IBM PowerSC

Express Edition

Versão 1.1.3

PowerSC Express Edition

IBM PowerSC

Express Edition

Versão 1.1.3

PowerSC Express Edition

Nota
Antes de usar esta informação e o produto que elas suportam, leia as informações em “Avisos” na página 33.

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

Índice

Sobre este Documento

Este documento fornece administradores de sistemas com informações completas sobre segurança de arquivo, de sistema e de rede.

Destaque

As seguintes convenções de destaque são usadas nesse documento:

Negrito	Identifica comandos, sub-rotinas, palavras-chave, arquivos, estruturas, diretórios e outros itens cujos nomes são predefinidos pelo sistema. Identifica também objetos gráficos como botões, rótulos e ícones que o usuário seleciona.
Itálico	Identifica parâmetros cujos nomes ou valores reais devem ser fornecidos pelo usuário.
`Monoespaçamento`	Identifica exemplos de valores de dados específicos, exemplos de texto como os que você pode ver exibidos, exemplos de porções de código do programa como os que você pode gravar sendo um programador, mensagens do sistema ou informações que você deve de fato digitar.

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, você pode usar o comando **ls** para listar arquivos. Se você digitar `LS`, o sistema responderá que o comando será `not found`. 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 se assegure de usar maiúsculas e minúsculas corretamente.

ISO 9000

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

IBM PowerSC Express Edition 1.1.3

O IBM® PowerSC Express Edition inclui o recurso Security and Compliance Automation que gerencia os perfis predefinidos para segurança e conformidade. O PowerSC Express Edition também inclui o recurso PowerSC Real Time Compliance, que pode ser configurado para fornecer alertas em tempo real quando ocorrem violações ou quando determinados arquivos críticos forem alterados.

O que Há de Novo no PowerSC Express Edition 1.1.3

Leia sobre informações novas ou alteradas significativamente para o O que há de novo na coleção de tópico do PowerSC Express Edition 1.1.3.

Como Ver o Que Há de Novo ou Foi Alterado

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

Dezembro de 2013

As informações a seguir fornecem um resumo do conteúdo novo e atualizado para PowerSC Express Edition 1.1.3:

- Incluiu informações sobre o arquivo README.ICEexpress no "Instalando o PowerSC Express Edition Versão 1.1.3" na página 2.
- Atualizou as informações sobre o suporte para a conformidade do Payment Card Industry – Data Security Standard para a versão 2.0 do padrão no "Conformidade do Payment Card Industry - Data Security Standard" na página 4.
- Incluiu o "Comando pscxpert" na página 28.

Maio de 2013

Incluiu uma tabela que descreve como o recurso AIX Security Expert assegura a conformidade com o Payment Card Industry – Data Security Standard para "Conformidade do Payment Card Industry - Data Security Standard" na página 4.

Novembro de 2012

As informações a seguir fornecem um resumo do conteúdo novo e atualizado para PowerSC Express Edition 1.1.2:

- Incluiu a documentação que descreve o recurso Real-Time Compliance no "PowerSC Real Time Compliance" na página 27.
- Incluída a documentação para o suporte dos padrões, conforme definido pelo "Health Insurance Portability and Accountability Act (HIPAA)" na página 17.

Conceitos do PowerSC Express Edition 1.1.3

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

O PowerSC Express Edition 1.1.3 fornece segurança e controle dos sistemas operacionais em uma nuvem ou em datacenters virtualizados e fornece uma visualização corporativa e recursos de gerenciamento. O

PowerSC Express Edition é um conjunto de recursos que inclui Security and Compliance Automation e Real-Time Compliance. A tecnologia de segurança 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 no processador em que cada componente está disponível.

