um código de erro de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gerenciamento de Senha (A):Implementa os procedimentos para criar, alterar e proteger senhas.	Assegure-se de que as contas sejam bloqueadas após 35 dias de inatividade.	**Comando**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1if TMOUT = (35x24x60x60){#chsec -f /etc/security/user -s user -aaccount_locked = true}**. **Valor de retorno**: Se o comando falhar ao configurar o valor de **account_locked** como **true**, o script sairá com um valor de 1. Caso contrário, o comando sairá com um valor de 0.
164.312 (c) (1)	Implementa as políticas e procedimentos para proteger o EPHI de alteração ou destruição incorreta.	Configure políticas de Execução Confiável (TE) como ON.	**Comando**: Ativa **CHKEXEC, CHKSHLIB, CHKSCRIPT, CHKKERNEXT, STOP_ON_CHKFAIL,TE=ON Por exemplo, trustchk –p TE=ON CHKEXEC = ON, CHKSHLIB,=ON, CHKSCRIPT=ON, CHKKERNEXT = ON**. **Valor de retorno**: Na falha, o script sai com um valor de 1.
164.312 (e) (1)	Implementa as medidas técnicas de segurança para evitar o acesso não autorizado à EPHI que está sendo transmitido em uma rede de comunicação eletrônica.	Determina se os conjuntos de arquivos **ssh** serão instalados. Se não, exibirá uma mensagem de erro.	**Comando**: **# lslpp –l | grep openssh > /dev/null 2>&1**. **Valor de retorno**: Se o código de retorno para esse comando for 0, o script sairá com um valor de 0. Se os conjuntos de arquivos ssh não estiverem instalados, o script sairá com um valos de 1 e exibirá a mensagem de erro `Instalar conjuntos de arquivos ssh para a transmissão segura`.

Os detalhes da tabela a seguir sobre várias funções da Regra de Segurança HIPAA e cada função inclui vários padrões e especificações de implementação.

Tabela 9. Detalhes de Funções e Implementação de HIPAA

Funções de HIPAA	Especificação de implementação	A implementação do aixpert	Comandos e valores de retorno
Criação de log de erro	Consolida erros de logs diferentes e envia emails para o administrador.	Determina se os erros de hardware existem. Determina se há erros irrecuperáveis a partir do arquivo **trcfile** no local, `/var/adm/ras/trcfile`. Envia os erros para **root@<hostname>**.	**Comando**: **errpt -d H**. **Valor de retorno**: se bem-sucedido, esse comando sairá com um valor de 0. Se malsucedido, o comando sairá com um valor de 1.

Tabela 9. Detalhes de Funções e Implementação de HIPAA (continuação)

Funções de HIPAA	Especificação de implementação	A implementação do aixpert	Comandos e valores de retorno
Ativação de FPM	Altera permissões de arquivo.	Altera a permissão de arquivos a partir de uma lista de permissões e arquivos usando o comando **fpm**.	**Comando**: **# fpm -1 <level> -f <commands file>**. **Valor de retorno**: se bem-sucedido, esse comando sairá com um valor de 0. Se malsucedido, o comando sairá com um valor de 1.
Ativação de RBAC	Cria os usuários **isso**, **so** e **sa** e designa as funções apropriadas aos usuários.	Sugere que você crie os usuários **isso**, **so** e **sa**. Designa funções apropriadas aos usuários.	**Comando**: **/etc/security/pscexpert/bin/RbacEnablement**.

Conformidade da North American Electric Reliability Corporation

A North American Electric Reliability Corporation (NERC) é uma corporação sem fins lucrativos que desenvolve a norma para a indústria de sistemas de energia elétrica. O PowerSC Standard Edition contém um perfil NERC pré-configurado, que fornece normas de segurança que podem ser usadas para proteger sistemas de energia elétrica críticos.

O perfil NERC segue as normas de Critical Infrastructure Protection (CIP).

O perfil NERC está localizado em `/etc/security/aixpert/custom/NERC.xml`. É possível reconfigurar os requisitos de CIP que são aplicados ao perfil NERC para o estado padrão, aplicando o perfil NERC_to_AIXDefault.xml que está localizado no diretório `/etc/security/aixpert/custom`. Esse processo não é o mesmo que a operação desfazer do perfil NERC.

A tabela a seguir fornece informações sobre as normas de CIP que são aplicadas ao sistema operacional AIX e como o PowerSC Standard Edition manipula as normas de CIP:

Tabela 10. Normas de CIP para o PowerSC Standard Edition

Norma de CIP	Implementação do AIX Security Expert	Local do script que modifica o valor
CIP-003-3 R5.1	Configure os parâmetros de segurança do sistema para evitar problemas, removendo os atributos set-user identification (SUID) e set-group identification (SGID) dos arquivos binários.	• `/etc/security/pscexpert/bin/filepermgr` • `/etc/security/pscexpert/bin/rmsuidfrmrcmds`
CIP-003-3 R5.1.1	Permite o controle de acesso baseado na função (RBAC) criando as funções de operador do sistema, administrador do sistema e responsável pela segurança do sistema de informações com as permissões necessárias.	`/etc/security/pscexpert/bin/EnableRbac`
CIP-005-3a R2.1-R2.4	Ativa o shell seguro (SSH) para acesso de segurança.	`/etc/security/pscexpert/bin/sshstart`
CIP-005-3a R2.5	Desativa os serviços não necessários e não seguros a seguir: • Daemon **lpd** • Common Desktop Environment (CDE)	`/etc/security/pscexpert/bin/comntrows`

Tabela 10. Normas de CIP para o PowerSC Standard Edition (continuação)

Norma de CIP	Implementação do AIX Security Expert	Local do script que modifica o valor
CIP-005-3a R2.5	Desativa os serviços não necessários e não seguros a seguir: • Daemon **timed** • Daemon **NTP** • Daemon **rwhod** • Daemon **DPID2** • Agente DHCP	`/etc/security/pscexpert/bin/rctcpip`
CIP-005-3a R2.5	Desativa os serviços não necessários e não seguros a seguir: • Daemon **comsat** • Daemon **dtspcd** • Daemon **fingerd** • Daemon **ftpd** • Daemon **rshd** • Daemon **rlogind** • Daemon **rexecd** • Daemon **systat** • Daemon **tfptd** • Daemon **talkd** • Daemon **rquotad** • Daemon **rstatd** • Daemon **rusersd** • Daemon **rwalld** • Daemon **sprayd** • Daemon **pcnfsd** • Daemon **telnet** • Serviço cmsd • Serviço ttdbserver • Serviço TCP echo • Serviço TCP discard • Serviço TCP chargen • Serviço TCP daytime • Serviço TCP time • Serviço UDP echo • Serviço UDP discard • Serviço UDP chargen • Serviço UDP daytime • Serviço UDP time	`/etc/security/pscexpert/bin/cominetdconf`
CIP-005-3a R2.5	Impinge a solicitação de negação de serviço para portas de mitigação.	`/etc/security/pscexpert/bin/tcptr_aixpert`
CIP-005-3a R3 CIP-007-3a R5, R6.5	Ativa a auditoria dos arquivos binários no sistema.	`/etc/security/pscexpert/bin/pciaudit`
CIP-005-3a R3	Atualiza o arquivo de configuração de auditoria com usuários, funções e eventos recém-criados.	`/etc/security/pscexpert/bin/auditconfig`
CIP-007-3a R3	Exibe uma mensagem para ativar o Trusted Network Connect (TNC).	`/etc/security/pscexpert/bin/GeneralMsg`
CIP-007-3a R4	Mantém a integridade do sistema detectando, removendo e a protegendo com relação aos tipos conhecidos de software malicioso.	`/etc/security/pscexpert/bin/manageITsecurity`

Tabela 10. Normas de CIP para o PowerSC Standard Edition (continuação)

Norma de CIP	Implementação do AIX Security Expert	Local do script que modifica o valor
CIP-007-3a R5.2.1	Permite que a senha seja mudada no primeiro login para todas as contas de usuários padrão que não estiverem bloqueadas.	`/etc/security/pscexpert/bin/pwdchg`
CIP-007-3a R5.2.2-R5.2.3	Bloqueia todas as contas de usuário padrão.	`/etc/security/pscexpert/dodv2/ lockacc_rlogin`
CIP-007-3a R5.3.1	Configura cada senha para um mínimo de 6 caracteres.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-3a R5.3.2	Configura cada senha para uma combinação de caracteres alfabéticos, numéricos e especiais.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-3a R5.3.3	Muda cada senha anualmente.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-3a R7	Exibe uma mensagem para ativar o Sistema de Arquivos com Criptografia (EFS).	`/etc/security/pscexpert/bin/GeneralMsg`
CIP-010-1	Exibe uma mensagem para ativar o Real Time Compliance (RTC).	`/etc/security/pscexpert/bin/GeneralMsg`

A lista a seguir exibe informações sobre as normas de CIP que são aplicadas ao sistema operacional AIX:

Norma CIP–003–3 — Segurança cibernética — Controles de gerenciamento da segurança

R5. Controle de acesso

A Entidade Responsável documenta e implementa um programa para gerenciar o acesso a informações protegidas do Critical Cyber Asset (CCA).

