IBM PowerSC

Standard Edition

Version 1.1.6

PowerSC Standard Edition

IBM PowerSC

Standard Edition

Version 1.1.6

PowerSC Standard Edition

Anmerkung

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 191 gelesen werden.

Diese Ausgabe bezieht sich auf IBM PowerSC Standard Edition Version 1.1.6 und alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuausgabe geändert wird.

Inhaltsverzeichnis

Zu diesem Dokument v

Neuerungen in PowerSC Standard Edition 1

PDF-Dateien zu PowerSC Standard Edition 3

PowerSC Standard Edition-Konzepte . . 5

PowerSC Standard Edition installieren . 7

Automation von Sicherheit und Konformität 9
Security and Compliance Automation-Konzepte . . 9
Konformität mit Department of Defense-STIG . . 10
Konformität mit Payment Card Industry - Data Security Standard 73
Konformität mit Sarbanes-Oxley Act und COBIT 90
Health Insurance Portability and Accountability Act (HIPAA) 90
NERC-Konformität (North American Electric Reliability Corporation) 96
Automation von Sicherheit und Konformität verwalten 98
Fehlgeschlagene Regel untersuchen 99
Fehlgeschlagene Regel aktualisieren 100
Angepasstes Sicherheitskonfigurationsprofil erstellen 100
Anwendungen mit AIX Profile Manager testen 100
Kontinuierliche Konformität von Systemen mit AIX Profile Manager überwachen 101
PowerSC-Sicherheits- und -Konformitätsautomation konfigurieren 101
Einstellungen für PowerSC-Konformitätsoptionen konfigurieren 101
PowerSC-Konformität über die Befehlszeile konfigurieren. 101
PowerSC-Konformität mit AIX Profile Manager konfigurieren 102

PowerSC Real Time Compliance . . . 105
PowerSC Real Time Compliance installieren . . . 105
PowerSC Real Time Compliance konfigurieren . . 105
Vom Feature PowerSC Real Time Compliance überwachte Dateien angeben 106
Alerts für PowerSC Real Time Compliance festlegen 106

Trusted Boot. 107
Trusted Boot-Konzepte 107
Planung für Trusted Boot 108
Voraussetzungen für Trusted Boot 108
Fehlerhebung vorbereiten 108
Hinweise zur Migration 109
Trusted Boot installieren. 109
Collector installieren 109
Prüffunktion installieren. 109
Trusted Boot konfigurieren 110
System registrieren 110
System attestieren 110
Trusted Boot verwalten 111
Attestierungsergebnisse interpretieren 111
Systeme löschen 111
Fehlerbehebung bei Trusted Boot 112

Trusted Firewall 115
Trusted Firewall-Konzepte 115
Trusted Firewall installieren 117
Trusted Firewall konfigurieren. 118
Trusted Firewall Advisor 118
Trusted Firewall-Protokollierung 118
Mehrere gemeinsam genutzte Ethernet-Adapter 119
Gemeinsam genutzte Ethernet-Adapter entfernen. 120
Regeln erstellen 120
Regeln inaktivieren 122

Trusted Logging 123
Virtuelle Protokolle 123
Virtuelle Protokolleinheiten erkennen 123
Trusted Logging installieren 124
Trusted Logging konfigurieren 125
AIX-Prüfsubsystem konfigurieren 125
syslog konfigurieren 125
Daten auf virtuelle Protokolleinheiten schreiben 126

Trusted Network Connect (TNC) . . . 127
Trusted Network Connect-Konzepte 127
Trusted Network Connect-Komponenten . . . 127
Sichere Kommunikation über Trusted Network Connect (TNC) 129
Trusted Network Connect-Protokoll 129
IMC- und IMV-Module 129
TNC-Anforderungen 130
TNC-Komponenten konfigurieren 130
Optionen für die TNC-Komponenten konfigurieren 131
Optionen für den Trusted Network Connect-Server (TNC) konfigurieren. 131
Weitere Optionen für den Trusted Network Connect-Client konfigurieren 132
Optionen für den TNC Patch Management-Server konfigurieren 132
E-Mail-Benachrichtigung für Trusted Network Connect-Server konfigurieren 134
IP-Referrer in VIOS konfigurieren 135
Trusted Network Connect-Komponenten (TNC) verwalten 135

Trusted Network Connect-Serverprotokolle anzeigen . . . 135
Richtlinien für den Trusted Network Connect-Client erstellen . . . 136
Verifizierung des Trusted Network Connect-Clients starten . . . 137
Verifizierungsergebnisse von Trusted Network Connect anzeigen . . . 137
Trusted Network Connect-Client aktualisieren 138
Patch-Management-Richtlinien verwalten . . . 138
Trusted Network Connect-Zertifikate importieren . . . 138
Berichterstellung im TNC-Server . . . 139
Fehler bei Trusted Network Connect und Patch Management beheben . . . 140

Grafische Benutzerschnittstelle von PowerSC . . . 141
PowerSC-GUI-Konzepte . . . 141
PowerSC-GUI-Sicherheit . . . 141
Endpunktinhalt auf der Seite "Konformität" eingeben . . . 142
PowerSC-GUI installieren . . . 142
PowerSC-GUI-Agent . . . 143
PowerSC-GUI-Server . . . 143
Voraussetzung für die PowerSC-GUI . . . 143
Sicherheitszertifikat für den Truststore an Endpunkte verteilen . . . 143
Truststore-Datei manuell auf Endpunkte kopieren . . . 144
Truststore-Datei mit einem Virtualisierungsmanager auf Endpunkte kopieren . . . 144
Benutzeraccounts einrichten . . . 145
Befehle und Scripts für die Gruppeneinrichtung ausführen . . . 145
PowerSC-GUI verwenden . . . 146
PowerSC-GUI-Sprache festlegen . . . 147
In der PowerSC-GUI navigieren . . . 147
Endpunkt- und Serverkommunikation verwalten 148
Endpunkt- und Serverkommunikation verifizieren . . . 148
Endpunkte aus der PowerSC-GUI-Überwachung entfernen . . . 148
Keystore-Anforderungen verifizieren und generieren . . . 149
Endpunkte organisieren und gruppieren . . . 150
Angepasste Gruppen erstellen . . . 150
Einer vorhandenen Gruppe zugewiesene Systeme hinzufügen oder entfernen . . . 150
Gruppe löschen . . . 151
Gruppe umbenennen . . . 151
Gruppe klonen . . . 151
Mit Konformitätsprofilen arbeiten . . . 151
Konformitätsprofile anzeigen . . . 152
Angepasstes Profil erstellen . . . 152
Profile auf Gruppenmitglieder kopieren . . . 153
Angepasstes Profil löschen . . . 153
Konformitätsstufen und -profile verwalten . . . 153
Konformitätsstufen und -profile anwenden . . . 154
Konformitätsstufen widerrufen . . . 154
Zuletzt angewendete Konformitätsstufe und zuletzt angewendetes Konformitätsprofil überprüfen . . . 155
Nicht angewendete Konformitätsstufe oder nicht angewendetes Konformitätsprofil überprüfen . . . 155
E-Mail-Benachrichtigung beim Eintreten eines Konformitätsereignisses senden . . . 156
Endpunktsicherheit überwachen . . . 156
Real Time Compliance (RTC) konfigurieren . . . 157
Frühere Version von RTC-Konfigurationsoptionen wiederherstellen . . . 157
Konfigurationsoptionen für Real Time Compliance (RTC) in andere Gruppen kopieren . . . 157
RTC-Dateiliste bearbeiten . . . 158
Frühere Konfiguration der Überwachungsoptionen von Real Time Compliance (RTC) wiederherstellen . . . 158
Überwachungsoptionen für Real Time Compliance-Dateilisten (RTC) in andere Gruppen kopieren . . . 158
RTC-Prüfung (Real Time Compliance) durchführen . . . 159
Trusted Execution (TE) konfigurieren . . . 159
Konfigurationsoptionen für Trusted Execution (TE) in andere Gruppen kopieren . . . 159
Trusted Execution-Dateiliste bearbeiten . . . 159
Überwachungsoptionen für Trusted Execution-Dateilisten in andere Gruppen kopieren . . . 160
Status anderer PowerSC-Features anzeigen . . . 160
Trusted Execution-Überwachung aktivieren und inaktivieren . . . 161
E-Mail-Benachrichtigung beim Eintreten eines Sicherheitsereignisses senden . . . 161
Mit Berichten arbeiten . . . 162
Berichtsgruppe auswählen . . . 162
Bericht per E-Mail verteilen . . . 163

PowerSC Standard Edition-Befehle 165
Befehl chvfilt . . . 165
Befehl genvfilt . . . 166
Befehl lsvfilt . . . 167
Befehl mkvfilt . . . 168
Befehl pmconf . . . 169
Befehl psconf . . . 173
Befehl pscuiserverctl . . . 181
Befehl pscxpert . . . 183
Befehl rmvfilt . . . 188
Befehl vlantfw . . . 188

Bemerkungen . . . 191
Hinweise zur Datenschutzrichtlinie . . . 192
Marken . . . 193

Index . . . 195

Zu diesem Dokument

Dieses Dokument enthält umfassende Informationen zu Dateien, Systemen und Netzsicherheit für Systemadministratoren.

Hervorhebung

In diesem Dokument werden die folgenden Hervorhebungskonventionen verwendet:

Fettschrift	Befehle, Subroutinen, Schlüsselwörter, Dateien, Strukturen, Verzeichnisse und andere Elemente, deren Namen vom System vorgegeben sind, werden in Fettschrift hervorgehoben. In Fettschrift werden auch grafische Objekte wie Schaltflächen, Beschriftungen und Symbole angegeben, die der Benutzer auswählt.
Kursivschrift	Parameter, die der Benutzer durch Namen oder Werte ersetzen muss, werden in Kursivschrift hervorgehoben.
`Monospace-Schrift`	Beispiele für bestimmte Datenwerte, Beispiele für Textanzeigen, Beispiele für Abschnitte von Programmcode, wie ihn ein Programmierer schreiben könnte, Systemnachrichten und Informationen, die Sie unverändert eingeben müssen, werden in Monospace-Schrift hervorgehoben.

Groß-/Kleinschreibung in AIX

Im Betriebssystem AIX wird grundsätzlich zwischen Groß- und Kleinbuchstaben unterschieden. Beispielsweise können Sie den Befehl **ls** zum Auflisten von Dateien verwenden. Wenn Sie `LS` eingeben, meldet das System, dass der Befehl `nicht gefunden wurde`. Ebenso sind `FILEA`, `FiLea` und `filea` in AIX drei unterschiedliche Dateien, die sich durchaus in einem Verzeichnis befinden können. Stellen Sie stets sicher, dass Sie die richtige Schreibweise verwenden, um unerwünschte Aktionen zu verhindern.

ISO 9000

Für die Entwicklung und Herstellung dieses Produkts wurden Qualitätssysteme gemäß ISO 9000 verwendet.

Neuerungen in PowerSC Standard Edition

Im Folgenden finden Sie Informationen zu neuen oder signifikant geänderten Informationen in der Themensammlung zu den PowerSC Standard Edition-Versionen.

In dieser PDF-Datei sind neue und geänderte Informationen anhand der Änderungsmarkierungen (|) am linken Rand erkennbar.

September 2017

Die folgenden Features wurden der PowerSC-GUI hinzugefügt:

- Sicherheits- und Konformitätsdashboard, in dem Sie auf einen Blick eine Zusammenfassung aller Informationen zu Ihrem Konformitäts- und echtzeitorientierten Dateiintegritätsstatus der höchsten Ebene finden
- Integration mit Virtualisierungsmanagern wie PowerVC durch Open-Stack-Integration, die eine automatisierte und sichere Erkennung von Endpunkten ermöglicht. Außerdem unterstützt die Integration eine Cloudumgebung mit Sicherheitssichtbarkeit ab dem ersten Moment der VM-Erstellung.
- Berichtsfunktionen für die Unterstützung von Prüfungen. Es sind jetzt Übersichts- und Detailberichte zur Konformität und Dateiintegrität in HTML-Format und als CSV-Dateien verfügbar. Sie können die sofortige oder tägliche Verteilung dieser Berichte planen.
- Erweiterter Profileditor, der Ihre Möglichkeiten zur Anpassung von Konformitätsregeln und -profilen verbessert. Es können jetzt Regeln aus mehreren Quellen kombiniert und über die GUI bearbeitet werden.
- Integration mit Informationsmanagern für Sicherheitsereignisse wie QRadar. Es werden syslog-Einträge für aussagefähige Konformitäts- und Dateiintegritätsereignisse bereitgestellt, die die Integration vereinfachen.
- Verbesserte Funktionen für das Rückgängigmachen von Operationen (UNDO), die die komplexe Aufgabe des Widerrufs eines angewendeten Profils vereinfachen. In PowerSC 1.1.6 wurden wichtige Schritte im Hinblick auf reibungslose UNDO-Funktionen für das PCI-Profil unternommen.
- Verbesserte GUI-Skalierbarkeit in Bezug auf die Konformität. Der GUI-Server ist horizontal skalierbar und jede Instanz kann bis zu 1.000 und mehr Endpunkte unterstützen.

Neue Features for Trusted Network Connect Patch Management (TNCPM):

- Es wurde ein Proxy-Server eingeführt, der eine zusätzliche Sicherheitsebene einführt, indem die Isolierung von TNCPM vom Internet zugelassen wird.
- Die Integration vorläufiger Fixes (iFix, Interim Fixes) in TNCPM ist jetzt voll automatisiert. TNCPM kann alle Schwachstellen im Betriebssystem überwachen und Patches anwenden, ohne dass ein Benutzereingriff erforderlich ist.
- Der Download von Open-Source-Packages ist jetzt in TNCPM integriert, was den Open-Source-Workflow optimiert.

Feature für die Erweiterung der Konformitätsfunktionalität:

- Es wurde eine Berichtsoption hinzugefügt, die Details zu den in einem Profil enthaltenen Regeln bereitstellt, wenn das Profil angewendet wird.

PDF-Dateien zu PowerSC Standard Edition

Die Dokumentation zu PowerSC Standard Edition ist auch in Form von PDF-Dateien verfügbar.

- PowerSC Standard Edititon
- Releaseinformationen zu PowerSC Standard Edition

PowerSC Standard Edition-Konzepte

In dieser Übersicht über PowerSC Standard Edition werden die Features, Komponenten und Hardwareunterstützung des Features PowerSC Standard Edition beschrieben.

PowerSC Standard Edition bietet Sicherheit und Steuerungsmöglichkeiten für Systeme, die in einer Cloud oder in virtualisierten Rechenzentren betrieben werden und stellt Unternehmen Anzeige- und Managementfunktionen bereit. PowerSC Standard Edition ist eine Suite von Features, zu denen Security and Compliance Automation, Trusted Boot, Trusted Firewall, Trusted Logging sowie Trusted Network Connect und Patch Management gehören. Die auf der Virtualisierungsebene eingesetzte Sicherheitstechnologie bietet zusätzliche Sicherheit für eigenständige Systeme.

Die folgende Tabelle enthält Details zu den Editionen, den in den Editionen enthaltenen Features, den Komponenten und der prozessorbasierten Hardware, auf der jede einzelne Komponente verfügbar ist.

Tabelle 1. PowerSC Standard Edition-Komponenten, Beschreibung, Betriebssystemunterstützung und Hardwareunterstützung

Komponenten	Beschreibung	Unterstütztes Betriebssystem	Unterstützte Hardware
Security and Compliance Automation	Automatisiert die Festlegung, Überwachung und Prüfung der Sicherheits- und Konformitätskonfiguration für die folgenden Standards: • Payment Card Industry Data Security Standard (PCI DSS) • Sarbanes-Oxley Act and COBIT Compliance (SOX/ COBIT) • U.S. Department of Defense (DoD) STIG • Health Insurance Portability and Accountability Act (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
Trusted Boot	Beurteilt das Boot-Image, das Betriebssystem und die Anwendungen und attestiert deren Vertrauensstellung mithilfe der VTPM-Technologie (Virtual Trusted Platform Module).	• AIX 6 with 6100-07 oder höher • AIX 7 with 7100-01 oder höher	POWER7-Firmware eFW7.4 oder höher
Trusted Firewall	Ermöglicht Zeit- und Ressourceneinsparungen durch Aktivierung des direkten Routings über angegebene virtuelle LANs (VLANs), die von demselben Virtual I/O Server gesteuert werden.	• AIX 6.1 • AIX 7.1 • AIX 7.2 • VIOS Version 2.2.1.4 oder höher	• POWER6 • POWER7 • POWER8 • Virtual I/O Server Version 6.1S oder höher
Trusted Logging	Die Protokolle von AIX werden in Echtzeit lokal in Virtual I/O Server (VIOS) gespeichert. Dieses Feature ermöglicht eine manipulationssichere Protokollierung und eine komfortable Protokollsicherung und -verwaltung.	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8

Tabelle 1. PowerSC Standard Edition-Komponenten, Beschreibung, Betriebssystemunterstützung und Hardwareunterstützung (Forts.)

Komponenten	Beschreibung	Unterstütztes Betriebssystem	Unterstützte Hardware
Trusted Network Connect und Patch Management	Verifiziert, dass alle AIX-Systeme in der virtuellen Umgebung die angegebene Softwareversion und den angegebenen Patch-Level haben, und stellt Management-Tools bereit, mit denen sichergestellt werden kann, dass alle AIX-Systeme die angegebene Softwareversion haben. Stellt Alerts bereit, wenn dem Netz ein veraltetes virtuelles System hinzugefügt wird oder wenn ein Sicherheitspatch ausgegeben wird, der sich auf die Systeme auswirkt.	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
Trusted Network Connect-Client	Der Trusted Network Connect-Client setzt eine der mit dem Betriebssystem aufgelisteten Komponenten voraus.	• AIX 6.1 with 6100-06 oder höher • SUMA-Konsolensystem (Service Update Management Assistant) von AIX Version 7.1 in der SUMA-Umgebung für das Patch-Management • SUMA-Konsolensystem (Service Update Management Assistant) von AIX Version 7.2.1 in der SUMA-Umgebung für das Patch-Management	

PowerSC Standard Edition installieren

Sie müssen für jede spezielle Funktion von PowerSC Standard Edition eine Dateigruppe installieren.

Die folgenden Dateigruppen sind für PowerSC Standard Edition und die grafische Benutzerschnittstelle von PowerSC verfügbar:

- `powerscStd.ice`: Wird auf AIX-Systemen installiert, die das PowerSC Standard Edition-Feature für die Automation von Sicherheit und Konformität (Security and Compliance Automation) erfordern. Das Konformitätsprogramm erfordert mindestens 5 MB verfügbaren Plattenspeicherplatz im Dateisystem "/".
- `powerscStd.vtpm`: Wird auf AIX-Systemen installiert, die das PowerSC Standard Edition-Feature für vertrauenswürdige Bootvorgänge (Trusted Boot) erfordern. Sie können die Dateigruppe "powerscStd.vtpm" vom AIX-Basisdatenträger oder von https://www-01.ibm.com/marketing/iwm/iwm/web/preLogin.do?source=aixbp&S_PKG=vtpm abrufen.
- `powerscStd.vlog`: Wird auf AIX-Systemen installiert, die das PowerSC Standard Edition-Feature für vertrauenswürdige Protokollierung (Trusted Logging) erfordern.
- `powerscStd.tnc_pm`: Wird auf AIX Version 7.1 TL4 oder höher mit dem SUMA-Konsolensystem (Service Update Management Assistant) in der SUMA-Umgebung für Patch Management Version 7.2.1.0 installiert. Für eine sichere Übertragung vorläufiger Fixes von der IBM Security-Website muss Curl 7.52.1-1 auf dem TNC Patch Management-Server installiert werden.
- `powerscStd.svm`: Wird auf AIX-Systemen installiert, die vom Routing-Feature von PowerSC Standard Edition profitieren können.
- `powerscStd.rtc`: Wird auf AIX-Systemen installiert, die das PowerSC Standard Edition-Feature für Echtzeitkonformität (Real Time Compliance) erfordern.
- `powerscStd.uiAgent.rte`: Wird auf AIX-Systemen installiert, die über die grafische Benutzerschnittstelle von PowerSC verwaltet werden. Für die Installation der Version 116 der Dateigruppe "powerscStd.uiAgent.rte" wird die Dateigruppe "powerscStd.ice" der Version 115 oder höher vorausgesetzt.
- `powerscStd.uiServer.rte`: Wird auf dem AIX-System installiert, das speziell für die Ausführung des PowerSC-GUI-Servers konfiguriert ist.

Sie können PowerSC Standard Edition und die grafische Benutzerschnittstelle von PowerSC über eine der folgenden Schnittstellen installieren:

- Befehl **installp** in der Befehlszeilenschnittstelle
- SMIT-Schnittstelle

Führen Sie zum Installieren von PowerSC Standard Edition über die SMIT-Schnittstelle die folgenden Schritte aus:

1. Führen Sie den folgenden Befehl aus:
   ```
   % smitty installp
   ```
2. Wählen Sie die Option **Software installieren** aus.
3. Wählen Sie die Eingabeeinheit oder das Eingabeverzeichnis für die Software aus, um die Position und die Installationsdatei des IBM Compliance Expert-Installationsimage anzugeben. Wenn das Installationsimage beispielsweise den Verzeichnispfad und den Dateinamen `/usr/sys/inst.images/powerscStd.vtpm` hat, müssen Sie den Dateipfad im Feld **EINGABE** eingeben.
4. Lesen Sie die Lizenzvereinbarung und akzeptieren Sie sie. Akzeptieren Sie die Lizenzvereinbarung, indem Sie mit dem Abwärtspfeil zu **Neue Lizenzvereinbarungen akzeptieren** navigieren, diese Option auswählen und dann die Tabulatortaste drücken, um den Wert in **Ja** zu ändern.
5. Drücken Sie die Eingabetaste, um die Installation zu starten.
6. Vergewissern Sie sich, dass nach Abschluss der Installation der Befehlsstatus **OK** angezeigt wird.

Weitere Informationen zum Installieren der grafischen Benutzerschnittstelle von PowerSC finden Sie unter „PowerSC-GUI installieren" auf Seite 142.

Softwarelizenz anzeigen

Die Softwarelizenz kann in der Befehlszeilenschnittstelle mit dem folgenden Befehl angezeigt werden:

```
% installp –lE –d Pfad/Dateiname
```

Pfad/Dateiname gibt das PowerSC Standard Edition-Installationsimage an.

Sie könnten beispielsweise den folgenden Befehl in der Befehlszeilenschnittstelle eingeben, um die Lizenzinformationen für PowerSC Standard Edition anzugeben:

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

Zugehörige Konzepte:

„PowerSC Standard Edition-Konzepte" auf Seite 5
In dieser Übersicht über PowerSC Standard Edition werden die Features, Komponenten und Hardwareunterstützung des Features PowerSC Standard Edition beschrieben.

„Trusted Boot installieren" auf Seite 109
Für die Installation von Trusted Boot sind verschiedene Hardware- und Softwarekonfigurationen erforderlich.

Zugehörige Tasks:

„Trusted Firewall installieren" auf Seite 117
Die Installation von PowerSC Trusted Firewall gleicht der Installation anderer PowerSC-Features.

„Trusted Logging installieren" auf Seite 124
Sie können das PowerSC-Feature Trusted Logging über die Befehlszeilenschnittstelle oder mit dem SMIT-Tool installieren.

„TNC-Komponenten konfigurieren" auf Seite 130
Jede der TNC-Komponenten (Trusted Network Connect) muss für die Ausführung in Ihrer speziellen Umgebung konfiguriert werden.

Automation von Sicherheit und Konformität

AIX Profile Manager verwaltet vordefinierte Profile für Sicherheit und Konformität. Das Feature PowerSC Real Time Compliance überwacht aktivierte AIX-Systeme fortlaufend, um sicherzustellen, dass sie konsistent und sicher konfiguriert sind.

Die XML-Profile automatisieren die empfohlene AIX-Systemkonfiguration von IBM, um die Konsistenz mit Payment Card Data Security Standard, Sarbanes-Oxley Act oder U.S. Department of Defense UNIX Security Technical Implementation Guide und Health Insurance Portability and Accountability Act (HIPAA) zu gewährleisten. Die Organisationen, die die Sicherheitsstandards einhalten, müssen die vordefinierten Systemsicherheitseinstellungen verwenden.

AIX Profile Manager wird als IBM® Systems Director-Plug-in eingesetzt, das die Anwendung von Sicherheitseinstellungen, die Überwachung von Sicherheitseinstellungen und die Prüfung von Sicherheitseinstellungen für das Betriebssystem AIX und VIOS-Systeme (Virtual I/O Server) vereinfacht. Zur Verwendung des Features für die Einhaltung von Sicherheitsbestimmungen muss die PowerSC-Anwendung auf den verwalteten AIX-Systemen installiert werden, die den Konformitätsstandards entsprechen. Das Feature Security and Compliance Automation ist in PowerSC Standard Edition enthalten.

Das PowerSC Standard Edition-Installationspaket 5765-PSE muss auf verwalteten AIX-Systemen installiert werden. Das Installationspaket installiert die Dateigruppe `powerscStd.ice`, die auf dem System mit AIX Profile Manager oder mit dem Befehl **pscxpert** implementiert werden kann. Zur Verwaltung und Verbesserung der XML-Profile wird PowerSC mit ICEE-Konformität (IBM Compliance Expert Express) aktiviert. Die XML-Profile werden von AIX Profile Manager verwaltet.

Anmerkung: Installieren Sie alle Anwendungen auf dem System, bevor Sie ein Sicherheitsprofil anwenden.

Security and Compliance Automation-Konzepte

Das PowerSC-Feature Security and Compliance Automation ist eine automatisierte Methode für die Konfiguration und Prüfung von AIX-Systemen entsprechend den Standards U.S. Department of Defense (DoD) Security Technical Implementation Guide (STIG), Payment Card Industry (PCI) Data Security Standard (DSS), Sarbanes-Oxley Act, COBIT (SOX/COBIT) und Health Insurance Portability and Accountability Act (HIPAA).

Mithilfe von PowerSC können die Konfiguration und Überwachung von Systemen überwacht werden, die mit Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.2, 2.0 oder 3.0 kompatibel sein müssen. Deshalb ist das PowerSC-Feature Security and Compliance Automation eine genaue und vollständige Methode für die Automation von Sicherheitskonfigurationen, mit deren Hilfe die IT-Konformitätsanforderungen von DoD UNIX STIG, PCI DSS, Sarbanes-Oxley Act, COBIT (SOX/COBIT) und Health Insurance Portability and Accountability Act (HIPAA) eingehalten werden können.

Anmerkung: Das PowerSC-Feature Security and Compliance Automation aktualisiert die vorhandenen XML-Profile, die von IBM Compliance Expert Express (ICEE) verwendet werden. Die PowerSC Standard Edition-XML-Profile können ähnlich wie bei ICEE auch mit dem Befehl **pscxpert** verwendet werden.

Die mit PowerSC Standard Edition bereitgestellten vorkonfigurierten Konformitätsprofile verringern den Verwaltungsaufwand, weil die Interpretation der Konformitätsdokumentation und die Implementierung der Standards als spezielle Systemkonfigurationsparameter wegfallen. Diese Technologie reduziert durch Automation der Prozesse den Aufwand für die Konformitätskonfiguration und -prüfung. IBMPowerSC

Standard Edition ist so konzipiert, dass die Systemvoraussetzungen für die Konformität mit externen Standards effizient verwaltet werden können, um so den Aufwand zu reduzieren und die Konformität zu verbessern.

Konformität mit Department of Defense-STIG

Das US-Verteidigungsministerium (DoD, Department of Defense) setzt Computersysteme mit hoher Sicherheit voraus. Diese vom DoD definierte Stufe von Sicherheit und Qualität entspricht der Qualität und Kundenbasis von AIX auf Power Systems-Servern.

Ein sicheres Betriebssystem wie AIX muss korrekt konfiguriert werden, um die angegebenen Sicherheitsziele zu erfüllen. Das DoD hat die Notwendigkeit von Sicherheitskonfigurationen aller Betriebssysteme in der Anordnung 8500.1 erkannt. Diese Anordnung hat die Richtlinie etabliert und der Defense Information Security Agency (DISA) in den USA die Verantwortung für die Bereitstellung von Anweisungen für die Sicherheitskonfiguration zugewiesen.

DISA hat die Prinzipien und Richtlinien im Security Technical Implementation Guide (STIG) für UNIX entwickelt, der eine Umgebung beschreibt, die mindestens den Sicherheitsanforderungen von DoD-Systemen entspricht, die mit MAC-Schutzstufe II (Mission Assurance Category), die sensible Informationen umfasst, betrieben werden. Das DoD hat strikte IT-Sicherheitsanforderungen aufgestellt und die Details der erforderlichen Konfigurationseinstellungen aufgelistet, um sicherzustellen, dass das System sicher arbeitet. Sie können die erforderlichen Expertenanweisungen nutzen. PowerSC Standard Edition unterstützt Sie bei der Automatisierung der Konfiguration von Einstellungen gemäß DoD-Definition.

Anmerkung: Alle angepassten Scriptdateien, die zur Aufrechterhaltung der DoD-Konformität bereitgestellt werden, sind im Verzeichnis `/etc/security/pscexpert/dodv2` enthalten.

PowerSC Standard Edition unterstützt die Anforderungen von Version 1, Release 2 des AIX-DoD-STIG. In den folgenden Tabellen finden Sie eine Zusammenfassung der Anforderungen, in denen auch beschrieben wird, wie Sie diese Konformität sicherstellen.