Tabela 1. Componentes, Descrição, Sistema Operacional Suportado e Hardware Suportado do PowerSC Express Edition

Componentes	Descrição	Sistema operacional suportado	Hardware suportado
Security and Compliance Automation	Automatiza a definição, monitoramento e auditoria de configuração de segurança e conformidade para os padrões a seguir: • Payment Card Industry Data Security Standard (PCI DSS) • Conformidade de Sarbanes-Oxley Act e COBIT (SOX/COBIT) • STIG do Department of Defense (DoD) dos Estados Unidos • Health Insurance Portability and Accountability Act (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6 • POWER7
Real-Time Compliance	Monitora uma sistema AIX ativado para manter a segurança e fornece alertas quando uma mudança no sistema viola uma regra identificada na política de configuração.	• 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	Não há nenhum requisito de hardware específico.

Instalando o PowerSC Express Edition Versão 1.1.3

O PowerSC Express Edition inclui o pacote `powerscExp.ice`. O pacote `powerscExp.ice` suporta o AIX 5.3, AIX 6.1 e AIX Versão 7.1.

O pacote `powerscExp.ice` deve ser instalado em todos os sistemas AIX que requerem o recurso PowerSC Express Edition Security and Compliance.

Instale o PowerSC Express 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 Express Edition usando a interface SMIT, conclua as etapas a seguir:

1. Execute o seguinte comando:
   ```
   % smitty installp
   ```
2. Selecione a opção **Instalar Software**.

3. Selecione o dispositivo de entrada ou o diretório para o software para especificar o local e o arquivo de instalação da imagem de instalação do IBM Compliance Expert. Por exemplo, se a imagem de instalação possuir o caminho do diretório e nome do arquivo `/usr/sys/inst.images/powerscExp.ice`, você deverá especificar o caminho do arquivo no campo **INPUT**.
4. Visualize e aceite o contrato de licença. Aceite o contrato de licença usando a seta para baixo para selecionar **ACEITAR novos contratos de licença** e pressione a tecla tab para alterar o valor para **Sim**.
5. Pressione **Enter** para iniciar a instalação.
6. Verifique se o status do comando será **OK** após a instalação ser concluída.

Um arquivo leia-me nomeado `README.ICEexpress` é instalado no diretório `/etc/security/aixpert`. Este arquivo contém os detalhes de implementação para os perfis de conformidade incluídos com o PowerSC Express Edition.

Visualizando a Licença de 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 do PowerSC Standard Edition.

Por exemplo, é possível inserir o comando a seguir usando a CLI para especificar as informações sobre licença relacionadas ao PowerSC Express Edition:

```
% installp -lE -d  /usr/sys/inst.images/powerscExp.ice
```

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 um plug-in do IBM Systems Director que simplifica a aplicação de configurações de segurança, monitoramento de configurações de segurança e auditoria de configurações de segurança para o sistema operacional AIX e os 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 Express Edition e no PowerSC Standard Edition.

O pacote de instalação do PowerSC Express Edition, 5765-G82, deve ser instalado nos sistemas gerenciados AIX. O pacote de instalação instala o conjunto de arquivos `powerscExp.ice` que pode ser implementado no sistema usando o AIX Profile Manager ou o comando **aixpert**. 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.

Conceitos de Security and Compliance Automation

O recurso PowerSC Security and Compliance é um método automatizado para configurar e auditar sistemas AIX de acordo com o Security Technical Implementation Guide (STIG) do Department of Defense (DoD) dos Estados Unidos.

O PowerSC ajuda a automatizar a configuração e o monitoramento de sistemas que devem estar em conformidade com o Payment Card Industry (PCI) Data Security Standard (DSS) versão 1.2. 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). Os perfis XML do PowerSC Express Edition podem ser usados com o comando **aixpert**, semelhante ao ICEE.

Os perfis de conformidade pré-configurados entregues com o PowerSC Express Edition reduzem a carga de trabalho administrativa de interpretar a documentação de conformidade e implementar os padrões, conforme os parâmetros de configuração do sistema específico. Essa tecnologia reduz o custo de configuração de conformidade e auditoria automatizando os processos. O IBM PowerSC Express 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. Esta diretiva estabeleceu a política e designou a responsabilidade para a Defense Information Security Agency (DISA) dos Estados Unidos para fornecer orientação de configuração de segurança.