- **R5.1:** A Entidade Responsável mantém uma lista da equipe designada que é responsável por autorizar o acesso lógico ou físico a informações protegidas.
- **R5.1.1:** A equipe é identificada pelo nome, título e as informações pelas quais ela é responsável por autorizar o acesso.

Norma CIP–005–3a — Segurança cibernética — Perímetros de segurança eletrônica

R2. Controles de acesso eletrônico

A Entidade Responsável implementa e documenta os processos organizacionais e mecanismos técnicos e processuais para controle de acesso eletrônico em todos os pontos de acesso eletrônico para os Perímetros de Segurança Eletrônica.

- **R2.1:** esses processos e mecanismos usam um modelo de controle de acesso que nega o acesso por padrão, de modo que as permissões de acesso explícito devem se especificadas
- **R2.2:** em todos os pontos de acesso ao(s) Perímetro(s) de Segurança Eletrônica, a Entidade Responsável ativa somente portas e serviços que são necessários para operações e para monitoramento de Ativos Cibernéticos no Perímetro de Segurança Eletrônica e documenta, individualmente ou por agrupamento especificado, a configuração de tais portas e serviços.
- **R2.3:** a Entidade Responsável implementa e mantém um procedimento para assegurar o acesso de discagem aos Perímetros de Segurança Eletrônica.
- **R2.4:** onde o acesso interativo externo para o Perímetro de Segurança Eletrônica está ativado, a Entidade Responsável implementa controles processuais e técnicos fortes nos pontos de acesso para assegurar a autenticidade da parte de acesso, onde tecnicamente factível.
- **R2.5:** a documentação necessária, no mínimo, identifica e descreve o seguinte:
  - **R2.5.1:** os processos para solicitação e autorização de acesso.
  - **R2.5.2:** os métodos de autenticação.

– **R2.5.3:** o processo de revisão para direitos de autorização, de acordo com a Norma CIP-004-3 Requisito R4.

– **R2.5.4:** os controles que são usados para assegurar conexões acessíveis por discagem.

R3. Acesso eletrônico de monitoramento

A Entidade Responsável implementa e documenta um processo eletrônico ou manual para acesso de monitoramento e criação de log em pontos de acesso para os Perímetros de Segurança Eletrônica, vinte e quatro horas por dia, sete dias por semana.

- **R3.1:** para Ativos Cibernéticos Críticos acessíveis por discagem que usam protocolos não roteáveis, a Entidade Responsável implementa e documenta os processos de monitoramento em cada ponto de acesso para o dispositivo de discagem, onde tecnicamente factível.
- **R3.2:** onde tecnicamente factível, os processos de monitoramento de segurança detectam e alertam para tentativas de, ou reais, acessos não autorizados. Esses alertas fornecem notificação apropriada para a equipe de resposta designada. Onde o alerta não é tecnicamente factível, a Entidade Responsável revisa ou obtém logs de acesso para tentativas de, ou reais, acessos não autorizados pelo menos a cada 90 dias.

Norma CIP–007–3a — Segurança cibernética — Gerenciamento da segurança do sistema

R2. Portas e serviços

A Entidade Responsável estabelece, documenta e implementa um processo para assegurar que somente as portas e os serviços necessários para operações normais e emergenciais sejam ativados.

- **R2.1:** a Entidade Responsável ativa somente as portas e os serviços necessários para operações normais e emergenciais.
- **R2.2:** a Entidade Responsável desativa outros serviços e portas, incluindo portas que são usadas para propósitos de teste, antes do uso de produção de todos os Ativos Cibernéticos dentro dos Perímetros de Segurança Eletrônica.
- **R2.3:** no caso onde as portas não usadas e os serviços não podem ser desativados devido a limitações técnicas, a Entidade Responsável documenta as medidas de compensação que são aplicadas para minimizar a exposição ao risco.

R3. Gerenciamento de correção de segurança

A Entidade Responsável, separadamente ou como um componente do processo de gerenciamento de configuração documentado que é especificado no CIP-003-3 Requisito R6, estabelece, documenta e implementa um programa de gerenciamento de correção de segurança para controlar, avaliar, testar e instalar correções de software de segurança cibernética aplicáveis para todos os Ativos Cibernéticos dentro dos Perímetros de Segurança Eletrônica.

- **R3.1:** a Entidade Responsável documenta a avaliação de correções de segurança e upgrades de segurança para aplicabilidade dentro de 30 dias de disponibilidade das correções ou dos upgrades.
- **R3.2:** a Entidade Responsável documenta a implementação de correções de segurança. Em qualquer caso em que a correção não for instalada, a Entidade Responsável documenta as medidas de compensação que são aplicadas para minimizar a exposição ao risco.

R4. Prevenção de software malicioso

A Entidade Responsável usa o software antivírus e outras ferramentas de prevenção de software malicioso (malware), onde tecnicamente viável, para detectar, evitar, impedir e minimizar a introdução, exposição e propagação de malware em todos os Ativos Cibernéticos dentro dos Perímetros de Segurança Eletrônica.

- **R4.1:** a Entidade Responsável documenta e implementa o antivírus e as ferramentas de prevenção de malware. No caso em que o software antivírus e as ferramentas de

prevenção de malware não forem instaladas, a Entidade Responsável documenta as medidas de compensação que são aplicadas para minimizar a exposição ao risco.

- **R4.2:** a Entidade Responsável documenta e implementa um processo para a atualização de assinaturas do antivírus e da prevenção de malware. O processo deve direcionar o teste e a instalação das assinaturas.

R5. Gerenciamento de conta

A Entidade Responsável estabelece, implementa e documenta controles técnicos e processuais que impingem a autenticação de acesso de, e a prestação de contas para, toda a atividade do usuário e que minimizam o risco de acesso de sistema desautorizado.

- **R5.1:** a Entidade Responsável verifica se as contas do sistema individuais e compartilhadas e as permissões de acesso autorizado são consistentes com o conceito de `necessidade de conhecimento` sobre funções de trabalho que são executadas.
  - **R5.1.1:** a Entidade Responsável revisa, pelo menos anualmente, as contas do usuário para verificar se os privilégios de acesso estão de acordo com a Norma CIP-003-3.
  - **R5.1.2:** a Entidade Responsável estabelece métodos, processos e procedimentos que geram logs de detalhe suficiente para criar trilhas de auditoria históricas de atividade de acesso da conta do usuário individual para um mínimo de 90 dias.
  - **R5.1.3:** a Entidade Responsável revisa, pelo menos anualmente, as contas do usuário para verificar se os privilégios de acesso estão de acordo com a Norma CIP-003-3.
- **R5.2:** a Entidade Responsável implementa uma política para minimizar e gerenciar o escopo e o uso aceitável de privilégios de conta de administrador, compartilhados e outros genéricos que incluam contas padrão de fábrica.
  - **R5.2.1:** a política inclui a remoção, desativação ou renomeação dessas contas onde possível. Para as contas que devem permanecer ativadas, as senhas devem ser mudadas antes de colocar qualquer sistema em serviço.
  - **R5.2.2:** a Entidade Responsável identifica os indivíduos com acesso a contas compartilhadas.
  - **R5.2.3:** onde tais contas devem ser compartilhadas, a Entidade Responsável possui uma política para gerenciar o uso dessas contas que limita o acesso somente aos usuários com autorização, uma trilha de auditoria do uso da conta (automatizada ou manual) e etapas para assegurar a conta se a equipe mudar (por exemplo, mudança em designação ou rescisão).
- **R5.3:** no mínimo, a Entidade Responsável é necessária para usar senhas, sujeitas ao seguinte, quando tecnicamente factível:
  - **R5.3.1:** cada senha deve ser no mínimo 6 caracteres.
  - **R5.3.2:** cada senha deve consistir em uma combinação de caracteres alfabéticos, numéricos e especiais.
  - **R5.3.3:** cada senha deve ser mudada pelo menos anualmente, ou mais frequentemente com base no risco.