Tabelle 2. Allgemeine DoD-Anforderungen

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
AIX00020	2	Die AIX Trusted Computing Base-Software muss implementiert werden.	**Position** `/etc/security/pscexpert/dodv2/trust` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
AIX00040	2	Der Befehl **securetcpip** muss verwendet werden.	**Position** `/etc/security/pscexpert/dodv2/dodsecuretcpip` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
AIX00060	2	Das System muss wöchentlich auf nicht berechtigte `setuid`-Dateien und nicht autorisierte Änderungen berechtigter `setuid`-Dateien hin überprüft werden.	**Position** `/etc/security/pscexpert/dodv2/trust` **Konformitätsaktion** Prüft wöchentlich, ob Änderungen an den angegebenen Dateien vorgenommen wurden.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
AIX00080	1	Das Attribut `SYSTEM` darf für keinen Account auf *none* gesetzt werden.	**Position** `/etc/security/pscexpert/dodv2/SYSattr` **Konformitätsaktion** Stellt sicher, dass das angegebene Attribut auf einen anderen Wert als *none* gesetzt ist. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
AIX00200	2	Das System darf keine gezielten Broadcasts durch das Gateway zulassen.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `direct_broadcast` auf *0*.
AIX00210	2	Das System muss einen Schutz vor ICMP-Attacken (Internet Control Message Protocol) in TCP-Verbindungen bereitstellen.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `tcp_icmpsecure` auf *1*.
AIX00220	2	Das System muss den TCP-Stack vor Attacken mit Verbindungsrücksetzungen, Synchronisationen (SYN) und Dateninjection schützen.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Stellt sicher, dass der Wert für die Netzoption `tcp_tcpsecure` auf *7* gesetzt ist.
AIX00230	2	Das System muss einen Schutz vor Attacken mit IP-Fragmentierung bereitstellen.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `ip_nfrag` auf *200*.
AIX00300	1,2,3	Auf dem System darf der Service `bootp` nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert den angegebenen Service.
AIX00310	2	Die `/etc/ftpaccess.ctl`-Dateien müssen vorhanden sein.	**Position** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Konformitätsaktion** Stellt sicher, dass die Datei vorhanden ist.
GEN000020	2	Das System muss beim Start im Einzelbenutzermodus eine Authentifizierung anfordern.	**Position** `/etc/security/pscexpert/dodv2/rootpasswd_home` **Konformitätsaktion** Stellt sicher, dass der Root-Account für alle bootfähige Partitionen ein Kennwort in der Datei `/etc/security/passwd` hat. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN000100	1	Das Betriebssystem muss ein unterstütztes Release sein.	**Position** `/etc/security/pscexpert/dodv2/dodv2cat1` **Konformitätsaktion** Zeigt die Ergebnisse der angegebenen Regeltests an.
GEN000120	2	Die aktuellsten Patches und Updates für die Systemsicherheit müssen installiert sein.	**Position** `/usr/sbin/instfix -i` `/etc/security/pscexpert/dodv2/dodv2cat1` **Konformitätsaktion** Muss mit dem Feature "Trusted Network Connect" konfiguriert werden.
GEN000140	2	Das System muss wöchentlich auf nicht berechtigte `setuid`-Dateien und nicht autorisierte Änderungen berechtigter `setuid`-Dateien hin überprüft werden.	**Position** `/etc/security/pscexpert/dodv2/trust` **Konformitätsaktion** Prüft wöchentlich, ob Änderungen an den angegebenen Dateien vorgenommen wurden.
GEN000220	2	Das System muss wöchentlich auf nicht berechtigte `setuid`-Dateien und nicht autorisierte Änderungen berechtigter `setuid`-Dateien hin überprüft werden.	**Position** `/etc/security/pscexpert/dodv2/trust` **Konformitätsaktion** Prüft wöchentlich, ob Änderungen an den angegebenen Dateien vorgenommen wurden.
GEN000240	2	Die Systemuhr muss mit einer autoritativen DoD-Zeitquelle synchronisiert werden.	**Position** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Konformitätsaktion** Stellt sicher, dass die Systemuhr kompatibel ist.
GEN000241	2	Die Systemuhr muss kontinuierlich oder mindestens einmal täglich synchronisiert werden.	**Position** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Konformitätsaktion** Stellt sicher, dass die Systemuhr kompatibel ist.
GEN000242	2	Das System muss mindestens zwei Zeitquellen für die Synchronisation der Systemzeit verwenden.	**Position** `/etc/security/pscexpert/dodv2/dodv2netrules` **Konformitätsaktion** Stellt sicher, dass mindestens eine Zeitquelle für die Synchronisation der Systemzeit verwendet wird.
GEN000280	2	Direktanmeldungen an den folgenden Accounttypen dürfen nicht zugelassen werden: • application • default • shared • utility	**Position** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Konformitätsaktion** Verhindert Direktanmeldungen an den angegebenen Accounts.
GEN000290	2	Das System darf keine unnötigen Accounts haben.	**Position** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Konformitätsaktion** Stellt sicher, dass keine nicht verwendeten Accounts vorhanden sind.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN000300 (zu GEN000320, GEN000380, GEN000880 gehörig)	2	Alle Accounts auf dem System müssen eindeutige Benutzer- oder Accountnamen und eindeutige Benutzer- oder Accountkennwörter haben.	**Position** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Konformitätsaktion** Stellt sicher, dass alle Accounts die angegebenen Anforderungen erfüllen. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN000320 (zu GEN000300, GEN000380, GEN000880 gehörig)	2	Alle Accounts auf dem System müssen eindeutige Benutzer- oder Accountnamen und eindeutige Benutzer- oder Accountkennwörter haben.	**Position** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Konformitätsaktion** Stellt sicher, dass alle Accounts die angegebenen Anforderungen erfüllen. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN000340	2	Benutzer-IDs (UIDs) und Gruppen-IDs (GIDs), die für Systemaccounts reserviert sind, dürfen keinen anderen Accounts bzw. Gruppen zugeordnet werden.	**Position** `/etc/security/pscexpert/dodv2/account` **Konformitätsaktion** Diese Einstellung wird automatisch aktiviert, um diese Regel durchzusetzen.
GEN000360	2	Benutzer-IDs (UIDs) und Gruppen-IDs (GIDs), die für Systemaccounts reserviert sind, dürfen keinen anderen Accounts bzw. Gruppen zugeordnet werden.	**Position** `/etc/security/pscexpert/dodv2/account` **Konformitätsaktion** Diese Einstellung wird automatisch aktiviert, um diese Regel durchzusetzen.
GEN000380 (zu GEN000300, GEN000320, GEN000880 gehörig)	2	Alle Accounts auf dem System müssen eindeutige Benutzer- oder Accountnamen und eindeutige Benutzer- oder Accountkennwörter haben.	**Position** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Konformitätsaktion** Stellt sicher, dass alle Accounts die angegebenen Anforderungen erfüllen.
GEN000400	2	Das DoD-Anmeldebanner muss umittelbar vor oder als Teil der Anmeldedialoge in der Konsole angezeigt werden.	**Position** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Konformitätsaktion** Zeigt das erforderliche Banner an.
GEN000402	2	Das DoD-Anmeldebanner muss umittelbar vor oder als Teil der Anmeldedialoge in der grafischen Desktopumgebung angezeigt werden.	**Position** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Konformitätsaktion** Das Anmeldebanner wird auf das DoD-Banner gesetzt.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN000410	2	Der FTPS- (File Transfer Protocol over SSL) oder FTP-Service (File Transfer Protocol) auf dem System muss mit dem DoD-Anmeldebanner konfiguriert werden.	**Position** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Konformitätsaktion** Zeigt das Banner an, wenn Sie FTP verwenden.
GEN000440	2	Erfolgreiche und nicht erfolgreiche An- und Abmeldeversuche müssen aufgezeichnet werden.	**Position** `/etc/security/pscexpert/dodv2/loginout` **Konformitätsaktion** Aktiviert die erforderliche Protokollierung.
GEN000452	2	Das System muss das Datum und die Uhrzeit der letzten erfolgreichen Accountammeldung zum Zeitpunkt jeder Anmeldung anzeigen.	**Position** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Konformitätsaktion** Zeigt die erforderlichen Informationen an.
GEN000460	2	Diese Regel inaktiviert einen Account nach drei aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen.	**Position** `/etc/security/pscexpert/dodv2/chusrattrdod` **Konformitätsaktion** Setzt den Grenzwert für Anmeldeversuche auf den angegebenen Wert.
GEN000480	2	Diese Regel setzt die Anmeldeverzögerungszeit auf 4 Sekunden.	**Position** `/etc/security/pscexpert/dodv2/chdefstanzadod` **Konformitätsaktion** Setzt die Anmeldeverzögerungszeit auf den erforderlichen Wert.
GEN000540	2	Diese Regel stellt sicher, dass die globalen Kennwortkonfigurationsdateien des Systems entsprechend den Kennwortanforderungen konfiguriert werden.	**Position** `/etc/security/pscexpert/dodv2/chusrattrdod` **Konformitätsaktion** Setzt die erforderlichen Kennworteinstellungen.
GEN000560	1	Alle Accounts auf dem System müssen gültige Kennwörter haben.	**Position** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Konformitätsaktion** Stellt sicher, dass Accounts Kennwörter haben.
GEN000580	2	Diese Regel stellt sicher, dass alle Kennwörter mindestens 14 Zeichen enthalten.	**Position** `/etc/security/pscexpert/dodv2/chusrattrdod` **Konformitätsaktion** Setzt die Mindestkennwortlänge auf 14 Zeichen.
GEN000585	2	Das System muss einen gemäß Federal Information Processing Standards (FIPS) 140-2 genehmigten kryptografischen Hashalgorithmus für die Generierung von Accountkennworthashwerten verwenden.	**Position** `/etc/security/pscexpert/dodv2/fipspasswd` **Konformitätsaktion** Stellt sicher, dass für die Kennworthashwerte ein genehmigter Hashalgorithmus verwendet wird.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN000590	2	Das System muss einen gemäß Federal Information Processing Standards (FIPS) 140-2 genehmigten kryptografischen Hashalgorithmus für die Generierung von Accountkennworthashwerten verwenden.	**Position** `/etc/security/pscexpert/dodv2/fipspasswd` **Konformitätsaktion** Stellt sicher, dass für die Kennworthashwerte ein genehmigter Hashalgorithmus verwendet wird.
GEN000595	2	Für die Generierung der Kennworthashwerte, die auf dem System gespeichert werden, muss ein gemäß FIPS 140-2 genehmigter kryptografischer Hashalgorithmus verwendet werden.	**Position** `/etc/security/pscexpert/dodv2/fipspasswd` **Konformitätsaktion** Stellt sicher, dass für die Kennworthashwerte ein genehmigter Hashalgorithmus verwendet wird.
GEN000640	2	Diese Regel setzt mindestens ein nicht alphabetisches Zeichen in einem Kennwort voraus.	**Position** `/etc/security/pscexpert/dodv2/chusrattrdod` **Konformitätsaktion** Legt die Mindestanzahl nicht alphabetischer Zeichen in einem Kennwort auf 1.
GEN000680	2	Diese Regel stellt sicher, dass Kennwörter nicht mehr als drei identische aufeinanderfolgende Zeichen enthalten.	**Position** `/etc/security/pscexpert/dodv2/chusrattrdod` **Konformitätsaktion** Setzt die Mindestanzahl identischer aufeinanderfolgender nicht alphabetischer Zeichen in einem Kennwort auf 3.
GEN000700	2	Diese Regel stellt sicher, dass die globalen Kennwortkonfigurationsdateien des Systems entsprechend den Kennwortanforderungen konfiguriert werden.	**Position** `/etc/security/pscexpert/dodv2/chusrattrdod` **Konformitätsaktion** Stellt sicher, dass das die Kennwortkonfigurationsdateien die Anforderungen erfüllen.
GEN000740	2	Alle Accountkennwörter für die nicht interaktive und automatisierte Verarbeitung müssen gesperrt werden (GEN000280). Direktanmeldungen an gemeinsam genutzten oder Standardanwendungs- oder -dienstprogrammaccounts dürfen nicht zugelassen werden. (GEN002640) Standardsystemaccounts müssen inaktiviert oder entfernt werden.	**Position** `/etc/security/pscexpert/dodv2/loginout` `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Konformitätsaktion** Diese Einstellung wird automatisch aktiviert.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN000740	2	Alle Accountkennwörter für die nicht interaktive und automatisierte Verarbeitung müssen mindestens einmal pro Jahr geändert oder ganz gesperrt werden.	**Position** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Konformitätsaktion** Stellt sicher, dass die angegebenen Kennwörter jährlich geändert oder gesperrt werden.
GEN000750	2	Diese Regel erfordert, dass neue Kennwörter mindestens 4 Zeichen enthalten, die nicht im alten Kennwort enthalten waren.	**Position** `/etc/security/pscexpert/dodv2/chusrattrdod` **Konformitätsaktion** Setzt die Mindestanzahl neuer Zeichen, die in einem neuen Kennwort erforderlich sind, auf 4.
GEN000760	2	Accounts müssen nach 35 Tagen Inaktivität gesperrt werden.	**Position** `/etc/security/pscexpert/dodv2/disableacctdod` **Konformitätsaktion** Sperrt Accounts nach 35 Tagen Inaktivität.
GEN000790	2	Das System muss die Verwendung von Wörtern aus einem Wörterbuch für Kennwörter verhindern.	**Position** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Konformitätsaktion** Stellt sicher, dass das festgelegte Standardkennwort sicher ist.
GEN000800	2	Diese Regel stellt sicher, dass die letzten fünf Kennwörter nicht wiederverwendet werden.	**Position** `/etc/security/pscexpert/dodv2/chusrattrdod` **Konformitätsaktion** Stellt sicher, dass das neue Kennwort keines der zuletzt verwendeten 5 Kennwörter ist.
GEN000880 (zu GEN000300, GEN000320, GEN000380 gehörig)	2	Alle Accounts auf dem System müssen eindeutige Benutzer- oder Accountnamen und eindeutige Benutzer- oder Accountkennwörter haben.	**Position** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Konformitätsaktion** Stellt sicher, dass alle Accounts die angegebenen Anforderungen erfüllen.
GEN000900	3	Das Ausgangsverzeichnis des Rootbenutzers darf nicht das Stammverzeichnis (/) sein.	**Position** `/etc/security/pscexpert/dodv2/rootpasswd_home` **Konformitätsaktion** Stellt sicher, dass das System die angegebene Voraussetzung erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN000940	2	Der Suchpfad für die ausführbaren Dateien des Root-Accounts muss der Anbieterstandardwert sein und darf nur absolute Pfade enthalten.	**Position** `/etc/security/pscexpert/dodv2/fixpathvars` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN000945	2	Der Bibliothekssuchpfad des Root-Accounts muss der Systemstandardwert sein und darf nur absolute Pfade enthalten.	**Position** `/etc/security/pscexpert/dodv2/fixpathvars` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN000950	2	Die Liste der vorinstallierten Bibliotheken des Root-Accounts muss leer sein.	**Position** `/etc/security/pscexpert/dodv2/fixpathvars` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN000960 (zu GEN003000, GEN003020, GEN003160, GEN003360, GEN003380 gehörig)	2	Der Root-Account darf keine Verzeichnisse mit globalem Schreibzugriff in seinem Suchpfad für ausführbare Dateien enthalten.	**Position** `/etc/security/pscexpert/dodv2/rmwwpaths` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN000980	2	Das System muss Direktanmeldungen des Root-Accounts verhindern, sofern sie nicht über die Systemkonsole erfolgen.	**Position** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN001000	2	Ferne Konsolen müssen inaktiviert oder vor unbefugtem Zugriff geschützt werden.	**Position** `/etc/security/pscexpert/dodv2/remoteconsole` **Konformitätsaktion** Stellt sicher, dass die angegebenen Konsolen inaktiviert werden.
GEN001020	2	Der Root-Account darf nicht für Direktanmeldungen verwendet werden.	**Position** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Konformitätsaktion** Inaktiviert Direktanmeldungen des Root-Accounts.
GEN001060	2	Das System muss erfolgreiche und nicht erfolgreiche Zugriffsversuche auf den Root-Account protokollieren.	**Position** `/etc/security/pscexpert/dodv2/loginout` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN001100	1	Rootkennwörter dürfen nie in Textform über ein Netz übertragen werden.	**Position** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN001120	2	Das System darf keine Rootanmeldungen mit dem Protokoll SSH zulassen.	**Position** /etc/security/pscexpert/dodv2/sshDoDconfig **Konformitätsaktion** Inaktiviert Rootanmeldungen für SSH.
GEN001440	3	Allen interaktiven Benutzern muss in der Datei /etc/passwd ein Ausgangsverzeichnis zugeordnet werden.	**Position** /etc/security/pscexpert/dodv2/grpusrpass_chk **Konformitätsaktion** Stellt sicher, dass alle interaktiven Benutzer das angegebene Verzeichnis haben.
GEN001475	2	Die Datei /etc/group darf keine Hashwerte für Gruppenkennwörter enthalten.	**Position** /etc/security/pscexpert/dodv2/passwdhash **Konformitätsaktion** Stellt sicher, dass keine Gruppenkennworthashwerte in der angegebenen Datei enthalten sind. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei DoDv2_to_AIXDefault.xml auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001600	2	Die Suchpfade für ausführbare Dateien von Ausführungssteuerscripts dürfen nur absolute Pfade enthalten.	**Position** /etc/security/pscexpert/dodv2/fixpathvars **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei DoDv2_to_AIXDefault.xml auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001605	2	Die Bibliothekssuchpfade von Ausführungssteuerscripts dürfen nur absolute Pfade enthalten.	**Position** /etc/security/pscexpert/dodv2/fixpathvars **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei DoDv2_to_AIXDefault.xml auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001610	2	Die Listen vorinstallierter Bibliotheken von Ausführungssteuerscripts dürfen nur absolute Pfade enthalten.	**Position** /etc/security/pscexpert/dodv2/fixpathvars **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei DoDv2_to_AIXDefault.xml auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN001840	2	Die Suchpfade für ausführbare Dateien aller globalen Initialisierungsdateien dürfen nur absolute Pfade enthalten.	**Position** `/etc/security/pscexpert/dodv2/fixpathvars` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001845	2	Die Bibliothekssuchpfade aller globalen Initialisierungsdateien dürfen nur absolute Pfade enthalten.	**Position** `/etc/security/pscexpert/dodv2/fixpathvars` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001850	2	Die Listen vorinstallierter Bibliotheken aller globalen Initialisierungsdateien dürfen nur absolute Pfade enthalten.	**Position** `/etc/security/pscexpert/dodv2/fixpathvars` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001900	2	Die Suchpfade für ausführbare Dateien aller lokalen Initialisierungsdateien dürfen nur absolute Pfade enthalten.	**Position** `/etc/security/pscexpert/dodv2/fixpathvars` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001901	2	Die Bibliothekssuchpfade aller lokalen Initialisierungsdateien dürfen nur absolute Pfade enthalten.	**Position** `/etc/security/pscexpert/dodv2/fixpathvars` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN001902	2	Die Listen vorinstallierter Bibliotheken aller lokalen Initialisierungsdateien dürfen nur absolute Pfade enthalten.	**Position** `/etc/security/pscexpert/dodv2/fixpathvars` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001940	2	Benutzerinitialisierungsdateien dürfen keine Programme mit globalem Schreibzugriff ausführen.	**Position** `/etc/security/pscexpert/dodv2/rmwwpaths` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN001980	2	Die Dateien `.rhosts`, `.shosts`, `hosts.equiv`, `shosts.equiv`, `/etc/passwd`, `/etc/shadow` und `/etc/group` dürfen kein Pluszeichen (+) enthalten, wenn keine Einträge für NIS+-Netzgruppen definiert werden.	**Position** `/etc/security/pscexpert/dodv2/dodv2netrules` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien die angegebenen Voraussetzungen erfüllen.
GEN002000	2	Es darf keine `.netrc`-Dateien auf dem System geben.	**Position** `/etc/security/pscexpert/dodv2/dodv2netrules` **Konformitätsaktion** Stellt sicher, dass keine der angegebenen Dateien auf dem System vorhanden sind. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN002020	2	Alle Dateien `.rhosts`, `.shosts` und `hosts.equiv` dürfen nur vertrauenswürdige Host/Benutzer-Paare enthalten.	**Position** `/etc/security/pscexpert/dodv2/dodv2netrules` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien diese Anforderung erfüllen.
GEN002040	1	Diese Regel inaktiviert die Dateien `.rhosts`, `.shosts`, `hosts.equiv` und `shosts.equiv`.	**Position** `/etc/security/pscexpert/dodv2/mvhostsfilesdod` **Konformitätsaktion** Inaktiviert die angegebenen Dateien.
GEN002120	1,2	Diese Regel prüft und konfiguriert Benutzershells.	**Position** `/etc/security/pscexpert/dodv2/usershells` **Konformitätsaktion** Erstellt die erforderlichen Shells. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN002140	1,2	Alle in der `/etc/passwd`-Liste referenzierten Shells müssen in der Datei `/etc/shells` aufgelistet werden. Ausgenommen sind Shells, die zur Verhinderung von Anmeldungen angegeben werden.	**Position** `/etc/security/pscexpert/dodv2/usershells` **Konformitätsaktion** Stellt sicher, dass die Shells in den richtigen Dateien aufgelistet sind. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN002280	2	Einheitendateien und -verzeichnisse dürfen nur von Benutzern mit einem Systemaccount bzw. gemäß Anbieterkonfiguration des Systems modifiziert werden.	**Position** `/etc/security/pscexpert/dodv2/wwdevfiles` **Konformitätsaktion** zeigt Einheitendateien, Einheitenverzeichnisse und alle anderen Dateien auf dem System in nicht öffentlichen Verzeichnissen mit globalem Schreibzugriff angezeigt.
GEN002300	2	Schreib- und oder Leseberechtigung für die für Sicherungen verwendeten Einheitendateien dürfen nur der Rootbenutzer und der Sicherungsbenutzer haben.	**Position** `/etc/security/pscexpert/dodv2/wwdevfiles` **Konformitätsaktion** zeigt Einheitendateien, Einheitenverzeichnisse und alle anderen Dateien auf dem System in nicht öffentlichen Verzeichnissen mit globalem Schreibzugriff angezeigt.
GEN002400	2	Das System muss wöchentlich auf nicht berechtigte `setuid`-Dateien und nicht autorisierte Änderungen berechtigter `setuid`-Dateien hin überprüft werden.	**Position** `/etc/security/pscexpert/dodv2/trust` **Konformitätsaktion** Prüft wöchentlich, ob Änderungen an den angegebenen Dateien vorgenommen wurden. **Anmerkung:** Es werden die beiden neuesten wöchentlichen Protokolle im Verzeichnis `/var/security/pscexpert` miteinander verglichen, um sicherzustellen, dass keine nicht autorisierten Aktivitäten stattgefunden haben.
GEN002420	2	Austauschbare Datenträger, ferne Dateisysteme und alle Dateisysteme, die keine genehmigten `setuid`-Dateien enthalten, müssen mit der Option *nosuid* gemountet werden.	**Position** `/etc/security/pscexpert/dodv2/fsmntoptions` **Konformitätsaktion** Stellt sicher, dass die über Fernzugriff gemounteten Dateisysteme die angegebenen Optionen haben. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN002430	2	Austauschbare Datenträger, ferne Dateisysteme und alle Dateisysteme, die keine genehmigten Gerätedateien enthalten, müssen mit der Option *nodev* gemountet werden.	**Position** `/etc/security/pscexpert/dodv2/fsmntoptions` **Konformitätsaktion** Stellt sicher, dass die über Fernzugriff gemounteten Dateisysteme die angegebenen Optionen haben. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN002480	2	Nur öffentliche Verzeichnisse dürfen Verzeichnisse mit globalem Schreibzugriff sein und Dateien mit globalem Schreibzugriff dürfen sich nur in öffentlichen Verzeichnissen befinden.	**Position** `/etc/security/pscexpert/dodv2/wwdevfiles` `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Meldet, wenn es sich Dateien mit globalem Schreibzugriff nicht in öffentlichen Verzeichnissen befinden.
GEN002640	2	Standardsystemaccounts müssen inaktiviert oder entfernt werden.	**Position** `/etc/security/pscexpert/dodv2/lockacc_rlogin` `/etc/security/pscexpert/dodv2/loginout` **Konformitätsaktion** Inaktiviert Standardsystemaccounts.
GEN002660	2	Die Prüfung (Auditing) muss aktiviert werden.	**Position** `/etc/security/pscexpert/dodv2/dodaudit` **Konformitätsaktion** Aktiviert den Befehl `dodaudit`, der die Prüfung aktiviert.
GEN002720	2	Das Prüfsystem muss so konfiguriert werden, dass fehlgeschlagene Versuche, auf Dateien und Programme zuzugreifen, geprüft werden.	**Position** `/etc/security/pscexpert/dodv2/dodaudit` **Konformitätsaktion** Aktiviert automatisch die angegebene Prüfung.
GEN002740	2	Das Prüfsystem muss so konfiguriert werden, dass das Löschen von Dateien geprüft wird.	**Position** `/etc/security/pscexpert/dodv2/dodaudit` **Konformitätsaktion** Aktiviert automatisch die angegebene Prüfung.
GEN002750	3	Das Prüfsystem muss so konfiguriert werden, dass das Erstellen von Accounts geprüft wird.	**Position** `/etc/security/pscexpert/dodv2/dodaudit` **Konformitätsaktion** Aktiviert automatisch die angegebene Prüfung.
GEN002751	3	Das Prüfsystem muss so konfiguriert werden, dass das die Änderung von Accounts geprüft wird.	**Position** `/etc/security/pscexpert/dodv2/dodaudit` **Konformitätsaktion** Aktiviert automatisch die angegebene Prüfung.
GEN002752	3	Das Prüfsystem muss so konfiguriert werden, dass Accounts, die inaktiviert werden, geprüft werden.	**Position** `/etc/security/pscexpert/dodv2/dodaudit` **Konformitätsaktion** Aktiviert automatisch die angegebene Prüfung.
GEN002753	3	Das Prüfsystem muss so konfiguriert werden, dass die Kündigung von Accounts geprüft wird.	**Position** `/etc/security/pscexpert/dodv2/dodaudit` **Konformitätsaktion** Aktiviert automatisch die angegebene Prüfung.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN002760	2	Das Prüfsystem muss so konfiguriert werden, dass alle administrativen, privilegierten und Sicherheitsaktionen geprüft werden.	**Position** `/etc/security/pscexpert/dodv2/dodaudit` **Konformitätsaktion** Aktiviert automatisch die angegebene Prüfung.
GEN002800	2	Das Prüfsystem muss so konfiguriert werden, dass Anmeldungen, Anmeldungen und Sitzungsinitialisierungen geprüft werden.	**Position** `/etc/security/pscexpert/dodv2/dodaudit` **Konformitätsaktion** Aktiviert automatisch die angegebene Prüfung.
GEN002820	2	Das Prüfsystem muss so konfiguriert werden, dass alle Änderungen an den eignerdefinierten Zugriffssteuerungsberechtigungen geprüft werden.	**Position** `/etc/security/pscexpert/dodv2/dodaudit` **Konformitätsaktion** Aktiviert automatisch die angegebene Prüfung.
GEN002825	2	Das Prüfsystem muss so konfiguriert werden, dass das Laden und Entladen dynamischer Kernelmodule geprüft werden.	**Position** `/etc/security/pscexpert/dodv2/dodaudit` **Konformitätsaktion** Aktiviert automatisch die angegebene Prüfung.
GEN002860	2	Die Prüfprotokolle müssen täglich gewechselt werden.	**Position** `/etc/security/pscexpert/dodv2/rotateauditdod` **Konformitätsaktion** Stellt sicher, dass die Prüfprotokolle turnusmäßig gewechselt werden.
GEN002960	2	Der Zugriff auf das Dienstprogramm `cron` muss mit der Datei `cron.allow` und/oder der Datei `cron.deny` gesteuert werden.	**Position** `/etc/security/pscexpert/dodv2/limitsysacc` **Konformitätsaktion** Stellt sicher, dass die kompatiblen Grenzwerte aktiviert werden.
GEN003000 (zu GEN000960, GEN003020, GEN003160, GEN003360, GEN003380 gehörig)	2	`Cron` darf keine Programme mit Gruppen- oder globalem Schreibzugriff ausführen.	**Position** `/etc/security/pscexpert/dodv2/rmwwpaths` **Konformitätsaktion** Stellt sicher, dass die kompatiblen Grenzwerte aktiviert werden. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN003020 (zu GEN000960, GEN003000, GEN003160, GEN003360, GEN003380 gehörig)	2	`Cron` darf keine Programme in Verzeichnissen oder Unterverzeichnissen mit globalem Schreibzugriff ausführen.	**Position** `/etc/security/pscexpert/dodv2/rmwwpaths` **Konformitätsaktion** Entfernt die Berechtigung für globalen Schreibzugriff aus den `cron`-Programmverzeichnissen. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN003060	2	Standardsystemaccounts (mit Ausnahme von Root) dürfen nicht in der Datei `cron.allow` aufgelistet werden oder müssen in die Datei `cron.deny` eingeschlossen werden, wenn die Datei `cron.allow` nicht vorhanden ist.	**Position** `cron.allow` oder `cron.deny` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN003160 (zu GEN000960, GEN003000, GEN003020, GEN003360, GEN003380 gehörig)	2	Die `Cron`-Protokollierung muss aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/rmwwpaths` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN003280	2	Der Zugriff auf das Dienstprogramm `at` muss mit den Dateien `at.allow` und `at.deny` gesteuert werden.	**Position** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN003300	2	Die Datei `at.deny` darf, sofern vorhanden, nicht leer sein.	**Position** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN003320	2	Standardsystemaccounts dürfen nicht in der Datei `at.allow` aufgelistet werden oder müssen in die Datei `at.deny` eingeschlossen werden, wenn die Datei `at.allow` nicht vorhanden ist.	**Position** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN003360 (zu GEN000960, GEN003000, GEN003020, GEN003160, GEN003380 gehörig)	2	Der `at`-Dämon darf keine Programme mit Gruppen- oder globalem Schreibzugriff ausführen.	**Position** `/etc/security/pscexpert/dodv2/rmwwpaths` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN003380 (zu GEN000960, GEN003000, GEN003020, GEN003160, GEN003360 gehörig)	2	Der `at`-Dämon darf keine Programme in Verzeichnissen oder Unterverzeichnissen mit globalem Schreibzugriff ausführen.	**Position** `/etc/security/pscexpert/dodv2/rmwwpaths` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN003510	2	Kernelkernspeicherauszüge dürfen nur bei Bedarf aktiviert werden.	**Position** `/etc/security/pscexpert/dodv2/coredumpdev` **Konformitätsaktion** Inaktiviert Kernelkernspeicherauszüge.
GEN003540	2	Das System muss nicht ausführbare Programmstapel verwenden.	**Position** `/etc/security/pscexpert/dodv2/sedconfigdod` **Konformitätsaktion** Erzwingt die Verwendung nicht ausführbarer Programmstacks.
GEN003600	2	Das System darf keine IPv4-Source-Routing-Pakete weiterleiten.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `ipsrcforward` auf *0*.
GEN003601	2	Die Größe für die TCP-Rückstandswarteschlange muss entsprechend definiert werden.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt die Netzoption `clean_partial_ conns` auf den Wert *1*.
GEN003603	2	Das System darf nicht auf ICMPv4-Echoanforderungen (Internet Control Message Protocol Version 4) antworten, die an eine Broadcastadresse gesendet werden.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `bcastping` auf *0*.
GEN003604	2	Das System darf nicht auf Anforderungen mit einer ICMP-Zeitmarke antworten, die an eine Broadcastadresse gesendet werden.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `bcastping` auf *0*.
GEN003605	2	Das System darf kein Reverse-Source-Routing auf TCP-Antworten anwenden.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `nonlocsrcroute` auf *0*.
GEN003606	2	Das System muss verhindern, dass lokale Anwendungen Source-Routing-Pakete generieren.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `ipsrcroutesend` auf *0*.
GEN003607	2	Das System darf keine IPv4-Source-Routing-Pakete akzeptieren.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Inaktiviert die Funktionalität zum Akzeptieren von IPv4-Source-Routing-Paketen.
GEN003609	2	Das System muss IPv4-ICMP-Umleitungsnachrichten ignorieren.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `ipignoreredirects` auf *1*.
GEN003610	2	Das System darf keine IPv4-ICMP-Umleitungsnachrichten senden.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `ipsendredirects` auf *0*.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN003612	2	Das System muss so konfiguriert werden, dass TCP-Syncookies verwendet werden, wenn eine TCP-SYN-Flood auftritt.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `clean_partial _conns` auf *1*.
GEN003640	2	Das Stammdateisystem muss Journaling oder eine andere Methode zur Gewährleistung der Dateisystemkonsistenz verwenden.	**Position** `/etc/security/pscexpert/dodv2/chkjournal` **Konformitätsaktion** Aktiviert Journaling für das Stammdateisystem.
GEN003660	2	Das System muss Informationsdaten zur Authentifizierung protokollieren.	**Position** `/etc/security/pscexpert/dodv2/chsyslogdod` **Konformitätsaktion** Aktiviert die Protokollierung von `auth`- und `info`-Daten.
GEN003700	2	Die Dämonprozesse `inetd` und `xinetd` müssen inaktiviert oder entfernt werden, wenn sie von Netzservices nicht verwendet werden.	**Position** `/etc/security/pscexpert/dodv2/dodv2services` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN003810	2	Die Services `portmap` und `rpcbind` dürfen nur bei Bedarf ausgeführt werden.	**Position** `/etc/security/pscexpert/dodv2/dodv2services` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN003815	2	Die Services `portmap` und `rpcbind` dürfen nur installiert werden, wenn sie verwendet werden.	**Position** `/etc/security/pscexpert/dodv2/dodv2services` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN003820-3860	1,2,3	Die Dämonprozesse `rsh`, `rexexec` und `telnet` und der Service `rlogind` dürfen nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN003865	2	Es dürfen keine Netzanalysetools installiert werden.	**Position** `/etc/security/pscexpert/dodv2/dodv2services` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN003900	2	Die Datei `hosts.lpd` (oder eine funktional entsprechende Datei) darf kein Pluszeichen (+) enthalten.	**Position** `/etc/security/pscexpert/dodv2/printers` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN004220	1	Administrationsaccounts dürfen keine Web-Browser ausführen, sofern dies nicht für die lokale Serviceadministration erforderlich ist.	**Position** `/etc/security/pscexpert/dodv2/dodv2cat1` **Konformitätsaktion** Zeigt die Ergebnisse der angegebenen Regeltests an.
GEN004460	2	Diese Regel protokolliert `auth`- und `info`-Daten.	**Position** `/etc/security/pscexpert/dodv2/chsyslogdod` **Konformitätsaktion** Aktiviert die Protokollierung von `auth`- und `info`-Daten.
GEN004540	2	Diese Regel inaktiviert den `sendmail`-Befehl help.	**Position** `/etc/security/pscexpert/dodv2/sendmailhelp` `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Konformitätsaktion** Inaktiviert den angegebenen Befehl.
GEN004580	2	Das System darf keine `.forward` -Dateien verwenden.	**Position** `/etc/security/pscexpert/dodv2/forward` **Konformitätsaktion** Inaktiviert die angegebenen Dateien. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN004600	1	Der `SMTP`-Service muss die aktuelle Version haben.	**Position** `/etc/security/pscexpert/dodv2/SMTP_ver` **Konformitätsaktion** Stellt sicher, dass die aktuelle Version des angegebenen Service aktiv ist. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN004620	2	Auf dem `sendmail`-Server muss das Debugging-Feature inaktiviert sein.	**Position** `/etc/security/pscexpert/dodv2/SMTP_ver` **Konformitätsaktion** Inaktiviert das Debugging-Feature für `sendmail`.
GEN004640	1	Der `SMTP`-Service darf keinen aktiven `uudecode`-Alias haben.	**Position** `/etc/security/pscexpert/dodv2/SMTPuucode` **Konformitätsaktion** Inaktiviert den `uudecode`-Alias.
GEN004710	2	Das unbefugte Umleiten von Mails muss eingeschränkt werden.	**Position** `/etc/security/pscexpert/dodv2/sendmaildod` **Konformitätsaktion** Schränkt das unbefugte Umleiten von Mails ein.
GEN004800	1,2,3	Unverschlüsseltes FTP darf auf dem System nicht verwendet werden.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN004820	2	Anonymous FTP darf auf dem System nur aktiv sein, wenn dies autorisiert ist.	**Position** `/etc/security/pscexpert/dodv2/anonuser` **Konformitätsaktion** Inaktiviert anonymes FTP auf dem System. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN004840	2	Wenn es sich bei dem System um einen Anonymous FTP-Server handelt, muss es im DMZ-Netz (Demilitarized Zone) isoliert werden.	**Position** `/etc/security/pscexpert/dodv2/anonuser` **Konformitätsaktion** Stellt sicher, dass sich ein Anonymous FTP-Server im System im DMZ-Netz befindet.
GEN004880	2	Die Datei `ftpusers` muss vorhanden sein.	**Position** `/etc/security/pscexpert/dodv2/chdodftpusers` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei auf dem System vorhanden ist.
GEN004900	2	Die `ftpusers`-Datei muss die Accountnamen enthalten, die das FTP-Protokoll nicht verwenden dürfen.	**Position** `/etc/security/pscexpert/dodv2/chdodftpusers` **Konformitätsaktion** Stellt sicher, dass die Datei die erforderlichen Accountnamen enthält.
GEN005000	1	Anonymous FTP-Accounts dürfen keine funktionsfähige Shell haben.	**Position** `/etc/security/pscexpert/dodv2/usershells` **Konformitätsaktion** Entfernt Shells aus Anonymous FTP-Accounts. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN005080	1	Der `TFTP`-Dämon muss im sicheren Modus ausgeführt werden, in dem der Zugriff nur auf ein einziges Verzeichnis im Hostdateisystem zugelassen wird.	**Position** `/etc/security/pscexpert/dodv2/tftpdod` **Konformitätsaktion** Stellt sicher, dass der Dämon die angegebenen Anforderungen erfüllt.
GEN005120	2	Der TFTP-Dämon muss entsprechend den Anbieterspezifikationen konfiguriert werden. Dazu gehören ein dedizierter TFTP-Benutzeraccount, eine Nicht-Anmeldeshell wie `/bin/false` und ein Ausgangsverzeichnis, deren Eigner der TFTP-Benutzer ist.	**Position** `/etc/security/pscexpert/dodv2/tftpdod` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN005140	1,2,3	Alle aktiven TFTP-Dämonprozesse müssen im Systemakkreditierungspaket autorisiert und genehmigt sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Stellt sicher, dass der Dämon berechtigt ist.
GEN005160	1,2	Ein X Window System-Host muss `.Xauthority`-Dateien schreiben.	**Position** `/etc/security/pscexpert/dodv2/dodv2disableX` **Konformitätsaktion** Stellt sicher, dass der Host die angegebenen Dateien geschrieben hat.
GEN005200	1,2	X Window System-Anzeigen können nicht öffentlich exportiert werden.	**Position** `/etc/security/pscexpert/dodv2/dodv2disableX` **Konformitätsaktion** Inaktiviert die Verteilung der angegebenen Programme.
GEN005220	1,2	Die Dateien `.Xauthority` und `X*.hosts` (oder funktional entsprechende Dateien) müssen verwendet werden, um den Zugriff auf den X Window System-Server einzuschränken.	**Position** `/etc/security/pscexpert/dodv2/dodv2disableX` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien verfügbar sind, um den Zugriff auf den Server einzuschränken.
GEN005240	1,2	Das Dienstprogramm .Xauthority darf nur den Zugriff auf berechtigte Hosts zulassen.	**Position** `/etc/security/pscexpert/dodv2/dodv2disableX` **Konformitätsaktion** Stellt sicher, dass der Zugriff auf berechtigte Hosts beschränkt wird.
GEN005260	2	Diese Regel inaktiviert X Window System-Verbindungen und den XServer-Anmeldemanager.	**Position** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Konformitätsaktion** Inaktiviert die erforderlichen Verbindungen und den Anmeldemanager.
GEN005280	1,2,3	Auf dem System darf der Service `UUCP` nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN005300	2	Für SNMP-Communitys müssen andere Enstellungen als die Standardeinstellungen definiert werden.	**Position** `/etc/security/pscexpert/dodv2/chsnmp` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005305	2	Der SNMP-Service darf nur SNMPv3 oder eine neuere Version verwenden.	**Position** `/etc/security/pscexpert/dodv2/chsnmp` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005306	2	Der SNMP-Service muss die Verwendung von FIPS 140-2 anfordern.	**Position** `/etc/security/pscexpert/dodv2/chsnmp` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN005440	2	Das System muss einen fernen syslog-Server (Protokollhost) verwenden.	**Position** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Konformitätsaktion** Stellt sicher, dass das System einen fernen syslog-Server verwendet.
GEN005450	2	Das System muss einen fernen syslog-Server (Protokollhost) verwenden.	**Position** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Konformitätsaktion** Stellt sicher, dass das System einen fernen syslog-Server verwendet.
GEN005460	2	Das System muss einen fernen syslog-Server (Protokollhost) verwenden.	**Position** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Konformitätsaktion** Stellt sicher, dass das System einen fernen syslog-Server verwendet.
GEN005480	2	Das System muss einen fernen syslog-Server (Protokollhost) verwenden.	**Position** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Konformitätsaktion** Stellt sicher, dass das System einen fernen syslog-Server verwendet.
GEN005500	2	Der SSH-Dämon muss so konfiguriert werden, dass ausschließlich Secure Shell Protocol Version 2 (SSHv2) verwendet wird.	**Position** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005501	2	Der SSH-Client muss so konfiguriert werden, dass ausschließlich das Protokoll SSHv2 verwendet wird.	**Position** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005504	2	Der SSH-Dämon darf nur für Managementnetzadressen empfangsbereit sein, sofern er nicht für andere Zwecke als Managementzwecke autorisiert ist.	**Position** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005505	2	Der SSH-Dämon muss so konfiguriert werden, dass nur Chiffrierwerte verwendet werden, die Federal Information Processing Standards (FIPS) 140-2 entsprechen.	**Position** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN005506	2	Der SSH-Dämon muss so konfiguriert werden, dass nur Chiffrierwerte verwendet werden, die Federal Information Processing Standards (FIPS) 140-2 entsprechen.	**Position** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005507	2	Der SSH-Dämon muss so konfiguriert werden, dass er ausschließlich Nachrichtenauthentifizierungscodes mit kryptografischen Hashalgorithmen verwendet, die den FIPS 140-2-Standards entsprechen.	**Position** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005510	2	Der SSH-Dämon muss so konfiguriert werden, dass nur Nachrichtenauthentifizierungscodes verwendet werden, die FIPS 140-2-Standards entsprechen.	**Position** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005511	2	Der SSH-Dämon muss so konfiguriert werden, dass nur Nachrichtenauthentifizierungscodes verwendet werden, die FIPS 140-2-Standards entsprechen.	**Position** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005512	2	Der SSH-Dämon muss so konfiguriert werden, dass er ausschließlich Nachrichtenauthentifizierungscodes mit kryptografischen Hashalgorithmen verwendet, die den FIPS 140-2-Standards entsprechen.	**Position** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005521	2	Der SSH-Dämon muss die Anmeldung auf bestimmte Benutzer und/oder Gruppen beschränken.	**Position** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005536	2	Der SSH-Dämon muss eine strikte Modusprüfung der Konfigurationsdateien für die Ausgangsverzeichnisse durchführen.	**Position** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN005537	2	Der SSH-Dämon muss die Trennung von Zugriffsrechten verwenden.	**Position** /etc/security/pscexpert/dodv2/sshDoDconfig **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005538	2	Der SSH-Dämon darf die rhosts-Authentifizierung mit dem RSA-Verschlüsselungssystem (Rivest-Shamir-Adleman) nicht zulassen.	**Position** /etc/security/pscexpert/dodv2/sshDoDconfig **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005539	2	Der SSH-Dämon darf keine Komprimierung bzw. die Komprimierung nur nach erfolgreicher Authentifizierung zulassen.	**Position** /etc/security/pscexpert/dodv2/sshDoDconfig **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005550	2	Der SSH-Dämon muss mit dem DoD-Anmeldebanner konfiguriert werden.	**Position** /etc/security/pscexpert/dodv2/sshDoDconfig **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005560	2	Stellt fest, ob ein Standardgateway für IPv4 konfiguriert ist.	**Position** /etc/security/pscexpert/dodv2/chkgtway **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei DoDv2_to_AIXDefault.xml auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern. **Anmerkung:** Wenn auf Ihrem System das Protokoll IPv6 ausgeführt wird, stellen Sie sicher, dass die Einstellung *ipv6_enabled* in der Datei /etc/security/pscexpert/ipv6.conf auf den Wert yes gesetzt ist. Wenn das System IPv6 nicht verwendet, stellen Sie sicher, dass *ipv6_enabled* auf no gesetzt ist.
GEN005570	2	Stellt fest, ob ein Standardgateway für IPv6 konfiguriert ist.	**Position** /etc/security/pscexpert/dodv2/chkgtway **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei DoDv2_to_AIXDefault.xml auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern. **Anmerkung:** Wenn auf Ihrem System das Protokoll IPv6 ausgeführt wird, stellen Sie sicher, dass die Einstellung *ipv6_enabled* in der Datei /etc/security/pscexpert/ipv6.conf auf den Wert yes gesetzt ist. Wenn das System IPv6 nicht verwendet, stellen Sie sicher, dass *ipv6_enabled* auf no gesetzt ist.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN005590	2	Auf dem System dürfen keine Dämonprozesse für Routing-Protokolle ausgeführt werden, sofern es sich bei dem System nicht um einen Router handelt.	**Position** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005590	2	Auf dem System dürfen keine Dämonprozesse für Routing-Protokolle ausgeführt werden, sofern es sich bei dem System nicht um einen Router handelt.	**Position** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN005600	2	Die IP-Weiterleitung für IPv4 darf nicht aktiviert sein, sofern es sich bei dem System nicht um einen Router handelt.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `ipforwarding` auf *0*.
GEN005610	2	Auf dem System darf die IP-Weiterleitung für IPv6 nicht aktiviert sein, sofern es sich bei dem System nicht um einen IPv6-Router handelt.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `ip6forwarding` auf *1*.
GEN005820	2	Die anonyme UID und GID für NFS müssen mit Werten ohne Berechtigungen konfiguriert werden.	**Position** `/etc/security/pscexpert/dodv2/nfsoptions` **Konformitätsaktion** Stellt sicher, dass die angegebenen IDs keine Berechtigungen haben.
GEN005840	2	Der NFS-Server muss so konfiguriert werden, dass der Dateisystemzugriff auf lokale Hosts beschränkt wird.	**Position** `/etc/security/pscexpert/dodv2/nfsoptions` **Konformitätsaktion** Konfiguriert den NFS-Server so, dass er den Zugriff auf lokale Hosts beschränkt.
GEN005880	2	Der NFS-Server darf keinen fernen Rootzugriffe zulassen.	**Position** `/etc/security/pscexpert/dodv2/nfsoptions` **Konformitätsaktion** Inaktiviert den fernen Rootzugriff auf dem NFS-Server.
GEN005900	2	Die Option *nosuid* muss in allen NFS-Client-Mounts aktiviert werden.	**Position** `/etc/security/pscexpert/dodv2/nosuid` **Konformitätsaktion** Aktiviert die Option *nosuid* in allen NFS-Client-Mounts.
GEN006060	2	Auf dem System darf `Samba` nicht ausgeführt werden, sofern es nicht erforderlich ist.	**Position** `/etc/security/pscexpert/dodv2/dodv2services` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN006380	1	Das System darf UDP nicht für NIS und NIS+ verwenden.	**Position** `/etc/security/pscexpert/dodv2/dodv2cat1` **Konformitätsaktion** Zeigt die Ergebnisse der angegebenen Regeltests an.
GEN006400	2	Das Protokoll Network Information System (NIS) darf nicht verwendet werden.	**Position** `/etc/security/pscexpert/dodv2/nisplus` **Konformitätsaktion** Inaktiviert das angegebene Protokoll. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN006420	2	NIS-Maps müssen mit schwer zu erratenden Domänennamen geschützt werden.	**Position** `/etc/security/pscexpert/dodv2/nisplus` **Konformitätsaktion** Stellt sicher, dass Domänennamen nicht leicht zu bestimmen sind.
GEN006460	2	Alle NIS+-Server müssen mit Sicherheitsstufe arbeiten.	**Position** `/etc/security/pscexpert/dodv2/nisplus` **Konformitätsaktion** Stellt sicher, dass der Server die erforderliche Mindestsicherheitsstufe hat. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN006480	2	Das System muss wöchentlich auf nicht berechtigte `setuid`-Dateien und nicht autorisierte Änderungen berechtigter `setuid`-Dateien hin überprüft werden.	**Position** `/etc/security/pscexpert/dodv2/trust` **Konformitätsaktion** Prüft wöchentlich, ob Änderungen an den angegebenen Dateien vorgenommen wurden.
GEN006560	2	Das System muss wöchentlich auf nicht berechtigte `setuid`-Dateien und nicht autorisierte Änderungen berechtigter `setuid`-Dateien hin überprüft werden.	**Position** `/etc/security/pscexpert/dodv2/trust` **Konformitätsaktion** Prüft wöchentlich, ob Änderungen an den angegebenen Dateien vorgenommen wurden.
GEN006580	2	Das System muss ein Zugriffssteuerungsprogramm verwenden.	**Position** `/etc/security/pscexpert/dodv2/checktcpd` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN006600	2	Das Zugriffssteuerprogramm des Systems muss jeden Versuch, auf das System zuzugreifen, protokollieren.	**Position** `/etc/security/pscexpert/dodv2/chsyslogdod` **Konformitätsaktion** Stellt sicher, dass Zugriffsversuche protokolliert werden.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN006620	2	Das Zugriffssteuerungsprogramm des Systems muss so konfiguriert werden, dass bestimmten Hosts der Systemzugriff gewährt bzw. verweigert wird.	**Position** `/etc/security/pscexpert/dodv2/chetchostsdod` **Konformitätsaktion** Konfiguriert die Dateien `hosts.deny` und `hosts.allow` mit den erforderlichen Einstellungen.
GEN007020	2	Stream Control Transmission Protocol (SCTP) muss inaktiviert werden.	**Position** `/etc/security/pscexpert/dodv2/dodv2netrules` **Konformitätsaktion** Inaktiviert das angegebene Protokoll.
GEN007700	2	Der IPv6-Protokollhandler darf nur bei Bedarf an den Netzstack gebunden werden.	**Position** `/etc/security/pscexpert/dodv2/rminet6` **Konformitätsaktion** Inaktiviert den IPv6-Protokollhandler im Netzstack, sofern der Handler nicht in der Datei `/etc/ipv6.conf` angegeben ist. **Anmerkung:** Wenn auf Ihrem System das Protokoll IPv6 ausgeführt wird, stellen Sie sicher, dass die Einstellung *ipv6_enabled* in der Datei `/etc/security/pscexpert/ipv6.conf` auf den Wert `yes` gesetzt ist. Wenn das System IPv6 nicht verwendet, stellen Sie sicher, dass *ipv6_enabled* auf `no` gesetzt ist.
GEN007780	2	Auf dem System dürfen keine `6to4`-Tunnel aktiviert werden.	**Position** `/etc/security/pscexpert/dodv2/rmiface` **Konformitätsaktion** Inaktiviert die angegebenen Tunnel. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN007820	2	Auf dem System dürfen keine IP-Tunnel konfiguriert werden.	**Position** `/etc/security/pscexpert/dodv2/rmtunnel` **Konformitätsaktion** Inaktiviert IP-Tunnel. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN007840	2	Der `DHCP`-Client muss inaktiviert werden, wenn er nicht verwendet wird.	**Position** `/etc/security/pscexpert/dodv2/dodv2services` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN007850	2	Der `DHCP`-Client darf keine dynamischen DNS-Aktualisierungen senden.	**Position** `/etc/security/pscexpert/dodv2/dodv2services` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN007860	2	Das System muss IPv6-ICMP-Umleitungsnachrichten ignorieren.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `ipignoreredirects` auf *1*.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN007880	2	Das System darf keine IPv6-ICMP-Umleitungen senden.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `ipsendredirects` auf *0*.
GEN007900	2	Das System muss einen gültigen Umkehrpfadfilter für den IPv6-Netzverkehr verwenden, wenn das System IPv6 verwendet.	**Position** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN007920	2	Das System darf keine IPv6-Source-Routing-Pakete weiterleiten.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `ip6srcrouteforward` auf *0*.
GEN007940: GEN003607	2	Das System darf keine IPv4- oder IPv6-Source-Routing-Pakete akzeptieren.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `ipsrcrouterecv` auf *0*.
GEN007950	2	Das System darf nicht auf ICMPv6-echo-Anforderungen antworten, die an eine Broadcastadresse gesendet werden.	**Position** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Konformitätsaktion** Setzt den Wert der Netzoption `bcastping` auf *0*.
GEN008000	2	Wenn das System Lightweight Directory Access Protocol (LDAP) für Authentifizierungs- oder Accoutinformationen verwendet, müssen Zertifikate, die für die Auhentifizierung beim LDAP-Server verwendet werden, über DoD-PKI oder eine vom DoD genehmigte Methode bereitgestellt werden.	**Position** `/etc/security/pscexpert/dodv2/ldap_config` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN008020	2	Wenn das System LDAP für Authentifizierungs- oder Accountinformationen verwendet, muss die LDAP-TLS-Verbindung ein Zertifikat mit einem gültigen vertrauenswürdigen Pfad vom Server anfordern.	**Position** `/etc/security/pscexpert/dodv2/ldap_config` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN008050	2	Wenn das System LDAP für Authentifizierungs- oder Accountinformationen verwendet, darf die Datei `/etc/ldap.conf` (oder eine äquivalente Datei) keine Kennwörter enthalten.	**Position** `/etc/security/pscexpert/dodv2/ldap_config` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN008380	2	Das System muss wöchentlich auf nicht berechtigte `setuid`-Dateien und nicht autorisierte Änderungen berechtigter `setuid`-Dateien hin überprüft werden.	**Position** `/etc/security/pscexpert/dodv2/trust` **Konformitätsaktion** Prüft wöchentlich, ob Änderungen an den angegebenen Dateien vorgenommen wurden.
GEN008520	2	Das System muss eine lokale Firewall verwenden, die den Host vor Port-Scans schützt. Die Firewall muss anfällige Ports 5 Minuten lang sperren, um den Host vor Port-Scans zu schützen.	**Position** `/etc/security/pscexpert/dodv2/ipsecshunports` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt.
GEN008540	2	Die lokale Firewall des Systems muss eine Richtlinie des Typs *deny-all*, *allow-by-exception* implementieren.	**Position** `/etc/security/pscexpert/dodv2/ipsecshunhosthls` **Konformitätsaktion** Stellt sicher, dass das System die angegebenen Anforderungen erfüllt. **Anmerkung:** Sie können weitere Filterregeln in der Datei `/etc/security/aixpert/bin/filter.txt` angeben. Diese Regeln werden vom Script `ipsecshunhosthls.sh` integriert, wenn Sie das Profil anwenden. Die Einträge müssen im folgenden Format angegeben werden: *Portnummer*`:`*IP-Adresse*`:` *Aktion* Die gültigen Werte für *Aktion* sind `Allow` und `Deny`.
GEN008600	1	Das System muss so konfiguriert werden, dass es nur über die Systembootkonfiguration gestartet wird.	**Position** `/etc/security/pscexpert/dodv2/dodv2cat1` **Konformitätsaktion** Stellt sicher, dass beim Starten des Systems nur die Systembootkonfiguration verwendet wird.
GEN008640	1	Das System darf keine austauschbaren Datenträger als Bootladeprogramm verwenden.	**Position** `/etc/security/pscexpert/dodv2/dodv2cat1` **Konformitätsaktion** Stellt sicher, dass das System nicht von einem austauschbaren Datenträger gestartet wird.
GEN009140	1,2,3	Auf dem System darf der Service `chargen` nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN009160	1,2,3	Auf dem System darf der Service `Calendar Management Service Daemon` (CMSD) nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009180	1,2,3	Auf dem System darf der Service `tool-talk database server` (ttdbserver) nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009190	1,2,3	Auf dem System darf der Service `comsat` nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009200-9330	1,2,3	Auf dem System dürfen keine anderen Services und Dämonprozesse aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009210	2	Auf dem System darf der Service `discard` nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009220	2	Auf dem System darf der Service `dtspc` nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009230	2	Auf dem System darf der Service `echo` nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009240	2	Auf dem System darf der Service `Internet Message Access Protocol (IMAP)` nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009250	2	Auf dem System darf der Service `PostOffice Protocol (POP3)` nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.

Tabelle 2. Allgemeine DoD-Anforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Kategorie der STIG-Regel	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN009260	2	Auf dem System dürfen die Services talk und `ntalk` nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009270	2	Auf dem System darf der Service `netstat` im InetD-Prozess nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009280	2	Auf dem System darf der Service `PCNFS` nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009290	2	Auf dem System darf der Service `systat` nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009300	2	Auf dem System darf der Service `inetd time` im `inetd`-Dämon nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009310	2	Auf dem System darf der Service `rusersd` nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009320	2	Auf dem System darf der Service `sprayd` nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009330	2	Auf dem System darf der Service `rstatd` nicht aktiv sein.	**Position** `/etc/security/pscexpert/dodv2/inetdservices` **Konformitätsaktion** Inaktiviert die erforderlichen Dämonprozesse und Services, indem die entsprechenden Einträge in der Datei `/etc/inetd.conf` auf Kommentar gesetzt werden.
GEN009340	2	Es dürfen keine X Server-Anmeldemanager aktiv sein, sofern sie nicht für das X11-Sitzungsmanagement benötigt werden.	**Position** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Konformitätsaktion** Diese Regel inaktiviert X Window System-Verbindungen und den XServer-Anmeldemanager.

Tabelle 3. DoD-Eigneranforderungen

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
AIX00085	Eigner der Datei `/etc/netsvc.conf` muss Root sein.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
AIX00090	Die Datei `/etc/netsvc.conf` muss die Gruppe bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, sys oder system als Eigner hat.
AIX00320	Eigner der Datei `/etc/ftpaccess.ctl` muss Root sein.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
AIX00330	Die Datei `/etc/ftpaccess.ctl` muss die Gruppe bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, sys oder system als Eigner hat.
GEN000250	Die Konfigurationsdatei für die Zeitsynchronisation (z. B. `/etc/ntp.conf`) muss Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN000251	Die Konfigurationsdatei für die Zeitsynchronisation (z. B. `/etc/ntp.conf`) muss die Gruppe bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, sys oder system als Eigner hat.
GEN001160	Alle Dateien und Verzeichnisse müssen einen gültigen Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass alle Dateien und Verzeichnisse einen gültigen Eigner haben.
GEN001170	Alle Dateien und Verzeichnisse müssen einen gültigen Gruppeneigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass alle Dateien und Verzeichnisse einen gültigen Eigner haben.
GEN001220	Alle Systemdateien, Programme und Verzeichnisse müssen einen Systemaccount als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass alle Systemdateien, Programme und Verzeichnisse einen Systemaccount als Eigner haben.

Tabelle 3. DoD-Eigneranforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN001240	Systemdateien, Programme und Verzeichnisse müssen eine Systemgruppe als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Alle Systemdateien, Programme und Verzeichnisse müssen eine Systemgruppe als Eigner haben.
GEN001320	NIS)/NIS+/yp-Dateien (Network Information Systems) müssen root, sys oder bin als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien root, sys oder bin als Eigner haben.
GEN001340	NIS/NIS+/yp-Dateien müssen die Gruppe sys, bin, other oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien sys, bin, other oder system als Eigner haben.
GEN001362	Die Datei `/etc/resolv.conf` muss Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN001363	Die Datei `/etc/resolv.conf` muss die Gruppe bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, sys oder system als Eigner hat.
GEN001366	Die Datei `/etc/hosts` muss Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN001367	Die Datei `/etc/hosts` muss die Gruppe bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, sys oder system als Eigner hat.
GEN001371	Die Datei `/etc/nsswitch.conf` muss Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN001372	Die Datei `/etc/nsswitch.conf` muss die Gruppe root, bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe root, bin, sys oder system als Eigner hat.

Tabelle 3. DoD-Eigneranforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN001378	Die Datei `/etc/passwd` muss Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN001379	Die Datei `/etc/passwd` muss die Gruppe bin, security, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, security, sys oder system als Eigner hat.
GEN001391	Die Datei `/etc/group` muss Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN001392	Die Datei `/etc/group` muss die Gruppe bin, security, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, security, sys oder system als Eigner hat.
GEN001400	Die Datei `/etc/security/passwd` muss Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN001410	Die Datei `/etc/security/passwd` muss die Gruppe bin, security, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, security, sys oder system als Eigner hat.
GEN001500	Die Ausgangsverzeichnisse aller interaktiven Benutzer müssen die entsprechenden Benutzer als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die Ausgangsverzeichnisse aller interaktiven Benutzer die entsprechenden Benutzer als Eigner haben.
GEN001520	Die Ausgangsverzeichnisse aller interaktiven Benutzer müssen die primäre Gruppe des Ausgangsverzeichniseigners als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die Ausgangsverzeichnisse aller interaktiven Benutzer die primäre Gruppe des Ausgangsverzeichniseigners als Eigner haben.

Tabelle 3. DoD-Eigneranforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN001540	Alle Dateien und Verzeichnisse, die in den Ausgangsverzeichnissen inaktiver Benutzer enthalten sind, müssen den Eigner des Ausgangsverzeichnisses als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass alle Dateien und Verzeichnisse, die in den Ausgangsverzeichnissen inaktiver Benutzer enthalten sind, den Eigner des Ausgangsverzeichnisses als Eigner haben.
GEN001550	Alle Dateien und Verzeichnisse, die in den Ausgangsverzeichnisses des Benutzers enthalten sind, müssen eine Gruppe, zu der der Eigner des Ausgangsverzeichnisses gehört, als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass alle Dateien und Verzeichnisse, die in den Ausgangsverzeichnisses des Benutzers enthalten sind, eine Gruppe, zu der der Eigner des Ausgangsverzeichnisses gehört, als Eigner haben.
GEN001660	Alle Systemstartdateien müssen Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Dateien ist.
GEN001680	Alle Systemstartdateien müssen die Gruppe sys, bin, other oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien die Gruppe sys, bin, other oder system als Eigner haben.
GEN001740	Alle globalen Initialisierungsdateien müssen Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Dateien ist.
GEN001760	Alle globalen Initialisierungsdateien müssen die Gruppe sys, bin, system oder security als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien die Gruppe sys, bin, system oder security als Eigner haben.
GEN001820	Alle Entwurfsdateien und -verzeichnisse (gewöhnlich in `/etc/skel`) müssen root oder bin als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien und Verzeichnisse root oder bin als Eigner haben.
GEN001830	Alle Entwurfsdateien (gewöhnlich in `/etc/skel`) müssen die Gruppe security als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dss die angegebenen Dateien die Gruppe security als Eigner haben.