A DISA desenvolveu os princípios e as orientações no UNIX STIG que fornece um ambiente que atende ou excede os requisitos de segurança de sistemas operacionais de DoD no nível confidencial da Mission Assurance Category (MAC) II, que contém informações confidenciais. A DoD dos Estados Unidos tem requisitos de segurança de TI rigorosos e enumerou os detalhes das definições de configuração necessárias para assegurar-se de que o sistema opera de maneira segura. É possível alavancar a orientação de especialista necessária. O PowerSC Express 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 de DoD estão no diretório `/etc/security/pscexpert/bin`.

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. Seção 1.1.5 e Seção 2.2.2: lista documentada de serviços e portas necessárias para negócios. Esse requisito é implementado desativando serviços desnecessários e inseguros.

Seção 1.3.6: Assegurando e sincronizando arquivos de configuração do roteador. Esse requisito é implementado configurando o valor *clean_partial_conns* de opção Rede como 1.

Requisito 2: Não usar padrões oferecidos pelo fornecedor para senhas do sistema e outros parâmetros de segurança.

Seção 2.1: Sempre alterar padrões oferecidos 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 do AIXPert e verifica se ele será concluído quando ele estiver executando os comandos, como o comando `aixpert -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:

- Seção 8.5.9: Altere as senhas de usuário pelo menos a cada 90 dias.
- Seção 8.5.10: Requer uma comprimento mínimo de senha de 7 caracteres.
- Seção 8.5.11: Use uma senha que contém caracteres numerais e alfabéticos.
- Seção 8.5.12: Não permita que um indivíduo envie uma nova senha que seja a mesma que as quatro senhas anteriores que foram usadas.
- Seção 8.5.13: Limite as tentativas de acesso repetidas bloqueando o ID do usuário após seis tentativas sem sucesso.
- Seção 8.5.14: Configure a duração de bloqueio para 30 minutos ou até que um administrador reative o ID do usuário.
- Seção 8.5.15: Requer que um usuário insira novamente uma senha para reativar um terminal após estar inativo durante 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.
Seção 10.2: Este requisito é implementado pelo acesso de criação de log 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.
Seção 12.3.9: Ativação de modems para fornecedores apenas quando necessário por 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 Express Edition reduz o gerenciamento de configuração que é necessário para atender as diretrizes definidas por PCI DSS. 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 Express 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.

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 Express Edition aborda os requisitos do padrão PCI DSS usando as funções do utilitário AIX Security Expert:

Tabela 2. Configurações Relacionadas às Conformidades de PCI DSS 2.0 Padrão

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do valor e a configuração necessária para conformidade (quando aplicável)
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 que seja possível alterar uma senha para 0 semanas.	**Local** `/etc/security/pscexpert/bin/chusrattr` **Valor compatível** minage=0
8.5.9	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.	**Local** `/etc/security/pscexpert/bin/chusrattr` **Valor compatível** maxage=13
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.	**Local** `/etc/security/pscexpert/bin/chusrattr` **Valor compatível** maxexpired=8