R6. Monitoramento de status de segurança

A Entidade Responsável assegura que todos os Ativos Cibernéticos dentro do Perímetro de Segurança Eletrônica, quando tecnicamente factível, implementem ferramentas automatizadas ou controles de processos organizacionais para monitorar eventos do sistema que estão relacionados à segurança cibernética.

- **R6.1:** a Entidade Responsável implementa e documenta os processos organizacionais e os mecanismos técnicos e processuais de monitoramento para eventos de segurança em todos os Ativos Cibernéticos dentro do Perímetro de Segurança Eletrônica.
- **R6.2:** os controles de monitoramento de segurança emitem alertas automatizados ou manuais para incidentes de segurança cibernética detectados.

- **R6.3:** a Entidade Responsável mantém logs de eventos do sistema que estão relacionados à segurança cibernética, onde tecnicamente factível, para suportar a resposta do incidente conforme requerido na Norma CIP-008-3.
- **R6.4:** a Entidade Responsável retém todos os logs que são especificados no Requisito R6 para 90 dias.
- **R6.5:** a Entidade Responsável revisa os logs de eventos do sistema que estão relacionados à segurança cibernética e mantém os registros que documentam a revisão dos logs.

R7. Descarte ou reimplementação

A Entidade Responsável estabelece e implementa métodos, processos e procedimento formais para descarte ou reimplementação de Ativos Cibernéticos dentro do(s) Perímetro(s) de Segurança Eletrônica conforme identificado e documentado na Norma CIP-005-3.

- **R7.1:** antes do descarte de tais ativos, a Entidade Responsável destrói e apaga a mídia de armazenamento de dados para evitar a recuperação desautorizada de dados sensíveis de segurança cibernética ou confiabilidade.
- **R7.2:** Antes da implementação de tais ativos, a Entidade Responsável, no mínimo, apaga a mídia de armazenamento de dados para evitar a recuperação desautorizada de dados sensíveis de segurança cibernética ou confiabilidade.

CIP–010–1 — Segurança cibernética — Avaliações de gerenciamento e vulnerabilidade de mudanças na configuração

R1: a Entidade Responsável implementa, de uma maneira que identifica, avalia e corrige as deficiências, um ou mais processos documentados que incluem coletivamente cada uma das partes de requisito aplicáveis.

Gerenciando Security and Compliance Automation

Aprenda sobre o processo de planejamento e implementação de perfis do PowerSC Security and Compliance Automation em um grupo de sistemas, de acordo com os procedimentos de controle e conformidade de TI aceitos.

Como parte da conformidade e controle de TI, os sistemas que executam classes de dados de carga de trabalho e de segurança semelhantes devem ser gerenciados e configurados consistentemente. Para planejar e implementar a conformidade em sistemas, conclua as tarefas a seguir:

Identificando os Grupos de Trabalho do Sistema

O estado de diretrizes de conformidade e controle de TI que os sistemas que executam as classes de dados de carga de trabalho e de segurança semelhantes devem ser gerenciados e configurados consistentemente. Portanto, você deve identificar todos os sistemas em um grupo de trabalho semelhante.

Usando um Sistema de Teste de Não Produção para a Configuração Inicial

Aplique perfil de conformidade do PowerSC apropriado no sistema de teste.

Considere os exemplos a seguir para aplicar perfis de conformidade para o sistema operacional AIX.

Exemplo 1: Aplicando `DoD.xml`

```
% aixpert -f /etc/security/aixpert/custom/DoD.xml
Processedrules=38       Passedrules=38  Failedrules=0   Level=AllRules

Input file=/etc/security/aixpert/custom/DoD.xml
```

Neste exemplo, não há nenhuma regra com falha, ou seja, `Failedrules=0`. Isso significa que todas as regras são aplicadas com sucesso e a fase de teste pode ser iniciada. Se houver falhas, a saída detalhada será gerada.

Exemplo 2: Aplicando `PCI.xml` com uma falha

```
# aixpert -f /etc/security/aixpert/custom/PCI.xml
do_action(): rule(pci_grpck) : failed.
Processedrules=85       Passedrules=84  Failedrules=1   Level=AllRules

Input file=/etc/security/aixpert/custom/PCI.xml
```

A falha da regra `pci_grpck` deve ser resolvida. As causas possíveis para a falha incluem os motivos a seguir:

- A regra não se aplica ao ambiente e deve ser removida.
- Há um problema no sistema que deve ser corrigido.

Investigando a Regra com Falha

Na maioria dos casos, não há falha ao aplicar um perfil do PowerSC Security and Compliance. No entanto, o sistema pode ter pré-requisitos relacionados à instalação que estão ausentes ou outros problemas que requerem atenção do administrador.

A causa da falha pode ser investigada usando o exemplo a seguir:

Visualize o arquivo `/etc/security/aixpert/custom/PCI.xml` e localize a regra com falha. Neste exemplo, a regra é `pci_grpck`. Execute o comando **fgrep**, procure a regra com falha `pci_grpck` e veja a regra XML associada.

```
fgrep -p pci_grpck /etc/security/aixpert/custom/PCI.xml
<AIXPertEntry name="pci_grpck" function="grpck"
<AIXPertRuleType type="DLS"/
<AIXPertDescription&gt;Implements portions of PCI Section 8.2,
Verificar definições de grupo: verifica a exatidão de definições de grupo e corrige os erros
</AIXPertDescription
<AIXPertPrereqList&gt;bos.rte.security,bos.rte.date,bos.rte.ILS</AIXPertPrereqList
<AIXPertCommand
/etc/security/aixpert/bin/execmds</AIXPertCommand
<AIXPertArgs
"/usr/sbin/grpck -y ALL; /usr/sbin/grpck -n ALL"</AIXPertArgs
<AIXPertGroup
User Group System and Password Definitions</AIXPertGroup
</AIXPertEntry
```

Na regra `pci_grpck`, o comando `/usr/sbin/grpck` pode ser visto.

Atualizando a Regra com Falha

Ao aplicar um perfil do PowerSC Security and Compliance, é possível detectar erros.

O sistema pode ter os pré-requisitos de instalação ausentes ou outros problemas que requerem atenção do administrador. Após determinar o comando subjacente da regra com falha, examine o sistema para entender o comando de configuração que está falhando. O sistema pode ter um problema de segurança. Também pode ser o caso em que uma regra específica não é aplicável ao ambiente do sistema. Em seguida, um perfil de segurança customizada deve ser criado.

Criando o Perfil de Configuração de Segurança Customizada

Se uma regra não for aplicável ao ambiente específico do sistema, a maioria das organizações de conformidade permitirão exceções documentadas.

Para remover uma regra e para criar uma política de segurança customizada e um arquivo de configuração, conclua as etapas a seguir:

1. Copie o conteúdo dos arquivos a seguir em um único arquivo nomeado /etc/security/aixpert/custom/<*my_security_policy*>.xml:

   /etc/security/aixpert/custom/[PCI.xml|DoD.xml|SOX-COBIT.xml]
2. Edite o arquivo <*my_security_policy*>.xml removendo a regra que não é aplicável da tag XML de abertura <AIXPertEntry name... à tag XML de término </AIXPertEntry.

É possível inserir regras de configuração adicionais para a segurança. Insira as regras adicionais no esquema AIXPertSecurityHardening XML. Não é possível alterar os perfis do PowerSC diretamente, mas é possível customizar os perfis.

Para a maioria dos ambientes, você deve criar uma política XML customizada. Para distribuir um perfil do cliente para outros sistemas, você deve copiar de forma segura a política XML customizada para o sistema que requer a mesma configuração. Um protocolo seguro, como Secure File Transfer Protocol (SFTP), é usado para distribuir uma política XML customizada para outros sistemas e o perfil é armazenado em um local seguro /etc/security/aixpert/custom/<*my_security_policy.xml*>/etc/security/aixpert/custom/

Efetue logon no sistema em que um perfil customizado deve ser criado e execute o comando a seguir:

```
pscxpert –f :  /etc/security/aixpert/custom/<my_security_policy>.xml
```

Testando os Aplicativos com o AIX Profile Manager

As configurações de segurança podem afetar aplicativos e a maneira que o sistema é acessado e gerenciado. É importante testar os aplicativos e os métodos de gerenciamento esperado do sistema antes de implementar o sistema em um ambiente de produção.

As normas de conformidade regulamentar impõem uma configuração de segurança mais rigorosa do que uma configuração pronta para utilização. Para testar o sistema, conclua as etapas a seguir:

1. Selecione **Visualizar e Gerenciar Perfis** na área de janela à direita da página de boas-vindas do AIX Profile Manager.
2. Selecione o perfil usado pelo modelo para implementar nos sistemas a serem monitorados.
3. Clique em **Comparar**.
4. Selecione o grupo gerenciado ou selecione sistemas individuais dentro do grupo e clique em **Incluir** para incluí-los na caixa selecionada.
5. Clique em **OK**.