Tabelle 3. DoD-Eigneranforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN001860	Alle lokalen Initialisierungsdateien müssen den Benutzer oder Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien den Benutzer oder Root als Eigner haben.
GEN001870	Lokale Initialisierungsdateien müssen die primäre Gruppe des Benutzers oder Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die lokalen Initialisierungsdateien die primäre Gruppe des Benutzers oder Root als Eigner haben.
GEN002060	Alle `.rhosts-`, `.shosts-`, `.netrc-` oder `hosts.equiv`-Dateien dürfen nur für Root oder den Eigner zugänglich sein.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass nur Root oder der Eigner auf die angegebenen Dateien zugreifen kann.
GEN002100	Die Datei `.rhosts` darf von Pluggable Authentication Module (PAM) nicht unterstützt werden.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei mit PAM nicht verfügbar ist.
GEN002200	Alle Shelldateien müssen root oder bin als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien root oder bin als Eigner haben.
GEN002210	Alle Shelldateien müssen die Gruppe root, bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien die Gruppe root, bin, sys oder system als Eigner haben.
GEN002340	Audioeinheiten müssen Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner aller Audioeinheiten ist.
GEN002360	Audioeinheiten müssen die Gruppe root root, sys, bin oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, ass Audioeinheiten die Gruppe root root, sys, bin oder system als Eigner haben.

Tabelle 3. DoD-Eigneranforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	**Beschreibung**	**Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind**
GEN002520	Alle öffentlichen Verzeichnisse müssen Root oder einen Anwendungsaccount als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass slle öffentlichen Verzeichnisse Root oder einen Anwendungsaccount als Eigner haben.
GEN002540	Stellt sicher, dass alle öffentlichen Verzeichnisse die Gruppe system oder eine Anwendungsgruppe als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass alle öffentlichen Verzeichnisse die Gruppe system oder eine Anwendungsgruppe als Eigner haben.
GEN002680	Systemprüfprotokolle müssen Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Dateien ist.
GEN002690	Systemprüfprotokolle müssen die Gruppe bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien die Gruppe bin, sys oder system als Eigner haben.
GEN003020	`Cron` darf keine Programme in Verzeichnissen oder Unterverzeichnissen mit globalem Schreibzugriff ausführen.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Verhindert, dass `cron` Programme in Verzeichnissen und Unterverzeichnissen mit globalem Schreibzugriff ausführt.
GEN003040	`Crontab` muss root oder den Crontab-Ersteller als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Crontab Root oder den Crontab-Ersteller als Eigner hat.
GEN003050	`Crontab`-Dateien müssen die Gruppe system, cron oder die primäre Gruppe des Crontab-Erstellers als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die `Crontab`-Dateien die Gruppe system, cron oder die primäre Gruppe des Crontab-Erstellers als Eigner haben.
GEN003110	`Cron`- und `crontab`-Verzeichnisse dürfen keine erweiterten Zugriffssteuerungslisten haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Verzeichnisse keine erweiterten Zugriffssteuerungslisten haben.

Tabelle 3. DoD-Eigneranforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN003120	`Cron`- und `Crontab`-Verzeichnisse müssen root oder bin als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Cron- und Crontab-Verzeichnisse root oder bin als Eigner haben.
GEN003140	`Cron` und `Crontab`-Verzeichnisse müssen die Gruppe system, sys, bin oder cron als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Verzeichnisse die Gruppe system, sys, bin oder cron als Eigner haben.
GEN003160	Die Cron-Protokollierung muss implementiert werden.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die Cron-Protokollierung implementiert ist.
GEN003240	Die Datei `cron.allow` muss root, bin oder sys als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei root, bin oder sys als Eigner hat.
GEN003250	Die Datei `cron.allow` muss die Gruppe system, bin, sys oder cron als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe system, bin, sys oder cron als Eigner hat.
GEN003260	Die Datei `cron.deny` muss root, bin oder sys als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei root, bin oder sys als Eigner hat.
GEN003270	Die Datei `cron.deny` muss die Gruppe system, bin, sys oder cron als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe system, bin, sys oder cron als Eigner hat.
GEN003420	Das Verzeichnis `at` muss root, bin, sys, daemon oder cron als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass das angegebene Verzeichnis root, sys, daemon oder cron als Eigner hat.

Tabelle 3. DoD-Eigneranforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN003430	Das Verzeichnis `at` muss die Gruppe system, bin, sys oder cron als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass das angegebene Verzeichnis die Gruppe system, bin, sys oder cron als Eigner hat.
GEN003460	Die Datei `at.allow` muss root, bin oder sys als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei root, bin oder sys als Eigner hat.
GEN003470	Die Datei `at.allow` muss die Gruppe system, bin, sys oder cron als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe system, bin, sys oder cron als Eigner hat.
GEN003480	Die Datei `at.deny` muss root, bin oder sys als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei root, bin oder sys als Eigner hat.
GEN003490	Die Datei `at.deny` muss die Gruppe system, bin, sys oder cron als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe system, bin, sys oder cron als Eigner hat.
GEN003720	Die Datei, `inetd.conf`, die Datei `xinetd.conf` und das Verzeichnis `xinetd.d` müssen root oder bin als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien und Verzeichnisse root oder bin als Eigner haben.
GEN003730	Die Datei `inetd.conf`, die Datei `xinetd.conf` und das Verzeichnis `xinetd.d` müssen die Gruppe bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien und Verzeichnisse die Gruppe bin, sys oder system als Eigner haben.
GEN003760	Die Datei `services` muss root oder bin als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass root oder bin Eigner der angegebenen Datei ist.

Tabelle 3. DoD-Eigneranforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN003770	Die Datei `services` muss die Gruppe bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, sys oder system als Eigner hat.
GEN003920	Die Datei `hosts.lpd` (oder eine äquivalente Datei) muss root, bin, sys oder lp als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei root, bin, sys oder lp als Eigner hat.
GEN003930	Die Datei `hosts.lpd` (oder eine äquivalente Datei) muss die Gruppe bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, sys oder system als Eigner hat.
GEN003960	Der Befehl **traceroute** muss root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass root der Eigner des Befehls ist.
GEN003980	Der Befehl **traceroute** muss die Gruppe sys, bin oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass der Befehl die Gruppe sys, bin oder system als Eigner hat.
GEN004360	Die Datei `alias` muss Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN004370	Die Datei `aliases` muss die Gruppe sys, bin oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe sys, bin oder system als Eigner hat.
GEN004400	Dateien, die über eine Mail-Datei `aliases` ausgeführt werden, müssen root als Eigner haben und sich in einem Verzeichnis befinden, das root als Eigner hat und nur von root modifiziert werden kann.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Dateien, die über eine Mail-Datei `aliases` ausgeführt werden, root als Eigner haben und sich in einem Verzeichnis befinden, das root als Eigner hat und nur von root modifiziert werden kann.

Tabelle 3. DoD-Eigneranforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN004410	Dateien, die über eine Mail-Datei `aliases` ausgeführt werden, müssen die Gruppe root, bin, sys oder other als Eigner haben. Außerdem müssen sich die Dateien in einem Verzeichnis befinden, das die Gruppe root, bin, sys oder other als Eigner hat.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien, die über eine Mail-Datei `aliases` ausgeführt werden, die Gruppe root, bin, sys oder other als Eigner haben und sich in einem Verzeichnis befinden, das die Gruppe root, bin, sys oder other als Eigner hat.
GEN004480	Die Protokolldatei des SMTP-Service muss root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN004920	Die Datei `ftpusers` muss Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN004930	Die Datei `ftpusers` muss die Gruppe bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, sys oder system als Eigner hat.
GEN005360	Die Datei `snmpd.conf` muss Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN005365	Die Datei `snmpd.conf` muss die Gruppe bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, sys oder system als Eigner hat.
GEN005400	Die Datei `/etc/syslog.conf` muss Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN005420	Die Datei `/etc/syslog.conf` muss die Gruppe bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, sys oder system als Eigner hat.

Tabelle 3. DoD-Eigneranforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN005610	Auf dem System darf die IP-Weiterleitung für IPv6 nicht aktiviert sein, sofern es sich bei dem System nicht um einen IPv6-Router handelt.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die IP-Weiterleitung für IPv6 nur aktiviert wird, wenn das System als IPv6-Router verwendet wird.
GEN005740	Die NFS-Exportkonfigurationsdatei muss root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN005750	Die NFS-Exportkonfigurationsdatei muss die Gruppe root, bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe root, bin, sys oder system als Eigner hat.
GEN005800	Alle über NFS-exportierten Systemdateien und Systemverzeichnisse müssen root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN005810	Alle über NFS exportierten Systemdateien und Systemverzeichnisse müssen die Gruppe root, bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien und Verzeichnisse die Gruppe root, bin, sys oder system als Eigner haben.
GEN006100	Die Datei `/usr/lib/smb.conf` muss Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN006120	Die Datei `/usr/lib/smb.conf` muss die Gruppe bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, sys oder system als Eigner hat.
GEN006160	Die Datei `/var/private/smbpasswd` muss Root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.

Tabelle 3. DoD-Eigneranforderungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN006180	Die Datei `/var/private/smbpasswd` muss die Gruppe sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe sys oder system als Eigner hat.
GEN006340	Die Dateien im Verzeichnis `/etc/news` müssen root oder news als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass das angegebene Verzeichnis root oder news als Eigner hat.
GEN006360	Die Dateien im Verzeichnis `/etc/news` müssen die Gruppe system oder news als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien die Gruppe system oder news als Eigner haben.
GEN008080	Wenn das System LDAP für Authentifizierungs- oder Accountinformationen verwendet, muss die Datei `/etc/ldap.conf` (oder eine äquivalente Datei) root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN008100	Wenn das System LDAP für Authentifizierungs- oder Accountinformationen verwendet, muss die Datei `/etc/ldap.conf` (oder eine äquivalente Datei) die Gruppe security, bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, sys oder system als Eigner hat.
GEN008140	Wenn das System LDAP für Authentifizierungs- oder Accountinformationen verwendet, muss die TLS-CA-Datei oder das TLS-Zertifikatsverzeichnis root als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass Root der Eigner der angegebenen Datei ist.
GEN008160	Wenn das System LDAP für Authentifizierungs- oder Accountinformationen verwendet, muss die TLS-CA-Datei oder das TLS-Zertifikatsverzeichnis die Gruppe root, bin, sys oder system als Eigner haben.	**Position** `/etc/security/pscexpert/dodv2/chowndodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebene Datei die Gruppe bin, sys oder system als Eigner hat.

Tabelle 4. DoD-Standards für Dateiberechtigungen

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
AIX00100	Die Datei `/etc/netsvc.conf` muss den Modus 0644 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.

Tabelle 4. DoD-Standards für Dateiberechtigungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
AIX00340	Die Datei `/etc/ftpaccess.ctl` muss den Modus 0640 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN000252	Die Konfigurationsdatei für die Zeitsynchronisation (z. B. `/etc/ntp.conf`) muss den Modus 0640 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN000920	Das Ausgangsverzeichnis des Root-Accounts (mit Ausnahme von `/`) muss den Modus 0700 haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass das Verzeichnis auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN001140	Systemdateien und -verzeichnisse dürfen keine ungeraden Zugriffsberechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Zugriffsberechtigungen konsistent sind.
GEN001180	Alle Dämondateien für Netzservices müssen den Modus 0755 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN001200	Alle Systembefehlsdateien müssen den Modus 0755 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN001260	Systemprotokolldateien müssen den Modus 0640 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.

Tabelle 4. DoD-Standards für Dateiberechtigungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN001280	Man-Page-Dateien müssen den Modus 0644 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN001300	Bibliotheksdateien müssen den Modus 0755 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN001360	NIS/NIS+/yp-Dateien müssen den Modus 0755 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN001364	Die Datei `/etc/resolv.conf` muss den Modus 0644 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN001368	Die Datei `/etc/hosts` muss den Modus 0644 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN001373	Die Datei `/etc/nsswitch.conf` muss den Modus 0644 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN001380	Die Datei `/etc/passwd` muss den Modus 0644 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.

Tabelle 4. DoD-Standards für Dateiberechtigungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN001393	Die Datei `/etc/group` muss den Modus 0644 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN001420	Die Datei `/etc/security/passwd` muss den Modus 0400 haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN001480	Alle Ausgangsverzeichnisse eines Benutzers müssen den Modus 0750 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN001560	Alle Dateien und Verzeichnisse, die in den Ausgangsverzeichnissen eines Benutzers enthalten sind, müssen den Modus 0750 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN001580	Alle Ausführungssteuerscripts müssen den Modus 0755 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN001640	Die Ausführungssteuerscripts dürfen keine Programme oder Scripts mit globalem Schreibzugriff ausführen.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Überprüft Programme wie `cron` auf Programme oder Scripts mit globalem Schreibzugriff.
GEN001720	Alle globalen Initialisierungsdateien müssen den Modus 0644 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.

Tabelle 4. DoD-Standards für Dateiberechtigungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN001800	Alle Entwurfsdateien (z. B. Dateien in `/etc/skel`) müssen den Modus 0644 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN001880	Alle lokalen Initialisierungsdateien müssen den Modus 0740 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN002220	Alle Shelldateien müssen den Modus 0755 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN002320	Audioeinheiten müssen den Modus 0660 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Audioeinheiten auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt sind.
GEN002560	Der **umask**-Standardwert für System und Benutzer muss 077 sein.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Einstellungen *077* gesetzt sind.
GEN002700	Systemprüfprotokolle müssen den Modus 0640 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN002717	Die ausführbaren Dateien für die Systemprüftools müssen den Modus 0750 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.

Tabelle 4. DoD-Standards für Dateiberechtigungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN002980	Die Datei `cron.allow` muss den Modus 0600 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN003080	Crontab-Dateien müssen den Modus 0600 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN003090	`Crontab`-Dateien dürfen keine erweiterten Zugriffssteuerungslisten (ACLs, Access Control List) haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien keine erweiterten ACLs haben.
GEN003100	Cron- und Crontab-Dateien müssen den Modus 0755 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Vereichnisse auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN003180	Die Datei `cronlog` muss den Modus 0600 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN003200	Die Datei `cron.deny` muss den Modus 0600 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN003252	Die Datei `at.deny` muss den Modus 0640 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.

Tabelle 4. DoD-Standards für Dateiberechtigungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN003340	Die Datei `at.allow` muss den Modus 0600 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN003400	Das Verzeichis `at` muss den Modus 0755 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass das Verzeichnis auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN003440	`At`-Jobs dürfen den Parameter **`umask`** nicht auf einen Wert setzen, der restriktiver ist als 077.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass der Parameter auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN003740	Die Dateien `inetd.conf` und `xinetd.conf` müssen den Modus 0440 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN003780	Die Datei `services` muss den Modus 0444 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN003940	Die Datei `hosts.lpd` (oder eine äquivalente Datei) muss den Modus 0644 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN004000	Die Datei `traceroute` muss den Modus 0700 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.

Tabelle 4. DoD-Standards für Dateiberechtigungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN004380	Die Datei `alias` muss den Modus 0644 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN004420	Dateien, die über eine Mail-Datei `aliases` ausgeführt werden, müssen den Modus 0755 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN004500	Die Protokolldatei des SMTP-Service muss den Modus 0644 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN004940	Die Datei `ftpusers` muss den Modus 0640 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN005040	Alle FTP-Benutzer müssen die **umask**-Standardeinstellung 077 haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Einstellung korrekt ist.
GEN005100	Der `TFTP`-Dämon muss den Modus 0755 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass der Dämon auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN005180	Alle `.Xauthority`-Dateien müssen den Modus 0600 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.

Tabelle 4. DoD-Standards für Dateiberechtigungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN005320	Die Datei `snmpd.conf` muss den Modus 0600 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN005340	MIB-Dateien (Management Information Base) müssen den Modus 0640 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN005390	Die Datei `/etc/syslog.conf` muss den Modus 0640 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN005522	Die Dateien mit dem öffentlichen SSH-Hostschlüssel müssen den Modus 0644 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN005523	Die Dateien mit dem privaten SSH-Hostschlüssel müssen den Modus 0600 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Dateien auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN006140	Die Datei `/usr/lib/smb.conf` muss den Modus 0644 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN006200	Die Datei `/var/private/smbpasswd` muss den Modus 0600 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.

Tabelle 4. DoD-Standards für Dateiberechtigungen (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN006260	Die Datei `/etc/news/hosts.nntp` (oder eine äquivalente Datei) muss den Modus 0600 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN006280	Die Datei `/etc/news/hosts.nntp.nolimit` (oder eine äquivalente Datei) muss den Modus 0600 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN006300	Die Datei `/etc/news/nnrp.access` (oder eine äquivalente Datei) muss den Modus 0600 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN006320	Die Datei `/etc/news/passwd.nntp` (oder eine äquivalente Datei) muss den Modus 0600 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN008060	Wenn das System LDAP für Authentifizierungs- oder Accountinformationen verwendet, muss die Datei `/etc/ldap.conf` (oder eine äquivalente Datei) den Modus 0644 oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die Datei auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt ist.
GEN008180	Wenn das System LDAP für Authentifizierungs- oder Accountinformationen verwendet, müssen die TLS-CA-Datei und/oder das TLS-CA-Verzeichnis den Modus 0644 (0755 für Verzeichnisse) oder einen Modus mit weniger Berechtigungen haben.	**Position** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien und/oder Vereichnisse auf den angegebenen Berechtigungsmodus oder einen Modus mit weniger Berechtigungen gesetzt sind.

Tabelle 5. DoD-Anforderungen für Zugriffskontrolllisten

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
AIX00110	Die Datei `/etc/netsvc.conf` darf keine erweiterte Zugriffssteuerungsliste (ACL, Access Control List) haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
AIX00350	Die Datei `/etc/ftpaccess.ctl` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN000253	Die Konfigurationsdatei für die Zeitsynchronisation (z. B. `/etc/ntp.conf`) darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN000930	Das Ausgangsverzeichnis des Root-Accounts darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 5. DoD-Anforderungen für Zugriffskontrolllisten (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN001190	Alle Dämondateien für Netzservices dürfen keine erweiterten ALCs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001210	Alle Systembefehlsdateien dürfen keine erweiterten ALCs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001270	Systemprotokolldateien dürfen keine erweiterten ACLs haben, sofern sie nicht für die Unterstützung autorisierter Software benötigt werden.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001310	Alle Bibliotheksdateien dürfen keine erweiterten ALCs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 5. DoD-Anforderungen für Zugriffskontrolllisten (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN001361	NIS/NIS+/yp-Befehlsdateien dürfen keine erweiterten ACLs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001365	Die Datei `/etc/resolv.conf` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001369	Die Datei `/etc/hosts` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001374	Die Datei `/etc/nsswitch.conf` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 5. DoD-Anforderungen für Zugriffskontrolllisten (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN001390	Die Datei `/etc/passwd` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001394	Die Datei `/etc/group` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001430	Die Datei `/etc/security/passwd` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001570	Alle Dateien und Verzeichnisse in den Benutzerausgangsverzeichnissen dürfen keine erweiterten ACLs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 5. DoD-Anforderungen für Zugriffskontrolllisten (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN001590	Alle Ausführungssteuerscripts dürfen keine erweiterten ACLs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001730	Alle globalen Initialisierungsdateien dürfen keine erweiterten ALCs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001810	Entwurfsdateien dürfen keine erweiterten ACLs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN001890	Lokale Initialisierungsdateien dürfen keine erweiterten ALCs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 5. DoD-Anforderungen für Zugriffskontrolllisten (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN002230	Alle Shelldateien dürfen keine erweiterten ALCs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN002330	Audioeinheiten dürfen keine erweiterten ACLs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN002710	Alle Systemprüfdateien dürfen keine erweiterten ALCs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN002990	Erweiterte ACLs müssen für die Dateien `cron.allow` und `cron.deny` inaktiviert werden.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 5. DoD-Anforderungen für Zugriffskontrolllisten (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN003090	Crontab-Dateien dürfen keine erweiterten ACLs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN003110	Cron- und Crontab-Verzeichnisse dürfen keine erweiterten ACLs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN003190	Die Cron-Protokolldateien dürfen keine erweiterten ACLs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN003210	Die Datei `cron.deny` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 5. DoD-Anforderungen für Zugriffskontrolllisten (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN003245	Die Datei `at.allow` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN003255	Die Datei `at.deny` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN003410	Das `at`-Verzeichnis darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN003745	Die Dateien `inetd.conf` und `xinetd.conf` dürfen keine erweiterten ACLs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 5. DoD-Anforderungen für Zugriffskontrolllisten (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN003790	Die Servicedatei darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN003950	Die Datei `hosts.lpd` (oder eine äquivalente Datei) darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN004010	Die Datei `traceroute` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN004390	Die Datei `alias` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 5. DoD-Anforderungen für Zugriffskontrolllisten (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN004430	Dateien, die über eine Mail-Datei `aliases` ausgeführt werden, dürfen keine erweiterten ACLs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN004510	Die Protokolldatei des SMTP-Service darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN004950	Die Datei `ftpusers` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN005190	Die `.Xauthority`-Dateien dürfen keine erweiterten ACLs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 5. DoD-Anforderungen für Zugriffskontrolllisten (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN005350	MIB-Dateien (Management Information Base) dürfen keine erweiterten ACLs haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN005375	Die Datei `snmpd.conf` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN005395	Die Datei `/etc/syslog.conf` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN006150	Die Datei `/usr/lib/smb.conf` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 5. DoD-Anforderungen für Zugriffskontrolllisten (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN006210	Die Datei `/var/private/smbpasswd` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN006270	Die Datei `/etc/news/hosts.nntp` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN006290	Die Datei `/etc/news/hosts.nntp.nolimit` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN006310	Die Datei `/etc/news/nnrp.access` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Tabelle 5. DoD-Anforderungen für Zugriffskontrolllisten (Forts.)

Department of Defense-STIG-Prüfpunkt-ID	Beschreibung	Position des Scripts, in dem die Aktion und die Ergebnisse der Aktion zur Einhaltung der Konformität definiert sind
GEN006330	Die Datei `/etc/news/passwd.nntp` darf keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Inaktiviert die angegebene erweiterte ACL. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN008120	Wenn das System LDAP für Authentifizierungs- oder Accountinformationen verwendet, darf die Datei `/etc/ldap.conf` (oder eine äquivalente Datei) keine erweiterte Zugriffssteuerungsliste (ACL) haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Stellt sicher, dass die angegebenen Dateien keine erweiterte ACL haben. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.
GEN008200	Wenn das System LDAP für Authentifizierungs- oder Accountinformationen verwendet, darf die die LDAP-TLS-CA-Datei oder das LDAP-TLS-Zertifikatsverzeichnis keine erweiterte ACL haben.	**Position** `/etc/security/pscexpert/dodv2/acldodfiles` **Konformitätsaktion** Stellt sicher, dass das angegebene Verzeichnis oder die angegebene Dateie keine erweiterte ACL hat. **Anmerkung:** Diese Einstellung wird nicht automatisch geändert, wenn die Richtlinie mit der Datei `DoDv2_to_AIXDefault.xml` auf die AIX-Standardrichtlinie zurückgesetzt wird. Sie müssen diese Einstellung manuell ändern.

Zugehörige Informationen:

Department of Defense STIG

Konformität mit Payment Card Industry - Data Security Standard

Payment Card Industry - Data Security Standard (PCI - DSS) kategorisiert die IT-Sicherheit in 12 Abschnitte, die als die 12 Anforderungs- und Sicherheitsbewertungsprozeduren bezeichnet werden.

Zu den von PCI-DSS definierten 12 Anforderungen und Sicherheitsbewertungsprozeduren für IT-Sicherheit gehören die folgenden Punkte:

Anforderung 1: Firewallkonfiguration zum Schutz der Daten des Karteninhabers installieren und verwalten

Dokumentierte Liste von Services und Ports, die für das Geschäft erforderlich sind. Diese Anforderung wird durch Inaktivieren der nicht benötigten und nicht sicheren Services implementiert.

Anforderung 2: Keine vom Anbieter bereitgestellten Standardwerte für Systemkennwörter und andere Sicherheitsparameter verwenden.

Ändern Sie die vom Anbieter bereitgestellten Standardwerte, bevor Sie ein System im Netz installieren. Diese Anforderung wird durch Inaktivieren des SNMP-Dämons (Simple Network Management Protocol) implementiert.

Anforderung 3: Gespeicherte Daten des Karteninhabers schützen.

Diese Anforderung wird durch Aktivieren des EFS-Features (Encrypted File System, verschlüsseltes Dateisystem) implementiert, das mit dem Betriebssystem AIX bereitgestellt wird.

Anforderung 4: Daten des Karteninhabers bei der Übertragung der Daten in offenen öffentlichen Netzen verschlüsseln.

Diese Anforderung wird durch Aktivieren des IPSEC-Features (IP Security, IP-Sicherheit) implementiert, das mit dem Betriebssystem AIX bereitgestellt wird.

Anforderung 5: Antivirensoftwareprogramme verwenden und regelmäßig aktualisieren.

Diese Anforderung wird mit dem Trusted Execution-Richtlinienprogramm implementiert. Trusted Execution ist die empfohlene Antivirensoftware und nativ für das Betriebssystem AIX. PCI erfordert, dass Sie die Protokolle des Trusted Execution-Programms erfassen, indem Sie SIEM (Security Information and Event Management, Management von Sicherheitsinformationen und -ereignissen) zur Überwachung der Alerts aktivieren. Wenn Sie das Trusted Execution-Programm im reinen Protokollmodus ausführen, stellt das Programm die Prüfungen nicht ein, wenn ein Fehler aufgrund einer Hashdiskrepanz auftritt.

Anforderung 6: Sichere Systeme und Anwendungen entwickeln und verwalten.

Zum Implementieren dieser Anforderung müssen Sie manuell die erforderlichen Patches für Ihr System installieren. Wenn Sie PowerSC Standard Edition erworben haben, können Sie das Feature Trusted Network Connect (TNC) verwenden.

Anforderung 7: Zugriff auf Karteninhaberdaten nach Geschäftsbedarf einschränken.

Sie können strikte Zugriffssteuerungsmaßnahmen implementieren, indem Sie mit dem RBAC-Feature Regeln und Rollen aktivieren. RBAC kann nicht automatisiert werden, weil RBAC für die Aktivierung die Eingabe eines Administrators erfordert.

`RbacEnablement` überprüft das System, um festzustellen, ob die Eigenschaften isso, so und sa für die Rollen auf dem System vorhanden sind. Wenn diese Eigenschaften nicht vorhanden sind, werden sie vom Script erstellt. Dieses Script kann auch im Rahmen der pscexpert-Prüfungen ausgeführt werden, die bei der Ausführung von Befehlen wie `pscxpert -c` durchgeführt werden.

Anforderung 8: Jeder Person, die Zugriff auf den Computer hat, eine eindeutige ID zuweisen.

Sie können diese Anforderung durch Aktivieren von PCI-Profilen implementieren. Die folgenden Regeln gelten für PCI-Profile:

- Benutzerkennwörter mindestens alle 90 Tage ändern
- Mindestkennwortlänge von 7 Zeichen voraussetzen
- Kennwort verwenden, das Ziffern und alphabetische Zeichen enthält
- Nicht zulassen, dass eine Person ein neues Kennwort einreicht, das einem der vorherigen verwendeten vier Kennwörter entspricht
- Wiederholte Zugriffsversuche durch Sperren der Benutzer-ID nach sechs nicht erfolgreichen Versuchen beschränken
- Sperrzeit von 30 Minuten festlegen bzw. Benutzer-ID sperren, bis ein Administrator sie erneut aktiviert
- Erneute Eingabe des Kennworts des Benutzers anfordern, um ein Terminal nach einer Inaktivität von 15 Minuten oder mehr zu reaktivieren

Anforderung 9: Physischen Zugriff auf die Daten des Karteninhabers beschränken.

Repositorys, die sensible Karteninhaberdaten enthalten, in einem Raum mit Zugangsbeschränkung aufbewahren.

Anforderung 10: Alle Zugriffe auf Netzressourcen und Karteninhaberdaten verfolgen und überwachen. Diese Anforderung wird durch Protokollierung von Zugriffen auf die Systemkomponenten implementiert, indem die automatischen Protokolle in den Systemkomponenten aktiviert werden.

Anforderung 11: Sicherheitssysteme und -prozesse regelmäßig testen.
Diese Anforderung wird durch Verwendung des Features Real-Time Compliance (RTC) implementiert.

Anforderung 12: Sicherheitsrichtlinie verwalten, die die Informationssicherheit für Mitarbeiter und Auftragnehmer umfasst.
Aktivierung von Modems für Anbieter nur bei Bedarf mit sofortiger Inaktivierung nach Verwendung. Diese Anforderung wird durch Inaktivierung der Rootanmeldung über Fernzugriff, Aktivierung bei Bedarf durch einen Systemadministrator und anschließende Inaktivierung implementiert.

PowerSC Standard Edition verringert das Konfigurationsmanagement, das erforderlich ist, um die von PCI DSS Version 2.0 und PCI DSS Version 3.0. definierten Richtlinien einzuhalten. Der gesamte Prozess kann jedoch nicht automatisiert werden.

Die Beschränkung den Zugriffs auf die Daten von Karteninhabern nach Geschäftsbedarf kann beispielsweise nicht automatisiert werden. Das Betriebssystem AIX stellt leistungsstarke Sicherheitstechnologien wie die rollenbasierte Zugriffssteuerung (RBAC, Role Based Access Control) bereit, aber PowerSC Standard Edition kann diese Konfiguration nicht automatisieren, weil die Einzelpersonen, die Zugriff benötigen, und die Einzelpersonen, die keinen Zugriff benötigen, nicht bestimmt werden können. IBM Compliance Expert kann die Konfiguration anderer Sicherheitseinstellungen, die den PCI-Anforderungen entsprechen, automatisieren.

Wenn das PCI-Profil auf eine Datenbankumgebung angewendet wird, werden mehrere TCP- und UDP-Ports, die vom Software-Stack verwendet werden, über Einschränkungen inaktiviert. Sie müssen diese Ports aktivieren und die Funktion Trusted Execution inaktivieren, um die Anwendung und die Workload ausführen zu können. Führen Sie die folgenden Befehle aus, um die Einschränkungen für die Ports zu entfernen und die Funktion Trusted Execution zu inaktivieren:

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

Anmerkung: Alle angepassten Sriptdateien, die zur Verwaltung der Konformität mit PCI-DSS bereitgestellt werden, sind im Verzeichnis `/etc/security/pscexpert/bin` enthalten.

In der folgenden Tabelle wird gezeigt, wie PowerSC Standard Edition die Anforderungen des PCI-DSS-Standards mithilfe der Funktionen des Dienstprogramms AIX Security Expert adressiert:

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
2.1	Vom Anbieter bereitgestellte Standardwerte vor der Installation eines Systems im Netz immer ändern. Dazu gehören Kennwörter, SNMP-Community-Zeichenfolgen (Simple Network Management Protocol) und das Entfernen nicht benötigter Zeichenfolgen.	Setzt die Mindestanzahl an Wochen, die vergehen müssen, bevor Sie ein Kennwort ändern können, mit dem Parameter **minage** auf 0.	`/etc/security/pscexpert/bin/chusrattr`

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0 (Forts.)

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
PCI Version 2 8.5.9 **PCI Version 3** 8.2.4	Benutzerkennwörter mindestens alle 90 Tage ändern.	Setzt die maximale Gültigkeitsdauer eines Kennworts mit dem Parameter **maxage** auf 13 Wochen.	/etc/security/pscexpert/bin/chusrattr
2.1	Vom Anbieter bereitgestellte Standardwerte vor der Installation eines Systems im Netz immer ändern. Dazu gehören Kennwörter, SNMP-Community-Zeichenfolgen (Simple Network Management Protocol) und das Entfernen nicht benötigter Zeichenfolgen.	Setzt die Anzahl der Wochen, die ein Account mit einem abgelaufenen Kennwort im System verbleibt, mit dem Parameter **maxexpired** auf 8 Wochen.	/etc/security/pscexpert/bin/chusrattr
PCI Version 2 8.5.10 **PCI Version 3** 8.2.3	Mindestkennwortlänge von 7 Zeichen voraussetzen.	Setzt die Mindestkennwortlänge mit dem Parameter **minlen** auf 7 Zeichen.	/etc/security/pscexpert/bin/chusrattr
PCI Version 2 8.5.11 **PCI Version 3** 8.2.3	Kennwörter verwenden, die numerische und alphabetische Zeichen enthalten.	Setzt die Mindestanzahl alphabetischer Zeichen, die in einem Kennwort erforderlich sind, auf 1. Diese Einstellung stellt sicher, dass das Kennwort alphabetische Zeichen enthält, indem der Parameter **minalpha** auf 1 gesetzt wird.	/etc/security/pscexpert/bin/chusrattr
PCI Version 2 8.5.11 **PCI Version 3** 8.2.3	Kennwörter verwenden, die numerische und alphabetische Zeichen enthalten.	Setzt die Mindestanzahl nicht alphabetischer Zeichen, die in einem Kennwort erforderlich sind, auf 1. Diese Einstellung stellt sicher, dass das Kennwort nicht alphabetische Zeichen enthält, indem der Parameter **minother** auf 1 gesetzt wird.	/etc/security/pscexpert/bin/chusrattr
PCI Version 2 2.1 **PCI Version 3** 8.2.2	Vom Anbieter bereitgestellte Standardwerte vor der Installation eines Systems im Netz immer ändern. Dazu gehören Kennwörter, SNMP-Community-Zeichenfolgen (Simple Network Management Protocol) und das Entfernen nicht benötigter Zeichenfolgen.	Setzt die maximale Anzahl an Wiederholungen eines Zeichens in einem Kennwort mit dem Parameter **maxrepeats** auf 8. Diese Einstellung gibt an, dass ein Zeichen in einem Kennwort unbegrenzt wiederholt werden kann, wenn es den anderen Kennwortbeschränkungen entspricht.	/etc/security/pscexpert/bin/chusrattr
PCI Version 2 8.5.12 **PCI Version 3** 8.2.5	Übergabe eines neuen Kennworts, das den letzten vier verwendeten Kennwörtern entspricht, durch Einzelbenutzer nicht zulassen.	Setzt die Anzahl der Wochen, nach denen ein Kennwort wiederverwendet werden kann, mit dem Parameter **histexpire** auf 52.	/etc/security/pscexpert/bin/chusrattr

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0 (Forts.)

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
PCI Version 2 8.5.12 **PCI Version 3** 8.2.5	Übergabe eines neuen Kennworts, das den letzten vier verwendeten Kennwörtern entspricht, durch Einzelbenutzer nicht zulassen.	Setzt die Anzahl der vorherigen Kennwörter, die nicht wiederverwendet werden können, mit dem Parameter **histsize** auf 4.	/etc/security/pscexpert/bin/chusrattr
PCI Version 2 8.5.13 **PCI Version 3** 8.1.6	Wiederholte Zugriffsversuche durch Sperren der Benutzer-ID nach sechs nicht erfolgreichen Versuchen beschränken.	Setzt die Anzahl aufeinanderfolgender nicht erfolgreicher Anmeldeversuche, nach denen ein Account gesperrt wird, mit dem Parameter **loginentries** für jeden Account ohne Rootrechte auf 6.	/etc/security/pscexpert/bin/chusrattr
PCI Version 2 8.5.13 **PCI Version 3** 8.1.6	Wiederholte Zugriffsversuche durch Sperren der Benutzer-ID nach sechs nicht erfolgreichen Versuchen beschränken.	Setzt die Anzahl aufeinanderfolgender nicht erfolgreicher Anmeldeversuche, nach denen ein Port inaktiviert wird, mit dem Parameter **logindisable** auf 6.	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg
PCI Version 2 8.5.14 **PCI Version 3** 8.1.7	Sperrzeit von mindestens 30 Minuten festlegen bzw. Port sperren, bis ein Administrator ihn erneut aktiviert.	Setzt die Sperrzeit für einen Port, der mit dem Attribut *logindisable* inaktiviert wurde, mit dem Parameter **loginreenable** auf 30 (Minuten).	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg
12.3.9	Technologien für Fernzugriff für Anbieter und Geschäftspartner nur bei Bedarf aktivieren und nach Verwendung sofort wieder inaktivieren.	Inaktiviert die Funktion für Rootanmeldung über Fernzugriff, indem die zugehörige Einstellung auf false gesetzt wird. Der Systemadministrator kann die Funktion für Fernanmeldung bei Bedarf aktivieren und unmittelbar nach Abschluss der Task wieder inaktivieren.	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user
8.1.1	Allen Benutzern eine eindeutige ID zuweisen, bevor ihnen der Zugriff auf Systemkomponenten oder Karteninhaberdaten erlaubt wird.	Aktiviert die Funktion, die sicherstellt, dass alle Benutzer einen eindeutigen Benutzernamen haben, um auf Systemkomponenten oder Karteninhaberdaten zugreifen zu können, indem diese Funktion auf true gesetzt wird.	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user
10.2	Prüfung (Auditing) auf dem System aktivieren.	Aktiviert die Prüfung der Binärdateien auf dem System.	/etc/security/pscexpert/bin/pciaudit
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich Common Desktop Environment (CDE), inaktivieren.	Inaktiviert die CDE-Funktion, wenn die Ebene für Layer Four Traceroute (LFT) nicht konfiguriert ist.	/etc/security/pscexpert/bin/comntrows

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0 (Forts.)

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `timed`, inaktivieren.	Stoppt den Dämon `timed` und setzt den entsprechenden Eintrag in der Datei `/etc/rc.tcpip`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/rctcpip`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `rwhod`, inaktivieren.	Stoppt den Dämon `rwhod` und setzt den entsprechenden Eintrag in der Datei `/etc/rc.tcpip`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/rctcpip`
PCI Version 2 2.1 **PCI Version 3** 2.1.1	Vom Anbieter bereitgestellte Standardwerte vor der Installation eines Systems im Netz ändern, einschließlich Inaktivierung des Dämons `SNMP`.	Stoppt den Dämon `SNMP` und setzt den entsprechenden Eintrag in der Datei `/etc/rc.tcpip`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/rctcpip`
PCI Version 2 2.1 **PCI Version 3** 2.1.1	Vom Anbieter bereitgestellte Standardwerte vor der Installation eines Systems im Netz ändern, einschließlich Inaktivierung des Dämons `SNMPMIBD`.	Inaktiviert den Dämon `SNMPMIBD`, indem der entsprechende Eintrag in der Datei `/etc/rc.tcpip`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar gesetzt wird.	`/etc/security/pscexpert/bin/rctcpip`
2.1	Vom Anbieter bereitgestellte Standardwerte vor der Installation eines Systems im Netz ändern, einschließlich Inaktivierung des Dämons `AIXMIBD`.	Inaktiviert den Dämon `AIXMIBD`, indem der entsprechende Eintrag in der Datei `/etc/rc.tcpip`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar gesetzt wird.	`/etc/security/pscexpert/bin/rctcpip`
2.1	Vom Anbieter bereitgestellte Standardwerte vor der Installation eines Systems im Netz ändern, einschließlich Inaktivierung des Dämons `HOSTMIBD`.	Inaktiviert den Dämon `HOSTMIBD`, indem der entsprechende Eintrag in der Datei `/etc/rc.tcpip`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar gesetzt wird.	`/etc/security/pscexpert/bin/rctcpip`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `DPID2`, inaktivieren.	Stoppt den Dämon `DPID2` und setzt den entsprechenden Eintrag in der Datei `/etc/rc.tcpip`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/rctcpip`
PCI Version 2 2.1 **PCI Version 3** 2.2.2	Vom Anbieter bereitgestellte Standardwerte vor der Installation eines Systems im Netz ändern, einschließlich Stoppen des `DHCP`-Servers.	Inaktiviert den `DHCP`-Server.	`/etc/security/pscexpert/bin/rctcpip`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des `DHCP`-Agenten, inaktivieren.	Stoppt und inaktiviert den `DHCP`-Relay-Agenten und setzt den entsprechenden Eintrag in der Datei `/etc/rc.tcpip`, der bewirkt, dass der Agent automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/rctcpip`

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0 (Forts.)

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `rshd`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `rshd` und des Shell-Service und setzt die entsprechenden Einträge in der Datei `/etc/inetd.conf`, die bewirken, dass die Instanzen automatisch gestartet werden, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `rlogind`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `rlogind` und des rlogin-Service. Das Dienstprogramm AIX Security Expert setzt auch die entsprechenden Einträge in der Datei `/etc/inetd.conf`, die bewirken, dass die Instanzen automatisch gestartet werden, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `rexecd`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `rexecd`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `comsat`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `comsat`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `fingerd`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `fingerd`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `systat`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `systat`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0 (Forts.)

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
2.1	Vom Anbieter bereitgestellte Standardwerte vor der Installation eines Systems im Netz ändern, einschließlich Inaktivierung des Befehls `netstat`.	Inaktiviert den Befehl `netstat`, indem der entsprechende Eintrag in der Datei `/etc/inetd.conf` auf Kommentar gesetzt wird.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.3	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `tftp`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `tftp`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `talkd`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `talkd`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `rquotad`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `rquotad`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `rstatd`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `rstatd`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `rusersd`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `rusersd`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0 (Forts.)

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `rwalld`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `rwalld`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `sprayd`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `sprayd`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Dämons `pcnfsd`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `pcnfsd`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Service `TCP`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Service `echo(tcp)`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Service automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des TCP-Service `discard`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Service `discard(tcp)`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Service automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des TCP-Service `chargen`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Service `chargen(tcp)`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Service automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0 (Forts.)

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des TCP-Service `daytime`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Service `daytime(tcp)`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Service automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des TCP-Service `time`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Service `timed(tcp)`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Service automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des Service `UDP`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Service `echo(udp)`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Service automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des UDP-Service `discard`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Service `discard(udp)`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Service automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des UDP-Service `chargen`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Service `chargen(udp)`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Service automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des UDP-Service `daytime`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Service `daytime(udp)`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Service automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0 (Forts.)

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des UDP-Service `time`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Service `timed(udp)`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Service automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.3	Nicht benötigte und nicht sichere Services, einschließlich des `FTP`-Service, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `ftpd`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.3	Nicht benötigte und nicht sichere Services, einschließlich des `telnet`-Service, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `telnetd`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Dämon automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich `dtspc`, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Dämons `dtspc`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inittab`, der bewirkt, dass der Dämon automatisch gestartet wird, wenn LFT nicht konfiguriert und CDE in der Datei `/etc/inittab` inaktiviert ist, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des `ttdbserver`-Service, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Service `ttdbserver`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Service automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 2.2.2	Nicht benötigte und nicht sichere Services, einschließlich des `cmsd`-Service, inaktivieren.	Stoppt und inaktiviert alle Instanzen des Service `cmsd`. Das Dienstprogramm AIX Security Expert setzt auch den entsprechenden Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass der Service automatisch gestartet wird, auf Kommentar.	`/etc/security/pscexpert/bin/cominetdconf`

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0 (Forts.)

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
PCI Version 2 2.2.3 **PCI Version 3** 2.2.4	Systemsicherheitsparameter konfigurieren, um Missbrauch zu verhindern.	Entfernt die SUID-Befehle (Set User ID), indem der entsprechende Eintrag in der Datei `/etc/inetd.conf`, der bewirkt, dass die Befehle automatisch aktiviert werden, auf Kommentar gesetzt wird.	`/etc/security/pscexpert/bin/rmsuidfrmrcmds`
PCI Version 2 2.2.3 **PCI Version 3** 2.2.4	Systemsicherheitsparameter konfigurieren, um Missbrauch zu verhindern.	Aktiviert die niedrigste Sicherheitsstufe für den Dateiberechtigungsmanager (File Permissions Manager).	`/etc/security/pscexpert/bin/filepermgr`
PCI Version 2 2.2.3 **PCI Version 3** 2.2.4	Systemsicherheitsparameter konfigurieren, um Missbrauch zu verhindern.	Ändert das NFS-Protokoll (Network File System) mit eingeschränkten Einstellungen, die den PCI-Sicherheitsanforderungen entsprechen. Zu diesen eingeschränkten Einstellungen gehört die Inaktivierung der Rootanmeldung über Fernzugriff und anonymer UID- und GID-Anmeldungen.	`/etc/security/pscexpert/bin/nfsconfig`
PCI Version 2 2.2.2 **PCI Version 3** 2.2.3	Nur erforderliche und sichere Services, Protokolle, Dämonprozess usw., die für den ordnungsgemäßen Betrieb des Systems erforderlich sind, aktivieren. Sicherheitsfeatures für alle erforderlichen Services, Protokolle und Dämonprozesse, die als nicht sicher eingestuft werden, implementieren.	Inaktiviert die Dämonprozesse `rlogind`, `rshd` und `tftpd`, die nicht sicher sind.	`/etc/security/pscexpert/bin/disrmtdmns`
PCI Version 2 2.2.2 **PCI Version 3** 2.2.3	Nur erforderliche und sichere Services, Protokolle, Dämonprozess usw., die für den ordnungsgemäßen Betrieb des Systems erforderlich sind, aktivieren. Sicherheitsfeatures für alle erforderlichen Services, Protokolle und Dämonprozesse, die als nicht sicher eingestuft werden, implementieren.	Inaktiviert die Dämonprozesse `rlogind`, `rshd` und `tftpd`, die nicht sicher sind.	`/etc/security/pscexpert/bin/rmrhostsnetrc`

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0 (Forts.)