Tabela 2. Configurações Relacionadas às Conformidades de PCI DSS 2.0 Padrão (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do valor e a configuração necessária para conformidade (quando aplicável)
8.5.10	Requer um comprimento mínimo da senha de pelo menos 7 caracteres.	Configura o comprimento mínimo da senha para 7 caracteres.	**Local** `/etc/security/pscexpert/bin/chusrattr` **Valor compatível** minlen=7
8.5.11	Use as senhas que contêm os caracteres numéricos e alfabéticos.	Configura o número mínimo de caracteres alfabéticos que são necessários em uma senha como 1. Essa configuração assegura que a senha contenha caracteres alfabéticos.	**Local** `/etc/security/pscexpert/bin/chusrattr` **Valor compatível** minalpha=1
8.5.11	Use as senhas que contêm os caracteres numéricos e alfabéticos.	Configura o número mínimo de caracteres não alfabéticos que são necessários em uma senha como 1. Essa configuração assegura que a senha contenha caracteres não alfabéticos.	**Local** `/etc/security/pscexpert/bin/chusrattr` **Valor compatível** minother=1
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 máximo de vezes que um caractere pode ser repetido em uma senha como 8. Esta configuração indica que um caractere em uma senha pode ser repetido um número ilimitado de vezes, contanto que ela esteja de acordo com as outras limitações da senha.	**Local** `/etc/security/pscexpert/bin/chusrattr` **Valor compatível** maxrepeats=8
8.5.12	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 como 52.	**Local** `/etc/security/pscexpert/bin/chusrattr` **Valor compatível** histexpire=52
8.5.12	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 é possível reutilizar como 4.	**Local** `/etc/security/pscexpert/bin/chusrattr` **Valor compatível** histsize=4
8.5.13	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 sem sucesso consecutivas que desativa uma conta como 6 tentativas para cada conta não raiz.	**Local** `/etc/security/pscexpert/bin/chusrattr` **Valor compatível** loginretries=6
8.5.13	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 sem sucesso consecutivas que desativa uma porta como 6 tentativas.	**Local** `/etc/security/pscexpert/bin/chdefstanza` `/etc/security/login.cfg` **Valor compatível** logindisable=6

Tabela 2. Configurações Relacionadas às Conformidades de PCI DSS 2.0 Padrão (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do valor e a configuração necessária para conformidade (quando aplicável)
8.5.14	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 é bloqueada após ser desativada pelo atributo *logindisable* como 30 minutos.	**Local** `/etc/security/pscexpert/bin/chdefstanza` `/etc/security/login.cfg` **Valor compatível** loginreenable=30
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.	**Local** `/etc/security/pscexpert/bin/chuserstanza` `/etc/security/user` **Valor compatível** rlogin=false root
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.	**Local** `/etc/security/pscexpert/bin/chuserstanza` `/etc/security/user` **Valor compatível** login=true root
10.2	Ative a auditoria no sistema.	Ativa a auditoria dos arquivos binários no sistema.	**Local** `/etc/security/pscexpert/bin/pciaudit` **Valor compatível** `h`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui o daemon `lpd`.	Para o daemon `lpd` e comenta a linha de entrada correspondente no arquivo `/etc/inittab` que inicia o daemon automaticamente.	**Local** `/etc/security/pscexpert/bin/comntrows` **Valor compatível** lpd: /etc/inittab : `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui o Common Desktop Environment (CDE).	Desativa a função CDE quando o Layer Four Traceroute (LFT) não for configurado.	**Local** `/etc/security/pscexpert/bin/comntrows` **Valor compatível** "dt" "/etc/inittab" ":" `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui o daemon `timed`.	Para o daemon `timed` e comenta a linha de entrada correspondente no arquivo `/etc/rc.tcpip` que inicia o daemon automaticamente.	**Local** `/etc/security/pscexpert/bin/rctcpip` **Valor compatível** timed `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui o daemon `NTP`.	Para o daemon `NTP` e comenta a linha de entrada correspondente no arquivo `/etc/rc.tcpip` que inicia o daemon automaticamente.	**Local** `/etc/security/pscexpert/bin/rctcpip` **Valor compatível** xntpd `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui o daemon `rwhod`.	Para o daemon `rwhod` e comenta a linha de entrada correspondente no arquivo `/etc/rc.tcpip` que inicia o daemon automaticamente.	**Local** `/etc/security/pscexpert/bin/rctcpip` **Valor compatível** rwhod `d`