A operação de comparação é iniciada.

Monitorando Sistemas para Conformidade Contínua com o AIX Profile Manager

As configurações de segurança podem afetar aplicativos e a maneira que o sistema é acessado e gerenciado. Isso é importante para monitorar os aplicativos e os métodos de gerenciamento esperado do sistema ao implementar o sistema em um ambiente de produção.

Para usar o AIX Profile Manager para monitorar um sistema AIX, conclua as etapas a seguir:

1. Selecione **Visualizar e Gerenciar Perfis** na área de janela à direita da página de boas-vindas do AIX Profile Manager.
2. Selecione o perfil usado pelo modelo para implementar nos sistemas a serem monitorados.
3. Clique em **Comparar**.
4. Selecione o grupo gerenciado ou selecione sistemas individuais dentro do grupo e inclua-os na caixa selecionada.

5. Clique em **OK**.

A operação de comparação é iniciada.

Configurando o PowerSC Security and Compliance Automation

Saiba o procedimento para configurar o PowerSC for Security and Compliance Automation a partir da linha de comandos e usando o AIX Profile Manager.

Definindo as Configurações de Opções de Conformidade do PowerSC

Saiba o básico do recurso PowerSC Security and Compliance Automation, teste a configuração em sistemas de teste de não produção e planeje e implemente as configurações. Ao aplicar uma configuração de conformidade, as configurações alterarão as definições de configuração numerosas no sistema operacional.

Nota: Algumas normas de conformidade e perfis desativam a Telnet, porque a Telnet usa senhas não criptografadas. Portanto, você deve ter o Open SSH instalado, configurado e funcionando. É possível usar qualquer outro meio de comunicação segura com o sistema que está sendo configurado. Esses padrões de conformidade requerem o login `root` para ser desativados. Configure um ou mais usuários não raiz antes de continuar aplicando as mudanças na configuração. Esta configuração não desativa a raiz e é possível efetuar login como um usuário não raiz e executar o comando **su** para a raiz. Teste se é possível estabelecer a conexão SSH com o sistema, efetue login como o usuário não raiz e execute o comando para `root`.

Para acessar os perfis de configuração DoD, PCI, SOX ou COBIT, use o diretório a seguir:

- Os perfis no sistema operacional AIX são colocados no diretório `/etc/security/aixpert/custom`.
- Os perfis no Virtual I/O Server (VIOS) são colocados no diretório `/etc/security/aixpert/core`.

Configurando a Conformidade do PowerSC a partir da Linha de Comandos

Implemente ou verifique o perfil de conformidade usando o comando **pscxpert** no sistema AIX e o comando **viosecure** no Virtual I/O Server (VIOS).

Para aplicar os perfis de conformidade do PowerSC em um sistema AIX, insira um dos comandos a seguir, que depende do nível de conformidade de segurança que você deseja aplicar.

Tabela 11. Comandos PowerSC para AIX

Comando	Padrão de conformidade
% pscxpert -f /etc/security/aixpert/custom/DoD.xml	*Guia de Implementação Técnica de Segurança do UNIX do Departamento de Defesa dos Estados Unidos*
% pscxpert -f /etc/security/aixpert/custom/Hipaa.xml	*Heath Insurance Portability and Accountability Act*
% pscxpert -f /etc/security/aixpert/custom/PCI.xml	*Padrão de segurança de dados Payment Card Industry*
% pscxpert -f /etc/security/aixpert/custom/SOX-COBIT.xml	*Lei Sarbanes Oxley de 2002 – Controle de TI COBIT*

Para aplicar os perfis de conformidade do PowerSC em um sistema VIOS, insira um dos comandos a seguir para o nível de conformidade de segurança que você deseja aplicar.

Tabela 12. Comandos PowerSC para o Virtual I/O Server

Comando	Padrão de Conformidade
% viosecure -file /etc/security/aixpert/custom/DoD.xml	*Guia de Implementação Técnica de Segurança do UNIX do Departamento de Defesa dos Estados Unidos*
% viosecure -file /etc/security/aixpert/custom/Hipaa.xml	*Heath Insurance Portability and Accountability Act*
% viosecure -file /etc/security/aixpert/custom/PCI.xml	*Padrão de segurança de dados Payment Card Industry*
% viosecure -file /etc/security/aixpert/custom/SOX-COBIT.xml	*Lei Sarbanes Oxley de 2002 – Controle de TI COBIT*

O comando **pscxpert** no sistema AIX e o comando **viosecure** no VIOS podem demorar para serem executados porque eles estão verificando ou configurando o sistema inteiro e fazendo mudanças na configuração relacionadas à segurança. A saída é semelhante ao exemplo a seguir:

```
Processedrules=38       Passedrules=38  Failedrules=0   Level=AllRules
```

No entanto, algumas regras falham dependendo do ambiente do AIX, de conjunto de instalação, e da configuração anterior.

Por exemplo, uma regra de pré-requisito pode falhar, porque o sistema não possui o conjunto de arquivos de instalação necessários. É necessário entender cada falha e resolvê-la antes de implementar os perfis de conformidade em todo o datacenter.

Conceitos relacionados:

"Gerenciando Security and Compliance Automation" na página 105
Aprenda sobre o processo de planejamento e implementação de perfis do PowerSC Security and Compliance Automation em um grupo de sistemas, de acordo com os procedimentos de controle e conformidade de TI aceitos.

Configurando a Conformidade do PowerSC com o AIX Profile Manager

Saiba o procedimento para configurar os perfis do PowerSC Security and Compliance, e para implementar a configuração em um sistema gerenciado AIX usando o AIX Profile Manager.

Para configurar os perfis do PowerSC Security and Compliance usando o AIX Profile Manager, conclua as etapas a seguir:

1. Efetue login no IBM Systems Director e selecione AIX Profile Manager.
2. Crie um modelo com base em um dos perfis de conformidade e segurança do PowerSC concluindo as etapas a seguir:
   a. Clique em **Visualizar e Gerenciar Modelos** na área de janela à direita da página de boas-vindas do AIX Profile Manager.
   b. Clique em **Criar**.
   c. Clique em **Sistema Operacional** na lista **Tipo de Modelo**.
   d. Forneça um nome para o modelo no campo **Nome de Modelo de Configuração**.
   e. Clique em **Continuar** > **Salvar**.
3. Selecione o perfil a ser usado com o modelo selecionando **Procurar** na opção **Selecionar qual perfil usar para este modelo**. Os perfis exibem os itens a seguir:
   - `ice_DLS.xml` é o nível de segurança padrão do sistema operacional AIX.
   - `ice_DoD.xml` é o Guia de Segurança e Implementação do Departamento de Defesa para configurações do UNIX.
   - `ice_HLS.xml` é uma segurança de alto nível genérico para configurações do AIX.
   - `ice_LLS.xml` é a segurança de baixo nível para configurações do AIX.
   - `ice_MLS.xml` é a segurança de nível médio para configurações do AIX.
   - `ice_PCI.xml` é a configuração de Payment Card Industry para o sistema operacional AIX.

- `ice_SOX.xml` é a configuração SOX ou COBIT as para o sistema operacional AIX.

4. Remova qualquer perfil da caixa de seleção.
5. Selecione **Incluir** para mover o perfil necessário na caixa selecionada.
6. Clique em **Salvar**.

Para implementar a configuração em um sistema gerenciado AIX, conclua as etapas a seguir:

1. Selecione **Visualizar e Gerenciar Modelos** na área de janela a direita da página de boas-vindas do AIX Profile Manager.
2. Selecione o modelo necessário a ser implementado.
3. Clique em **Implementar**.
4. Selecione os sistemas a serem implementados no perfil, e clique em **Incluir** para mover o perfil necessário na caixa selecionada.
5. Clique em **OK** para implementar o modelo de configuração. O sistema está configurado de acordo com o modelo selecionado do perfil.

Para que a implementação seja bem-sucedida para DoD, PCI ou SOX, o PowerSC Standard Edition deve ser instalado no terminal do sistema AIX. Se o sistema que está sendo implementado não tiver o PowerSC instalado, a implementação falhará. O IBM Systems Director implementa o modelo de configuração para o sistema AIX selecionado e os configura de acordo com os requisitos de conformidade.

Informações relacionadas:

AIX Profile Manager

IBM Systems Director

PowerSC Real Time Compliance

O recurso PowerSC Real Time Compliance monitora continuamente sistemas AIX ativados para assegura-se de que sejam configurados continuamente e com segurança.