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
PCI Version 2 2.2.2 **PCI Version 3** 2.2.3	Nur erforderliche und sichere Services, Protokolle, Dämonprozess usw., die für den ordnungsgemäßen Betrieb des Systems erforderlich sind, aktivieren. Sicherheitsfeatures für alle erforderlichen Services, Protokolle und Dämonprozesse, die als nicht sicher eingestuft werden, implementieren.	Inaktiviert die Dämonprozesse `logind`, `rshd` und `tftpdpci_rmetchostsequiv`, die nicht sicher sind.	`/etc/security/pscexpert/bin/rmetchostsequiv`
PCI Version 2 1.3.6 **PCI Version 3** 2.2.3	Prüfung mit Statusüberwachung oder Paketfilterung implementieren, bei denen nur eingerichtete Verbindungen im Netz zugelassen werden.	Aktiviert die Netzoption **`clean_partial_conns`**, indem sie auf 1 gesetzt wird.	`/etc/security/pscexpert/bin/ntwkopts`
PCI Version 2 2.2.2 **PCI Version 3** 2.2.3	Prüfung mit Statusüberwachung oder Paketfilterung implementieren, bei denen nur eingerichtete Verbindungen im Netz zugelassen werden.	Aktiviert die TCP-Sicherheit durch Festlegung der Netzoption **`tcp_tcpsecure`** mit dem Wert 7. Diese Einstellung bietet Schutz vor Datenattacken, Zurücksetzungsattacken und TCP-Verbindungsanforderungsattacken (SYN).	`/etc/security/pscexpert/bin/ntwkopts`
1.2	Schutz vor unbefugten Zugriffen auf nicht verwendete Ports.	Konfiguriert das System so, dass die Hosts 5 Minuten lang gesperrt werden, um zu verhindern, dass andere System auf nicht verwendete Ports zugreifen.	`/etc/security/pscexpert/bin/ipsecshunhosthls` **Anmerkung:** Sie können weitere Filterregeln in der Datei `/etc/security/aixpert/bin/filter.txt` angeben. Diese Regeln werden vom Script `ipsecshunhosthls.sh` integriert, wenn Sie das Profil anwenden. Die Einträge müssen im folgenden Format angegeben werden: *`Portnummer`*`:`*`IP-Adresse`*`:` *`Aktion`* Die gültigen Werte für *Aktion* sind `Allow` (Zulassen) und `Deny` (Verweigern).
1.2	Host for Port-Scans schützen.	Konfiguriert das System so, dass anfällige Ports 5 Minuten lang umgangen werden, um Port-Scans zu verhindern.	`/etc/security/pscexpert/bin/ipsecshunports` **Anmerkung:** Sie können weitere Filterregeln in der Datei `/etc/security/aixpert/bin/filter.txt` angeben. Diese Regeln werden vom Script `ipsecshunhosthls.sh` integriert, wenn Sie das Profil anwenden. Die Einträge müssen im folgenden Format angegeben werden: *`Portnummer`*`:`*`IP-Adresse`*`:` *`Aktion`* Die gültigen Werte für *Aktion* sind `Allow` (Zulassen) und `Deny` (Verweigern).
7.1.1	Berechtigungen für die Objekterstellung beschränken.	Setzt die Standardberechtigungen für die Objekterstellung mit dem Parameter **`umask`** auf 22.	`/etc/security/pscexpert/bin/chusrattr`

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0 (Forts.)

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
7.1.1	Systemzugriff beschränken.	Stellt sicher, dass nur die Root-ID in der Datei `cron.allow` aufgelistet wird, und entfernt die Datei `cron.deny` vom System.	`/etc/security/pscexpert/bin/limitsysacc`
6.5.8	Punkt aus Rootpfad entfernen.	Entfernt die Punkte in den folgenden Dateien im Rootausgangsverzeichnis aus der Umgebungsvariablen PATH: • .cshrc • .kshrc • .login • .profile	`/etc/security/pscexpert/bin/rmdotfrmpathroot`
6.5.8	Punkt aus anderen Pfaden als dem Rootpfad entfernen:	Entfernt die Punkte in den folgenden Dateien im Benutzerausgangsverzeichnis aus der Umgebungsvariablen *PATH*: • .cshrc • .kshrc • .login • .profile	`/etc/security/pscexpert/bin/rmdotfrmpathnroot`
2.2.3	Systemzugriff beschränken.	Fügt die Rootbenutzerberechtigung und den Benutzernamen in der Datei `/etc/ftpusers` hinzu.	`/etc/security/pscexpert/bin/chetcftpusers`
2.1	Gastaccount entfernen.	Entfernt den Gastaccount und dessen Dateien.	`/etc/security/pscexpert/bin/execmds`
6.5.2	Starten von Programmen im Inhaltsbereich verhindern.	Aktiviert das Feature SED (Stack Execution Disable).	`/etc/security/pscexpert/bin/sedconfig`
8.2	Sicherstellen, dass kein schwaches Kennwort für Root verwendet wird.	Startet eine Integritätsprüfung für das Rootkennwort und stellt damit sicher, dass ein sicheres Rootkennwort verwendet wird.	`/etc/security/pscexpert/bin/chuserstanza`
PCI Version 2 8.5.15 **PCI Version 3** 8.1.8	Zugriff auf das System durch Festlegung eines Limits für Sitzungsinaktivität beschränken.	Setzt das Limit für die Inaktivitätsdauer auf 15 Minuten. Wenn die Sitzung mehr als 15 Minuten inaktiv ist, müssen Sie das Kennwort erneut eingeben.	`/etc/security/pscexpert/bin/autologoff`
1.3.5	Datenverkehr mit Zugriff auf Karteninhaberinformationen beschränken.	Richtet eine hohe Regulierung des TCP-Datenverkehrs ein, um das Risiko von DoS-Attacken (Denial-of-Service) an Ports zu mindern.	`/etc/security/pscexpert/bin/tcptr_pscexpert`
1.3.5	Sichere Verbindung bei der Migration von Daten aufrecht erhalten.	Aktiviert die automatisierte Erstellung von IPSec-Tunneln (IP Security) zwischen Virtual I/O Server-Instanzen während der Live-Partitionsmigration.	`/etc/security/pscexpert/bin/cfgsecmig`

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0 (Forts.)

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
1.3.5	Beschränkt Pakete von unbekannten Quellen.	Lässt die Pakete von Hardware Management Console zu.	`/etc/security/pscexpert/bin/ipsecpermithostorport`
5.1.1	Antivirensoftware pflegen.	Bewahrt die Systemintegrität durch Erkennen bekannter Typen von Schadsoftware, das Entfernen von Schadsoftware und den Schutz vor Schadsoftware.	`/etc/security/pscexpert/bin/manageITsecurity`
PCI Version 2 Abschnitt 7 **PCI Version 3** Abschnitt 7	Bedarfsgesteuerte Zugriffe verwalten.	Aktiviert die rollenbasierte Zugriffssteuerung (RBAC, Role-based Access Control) durch Erstellung von Benutzerrollen für den Systembediener, den Systemadministrator und den Sicherheitsbeauftragten für Informationssysteme mit den erforderlichen Berechtigungen.	`/etc/security/pscexpert/bin/EnableRbac`
PCI Version 2 In Profilen der Version 2 nicht enthalten, neu in Version 3. **PCI Version 3** 2.3	Weitere Sicherheitsfeatures für alle erforderlichen Services, Protokolle und Dämonprozesse, die als nicht sicher eingestuft werden, implementieren.	Verwendet sichere Technologien wie Secure Shell (SSH), SSH File Transfer Protocol (S-FTP), Secure Sockets Layer (SSL) oder Internet Protocol Security Virtual Private Network (IPsec VPN), um nicht sichere Services wie NetBIOS, Dateifreigabe, Telnet und FTP zu schützen. Außerdem wird der SSH-Dämon so konfiguriert, dass nur das Protokoll SSHv2 verwendet wird.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI Version 2 In Profilen der Version 2 nicht enthalten, neu in Version 3. **PCI Version 3** 2.3	Der SSH-Client muss so konfiguriert werden, dass nur das SSHv2-Protokoll verwendet wird.	Konfiguriert den SSH-Client für die Verwendung des SSHv2-Protokolls.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI Version 2 In Profilen der Version 2 nicht enthalten, neu in Version 3. **PCI Version 3** 2.3	Der SSH-Dämon darf nur für Managementnetzadressen empfangsbereit sein, sofern er nicht für andere Zwecke als Managementzwecke autorisiert ist.	Stellt sicher, dass der SSH-Dämon nur für Empfangsbereitschaft konfiguriert ist.	`/etc/security/pscexpert/bin/sshPCIconfig`

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0 (Forts.)

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
PCI Version 2 In Profilen der Version 2 nicht enthalten, neu in Version 3. **PCI Version 3** 2.3	Der SSH-Dämon muss so konfiguriert werden, dass nur genehmigte Verschlüsselungen gemäß FIPS 140-2 verwendet werden.	Stellt sicher, dass der SSH-Dämon nur die FIPS 140-2-Verschlüsselungen verwenden.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI Version 2 In Profilen der Version 2 nicht enthalten, neu in Version 3. **PCI Version 3** 2.3	Der SSH-Dämon muss so konfiguriert werden, dass nur Nachrichtenauthentifizierungscodes verwendet werden, die die gemäß FIPS 140-2 genehmigten kryptografischen Hashalgorithmen verwenden.	Stellt sicher, dass die Nachrichtenauthentifizierungscodes die genehmigten Algorithmen ausführen.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI Version 2 In Profilen der Version 2 nicht enthalten, neu in Version 3. **PCI Version 3** 2.3	Der SSH-Dämon muss die Möglichkeit der Anmeldung auf bestimmte Benutzer oder Gruppen beschränken.	Beschränkt die Anmeldung am System auf bestimmte Benutzer und Gruppen.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI Version 2 In Profilen der Version 2 nicht enthalten, neu in Version 3. **PCI Version 3** 2.3	Das System muss bei der Anmeldung das Datum und die Uhrzeit der letzten erfolgreichen Accountanmeldung anzeigen.	Verwaltet die Informationen der letzten erfolgreichen Anmeldung und zeigt diese bei der nächsten erfolgreichen Anmeldung an.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI Version 2 In Profilen der Version 2 nicht enthalten, neu in Version 3. **PCI Version 3** 2.3	Der SSH-Dämon muss eine strikte Modusprüfung der Konfigurationsdateien für die Ausgangsverzeichnisse durchführen.	Stellt sicher, dass die Konfigurationsdateien für die Ausgangsverzeichnisse auf die richtigen Modi eingestellt sind.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI Version 2 In Profilen der Version 2 nicht enthalten, neu in Version 3. **PCI Version 3** 2.3	Der SSH-Dämon muss die Trennung von Zugriffsrechten verwenden.	Stellt sicher, dass der SSH-Dämon das richtige Maß von Trennung seiner Zugriffsrechte verwendet.	`/etc/security/pscexpert/bin/sshPCIconfig`

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0 (Forts.)

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
PCI Version 2 In Profilen der Version 2 nicht enthalten, neu in Version 3. **PCI Version 3** 2.3	Der SSH-Dämon darf die RSA-Authentifizierung für rhosts nicht zulassen.	Inaktiviert die RSA-Authentifizierung für rhosts bei der Verwendung des SSH-Dämons.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI Version 2 1.1.5 2.2.2 **PCI Version 3** 10.4	Konfigurationsstandards und -prozesse untersuchen, um sicherzustellen, dass gemäß den PCI-DSS-Anforderungen 6.1 und 6.2 eine Technologie für Zeitsynchronisation implementiert ist und auf dem aktuellen Stand gehalten wird.	Aktiviert den ntp-Dämon.	`/etc/security/pscexpert/bin/rctcpip`
PCI Version 2 In Profilen der Version 2 nicht enthalten, neu in Version 3. **PCI Version 3** 8.1.5	Nicht verwendete Benutzeraccounts inaktivieren.	Inaktiviert Benutzeraccounts nach 35 Tagen Inaktivität.	`/etc/security/pscexpert/bin/disableacctpci`
PCI Version 3 2.2.3	Secure Sockets Layer (SSL) v3 und Transport Layer Security (TLS) v1.0 in Anwendungen inaktivieren.	Inaktiviert SSLv3 und TLS v1.0 in der Konfiguration des Courier-POP3-Servers (Pop3d).	`/etc/security/pscexpert/bin/disableSSL`
PCI Version 3 2.2.3	SSL v3 und TLS v1.0 in Anwendungen inaktivieren.	Inaktiviert SSLV3 und TLS v1.0 im Courier-IMAP-Server (imapd).	`/etc/security/pscexpert/bin/disableSSL`
PCI Version 3 8.2.1	SSL v3 und TLS v1.0 in Anwendungen inaktivieren.	Überprüft, ob TLS 1.1 oder höher für die Sicherheit in der NTP-Konfigurationsdatei (Network Time Protocol) akzeptiert wird.	`/etc/security/pscexpert/bin/checkNTP`
PCI Version 3 2.2.3	SSL v3 und TLS v1.0 in Anwendungen inaktivieren.	Überprüft, ob TLS 1.1 oder höher für die Sicherheit in der FTPD-Konfigurationsdatei (File Transfer Protocol Daemon) akzeptiert wird.	`/etc/security/pscexpert/bin/secureFTP`
PCI Version 3 2.2.3	SSL v3 und TLS v1.0 in Anwendungen inaktivieren.	Überprüft, ob TLS 1.1 oder höher für die Sicherheit in der FTP-Konfigurationsdatei (File Transfer Protocol) akzeptiert wird.	`/etc/security/pscexpert/bin/secureFTP`
PCI Version 3 2.2.3	SSL v3 und TLS v1.0 in Anwendungen inaktivieren.	Inaktiviert SSLv3 und TLS v1.0 in der sendmail-Konfiguration.	`/etc/security/pscexpert/bin/sendmailPCIConfig`
PCI Version 3 2.2.3	SSL v3 und TLS v1.0 in Anwendungen inaktivieren.	Prüft, ob die SSL-Version in AIX höher ist als 1.0.2.	`/etc/security/pscexpert/bin/sslversion`

Tabelle 6. Einstellungen für den Konformitätsstandard PCI-DSS Version 2.0 und Version 3.0 (Forts.)

Implementiert diese PCI-DSS-Standards	Implementierungsspezifikation	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
PCI Version 3 8.2.1	Zwei-Faktor-Authentifizierung erzwingen.	Erzwingt die Zwei-Faktor-Authentifizierung wie SHA-256 oder SHA-512.	`/etc/security/pscexpert/bin/pwdalgchk`

Zugehörige Informationen:

Payment Card Industry - Data Security Standard

Konformität mit Sarbanes-Oxley Act und COBIT

Der Sarbanes-Oxley (SOX) Act von 2002, der auf dem 107. Kongress der USA basiert, dient der Überwachung öffentlicher Unternehmen, die den Sicherheitsgesetzen und zugehörigen Verordnungen unterliegen, um das Interesse von Investoren zu schützen.

SOX Section 404 schreibt die Managementbewertung über interne Kontrollinstrumente vor. In den meisten Organisationen umfassen die internen Kontrollinstrumente die IT-Systeme, die die Finanzdaten des Unternehmens verarbeiten und berichten. SOX Act enthält auch spezielle Details zur IT und IT-Sicherheit. Viele SOX-Prüffunktionen stützen sich auf Standards wie COBIT als Methode für die Messung und Prüfung der richtigen IT-Governance und IT-Steuerung. Die PowerSC Standard Edition-XML-Konfigurationsoption SOX/COBIT stellt die Sicherheitskonfiguration von AIX- und VIOS-Systemen (Virtual I/O Server) bereit, die zur Einhaltung der COBIT-Konformitätsrichtlinien erforderlich ist.

IBM Compliance Expert Express Edition wird unter der folgenden Version des Betriebssystems AIX ausgeführt:

- AIX 6.1
- AIX 7.1
- AIX 7.2

Die Einhaltung externer Standards gehört in den Zuständigkeitsbereich eines AIX-Systemadministrators. IBM Compliance Expert Express Edition vereinfacht die Verwaltung von Betriebssystemeinstellungen und Berichten, die für die Einhaltung von Standards erforderlich sind.

Die mit IBM Compliance Expert Express Edition bereitgestellten vorkonfigurierten Konformitätsprofile verringern den Verwaltungsaufwand, weil die Interpretation der Konformitätsdokumentation und die Implementierung der Standards als spezielle Systemkonfigurationsparameter wegfallen.

Die Funktionalität von IBM Compliance Expert Express Edition ist so konzipiert, dass die Systemvoraussetzungen für die Konformität mit externen Standards effizient verwaltet werden können, um so den Aufwand zu reduzieren und die Konformität zu verbessern. Alle externen Sicherheitsstandards enthalten auch noch andere Aspekte als die Systemkonfigurationseinstellungen. Die Verwendung von IBM Compliance Expert Express Edition kann die Einhaltung von Standards nicht sicherstellen. Compliance Expert vereinfacht die Verwaltung von Systemkonfigurationseinstellungen, sodass Administratoren sich auf andere Aspekte der Einhaltung von Standards konzentrieren können.

Zugehörige Informationen:

COBIT

Health Insurance Portability and Accountability Act (HIPAA)

Health Insurance Portability and Accountability Act (HIPAA) ist ein Sicherheitsprofil, das sich auf den Schutz elektronisch geschützter Gesundheitsdaten (EPHI, Electronically Protected Health Information) konzentriert.

Die HIPAA-Sicherheitsregel konzentriert sich insbesondere auf den Schutz von EPHI und nur ein Teil der Behörden unterliegen je nach ihren Funktionen und der Verwendung von EPHI der HIPAA-Sicherheitsregel.

Alle mit HIPAA abgedeckten Entitäten müssen ähnlich wie einige Bundesbehörden die HIPAA-Sicherheitsregel einhalten.

Die HIPAA-Sicherheitsregel konzentriert sich auf den Schutz der Vertraulichkeit, der Integrität und der Verfügbarkeit von EPHI.

Die EPHI, die von einer durch die Regel abgedeckten Entität erstellt, empfangen, verwaltet oder übertragen werden, müssen vor erwarteten Sicherheitsbedrohungen, Risiken und unzulässiger Verwendung und Offenlegung geschützt werden.

Die Anforderungen, Standards und Implementierungsspezifikationen der HIPAA-Sicherheitsregel gelten für die folgenden Entitäten:

- Anbieter im Gesundheitswesen
- Krankenkassenleistungen
- Clearinghouses im Gesundheitswesen
- Verschreibung von Medikamenten und Sponsoren von Medikamentenkarten

Die folgende Tabelle enthält Details zu den verschiedenen Abschnitten der HIPAA-Sicherheitsregel. Jeder Abschnitt enthält mehrere Standards und Implementierungsspezifikationen.

Anmerkung: Alle angepassten Scriptdateien, die zur Verwaltung der Konformität mit HIPAA bereitgestellt werden, sind im Verzeichnis `/etc/security/pscexpert/bin` enthalten.

Tabelle 7. HIPAA-Regeln und Implementierungsdetails

Abschnitte der HIPAA-Sicherheitsregel	**Implementierungsspezifikation**	**aixpert-Implementierung**	**Befehle und Rückgabewerte**
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 164.312 (b)	Implementiert die Prozeduren für eine regelmäßige Überprüfung der Datensätze der Aktivitäten im Informationssystem, wie z. B. Prüfprotokolle, Zugriffsberichte und Sicherheitsvorfallberichte.	Bestimmt, ob die Prüfung im System aktiviert ist.	**Befehl**: **#audit query**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieser Befehl mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Wert 1.
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 166.312 (b)	Implementiert die Prozeduren für eine regelmäßige Überprüfung der Datensätze der Aktivitäten im Informationssystem, wie z. B. Prüfprotokolle, Zugriffsberichte und Sicherheitsvorfallberichte.	Aktiviert die Prüfung im System. Konfiguriert auch die zu erfassenden Ereignisse.	**Befehl**: **# audit start >/dev/null 2>&1**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieser Befehl mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Wert 1. Die folgenden Ereignisse werden geprüft: **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**

Tabelle 7. HIPAA-Regeln und Implementierungsdetails (Forts.)

Abschnitte der HIPAA-Sicherheitsregel	Implementierungsspezifikation	aixpert-Implementierung	Befehle und Rückgabewerte
164.312 (a) (2) (iV)	Verschlüsselung und Entschlüsselung (A):Implementiert einen Mechanismus für die Verschlüsselung und Entschlüsselung der EPHI.	Bestimmt, ob das verschlüsselte Dateisystem (EFS, Encrypted File System) auf dem System aktiviert wird.	**Befehl**: **# efskeymgr -V >/dev/null 2>&1**. **Rückgabewert**: Wenn EFS bereits aktiviert ist, wird dieser Befehl mit dem Wert 0 beendet. Wenn EFS nicht aktiviert ist, wird dieser Befehl mit dem Wert 1 beendet.
164.312 (a) (2) (iii)	Automatische Abmeldung (A): Implementiert die elektronischen Prozeduren zur Beendigung einer elektronischen Sitzung nach einem vordefinierten Inaktivitätszeitraum.	Konfiguriert das System so, dass die Abmeldung von interaktiven Prozessen nach 15 Minuten Inaktivität erfolgt.	**Befehl**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1** **echo "TMOUT=900 ; TIMEOUT=900; export TMOUT TIMEOUT**. **Rückgabewert**: Wenn der Befehl den Wert **TMOUT=15** nicht findet, wird das Script mit dem Wert 1 beendet. Andernfalls wird der Befehl mit dem Wert 0 beendet.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Stellt sicher, dass alle Kennwörter mindestens 14 Zeichen enthalten.	**Befehl**: **chsec -f /etc/security/user -s user -a minlen=8**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Stellt sicher, dass alle Kennwörter mindestens zwei alphabetische Zeichen enthalten, von denen eines ein Großbuchstabe sein muss.	**Befehl**: **chsec -f /etc/security/user -s user –a minalpha=4**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Setzt die Mindestanzahl nicht alphabetischer Zeichen in einem Kennwort auf 2.	**Befehl**: **#chsec –f /etc/security/user –s user –a minother=2**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Stellt sicher, dass alle Kennwörter keine identischen Zeichen enthalten.	**Befehl**: **#chsec –f /etc/security/user –s user –a maxrepeats=1**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.

Tabelle 7. HIPAA-Regeln und Implementierungsdetails (Forts.)

Abschnitte der HIPAA-Sicherheitsregel	Implementierungsspezifikation	aixpert-Implementierung	Befehle und Rückgabewerte
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Stellt sicher, dass ein Kennwort nicht mit den vorherigen fünf Kennwörtern übereinstimmen darf.	**Befehl**: **#chsec –f /etc/security/user –s user –a histsize=5**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Legt eine maximale Kennwortgültigkeit von 13 Wochen fest.	**Befehl**: **#chsec –f /etc/security/user –s user –a maxage=8**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Entfernt jegliche Anforderung bezüglich der Mindestzeit für die Änderung eines Kennworts.	**Befehl**: **#chsec –f /etc/security/user –s user –a minage=2**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Setzt die maximale Anzahl an Wochen, nach der ein abgelaufenes Kennwort geändert werden muss, nachdem der vom Benutzer mit dem Parameter **maxage** festgelegte Wert abgelaufen ist, auf 4.	**Befehl**: **#chsec –f /etc/security/user –s user –a maxexpired=4**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Setzt die Mindestanzahl der nicht wiederverwendbaren Zeichen aus dem alten Kennwort auf 4.	**Befehl**: **#chsec –f /etc/security/user –s user –a mindiff=4**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Gibt an, dass 5 Tage gewartet wird, bevor das System eine Warnung bezüglich einer erforderlichen Kennwortänderung ausgibt.	**Befehl**: **#chsec –f /etc/security/user –s user –a pwdwarntime = 5**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.

Tabelle 7. HIPAA-Regeln und Implementierungsdetails (Forts.)

Abschnitte der HIPAA-Sicherheitsregel	Implementierungsspezifikation	aixpert-Implementierung	Befehle und Rückgabewerte
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Verifiziert die Richtigkeit von Benutzerdefinitionen und behebt die Fehler.	**Befehl**: **/usr/bin/usrck -y ALL** **/usr/bin/usrck –n ALL**. **Rückgabewertvalue**: Der Befehl gibt keinen Wert zurück. Der Befehl prüft und behebt die Fehler ggf.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Sperrt den Account nach drei aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen.	**Befehl**: **#chsec –f /etc/security/user –s user –a loginretries=3**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Legt eine Verzögerung von 5 Sekunden nach einer nicht erfolgreichen Anmeldung fest, bevor die nächste erfolgt.	**Befehl**: **chsec -f /etc/security/login.cfg -s default -a logindelay=5**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Setzt die Anzahl nicht erfolgreicher Anmeldeversuche an einem Port, bevor der Port gesperrt wird, auf 10.	**Befehl**: **chsec -f /etc/security/lastlog -s username -a \ unsuccessful_login_count=10**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Setzt das Zeitintervall an einem Port für die nicht erfolgreichen Anmeldeversuche vor Inaktivierung des Ports auf 60 Sekunden.	**Befehl**: **#chsec -f /etc/security/lastlog -s user –a time_last_unsuccessful_ login=60**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Setzt das Zeitintervall, nach dem ein inaktivierter Port wieder freigegeben wird, auf 30 Minuten.	**Befehl**: **#chsec -f /etc/security/login.cfg -s default -a loginreenable = 30**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.

Tabelle 7. HIPAA-Regeln und Implementierungsdetails (Forts.)

Abschnitte der HIPAA-Sicherheitsregel	Implementierungsspezifikation	aixpert-Implementierung	Befehle und Rückgabewerte
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Setzt das Zeitintervall für die Eingabe eines Kennworts auf 30 Sekunden.	**Befehl**: **chsec -f /etc/security/login.cfg -s usw -a logintimeout=30**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieses Script mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Fehlercode 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Kennwortmanagement (A):Implementiert die Prozeduren für das Erstellen, Ändern und Schützen von Kennwörtern.	Stellt sicher, dass Accounts nach 35 Tagen Inaktivität gesperrt werden.	**Befehl**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1if TMOUT = (35x24x60x60){#chsec -f /etc/security/user -s user -aaccount_locked = true}**. **Rückgabewert**: Wenn der Befehl den Parameter **account_locked** nicht auf **true** setzen kann, wird das Script mit dem Wert 1 beendet. Andernfalls wird der Befehl mit dem Wert 0 beendet.
164.312 (c) (1)	Implementiert die Richtlinien und Prozeduren für den Schutz der EPHI vor unzulässiger Änderung und Vernichtung.	Aktiviert die TE-Richtlinien (Trusted Execution).	**Befehl**: Aktiviert **CHKEXEC, CHKSHLIB, CHKSCRIPT, CHKKERNEXT, STOP_ON_CHKFAIL,TE=ON, z. B. trustchk –p TE=ON CHKEXEC = ON, CHKSHLIB,=ON, CHKSCRIPT=ON, CHKKERNEXT = ON**. **Rückgabewert**: Bei einem Fehler wird das Script mit dem Wert 1 beendet.
164.312 (e) (1)	Implementiert die technischen Sicherheitsmessungen zur Verhinderung unbefugter Zugriffe auf die EPHI, die über ein elektronisches Kommunikationsnetz übertragen werden.	Bestimmt, ob die **ssh**-Dateigruppen installiert sind. Wenn nicht, wird eine Fehlernachricht angezeigt.	**Befehl**: **# lslpp –l | grep openssh > /dev/null 2>&1**. **Rückgabewert**: Wenn der Befehl den Rückgabecode 0 zurückgibt, wird das Script mit dem Wert 0 beendet. Wenn keine SSH-Dateigruppen installiert sind, wird das Script mit dem Wert 1 beendet und die Fehlernachricht `Install ssh filesets for secure transmission` angezeigt.

Die folgende Tabelle enthält Details zu den verschiedenen Funktionen der HIPAA-Sicherheitsregel. Jede Funktion enthält mehrere Standards und Implementierungsspezifikationen.

Tabelle 8. HIPAA-Funktionen und Implementierungsdetails

HIPAA-Funktionen	Implementierungsspezifikation	aixpert-Implementierung	Befehle und Rückgabewerte
Fehlerprotokollierung	Konsolidiert Fehler aus verschiedenen Protokollen und sendet E-Mails an den Administrator.	Bestimmt, ob Hardwarefehler vorliegen. Bestimmt, ob nicht behebbare Fehler in der **trcfile**-Datei an der Position `/var/adm/ras/trcfile` aufgezeichnet wurden. Sendet die Fehler an **root@<Hostname>**.	**Befehl**: **errpt -d H**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieser Befehl mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Wert 1.

Tabelle 8. HIPAA-Funktionen und Implementierungsdetails (Forts.)

HIPAA-Funktionen	Implementierungsspezifikation	aixpert-Implementierung	Befehle und Rückgabewerte
FPM-Aktivierung	Ändert Dateiberechtigungen.	Ändert die Berechtigungen von Dateien aus einer Liste mit Berechtigungen und Dateien mithilfe des Befehls **fpm**.	**Befehl**: **# fpm -1 <level> -f <Befehlsdatei>**. **Rückgabewert**: Bei erfolgreicher Ausführung wird dieser Befehl mit dem Wert 0 beendet, bei nicht erfolgreicher Ausführung mit dem Wert 1.
RBAC-Aktivierung	Erstellt die Benutzer **isso**, **so** und **sa** und weist den Benutzern entsprechende Rollen zu.	Schlägt vor, die Benutzer **isso**, **so** und **sa** zu erstellen. Weist den Benutzern entsprechende Rollen zu.	**Befehl**: **/etc/security/pscexpert/bin/RbacEnablement**.

Zugehörige Informationen:

Health Insurance Portability and Accountability Act (HIPAA)

NERC-Konformität (North American Electric Reliability Corporation)

North American Electric Reliability Corporation (NERC) ist ein gemeinnütziges Unternehmen, das Standards für die Stromversorgungsbranche entwickelt. PowerSC Standard Edition enthält ein vorkonfiguriertes NERC-Profil, das Sicherheitsstandards unterstützt, mit denen kritische Stromversorgungssysteme geschützt werden können.

Das NERC-Profil entspricht den CIP-Standards (Critical Infrastructure Protection, Schutz kritischer Infrastrukturen).

Sie finden das NERC-Profil im Pfad `/etc/security/aixpert/custom/NERC.xml`. Die auf das NERC-Profil angewendeten CIP-Anforderungen können auf den Standard zurückgesetzt werden, indem das im Verzeichnis `/etc/security/aixpert/custom` enthaltene Profil "NERC_to_AIXDefault.xml" angewendet wird. Dieser Prozess ist nicht dasselbe wie das Widerrufen des NERC-Profils.

Die folgende Tabelle enthält Informationen zu den CIP-Standards, die auf das Betriebssystem AIX angewendet werden, sowie Informationen zur Behandlung der CIP-Standards in PowerSC Standard Edition:

Tabelle 9. CIP-Standards für PowerSC Standard Edition

CIP-Standard	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
CIP-003-3 R5.1	Konfiguriert Systemsicherheitsparameter, um Probleme zu verhindern, indem die SUID- (set-user identification) und SGID-Attribute (set-group identification) aus den Binärdateien entfernt werden.	• `/etc/security/pscexpert/bin/filepermgr` • `/etc/security/pscexpert/bin/rmsuidfrmrcmds`
CIP-003-3 R5.1.1	Aktiviert die rollenbasierte Zugriffssteuerung (RBAC, Role-based Access Control) durch Erstellung von Benutzerrollen für den Systembediener, den Systemadministrator und den Sicherheitsbeauftragten für Informatiossysteme mit den erforderlichen Berechtigungen.	`/etc/security/pscexpert/bin/EnableRbac`
CIP-005-3a R2.1-R2.4	Aktiviert Secure Shell (SSH) für den Sicherheitszugriff.	`/etc/security/pscexpert/bin/sshstart`

Tabelle 9. CIP-Standards für PowerSC Standard Edition (Forts.)

CIP-Standard	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
CIP-005-3a R2.5 CIP-007-5 R1.1	Inaktiviert die folgenden unnötigen und nicht sicheren Services: • **lpd**-Dämon • Common Desktop Environment (CDE)	`/etc/security/pscexpert/bin/comntrows`
CIP-005-3a R2.5 CIP-007-5 R1.1	Inaktiviert die folgenden unnötigen und nicht sicheren Services: • **timed**-Dämon • **NTP**-Dämon • **rwhod**-Dämon • **DPID2**-Dämon • DHCP-Agent	`/etc/security/pscexpert/bin/rctcpip`
CIP-005-3a R2.5 CIP-007-5 R1.1	Inaktiviert die folgenden unnötigen und nicht sicheren Services: • **comsat**-Dämon • **dtspcd**-Dämon • **fingerd**-Dämon • **ftpd**-Dämon • **rshd**-Dämon • **rlogind**-Dämon • **rexecd**-Dämon • **systat**-Dämon • **tfptd**-Dämon • **talkd**-Dämon • **rquotad**-Dämon • **rstatd**-Dämon • **rusersd**-Dämon • **rwalld**-Dämon • **sprayd**-Dämon • **pcnfsd**-Dämon • **telnet**-Dämon • cmsd-Service • ttdbserver-Service • TCP-Service echo • TCP-Service discard • TCP-Service chargen • TCP-Service daytime • TCP-Service time • UDP-Service echo • UDP-Service discard • UDP-Service chargen • UDP-Service daytime • UDP-Service time	`/etc/security/pscexpert/bin/cominetdconf`
CIP-005-3a R2.5 CIP-007-5 R1.1	Setzt die Denial-of-Service-Anforderung für die Risikominderung an Ports durch.	`/etc/security/pscexpert/bin/tcptr_aixpert`
CIP-005-3a R3 CIP-007-3a R5, R6.5 CIP-007-5 R4.4	Aktiviert die Prüfung der binären Dateien auf dem System.	`/etc/security/pscexpert/bin/pciaudit`

Tabelle 9. CIP-Standards für PowerSC Standard Edition (Forts.)

CIP-Standard	AIX Security Expert-Implementierung	Position des Scripts, das den Wert ändert
CIP-007-3a R3 CIP-007-5 R2.1	Zeigt eine Nachricht zum Aktivieren von Trusted Network Connect (TNC) an.	/etc/security/pscexpert/bin/GeneralMsg
CIP-007-3a R4 CIP-007-5 R3.3	Bewahrt die Systemintegrität durch Erkennen bekannter Typen von Schadsoftware, das Entfernen von Schadsoftware und den Schutz vor Schadsoftware.	/etc/security/pscexpert/bin/manageITsecurity
CIP-007-3a R5.2.1	Ermöglicht eine Kennwortänderung bei der ersten Anmeldung für alle Standardbenutzeraccounts, die nicht gesperrt sind.	/etc/security/pscexpert/bin/pwdchg
CIP-007-3a R5.2.2-R5.2.3	Sperrt alle Benutzeraccounts.	/etc/security/pscexpert/dodv2/lockacc_rlogin
CIP-007-3a R5.3.1	Legt eine Mindestlänge von 6 Zeichen für jedes Kennwort fest.	/etc/security/pscexpert/bin/chusrattr
CIP-007-5 R5.5.1	Legt eine Mindestlänge von 8 Zeichen für jedes Kennwort fest.	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R5.3.2 CIP-007-5 R5.5.2	Legt fest, dass jedes Kennwort aus einer Kombination aus alphanumerischen, numerischen und Sonderzeichen bestehen muss.	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R5.3.3 CIP-007-5 R5.6	Ändert jedes Kennwort jährlich.	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R7	Zeigt eine Nachricht zum Aktivieren von Encrypted File System (EFS) an.	/etc/security/pscexpert/bin/GeneralMsg
CIP-007-5 R5.7	Beschränkt die Anzahl nicht erfolgreicher Authentifizierungsversuche.	/etc/security/pscexpert/bin/chusrattr
CIP-010-1 CIP-010-2 R2.1	Zeigt eine Nachricht zum Aktivieren von Real Time Compliance (RTC) an.	/etc/security/pscexpert/bin/GeneralMsg

Zugehörige Informationen:

North American Electric Reliability Corporation

Automation von Sicherheit und Konformität verwalten

Im Folgenden werden die Planung und Implementierung von PowerSC-Profilen für die Automation von Sicherheit und Konformität für eine Gruppe von Systemen gemäß den akzeptierten IT-Governance- und Konformitätsprozeduren beschrieben.

Im Rahmen der Konformität und IT-Governance müssen Systeme, auf denen ähnliche Workloads und Sicherheitsklassen von Daten ausgeführt werden, konsistent verwaltet und konfiguriert werden. Führen Sie zum Planen und Implementieren der Konformität auf Systemen die folgenden Aufgaben aus:

Arbeitsgruppen des Systems ermitteln

In den Konformitäts- und IT-Governance-Richtlinien ist festgelegt, dass die Systeme, auf denen ähnliche Workloads und Sicherheitsklassen von Daten ausgeführt werden, konsistent verwaltet und konfiguriert werden müssen. Deshalb müssen Sie alle Systeme in einer ähnlichen Arbeitsgruppe ermitteln.

Nicht in der Produktionsumgebung implementiertes Testsystem für die Erstkonfiguration verwenden

Wenden Sie das entsprechende PowerSC-Konformitätsprofil auf das Testsystem an.

Verwenden Sie zum Anwenden von Konformitätsprofilen auf das Betriebssystem AIX die folgenden Beispiele als Anleitung.

Beispiel 1: `DoD.xml` anwenden

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

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

In diesem Beispiel gibt es keine fehlgeschlagenen Regeln, d. h. `Failedrules=0`. Das bedeutet, dass alle Regeln erfolgreich angewendet wurden und dass die Testphase eingeleitet werden kann. Beim Auftreten von Fehlern wird eine detaillierte Ausgabe generiert.

Beispiel 2: `PCI.xml` mit einem Fehler anwenden

```
# 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
```

Der Fehler bei der Regel `pci_grpck` muss behoben werden. Zu den möglichen Fehlerursachen gehören die folgenden:

- Die Regel ist für die Umgebung nicht zutreffend und muss entfernt werden.
- Es liegt ein Problem auf dem System vor, das behoben werden muss.

Fehlgeschlagene Regel untersuchen

In den meisten Fällen tritt beim Anwenden eines PowerSC-Sicherheits- und -Konformitätsprofils kein Fehler auf. Das System kann jedoch Komponenten für die Installation voraussetzen, die fehlen, oder es können andere Probleme auftreten, die vom Administrator behoben werden müssen.

Die Ursache für den Fehler kann mithilfe des folgenden Beispiels untersucht werden:

Sehen Sie sich die Datei `/etc/security/aixpert/custom/PCI.xml` an und suchen Sie die fehlgeschlagene Regel. In diesem Beispiel handelt es sich um die Regel `pci_grpck`. Führen Sie den Befehl **fgrep** aus, suchen Sie die fehlgeschlagene Regel `pci_grpck` und sehen Sie sich die zugeordnete XML-Regel an.

```
fgrep -p pci_grpck /etc/security/aixpert/custom/PCI.xml
<AIXPertEntry name="pci_grpck" function="grpck"
<AIXPertRuleType type="DLS"/
<AIXPertDescription&gt;Implementiert Teile von PCI Section 8.2,
Gruppendefinitionen prüfen: Überprüft die Richtigkeit der Gruppendefinitionen
und behebt die Fehler
</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
```

In der Regel `pci_grpck` sehen Sie den Befehl `/usr/sbin/grpck`.

Fehlgeschlagene Regel aktualisieren

Beim Anwenden eines PowerSC-Sicherheits- und -Konformitätsprofils können Sie Fehler feststellen.

Auf dem System können Installationsvoraussetzungen fehlen oder es können andere Probleme vorliegen, die vom Administrator behoben werden müssen. Nachdem Sie den Befehl, der der fehlgeschlagenen Regel zugrunde liegt, bestimmt haben, untersuchen Sie das System, um den fehlgeschlagenen Konfigurationsbefehl zu ermitteln. Möglicherweise liegt ein Sicherheitsproblem auf dem System vor. Es ist auch möglich, dass eine bestimmte Regel für die Umgebung des Systems nicht zutreffend ist. In diesem Fall muss ein angepasstes Sicherheitsprofil erstellt werden.

Angepasstes Sicherheitskonfigurationsprofil erstellen

Wenn eine Regel für die jeweilige Umgebung des Systems nicht zutrifft, lassen die meisten Konformitätsorganisationen dokumentierte Ausnahmen zu.

Führen Sie die folgenden Schritte aus, um eine Regel zu entfernen und eine angepasste Sicherheitsrichtlinie und Konfigurationsdatei zu erstellen:

1. Kopieren Sie den Inhalt der folgenden Dateien in eine einzige Datei mit dem Namen `/etc/security/aixpert/custom/<my_security_policy>.xml`:

   ```
   /etc/security/aixpert/custom/[PCI.xml|DoD.xml|SOX-COBIT.xml]
   ```

2. Bearbeiten Sie die Datei `<my_security_policy>.xml`, indem Sie die nicht zutreffende Regel ab dem Anfangs-XML-Tag `<AIXPertEntry Name...` bis zum End-XML-Tag `</AIXPertEntry` entfernen.

Sie können weitere Konfigurationsregeln für die Sicherheit einfügen. Fügen Sie die weiteren Regeln im `AIXPertSecurityHardening`-XML-Schema ein. Die PowerSC-Profile können nicht direkt geändert werden, aber Sie können die Profile anpassen.

Für die meisten Umgebungen müssen Sie eine angepasste XML-Richtlinie erstellen. Zur Verteilung eines angepassten Profils an andere Systeme müssen Sie die angepasste XML-Richtlinie sicher auf das System kopieren, das dieselbe Konfiguration erfordert. Es wird ein sicheres Protokoll wie Secure File Transfer Protocol (SFTP) für die Verteilung einer angepassten XML-Richtlinie an andere Systeme verwendet und das Profil wird an der sicheren Position `/etc/security/aixpert/custom/<my_security_policy.xml>/etc/security/aixpert/custom/` gespeichert.

Melden Sie sich an dem System an, auf dem ein angepasstes Profil erstellt werden muss, und führen Sie den folgenden Befehl aus:

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

Anwendungen mit AIX Profile Manager testen

Die Sicherheitskonfigurationen können sich auf Anwendungen und auf den Zugriff und die Verwaltung von Systemen auswirken. Es ist wichtig, die Anwendungen und die erwarteten Managementmethoden des Systems vor der Implementierung des Systems in einer Produktionsumgebung zu testen.

Die Standards für die Einhaltung von Vorschriften erfordern eine Sicherheitskonfiguration, die strikter ist als eine Out-of-the-box-Konfiguration. Führen Sie zum Testen des Systems die folgenden Schritte aus:

1. Wählen Sie auf der Einführungsseite von AIX Profile Manager im rechten Teilfenster **View and Manage profiles** aus.
2. Wählen Sie das Profil aus, das von der Vorlage für die Implementierung auf den zu überwachenden Systemen verwendet wird.
3. Klicken Sie auf **Compare**.
4. Wählen Sie die verwaltete Gruppe oder einzelne Systeme innerhalb der Gruppe aus und klicken Sie dann auf **Add**, um Sie dem ausgewählten Feld hinzuzufügen.
5. Klicken Sie auf **OK**.

Der Vergleichsoperation wird gestartet.

Kontinuierliche Konformität von Systemen mit AIX Profile Manager überwachen

Die Sicherheitskonfigurationen können sich auf Anwendungen und auf den Zugriff und die Verwaltung von Systemen auswirken. Es ist wichtig, die Anwendungen und die erwarteten Managementmethoden des Systems bei der Implementierung des Systems in einer Produktionsumgebung zu überwachen.

Führen Sie die folgenden Schritte aus, um ein AIX-System mit AIX Profile Manager zu überwachen:

1. Wählen Sie auf der Einführungsseite von AIX Profile Manager im rechten Teilfenster **View and Manage profiles** aus.
2. Wählen Sie das Profil aus, das von der Vorlage für die Implementierung auf den zu überwachenden Systemen verwendet wird.
3. Klicken Sie auf **Compare**.
4. Wählen Sie die verwaltete Gruppe oder einzelne Systeme innerhalb der Gruppe aus und fügen Sie sie dem ausgewählten Feld hinzu.
5. Klicken Sie auf **OK**.

Der Vergleichsoperation wird gestartet.

PowerSC-Sicherheits- und -Konformitätsautomation konfigurieren

Im Folgenden wird beschrieben, wie Sie PowerSC für die Sicherheits- und Konformitätsautomation über die Befehlszeile oder AIX Profile Manager konfigurieren.

Einstellungen für PowerSC-Konformitätsoptionen konfigurieren

Im Folgenden werden die Grundlagen des PowerSC-Features Security and Compliance Automation, das Testen der Konfiguration auf Testsystemen, die nicht im Produktionsbetrieb eingesetzt werden, sowie die Planung und Implementierung der Einstellungen beschrieben. Wenn Sie eine Konformitätskonfiguration anwenden, ändern die Einstellung zahlreiche Konfigurationseinstellungen im Betriebssystem.

Anmerkung: In einigen Konformitätsstandards und -profilen ist Telnet inaktiviert, weil Telnet Klartextkennwörter verwendet. Deshalb muss Open SSH installiert, konfiguriert und funktionsfähig sein. Sie können aber auch jedes andere sichere Kommunikationsmittel für das zu konfigurierende System verwenden. Diese Konformitätsstandards erfordern die Inaktivierung der `Rootanmeldung`. Konfigurieren Sie mindestens einen Benutzer ohne Rootrechte, bevor Sie mit dem Anwenden der Konfigurationsänderungen fortfahren. Bei dieser Konfiguration wird Root nicht inaktiviert, und Sie können sich als Benutzer ohne Rootrechte anmelden und dann mit dem Befehl **su** einen Benutzerwechsel zu Root vornehmen. Testen Sie, ob Sie die SSH-Verbindung zum System herstellen können. Melden Sie sich als Benutzer ohne Rootrechte an und führen Sie dann den Befehl zum Wechsel zum `Rootbenutzer` aus.