Tabela 2. Configurações Relacionadas às Conformidades de PCI DSS 2.0 Padrão (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do valor e a configuração necessária para conformidade (quando aplicável)
2.1	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.	**Local** /etc/security/pscexpert/bin/rctcpip **Valor compatível** snmpd d
2.1	Altere padrões fornecidos pelo fornecedor antes de instalar um sistema na rede, que inclui desativar o daemon SNMPMIBD.	Desativa o daemon SNMPMIBD.	**Local** /etc/security/pscexpert/bin/rctcpip **Valor compatível** snmpmibd d
2.1	Altere padrões fornecidos pelo fornecedor antes de instalar um sistema na rede, que inclui desativar o daemon AIXMIBD.	Desativa o daemon AIXMIBD.	**Local** /etc/security/pscexpert/bin/rctcpip **Valor compatível** aixmibd d
2.1	Altere padrões fornecidos pelo fornecedor antes de instalar um sistema na rede, que inclui desativar o daemon HOSTMIBD.	Desativa o daemon HOSTMIBD.	**Local** /etc/security/pscexpert/bin/rctcpip **Valor compatível** hostmibd d
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui o daemon DPID2.	Para o daemon DPID2 e comenta a linha de entrada correspondente no arquivo /etc/rc.tcpip que inicia o daemon automaticamente.	**Local** /etc/security/pscexpert/bin/rctcpip **Valor compatível** dpid2 d
2.1	Altere padrões fornecidos pelo fornecedor antes de instalar um sistema na rede, que inclui parar o servidor DHCP.	Desativa o servidor DHCP.	**Local** /etc/security/pscexpert/bin/rctcpip **Valor compatível** dhcpsd d
1.1.5 2.2.2	Desativa serviços desnecessários e inseguros, que inclui 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.	**Local** /etc/security/pscexpert/bin/rctcpip **Valor compatível** dhcprd d
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui o daemon rshd.	Para e desativa todas as instâncias do daemon rshd e o serviço rshdpci_shell e comenta a linha de entradas correspondentes no arquivo /etc/inetd.conf que inicia as instâncias automaticamente.	**Local** /etc/security/pscexpert/bin/cominetdconf **Valor compatível** shell tcp d
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui o daemon rlogind.	Para e desativa todas as instâncias do daemon rlogind e do serviço rlogindpci.rlogin. O utilitário AIX Security Expert também comenta a linha de entradas correspondentes no arquivo /etc/inetd.conf que inicia as instâncias automaticamente.	**Local** /etc/security/pscexpert/bin/cominetdconf **Valor compatível** login tcp d

Tabela 2. Configurações Relacionadas às Conformidades de PCI DSS 2.0 Padrão (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do valor e a configuração necessária para conformidade (quando aplicável)
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** exec tcp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** comsat udp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** finger tcp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** systat tcp `d`
2.1	Altere padrões fornecidos pelo fornecedor antes de instalar um sistema na rede, que inclui desativar o comando `netstat`.	Desativa o comando `netstat`.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** netstat tcp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** tftp udp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** talk udp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** rquotad udp `d`

Tabela 2. Configurações Relacionadas às Conformidades de PCI DSS 2.0 Padrão (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do valor e a configuração necessária para conformidade (quando aplicável)
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** rstatd udp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** rusersd udp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** rwalld udp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** sprayd udp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** pcnfsd udp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** echo tcp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** discard tcp `d`

Tabela 2. Configurações Relacionadas às Conformidades de PCI DSS 2.0 Padrão (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do valor e a configuração necessária para conformidade (quando aplicável)
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui o serviço `chargen` de TCP.	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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** chargen tcp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** daytime tcp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** time tcp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** echo udp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** discard udp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui o serviço `chargen` de UDP.	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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** chargen udp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** daytime udp `d`

Tabela 2. Configurações Relacionadas às Conformidades de PCI DSS 2.0 Padrão (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do valor e a configuração necessária para conformidade (quando aplicável)
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** time udp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** ftp tcp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** telnet tcp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui `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`.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** dtspc tcp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** ttdbserver tcp `d`
1.1.5 2.2.2	Desative serviços desnecessários e inseguros, que inclui 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.	**Local** `/etc/security/pscexpert/bin/cominetdconf` **Valor compatível** cmsd udp `d`
2.2.3	Configure os parâmetros de segurança do sistema para evitar mau uso.	Remove os comandos Set User ID (SUID).	**Local** `/etc/security/pscexpert/bin/rmsuidfrmrcmds` **Valor compatível** `R`