O recurso PowerSC Real Time Compliance funcionará com as políticas do PowerSC Compliance Automation e do AIX Security Expert para fornecer notificação quando ocorrerem violações de conformidade ou quando um arquivo monitorado for alterado. Quando a política de configuração de segurança de um sistema for violada, o recurso PowerSC Real Time Compliance enviará um email ou uma mensagem de texto para alertar o administrador do sistema.

O recurso PowerSC Real Time Compliance é um recurso de segurança passiva que suporta perfis de conformidade predefinidos ou alterados que incluem o Security Technical Implementation Guide do Departamento de Defesa, o Payment Card Industry Data Security Standard, a Lei Sarbanes-Oxley e a conformidade COBIT. Ele fornece uma lista padrão de arquivos a serem monitorados para mudanças, mas é possível incluir arquivos na lista.

Instalando o PowerSC Real Time Compliance

O recurso PowerSC Real Time Compliance é instalado com o PowerSC Standard Edition versão 1.1.4, ou mais recente, e não faz parte do sistema operacional AIX base.

Para instalar o PowerSC Real Time Compliance, conclua as etapas a seguir:

1. Assegure-se de que você esteja executando um dos sistemas operacionais AIX a seguir no sistema em que você está instalando o recurso PowerSC Real Time Compliance:
   - O IBM AIX 6 com Tecnologia Nível 7 ou posterior, com o AIX Common Event Infrastructure para o AIX e Clusters do AIX (bos.ahafs 6.1.7.0) ou posterior
   - IBM AIX 7 com Tecnologia Nível 1 ou posterior, com o AIX Event Infrastructure para AIX e Clusters do AIX (bos.ahafs 7.1.1.0) ou posterior
   - AIX Versão 7.2, ou mais recente, com o AIX Event Infrastructure for AIX e Clusters do AIX (bos.ahafs 7.2.0.0), ou mais recente
2. Para atualizar ou instalar o conjunto de arquivos do recurso PowerSC Real Time Compliance, instale o conjunto de arquivos `powerscStd.rtc` a partir do pacote de instalação ara o PowerSC Standard Edition versão 1.1.4, ou mais recente.

Configurando o PowerSC Real Time Compliance

Será possível configurar o PowerSC Real Time Compliance para enviar alertas, quando ocorrerem violações de um perfil de conformidade ou mudanças em um arquivo monitorado. Alguns exemplos dos perfis incluem o Security Technical Implementation Guide do Departamento de Defesa, o Payment Card Industry Data Security Standard, a Lei Sarbanes-Oxley e COBIT.

É possível configurar os PowerSC Real Time Compliance usando um dos métodos a seguir:

- Insira o comando **mkrtc**.
- Execute a ferramenta SMIT inserindo o comando a seguir:

  ```
  smit RTC
  ```

Identificando Arquivos Monitorados pelo Recurso PowerSC Real Time Compliance

O recurso PowerSC Real Time Compliance monitora uma lista padrão de arquivos das configurações de segurança de alto nível para mudanças, que pode ser customizado incluindo ou removendo arquivos da lista de arquivos no arquivo `/etc/security/rtc/rtcd_policy.conf`.

Há dois métodos de identificar o modelo de conformidade aplicado em um sistema. Um método é usar o comando **pscxpert** e o outro é usar o AIX Profile Manager com o IBM Systems Director.

Quando o perfil de conformidade for identificado, será possível incluir arquivos adicionais na lista de arquivos a serem monitorados, incluindo os arquivos adicionais no arquivo `/etc/security/rtc/rtcd_policy.conf`. Após o arquivo ser salvo, a nova lista será usada imediatamente como uma linha de base e monitorada para mudanças sem reiniciar o sistema.

Configurando Alertas para PowerSC Real Time Compliance

Você deve configurar a notificação do recurso PowerSC Real Time Compliance, indicando o tipo de alertas e os destinatários dos alertas.

O daemon rtcd, que é o componente principal do recurso PowerSC Real Time Compliance, obtém suas informações sobre os tipos de alertas e os destinatários a partir do arquivo de configuração `/etc/security/rtc/rtcd.conf`. É possível editar esse arquivo para atualizar as informações usando um editor de texto.

Informações relacionadas:

Formato de arquivo /etc/security/rtc/rtcd.conf para Real-Time Compliance

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 117
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 coletar logs de auditoria, desconectar o sistema da rede, desligar o sistema e alertar usuários).
- Havia algum outro sistema comprometido que deveria ser verificado?

Conceitos relacionados:

"Resolvendo Problemas de Inicialização Confiável" na página 117
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 1.1.4" na página 7
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 13. 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.
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.

Tabela 13. Resolução de Problemas de Alguns dos Cenários Comuns para a Falha (continuação)

Motivo para a Falha	Possíveis Causas da Falha	Correção Sugerida
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 114
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 113
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 na página 122, 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.

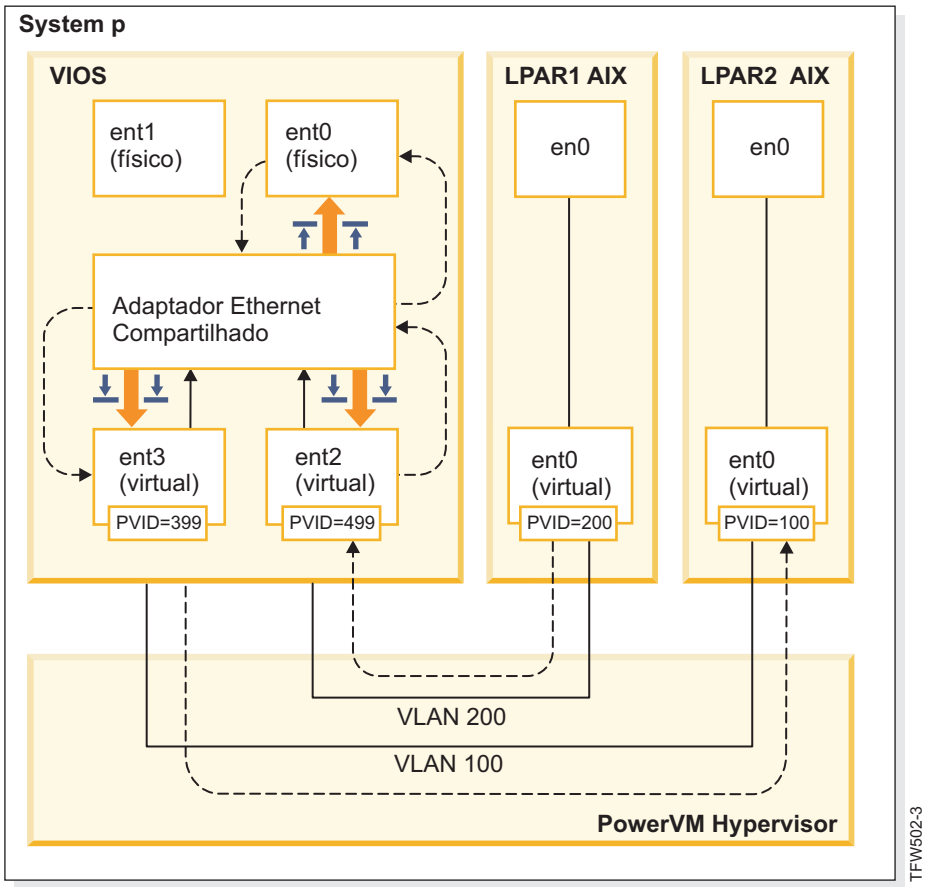

Figura 1. Exemplo de transferência de informações de LAN cruzada sem o Firewall Confiável

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 123.