Verwenden Sie für den Zugriff auf die DoD-, PCI-, SOX- und COBIT-Konfigurationsprofile das folgende Verzeichnis:

- Die Profile im Betriebssystem AIX werden im Verzeichnis `/etc/security/aixpert/custom` gespeichert.
- Die Profile in Virtual I/O Server (VIOS) werden im Verzeichnis `/etc/security/aixpert/core` gespeichert.

PowerSC-Konformität über die Befehlszeile konfigurieren

Sie können das Konformitätsprofil mit dem Befehl **pscxpert** auf dem AIX-System und mit dem Befehl **viosecure** in Virtual I/O Server (VIOS) implementieren oder prüfen.

Zum Anwenden der PowerSC-Konformitätsprofile auf einem AIX-System geben Sie einen der folgenden Befehle ein. Welchen Befehl Sie eingeben müssen, richtet sich nach der Stufe der Sicherheitskonformität,

die Sie anwenden möchten.

Tabelle 10. PowerSC-Befehle für AIX

Befehl	Konformitätsstandard
% pscxpert -f /etc/security/aixpert/custom/DoD.xml	*US Department of Defense UNIX Security Technical Implementation Guide*
% pscxpert -f /etc/security/aixpert/custom/Hipaa.xml	*Heath Insurance Portability and Accountability Act*
% pscxpert -f /etc/security/aixpert/custom/PCI.xml	*Payment Card Industry Data Security Standard*
% pscxpert -f /etc/security/aixpert/custom/SOX-COBIT.xml	*Sarbanes-Oxley Act of 2002 – COBIT IT Governance*

Zum Anwenden der PowerSC-Konformitätsprofile auf einem VIOS-System geben Sie einen der folgenden Befehle ein. Welchen Befehl Sie eingeben müssen, richtet sich nach der Stufe der Sicherheitskonformität, die Sie anwenden möchten.

Tabelle 11. PowerSC-Befehle für Virtual I/O Server

Befehl	Konformitätsstandard
% viosecure -file /etc/security/aixpert/custom/DoD.xml	*US Department of Defense UNIX Security Technical Implementation Guide*
% viosecure -file /etc/security/aixpert/custom/Hipaa.xml	*Heath Insurance Portability and Accountability Act*
% viosecure -file /etc/security/aixpert/custom/PCI.xml	*Payment Card Industry Data Security Standard*
% viosecure -file /etc/security/aixpert/custom/SOX-COBIT.xml	*Sarbanes-Oxley Act of 2002 – COBIT IT Governance*

Die Ausführung des Befehls **pscxpert** auf dem AIX-System und die Ausführung des Befehls **viosecure** in VIOS können eine gewisse Zeit dauern, weil beide Befehle das vollständige System prüfen bzw. konfigurieren und sicherheitsrelevante Konfigurationsänderungen vornehmen. Die Ausgabe gleicht dem folgenden Beispiel:

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

Einige Regeln schlagen jedoch je nach AIX-Umgebung, Installationsgruppe und früherer Konfiguration fehl.

Eine vorausgesetzte Regel kann beispielsweise fehlschlagen, weil die erforderliche Installationsdateigruppe nicht auf dem System vorhanden ist. Sie müssen jeden Fehler untersuchen und beheben, bevor Sie die Konformitätsprofile im Rechenzentrum implementieren.

Zugehörige Konzepte:

„Automation von Sicherheit und Konformität verwalten" auf Seite 98
Im Folgenden werden die Planung und Implementierung von PowerSC-Profilen für die Automation von Sicherheit und Konformität für eine Gruppe von Systemen gemäß den akzeptierten IT-Governance- und Konformitätsprozeduren beschrieben.

PowerSC-Konformität mit AIX Profile Manager konfigurieren

Im Folgenden wird die Prozedur zum Konfigurieren der PowerSC-Sicherheits- und -Konformitätsprofile und zum Implementieren der Konfiguration auf einem verwalteten AIX-System mit AIX Profile Manager beschrieben.

Führen Sie zum Konfigurieren der PowerSC-Sicherheits- und -Konformitätsprofile mit AIX Profile Manager die folgenden Schritte aus:

1. Melden Sie sich bei IBM Systems Director an und wählen Sie AIX Profile Manager aus.
2. Erstellen Sie wie folgt eine Vorlage, die auf einem der PowerSC-Sicherheits- und -Konformitätsprofile basiert:
   a. Klicken Sie auf der Einführungsseite von AIX Profile Manager im rechten Teilfenster auf **View and manage templates**.

b. Klicken Sie auf **Create**.
c. Klicken Sie in der Liste **Template type** auf **Operating System**.
d. Geben Sie im Feld **Configuration template name** einen Namen für die Vorlage ein.
e. Klicken Sie auf **Continue** > **Save**.

3. Wählen Sie das Profil aus, das Sie für die Vorlage verwenden möchten. Klicken Sie dazu unterhalb der Option **Select which profile to use for this template** auf **Browse**. In den Profilen werden die folgenden Elemente angezeigt:
   - `ice_DLS.xml`: Standardsicherheitsstufe des Betriebssystems AIX
   - `ice_DoD.xml`: Sicherheits- und Implementierungsrichtlinie des US-Verteidigungsministeriums für UNIX-Einstellungen
   - `ice_HLS.xml`: Generische Sicherheit für AIX-Einstellungen auf hoher Ebene
   - `ice_LLS.xml`: Sicherheit für AIX-Einstellungen auf unterer Ebene
   - `ice_MLS.xml`: Sicherheit für AIX-Einstellungen auf mittlerer Ebene
   - `ice_PCI.xml`: PCI-Einstellung (Payment Card Industry) für das Betriebssystem AIX
   - `ice_SOX.xml`: SOX- oder COBIT-Einstellungen für das Betriebssystem AIX
4. Entfernen Sie alle Profile aus dem ausgewählten Feld.
5. Wählen Sie **Add** aus, um das erforderliche Profil in das ausgewählte Feld zu verschieben.
6. Klicken Sie auf **Save**.

Gehen Sie zum Implementieren der Konfiguration auf einem verwalteten AIX-System wie folgt vor:

1. Wählen Sie auf der Einführungsseite von AIX Profile Manager im rechten Teilfenster **View and Manage Templates** aus.
2. Wählen Sie die zu implementierende erforderliche Vorlage aus.
3. Klicken Sie auf **Deploy**.
4. Wählen Sie die Systeme für die Implementierung des Profils aus und klicken Sie dann auf **Add**, um das erforderliche Profil in das ausgewählte Feld zu verschieben.
5. Klicken Sie auf **OK**, um die Konfigurationsvorlage zu implementieren. Daraufhin wird das System entsprechend der ausgewählten Vorlage des Profils konfiguriert.

Damit die Implementierung für DoD, PCI und SOX erfolgreich durchgeführt wird, muss PowerSC Standard Edition am Endpunkt des AIX-Systems installiert sein. Wenn PowerSC nicht auf dem Implementierungssystem installiert ist, schlägt die Implementierung fehl. IBM Systems Director implementiert die Konfigurationsvorlage auf den Endpunkten des ausgewählten AIX-Systems und konfiguriert sie entsprechend den Konformitätsanforderungen.

Zugehörige Informationen:

AIX Profile Manager

IBM Systems Director

PowerSC Real Time Compliance

Das Feature PowerSC Real Time Compliance überwacht aktivierte AIX-Systeme fortlaufend, um sicherzustellen, dass sie konsistent und sicher konfiguriert sind.

Das Feature PowerSC Real Time Compliance arbeitet mit den PowerSC Compliance Automation- und AIX Security Expert-Richtlinien, um Benachrichtigungen zu versenden, Konformitätsverstöße auftreten oder wenn sich eine überwachte Datei ändert. Wenn gegen die Sicherheitskonfigurationsrichtlinie eines Systems verstoßen wird, sendet das Feature PowerSC Real Time Compliance eine E-Mail oder eine Textnachricht, um den Systemadministrator darüber zu benachrichtigen.

Das Feature PowerSC Real Time Compliance ist ein passives Sicherheitsfeature, das vordefinierte und geänderte Konformitätsprofile unterstützt, zu denen Department of Defense Security Technical Implementation Guide, Payment Card Industry Data Security Standard, Sarbanes-Oxley Act und COBIT gehören. Das Feature stellt eine Standardliste mit Dateien bereit, die auf Änderungen hin überwacht werden, aber Sie können der Liste Dateien hinzufügen.

PowerSC Real Time Compliance installieren

Das Feature PowerSC Real Time Compliance wird mit PowerSC Standard Edition Version 1.1.4 oder höher installiert und ist nicht Teil des AIX-Basisbetriebssystems.

Führen Sie zum Installieren von PowerSC Standard Edition die folgenden Schritte aus:

1. Stellen Sie sicher, dass eines der folgenden AIX-Betriebssysteme auf dem System ausgeführt wird, auf dem Sie das Feature PowerSC Standard Edition installieren:
   - IBM AIX 6 with Technology Level 7 oder höher mit AIX Event Infrastructure for AIX und AIX Clusters (bos.ahafs 6.1.7.0) oder höher
   - IBM AIX 7 with Technology Level 1 oder höher mit AIX Event Infrastructure for AIX und AIX Clusters (bos.ahafs 7.1.1.0) oder höher
   - AIX Version 7.2 oder höher mit AIX Event Infrastructure for AIX und AIX Clusters (bos.ahafs 7.2.0.0) oder höher
2. Zum Aktualisieren oder Installieren der Dateigruppe für das Feature PowerSC Standard Edition installieren Sie die Dateigruppe `powerscStd.rtc` aus dem Installationspaket für PowerSC Standard Edition Version 1.1.4 oder höher.

PowerSC Real Time Compliance konfigurieren

Sie können PowerSC Real Time Compliance so konfigurieren, dass Alerts gesendet werden, wenn Verstöße gegen ein Konformitätsprofil bzw. Änderungen an einer überwachten Datei erkannt werden. Beispiele für diese Profile sind Department of Defense Security Technical Implementation Guide, Payment Card Industry Data Security Standard, Sarbanes-Oxley Act und COBIT.

Sie können PowerSC Real Time Compliance mit einer der folgenden Methoden konfigurieren:

- Geben Sie den Befehl **mkrtc** ein.
- Führen Sie das Tool SMIT mit dem folgenden Befehl aus:

  ```
  smit RTC
  ```

Vom Feature PowerSC Real Time Compliance überwachte Dateien angeben

Das Feature PowerSC Real Time Compliance überwacht eine Standardliste von Dateien aus den übergeordneten Sicherheitseinstellungen auf Änderungen hin. Diese Dateiliste kann durch Hinzufügen und Entfernen von Dateien in der Datei `/etc/security/rtc/rtcd_policy.conf` angepasst werden.

Die Konformitätsvorlage, die auf ein System angewendet wird, kann mit zwei Methoden angegeben werden. Eine Methode ist der Befehl **pscxpert** und die andere Methode ist die Verwendung von AIX Profile Manager mit IBM Systems Director.

Nachdem Sie das Konformitätsprofil angegeben haben, können Sie der Liste der zu überwachenden Dateien weitere Dateien hinzufügen, indem Sie sie in die Datei `/etc/security/rtc/rtcd_policy.conf` einschließen. Nach dem Speichern der Datei wird die neue Liste sofort als Baseline verwendet und auf Änderungen hin überwacht, ohne das System erneut zu starten.

Alerts für PowerSC Real Time Compliance festlegen

Sie müssen die Benachrichtigung durch das Feature PowerSC Real Time Compliance konfigurieren, indem Sie den Typ der Alerts und die Empfänger der Alerts angeben.

Der rtcd-Dämon, der die Hauptkomponente des Features PowerSC Real Time Compliance ist, ruft seine Informationen zu den Typen von Alerts und Empfängern aus der Konfigurationsdatei `/etc/security/rtc/rtcd.conf` ab. Sie können diese Datei in einem Texteditor bearbeiten, um die Informationen zu aktualisieren.

Zugehörige Informationen:

Format der Datei /etc/security/rtc/rtcd.conf für Real-Time Compliance

Trusted Boot

Das Feature Trusted Boot verwendet das Virtual Trusted Platform Module (VTPM), eine virtuelle Instanz des Trusted Computing Group-TPM. Das VTPM wird verwendet, um die Messwerte des Systemboots für künftige Verifizierung sicher zu speichern.

Trusted Boot-Konzepte

Es ist wichtig, dass Sie die Integrität des Bootprozesses verstehen und wissen, wie ein Bootprozess als vertrauenswürdiger oder nicht vertrauenswürdiger Bootprozess klassifiziert wird.

Sie können mit der Hardware Management Console (HMC) maximal 60 logische Partitionen (LPAR) mit aktiviertem VTPM für jedes physische System konfigurieren. Sofern konfiguriert, ist das VTPM für jede LPAR eindeutig. Zusammen mit der AIX-Technologie Trusted Execution bietet das VTPM Sicherheit und Zusicherung für die folgenden Partitionen:

- Boot-Image auf der Platte
- Vollständiges Betriebssystem
- Anwendungsebenen

Ein Administrator kann vertrauenswürdige und nicht vertrauenswürdige Systeme über eine zentrale Konsole anzeigen, die mit der im AIX-Erweiterungspaket verfügbaren Prüffunktion **openpts** installiert wird. Die **openpts**-Konsole verwaltet einen oder mehrere Power Systems-Server und überwacht oder attestiert den Vertrauensstatus von AIX Profile Manager-Systemen im Rechenzentrum. Attestierung ist der Prozess, bei dem die Prüffunktion feststellt (oder attestiert), ob ein Collector einen vertrauenswürdigen Bootprozess ausgeführt hat.

Vertrauenswürdiger Bootstatus

Eine Partition wird als vertrauenswürdig eingestuft, wenn die Prüffunktion die Integrität des Collectors erfolgreich attestiert. Die Prüffunktion ist die ferne Partition, die bestimmt, ob ein Collector einen vertrauenswürdigen Bootprozess ausgeführt hat. Der Collector ist die AIX-Partition, der ein VTPM (Virtual Trusted Platform Module) zugeordnet ist und auf der Trusted Software Stack (TSS) installiert ist. Er zeigt an, dass die im VTPM aufgezeichneten Messwerte mit einem Referenzsatz in der Prüffunktion überstimmen. Ein Trusted Boot-Status zeigt an, ob die Partition in vertrauenswürdiger Weise gebootet wurde. Diese Aussage bezieht sich auf die Integrität des Systembootprozesses und nicht auf die aktuelle oder kontinuierliche Sicherheitsstufe des Systems.

Nicht vertrauenswürdiger Bootstatus

Einer Partition wird der Status nicht vertrauenswürdig zugewiesen, wenn die Prüffunktion die Integrität des Bootprozesses nicht erfolgreich attestieren kann. Dieser Status zeigt an, dass ein Aspekt des Bootprozesses mit den Referenzinformationen in der Prüffunktion nicht konsistent ist. Zu den möglichen Ursachen für eine fehlgeschlagene Attestierung gehören das Booten über eine andere Booteinheit, das Booten eines anderen Kernel-Image und das Ändern des vorhandenen Boot-Image.

Zugehörige Konzepte:

„Fehlerbehebung bei Trusted Boot" auf Seite 112
Im Folgenden sind einige der gängigen Szenarien und Fehlerbehebungsschritte beschrieben, die ausgeführt werden müssen, um den Grund für Attestierungsfehler bei der Verwendung von Trusted Boot zu ermitteln.

Planung für Trusted Boot

Im Folgenden werden die erforderlichen Hardware- und Softwarekonfigurationen für die Installation von Trusted Boot beschrieben.

Voraussetzungen für Trusted Boot

Die Installation von Trusted Boot umfasst die Konfiguration des Collectors und der Prüffunktion.

Wenn Sie die erneute Installation des Betriebssystems AIX auf einem System vorbereiten, auf dem Trusted Boot bereits installiert ist, müssen Sie die Datei `/var/tss/lib/tpm/system.data` kopieren und nach Abschluss der erneuten Installation dann die Datei an derselben Position überschreiben. Wenn Sie diese Datei nicht kopieren, müssen Sie das virtualisierte TPM über die Managementkonsole entfernen und anschließend erneut auf der Partition installieren.

Collector

Im Folgenden sind verschiedene Konfigurationsanforderungen für die Installation eines Collectors beschrieben:

- POWER7-Hardware auf einem 740-Firmware-Release
- Installation von IBM AIX 6 with Technology Level 7 oder Installation von IBM AIX 7 with Technology Level 1
- Installation von Hardware Management Console (HMC) Version 7.4 oder höher
- Konfiguration der Partition mit VTPM und mindestens 1 GB Hauptspeicher
- Installation von Secure Shell (SSH), z. B. OpenSSH oder eine äquivalente Funktionalität

Prüffunktion

Die Prüffunktion **openpts** kann über die Befehlszeilenschnittstelle und die grafische Benutzerschnittstelle, die auf einer Reihe von Plattformen ausgeführt werden kann, aufgerufen werden. Die AIX-Version der OpenPTS-Prüffunktion ist im AIX-Erweiterungspaket verfügbar. Die Versionen der OpenPTS-Prüffunktion für Linux und andere Plattformen können aus dem Web heruntergeladen werden. Zu den Konfigurationsanforderungen gehören die folgenden:

- Installation von Secure Shell (SSH), z. B. OpenSSH oder eine äquivalente Funktionalität
- Einrichten der Netzkonnektivität (über SSH) zum Collector
- Installation von Java™ 1.6 oder höher für den Zugriff auf die **openpts**-Konsole über die grafische Schnittstelle

Fehlerhebung vorbereiten

Die im Folgenden beschriebenen Informationen zu Trusted Boot dienen als Anleitung für die Identifizierung von Situationen, in denen eine Abhilfe erforderlich sein kann. Sie haben keine Auswirkungen auf den Bootprozess.

Es gibt viele Bedingungen, die zum Fehlschlagen der Attestierung führen können, und es ist schwierig vorherzusagen, welche Bedingung eintritt. Die jeweils auszuführende Aktion richtet sich nach der vorliegenden Bedingung. Es empfiehlt sich jedoch, sich auf einige schwerwiegende Szenarien vorzubereiten und eine Richtlinie oder einen Workflow für die Behandlung solcher Vorfälle zu haben. Abhilfe ist die Korrekturmaßnahme, die ausgeführt werden muss, wenn bei der Attestierung gemeldet wird, dass einer oder mehrerer Collectors nicht vertrauenswürdig sind.

Wenn beispielsweise ein Attestierungsfehler auftritt, weil das Boot-Image von den Referenzinformationen der Prüffunktion abweicht, sollten Sie Antworten auf die folgenden Fragen haben:

- Wie können Sie verifizieren, dass das Sicherheitsrisiko wirklich besteht?

- Wurden geplante Wartungsarbeiten ausgeführt, AIX-Upgrades durchgeführt oder kürzlich neue Hardwarekomponenten installiert?
- Können Sie sich an den Administrator wenden, der Zugriff auf diese Informationen hat?
- Wann wurde das System zuletzt in einem vertrauenswürdigen Zustand gebootet?
- Welche Aktion muss ausgeführt werden, falls sich die Sicherheitsbedrohung als gültig herausstellt? (Zu den Empfehlungen gehören die Erfassung von Prüfprotokollen, das Trennen des Systems vom Netz, das Ausschalten des Systems und das Senden von Alerts an Benutzer.)
- Wurden weitere Systeme kompromittiert, die geprüft werden müssen?

Zugehörige Konzepte:

„Fehlerbehebung bei Trusted Boot" auf Seite 112
Im Folgenden sind einige der gängigen Szenarien und Fehlerbehebungsschritte beschrieben, die ausgeführt werden müssen, um den Grund für Attestierungsfehler bei der Verwendung von Trusted Boot zu ermitteln.

Hinweise zur Migration

Berücksichtigen Sie vor der Migration einer Partition, die für Virtual Trusted Platform Module (VTPM) aktiviert ist, die folgenden Voraussetzungen.

Ein Vorteil eines VTPM gegenüber einem physischen TPM ist der, dass es die Migration der Partition zwischen Systemen unter Beibehaltung des VTPM ermöglicht. Um die logische Partition sicher zu migrieren, verschlüsselt die Firmware die VTPM-Daten vor der Übertragung. Die folgenden Sicherheitsmaßnahmen müssen vor der Migration implementiert werden, um eine sichere Migration zu gewährleisten:

- Aktivieren Sie IPSEC für den Virtual I/O Server (VIOS), der die Migration durchführt.
- Legen Sie den vertrauenswürdigen Systemschlüssel über die Hardware Management Console (HMC) fest, um die verwalteten Systeme zu steuern, die in der Lage sind, die VTPM-Daten nach der Migration zu entschlüsseln. Das Zielsystem für die Migration muss denselben Schlüssel haben wie das Quellensystem, damit die Daten erfolgreich migriert werden können.

Zugehörige Informationen:

HMC verwenden

VIOS-Migration

Trusted Boot installieren

Für die Installation von Trusted Boot sind verschiedene Hardware- und Softwarekonfigurationen erforderlich.

Zugehörige Informationen:

„PowerSC Standard Edition installieren" auf Seite 7
Sie müssen für jede spezielle Funktion von PowerSC Standard Edition eine Dateigruppe installieren.

Collector installieren

Sie müssen den Collector mit der Dateigruppe von der AIX-Basis-CD installieren.

Wenn Sie den Collector installieren möchten, installieren Sie die Pakete `powerscStd.vtpm` und `openpts-.collector`, die sich auf der Basis-CD befinden, mit dem Befehl **smit** oder mit dem Befehl **installp**.

Prüffunktion installieren

Die Komponente für die OpenPTS-Prüffunktion kann unter dem Betriebssystem AIX und auf anderen Plattformen ausgeführt werden.

Die AIX-Version der Prüffunktion kann mit dem AIX-Erweiterungspaket aus der Dateigruppe installiert werden. Um die Prüffunktion unter dem Betriebssystem AIX zu installieren, installieren Sie das Paket `openpts.verifier` aus dem AIX-Erweiterungspaket mit dem Befehl **smit** oder **installp**. Dieser Befehl installiert sowohl die Befehlszeilenversion oder auch GUI-Version der Prüffunktion.

Die OpenPTS-Prüffunktion für andere Betriebssysteme kann über `Download Linux OpenPTS Verifier For Use With AIX Trusted Boot` heruntergeladen werden.

Zugehörige Informationen:

Linux OpenPTS Verifier für AIX Trusted Boot herunterladen

Trusted Boot konfigurieren

Im Folgenden wird die Prozedur zum Registrieren eines Systems und zum Attestieren eines Systems für Trusted Boot beschrieben.

System registrieren

Im Folgenden wird beschrieben, wie Sie ein System mit der Prüffunktion registrieren.

Die Registrierung eines Systems ist der Prozess, bei dem ein anfänglicher Satz von Messwerten an die Prüffunktion übergeben wird, der die Basis für nachfolgende Attestierungsanforderungen bildet. Verwenden Sie zum Registrieren eines Systems über die Befehlszeile den folgenden Befehl in der Prüffunktion:

```
openpts -i <Hostname>
```

Informationen zur registrierten Partition finden Sie im Verzeichnis `$HOME/.openpts`. Jeder neuen Partition wird während des Registrierungsprozesses eine eindeutige ID zugewiesen und die Informationen zu den registrierten Partitionen werden in dem Verzeichnis gespeichert, das der eindeutigen ID entspricht.

Führen Sie zum Registrieren eines Systems über die grafische Schnittstelle die folgenden Schritte aus:

1. Starten Sie die grafische Schnittstelle mit dem Befehl **/opt/ibm/openpts_gui/openpts_GUI.sh**.
2. Wählen Sie im Navigationsmenü den Eintrag **Enroll** aus.
3. Geben Sie den Hostnamen und die SSH-Berechtigungsnachweise des Systems ein.
4. Klicken Sie auf **Enroll**.

Zugehörige Konzepte:

„System attestieren"
Im Folgenden wird die Prozedur zum Attestieren eines Systems über die Befehlszeile und über die grafische Schnittstelle beschrieben.

System attestieren

Im Folgenden wird die Prozedur zum Attestieren eines Systems über die Befehlszeile und über die grafische Schnittstelle beschrieben.

Verwenden Sie den folgenden Befehl in der Prüffunktion, um die Integrität eines Systemboots abzufragen:

```
openpts <Hostname>
```

Führen Sie die folgenden Schritte aus, um ein System über die grafische Schnittstelle zu attestieren:

1. Wählen Sie im Navigationsmenü eine Kategorie aus.
2. Wählen Sie die zu attestierenden Systeme aus.
3. Klicken Sie auf **Attest**.

System ohne Kennwort registrieren und attestieren

Die Attestierungsanforderung wird über Secure Shell (SSH) gesendet. Installieren Sie das Zertifikat der Prüffunktion im Collector, um SSH-Verbindungen ohne Kennwort zuzulassen.

Führen Sie die folgenden Schritte aus, um das Zertifikat der Prüffunktion auf dem System des Collectors zu installieren:

- Führen Sie in der Prüffunktion die folgenden Befehle aus:

```
ssh-keygen    # Keine Kennphrase
scp ~/.ssh/id_rsa.pub <Collector>:/tmp
```

- Führen Sie auf dem Collectorsystem den folgenden Befehl aus:

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

Trusted Boot verwalten

Im Folgenden wird die Prozedur zur Verwaltung der Attestierungsergebnisse von Trusted Boot beschrieben.

Attestierungsergebnisse interpretieren

Im Folgenden wird die Prozedur zum Anzeigen und Interpretieren der Attestierungsergebnisse beschrieben.

Eine Attestierung kann einen der folgenden Status zur Folge haben:

1. Attestation request failed: Die Attestierungsanforderung wurde nicht erfolgreich ausgeführt. Im Abschnitt Fehlerbehebung sind die möglichen Ursachen für den Fehler beschrieben.
2. System integrity valid: Die Attestierung wurde erfolgreich durchgeführt und beim Systemboot werden die Referenzinformationen in der Prüffunktion abgeglichen. Dies ist ein Hinweis auf einen erfolgreichen vertrauenswürdigen Bootvorgang (Trusted Boot).
3. System integrity invalid: Die Attestierungsanforderung wurde ausgeführt, aber es wurde eine Diskrepanz zwischen den während des Systemboots erfassten Informationen und den Referenzinformationen in der Prüffunktion gefunden. Dies ist ein Hinweis auf einen nicht vertrauenswürdigen Bootvorgang.

Bei der Attestierung wird mit der folgenden Nachricht auch gemeldet, ob eine Aktualisierung auf den Collector angewendet wurde:

System update available: Diese Nachricht zeigt an, dass eine Aktualisierung auf den Collector angewendet wurde und dass ein Satz aktualisierter Referenzinformationen verfügbar ist, der für den nächsten Bootvorgang wirksam ist. Der Benutzer wird von der Prüffunktion aufgefordert, die Aktualisierungen zu akzeptieren oder zurückzuweisen. Der Benutzer kann diese Aktualisierungen akzeptieren, wenn er erkennt, dass Wartungsaktionen im Collector ausgeführt werden.

Führen Sie die folgenden Schritte aus, um einen Attestierungsfehler über die grafische Benutzerschnittstelle zu untersuchen:

1. Wählen Sie im Navigationsmenü eine Kategorie aus.
2. Wählen Sie ein zu überprüfendes System aus.
3. Klicken Sie doppelt auf den Eintrag für das System. Es erscheint ein Eigenschaftenfenster. Dieses Fenster enthält Protokollinformationen zur fehlgeschlagenen Attestierung.

Systeme löschen

Im Folgenden wird die Prozedur zum Löschen eines Systems aus der Datenbank der Prüffunktion beschrieben.

Führen Sie den folgenden Befehl aus, um ein System aus der Datenbank der Prüffunktion zu entfernen:

`openpts -r <Hostname>`

Fehlerbehebung bei Trusted Boot

Im Folgenden sind einige der gängigen Szenarien und Fehlerbehebungsschritte beschrieben, die ausgeführt werden müssen, um den Grund für Attestierungsfehler bei der Verwendung von Trusted Boot zu ermitteln.

Der Befehl **openpts** deklariert ein System als ungültig, wenn der aktuelle Bootstatus des Systems nicht mit den Referenzinformationen in der Prüffunktion übereinstimmt. Der Befehl **openpts** bestimmt die mögliche Ursache für die nicht vorhandene Integrität. Es gibt verschiedene Variablen in einem vollständigen AIX-Bootprozess und eine fehlgeschlagene Attestierung erfordert eine Analyse, um die Fehlerursache zu bestimmen.

In der folgenden Tabelle sind einige der gängigen Szenarien und Fehlerbehebungsschritte zur Ermittlung der Fehlerursache aufgelistet:

Tabelle 12. Fehlerbehebung für einige gängige Fehlerszenarien

Fehlersymptom	Mögliche Fehlerursachen	Vorgeschlagene Fehlerbehebung

Die Attestierung wurde nicht durchgeführt.	• Falscher Hostname
	• Keine Netzroute zwischen der Quelle und dem Ziel
	• Falsche Sicherheitsberechtigungsnachweise
		Überprüfen Sie die SSH-Verbindung (Secure Shell) mit dem folgenden Befehl:
		`ssh ptsc@hostname`
		
		Wenn die SSH-Verbindung erfolgreich hergestellt wird, prüfen Sie, ob die folgenden Ursachen für den Attestierungsfehler vorliegen:
		• Auf dem System, das attestiert wird, wird der **tcsd**-Dämon nicht ausgeführt.
		• Das System, das attestiert wird, wurde nicht mit dem Befehl **ptsc** initialisiert. Dieser Prozess muss automatisch während des Systemstarts ausgeführt werden, aber das Vorhandensein eines Verzeichnisses `/var/ptsc/` im Collector überprüfen. Wenn das Verzeichnis `/var/ptsc/` nicht vorhanden ist, führen Sie den folgenden Befehl im Collector aus:
		`ptsc -i`

Die CEC-Firmware wurde geändert.	• Es wurde ein Firmware-Upgrade angewendet. • Die LPAR wurde auf ein System migriert, auf dem eine andere Version der Firmware ausgeführt wird.	Überprüfen Sie den Firmware-Level des Systems, das die LPAR hostet.
Die Ressourcen, die der LPAR zugeordnet sind, haben sich geändert.	Die CPU oder der Hauptspeicher, die bzw. der der LPAR zugeordnet ist, wurde geändert.	Überprüfen Sie das Partitionsprofil in der HMC.
Die Firmware für die in der LPAR verfügbaren Adapter hat sich geändert.	Es wurde eine Hardwareeinheit in der LPAR hinzugefügt oder entfernt.	Überprüfen Sie das Partitionsprofil in der HMC.
Die Liste der der LPAR zugeordneten Einheiten hat sich geändert.	Es wurde eine Hardwareeinheit in der LPAR hinzugefügt oder entfernt.	Überprüfen Sie das Partitionsprofil in der HMC.

Tabelle 12. Fehlerbehebung für einige gängige Fehlerszenarien (Forts.)

Fehlersymptom	Mögliche Fehlerursachen	Vorgeschlagene Fehlerbehebung
Das Boot-Image mit dem Betriebssystemkernel hat sich geändert.	• Es wurde eine AIX-Aktualisierung angewendet und die Prüffunktion war über diese Aktualisierung nicht informiert. • Der Befehl **bosboot** wurde ausgeführt.	• Überprüfen Sie zusammen mit dem Administrator des Collectors, ob vor der letzten Neustartoperation Wartungsarbeiten vorgenommen wurden. • Überprüfen Sie die Protokolle des Collectors auf Wartungsaktivitäten hin.
Die LPAR wurde über eine andere Einheit gebootet.	• Unmittelbar nach der Netzinstallation wurde eine Registrierung durchgeführt. • Das System wird über eine Wartungseinheit gebootet.	Die Booteinheit und die Flags können mit dem Befehl **bootinfo** geprüft werden. Wenn die Registrierung unmittelbar nach der NIM-Installation (Network Installation Management) und vor der Neustartoperation durchgeführt wurde, beziehen sich die registrierten Details auf die Netzinstallation und nicht auf den nächsten Plattenboot. Diese Registrierung kann durch Entfernen der Registrierung und erneute Registrierung der logischen Partition repariert werden.
Das SMS-Bootmenü (System Management Services) wurde aufgerufen.		Der Bootprozess muss ununterbrochen ohne Benutzeraktion ausgeführt werden, damit ein System als vertrauenswürdig eingestuft wird. Wenn das SMS-Bootmenü aufgerufen wird, gilt der Bootprozess als ungültig.
Die TE-Datenbank wurde geändert (Trusted Execution).	• Es wurden Binärdateien in der TE-Datenbank hinzugefügt oder entfernt. • Es wurden Binärdateien in der Datenbank aktualisiert.	Führen Sie den Befehl **trustchk** aus, um die Datenbank zu überprüfen.

Zugehörige Konzepte:

„Fehlerhebung vorbereiten" auf Seite 108
Die im Folgenden beschriebenen Informationen zu Trusted Boot dienen als Anleitung für die Identifizierung von Situationen, in denen eine Abhilfe erforderlich sein kann. Sie haben keine Auswirkungen auf den Bootprozess.

„Trusted Boot-Konzepte" auf Seite 107
Es ist wichtig, dass Sie die Integrität des Bootprozesses verstehen und wissen, wie ein Bootprozess als vertrauenswürdiger oder nicht vertrauenswürdiger Bootprozess klassifiziert wird.

Zugehörige Informationen:

HMC verwenden

Trusted Firewall

Das Feature Trusted Firewall bietet eine Sicherheit auf Virtualisierungsebene, die die Leistung und Ressourceneffizienz bei der Kommunikation verschiedener VLAN-Sicherheitszonen auf demselben Power Systems-Server verbessert. Trusted Firewall verringert die Last im externen Netz, indem die Funktion für die Filterung von Firewallpaketen, die bestimmten Regeln entsprechen, auf die Virtualisierungsebene ausgelagert wird. Diese Filterfunktion wird mit einfach definierten Netzfilterregeln gesteuert, die die Übertragung von vertrauenswürdigem Datenverkehr zwischen VLAN-Sicherheitszonen zulassen, ohne die virtuelle Umgebung verlassen zu müssen. Trusted Firewall schützt und leitet internen Netzverkehr zwischen den Betriebssystemen AIX, IBM i und Linux weiter.

Trusted Firewall-Konzepte

Für die Verwendung von Trusted Firewall wird das Verständnis verschiedener Basiskonzepte vorausgesetzt.

Die Power Systems-Hardware kann mit mehreren VLAN-Sicherheitszonen konfiguriert werden. Eine benutzerkonfigurierte Richtlinie, die als Trusted Firewall-Filterregel erstellt wird, lässt zu, dass vertrauenswürdiger Netzdatenverkehr über die VLAN-Sicherheitszonen übertragen werden kann und intern auf der Virtualisierungsebene verbleibt. Dieses Verfahren gleicht der Einführung einer an das Netz angeschlossenen physischen Firewall in die virtualisierte Umgebung, die eine leistungseffizientere Methode für die Implementierung von Firewallfunktionen für virtualisierte Rechenzentren darstellt.

Mit Trusted Firewall können Sie Regeln konfigurieren, um die direkte Übertragung bestimmter Typen von Datenverkehr von einem VLAN in einem Virtual I/O Server (VIOS) an ein anderes VLAN in demselben VIOS zuzulassen und gleichzeitig durch die Beschränkung anderer Datenverkehrstypen ein hohes Sicherheitsniveau beizubehalten. Es handelt sich um eine konfigurierbare Firewall auf der Virtualisierungsebene von Power Systems-Servern.

Das Beispiel in Abb. 1 auf Seite 116 veranschaulicht, wie Informationen sicher und effizient von LPAR1 in VLAN 200 und LPAR2 in VLAN 100 übertragen werden. Ohne Trusted Firewall werden Informationen, die von LPAR1 für LPAR2 bestimmt sind, aus dem internen Netz an den Router gesendet, der die Informationen dann zurück an LPAR2 weiterleitet.

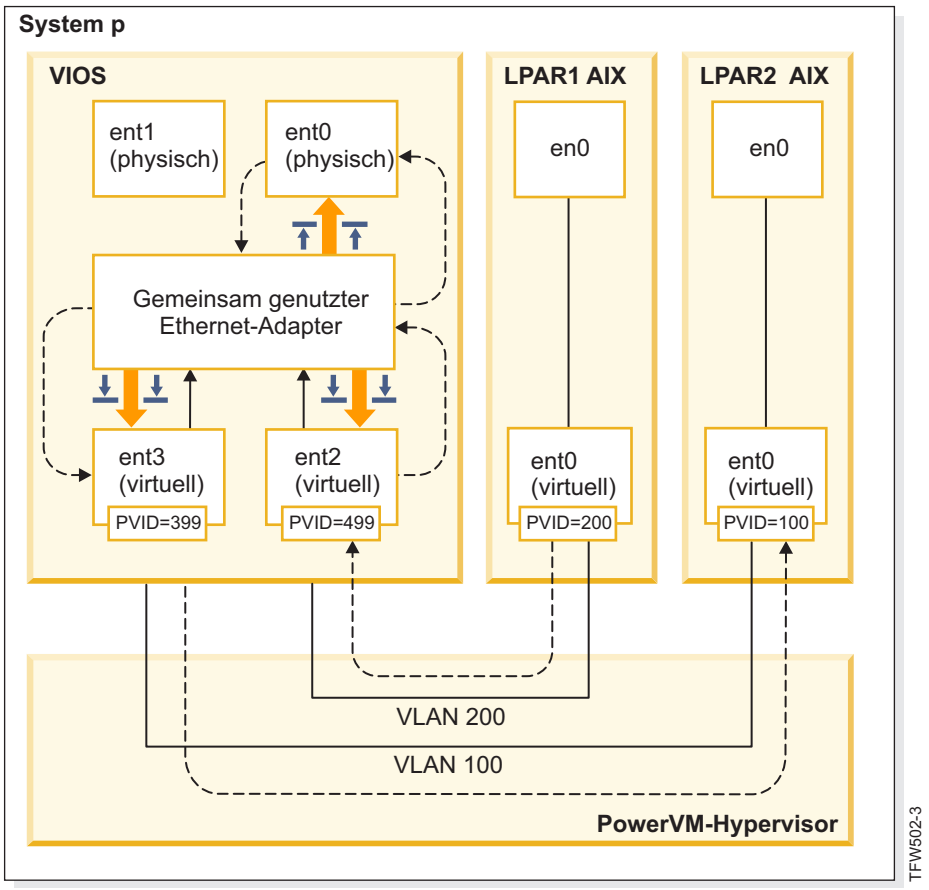

Abbildung 1. Beispiel für die VLAN-übergreifende Informationsübertragung ohne Trusted Firewall

Mit Trusted Firewall können Sie Regeln konfigurieren, um die Übertragung von Informationen von LPAR1 an LPAR2 ohne Verlassen des internen Netzes zuzulassen. Dieser Pfad wird in Abb. 2 auf Seite 117 gezeigt.

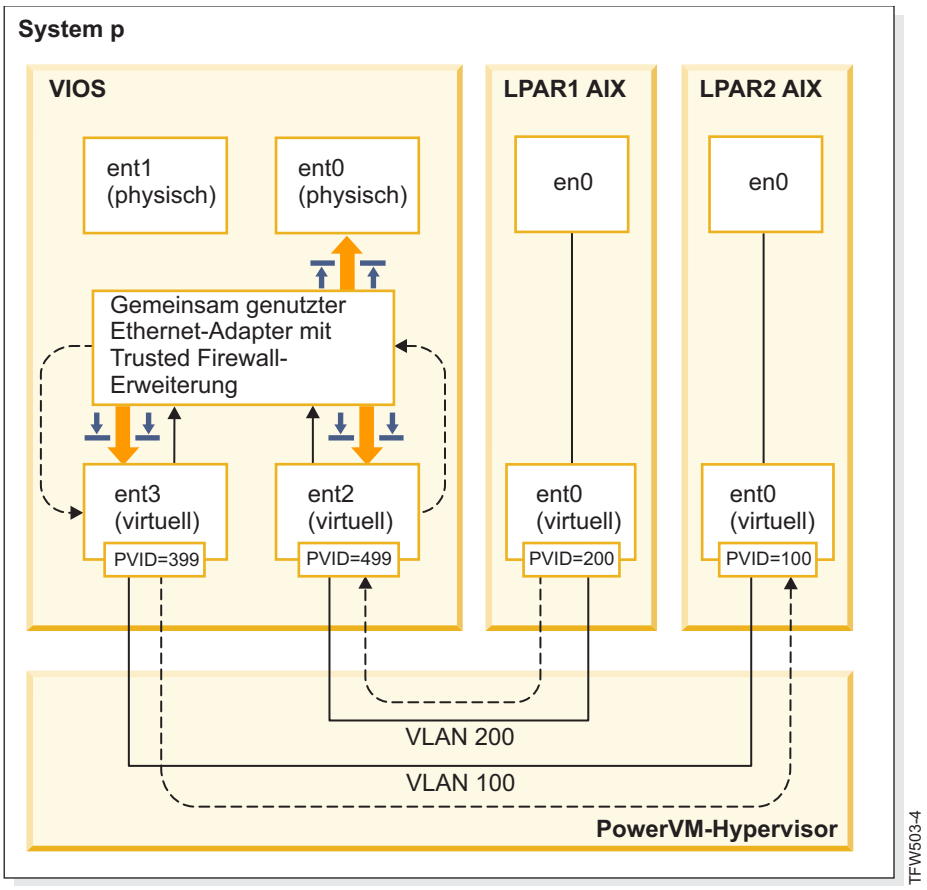

Abbildung 2. Beispiel für die VLAN-übergreifende Übertragung von Informationen mit Trusted Firewall

Konfigurationsregeln, die die sichere Übertragung bestimmter Informationen über VLANs zulassen, verkürzen den Pfad der Informationen an ihr Ziel. Trusted Firewall verwendet den gemeinsam genutzten Ethernet-Adapter (SEA, Shared Ethernet Adapter) und die Kernelerweiterung SVM (Security Virtual Machine), um diese Kommunikation zu ermöglichen.

Gemeinsam genutzter Ethernet-Adapter
Der gemeinsam genutzte Ethernet-Adapter (SEA, Shared Ethernet Adapter) ist der Punkt, an dem die Weiterleitung beginnt und endet. Wenn die SVM registriert ist, empfängt der gemeinsam genutzte Ethernet-Adapter die Pakete und leitet sie an die SVM weiter. Wenn die SVM feststellt, dass das Paket für eine LPAR auf demselben Power Systems-Server bestimmt ist, wird der Header der Ebene 2 des Pakets aktualisiert. Das Paket wird zur Weiterleitung an sein endgültiges Ziel innerhalb des Systems oder im externen Netz an den gemeinsam genutzten Ethernet-Adapter zurückgegeben.

Security Virtual Machine
In der SVM werden die Filterregeln angewendet. Die Filterregeln sind erforderlich, um die Sicherheit im internen Netz zu gewährleisten. Nach der Registrierung der SVM beim gemeinsam genutzten Ethernet-Adapter werden die Pakete an die SVM weitergeleitet, bevor sie an das externe Netz gesendet werden. Basierend auf den aktiven Filterregeln bestimmt die SVM, ob ein Paket im internen Netz verbleibt oder in das externe Netz verschoben wird.

Trusted Firewall installieren

Die Installation von PowerSC Trusted Firewall gleicht der Installation anderer PowerSC-Features.

Voraussetzungen:

- In den PowerSC-Versionen vor Version 1.1.1.0 ist die erforderliche Dateigruppe für die Installation von Trusted Firewall nicht enthalten. Stellen Sie sicher, dass Sie die PowerSC-Installations-CD für Version 1.1.1.0 oder höher haben.
- Um Trusted Firewall nutzen zu können, müssen Sie Ihre virtuellen LANs (VLANs) bereits mit der Hardware Management Console (HMC) oder mit Virtual I/O Server (VIOS) konfiguriert haben.

Trusted Firewall wird als zusätzliche Dateigruppe auf der Installations-CD von PowerSC Standard Edition bereitgestellt. Der Dateiname ist `powerscStd.svm.rte`. Sie können Trusted Firewall einer vorhandenen Instanz von PowerSC Version 1.1.0.0 oder höher hinzufügen oder das Feature im Rahmen einer Neuinstallation von PowerSC Version 1.1.1.0 oder höher installieren.

Gehen Sie wie folgt vor, um die Trusted Firewall-Funktion einer vorhandenen PowerSC-Instanz hinzuzufügen:

1. Stellen Sie sicher, dass Sie VIOS Version 2.2.1.4 oder höher ausführen.
2. Legen Sie die PowerSC-Installations-CD für Version 1.1.1.0 ein oder laden Sie das Image der Installations-CD herunter.
3. Verwenden Sie den Befehl **oem_setup_env** für den Rootzugriff.
4. Verwenden Sie den Befehl **installp** oder das Tool SMIT, um die Dateigruppe `PowerscStd.svm.rte` zu installieren.

Zugehörige Informationen:

„PowerSC Standard Edition installieren" auf Seite 7
Sie müssen für jede spezielle Funktion von PowerSC Standard Edition eine Dateigruppe installieren.

Trusted Firewall konfigurieren

Nach der Installation des Features Trusted Firewall müssen weitere Konfigurationseinstellungen vorgenommen werden.

Trusted Firewall Advisor

Trusted Firewall Advisor analysiert den Systemdatenverkehr von verschiedenen logischen Partitionen (LPARs), Informationen bereitzustellen, anhand derer bestimmt werden kann, ob sich die Systemleistung durch die Ausführung von Trusted Firewall verbessert.

Wenn die Funktion Trusted Firewall Advisor sehr viel Datenverkehr von verschiedenen virtuellen LANs LANs (VLANs) aufzeichnet, die sich in demselben zentralen elektronischen Komplex befinden, sollte Ihr System von der Aktivierung von Trusted Firewall profitieren.