Tabela 2. Configurações Relacionadas às Conformidades de PCI DSS 2.0 Padrão (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do valor e a configuração necessária para conformidade (quando aplicável)
2.2.3	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.	**Local** `/etc/security/pscexpert/bin/filepermgr` **Valor compatível** `l`
2.2.3	Configure os parâmetros de segurança do sistema para evitar mau uso.	Ativa os parâmetros de segurança fornecidos pelo protocolo Network File System.	**Local** `/etc/security/pscexpert/bin/nfsconfig` **Valor compatível** `e`
2.2.2	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.	**Local** `/etc/security/pscexpert/bin/disrmtdmns` **Valor compatível** `x`
2.2.2	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.	**Local** `/etc/security/pscexpert/bin/rmrhostsnetrc` **Valor compatível** `h`
2.2.2	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.	**Local** `/etc/security/pscexpert/bin/rmetchostsequiv` **Valor compatível** Nenhum valor compatível é necessário.
1.3.6	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.	**Local** `/etc/security/pscexpert/bin/ntwkopts` **Valor compatível** clean_partial_conns=1 s
1.3.6	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).	**Local** `/etc/security/pscexpert/bin/ntwkopts` **Valor compatível** tcp_tcpsecure=7 s
	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 as portas não usadas.	**Local** `/etc/security/pscexpert/bin/ipsecshunhosthls` **Valor compatível** Nenhum valor compatível é necessário.

Tabela 2. Configurações Relacionadas às Conformidades de PCI DSS 2.0 Padrão (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do valor e a configuração necessária para conformidade (quando aplicável)
	Proteja o host a partir de varreduras de porta.	Configura o sistema para evitar portas vulneráveis por 5 minutes minutos, que evita varreduras de porta.	**Local** `/etc/security/pscexpert/bin/ipsecshunports` **Valor compatível** Nenhum valor compatível é necessário.
	Limite as permissões de criação de objeto.	Configura as permissões de criação de objeto padrão como 22.	**Local** `/etc/security/pscexpert/bin/chusrattr` **Valor compatível** umask=22
	Limite o acesso de sistema.	Torna o ID raiz o único que está listado no arquivo `cron.allow` e remove o arquivo `cron.deny` do sistema.	**Local** `/etc/security/pscexpert/bin/limitsysacc` **Valor compatível** `h`
	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	**Local** `/etc/security/pscexpert/bin/rmdotfrmpathroot` **Valor compatível** Nenhum valor compatível é necessário.
	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	**Local** `/etc/security/pscexpert/bin/rmdotfrmpathnroot` **Valor compatível** Nenhum valor compatível é necessário.
	Limite o acesso de sistema.	Inclui o recurso de usuário raiz e o nome de usuário no arquivo `/etc/ftpusers`.	**Local** `/etc/security/pscexpert/bin/chetcftpusers` **Valor compatível** `a`
	Remova a conta guest.	Remove a conta guest e seus arquivos.	**Local** `/etc/security/pscexpert/bin/execmds` **Valor compatível** "rmuser guest; rm -rf /home/guest; ODMDIR=/etc/objrepos odmdelete -qloc0=/home/guest -o inventory"
	Evite programas de ativação na área de conteúdo.	Ativa o recurso Stack Execution Disable (SED).	**Local** `/etc/security/pscexpert/bin/sedconfig` **Valor compatível** Nenhum valor compatível é necessário.