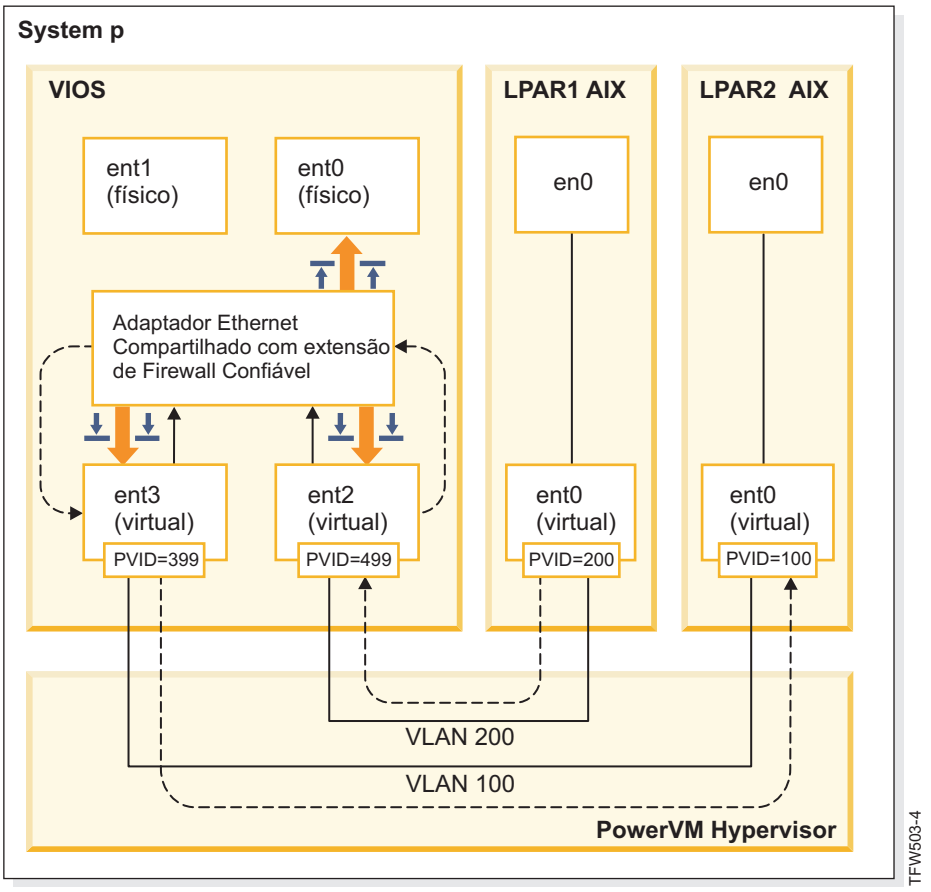

Figura 2. Exemplo de Transferência de Informações de VLAN Cruzada com Firewall Confiável

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 1.1.4" na página 7
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.

Consultor do Trusted Firewall

O Consultor do Trusted Firewall analisa o tráfego do sistema a partir de diferentes partições lógicas (LPARs) para fornecer informações para determinar se a execução do Trusted Firewall melhora o desempenho do sistema.

Se a função Consultor do Trusted Firewall registrar uma quantia significativa de tráfego de diferentes LANs virtuais (VLANs) que estão no mesmo complexo central de eletrônica, a ativação do Trusted Firewall deverá beneficiar seu sistema.

Para ativar o Consultor do Trusted Firewall, insira o comando a seguir:

```
vlantfw -m
```

Para exibir os resultados do Consultor do Trusted Firewall, insira o comando a seguir:

```
vlantfw -D
```

Para desativar o Consultor do Trusted Firewall, 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 Consultor do Trusted Firewall determina que rotear o tráfego internamente melhora a eficiência, a criação de log do Trusted Firewall mantém uma lista de caminhos no arquivo `svm.log`. O tamanho do arquivo `svm.log` é limitado a 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`.

Nota: É possível executar os comandos para iniciar e parar a criação de log do Trusted Firewall somente quando você estiver autenticado como um usuário raiz.

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.

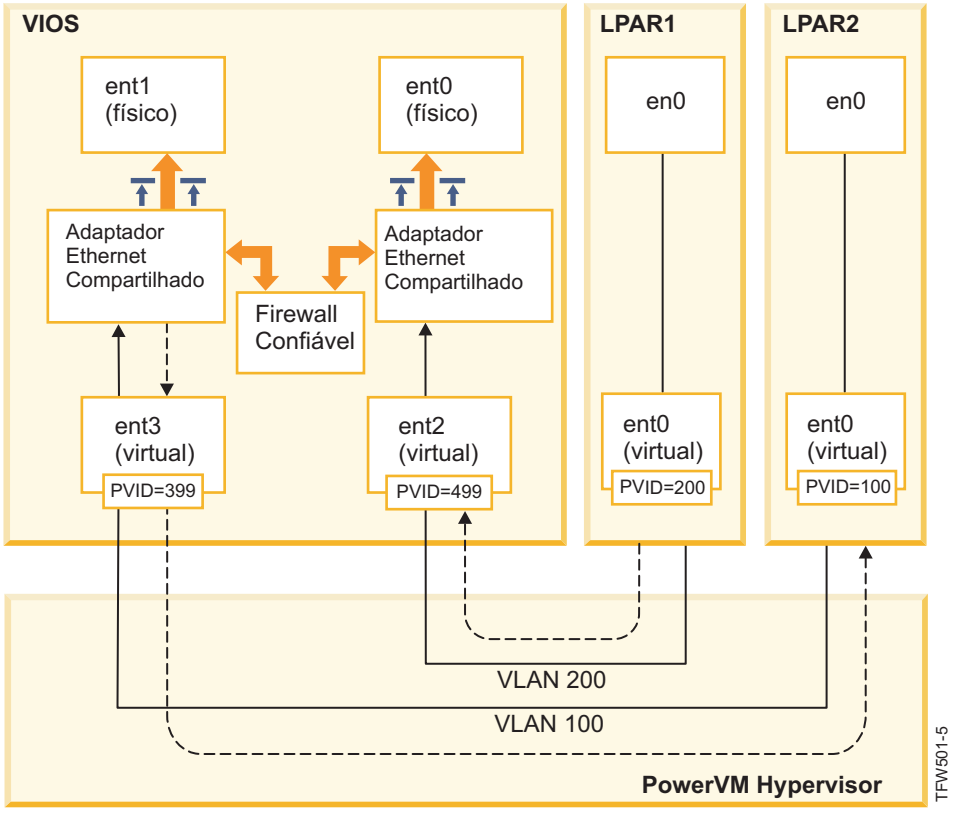

Figura 3. Configuração usando múltiplos Adaptadores Ethernet Compartilhados em um único VIOS

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 146

"Comando mkvfilt" na página 148

"Comando vlantfw" na página 164

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 126
É possível criar regras para ativar o roteamento de VLAN cruzada de Firewall Confiável.

Referências relacionadas:

"Comando lsvfilt" na página 147

"Comando rmvfilt" na página 163

Criação de Log Confiável

O PowerVM Trusted Logging permite que partições lógicas AIX (LPARs) gravem nos arquivos de log que são armazenados em um Virtual I/O Server (VIOS) conectado. 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`.

O Trusted Logging permite que dados do log de vários LPARs clientes sejam consolidados em um único sistema de arquivos, que é acessível a partir do 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 do VIOS para qualquer valor, mas o nome do cliente é geralmente o mesmo para todos os logs virtuais que estão 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 1.1.4” na página 7
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 129.

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 129.

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 152

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 139.
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 152

Informações relacionadas:

"Instalando o PowerSC Standard Edition 1.1.4" na página 7
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 152

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 152

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 152

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 152

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 152

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 152

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 152

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 152

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 152

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 152

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 149

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 152

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 152

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 14. 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.

Tabela 14. Resolução de problemas nas definições de configuração para TNC e sistema de gerenciamento de Correção (continuação)

Problema	**Solução**
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 148

"Comando vlantfw" na página 164

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 127
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 146

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 intervao é um valor de número inteiro que representa minutos ou representa o formato a seguir: **d** (nº de dias): **h** (horas): **m** (minutos). O intervalo suportado para o *download_interval* é de 30 a 525600 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.
-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. O intervalo suportado para o *<ifix interval>* é de 30 a 525600 minutos.