Geben Sie den folgenden Befehl ein, um Trusted Firewall Advisor zu aktivieren:

```
vlantfw -m
```

Geben Sie den folgenden Befehl ein, um die Ergebnisse von Trusted Firewall Advisor anzuzeigen:

```
vlantfw -D
```

Geben Sie den folgenden Befehl ein, um Trusted Firewall Advisor zu inaktivieren:

```
vlantfw -M
```

Trusted Firewall-Protokollierung

Bei der Trusted Firewall-Protokollierung wird eine Liste mit Netzverkehrspfaden im zentralen elektronischen Komplex kompiliert. In der Liste sind die Filter aufgeführt, die Trusted Firewall für die Weiterleitung des Datenverkehrs verwendet.

Wenn Trusted Firewall Advisor feststellt, dass sich die Effizienz durch interne Weiterleitung des Datenverkehrs verbessert, verwaltet die Trusted Firewall-Protokollierung eine Liste mit Pfaden in der Datei

`svm.log`. Die Größe der Datei `svm.log` ist auf 16 MB beschränkt. Wenn die Einträge den Grenzwert von 16 MB überschreiten, werden die ältesten Einträge aus der Protokolldatei entfernt.

Geben Sie den folgenden Befehl ein, um die Trusted Firewall-Protokollierung zu starten:

```
vlantfw -l
```

Geben Sie den folgenden Befehl ein, um die Trusted Firewall-Protokollierung zu stoppen:

```
vlantfw -L
```

Sie finden die Protokolldatei an der folgenden Position: `/home/padmin/svm/svm.log`.

Anmerkung: Die Befehle zum Starten und Stoppen der Trusted Firewall-Protokollierung können Sie nur ausführen, wenn Sie als Rootbenutzer authentifiziert sind.

Mehrere gemeinsam genutzte Ethernet-Adapter

Sie können Trusted Firewall auf Systemen konfigurieren, die mehrere gemeinsam genutzte Ethernet-Adapter (SEA, Shared Ethernet Adapter) verwenden.

Einige Konfigurationen verwenden mehrere gemeinsam genutzte Ethernet-Adapter in demselben Virtual I/O Server (VIOS). Mehrere gemeinsam genutzte Ethernet-Adapter bieten Vorteile in Bezug auf den Ausfallschutz und gleichmäßige Ressourcenbelastung. Trusted Firewall unterstützt das Routing über mehrere gemeinsam genutzte Ethernet-Adapter, sofern sie sich in demselben VIOS befinden.

Abb. 3 zeigt eine Umgebung, in der mehrere gemeinsam genutzte Ethernet-Adapter verwendet werden.

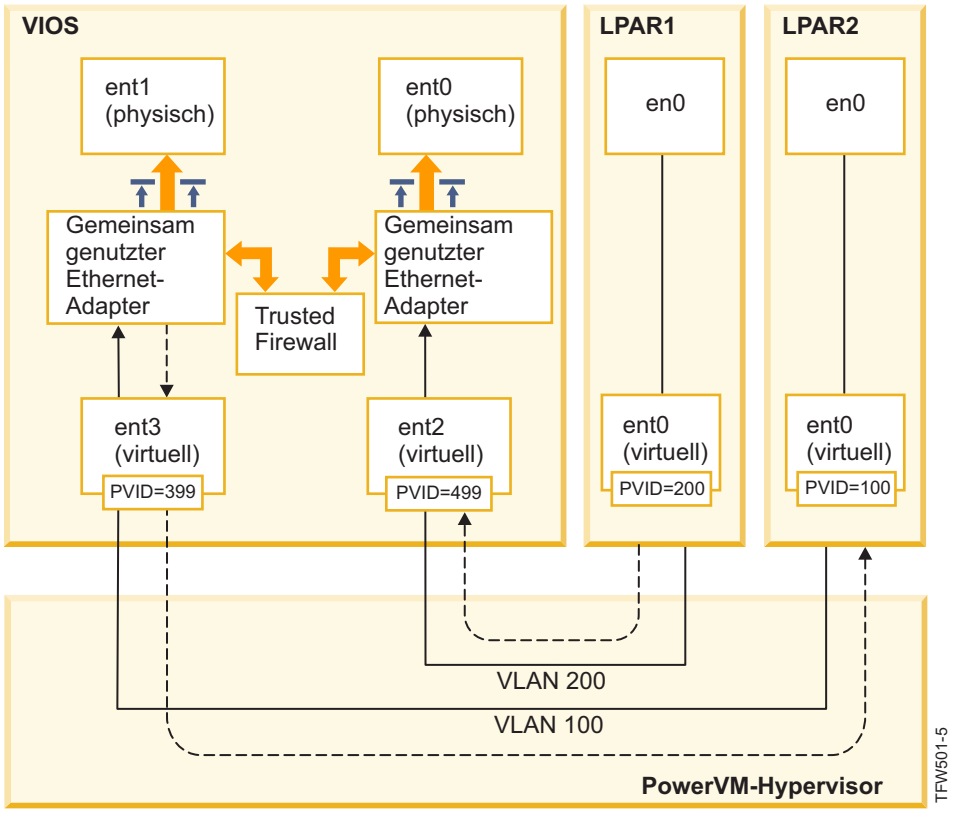

Abbildung 3. Konfiguration mit mehreren gemeinsam genutzten Ethernet-Adaptern in einem einzigen VIOS

Im Folgenden sind Beispiele von Konfigurationen mit mehreren gemeinsam genutzten Ethernet-Adaptern beschrieben, die von Trusted Firewall unterstützt werden:

- Die gemeinsam genutzten Ethernet-Adapter sind mit Trunkadaptern in demselben virtuellen Switch für Power Hypervisor konfiguriert. Diese Konfiguration wird unterstützt, weil jeder gemeinsam genutzte Ethernet-Adapter Netzverkehr mit anderen VLAN-IDs empfängt.
- Die gemeinsam genutzten Ethernet-Adapter sind mit Trunkadaptern in verschiedenen virtuellen Switches für Power Hypervisor konfiguriert und jeder Trunkadapter befindet sich in einem VLAN mit einer jeweils anderen ID. In dieser Konfiguration empfängt jeder gemeinsam genutzte Ethernet-Adapter weiterhin Netzverkehr mit verschiedenen VLAN-IDs.
- Die gemeinsam genutzten Ethernet-Adapter sind mit Trunkadaptern in verschiedenen virtuellen Switches für Power Hypervisor konfiguriert und in den virtuellen Switches werden dieselben VLAN-IDs wiederverwendet. In diesem Fall hat der Datenverkehr für die beiden gemeinsam genutzten Ethernet-Adapter dieselben VLAN-IDs.

  Ein Beispiel für diese Konfiguration ist die Verwendung von LPAR2 in VLAN200 mit dem virtuellen Switch 10 und LPAR3 in VLAN200 mit dem virtuellen Switch 20. Da beide LPARs und die entsprechenden gemeinsam genutzten Ethernet-Adapter dieselbe VLAN-ID (VLAN200) verwenden, haben beide gemeinsam genutzten Ethernet-Adapter Zugriff auf die Pakete mit dieser VLAN-ID.

Es ist nicht möglich, Bridging in mehreren VIOS-Instanzen zu aktivieren. Aus diesem Grund werden die folgenden Konfigurationen mit mehreren gemeinsam genutzten Ethernet-Adaptern von Trusted Firewall nicht unterstützt:

- Mehrere VIOS-Instanzen und mehrere Treiber für gemeinsam genutzte Ethernet-Adapter
- Redundante Lastteilung auf gemeinsam genutzte Ethernet-Adapter: Trunkadapter, die für das VLAN-übergreifende Routing konfiguriert sind, können nicht auf VIOS-Server aufgeteilt werden.

Gemeinsam genutzte Ethernet-Adapter entfernen

Die Schritte zum Entfernen gemeinsam genutzter Ethernet-Adapter (SEA, Shared Ethernet Adapter) vom System müssen in einer bestimmten Reihenfolge ausgeführt werden.

Führen Sie die folgenden Schritte aus, um einen gemeinsam genutzten Ethernet-Adapter von Ihrem System zu entfernen:

1. Entfernen Sie die SVM (Security Virtual Machine), die dem gemeinsam genutzten Ethernet-Adapter zugeordnet ist, mit dem folgenden Befehl:

   ```
   rmdev -dev svm
   ```

2. Entfernen Sie den gemeinsam genutzten Ethernet-Adapter mit dem folgenden Befehl:

   ```
   rmdev -dev ID des gemeinsam genutzten Ethernet-Adapters
   ```

Anmerkung: Das Entfernen des gemeinsam genutzten Ethernet-Adapters vor dem Entfernen der SVM kann zu einem Systemausfall führen.

Regeln erstellen

Sie können Regeln erstellen, um VLAN-übergreifendes Routing mit Trusted Firewall zu aktivieren.

Wenn Sie die Routing-Features von Trusted Firewall aktivieren möchten, müssen Sie Regeln erstellen, mit denen Sie die zulässigen Kommunikationen festlegen. Für eine erweiterte Sicherheit gibt es keine einzelne Regel, die die Kommunikation zwischen allen VLANs im System zulässt. Jede zulässige Verbindung erfordert eine eigene Regel, obwohl jede Regel, die aktiviert wird, die Kommunikation in beide Richtungen für ihre angegebenen Endpunkte zulässt.

Da die Regelerstellung in der VIOS-Schnittstelle (Virtual I/O Server) erstellt wird, sind weitere Informationen zu den Befehlen in der Sammlung der Abschnitte zu VIOS im Information Center zur Power Systems-Hardware verfügbar.

Führen Sie zum Erstellen einer Regel die folgenden Schritte aus:

1. Öffnen Sie die VIOS-Befehlszeilenschnittstelle.

2. Initialisieren Sie den SVM-Treiber mit dem folgenden Befehl:
   ```
   mksvm
   ```
3. Starten Sie Trusted Firewall mit dem Startbefehl:
   ```
   vlantfw -s
   ```
4. Geben Sie den folgenden Befehl ein, um alle bekannten LPAR-IP- und -MAC-Adressen anzuzeigen:
   ```
   vlantfw -d
   ```

   Sie benötigen die IP- und MAC-Adressen der logischen Partitionen (LPARs), für die Sie Regeln erstellen.
5. Geben Sie einen der folgenden Befehle (in einer einzigen Zeile) ein, um die Filterregel zu erstellen, mit der die Kommunikation zwischen den beiden LPARs (LPAR1 und LPAR2) zugelassen wird:
   ```
   genvfilt -v4 -a P -z [VLAN-ID_LPAR1] -Z [VLAN-ID_LPAR2] -s [IP-Adresse_LPAR1]
        -d [IP-Adresse_LPAR2]
   genvfilt -v4 -a P -z [VLAN-ID_LPAR1] -Z [VLAN-ID_LPAR2] -s [IP-Adresse_LPAR1] -d
        [IP-Adresse_LPAR2]-o any -p 0 -O gt -P 23
   ```

   Anmerkung: Eine Filterregel lässt je nach Port- und Protokolleinträgen standardmäßig die Kommunikation in beide Richtungen zu. Mit dem folgenden Befehl aktivieren Sie beispielsweise Telnet zwischen LPAR1 und LPAR2:
   ```
   genvfilt -v4 -a-P -z [VLAN-ID_LPAR1] -Z [VLAN-ID_LPAR2] -s [IP-Adresse_LPAR1] -d
       [IP-Adresse_LPAR2]-o any -p 0 -O eq -P 23
   ```
6. Aktivieren Sie mit dem Befehl alle Filterregeln im Kernel:
   ```
   mkvfilt -u
   ```

Anmerkung: Diese Prozedur aktiviert diese Regel und alle anderen Filterregeln auf dem System.

Weitere Beispiele

Die folgenden Beispiele zeigen weitere Filterregeln, die Sie mit Trusted Firewall erstellen können.

- Geben Sie den folgenden Befehl ein, um die Secure Shell-Kommunikation von der LPAR in VLAN 100 mit der LPAR in VLAN 200 zuzulassen:
  ```
  genvfilt -v4 -a P -z 100 -Z 200 -o any -p 0 -O eq -P 22 -c tcp
  ```
- Geben Sie den folgenden Befehl ein, um den Datenverkehr zwischen allen Ports (0-499) zuzulassen:
  ```
  genvfilt -v4 -a P -z 100 -z 200 -o lt -p 500 -O lt -P 500 -c tcp
  ```
- Geben Sie den folgenden Befehl ein, um TCP-Datenverkehr zwischen den LPARs uneingeschränkt zuzulassen:
  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c tcp
  ```

  Wenn Sie keine Ports oder Portoperationen angeben, können alle Ports für den Datenverkehr verwendet werden.
- Geben Sie den folgenden Befehl ein, um ICMP-Messaging (Internet Control Message Protocol) zwischen LPARs zuzulassen:
  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c icmp
  ```

Zugehörige Konzepte:

„Regeln inaktivieren” auf Seite 122
Sie können Regeln, die das VLAN-übergreifende Routing im Feature Trusted Firewall aktivieren, inaktivieren.

Zugehörige Verweise:

„Befehl genvfilt” auf Seite 166

„Befehl mkvfilt” auf Seite 168

„Befehl vlantfw” auf Seite 188

Zugehörige Informationen:

Virtual I/O Server (VIOS)

Regeln inaktivieren

Sie können Regeln, die das VLAN-übergreifende Routing im Feature Trusted Firewall aktivieren, inaktivieren.

Da die Regeln in der VIOS-Schnittstelle (Virtual I/O Server) inaktiviert werden, sind weitere Informationen zu den Befehlen in der Sammlung der Abschnitte zu VIOS im Information Center zur Power Systems-Hardware verfügbar.

Führen Sie zum Inaktivieren einer Regel die folgenden Schritte aus:

1. Öffnen Sie die VIOS-Befehlszeilenschnittstelle.
2. Geben Sie den folgenden Befehl ein, um alle aktiven Filterregeln anzuzeigen:

   ```
   lsvfilt -a
   ```

   Sie können das Flag **-a** weglassen, um alle Filterregeln anzuzeigen, die im Object Data Manager gespeichert sind.
3. Notieren Sie die Identifikationsnummer für die Filterregel, die Sie inaktivieren. In diesem Beispiel ist die Identifikationsnummer der Filterregel 23.
4. Verwenden Sie den folgenden Befehl, um die Filterregel 23 zu inaktivieren, wenn diese im Kernel aktiv ist:

   ```
   rmvfilt -n 23
   ```

   Geben Sie den folgenden Befehl ein, um alle Filterregeln im Kernel zu inaktivieren:

   ```
   rmvfilt -n all
   ```

Zugehörige Konzepte:

„Regeln erstellen” auf Seite 120
Sie können Regeln erstellen, um VLAN-übergreifendes Routing mit Trusted Firewall zu aktivieren.

Zugehörige Verweise:

„Befehl lsvfilt” auf Seite 167

„Befehl rmvfilt” auf Seite 188

Trusted Logging

PowerVM Trusted Logging ermöglicht logischen AIX-Partitionen (LPARs), in Protokolldateien zu schreiben, die in einem zugeordneten Virtual I/O Server (VIOS) gespeichert sind. Die Daten werden über den Hypervisor direkt an VIOS übertragen und es ist keine Netzkonnektivität zwischen der Client-LPAR und VIOS erforderlich.

Virtuelle Protokolle

Der VIOS-Administrator (Virtual I/O Server) erstellt und verwaltet die Protokolldateien, die unter dem Betriebssystem AIX als virtuelle Protokolleinheiten im Verzeichnis `/dev` ähnlich wie die virtuellen Platten oder virtuellen optischen Datenträger bereitgestellt werden.

Das Speichern von Protokolldateien als virtuelle Protokolle erhöht das Vertrauen in die Datensätze, weil sie von einem Benutzer mit Rootberechtigungen auf der Client-LPAR, auf der sie generiert wurden, nicht geändert werden können. Derselben Client-LPAR können mehrere virtuelle Protokolleinheiten zugeordnet werden und jedes Protokoll ist eine andere Datei im Verzeichnis `/dev`.

Mit Trusted Logging können Protokolldaten mehrerer Client-LPARs in einem einzigen Dateisystem konsolidiert werden, das über VIOS zugänglich ist. Deshalb stellt VIOS eine einzige Position auf dem System für die Protokollanalyse und -archivierung bereit. Der Administrator der Client-LPAR kann Anwendungen und das Betriebssystem AIX so konfigurieren, dass Daten ähnlich wie in die lokalen Dateien stattdessen auf die virtuellen Protokolleinheiten geschrieben werden. Das AIX-Prüfsubsystem kann so konfiguriert werden, dass die Prüfdatensätze in virtuelle Protokolle umgeleitet werden, und andere AIX-Services wie syslog arbeiten mit ihrer vorhandenen Konfiguration, um Daten in die virtuellen Protokolle umzuleiten.

Zum Konfigurieren des virtuellen Protokolls muss der VIOS-Administrator einen Namen für das virtuelle Protokoll angeben, der sich aus den folgenden Komponenten zusammensetzt:

- Client
- Protokollname

Die Namen der beiden Komponenten können vom VIOS-Administrator auf einen beliebigen Wert gesetzt werden, aber der Clientname ist gewöhnlich für alle virtuellen Protokolle, die einer bestimmten LPAR zugeordnet sind, derselbe (z. B. der Hostname der LPAR). Der Protokollname gibt den Zweck des Protokolls an (z. B. audit oder syslog).

In einer AIX LPAR wird jede virtuelle Protokolleinheit in Form von zwei funktional äquivalenten Dateien im Dateisystem `/dev` dargestellt. Die erste Datei wird nach der Einheit benannt, z. B. `/dev/vlog0`, und die zweite Datei erhält einen Namen, der durch Verkettung des Präfix `vl` mit dem Protokollnamen und der Einheitennummer gebildet wird. Wenn beispielsweise die virtuelle Protokolleinheit `vlog0` den Protokollnamen `audit` hat, ist sie im Dateisystem `/dev` als `vlog0` und als `vlaudit0` verfügbar.

Zugehörige Informationen:

Virtuelle Protokolle erstellen

Virtuelle Protokolleinheiten erkennen

Nachdem ein VIOS-Administrator virtuelle Protokolleinheiten erstellt und sie einer Client-LPAR zugeordnet hat, muss die Einheitenkonfiguration der Client-LPAR aktualisiert werden, damit Einheiten sichtbar werden.

Der Administrator der Client-LPAR aktualisiert die Einstellungen mit einer der folgenden Methoden:

- Client-LPAR neu starten
- Befehl **cfgmgr** ausführen

Führen Sie den Befehl **lsdev** zum Anzeigen der virtuellen Protokolleinheiten aus. Den Einheiten wird standardmäßig das Präfix `vlog` vorangestellt. Im Folgenden sehen Sie ein Beispiel für die **lsdev**-Befehlsausgabe auf einer AIX-LPAR, für die zwei virtuelle Protokolleinheiten vorhanden sind:

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

Überprüfen Sie die Eigenschaften einer virtuellen Protokolleinheit mit dem Befehl `lsattr –El <Einheitenname>`, der eine Ausgabe ähnlich der folgenden erzeugt:

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

In dieser Ausgabe werden der Clientname, der Einheitenname und die Menge an Protokolldaten, die von VIOS gespeichert werden können, angezeigt.

Im virtuellen Protokoll werden die folgenden beiden Typen von Protokolldaten gespeichert:

- Protokolldaten: Die unaufbereiteten Protokolldaten, die von Anwendungen in der AIX-LPAR generiert werden.
- Statusdaten: Informationen zu Einheitenoperationen (Konfiguration, Öffnen, Schließen und weiteren Operationen, die zur Analyse von Protokollaktivitäten verwendet werden).

Der VIOS-Administrator legt mit den Attributen `max_log_size` und `max_state_size` die Menge an **Protokolldaten** bzw. **Statusdaten**, die für jedes virtuelle Protokoll gespeichert werden können, fest. Wenn die gespeicherten Daten den festgelegten Grenzwert überschreiten, werden die ältesten Protokolldaten überschrieben. Der VIOS-Administrator muss sicherstellen, dass die Protokolldaten häufig erfasst und archiviert werden, um die Protokolle beizubehalten.

Trusted Logging installieren

Sie können das PowerSC-Feature Trusted Logging über die Befehlszeilenschnittstelle oder mit dem SMIT-Tool installieren.

Die Voraussetzungen für die Installation von Trusted Logging sind VIOS 2.2.1.0 oder höher und IBM AIX 6 with Technology Level 7 oder IBM AIX 7 with Technology Level 1.

Die Datei für die Installation des Features Trusted Logging ist `powerscStd.vlog` und auf der Installations-CD von PowerSC Standard Edition enthalten.

Gehen Sie zum Installieren der Funktion Trusted Logging wie folgt vor:

1. Stellen Sie sicher, dass Sie VIOS Version 2.2.1.0 oder höher ausführen.
2. Legen Sie die PowerSC-Installations-CD ein oder laden Sie das Image der Installations-CD herunter.
3. Verwenden Sie den Befehl **installp** oder das Tool SMIT, um die Dateigruppe `powerscStd.vlog` zu installieren.

Zugehörige Informationen:

„PowerSC Standard Edition installieren” auf Seite 7
Sie müssen für jede spezielle Funktion von PowerSC Standard Edition eine Dateigruppe installieren.

Trusted Logging konfigurieren

Im Folgenden ist die Prozedur zum Konfigurieren von Trusted Logging im AIX-Prüfsubsystem und syslog beschrieben.

AIX-Prüfsubsystem konfigurieren

Das AIX-Prüfsubsystem kann so konfiguriert werden, dass nicht nur Protokolle in das lokale Dateisystem, sondern auch binäre Daten auf eine virtuelle Protokolleinheit geschrieben werden.

Anmerkung: Vor der Konfiguration des AIX-Prüfsubsystems müssen Sie die im Abschnitt „Virtuelle Protokolleinheiten erkennen" auf Seite 123 beschriebene Prozedur ausführen.

Führen Sie die folgenden Schritte aus, um das AIX-Prüfsubsystem zu konfigurieren:

1. Konfigurieren Sie das AIX-Prüfsubsystem so, dass Daten im Binärmodus (`auditbin`) protokolliert werden.
2. Aktivieren Sie Trusted Logging für die AIX-Prüfung, indem Sie die Konfigurationsdatei `/etc/security/audit/config` bearbeiten.
3. Fügen Sie der Zeilengruppe `bin:` den Parameter `virtual_log = /dev/vlog0` hinzu.

   Anmerkung: Die Anweisung ist gültig, wenn der LPAR-Administrator möchte, dass `auditbin`-Daten in `/dev/vlog0` geschrieben werden.
4. Starten Sie das AIX-Prüfsubsystem mit der folgenden Befehlsreihenfolge erneut:

   ```
   audit shutdown
   audit start
   ```

Daraufhin werden nicht nur Protokolle in das lokale Dateisystem, sondern über die angegebene virtuelle Protokolleinheit auch Prüfdatensätze in Virtual I/O Server (VIOS) geschrieben. Die Protokolle werden unter der Steuerung der vorhandenen Parameter `bin1` und `bin2` in die Zeilengruppe `bin:` der Konfigurationsdatei `/etc/security/audit/config` gespeichert.

Zugehörige Informationen:

Prüfsubsystem

syslog konfigurieren

syslog kann durch das Hinzufügen von Regeln zur Datei `/etc/syslog.conf` so konfiguriert werden, dass Nachrichten in virtuelle Protokolle geschrieben werden.

Anmerkung: Vor der Konfiguration der Datei `/etc/syslog.conf` müssen Sie die im Abschnitt „Virtuelle Protokolleinheiten erkennen" auf Seite 123 beschriebene Prozedur ausführen.

Sie können die Datei `/etc/syslog.conf` so bearbeiten, dass die Protokollnachrichten basierend auf den folgenden Kriterien zugeordnet werden:

- Funktion
- Prioritätsstufe

Wenn Sie die virtuellen Protokolle für syslog-Nachrichten verwenden möchten, müssen Sie die Datei `/etc/syslog.conf` mit Regeln konfigurieren, sodass die gewünschten Nachrichten in das entsprechende virtuelle Protokoll im Verzeichnis `/dev` geschrieben werden.

Fügen Sie beispielsweise die folgende Zeile zur Datei `/etc/syslog.conf` hinzu, wenn die von allen Funktionen generierten Debugnachrichten in das virtuelle Protokoll `vlog0` geschrieben werden sollen:

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

Anmerkung: Verwenden Sie die Protokollrotationsfunktionen, die im Dämon `syslogd` verfügbar sind, nicht für Befehle, die Daten in virtuelle Protokolle schreiben. Die Dateien im Dateisystem `/dev` sind keine regulären Dateien und können weder umbenannt noch entfernt werden. Der VIOS-Administrator muss die Rotation virtueller Protokolle in VIOS konfigurieren.

Der Dämon `syslogd` muss nach der Konfiguration mit dem folgenden Befehl erneut gestartet werden:

```
refresh -s syslogd
```

Zugehörige Informationen:

syslogd-Dämon

Daten auf virtuelle Protokolleinheiten schreiben

Es werden beliebige Daten auf eine virtuelle Protokolleinheit geschrieben, indem die entsprechende Datei im Verzeichnis `/dev` geöffnet und Daten in die Datei geschrieben werden. Ein virtuelles Protokoll kann jeweils nur von einem einzigen Prozess geöffnet werden.

Beispiel:

Geben Sie den folgenden Befehl ein, um Nachrichten mit dem Befehl **echo** auf die virtuellen Protokolleinheiten zu schreiben:

```
echo "Protokollnachricht" > /dev/vlog0
```

Geben Sie den folgenden Befehl ein, um Dateien mit dem Befehl **cat** auf den virtuellen Protokolleinheiten zu speichern:

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

Die maximale Größe für jede einzelne Schreiboperation ist auf 32 KB beschränkt und Programme, die versuchen, mehr Daten in einer einzelnen Schreiboperation zu schreiben, empfangen einen E/A-Fehler. Die CLI-Dienstprogramme (Command-Line Interface, Befehlszeilenschnittstelle) wie der Befehl **cat** teilen die Übertragungen automatisch in 32-KB-Schreiboperationen auf.

Trusted Network Connect (TNC)

Trusted Network Connect (TNC) ist Teil der Trusted Computing Group (TCG), die Spezifikationen für die Verifizierung der Endpunktintegrität bereitstellt. TNC hat eine definierte offene Lösungsarchitektur, die Administratoren bei der Durchsetzung von Richtlinien für eine effiziente Zugriffssteuerung auf die Netzinfrastruktur unterstützt.

Trusted Network Connect (TNC) setzt sich aus vier Komponenten zusammen:

- TNC-Server
- TNC Patch Management
- TNC-Server
- TNC-IP-Referrer

Trusted Network Connect-Konzepte

Im Folgenden finden Sie Informationen zu den Komponenten, zur Konfiguration der sicheren Kommunikation und zum Patch-Management-System von Trusted Network Connect (TNC).

Trusted Network Connect-Komponenten

Im Folgenden werden die Komponenten des TNC-Frameworks (Trusted Network Connect) beschrieben.

Das TNC-Modell setzt sich aus den folgenden Komponenten zusammen:

TNC-Server (Trusted Network Connect)

Der TNC-Server (Trusted Network Connect) identifiziert die Clients, die dem Netz hinzugefügt werden, und leitet die Verifizierung dieser Clients ein.

Der TNC-Client stellt dem Server die erforderlichen Dateigruppeninformationen zur Verifizierung bereit. Der Server bestimmt, ob der Client die Version hat, die vom Administrator konfiguriert wurde. Wenn der Client nicht kompatibel ist, benachrichtigt der TNC-Server den Administrator über die erforderlichen Korrekturmaßnahmen.

Der TNC-Server leitet die Verifizierung der Clients ein, die versuchen, auf das Netz zuzugreifen. Der TNC-Server lädt einen Satz von IMVs (Integrity Measurement Verifier), die die Integritätsmesswerte von Clients anfordern und verifizieren können. AIX hat einen Standard-IMV, der die Dateigruppe und den Sicherheits-Patch-Level der Systeme verifiziert. Der TNC-Server ist ein Framework, das mehrere IMV-Module lädt und verwaltet. Bei der Verifizierung eines Clients stützt der Server sich auf die IMVs, die Informationen vom Client anfordern und die Clients verifizieren.

TNC Patch Management

Der TNC-Server (Trusted Network Connect) kann mit Service Update Management Assistant (SUMA) und cURL zu einer Patch-Management-Lösung integriert werden.

Der Patch-Manager lädt die aktuellen Service-Packs und Sicherheitsfixes herunter, die auf der IBM ECC- und der Fix Central-Website verfügbar sind. Der TNC Patch Management-Dämon überträgt die neuesten aktualisierten Informationen mit einer Push-Operation auf den TNC-Server, die als Baseline-Dateigruppe für die Verifizierung der Clients dienen.

Der **tncpmd**-Dämon muss für die Verwaltung von SUMA-Downloads und die Push-Übertragung von Dateigruppeninformationen auf den TNC-Server konfiguriert werden. Dieser Dämon muss sich auf einem System befinden, der mit dem Internet verbunden ist, damit die Aktualisierungen automatisch herunter-

geladen werden. Wenn Sie den TNC Patch Management-Server ohne Verbindung zum Internet verwenden möchten, können Sie ein benutzerdefiniertes Fix-Repository beim TNC Patch Management-Server registrieren.

Anmerkung: Der TNC-Server und der **tncpmd**-Dämon können sich auf demselben System befinden.

Patch Management wird mit einer der folgenden Methoden bereitgestellt:

- Über die Befehlszeilenschnittstelle (pmconf)
- Über den Dämon (tncpmd2)

Befehlszeilenschnittstelle (pmconf) für die Unterstützung des Patch-Managements verwenden:

SUMA und cURL werden aufgerufen, wenn ein Service-Pack-Level (SP-Level) mit dem Befehl **pmconf add** heruntergeladen wird.

Wenn Sie ein Service-Pack-Level (SP-Level) mit dem Befehl **pmconf add** herunterladen, wird SUMA aufgerufen, um den SP-Level herunterzuladen und bei TNC zu registrieren. Außerdem wird cURL aufgerufen, um alle neuen und fehlenden Sicherheitsfixes herunterzuladen.

Mit den folgenden Argumenten für den Befehl **pmconf get** können Sie die Verwaltung von Sicherheitsfixes noch genauer steuern:

- **display-only**: Ermöglicht dem Benutzer, die Beschreibung von Schwachstellen zu prüfen, die von den für den SP-Level gültigen Sicherheitsfixes behoben werden. Die Sicherheitsfixes werden mit diesem Befehl nicht heruntergeladen.
- **download-only**: Ermöglicht dem Benutzer, Sicherheitsfixes in ein benutzerdefiniertes Downloadverzeichnis herunterzuladen, aber nicht anzuwenden. Es werden keine Fixes angewendet.

Dämon (tncpmd2) für die Unterstützung des Patch-Managements verwenden:

Die Scheduler-Komponente des Dämons kann so konfiguriert werden, dass automatisch nach Aktualisierungen (Updates) gesucht wird, die sich auf die Sicherheit von TNC-Clients auswirken.

Ein Downloadintervall steuert, wie oft der Scheduler prüft, ob neue Service-Pack-Levels verfügbar sind. Wenn ein neuer Service-Pack-Level für einen Technology Level (TL), der momentan bei TNC registriert ist, erkannt wird, werden der neue Service-Pack-Level und alle fehlenden oder neuen Sicherheitsfixes heruntergeladen und dem Repository hinzugefügt. Das Downloadintervall wird mit dem Befehl **pmconf init** festgelegt. Es wird empfohlen, mindestens ein Downloadintervall von einmal pro Monat (43.200 Minuten) festzulegen.

Ein Downloadintervall für vorläufige Fixes steuert, wie oft der Scheduler prüft, ob neue vorläufige Sicherheitsfixes veröffentlicht wurden. Alle neuen Sicherheitsfixes werden heruntergeladen und dem Repository hinzugefügt. Es wird empfohlen, ein Downloadintervall von einmal pro Tag (1440 Minuten) festzulegen.

Trusted Network Connect-Client

Der TNC-Client (Trusted Network Connect) stellt Informationen bereit, die der TNC-Server für die Verifizierung benötigt.

Der Server stellt fest, ob der Client die vom Administrator konfigurierte Version hat. Wenn der Client nicht kompatibel ist, benachrichtigt der TNC-Server den Administrator über die erforderlichen Aktualisierungen.

Der TNC-Client lädt die IMCs beim Start und verwendet die IMCs, um die erforderlichen Informationen zusammenzustellen.

IP-Referrer für Trusted Network Connect

Der TNC-Server (Trusted Network Connect) kann die Verifizierung von Clients im Netz automatisch einleiten. Der in der VIOS-Partition (Virtual I/O Server) ausgeführte IP-Referrer erkennt die neuen Clients, die von VIOS bedient werden, und sendet deren IP-Adressen an den TNC-Server. Der TNC-Server verifiziert den Client anhand der definierten Richtlinie.

Sichere Kommunikation über Trusted Network Connect (TNC)

Die TNC-Dämonprozesse (Trusted Network Connect) kommunizieren über die verschlüsselten Kanäle, die mit Transport Layer Security (TLS) oder Secure Sockets Layer (SSL) aktiviert werden.

Durch die sichere Kommunikation wird sichergestellt, dass die im Netz übertragenen Daten und Befehle authentifiziert und sicher sind. Jedes System muss einen eigenen Schlüssel und ein eigenes Zertifikat haben, die bei der Ausführung des Initialisierungsbefehls für die Komponenten generiert werden. Dieser Prozess ist für den Administrator vollständig transparent und erfordert weniger Administratorbeteiligung.

Zur Überprüfung eines neuen Clients muss das Zertifikat des Clients in die Datenbank des Servers importiert werden. Das Zertifikat wird zunächst als nicht vertrauenswürdig markiert. Dann verwendet der Administrator den Befehl **psconf**, um die Zertifikate wie folgt anzuzeigen und als vertrauenswürdig zu markieren:

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

Wenn Sie einen anderen Schlüssel und ein anderes Zertifikat verwenden möchten, können Sie mit dem Befehl **psconf** das Zertifikat importieren.

Geben Sie den folgenden Befehl ein, um das Zertifikat vom Server zu importieren:

```
psconf import  -S -k<Name der Schlüsseldatei> -f<Name der Schlüsseldatei>
```

Geben Sie den folgenden Befehl ein, um das Zertifikat vom Client zu importieren:

```
psconf import -C -k<Name der Schlüsseldatei> -f<Name der Schlüsseldatei>
```

Trusted Network Connect-Protokoll

Das TNC-Protokoll (Trusted Network Connect) wird mit dem TNC-Framework verwendet, um die Netzintegrität zu bewahren.

TNC stellt Spezifikationen zur Verifizierung der Endpunktintegrität bereit. Die Endpunkte, die Zugriff anfordern, werden basierend auf den Integritätsmesswerten kritischer Komponenten bewertet, die sich auf die Betriebsumgebung auswirken können. Das TNC-Framework ermöglicht Administratoren, die Integrität der Systeme im Netz zu überwachen. TNC wird mit der AIX-Patchverteilungsinfrastruktur zu einer vollständigen Patch-Management-Lösung integriert.

Die TNC-Spezifikationen müssen die Anforderungen der AIX- und POWER-Familie-Systemarchitektur erfüllen. Die Komponenten von TNC bieten eine vollständige Patch-Management-Lösung im Betriebssystem AIX. Diese Konfiguration ermöglicht Administratoren eine effiziente Verwaltung der Softwarekonfiguration in AIX-Implementierungen. Sie stellt Tools für die Verifizierung der Patch-Levels der Systeme und für die Generierung von Berichten über die nicht kompatiblen Clients bereit. Außerdem vereinfacht das Patch-Management den Download der Patches und deren Installation.

IMC- und IMV-Module

Der TNC-Server (Trusted Network Connect) oder der TNC-Client verwendet intern die IMC- (Integrity Measurement Collector) und IMV-Module (Integrity Measurement Verifier) für die Serververifizierung.

Dieses Framework ermöglicht das Laden mehrerer IMC- und IMV-Module in den Server und in die Clients. Das Modul, das die Verifizierung auf Betriebssystem- und Dateigruppenebene durchführt, wird

standardmäßig mit dem Betriebssystem AIX geliefert. Verwenden Sie einen der folgenden Pfade, um auf die mit dem Betriebssystem AIX gelieferten Module zuzugreifen:

- `/usr/lib/security/tnc/libfileset_imc.a`: Erfasst die installierte Betriebssystemversion und die Informationen zur installierten Dateigruppe vom Clientsystem und sendet diese zur Verifizierung an das IMV-Modul (TNC-Server).
- `/usr/lib/security/tnc/libfileset_imv.a`: Fordert die Betriebssystemversion und die Dateigruppeninformationen vom Client an und vergleicht sie mit den Baseline-Informationen. Außerdem wird der Status des Clients in der Datenbank des TNC-Servers aktualisiert. Geben Sie zum Anzeigen des Status den folgenden Befehl ein:

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

Zugehörige Verweise:

„Befehl psconf" auf Seite 173

TNC-Anforderungen

Wenn Sie alle Features jeder TNC-Komponente uneingeschränkt nutzen möchten, müssen Sie sicherstellen, dass die Mindestvoraussetzungen in Ihrer Umgebung erfüllt sind.

TNC Patch Management

AIX	SUMA	OpenSSL	Notes
7.2 TL1	7.2.1.0	1.0.2	Bereitstellung mit dem Betriebssystem
7.2 TL0	7.2.1.0	1.0.2	SUMA/Java müssen möglicherweise gesondert installiert werden.
7.1 TL4	7.2.1.0	1.0.2	SUMA/Java müssen möglicherweise gesondert installiert werden.
7.1 TL1, TL2, TL3			Keine Unterstützung für den Download von Service-Pack-Levels für AIX 7.2
7.1 TL0			Unterstütztes Mindest-Release-Level für TNCPM

TNC-Komponenten konfigurieren

Jede der TNC-Komponenten (Trusted Network Connect) muss für die Ausführung in Ihrer speziellen Umgebung konfiguriert werden.

Zum Konfigurieren der TNC-Komponenten muss jeder Schritt in der folgenden Prozedur ausgeführt werden.

1. Ermitteln Sie die IP-Adressen der Systeme, auf denen der TNC-Server, der TNC Patch Management-Server (TNCPM) und der TNC-IP-Referrer für Virtual I/O Server (VIOS) konfiguriert werden.
2. Konfigurieren Sie den NIM-Server (Network Installation Management). Das als TNCPM-Server konfigurierte System ist der NIM-Master. Auf diesem System muss die Dateigruppe `sets:bos.sysmgt.nim.master` installiert werden.
3. Sie müssen Autonomic Health Advisor (AHA) für die automatische Benachrichtigung des TNC-Servers über neue Service-Packs und Sicherheitsfixes aktivieren. Wenn AHA nicht aktiviert ist, aktualisiert der TNC-Scheduler den TNC-Server in den geplanten Intervallen. Geben Sie zum Aktivieren von AHA für automatische Benachrichtigung den folgenden Befehl ein:

   ```
   mkdir /aha
    /usr/sbin/mount -v ahafs  /aha /aha
   ```

4. Geben Sie zum Initialisieren der Fix-Repositorys für TNC Patch Management den folgenden Befehl (in einer einzigen Zeile!) ein:

   ```
   pmconf init -i <Downloadintervall> -l <TL-Liste> [-A] [-P <Downloadpfad>]
   [-x <Intervall_für_vorläufige_Fixes>] [-K <Schlüssel_für_vorläufigen_Fix>]
   ```

   Im Folgenden sehen Sie ein Beispiel für den Befehl **pmconf**:

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

   Der Befehl **init** lädt das neueste Service-Pack für jeden Technology Level herunter und stellt es dem TNC-Server bereit. Die aktualisierten Service-Packs ermöglichen dem TNC-Server, eine grundlegende TNC-Clientprüfung durchzuführen, und dem TNC Patch Management-Server, die TNC-Clientaktualisierungen zu installieren. Geben Sie das Flag **-A** an, um während der Ausführung der Clientaktualisierungen alle Lizenzvereinbarungen zu akzeptieren. Standardmäßig befinden sich die vom TNC Patch Management-Server heruntergeladenen Fix-Repositorys in der Datei `/var/tnc/tncpm/fix_repository`. Verwenden Sie das Flag **-P**, um ein anderes Verzeichnis anzugeben.
5. Konfigurieren Sie den TNCPM-Server. Der TNCPM-Server kann auf dem NIM-System konfiguriert werden. Der TNCPM-Server verwendet SUMA, um die Patches von IBM Fix Central und ECC-Websites herunterzuladen. Der TNCPM-Server verwendet cURL, um vorläufige Fixes von der IBM Security-Website herunterzuladen. Das System muss mit dem Internet verbunden sein, um die Aktualisierungen herunterladen zu können. Geben Sie den folgenden Befehl ein, um den TNCPM-Server zu konfigurieren:

   ```
   pmconf mktncpm [pmport=<Port>]tncserver=<Host:Port>
   ```

   Beispiel:

   ```
   pmconf mktncpm pmport=20000 tncserver=1.1.1.1:10000
   ```
6. Konfigurieren Sie die Richtlinien im TNC-Server. Informationen zum Erstellen der Richtlinien für die Prüfung der Clients finden Sie unter „Richtlinien für den Trusted Network Connect-Client erstellen" auf Seite 136.
7. Konfigurieren Sie die Clients mit dem folgenden Befehl:

   ```
   psconf mkclient tncport=<Port> tncserver=<Server-IP-Adresse>:<Port>
   ```

   Beispiel:

   ```
   psconf mkclient tncport=10000 tncserver=10.1.1.1:10000
   ```
8. Schließen Sie die Konfiguration der TNC-Komponenten ab, indem Sie die optionalen Schritte für jede Komponente ausführen.

Zugehörige Verweise:

„Befehl psconf" auf Seite 173

Zugehörige Informationen:

„PowerSC Standard Edition installieren" auf Seite 7
Sie müssen für jede spezielle Funktion von PowerSC Standard Edition eine Dateigruppe installieren.

Installation mit NIM

IBM Fix Central

Onlinehilfecenter von Passport Advantage

Optionen für die TNC-Komponenten konfigurieren

Sie können eine oder mehrere Optionen für jede der TNC-Komponenten konfigurieren.

Optionen für den Trusted Network Connect-Server (TNC) konfigurieren

Im Folgenden sind die Schritte zum Konfigurieren des TNC-Servers beschrieben.

Wenn Sie den TNC-Server konfigurieren möchten, muss die Datei `/etc/tnccs.conf` einen Wert wie den folgenden enthalten:

```
component = SERVER
```

Geben Sie den folgenden Befehl ein, um ein System als Server zu konfigurieren:

```
psconf mkserver tncport=<Port> pmserver=<IP-Adresse|Hostname[,IP-Adresse2|Hostname2..]:Port>
[recheck_interval=<Zeit in Minuten>]
```

Beispiel:

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

Anmerkung: Der `tncport`-Port und der `pmserver`-Port müssen verschiedene Werte sein. Wenn Sie keinen Wert für den Parameter `recheck_interval` angeben, wird der Standardwert von 1440 Minuten verwendet.

Der Standardportwert 42830 wird für den `tncport`-Port verwendet und der Standardwert 38240 für den `pmserver`-Port.

Zugehörige Verweise:

„Befehl psconf" auf Seite 173

Weitere Optionen für den Trusted Network Connect-Client konfigurieren

Im Folgenden sind die Schritte zum Konfigurieren des TNC-Clients (Trusted Network Connect) und die erforderlichen Konfigurationseinstellungen für das Setup beschrieben.

Wenn Sie den TNC-Client konfigurieren möchten, muss die Datei `/etc/tnccs.conf` einen Wert wie den folgenden enthalten:

```
component = CLIENT
```

Geben Sie den folgenden Befehl ein, um ein System als Client zu konfigurieren:

```
psconf mkclient tncport=<Port> tncserver=<IP-Adresse:Port>
```

Beispiel:

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

Anmerkung: Der Wert für den Server-Port und der `tncport`-Wert, der einen Client-Port angibt, müssen identisch sein.

Zugehörige Verweise:

„Befehl psconf" auf Seite 173

Optionen für den TNC Patch Management-Server konfigurieren

Der Trusted Network Connect Patch Manager-Server (TNCPM) kann mit SUMA und cURL integriert werden, um eine umfassende Patch-Management-Lösung bereitzustellen.

Der TNCPM-Server muss auf dem NIM-Server (Network Installation Management) konfiguriert werden, damit die TNC-Clients aktualisiert werden können.

Für die Unterstützung des automatischen Downloads von IBM Security Advisory und vorläufigen Fixes können Sie ein Intervall für vorläufige Fixes festlegen. Dieses Feature ermöglicht die automatische Benachrichtigung über neu veröffentlichte vorläufige Sicherheitsfixes und die zugehörigen CVE-IDs (Common Vulnerabilities and Exposures). Alle Sicherheitsempfehlungen und vorläufigen Sicherheitsfixes werden vor der Registrierung bei TNC verifiziert. Den öffentlichen Schlüssel zur Vermeidung von IBM AIX-Schwachstellen, der zum automatischen Herunterladen vorläufiger Fixes erforderlich ist, finden Sie auf

der Website zur IBM AIX-Sicherheit. Der automatische Download von Service-Packs und vorläufigen Fixes wird inaktiviert, indem das Downloadintervall und das Intervall für vorläufige Fixes auf 0 gesetzt werden.