Tabela 2. Configurações Relacionadas às Conformidades de PCI DSS 2.0 Padrão (continuação)

Implementa essas normas de PCI DSS	Especificação de implementação	A implementação do AIX Security Expert	Local do valor e a configuração necessária para conformidade (quando aplicável)
	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.	**Local** `/etc/security/pscexpert/bin/chuserstanza` **Valor compatível** /etc/security/user dictionlist=/etc/security/aixpert/dictionary/English rootpci_rootpwdintchk
8.5.15	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.	**Local** `/etc/security/pscexpert/bin/autologoff` **Valor compatível** `900`
	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.	**Local** `/etc/security/pscexpert/bin/tcptr_aixpert` **Valor compatível** `pci`
	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.	**Local** `/etc/security/pscexpert/bin/cfgsecmig` **Valor compatível** `on`
1.3.5	Limite os pacotes a partir de origens desconhecidas.	Ativa os pacotes do Hardware Management Console.	**Local** `/etc/security/pscexpert/bin/ipsecpermithostorport` **Valor compatível** Nenhum valor compatível é necessário.
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.	**Local** `/etc/security/pscexpert/bin/manageITsecurity` **Valor compatível** Nenhum valor compatível é necessário.
	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.	**Local** `/etc/security/pscexpert/bin/EnableRbac` **Valor compatível** Nenhum valor compatível é necessário.

Informações relacionadas:

Conformidade de Payment Card Industry DSS

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 Express 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 no AIX 7.1, AIX 6.1 e AIX 5.3.

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
- Conformidade de Sarbanes-Oxley (SOX)

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 3. 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.
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.

Tabela 3. 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.	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.
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.

Tabela 3. 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 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.
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.

Tabela 3. 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 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.
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 4. 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.
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 usuários **isso**, **so**, **sa** e designa funções apropriadas aos usuários.	Sugere que você crie usuários **isso**, **so**, **sa**. Designa funções apropriadas aos usuários.	**Comando**: **/etc/security/aixpert/bin/RbacEnablement**.