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*>] **[default_policy=**<*yes* | *no* >] **[clientData_interval=**<*time in mins* > | **d** (days) : **h** (hours) : **m**
| (minutes)] **[clientDataPath=**<*Full_path* >]

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

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

psconf chserver attribute = *value*

| **psconf clientData -i** *host* **[-l | -g]**

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**.
clientData	Cria uma captura instantânea de informações (nível do sistema operacional e conjuntos de arquivos instalados) sobre o cliente TNC. O caminho *clientDataPath* identifica onde as informações de coleção de capturas instantâneas estão armazenadas. O local padrão está no diretório `/var/tnc/clientData/` no servidor TNC. É possível mudar ou configurar o caminho *clientDataPath* usando o subcomando **chserver** ou **mkserver**. É possível iniciar a coleção de capturas instantâneas do cliente TNC a partir da linha de comandos executando o subcomando **clientData** no servidor TNC. O subcomando **clientData** executado a partir da linha de comandos é independente do intervalo **clientData_interval**.
clientData_interval	É possível usar o subcomando **chserver** ou **mkserver** para configurar a coleção de capturas instantâneas para ocorrer em intervalos regulares, especificando um valor para o intervalo **clientData_interval**. A coleção de capturas instantâneas inicia automaticamente quando o intervalo **clientData_interval** possui um valor diferente de 0 (zero). Por padrão, a coleção de capturas instantâneas é desativada pelo planejador. Para ativar o planejador, especifique um valor **clientData_interval** que seja maior ou igual a 30. Para desativar o planejador, especifique um valor de **clientData_interval** de 0 (zero). A faixa suportada para o intervalo **clientData_interval** é de 30 a 525600 minutos.
dbpath	Especifica o local do banco de dados TNC. O valor padrão é `/var/tnc`.
default_policy	Ativa ou desativa a verificação automática dos clientes TNC para a correção temporária (ifix) e APARs no mesmo nível que o cliente. Especifique *yes* para ativar a verificação automática. Especifique *no* para desativar a verificação automática. Para obter informações adicionais sobre o subcomando **default_policy**, veja a Tabela default_policy.
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. A faixa suportada para o intervalo **recheck_interval** é de 30 a 525600 minutos. **Nota:** Um valor de **recheck_interval=0** significa que o planejador não inicia a verificação dos clientes em intervalos regulares e os clientes registrados são verificados automaticamente quando iniciam. Nesses casos, o cliente pode ser manualmente verificado.
relatório	Gera um relatório que possui uma extensão de arquivo .txt ou .csv.
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.

Item	Descrição
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.

A tabela a seguir exibe os resultados da configuração do subcomando **default_policy** para os valores *yes* ou *no*:

Tabela 15. Resultados do subcomando default_policy

FSpolicy (política de conjunto de arquivos)	**política padrão=***yes*	**política padrão=***no*
O cliente TNC pertence a uma política de conjunto de arquivos com uma correção temporária (iFix) e grupos de APARs definidos	A política padrão é substituída pelo iFix e APARs fornecidos na política de conjunto de arquivos.	A política padrão não é usada. O iFix e os APARs fornecidos na política de conjunto de arquivos são considerados durante o processo de verificação para o cliente TNC.
O cliente TNC pertence a uma política de conjunto de arquivos sem um iFix e grupos de APARs definidos	A política padrão é usada com o iFix e os APARs durante o processo de verificação para o cliente TNC. Somente o iFix e os APARs que correspondem ao nível do cliente TNC são usados durante o processo de verificação.	A política padrão não é usada.

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 e-mail seguido por uma lista de nomes de grupos 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	Execute o subcomando **clientData** no cliente TNC especificado. Esse sinalizador está disponível somente com o subcomando **clientData**.

Item	Descrição
-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.
-l	Lista os detalhes da captura instantânea no servidor TNC para o cliente TNC especificado. Esse sinalizador está disponível somente com o subcomando **clientData**.
-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.
-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
    ```
18. Para exibir as informações de captura instantânea que foram reunidas com o subcomando **clientData**, insira o comando a seguir:
    ```
    psconf clientData -l [ip|host]
    ```
19. Para exibir o histórico para o cliente TNC, insira o comando a seguir:
    ```
    psconf list –H –i [ip|ALL]
    ```

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 pscxpert

Propósito

Auxilia o administrador do sistema para definir a configuração de segurança.

Sintaxe

pscxpert -l {high | medium | low | default | sox-cobit} **[-p]**

pscxpert -l {h | m | l | d | s} **[-p]**

pscxpert -f Profile **[-p]**

pscxpert -u **[-p]**

pscxpert -c **[-p]** **[-r** | **-R]** **[-P** Profile] **[-l** Level]

pscxpert -t

pscxpert -l <Level> **[-p]** <**-a** *File1* | **-n** *File2* | **-a** *File3* **-n** *File4*>

pscxpert -f Profile **-a** File **[-p]**

pscxpert -d

Descrição

O comando **pscxpert** configura várias definições de configuração do sistema para ativar o nível de segurança especificado.

Executar o comando **pscxpert** apenas com o conjunto de sinalizadores **-l** implementa as configurações de segurança imediatamente sem permitir que o usuário configure as definições. Por exemplo, a execução do comando **pscxpert -l high** aplica todas as configurações de segurança de alto nível no sistema automaticamente. No entanto, a execução do comando **pscxpert -l** com as sinalizações **-n** e **-a** salva as configurações de segurança em um arquivo especificado pelo parâmetro *File*. Em seguida, o sinalizador **-f** aplica as novas configurações.

Após a seleção inicial, um menu é exibido detalhando em itens de todas as opções de configuração de segurança que estão associadas ao nível de segurança selecionado. Essas opções podem ser aceitas no todo ou alternadas individualmente, ligar ou desligar. Após as mudanças secundárias, o comando **pscxpert** continuará a aplicar as configurações de segurança ao sistema de computador.

Execute o comando **pscxpert** como o usuário raiz do Virtual I/O Server de destino. Quando você não tiver efetuado login como usuário raiz do Virtual I/O Server de destino, execute o comando **oem_setup_env** antes de executar o comando.

Se você executar o comando **pscxpert** quando outra instância do comando **pscxpert** já estiver em execução, o comando **pscxpert** sairá com uma mensagem de erro.

Nota: Execute novamente o comando **pscxpert** após as principais mudanças dos sistemas, como a instalação ou atualizações de software. Se um item de configuração de segurança específico não for selecionado quando o comando **pscxpert** for executado novamente, o item de configuração será ignorado.

Sinalizadores

Item	Descrição
-a	As configurações com as opções de nível de segurança associadas são gravadas no arquivo especificado em um formato abreviado.
-c	Verifica as configurações de segurança com relação ao conjunto de regras aplicado anteriormente. Se a verificação com relação a uma regra falhar, as versões anteriores da regra também serão verificadas. Esse processo continuará até que a verificação seja transmita ou até que todas as instâncias da regra com falha no arquivo `/etc/security/aixpert/core/appliedaixpert.xml` sejam verificadas. É possível executar essa verificação com relação a qualquer perfil padrão ou perfil customizado.
-d	Exibe a definição de tipo de documento (DTD).

Item	Descrição
-f	Aplica as configurações de segurança que são fornecidas no arquivo *Profile* especificado. Os perfis estão no diretório `/etc/security/aixpert/custom`. Os perfis disponíveis incluem os perfis padrão a seguir: **DataBase.xml** Esse arquivo contém os requisitos para as configurações do banco de dados padrão. **DoD.xml** Esse arquivo contém os requisitos para as configurações do Security Technical Implementation Guide (STIG) do Departamento de Defesa. **DoD_to_AIXDefault.xml** Isso muda as configurações para as configurações padrão do AIX. **DoDv2.xml** Esse arquivo contém os requisitos para a versão 2 das configurações do Department of Defense Security Technical Implementation Guide (STIG). **DoDv2_to_AIXDefault.xml** Isso muda as configurações para as configurações padrão do AIX. **Hipaa.xml** Esse arquivo contém os requisitos para as configurações do Health Insurance Portability and Accountability Act (HIPAA). **NERC.xml** Esse arquivo contém os requisitos para as configurações do North American Electric Reliability Corporation (NERC). **NERC_to_AIXDefault.xml** Esse arquivo muda as configurações do NERC para as configurações padrão do AIX. **PCI.xml** Esse arquivo contém os requisitos para as configurações do Payment card industry Data Security Standard. **PCIv3.xml** Esse arquivo contém os requisitos para as configurações do Padrão de Segurança de Dados do Setor de Cartão de Pagamento Versão 3. **PCI_to_AIXDefault.xml** Esse arquivo muda as configurações para as configurações padrão do AIX. **PCIv3_to_AIXDefault.xml** Esse arquivo muda as configurações para as configurações padrão do AIX. **SOX-COBIT.xml** Esse arquivo contém os requisitos para as configurações da Lei Sarbanes Oxley e COBIT. Também é possível criar perfis customizados no mesmo diretório e aplicá-los em suas configurações, renomeando e modificando os arquivos XML existentes. Por exemplo, o comando a seguir aplica o perfil HIPAA para seu sistema: `pscxpert -f /etc/security/aixpert/custom/Hipaa.xml` Ao especificar a sinalização **-f**, as configurações de segurança são aplicadas consistentemente de sistema para sistema, transferindo e aplicando com segurança um arquivo **appliedaixpert.xml** de sistema para sistema. Todas as regras aplicadas com sucesso são gravadas no arquivo `/etc/security/aixpert/core/appliedaixpert.xml` e as regras de ação `undo` correspondentes são gravadas no arquivo `/etc/security/aixpert/core/undo.xml`.