Sie können die Registrierung von Service-Packs und vorläufigen Fixes auch manuell aktualisieren. Geben Sie den folgenden Befehl ein, um IBM Security Advisory zusammen mit den zugehörigen vorläufigen Fixes manuell zu registrieren:

```
pmconf add -y <Empfehlungsdatei> -v <Signaturdatei>  -e <TAR-Datei mit vorläufigem Fix>
```

Geben Sie den folgenden Befehl ein, um einen eigenständigen vorläufigen Fix manuell zu registrieren:

```
pmconf add -p <SP> -e <Datei mit vorläufigem Fix>
```

Geben Sie die folgenden Befehl ein, um einen neuen Technology Level zu registrieren und um das zugehörige neueste Service-Pack herunterzuladen:

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

Geben Sie den folgenden Befehl ein, um ein Service-Pack, das nicht die aktuellste Version ist, oder ein Technology Level für Verifizierung und Clientaktualisierungen herunterzuladen:

```
pmconf add -l <TL-Liste> -d
pmconf add -s <SP-Liste>
```

Geben Sie den folgenden Befehl ein, um ein Fix-Repository für Service-Packs oder Technology Levels, das auf dem System vorhanden ist, zu registrieren:

```
pmconf add -s <SP> -p <benutzerdefiniertes_Fix-Repository>
pmconf add -l <TL> -p <benutzerdefiniertes_Fix-Repository>
```

Geben Sie den folgenden Befehl ein, um ein System als Patch-Management-Server zu konfigurieren:

```
pmconf mktncpm [pmport=<Port>] tncserver=IP-Liste[:Port]
```

Im Folgenden sehen Sie ein Beispiel für diesen Befehl:

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

Der TNC Patch Management-Server unterstützt immer das Management von Sicherheits-APARs (Authorized Problem Analysis Reports). Geben Sie den folgenden Befehl ein, um den TNC Patch Management für die Verwaltung anderer APAR-Typen zu konfigurieren:

```
pmconf add -t <Liste_der_APAR-Typen>
```

Im vorherigen Beispiel steht <Liste_der_APAR-Typen> für eine durch Kommas getrennte Liste, die die folgenden Typen von APARs enthält:

- HIPER
- PE
- Enhancement

Geben Sie einen oder mehrere der folgenden Befehle ein, um die TNCPM-Open-Package-Repositorys zu verwalten:

```
pmconf add -o <Paketname> -V <Version> -T [installp|rqm] -D <benutzerdefinierter Pfad>
pmconf delete -o <Paketname> -V <Version>
pmconf list -o <Paketname> -V <Version>
pmconf list -O [-c] [-q]
```

Open Packages werden dem folgenden Standardverzeichnis hinzugefügt:

```
/var/tnc/tncpm/fix_repository/packages
```

Benutzerdefinierter Pfad = Paketposition auf dem System

Geben Sie den folgenden Befehl ein, um beschreibende Informationen, die von Sicherheitsfixes für einen bestimmten Service-Pack-Level adressiert werden, anzuzeigen, ohne die Fixes auf das Repository anzuwenden:

```
pmconf get -L -p <SP>
```

Beispiel:

```
pmconf get -L -p 7200-01-01
```

Geben Sie den folgenden Befehl ein, um Sicherheitsfixes für einen bestimmten Service-Pack-Level herunterzuladen, ohne die Fixes auf das Repository anzuwenden:

```
pmconf get -p <SP> -D <Downloadverzeichnis>
```

Anmerkung: Das *Downloadverzeichnis* muss vorhanden sein, bevor dieser Befehl ausgeführt wird.

Beispiel:

```
pmconf get -p 7200-01-01 -D /tmp/ifixes_7200-01-01
```

Der TNC Patch Management-Server unterstützt den Befehl **syslog** für das Herunterladen von Service-Packs, Technology Levels und Clientaktualisierungen. Die Funktion ist `user` und die Priorität ist `info`, z. B. `user.info`.

Der TNC Patch Management-Server verwaltet auch ein Protokoll mit allen Clientaktualisierungen im Verzeichnis `/var/tnc/tncpm/log/update/<ip>/<Zeitmarke>`.

Zugehörige Verweise:

„Befehl psconf" auf Seite 173

Zugehörige Informationen:

IBM AIX Security

E-Mail-Benachrichtigung für Trusted Network Connect-Server konfigurieren

Im Folgenden wird beschrieben, wie Sie die E-Mail-Benachrichtigung für den TNC-Server (Trusted Network Connect) konfigurieren.

Der TNC-Server überprüft den Patch-Level des Clients und sendet dann eine E-Mail mit dem Ergebnis und der erforderlichen Korrekturmaßnahme an den Administrator, wenn er feststellt, dass der Client nicht kompatibel ist.

Geben Sie den folgenden Befehl ein, um die E-Mail-Adresse des Administrators zu konfigurieren:

```
psconf add –e <E-Mail-ID>[ipgroup=[±]G1, G2 ..]
```

Beispiel:

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

Im vorherigen Beispiel wird die E-Mail für die IP-Gruppen *vayugrp1* und *vayugrp2* an die E-Mail-Adresse abc@ibm.com gesendet.

Geben Sie den folgenden Befehl ein, um eine E-Mail an eine globale E-Mail-Adresse für die IP-Gruppe zu senden, der keine E-Mail-Adresse zugewiesen ist:

```
psconf add –e <E-Mail-Adresse>
```

Beispiel:

```
psconf add –e abc@ibm.com
```

Wenn im vorherigen Beispiel einer IP-Gruppe keine E-Mail-Adresse zugewiesen ist, wird die E-Mail an die E-Mail-Adresse abc@ibm.com gesendet. Diese Adresse dient als globale E-Mail-Adresse.

Zugehörige Verweise:

„Befehl psconf" auf Seite 173

IP-Referrer in VIOS konfigurieren

Im Folgenden wird beschrieben, wie Sie den IP-Referrer in Virtual I/O Server (VIOS) konfigurieren, sodass automatisch eine Prüfung eingeleitet wird.

Anmerkung: Vor der Konfiguration des IP-Referrers müssen Sie die SVM-Kernelerweiterung in Virtual I/O Server (VIOS) konfigurieren.

Zum Konfigurieren des TNC-IP-Referrers muss die Konfigurationsdatei `/etc/tnccs.conf` eine Einstellung wie `component = IPREF` enthalten.

Mit dem folgenden Befehl können Sie ein System als Client konfigurieren:

```
psconf mkipref tncport=<Port> tncserver=<IP-Adresse:Port>
```

Beispiel:

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

Der `tncserver`-Portwert und der `tncport`-Wert, der den Client-Port angibt, müssen identisch sein.

Konfigurieren Sie den TNC-IP-Referrer in VIOS. Diese Konfiguration in VIOS löst die Überprüfung für die Clients aus, die eine Verbindung zum Netz herstellen. Geben Sie den folgenden Befehl ein, um den Referrer zu konfigurieren:

```
psconf mkipref tncport=<Port> tncserver=<IP-Adresse:Port>
```

Beispiel:

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

Anmerkung: Der Wert für den Server-Port und der Wert für den TNC-Port, der den Client-Port angibt, müssen identisch sein.

Zugehörige Verweise:

„Befehl psconf" auf Seite 173

Trusted Network Connect-Komponenten (TNC) verwalten

Im Folgenden wird beschrieben, wie Sie Trusted Network Connect (TNC) verwalten, um Aufgaben wie das Hinzufügen der Clients, Richtlinien, Protokolle, Prüfergebnisse, das Aktualisieren von Clients und TNC-relevanten Zertifikaten zu implementieren.

Trusted Network Connect-Serverprotokolle anzeigen

Im Folgenden wird beschrieben, wie Sie die Protokolle des TNC-Servers (Trusted Network Connect) anzeigen.

Der TNC-Server protokolliert die Verifizierungsergebnisse aller Clients. Führen Sie zum Anzeigen des Protokolls den Befehl **psconf** wie folgt aus:

```
psconf list –H –i <IP-Adresse |ALL>
```

Zugehörige Verweise:

„Befehl psconf" auf Seite 173

Richtlinien für den Trusted Network Connect-Client erstellen

Im Folgenden wird beschrieben, wie Sie Richtlinien für den Trusted Network Connect-Client (TNC) konfigurieren.

Die psconf-Konsole ist die Schnittstelle für die Verwaltung der TNC-Richtlinien. Jedem Client und jeder Gruppe von Clients kann eine Richtlinie zugeordnet werden.

Die folgenden Richtlinien können erstellt werden:

- Eine IP-Gruppe (Internet Protocol) enthält mehrere Client-IP-Adressen.
- Jede Client-IP-Adresse kann nur zu einer einzigen Gruppe gehören.
- Die IP-Gruppe wird einer Richtliniengruppe zugeordnet.
- Eine Richtliniengruppe enthält verschiedene Arten von Richtlinien. Die Dateigruppenrichtlinie legt beispielsweise die erforderliche Betriebssystemversion des Clients fest (d. h. Release, Technology Level und Service-Pack). Eine Richtliniengruppe kann mehrere Dateigruppenrichtlinien enthalten und der Client, der auf diese Richtlinie verweist, muss die Version haben, die von einer der Dateigruppenrichtlinien festgelegt wird.

Die folgenden Befehle veranschaulichen, wie eine IP-Gruppe, eine Richtliniengruppe und Dateigruppenrichtlinien erstellt werden.

Geben Sie zum Erstellen einer IP-Gruppe den folgenden Befehl ein:

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

Beispiel:

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

Anmerkung: Für eine Gruppe muss mindestens eine IP-Adresse angegeben werden. Mehrere IP-Adressen müssen durch Kommas voneinander getrennt werden.

Geben Sie zum Erstellen einer Dateigruppenrichtlinie den folgenden Befehl ein:

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

Beispiel:

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

Anmerkung: Die Buildinformationen müssen im Format <rel00-TL-sp> angegeben werden.

Geben Sie zum Erstellen einer Richtlinie und zum Zuweisen einer IP-Gruppe den folgenden Befehl ein:

```
psconf add –P <Richtlinienname> ipgroup=[±] <IP-Gruppe1, IP-Gruppe2 ...]
```

Beispiel:

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

Geben Sie zum Zuweisen einer Dateigruppenrichtlinie zu einer Richtlinie den folgenden Befehl ein:

```
psconf add –P <Richtlinienname> fspolicy=[±]<Dateigruppenrichtlinie1, Dateigruppenrichtlinie2 ...>
```

Beispiel:

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

Geben Sie zum Hinzufügen einer OpenPackage-Richtlinie den folgenden Befehl ein:

```
pconf add -O <OpenPackage-Gruppe> <OpenPackage-Name:Version>
```

Im Folgenden sehen Sie ein Beispiel für das Hinzufügen einer OpenPackage-Richtlinie:

```
psconf add –O opengrp2 openssl:1.0.1.516
```

Geben Sie zum Zuweisen einer OpenPackage-Richtlinie zur Dateigruppenrichtlinie den folgenden Befehl ein:

```
psconf add -O opengrp2 fspolicy=fspolicy1
```

Anmerkung: Wenn mehrere Dateigruppenrichtlinien angegeben werden, setzt das System die am besten geeignete Richtlinie auf dem Client um. Wenn sich der Client beispielsweise auf `6100-02-01` befindet und Sie die Dateigruppenrichtlinien `7100-03-04` und `6100-02-03` angeben, wird `6100-02-03` auf dem Client umgesetzt.

Zugehörige Verweise:

„Befehl psconf" auf Seite 173

Verifizierung des Trusted Network Connect-Clients starten

Im Folgenden wird beschrieben, wie Sie den TNC-Client (Trusted Network Connect) verifizieren.

Verwenden Sie für die Clientverifizierung eine der folgenden Methoden:

- Der IP-Referrer-Dämon in Virtual I/O Server (VIOS) leitet die Client-ID an den TNC-Server weiter: Die Client-LPAR übernimmt die IP-Adresse und versucht, auf das Netz zuzugreifen. Der IP-Referrer-Dämon in VIOS erkennt die neue IP-Adresse und leitet sie an den TNC-Server weiter. Der TNC-Server leitet die Verifizierung beim Empfang der neuen IP-Adresse ein.
- Der TNC-Server verifiziert den Client in regelmäßigen Abständen: Der Administrator kann die Client-IP-Adressen, die verifiziert werden müssen, in der TNC-Richtliniendatenbank hinzufügen. Der TNC-Server verifiziert die Clients, die in der Datenbank vorhanden sind. Die erneute Verifizierung findet automatisch in einem regelmäßigen Intervall statt, das mit dem Attribut `recheck_interval` in der Konfigurationsdatei `/etc/tnccs.conf` definiert ist.
- Der Administrator leitet die Clientverifizierung manuell ein: Der Administrator kann die Verifizierung mit dem folgenden Befehl manuell einleiten, um zu prüfen, ob dem Netz ein Client hinzugefügt wurde:

  ```
  pconf verify -i <IP-Adresse>
  ```

Anmerkung: Für Ressourcen, die nicht mit einem VIOS verbunden sind, können die Clients verifiziert und aktualisiert werden, wenn sie dem TNC-Server manuell hinzugefügt werden.

Zugehörige Verweise:

„Befehl psconf" auf Seite 173

Verifizierungsergebnisse von Trusted Network Connect anzeigen

Im Folgenden wird beschrieben, wie Sie die Verifizierungsergebnisse des TNC-Clients (Trusted Network Connect) anzeigen.

Geben Sie den folgenden Befehl ein, um die Verifizierungsergebnisse der Clients im Netz anzuzeigen:

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

Dieser Befehl zeigt alle Clients mit dem Status **IGNORED** (Ignoriert), **COMPLIANT** (Kompatibel) und **FAILED** (Fehlgeschlagen) an.

- **IGNORED**: Die Client-IP-Adresse wird in der IP-Liste ignoriert (d. h., der Client kann von der Verifizierung ausgeschlossen werden).
- **COMPLIANT**: Die Verifizierung des Clients war erfolgreich (d. h., der Client ist mit der Richtlinie kompatibel).
- **FAILED**: Die Verifizierung des Clients ist fehlgeschlagen (d. h., der Client ist nicht mit der Richtlinie kompatibel und es muss eine Verwaltungsaktion ausgeführt werden).

Führen Sie zur Bestimmung der Fehlerursache den Befehl **psconf** mit der Client-IP-Adresse, deren Verifizierung fehlgeschlagen ist, aus:

```
psconf list -s ALL -i <IP-Adresse>
```

Zugehörige Verweise:

„Befehl psconf" auf Seite 173

Trusted Network Connect-Client aktualisieren

Der TNC-Server (Trusted Network Connect) verifiziert einen Client und aktualisiert die Datenbak mit dem Status des Clients und dem Ergebnis der Verifizierung. Der Administrator kann die Ergebnisse anzeigen und die Aktionen zum Aktualisieren des Clients ausführen.

Geben Sie den folgenden Befehl ein, um einen Client einer früheren Version zu aktualisieren:

```
psconf update -i <ip> -r <Buildinformationen> [-a APAR1,APAR2...]
```

Beispiel:

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

Der Befehl **psconf** aktualisiert den Client mit dem Build und den APAR-Installationen, sofern diese nicht installiert sind.

Geben Sie zum Aktualisieren des Clients mit Open Packages den folgenden Befehl ein:

```
psconf update -i <IP-Adresse> -O opengrp2
```

Zugehörige Verweise:

„Befehl psconf" auf Seite 173

Patch-Management-Richtlinien verwalten

Der Befehl **pmconf** wird verwendet, um die Patch-Management-Richtlinien zu konfigurieren.

Die Patch-Management-Richtlinien enthalten Informationen wie die IP-Adresse des TNC-Servers und das Zeitintervall zum Einleiten einer SUMA-Aktualisierung.

Geben Sie den folgenden Befehl ein, um die Patch-Management-Richtlinie zu verwalten:

```
pmconf mktncpm [pmport=<Port>] tncserver=<Host:Port>
```

Beispiel:

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

Anmerkung: Die Portwerte für `pmport` und `tncserver` müssen verschieden sein.

Zugehörige Verweise:

„Befehl pmconf" auf Seite 169

Trusted Network Connect-Zertifikate importieren

Im Folgenden wird beschrieben, wie Sie ein Zertifikat importieren und Daten in einem Netz sicher übertragen.

Die TNC-Dämonprozesse (Trusted Network Connect) kommunizieren über die verschlüsselten Kanäle, die mit dem TLS- (Transport Layer Security) oder SSL-Protokoll (Secure Sockets Layer) aktiviert werden. Dieser Dämon stellt sicher, dass die Daten und Befehle, die im Netz übertragen werden, authentifiziert und sicher sind. Jedes System hat einen eigenen Schlüssel und ein eigenes Zertifikat, die bei der Ausführung des Initialisierungsbefehls für die Komponenten generiert werden. Dieser Prozess ist für den Administrator transparent und erfordert weniger Administratorbeteiligung. Wenn ein Client zum ersten Mal verifiziert wird, wird dessen Zertifikat in die Datenbank des Servers importiert. Das Zertifikat wird zu-

nächst als nicht vertrauenswürdig markiert. Der Administrator verwendet den Befehl **psconf**, um die Zertifikate wie folgt anzuzeigen und als vertrauenswürdig zu markieren:

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

Wenn der Administrator einen anderen Schlüssel und ein anderes Zertifikat verwenden möchte, kann er mit dem Befehl **psconf** den Schlüssel und das Zertifikat importieren.

Geben Sie den folgenden Befehl ein, um das Zertifikat von einem Server zu importieren:

```
psconf import  -S -k <Name der Schlüsseldatei> -f <Dateiname>
```

Geben Sie den folgenden Befehl ein, um das Zertifikat von einem Client zu importieren:

```
psconf import  -C -k <Name der Schlüsseldatei> -f <Dateiname>
```

Zugehörige Verweise:

„Befehl psconf" auf Seite 173

Berichterstellung im TNC-Server

Der TNC-Server (Trusted Network Connect) unterstützt das CSV-Format (Comma-Separated Values, durch Kommas getrennte Werte) und das Textausgabeformat für Berichte über allgemeine Schwachstellen und Sicherheitslücken (CVE, Common Vulnerabilities and Exposures), IBM Security Advisory, TNC-Serverrichtlinien, Sicherheitsfixes für TNC-Clients sowie registrierte Service-Packs und vorläufige Fixes.

Im CVE-Bericht werden alle allgemeinen Sicherheitslücken und Schwachstellen für die registrierten Service-Packs angezeigt. Geben Sie den folgenden Befehl ein, um die Ergebnisse diese Berichts anzuzeigen:

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

Im IBM Security Advisory-Bericht werden die bekannten Sicherheitsschwachstellen in der installierten IBM Software angezeigt. Geben Sie den folgenden Befehl ein, um die Ergebnisse diese Berichts anzuzeigen:

```
psconf report -A <Empfehlungsname>
```

Im Bericht über die TNC-Serverrichtlinien werden die Sicherheitsrichtlinien angezeigt, die auf dem TNC-Server durchgesetzt werden. Geben Sie den folgenden Befehl ein, um die Ergebnisse diese Berichts anzuzeigen:

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

Im Bericht über die TNC-Client-Fixes werden die installierten und fehlenden vorläufigen Fixes für den TNC-Client angezeigt. Geben Sie den folgenden Befehl ein, um die Ergebnisse diese Berichts anzuzeigen:

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

Sie können auch einen Bericht ausführen, der eine Liste mit den registrierten Service-Packs und den zugehörigen APARs (Authorized Program Analysis Reports) und vorläufigen Fixes generiert. Geben Sie den folgenden Befehl ein, um die Ergebnisse diese Berichts anzuzeigen:

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

Geben Sie den folgenden Berichtsbefehl ein, um eine Liste mit den registrierten Open-Source-Paketen anzuzeigen:

```
psconf report -O ALL -o TEXT
```

Zugehörige Verweise:

„Befehl psconf" auf Seite 173

Fehler bei Trusted Network Connect und Patch Management beheben

Im Folgenden sind die möglichen Ursachen für Fehler und die Schritte zur Behebung von Fehlern in TNC und im Patch-Management-System beschrieben.

Zur Behebung von Fehlern in TNC und im Patch-Management-System überprüfen Sie die Konfigurationseinstellungen, die in der folgenden Tabelle aufgelistet sind.

Tabelle 13. Fehler in den Konfigurationseinstellungen für TNC und Patch-Management-Systeme beheben

Problem	Lösung
Der TNC-Server wird nicht gestartet oder er reagiert nicht.	Führen Sie die folgende Prozedur aus: 1. Stellen Sie mit dem folgenden Befehl fest, ob der Dämon für den TNC-Server aktiv ist: `ps –eaf | grep tnccsd` 2. Sollte der Dämon nicht aktiv sein, löschen Sie die Datei `/var/tnc/.tncsock`. 3. Starten Sie den Server erneut. Sollte das Problem damit nicht behoben sein, suchen Sie in der Konfigurationsdatei `/etc/tnccs.conf` im TNC-Server nach dem Eintrag `component = SERVER`.
Der TNC Patch Management-Server wird nicht gestartet oder er reagiert nicht.	• Stellen Sie mit dem folgenden Befehl fest, ob der Dämon für den TNC Patch Management-Server aktiv ist: `ps –eaf | grep tncpmd` • Suchen Sie in der Konfigurationsdatei `/etc/tnccs.conf` im TNC Patch Management-Server nach dem Eintrag `component = TNCPM`.
Der TNC-Client wird nicht gestartet oder er reagiert nicht.	• Stellen Sie mit dem folgenden Befehl fest, ob der Dämon für den TNC-Client aktiv ist: `ps –eaf | grep tnccsd` • Suchen Sie in der Konfigurationsdatei `/etc/tnccs.conf` im TNC-Client nach dem Eintrag `component = CLIENT`.
Der TNC-IP-Referrer in Virtual I/O Server (VIOS) ist nicht aktiv.	• Stellen Sie mit dem folgenden Befehl fest, ob der Dämon für den TNC-IP-Referrer aktiv ist: `ps –eaf | grep tnccsd` • Suchen Sie in der Konfigurationsdatei `/etc/tnccs.conf` in VIOS nach dem Eintrag `component = IPREF`.
Ein System kann nicht gleichzeitig als TNC-Server und als TNC-Client konfiguriert werden.	Der TNC-Server und der TNC-Client kann nicht gleichzeitig auf demselben System ausgeführt werden.
Die Dämonprozesse sind aktiv, aber die Verifizierung findet nicht statt.	Aktivieren Sie die Protokollnachrichten nach den Dämonprozessen. Definieren Sie die Protokolleinstellung `level=info` in der Datei `/etc/tnccs.conf`. Sie können die Protokollnachrichten analysieren.

Grafische Benutzerschnittstelle von PowerSC

In diesem Abschnitt finden Sie eine Beschreibung der grafischen Benutzerschnittstelle von IBM PowerSC, einschließlich Informationen zur Installation, Verwaltung und Verwendung der Schnittstelle.

Die IBM PowerSC-GUI verbesssert die Benutzerfreundlichkeit des Produkts PowerSC Standard Edition und ist eine Alternative zur Befehlszeilen- und Protokolldateiinteraktion. Die PowerSC-GUI ist eine zentrale Managementkonsole für die Visualisierung von Endpunkten und deren Status: Anwenden, Widerrufen und Prüfen von Konformitätsstufen, Gruppierung von Systemen für die Anwendung von Aktionen für Konformitätsstufen und Anzeige und Anpassung von Konformitätskonfigurationsprofilen.

Außerdem enthält die PowerSC-GUI FIM (File Integrity Monitoring). FIM beinhaltet Real Time Compliance (RTC) und Trusted Execution (TE). Über die PowerSC-GUI können Sie RTC und TE konfigurieren und Ereignisse in Echtzeit anzeigen. Die PowerSC-GUI bietet darüber hinaus zahlreiche Funktionen für die Profilbearbeitung und die Berichterstellung.

PowerSC-GUI-Konzepte

Vor der Verwendung der PowerSC-GUI sollten Sie sich mit den allgemeinen Konzepten in Bezug auf Sicherheit und Endpunkterkennung vertraut machen.

PowerSC-GUI-Sicherheit

Die PowerSC-GUI gewährleistet die Sicherheit durch bidirektionale HTTPS-Kommunikation zwischen dem PowerSC-GUI-Server und den PowerSC-GUI-Agenten auf den einzelnen AIX-Endpunkten.

Der TLS-Handshakeprozess verwendet Zertifikate, die auf dem PowerSC-GUI-Server und den PowerSC-GUI-Agenten verfügbar sind. Der TLS-Handshakeprozess unterstützt die Einzelauthentifizierung in beide Richtungen, weil entweder der PowerSC-GUI-Agent oder der PowerSC-GUI-Server die Kommunikation einleiten kann. Der Agent erstellt eine generierte Zufallszahl (Nonce), die bei der Erstverbindung an den PowerSC-GUI-Server gesendet wird. Der PowerSC-GUI-Server schließt diese Nonce dann in jeden Befehl ein, der an diesen Agenten gesendet wird. Diese Nonce ist eine weitere Bestätigungsebene für den Endpunktagenten, der einen Befehl ausführt, der vom authentischen PowerSC-GUI-Server stammt. Der Endpunkt muss sicherstellen, dass die Quelle des Web-Service-Aufrufs vertrauenswürdig ist. Der anfängliche Handshake und die Nonce stellen die Vertrauensbeziehung sicher.

Die gesamte Kommunikation zwischen den PowerSC-GUI-Agenten und dem PowerSC-GUI-Server wird mit Protokollen und Cipher-Suites verschlüsselt, die mit den Sicherheitsanforderungen der geschützten Systeme konsistent sind. Momentan ist die Protokollversion TLS 1.2. Der PowerSC-GUI-Server interagiert mit allen PowerSC-GUI-Agenten und mit allen PowerSC-GUI-Benutzern. Deshalb muss der PowerSC-GUI-Server ein Zertifikat haben, das von allen Verbindungen, die über die Web-Browser der Benutzer hergestellt werden, anerkannt wird, z. B. ein Zertifikat von einer Standardzertifizierungsstelle wie Verisign oder von einer intern anerkannten Zertifizierungsstelle.

Während der Installation erstellt der PowerSC-GUI-Server ein selbst signiertes Zertifikat für die eigene Verwendung. Dieses Zertifikat kann unbegrenzt verwendet werden, ist aber eigentlich nur zur temporären Verwendung bestimmt und kann durch ein vom Benutzer bereitgestelltes weithin anerkanntes Zertifikat ersetzt werden. Bei der Installation des PowerSC-GUI-Servers wird außerdem ein Signierzertifikat erstellt, das für die Unterzeichnung aller Endpunktzertifikate verwendet wird.

Der Installationsprozess erstellt für jeden Endpunkt automatisch eine Truststore-Datei. Die Truststore-Datei ist für alle Endpunkte dieselbe und muss vom PowerSC-GUI-Server auf jeden Endpunkt kopiert werden. Diese Kombination von Zertifikaten auf dem PowerSC-GUI-Server und auf den Endpunkten gewährleistet eine hohe Kommunikationssicherheit.

Weitere Sicherheitssteuerelemente werden bei der Verwendung von UNIX-Gruppen bereitgestellt. Für die Anmeldung an der PowerSC-GUI muss jeder Benutzer Mitglied der angegebenen UNIX-Gruppe sein, unabhängig von, ob es sich um einen LDAP-Benutzer oder einen lokalen Benutzer, der vom Betriebssystem definiert wurde, handelt. Der Administrator kann die Gruppenzugehörigkeit mit dem Befehl **pscuiserverctl** festlegen und ändern.

Nach der Anmeldung sind Sie möglicherweise weiterhin auf den Anzeigemodus beschränkt. Mit der Funktion für Benutzerberechtigung können Sie Aktionen für Endpunkte ausführen, die über UNIX-Gruppenzugehörigkeiten gesteuert werden. Zur Ausführung aller Aktionen müssen Sie zu einer UNIX-Gruppe gehören, die berechtigt ist, den Endpunkt zu verwalten. Weitere Informationen finden Sie im Abschnitt Gruppen mit Zugriffsberechtigungen angeben.

Standardmäßig kann jeder Benutzer, der zur Sicherheitsgruppe gehört, jeden Endpunkt verwalten, der in der PowerSC-GUI sichtbar ist. Der PowerSC-Administrator kann den Benutzerzugriff mit dem Befehl **setGroups.sh** auf der Ebene einzelner Endpunkte beschränken.

Es gibt eine Reihe von Konfigurationsbefehlen, die nur von einem Benutzer mit Verwaltungsaufgaben ausgeführt werden können. Dazu gehören beispielsweise das Ändern der globalen E-Mail-Einstellungen und die Erstellung eines neuen Profils. Die Berechtigung für Benutzer mit Verwaltungsaufgaben wird mithilfe von UNIX-Gruppen festgelegt und kann mit dem Befehl **pscuiserverctl** konfiguriert werden.

Endpunktinhalt auf der Seite "Konformität" eingeben

Der PowerSC-GUI-Server und der PowerSC-GUI-Agent kommunizieren mit dem Endpunkt, um die Konformitätsstufe zu bestimmen.

Der Agent versucht beim Start, eine Verbindung zum PowerSC-GUI-Server herzustellen, und versucht es dann sporadisch wieder, bis er erfolgreich ist. Sobald die Verbindung hergestellt wurde, wird ein einmaliger Sicherheitshandshake zwischen dem Agenten und dem Server durchgeführt. Nachdem der Sicherheitshandshake zwischen dem Agenten und dem Server das erste Mal erfolgreich ausgehandelt wurde, erstellt der Server ein Domänenelement mit einer eindeutigen ID (UID, Unique Identifier) für die interne Darstellung des Endpunkts und übergibt die UID an den Endpunkt zurück. Die UID wird dann in jede Kommunikation zwischen dem Agenten und dem Server eingeschlossen. Diese Aktion schließt den Erkennungsprozess ab. Der PowerSC-GUI-Server und der Endpunkt können in beide Richtungen sicher kommunizieren.

Nach Abschluss des anfänglichen Sicherheitshandshakes bzw. nach dem Neustart des PowerSC-GUI-Agenten versucht der PowerSC-GUI-Agent, die aktuellen Konformitätsstatusinformationen für seinen Endpunkt zu bestimmen, und aktualisiert den PowerSC-GUI-Server. Die Existenz des Endpunkts und der aktuellen Konformitätsinformationen werden verwendet, um die Seite zum Konformitätsstatus der PowerSC-GUI zu füllen. Wenn keine Konformitätsstatusinformationen bestimmt werden können, ist der Eintrag auf der Seite zum Konformitätsstatus nicht verfügbar.

Der PowerSC-GUI-Server enthält Darstellungen aller bekannten Endpunkte, die automatisch bei der Herstellung der Erstverbindung und -kommunikation zwischen Agent und Server erstellt werden. Während die Endpunktagenten Änderungen beim Konformitätsstatus des Endpunkts verfolgen, werden die Änderungen an den Server übergeben und beibehalten. Alle Benutzerinteraktionen in der PowerSC-GUI mit einem Endpunkt erfolgen über den PowerSC-GUI-Server. Die Benutzerschnittstelle interagiert nicht direkt mit Endpunkten und Endpunktagenten.

PowerSC-GUI installieren

Die PowerSC-GUI-Agenten und die PowerSC-GUI-Serverkomponenten werden während der Installation von PowerSC Standard Edition über die `installp`-Dateigruppen installiert.

PowerSC-GUI-Agent

Der PowerSC-GUI-Agent wird auf jedem AIX-Endpunkt installiert. Der PowerSC-GUI-Agent verfolgt die Aktivitäten auf dem Endpunkt und stellt diese Informationen dem PowerSC-GUI-Server bereit.

Der PowerSC-GUI-Agent führt auch die Befehle aus, die in der PowerSC-GUI ausgelöst werden. Die gesamte Kommunikation zwischen PowerSC-GUI-Agenten und dem PowerSC-GUI-Server wird verschlüsselt.

Der Befehl `installp` installiert das PowerSC Standard Edition-Basisprodukt und den PowerSC-GUI-Agenten. Für die Installation des PowerSC-GUI-Agenten wird die `installp`-Dateigruppe `powerscStd.uiAgent.rte` verwendet. Im folgenden Beispiel sehen Sie den Befehl `installp`, der auf jedem Endpunkt ausgeführt wird.

Anmerkung: Im folgenden Beispiel werden die Installationsprogrammimages im Verzeichnis `/tmp/inst.images/` dekomprimiert.

```
#installp -agXYd /tmp/inst.images powerscStd.ice powerscStd.license powerscStd.uiAgent.rte
```

PowerSC-GUI-Server

Der PowerSC-GUI-Server kann auf jedem AIX-System ausgeführt werden, aber es wird empfohlen, eine dedizierte AIX-LPAR zu erstellen, auf der Sie den PowerSC-GUI-Server installieren und ausführen.

Der Befehl **installp** installiert das PowerSC Standard Edition-Basisprodukt und den PowerSC-GUI-Server. Für die Installation des PowerSC-GUI-Servers wird die **installp**-Dateigruppe `powerscStd.uiServer.rte` verwendet. Im folgenden Beispiel sehen Sie den Befehl **installp**, der auf einem Endpunkt ausgeführt wird.

Anmerkung: Im folgenden Beispiel werden die Installationsprogrammimages im Verzeichnis `/tmp/inst.images/` dekomprimiert.

```
#installp -agXYd /tmp/inst.images powerscStd.ice powerscStd.license powerscStd.uiServer.rte
```

Voraussetzung für die PowerSC-GUI

In Folgenden sind die Hardware- und Softwarevoraussetzungen für die PowerSC-GUI beschrieben.

Hardware

- Die PowerSC-GUI-Serverkomponenten müssen auf einer separaten LPAR oder VM, auf der AIX 7.1 installiert oder höher installiert ist, installieren.
- Die PowerSC-GUI-Agentenkomponenten müssen auf jedem AIX-Endpunkt installiert werden.

Software

- Der PowerSC-GUI-Server setzt AIX 7.1 oder höher voraus.
- Auf dem PowerSC-GUI-Server muss der sendmail-Dämon ausgeführt werden.
- Die Dateigruppe `bos.loc.utf.<SPRACHE>` muss installiert werden, damit die Beschreibungen von Profilregeln in der PowerSC-GUI auch in anderen Sprachen als Englisch korrekt angezeigt werden.

Sicherheitszertifikat für den Truststore an Endpunkte verteilen

Systemadministratoren müssen das Sicherheitszertifikat für den Truststore auf allen Endpunkten implementieren.

Während der Installation wird eine Truststore-Datei erstellt, die von allen Endpunkten verwendet werden kann. Der Name der Datei ist `endpointTruststore.jks`. Die Datei wird im Verzeichnis `/etc/security/powersc/uiServer/` gespeichert.

Nach der Installation müssen Sie die Datei endpointtruststore.jks auf jedem Endpunkt für den PowerSC-GUI-Agenten auf diesem Endpunkt kopieren, um eine Verbindung zum PowerSC-GUI-Server herzustellen und um den Prozess einzuleiten, der zur Erstellung des Keystores auf dem Endpunkt führt.

Sie können die Truststore-Datei auf eine der folgenden Arten verteilen:

- Kopieren Sie die Datei endpointTruststore.jks manuell auf jeden Endpunkt.
- Wenn PowerVC (oder ein anderer Virtualisierungsmanager) in Ihrer Umgebung verwendet wird, kann die Datei endpointTruststore.jks in das PowerVC-Image kopiert werden. Bei der Implementierung des PowerVC-Image auf einem Endpunkt sind dann der PowerSC-GUI-Agent und die Truststore-Datei enthalten.

Nach der Implementierung der Datei endpointTruststore.jks mit einer dieser Methoden verwendet der PowerSC-GUI-Agent beim Start eines Endpunkts die Truststore-Datei, um die Position zu bestimmen, an der der PowerSC-GUI-Server ausgeführt wird. Der PowerSC-GUI-Agent sendet dann eine Nachricht mit einer Anforderung zum Beitritt zur Liste verfügbarer und überwachter Endpunkte an den PowerSC-GUI-Server.

Truststore-Datei manuell auf Endpunkte kopieren

Systemadministratoren müssen die Truststore-Datei manuell auf jeden vorhandenen Endpunkt in ihrer Umgebung kopieren.

Die Truststore-Datei muss auf auch jeden neuen Endunkt, der hinzugefügt wird, kopiert werden.

Anmerkung: Wenn Sie einen Datenvirtualisierungsmanager wie PowerVC haben, können Sie die Truststore-Datei auf einen neuen Endpunkt kopieren, indem Sie ein Image erstellen, das sowohl den PowerSC-GUI-Agenten als auch die Truststore-Datei enthält. Siehe „Truststore-Datei mit einem Virtualisierungsmanager auf Endpunkte kopieren".

1. Führen Sie den folgenden **scp**-Befehl aus, um die Endpunkt-Truststore-Datei /etc/security/powersc/uiServer/endpointTruststore.jks in die Datei /etc/security/powersc/uiAgent/endpointTruststore.jks auf jedem Endpunkt zu kopieren:

   ```
   # scp endpointTruststore.jks user@endpoint-host-name:
                          /etc/security/powersc/uiAgent
   ```

2. Führen Sie die folgenden Befehle auf dem Endpunkt aus, um die Endpunktagenten nach der Installation des Sicherheitszertifikats erneut zu starten:

   ```
   stopsrc -s pscuiagent
   startsrc -s pscuiagent
   ```

3. Wiederholen Sie die Schritte 1 und 2 für jeden vorhandenen Endpunkt und für jeden neuen Endpunkt (wenn Sie keinen Datenvirtualisierungsmanager haben).

Truststore-Datei mit einem Virtualisierungsmanager auf Endpunkte kopieren

Systemadministratoren können einen Virtualisierungsmanager wie PowerVC verwenden, um die Truststore_Datei unter Verwendung eines Imge, das den PowerSC-Agenten und die Truststore-Datei enthält, auf jeden neuen Endpunkt zu kopieren.

1. Kopieren Sie die Truststore-Datei des Endpunkts, /etc/security/powersc/uiServer/endpointTruststore.jks, in das PowerVC-Image.
2. Implementieren Sie das PowerVC-Image auf jedem neuen Endpunkt, der dem System hinzugefügt wird.

Benutzeraccounts einrichten

Für die Anmeldung an der PowerSC-GUI muss standardmäßig jeder Benutzer Mitglied der Sicherheitsgruppe sein, unabhängig von, ob es sich um einen LDAP-Benutzer oder einen lokalen Benutzer, der vom Betriebssystem definiert wurde, handelt.

Der Administrator kann diese erforderliche Gruppenzugehörigkeit mit dem Befehl **pscuiserverctl** ändern. Nach der Anmeldung an der PowerSC-GUI kann ein Benutzer nur den Status von Endpunkten anzeigen, wenn sein Benutzeraccount zu einer UNIX-Gruppe gehört, die berechtigt ist, den Endpunkt zu verwalten. Der Administrator kann die Benutzeraccounteinstellungen für die jeweilige Endpunktebene mit dem Befehl **setGroups.sh** ändern.

Beachten Sie Folgendes:

- Es besteht eine Viele-zu-viele-Beziehung zwischen Endpunkten und AIX-Gruppen:
  - Eine AIX-Gruppe kann mehreren Endpunkten zugeordnet werden.
  - Ein Endpunkt kann mehreren AIX-Gruppen zugeordnet werden.
- Nachdem sich ein Benutzer an der PowerSC-GUI angemeldet hat, wird anhand von Gruppenzuordnungen bestimmt, ob ein Benutzer Befehle für bestimmte Endpunkte ausführen oder nur den Status des Endpunkts anzeigen darf.
  - Zur Ausführung von Befehlen für einen bestimmten Endpunkt über die PowerSC-GUI muss der Benutzer einer der Gruppen, die diesem Endpunkt zugeordnet sind, zugeordnet sein.
  - Die Gruppenzugehörigkeit des Benutzers wird mit dem Satz von Gruppen verglichen, die jedem Endpunkt zugeordnet sind. Wenn die Gruppenzugehörigkeit des Benutzers Gruppen entspricht, die den einzelnen Endpunkten zugeordnet sind, darf der Benutzer Befehle wie **Profile anwenden**, **Rückgängig** und **Prüfen** für diesen Endpunkt ausführen. Wenn die Gruppenzugehörigkeit des Benutzers mit keiner der Gruppen übereinstimmt, die den einzelnen Endpunkten zugeordnet sind, kann der Benutzer nur den Status für diesen Endpunkt anzeigen.

Die folgenden Shell-Scripts sind im PowerSC-GUI-Server im Verzeichnis `/opt/powersc/uiServer/bin/` verfügbar.

Tabelle 14. Gruppen-Shell-Scripts

Shell-Script	Beschreibung
`pscuiserverctl`	Gibt eine AIX-Anmeldegruppe (UNIX) an, zu der ein Benutzer gehören muss, um sich an der PowerSC-GUI anmelden zu können. Der Benutzer muss nur Mitglied einer der Gruppen sein.
`setGroups.sh`	Gibt eine oder mehrere AIX-Gruppen an, zu denen ein Benutzer gehören muss, um Befehle für bestimmte Endpunkte ausführen zu können.

Befehle und Scripts für die Gruppeneinrichtung ausführen

Systemadministratoren müssen den Befehl **pscuiserverctl** und das Script **setGroups** ausführen, um festzulegen, welche Betriebssystemgruppen sich an der PowerSC-GUI anmelden, Administratorfunktionen ausführen und Befehle auf bestimmten Endpunkten ausführen dürfen.

1. Wechseln Sie auf dem PowerSC-GUI-Server in das Verzeichnis `/opt/powersc/uiServer/bin/`.
2. Führen Sie den folgenden Befehl aus, um die AIX-Gruppe anzugeben, zu der ein Benutzer gehören muss, um sich an der PowerSC-GUI anmelden zu können. Die angegebene Gruppe wird in die Datei `/etc/security/powersc/uiServer/uiServer.conf` geschrieben.

   ```
   pscuiserverctl set logonGroupList abp,security
   ```

   Tipp: Vor der Ausführung des Befehls können Sie den Befehl **groups** *Benutzername* verwenden, um die Gruppen anzuzeigen, in denen der Benutzer Mitglied ist.

3. Führen Sie den folgenden Befehl aus, um die UNIX-Gruppen anzugeben, die Administratorfunktionen in der PowerSC-GUI ausführen dürfen.

   ```
   pscuiserverctl set administratorGroupList unixgrpadmin1,unixgrpadmin2
   ```

4. Führen Sie das folgende Script aus, um die AIX-Gruppen anzugeben, in denen ein Benutzer Mitglied sein muss, um Befehle auf bestimmten Endpunkten ausführen zu können. Sie müssen die vollständig qualifizierten Hostnamen der Endpunkte angeben. Die angegebenen Gruppen werden in die Datei `/etc/security/powersc/uiServer/groups.txt` geschrieben.

   ```
   ./setGroups.sh Gruppenname "durch Kommas getrennte Liste mit Hostnamen von Endpunkten"
   ```

   Anmerkung: Bei der Suche nach Endpunkten wird ein begrenzter Satz von Platzhalterzeichen unterstützt. Die folgenden Spezifikationen sind beispielsweise gültig, um alle Endpunkte anzugeben, deren Name mit "Boston_" beginnt oder mit ".rs.com" endet:

   - ./setGroups.sh groupname "Boston_*"
   - ./setGroups.sh groupname "*.rs.com"

   Tipp: Der Stern (*) ist das einzige unterstützte Platzhalterzeichen für diesen Befehl. Er kann nur am Anfang oder am Ende einer Zeichenfolge verwendet werden.

PowerSC-GUI verwenden

Sie können in der PowerSC-GUI die auf Ihrem System erkannten Endpunkte anzeigen, angepasste Gruppen erstellen, angepasste Profile erstellen, angepasste Profile auf Endpunkte kopieren und Profile anwenden. Außerdem können Sie die Kommunikation zwischen den Endpunkten und dem PowerSC-GUI-Server überprüfen und die Kommunikation zwischen einem Endpunkt und dem PowerSC-GUI-Server stoppen.

Die Hauptseite der PowerSC-GUI enthält die folgenden Abschnitte:

- Ablage **Gruppen**: Listet die für Ihre Umgebung definierten Gruppen auf. Gruppen sind Sammlungen von Endpunkten, die basierend auf einer Gemeinsamkeit gruppiert werden. Die Gruppe **Alle Systeme** wird bei der Erkennung der Endpunkte in Ihrer Umgebung automatisch erstellt. Sie können angepasste Gruppen erstellen. Sie können beispielsweise eine Gruppe von Endpunkten erstellten, deren Gemeinsamkeit HIPPA ist.
- **Konformität**: Diese Seite enthält drei Abschnitte:
  - Im oberen Teilfenster werden statistische Informationen zu der Gruppe angezeigt, die Sie in der Ablage **Gruppen** ausgewählt haben. Die statistischen Informationen enthalten die Ergebnisse der letzten Konformitätsstufen, die auf die Endpunkte in der ausgewählten Gruppe angewendet wurden. Sie können für die ausgewählte Gruppe den Prozentsatz der erfolgreich und nicht erfolgreich angewendeten Systemregeln, die Gesamtanzahl der geprüften Regeln und die speziellen Regeln, die nicht eingehalten wurden, anzeigen.
  - Das mittlere Teilfenster ist eine Taskleiste, über die Aktionen auf einem oder mehreren Endpunkten ausgeführt werden können. Sie können eine Konformitätsstufe anwenden, widerrufen und überprüfen.
  - Im unteren Teilfenster wird eine Tabelle angezeigt, die alle Endpunkte oder eine Gruppe von Endpunkten enthält, die in Ihrer Umgebung verfügbar sind. Die Tabelle enthält für jeden Endpunkt die folgenden Informationen:
    - Systemname
    - Konformitätsregeltyp
    - Zeit und Datum, an dem Konformitätsstufe auf den Endpunkt angewendet wurde
    - Zeit und Datum, an dem Konformitätsstufe auf dem Endpunkt überprüft wurde
    - Konformitätsstufenstatus
    - Anzahl der Regeln auf dem Endpunkt, die nicht eingehalten wurden
    - Anzahl der Regeln auf dem Endpunkt, die laut Konformitätsstufenprüfung eingehalten wurden

- **Sicherheit**: Diese Seite enthält zwei Abschnitte:
  - Im oberen Teilfenster werden Sicherheitsinformationen zu der Gruppe, die Sie in der Ablage **Gruppen** ausgewählt haben, in Echtzeit angezeigt. Sie können für die ausgewählte Gruppe die Gesamtanzahl der RTC-Ereignisse (Real time Compliance), die Gesamtanzahl der TE-Ereignisse (Trusted Execution), den Prozentsatz der Endpunkte, die in Bezug auf die TNC-Patches auf dem neuesten Stand sind, den Prozentsatz der Endpunkte, auf denen Trusted Boot ist, die Anzahl der Endpunkte, auf denen Trusted Firewall installiert ist, und den Prozentsatz der Endpunkte, auf denen Trusted Logging installiert ist, anzeigen.
  - Im unteren Teilfenster wird eine Tabelle angezeigt, die die Systemendpunkte in der Gruppe enthält. Die Tabelle enthält für jeden Endpunkt die folgenden Informationen:
    - Name des Systemendpunkts
    - Anzeiger für Dateiintegritätsereignisse
    - RTC-Aktivierungsstatus
    - TE-Aktivierungsstatus
    - Aktualitätsstatus für TNC-Patches
- **Berichte**: Diese Seite enthält Konformitäts- und Dateiintegritätsberichte. Es sind sowohl Übersichts- als auch Detailberichte verfügbar.
- **Profileditor**. Diese Seite enthält drei Abschnitte:
  - Das obere Teilfenster enthält ein Dropdown-Menü, in dem die verfügbaren integrierten und angepassten Profile aufgelistet werden.
  - Das mittlere Teilfenster ist eine Taskleiste, über die Profile gelöscht, neue Profile erstellt und Profile auf Endpunkte, die zu einer Gruppe gehören, kopiert werden können.
  - Im unteren Teilfenster wird eine Tabelle angezeigt, die alle Regeln enthält, die im ausgewählten Profil enthalten sind. Für jede Regel werden die folgenden Informationen angezeigt:
    - Konformitätsregelname
    - Konformitätsregeltyp
    - Beschreibung der Regel

PowerSC-GUI-Sprache festlegen

Die PowerSC-GUI kann in verschiedenen Sprachen wiedergegeben werden.