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 identificação XML de abertura <AIXPertEntry name... para a identificação 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:

```
aixpert –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 **aixpert** 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 5. Comandos PowerSC para AIX

Comando	Padrão de conformidade
% aixpert -f /etc/security/aixpert/custom/DoD.xml	*Guia de Implementação Técnica de Segurança do UNIX do Departamento de Defesa dos Estados Unidos*
% aixpert -f /etc/security/aixpert/custom/PCI.xml	*Padrão de segurança de dados Payment Card Industry*
% aixpert -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 6. 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/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 **aixpert** no sistema AIX e o comando **viosecure** no VIOS pode demorar para ser executado, porque estão verificando ou configurando o sistema inteiro e fazendo mudanças na configuração relacionada 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 22
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 Express Edition ou 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 Express Edition e não faz parte do sistema operacional AIX de base.

Para instalar o PowerSC Express Edition, que inclui 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
2. Se você já tiver instalado o PowerSC Express Edition versão 1.1.2.0 ou posterior, será possível incluir os arquivos necessários para o recurso PowerSC Real Time Compliance reinstalando o PowerSC Express Edition ou atualizando a versão instalada do recurso PowerSC Real Time Compliance para a versão mais recente.
3. Para atualizar o conjunto de arquivos do recurso PowerSC Real Time Compliance, instale o conjunto de arquivos `powerscExp.rtc` do pacote de instalação para PowerSC Express Edition versão 1.1.2.0 ou posterior.
4. Para uma nova instalação do PowerSC Express Edition versão 1.1.2.0 ou anterior, siga as instruções em Instalando o PowerSC Express Edition Versão 1.1.2 ou anterior.

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 **aixpert** 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.

Para obter mais informações sobre as opções e sobre como modificar esse arquivo, consulte as informações sobre o arquivo rtcd.conf.

Informações relacionadas:

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

---

Comandos do PowerSC Express Edition

Os comandos disponíveis com o PowerSC Express Edition fornecem o método de alterar as definições de conformidade usando a linha de comandos.

Comando pscxpert

Propósito

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

Sintaxe

pscxpert

pscxpert -l h|alto | m|médio | l|baixo | d|padrão [-p] [-n -o *filename*] [**-a -o** *filename*]

pscxpert -c [-P *filename*] **[-r] [-R] [-l h|alto | m|médio | l|baixo | d|padrão] [-p]**

pscxpert -u [-p]

pscxpert -d

pscxpert [**-f** *profile_name*]

pscxpert [**-f** *profile_name*] [**-a -o** *filename*] [**-p**]

pscxpert -t

Descrição

O comando **pscxpert** configura uma variedade de definições de configuração do sistema para ativar o nível de segurança desejado.

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, executar o comando **pscxpert -l** com as opções **-n** e **-o** *filename* salva as configurações de segurança para um arquivo especificado pelo parâmetro *filename*. Em seguida, o sinalizador **-f** aplica as novas configurações.

Após a seleção inicial, um menu é exibido detalhando em itens todas as opções de configuração de segurança 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.

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 do nível de segurança associado são gravadas no arquivo especificado pelo sinalizador **-o**, em formato abreviado. Você deve especificar a opção **-o** ao especificar a opção **-a**.
-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.
-d	Exibe a definição de tipo de documento (DTD).

Item	Descrição
-f	Aplica as configurações de segurança fornecidas no arquivo especificado *profile_name*. Os perfis estão localizados 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 altera as configurações para as configurações do AIX padrão **Hipaa.xml** Esse arquivo contém os requisitos para as configurações do Health Insurance Portability and Accountability Act (HIPAA). **PCI.xml** Esse arquivo contém os requisitos para as configurações do Payment card industry Data Security Standard. **PCI_to_AIXDefault.xml** Esse arquivo altera as configurações para as configurações do AIX padrão **SCBPS.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 opção **-f**, as configurações de segurança serão aplicadas consistentemente de sistema para sistema por segurança transferindo e aplicando 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**.
-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. Se você especificar ambos os sinalizadores **-l** e **-n**, as configurações de segurança não serão implementadas no sistema; no entanto, elas são gravadas apenas no arquivo especificado no sinalizador **-o**. 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 opção **d | default**, a opção poderá sobrescrever as configurações de segurança definidas que você tinha definido anteriormente usando o comando **pscxpert** ou independentemente e restaurar o sistema para sua configuração aberta tradicional.
-n	Grava as configurações com as opções do nível de segurança associado ao arquivo especificado pelo sinalizador **-o**. Você deve especificar a opção **-o** ao usar a opção **-n**.

Item	Descrição
-o	Armazena a saída de segurança no arquivo especificado pela variável *filename*. As permissões de leitura e gravação do arquivo de saída são configuradas como raiz como uma precaução de segurança. Esse arquivo deve ser protegido com relação ao acesso não desejado.
-p	Especifica que a saída das regras de segurança é exibida usando a saída detalhada. A opção **-p** registrará as regras processadas no subsistema de auditoria se a opção **auditing** estiver ativada. Esta opção pode ser usada com qualquer uma das opções **-l**, **-u**, **-c** e **-f**.
-P	Aceita o nome de perfil como entrada. Esta opção é usada juntamente com a opção **-c**. A opção **-c** juntamente com a opção **-P** é usada para verificar a compatibilidade do sistema com o perfil transmitido.
-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 o sinalizador **-r** , mas esse sinalizador também anexa uma descrição sobre cada script ou o programa usado para implementar a definição de configuração.
-t	Exibe o tipo do perfil aplicado no sistema.
-u	Desfaz as configurações de segurança aplicadas.

Parâmetros

Item	Descrição
nome do arquivo	O arquivo de saída que armazena as configurações de segurança. A permissão raiz é necessária para acessar esse arquivo.
profile_name	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 -o /etc/security/pscexpert/plugin/myPreferredSettings.xml
   ```

   Após concluir este comando, o arquivo de saída poderá ser editado e as funções de segurança específicas poderão ser comentadas incluindo-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 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. Isso 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.

Avisos

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

LICENÇA DE COPYRIGHT:

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

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

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

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

Considerações sobre Política de Privacidade

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

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

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

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

Marcas Registradas

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

UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.

Índice Remissivo

Impresso no Brasil