Item	Descrição
-l	Define as configurações de segurança do sistema para o nível especificado. Este sinalizador possui as opções a seguir: **h | high** Especifica as opções de segurança de alto nível. **m | medium** Especifica opções de segurança de nível médio. **l | low** Especifica as opções de segurança de baixo nível. **d | default** Especifica as opções de segurança de nível padrão do AIX. **s | sox-cobit** Especifica as opções de segurança Lei Sarbanes-Oxley e COBIT. Se você especificar ambas as sinalizações, **-l** e **-n**, as configurações de segurança não serão implementadas no sistema; no entanto, elas serão gravadas somente no arquivo especificado. Todas as regras aplicadas com sucesso são gravadas no arquivo `/etc/security/aixpert/core/appliedaixpert.xml` e as regras de ação desfazer correspondentes são gravadas no arquivo `/etc/security/aixpert/core/undo.xml`. **Atenção:** Ao usar a sinalização **d | default**, a sinalização pode sobrescrever as definições de segurança configuradas que você tinha configurado anteriormente, usando o comando **pscxpert** ou independentemente, e restaura o sistema para sua configuração aberta tradicional.
-n	Grava as configurações com as opções de nível de segurança associadas no arquivo especificado.
-p	Especifica que a saída das regras de segurança é exibida usando a saída detalhada. A sinalização **-p** registra as regras que são processadas no subsistema de auditoria se a opção **auditing** estiver ativada. Essa opção pode ser usada com qualquer uma das sinalizações **-l**, **-u**, **-c** e **-f**.
-P	Aceita o nome de perfil como entrada. Essa opção é usada juntamente com as sinalizações **-c**. As sinalizações **-c** e **-P** são usadas para verificar a compatibilidade do sistema com o perfil passado.
-r	Grava as configurações existentes do sistema para o arquivo `/etc/security/aixpert/check_report.txt`. É possível usar a saída em relatórios de auditoria de segurança ou conformidade. O relatório descreve cada configuração, como ela pode relacionar a um requisito de conformidade regulamentar e se a verificação foi aprovada ou se falhou.
-R	Produz a mesma saída que a sinalização **-r**, mas esta sinalização depende de uma descrição sobre cada script ou programa que é usado para implementar a definição de configuração.
-t	Exibe o tipo do perfil que é aplicado no sistema.
-u	Desfaz as configurações de segurança aplicadas. **Nota:** Não é possível usar a sinalização **-u** para reverter a aplicação dos perfis DoD, DoDv2, NERC, PCI ou PCIv3. Para remover esses perfis após eles serem incluídos, aplique o perfil que termina com `_AIXDefault.xml`. Por exemplo, para remover o perfil NERC.xml, deve-se aplicar o perfil NERC_to_AIXDefault.xml.

Parâmetros

Item	Descrição
File	O arquivo de saída que armazena as configurações de segurança. A permissão raiz é necessária para acessar esse arquivo.
Level	O nível customizado para verificar com relação às configurações aplicadas anteriormente.
Profile	O nome do arquivo do perfil que fornece as regras de conformidade para o sistema. A permissão raiz é necessária para acessar esse arquivo.

Segurança

O comando **pscxpert** pode ser executado apenas por raiz.

Exemplos

1. Para gravar todas as opções de segurança de alto nível para um arquivo de saída, insira o comando a seguir:

   ```
   pscxpert -l high -n /etc/security/pscexpert/plugin/myPreferredSettings.xml
   ```

   Após a execução desse comando, o arquivo de saída pode ser editado e as funções de segurança específicas podem ser comentadas colocando-as na sequência de comentários XML padrão (<-- inicia o comentário e -\> fecha o comentário).
2. Para aplicar as configurações de segurança do arquivo de configuração do Departamento de Defesa STIG, insira o comando a seguir:

   ```
   pscxpert -f /etc/security/aixpert/custom/DoD.xml
   ```
3. Para aplicar as configurações de segurança do arquivo de configuração HIPAA, insira o comando a seguir:

   ```
   pscxpert -f /etc/security/aixpert/custom/Hipaa.xml
   ```
4. Para verificar as configurações de segurança do sistema e para registrar as regras que falharam no subsistema de auditoria, insira o comando a seguir:

   ```
   pscxpert -c -p
   ```
5. Para verificar o nível customizado das configurações de segurança para o perfil NERC no sistema e para registrar as regras que falharam no subsistema de auditoria, insira o comando a seguir:

   ```
   pscxpert -c -p -l NERC
   ```
6. Para gerar relatórios e gravá-los no arquivo `/etc/security/aixpert/check_report.txt`, insira o comando a seguir:

   ```
   pscxpert -c -r
   ```

Local

Item	Descrição
/usr/sbin/pscxpert	Contém o comando **pscxpert**.

Arquivos

Item	Descrição
/etc/security/aixpert/log/aixpert.log	Contém um registro de rastreio de configurações de segurança aplicadas. Esse arquivo não usa o padrão syslog. O comando **pscxpert** grava diretamente no arquivo, possui permissões de leitura/gravação e requer segurança raiz.
/etc/security/aixpert/log/firstboot.log	Contém um log de rastreio das configurações de segurança que foram aplicadas durante a primeira inicialização de uma instalação Secure by Default (SbD).
/etc/security/aixpert/core/undo.xml	Contém uma listagem XML de configurações de segurança, que podem ser desfeitas.

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 127
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 146

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos EUA.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte seu representante IBM local para obter informações sobre os 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 usados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser usado em substituição a este produto, programa ou serviço. No entanto, é de responsabilidade do usuário avaliar e verificar a operação de qualquer produto, programa ou serviço não IBM.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento dessa publicação não concede ao Cliente nenhuma licença para essas patentes. Consultas sobre licença podem ser enviadas, 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 consultas sobre licença relacionadas a informações de conjunto de caracteres de byte duplo (DBCS) entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie consultas, 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 ao Reino Unido ou qualquer outro país em que tais disposições não estejam de acordo com a lei 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 INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a renúncia de responsabilidade de garantias expressas ou implícitas em certas transações; portanto, essa instrução pode não se aplicar ao Cliente.

Estas informações podem incluir imprecisões técnicas ou erros tipográficos. Periodicamente, são feitas mudanças nas informações aqui contidas; tais mudanças serão incorporadas em novas edições desta publicação. A IBM pode, a qualquer momento, fazer melhorias e/ou mudanças nos produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a websites não IBM são fornecidas somente por conveniência e não representam de forma alguma um endosso a estes websites. Os materiais contidos nesses websites não fazem parte dos materiais para este produto IBM e o uso desses websites é de total responsabilidade do Cliente.

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

Licenciados deste programa que desejam obter informações sobre este assunto com o propósito de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo 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 apropriados, 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 IBM Customer Agreement, Contrato de Licença do Programa Internacional IBM ou 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 essas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários desta publicação devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não IBM foram obtidas dos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes publicamente disponíveis. A IBM não testou esses produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Perguntas sobre as capacidades de produtos não IBM devem ser direcionadas aos respectivos fornecedores.

Todas as instruções relacionadas à direção ou intento futuros da IBM estão sujeitas a mudanças ou retirada sem aviso prévio e representam somente metas e objetivos.

Todos os preços IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a mudanças sem aviso. Os preços do revendedor podem variar.

Estas informações são somente para propósitos de planejamento. As informações aqui contidas estão sujeitas a mudanças antes da disponibilização dos produtos.

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

LICENÇA DE COPYRIGHT:

Estas informações contêm programas de aplicativos de amostra no idioma de origem, ilustrando as técnicas de programação em várias plataformas operacionais. O Cliente pode copiar, modificar e distribuir esses programas de amostra sem a necessidade de pagamento à IBM, para os propósitos de desenvolvimento, uso, marketing ou distribuição de programas de aplicativos em conformidade com a interface de programação de aplicativos para a plataforma operacional para a qual os programas de amostra são escritos. Esses exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou assegurar a confiabilidade, capacidade de manutenção ou função desses programas. Os programas de amostra são fornecidos "NO ESTADO EM QUE SE ENCONTRAM", sem garantia de nenhum tipo. A IBM não poderá ser responsabilizada por nenhum dano decorrente do uso dos programas de amostra.

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

Partes deste código são derivadas de Programas de Amostra da IBM Corp.

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 comerciais ou marcas registradas da International Business Machines Corp., registradas em vários países no mundo todo. Outros nomes de produtos e serviços podem ser marcas comerciais da IBM ou de outras empresas. Uma lista atual de marcas comerciais 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 comerciais e logotipos baseados em Java são marcas comerciais ou marcas registradas da Oracle e/ou de suas afiliadas.

Índice Remissivo

R

S

T

V

Impresso no Brasil