Klicken Sie zum Auswählen der Sprache für die PowerSC-GUI in der Menüleiste der Hauptseite auf das Symbol **Sprache und Einstellungen**. Daraufhin wird die aktuelle Sprache, die für die Wiedergabe der Schnittstelle verwendet wird, im Menü angezeigt. Zum Ändern der Sprache klicken Sie auf das entsprechende Symbol. Wählen Sie die Sprache für Ihre Sitzung in der Liste der verfügbaren Sprachen aus.

In der PowerSC-GUI navigieren

In der PowerSC-GUI können Sie die Endpunkt- und Serverkommunikation einrichten und verwalten, Endpunkte organisieren und gruppieren, integrierte und angepasste Konformitätsstufen und -profile überwachen und anwenden, die Endpunktsicherheit überwachen und konfigurieren sowie Berichte geplant generieren und verteilen.

1. Öffnen Sie die PowerSC-GUI. Daraufhin wird die Startseite der PowerSC-GUI angezeigt.
2. Zur Verwaltung der Endpunkt- und Serverkommunikation klicken Sie in der Menüleiste der Hauptseite auf das Symbol **Sprache und Einstellungen**. Klicken Sie auf das Symbol **Endpunktverwaltung**, um die Kommunikation zwischen den Endpunkten und dem PowerSC-GUI-Server zu prüfen oder zu stoppen. Weitere Informationen finden Sie unter „Endpunkt- und Serverkommunikation verwalten” auf Seite 148.

3. Klicken Sie im Navigationsteilfenster der Seite "Konformität" oder "Sicherheit" auf die Ellipse mit den horizontalen Linien, um den Gruppeneditor zu öffnen. Mit dem Gruppeneditor können Sie angepasste Gruppen von Endpunkten erstellen. Weitere Informationen finden Sie unter „Angepasste Gruppen erstellen” auf Seite 150.
4. Klicken Sie zum Erstellen angepasster Konformitätsprofile und zum Kopieren von Profilen auf Endpunkte auf das Register **Profileditor**. Weitere Informationen finden Sie unter „Mit Konformitätsprofilen arbeiten” auf Seite 151.
5. Klicken Sie zum Überwachen und Anwenden integrierter und angepasster Konformitätsstufen und -profile auf das Register **Konformität**. Weitere Informationen finden Sie unter Konformitätsstufen und -profile anwenden.
6. Klicken Sie zum Überwachen und Konfigurieren der Endpunktsicherheit auf das Register **Sicherheit**. Weitere Informationen finden Sie unter Endpunktsicherheit überwachen.
7. Klicken Sie zum bedarfsgesteuerten oder geplanten Generieren und Verteilen von Berichten auf das Register **Berichte**. Weitere Informationen finden Sie unter Mit Berichten arbeiten.

Endpunkt- und Serverkommunikation verwalten

Auf der Seite **Endpunktverwaltung** können Sie die Kommunikation zwischen den Endpunkten und dem PowerSC-GUI-Server prüfen oder stoppen. Außerdem können Sie Keystore-Anforderungen prüfen und generieren.

Endpunkt- und Serverkommunikation verifizieren

Sie können die Kommunikation zwischen erkannten Endpunkten und dem PowerSC-GUI-Server verifizieren.

1. Klicken Sie in der Menüleiste der Hauptseite auf das Symbol **Sprache und Einstellungen**. Klicken Sie auf **Endpunktverwaltung**. Daraufhin wird die Seite "Endpunktverwaltung" geöffnet.
2. Wählen Sie in der Ablage **Gruppen** die Gruppe aus, die die Endpunkte enthält, die Sie verifizieren möchten. Die Endpunkte für diese Gruppe werden in der Endpunkttabelle aufgelistet.
3. Alle Systemendpunkte für eine ausgewählte Gruppe werden in der Konformitätstabelle angezeigt. Sie können die angezeigten Endpunkte mithilfe des Felds **Nach Text filtern** filtern. Geben Sie den Filtertext im Feld ein und drücken Sie die Eingabetaste. Daraufhin wird die Liste der Endpunkte aus der ausgewählten Gruppe dynamisch gefiltert, sodass nur die Zeilen angezeigt werden, die Ihren Text enthalten.
4. Klicken Sie zum Aktualisieren der angezeigten Statusinformationen auf **Tabelle aktualisieren**.
5. Wählen Sie das Kontrollkästchen für jeden Endpunkt aus, den Sie verifizieren möchten.
6. Klicken Sie auf das Symbol **Verifizieren**.
7. In den Spalten **Verifiziert** und **Konnektivitätsdiagnose** wird eine Bestätigungsnachricht zur gültigen Verbindung angezeigt.

Endpunkte aus der PowerSC-GUI-Überwachung entfernen

Nachdem ein Endpunkt erkannt wurde, wird er fortlaufend überwacht. Wenn der Endpunkt aus Ihrer Umgebung entfernt wird, müssen Sie ihn auch von Ihrem PowerSC-GUI-Server entfernen.

Führen Sie die folgenden Schritte aus, um Endpunkte aus der Überwachung in der PowerSC-GUI zu entfernen:

1. Klicken Sie in der Menüleiste der Hauptseite auf das Symbol **Sprache und Einstellungen**. Klicken Sie auf **Endpunktverwaltung**. Daraufhin wird die Seite "Endpunktverwaltung" geöffnet.
2. Wählen Sie in der Ablage **Gruppen** die Gruppe aus, die die Endpunkte enthält, die Sie entfernen möchten. Die Endpunkte für diese Gruppe werden in der Endpunkttabelle aufgelistet.
3. Alle Systemendpunkte für eine ausgewählte Gruppe werden in der Konformitätstabelle angezeigt. Sie können die angezeigten Endpunkte mithilfe des Felds **Nach Text filtern** filtern. Geben Sie den Filter-

text im Feld ein und drücken Sie die Eingabetaste. Daraufhin wird die Liste der Endpunkte aus der ausgewählten Gruppe dynamisch gefiltert, sodass nur die Zeilen angezeigt werden, die Ihren Text enthalten.

4. Klicken Sie zum Aktualisieren der angezeigten Statusinformationen auf **Tabelle aktualisieren**.
5. Wählen Sie das Kontrollkästchen für jeden Endpunkt aus, den Sie nicht mehr überwachen möchten.
6. Klicken Sie auf das Symbol **Löschen**.
7. In den Spalten **Zeitmarke der Verifizierung** und **Konnektivitätsdiagnose** wird eine Bestätigungsnachricht zum Löschen des Endpunkts angezeigt.

Keystore-Anforderungen verifizieren und generieren

Sie müssen für jeden Endpunkt verifizieren, dass eine Keystore-Anforderung gültig ist. Wenn die Anforderung gültig ist, können Sie einen Keystore für den Endpunkt generieren.

Wenn ein Endpunkt zum ersten Mal gestartet wird, verwendet der PowerSC-GUI-Agent die Truststore-Datei, um die Ausführungsposition des PowerSC-GUI-Servers zu bestimmen. Der PowerSC-GUI-Agent sendet dann eine Nachricht mit einer Anforderung zum Beitritt zur Liste verfügbarer überwachter Endpunkte an den PowerSC-GUI-Server.

Auf der Seite **Endpunktverwaltung Keystore-Anforderungen** können Sie verifizieren, dass eine Keystore-Anforderung gültig ist und dann einen Keystore für den Endpunkt generieren.

1. Klicken Sie in der Menüleiste der Hauptseite auf das Symbol **Sprache und Einstellungen**. Klicken Sie auf **Endpunktverwaltung**. Die Verwaltungsseite **Endpunkt - Alle Systeme** wird geöffnet.
2. In der Spalte **Systemname** wird jeder bekannte Endpunkt aufgelistet. Klicken Sie auf **Keystore-Anforderungen**, um zu prüfen, ob es anstehende Keystore-Anforderungen gibt. Die Seite **Endpunktverwaltung Keystore-Anforderungen** wird geöffnet.
3. Die Keystore-Anforderungen für alle neuen oder hinzugefügten Server werden in der Spalte **Hostname** aufgelistet. Nachdem Sie bestätigt haben, dass Sie einen Keystore für den Endpunkt generieren möchten, wählen Sie das Kontrollkästchen für den Endpunkt aus und klicken Sie auf **Verifizieren**.
4. Die Verifizierung wird von PowerVC durchgeführt. Geben Sie Ihre Benutzer-ID und Ihr Kennwort im Fenster **PowerVC-Berechtigungsnachweise erforderlich** an. Klicken Sie auf **OK**. Wenn PowerVC nicht installiert ist, überspringen Sie diesen Schritt und fahren Sie mit dem nächsten fort.

   Anmerkung: Bei der Verifizierung wird mithilfe der Openstack-APIs geprüft, ob PowerVC den neu deklarierten Endpunkt erkennt. Wenn PowerVC nicht in der Benutzerumgebung vorhanden ist oder wenn powervcKeystoneUrl nicht ordnungsgemäß (mit pscuiserverctl) konfiguriert wurde, kann PowerSC den Endpunkt nicht verifizieren.
5. Nach der Verifizierung wird eine Nachricht als Kurzinfotext in der Spalte **Hostname** angezeigt. In der Nachricht wird bestätigt, ob PowerVC den neuen Endpunkt erkennt. Basierend auf den Informationen in der Nachricht können Sie den Keystore generieren.
6. Klicken Sie zum Generieren des Keystores auf **Keystore generieren**. Die Endpunktzeile in der Tabelle blinkt, während der Keystore generiert wird. Nach Abschluss der Generierung ändert sich der Wert in der Spalte **Keystore generiert** von **nein** in **ja**.

   Anmerkung: Wenn Sie den Endpunkt nicht mit PowerVC verifiziert haben, wird eine Nachricht angezeigt, in der gefragt wird, ob die Verifizierung fortgesetzt werden soll. Klicken Sie auf **Fortfahren**, wenn Sie den Endpunkt erkennen und den Keystore generieren möchten.

   Es kann einige Minuten dauern, bis der PowerSC-Agent erkennt, dass der Keystore generiert wurde. Nachdem der Agent den Keystore installiert hat, wird der neue Endpunkt als vollständig verwalteter Endpunkt auf den Seiten **Endpunktverwaltung - Alle Systeme**, **Konformität**, **Sicherheit** und **Berichte** der PowerSC-GUI aufgelistet.

7. Wenn Sie keinen Keystore für den Endpunkt generieren möchten, können Sie die Anforderung entfernen. Wählen Sie das Kontrollkästchen für den Endpunkt, den Sie entfernen möchten, aus und klicken Sie dann auf das Symbol **Löschen**.
8. Alle Endpunkte, die auf eine Keystore-Verifizierung warten, werden in der Endpunkttabelle angezeigt. Sie können die angezeigten Endpunkte mithilfe des Felds **Nach Text filtern** filtern. Geben Sie den Filtertext in dem Feld ein und drücken Sie dann die Eingabetaste. Daraufhin wird die Liste der Endpunkte dynamisch gefiltert, sodass nur die Zeilen angezeigt werden, die Ihren Text enthalten.
9. Klicken Sie zum Aktualisieren der Informationen in der Endpunkttabelle auf **Tabelle aktualisieren**.

Endpunkte organisieren und gruppieren

Systemadministratoren können Endpunkte basierend auf einer allgemeinen Eigenschaft organisieren und gruppieren. Sie können angepasste Gruppen definieren, die einen explizit ausgewählten Satz von Endpunkten enthalten, die mit der PowerSC-GUI verwaltet werden.

Wenn Sie beispielsweise 3-4 Umgebungen haben, können Sie Gruppen erstellen, die Produktionsendpunkte, Testendpunkte und Qualitätssicherungsendpunkte enthalten.

Während der Installation wird eine Standardgruppe mit dem Namen **Alle Systeme** erstellt. Diese Gruppe enthält alle Endpunkte, die in der Umgebung erkannt werden.

Angepasste Gruppen erstellen

Sie können eine angepasste Gruppe mit einer explizit ausgewählten Aufzählungsliste von Endpunkten erstellen.

1. Wählen Sie in der Ablage **Gruppen** die Aktion **Neue Gruppe erstellen** aus. Daraufhin wird die Seite **Neue Gruppe erstellen** geöffnet. Wenn die Ablage **Gruppen** nicht erweitert wird, klicken Sie im linken Teilfenster der Hauptseite der Schnittstelle auf die Ellipse mit den horizontalen Linien.
2. Geben Sie einen eindeutigen Namen für die neue Gruppe ein und drücken Sie dann die Eingabetaste. Die neue Gruppe wird der Ablage **Gruppen** hinzugefügt.
3. Fügen Sie die Systeme hinzu, die Sie in diese Gruppe einschließen möchten. Wählen Sie im Feld **Alle Systeme** in der Liste der verfügbaren Endpunktsysteme die Systeme aus, die Sie in die Gruppe einschließen möchten. Klicken Sie auf den Rechtspfeil, um alle ausgewählten Systeme in die neue Gruppe zu verschieben. Wenn Sie Endpunktsysteme aus der Gruppe entfernen möchten, heben Sie den Endpunkt in der neuen Gruppenliste hervor und klicken Sie dann auf den Linkspfeil.
4. Nachdem Sie die Gruppenmitglieder hinzugefügt bzw. entfernt haben, speichern Sie Ihre Änderungen, indem Sie in der Menüleiste des Inhaltsteilfensters auf das Symbol **Speichern** klicken.
5. Klicken Sie auf die Ellipse mit den horizontalen Linien, um in die Ablage **Gruppen** zurückzukehren. Die neue Gruppe wird aufgelistet.

Einer vorhandenen Gruppe zugewiesene Systeme hinzufügen oder entfernen

Sie können Endpunkte, die einer vorhandenen Gruppe zugewiesen sind, hinzufügen und entfernen.

1. Klicken Sie in der Ablage **Gruppen** auf die Ellipse rechts neben der Gruppe, der Sie ein Endpunktsystem hinzufügen bzw. aus der Sie ein Endpunktsystem entfernen möchten. Wenn die Ablage **Gruppen** nicht erweitert wird, klicken Sie im linken Teilfenster der Hauptseite der Schnittstelle auf die Ellipse mit den horizontalen Linien.
2. Klicken Sie auf **Gruppe bearbeiten**.
3. Wenn Sie der Gruppe ein Endpunktsystem hinzufügen möchten, wählen Sie das System in der Liste **Alle Systeme** aus und klicken Sie dann auf den Rechtspfeil. Das System wird der Liste *Gruppenname* hinzugefügt.

4. Wenn Sie einen Endpunkt aus der Gruppe entfernen möchten, wählen Sie das System in der Liste **Gruppensysteme** aus und klicken Sie dann auf den Linkspfeil. Das System wird aus der Liste *Gruppenname* entfernt.
5. Klicken Sie auf das Symbol **Gruppenänderungen speichern**, um Ihre Änderungen zu speichern.
6. Wenn Sie ein System aus der Gruppe löschen möchten, wählen Sie das System aus und klicken Sie dann auf den Linkspfeil.
7. Wenn Sie die an der Gruppe vorgenommenen Änderungen abbrechen möchten, klicken Sie auf **Gruppenänderungen abbrechen**.
8. Klicken Sie auf die Ellipse neben **Gruppen**, um zur Ablage **Gruppen** zurückzukehren.

Gruppe löschen

Sie können Gruppen, die nicht mehr zutreffend sind, löschen.

1. Klicken Sie in der Ablage **Gruppen** auf die Ellipse rechts neben der Gruppe, die Sie löschen möchten. Wenn die Ablage **Gruppen** nicht erweitert wird, klicken Sie im Navigationsteilfenster der Hauptseite der Schnittstelle auf die Ellipse mit den horizontalen Linien.
2. Klicken Sie auf **Gruppe löschen**. Die Gruppe wird gelöscht und aus der Liste der Gruppen in der Ablage **Gruppen** entfernt.

Gruppe umbenennen

Sie können eine Gruppe von Endpunkten umbenennen.

1. Klicken Sie in der Ablage **Gruppen** auf die Ellipse rechts neben der Gruppe, die Sie umbenennen möchten. Wenn die Ablage **Gruppen** nicht erweitert wird, klicken Sie im Navigationsteilfenster der Hauptseite der Schnittstelle auf die Ellipse mit den horizontalen Linien.
2. Klicken Sie auf **Gruppe umbenennen**. Geben Sie den neuen Namen für die Gruppe im Feld **Gruppenname** an.

Gruppe klonen

Sie können eine Gruppe klonen, um ein Duplikat mit denselben Endpunkten und einem neuen Namen zu erstellen.

1. Klicken Sie in der Ablage **Gruppen** auf die Ellipse rechts neben der Gruppe, die Sie löschen möchten. Wenn die Ablage **Gruppen** nicht erweitert wird, klicken Sie im Navigationsteilfenster der Hauptseite der Schnittstelle auf die Ellipse mit den horizontalen Linien.
2. Klicken Sie auf **Gruppe klonen**. Die Gruppe wird kopiert und der Gruppe wird ein neuer Name zugewiesen.

Mit Konformitätsprofilen arbeiten

Mit dem Profileditor in der PowerSC-GUI können Sie die integrierten Konformitätsprofile anzeigen, angepasste Profile erstellen und Profile auf Systemendpunkte kopieren.

Das Produkt PowerSC Standard Edition wird mit einem Satz integrierter Profile geliefert, mit denen Sie Ihre Systemendpunkte so konfigurieren können, dass jeder Endpunkt die folgenden Sicherheitsstandards erfüllt:

- Payment Card Industry - Data Security Standard (PCI)
- Sarbanes-Oxley Act and COBIT (SOX-COBIT)
- US Department of Defense STIG (DoD)
- Health Insurance Portability and Accountability Act (HIPAA)
- North American Electric Reliability Corporation (NERC)

Weitere Informationen zu den integrierten Profilen finden Sie im Abschnitt „Security and Compliance Automation-Konzepte” auf Seite 9.

Jedes der integrierten Profile enthält Regeln, die auf einen Endpunkt angewendet werden müssen, um die Sicherheitsanforderungen zu erfüllen. Wenn Sie nur einen Teil oder eine andere Kombination dieser Regeln anwenden oder Konformitätsstufen anpassen müssen, können Sie ein angepasstes Profil erstellen.

In den meisten Umgebungen bearbeiten Administratoren die Konformitätsdateien häufig, um problematische Regeln zu entfernen. Nach Abschluss der Kompatibilitätsprüfungen werden die Konformitätsregeldateien als stabil eingestuft und auf den Produktionsservern implementiert.

Sie können in der PowerSC-GUI angepasste Profile erstellen, indem Sie Regeln aus integrierten (oder anderen angepassten) Profilen kombinieren.

Konformitätsprofile anzeigen

Sie können die in jedem der integrierten und angepassten Profile enthaltenen Regeln anzeigen.

1. Wählen Sie auf der Hauptseite das Register **Profileditor** aus. Daraufhin wird die Seite **Profileditor** geöffnet.
2. Klicken Sie auf den Abwärtspfeil, um die Liste der Profile zu öffnen. Im Dropdown-Menü werden die verfügbaren **integrierten Profile** und **angepassten Profile** aufgelistet.
3. Wählen Sie das anzuzeigende Profil aus. Jede im Profil enthaltene Regel wird mit Namen, Typ und Beschreibung angezeigt. Weitere Informationen zu den Regeln finden Sie im Abschnitt „Security and Compliance Automation-Konzepte" auf Seite 9.
4. Alle Regeln für das ausgewählte Profil werden in der Profiltabelle angezeigt. Sie können die angezeigten Profile mithilfe des Felds **Nach Text filtern** filtern. Geben Sie den Filtertext im Textfeld ein. Daraufhin wird die Liste der Regeln im ausgewählten Profil aktualisiert.

Angepasstes Profil erstellen

Sie können ein neues Profil erstellen, das auf einem vorhandenen Profil basiert, und dieses neue Profil dann so anpassen, dass es nur einen bestimmten Satz von Regeln enthält.

1. Wählen Sie auf der Hauptseite das Register **Profileditor** aus. Daraufhin wird die Seite **Profileditor** geöffnet.
2. Klicken Sie auf den Abwärtspfeil, um die Liste der Profile zu öffnen. Im Dropdown-Menü werden die verfügbaren **integrierten Profile** und **angepassten Profile** aufgelistet.
3. Wählen Sie das Profil aus, das Sie als Basis für Ihr neues Profil verwenden möchten.
4. Klicken Sie auf das Symbol **Neues Profil erstellen**. Daraufhin erscheint das Fenster "Name und Typ des neuen Profils".
5. Geben Sie den Namen für Ihr neues Profil im Feld **Profilname** ein.
6. Geben Sie den Typ im Feld **Profiltyp** ein. Der Typ, den Sie eingeben, gibt gewöhnlich den Typ der integrierten Richtlinie, auf dem das neue Profil basiert, und eine eindeutige ID an, z. B. PCIxx, SOX-COBITxy, DoDxyz, HIPAAwxyz oder NERCabc.
7. Klicken Sie auf **Bestätigen**.
8. Wenn Sie dem angepassten Profil eine Regel hinzufügen möchten, wählen Sie die Regel aus dem ursprünglichen Profil aus, das Sie als Basis für das angepasste Profil verwenden, und klicken Sie dann auf den Rechtspfeil. Die Regel wird dem neuen angepassten Profil hinzugefügt. Wiederholen Sie diese Schritte für jede Regel, die Sie einschließen möchten.
9. Wenn Sie eine Regel aus dem angepassten Profil entfernen möchten, wählen Sie die Regel im angepassten Profil aus und klicken Sie dann auf den Linkspfeil. Die Regel wird aus dem neuen angepassten Profil entfernt. Wiederholen Sie diese Schritte für jede Regel, die Sie entfernen möchten.
10. Klicken Sie auf **Speichern**, nachdem Sie alle gewünschten Regeln hinzugefügt haben.

Profile auf Gruppenmitglieder kopieren

Sie können angepasste Profile auf eine Gruppe von Endpunkten kopieren. Nachdem das angepasste Profil auf den Endpunkt kopiert wurde, kann es auf den Endpunkt angewendet werden. Es kann auch geprüft werden, ob es fehlerfrei auf den Endpunkt angewendet werden kann.

1. Wählen Sie auf der Hauptseite das Register **Profileditor** aus. Daraufhin wird die Seite **Profileditor** geöffnet.
2. Klicken Sie auf den Abwärtspfeil, um die Liste der Profile zu öffnen. Im Dropdown-Menü werden die verfügbaren **integrierten Profile** und **angepassten Profile** aufgelistet.
3. Wählen Sie das Profil aus, das Sie auf die Mitglieder einer Gruppe kopieren möchten.
4. Klicken Sie auf das Symbol **Profil auf Gruppenmitglieder kopieren**. Das Fenster *Profilname* **auf Mitglieder der folgenden Gruppe kopieren** wird geöffnet.
5. Jede Gruppe, die Sie für Ihre Organisation erstellt haben, wird mit einem zugehörigen Kontrollkästchen aufgelistet. Wählen Sie das Kontrollkästchen für jede Gruppe aus, in die Sie das ausgewählte Profil kopieren möchten.
6. Klicken Sie auf **Kopieren**.
7. Wenn Sie das Profil anwenden oder überprüfen möchten, kehren Sie auf die Seite **Konformität** zurück, indem Sie das Register **Konformität** auswählen.

Angepasstes Profil löschen

Sie können angepasste Profile löschen

1. Wählen Sie auf der Hauptseite das Register **Profileditor** aus. Daraufhin wird die Seite **Profileditor** geöffnet.
2. Klicken Sie auf den Abwärtspfeil, um die Liste der Profile zu öffnen. Im Dropdown-Menü werden die verfügbaren **integrierten Profile** und **angepassten Profile** aufgelistet.
3. Erweitern Sie die Liste **Angepasste Profile**.
4. Wählen Sie das zu löschende Profil aus.
5. Klicken Sie auf das Symbol **Profil löschen**. Daraufhin wird das ausgewählte angepasste Profil gelöscht.

Konformitätsstufen und -profile verwalten

Systemadministratoren können integrierte und angepasste Konformitätsstufen und -profile auf mehreren Endpunkten anwenden, überprüfen und widerrufen.

In der folgenden Tabelle sind die vordefinierten Profile und Konformitätsstufen aufgelistet, die von PowerSC Standard Edition unterstützt werden.

Tabelle 15. Von PowerSC Standard Edition unterstützte vordefinierte Profile und Konformitätsstufen

Profile	Stufen
Database	niedrig
DoD	mittel
DoD_to_AIXDefault	hoch
DoDv2	Standard
DoDv2_to_AIXDefault	
HIPAA	
NERC	
NERC_to_AIXDefault	
NERCv5	
NERCv5_to_AIXDefault	
PCI	

Tabelle 15. Von PowerSC Standard Edition unterstützte vordefinierte Profile und Konformitätsstufen (Forts.)

Profile	Stufen
PCI_to_AIXDefault	
PCIv3	
PCIv3_to_AIXDefault	
SOX-COBIT	

Auf der Seite **Konformität** in der PowerSC-GUI können Sie die folgenden Aufgaben ausführen:

- Vordefiniertes Profil oder vordefinierte Stufe auswählen und auf einen oder mehrere Endpunkte anwenden
- Widerrufsoperation auf einem oder mehreren Endpunkten auslösen
- Definiertes Profil oder definierte Stufe mit dem aktuellen Status eines oder mehrerer Endpunkte vergleichen. Die Prüfoperation zieht keine Änderungen am Endpunkt nach sich, setzt aber die **Zeitmarke der Prüfung**, um anzuzeigen, wann die letzte Prüfung durchgeführt wurde.

Konformitätsstufen und -profile anwenden

Sie können eine Konformitätsstufe oder ein Konformitätsprofil auf einen oder mehrere Endpunkte in einer ausgewählten Gruppe anwenden.

1. Wählen Sie auf der Hauptseite das Register **Konformität** aus. Daraufhin wird die Seite **Konformität** geöffnet.
2. Wählen Sie in der Ablage **Gruppen** die Gruppe aus, die die Endpunkte enthält, auf die Sie Konformitätsstufen und -profile anwenden möchten.
3. Alle Systemendpunkte für eine ausgewählte Gruppe werden in der Konformitätstabelle angezeigt. Sie können die angezeigten Endpunkte mithilfe des Textfelds **Nach Text filtern** filtern. Geben Sie den Filtertext im Textfeld ein und drücken Sie die Eingabetaste. Daraufhin wird die Liste der Endpunkte aus der ausgewählten Gruppe dynamisch gefiltert, sodass nur die Zeilen angezeigt werden, die Ihren Text enthalten.
4. Klicken Sie zum Aktualisieren der angezeigten Statusinformationen auf **Tabelle aktualisieren**. Klicken Sie auf **Aktualisierungsintervall**, um festzulegen, wie oft die Anzeige automatisch aktualisiert wird.
5. In der Spalte **Konformitätsregeltyp** können Sie die Stufen und Profile sehen, de auf den zugeordneten Endpunkt kopiert wurden. Wählen Sie die Stufe oder das Profil aus, die bzw. das Sie auf den Endpunkt anwenden möchten. Wählen Sie das zugehörige Kontrollkästchen aus.
6. Wiederholen Sie den Schritt 5 für jeden Endpunkt in der Gruppe, auf den Sie Konformitätsstufen und -profile anwenden möchten.
7. Klicken Sie auf das Symbol **Profile anwenden**.
8. Die ausgewählten Konformitätsstufen und -profile werden auf jeden der ausgewählten Endpunkte angewendet. Wenn Regeln nicht angewendet werden können, wird angenommen, dass sie fehlgeschlagen sind. Wenn eine oder mehrere Regeln fehlschlagen, wird der Endpunkt mit einem roten Balken markiert und der Text **Fehlgeschlagen** wird in der Spalte **Anzahl nicht eingehaltener Regeln** angezeigt.
9. In der Spalte **Anzahl nicht eingehaltener Regeln** für jeden markierten Endpunkt sehen Sie, warum die Regel nicht eingehalten wurde (fehlgeschlagen ist). Sie können die angewendeten Regeln anpassen, indem Sie ein eingepasstes Profil erstellen oder ein angepasstes Profil bearbeiten.

Konformitätsstufen widerrufen

Sie können die zuletzt angewendete Konformitätsstufe bzw. das zuletzt angewendete Konformitätsprofil, die bzw. das auf einen oder mehrere Endpunkte in einer ausgewählten Gruppe angewendet wurde, widerrufen.

Führen Sie die folgenden Schritte aus, um Konformitätsstufen zu widerrufen:

1. Wählen Sie auf der Hauptseite das Register **Konformität** aus. Daraufhin wird die Seite **Konformität** geöffnet.
2. Wählen Sie in der Ablage **Gruppen** die Gruppe aus, die die Endpunkte enthält, für die Sie Konformitätsstufen und -profile widerrufen möchten.
3. Alle Endpunkte für eine ausgewählte Gruppe werden in der Konformitätstabelle angezeigt. Sie können die angezeigten Endpunkte mithilfe des Textfelds **Nach Text filtern** filtern. Geben Sie den Filtertext im Textfeld ein und drücken Sie die Eingabetaste. Daraufhin wird die Liste der Endpunkte aus der ausgewählten Gruppe dynamisch gefiltert, sodass nur die Zeilen angezeigt werden, die Ihren Text enthalten.
4. Klicken Sie zum Aktualisieren der angezeigten Statusinformationen auf **Tabelle aktualisieren**. Klicken Sie auf **Aktualisierungsintervall**, um festzulegen, wie oft die Anzeige automatisch aktualisiert wird.
5. Gehen Sie wie folgt vor, um eine Stufe oder ein Profil, die bzw. das auf einen Endpunkt angewendet wurde, zu widerrufen:
   a. Wählen Sie das zugehörige Kontrollkästchen für den Endpunkt aus.
   b. Klicken Sie auf das Symbol **Rückgängig**.

Zuletzt angewendete Konformitätsstufe und zuletzt angewendetes Konformitätsprofil überprüfen

Sie können die zuletzt angewendete Konformitätsstufe bzw. das zuletzt angewendete Konformitätsprofil, die bzw. das auf einen oder mehrere Endpunkte in einer ausgewählten Gruppe angewendet wurde, überprüfen.

1. Wählen Sie auf der Hauptseite das Register **Konformität** aus. Daraufhin wird die Seite **Konformität** geöffnet.
2. Wählen Sie in der Ablage **Gruppen** die Gruppe aus, die die Endpunkte enthält, für die Sie Konformitätsstufen und -profile überprüfen möchten.
3. Alle Endpunkte für eine ausgewählte Gruppe werden in der Konformitätstabelle angezeigt. Sie können die angezeigten Endpunkte mithilfe des Textfelds **Nach Text filtern** filtern. Geben Sie den Filtertext im Textfeld ein und drücken Sie die Eingabetaste. Daraufhin wird die Liste der Endpunkte aus der ausgewählten Gruppe dynamisch gefiltert, sodass nur die Zeilen angezeigt werden, die Ihren Text enthalten.
4. Klicken Sie zum Aktualisieren der angezeigten Statusinformationen auf **Tabelle aktualisieren**. Klicken Sie auf **Aktualisierungsintervall**, um festzulegen, wie oft die Anzeige automatisch aktualisiert wird.
5. Wählen Sie das zugehörige Kontrollkästchen für den Namen des Endpunktsystems aus, für das Sie die zuletzt angewendete Stufe bzw. das zuletzt angewendete Profil überprüfen möchten.
6. Wiederholen Sie den Schritt 5 auf Seite 154 für jeden Endpunkt in der Gruppe, für den Sie die Konformitätsstufen und -profile überprüfen möchten.
7. Klicken Sie auf das Symbol **Prüfen**.
8. Der Endpunkt wird überprüft, um festzustellen, ob die Regeln in der Konformitätsstufe bzw. im Konformitätsprofil angewendet werden können. Die Endpunkte werden nicht aktualisiert. Wenn Regeln nicht angewendet werden können, werden sie bei Anwendung als fehlgeschlagen (nicht eingehalten) eingestuft. Wenn eine oder mehrere Regeln fehlschlagen, wird der Endpunkt mit einem roten Balken markiert und der Text **Fehlgeschlagen** wird in der Spalte **Anzahl nicht eingehaltener Regeln** angezeigt.
9. In der Spalte **Anzahl nicht eingehaltener Regeln** für jeden markierten Endpunkt sehen Sie, warum die Regel nicht eingehalten wurde (fehlgeschlagen ist). Sie können die angewendeten Regeln anpassen, indem Sie ein eingepasstes Profil erstellen.

Nicht angewendete Konformitätsstufe oder nicht angewendetes Konformitätsprofil überprüfen

Sie können eine Konformitätsstufe bzw. Konformitätsprofil, die bzw. das nicht auf einen oder mehrere Endpunkte in einer ausgewählten Gruppe angewendet wurde, überprüfen.

1. Wählen Sie auf der Hauptseite das Register **Konformität** aus. Daraufhin wird die Seite **Konformität** geöffnet.
2. Wählen Sie in der Ablage **Gruppen** die Gruppe aus, die die Endpunkte enthält, für die Sie die Auswirkungen einer Konformitätsstufe und eines Konformitätsprofils überprüfen möchten.
3. Alle Endpunkte für eine ausgewählte Gruppe werden in der Konformitätstabelle angezeigt. Sie können die angezeigten Endpunkte mithilfe des Textfelds **Nach Text filtern** filtern. Geben Sie den Filtertext im Textfeld ein und drücken Sie die Eingabetaste. Daraufhin wird die Liste der Endpunkte aus der ausgewählten Gruppe dynamisch gefiltert, sodass nur die Zeilen angezeigt werden, die Ihren Text enthalten.
4. Klicken Sie zum Aktualisieren der angezeigten Statusinformationen auf **Tabelle aktualisieren**. Klicken Sie auf **Aktualisierungsintervall**, um festzulegen, wie oft die Anzeige automatisch aktualisiert wird.
5. Wählen Sie das zugehörige Kontrollkästchen für den Namen des Endpunktsystems aus, für das Sie die zuletzt angewendete Stufe bzw. das zuletzt angewendete Profil überprüfen möchten. Sie können mehrere Endpunkte auswählen.
6. Öffnen Sie die Dropdown-Liste **Letzter geprüfter Typ**. Wählen Sie eine der folgenden Optionen aus:
   - **Alle verfügbaren Stufen**: Zeigt eine Liste aller verfügbaren Stufen an, die Sie für einen Endpunkt überprüfen können.
   - **Alle verfügbaren Profile**: Zeigt eine Liste aller verfügbaren Profile an, die Sie für einen Endpunkt überprüfen können.
7. Wählen Sie die Stufe bzw. das Profil aus, das Sie für einen Endpunkt überprüfen möchten.
8. Klicken Sie auf das Symbol **Prüfen**. Die Ergebnisse der Prüfung werden zurückgegeben und unter dem Endpunkt aufgelistet.

E-Mail-Benachrichtigung beim Eintreten eines Konformitätsereignisses senden

Über die Seite "Konformität" können Sie eine E-Mail-Benachrichtigung an einen oder mehrere Empfänger senden, wenn ein Konformitätsereignis eintritt.

1. Wählen Sie auf der Hauptseite das Register **Konformität** aus. Daraufhin wird die Seite **Konformität** geöffnet.
2. Klicken Sie oben rechts in der Menüleiste auf das Symbol **E-Mail-Einstellungen**. Daraufhin wird das Fenster **E-Mail-Einstellungen** geöffnet.
3. Wählen Sie das Kontrollkästchen **E-Mails an mich senden** aus.
4. Geben Sie die E-Mail-Adressen der gewünschten Empfänger in Form einer durch Kommas getrennten Liste im Feld **Adressen (durch Kommas getrennt)** ein.

Endpunktsicherheit überwachen

Über die Seite **Sicherheit** können Sie die Endpunktsicherheit in Echtzeit überwachen.

Auf der Seite "Sicherheit" wird der Status der Endpunkte angezeigt, die von Real Time Compliance (RTC) und Trusted Execution (TE) überwacht werden.

RTC, eine Unterkomponente von PowerSC, und TE, eine Komponente von AIX, stellen File Integrity Monitoring (FIM) dar. FIM überwacht wichtige Dateien auf Änderungen hin, um sicherzustellen, dass Ereignisse, die sich auf die Dateien auswirken, autorisiert sind. Zu den Ereignissen, die sich auf die Sicherheit auswirken, gehören unerwartete Änderungen an den Dateiberechtigungen, die Aktualisierung von Dateiinhalten und Installationen ungeplanter Anwendungen. Sie müssen diese Ereignisse erkennen, um wichtige Dateien und Anwendungen zu schützen.

Bei der Seite **Sicherheit** handelt es sich um eine Seite für Echtzeitüberwachung der PowerSC-GUI. Auf dieser Seite werden Ereignisse angezeigt, die generiert werden, wenn sich Dateien, die von RTC oder TE

überwacht werden, ändern. Die Ereignisse enthalten Details zum Zeitpunkt der am Dateiinhalt vorgenommenen Änderungen, zum Zeitpunkt des Zugriffs auf den Endpunkt oder zum Zeitpunkt der Konfigurationsänderung.

Sie können auf der Seite **Sicherheit** die folgenden Aufgaben ausführen:

- Echtzeitüberwachungsdaten von RTC und TE anzeigen
- RTC und TE für alle Endpunkte konfigurieren
- Status anderer PowerSC-Produkte auf Endpunkten anzeigen
- TE ein- und ausschalten

Real Time Compliance (RTC) konfigurieren

Auf der Seite **Sicherheit** können Sie das Produkt Real Time Compliance (RTC) für einen bestimmten Endpunkt oder eine Gruppe von Endpunkten konfigurieren.

1. Klicken Sie auf die Ellipse rechts von dem Endpunkt, für den Sie die RTC-Konfiguration bearbeiten möchten.
2. Klicken Sie auf **RTC konfigurieren**. Daraufhin wird das Fenster "RTC-Richtlinienkonfiguration" geöffnet.
3. Alle verfügbaren RTC-Konfigurationsoptionen werden mit einer Erläuterung aufgelistet. Zum Ändern einer oder mehrerer RTC-Konfigurationsoptionen wählen Sie das entsprechende Kontrollkästchen links von der jeweiligen Option aus bzw. ab. In manchen Fällen werden die geänderten Optionen erst nach einem Neustart des Servers wirksam.
4. Klicken Sie auf **Speichern**.

Frühere Version von RTC-Konfigurationsoptionen wiederherstellen

Sie können eine frühere Version von RTC-Konfigurationsoptionen (Real Time Compliane), d. h. RTC-Konfigurationsoptionen, die zu einem früheren Datum und Zeitpunkt gültig waren, wiederherstellen.

1. Klicken Sie auf die Ellipse rechts von dem Endpunkt, für den Sie ein Rollback der RTC-Konfigurationsoptionen auf eine frühere Version durchführen möchten.
2. Klicken Sie auf **RTC-Rollback durchführen**. Die Zeitmarken für jede Konfigurationsversion von RTC werden aufgelistet.
3. Klicken Sie auf die Zeitmarke für die Konfigurationsversion, auf die Sie den Endpunkt zurücksetzen möchten. Daraufhin werden die RTC-Konfigurationsoptionen, die an diesem Datum und zu diesem Zeitpunkt gültig waren, wiederhergestellt.

Konfigurationsoptionen für Real Time Compliance (RTC) in andere Gruppen kopieren

Sie können die Konfigurationsoptionen für Real Time Compliance (RTC) in eine andere Gruppe von Endpunkten oder in einen bestimmten Satz von Endpunkten kopieren.

1. Klicken Sie auf die Ellipse rechts von dem Endpunkt, dessen Konfigurationsoptionen Sie in eine andere Gruppe von Endpunkten oder in einen bestimmten Satz von Endpunkten kopieren möchten.
2. Klicken Sie auf **RTC-Konfiguration kopieren**. Jede Gruppe von Endpunkten, einschließlich der Gruppe **Alle Systeme**, werden aufgelistet.
3. Wählen Sie die Endpunktgruppe bzw. die speziellen Endpunkte auf eine der folgenden Arten aus:
   - Wählen Sie das Kontrollkästchen für die Gruppe von Endpunkten in der Liste verfügbarer Gruppen aus. Die Konfigurationsoptionen werden auf jeden Endpunkt in der Gruppe kopiert.
   - Verwenden Sie den Rechtspfeil, um eine Gruppe zu erweitern, damit eine Liste aller Endpunkte in der Gruppe angezeigt wird. Wählen Sie das Kontrollkästchen jedes Endpunkts der Gruppe aus, auf den Sie die Konfigurationsoptionen kopieren möchten.
   - Erweitern Sie die Liste der Endpunkte in der Gruppe **Alle Systeme**. Wählen Sie das Kontrollkästchen jedes Endpunkts der Gruppe aus, auf den Sie die Konfigurationsoptionen kopieren möchten.

4. Klicken Sie auf **OK**. Daraufhin werden die Konfigurationsoptionen in die ausgewählte Gruppe bzw. auf die ausgewählten Endpunkte kopiert.

RTC-Dateiliste bearbeiten

Sie können die Überwachungsoptionen von Real Time Compliance (RTC) für jede Datei auf einem Endpunkt anzeigen und bearbeiten.

1. Klicken Sie auf die Ellipse rechts von dem Endpunkt, der die Dateien hostet, deren RTC-Überwachungsoptionen Sie anzeigen oder bearbeiten möchten.
2. Klicken Sie auf **RTC-Dateiliste bearbeiten**. Daraufhin wird die Seite **Konfiguration der RTC-Dateiliste** geöffnet, auf der alle Verzeichnisse und Dateien aufgelistet werden, die sich auf dem Endpunkt befinden. Ein Häkchen im Symbol für den jeweiligen Verzeichnisordner zeigt an, dass mindestens eine Datei in diesem Verzeichnis überwacht wird.
3. Wenn die Datei, deren Optionen Sie bearbeiten möchten, in einem Verzeichnis enthalten ist, klicken Sie doppelt auf das Verzeichnis, um die Dateien aufzulisten. Daraufhin werden alle Dateien in dem Verzeichnis aufgelistet.
4. Die Überwachungsoptionen für jede Datei auf dem Endpunkt werden in den Spalten **Inhalt** und **Attribute** aufgelistet. Wenn die Datei auf Inhaltsänderungen hin überwacht wird, ist das Kontrollkästchen in der Spalte **Inhalt** ausgewählt. Wenn die Datei auf Attributänderungen hin überwacht wird, ist das Kontrollkästchen in der Spalte **Attribute** ausgewählt. Zum Bearbeiten der Überwachungsoptionen wählen Sie die Kontrollkästchen für die gewünschten Dateien auf dem Endpunkt aus bzw. ab.
5. Klicken Sie auf **Speichern**.

Frühere Konfiguration der Überwachungsoptionen von Real Time Compliance (RTC) wiederherstellen

Sie können ein Rollback auf eine frühere Version der Dateien, die von RTC überwacht werden, durchführen.

1. Klicken Sie auf die Ellipse rechts von dem Endpunkt, für den Sie ein Rollback der RTC-Überwachungsoptionen auf eine frühere Version durchführen möchten.
2. Klicken Sie auf **Rollback der RTC-Dateiliste durchführen**. Daraufhin werden die Zeitmarken für jede Konfigurationsversion der überwachten Dateien aufgelistet.
3. Klicken Sie auf die Zeitmarke für die Konfigurationsversion der Überwachungsoptionen, auf die Sie den Endpunkt zurücksetzen möchten. Daraufhin werden die Konfigurationsoptionen, die an diesem Datum und zu diesem Zeitpunkt gültig waren, wiederhergestellt.

Überwachungsoptionen für Real Time Compliance-Dateilisten (RTC) in andere Gruppen kopieren

Sie können die Überwachungsoptionen von Real Time Compliance (RTC) in eine andere Gruppe von Endpunkten oder in einen bestimmten Satz von Endpunkten kopieren.

1. Klicken Sie auf die Ellipse rechts von dem Endpunkt, dessen Überwachungsoptionen Sie in eine andere Gruppe von Endpunkten oder in einen bestimmten Satz von Endpunkten kopieren möchten.
2. Klicken Sie auf **RTC-Dateiliste kopieren**. Jede Gruppe von Endpunkten, einschließlich der Gruppe **Alle Systeme**, werden aufgelistet.
3. Wählen Sie die Endpunktgruppe bzw. die speziellen Endpunkte auf eine der folgenden Arten aus:
   - Wählen Sie das Kontrollkästchen für die Gruppe von Endpunkten in der Liste verfügbarer Gruppen aus. Die Überwachungsoptionen werden auf jeden Endpunkt in der Gruppe kopiert.
   - Verwenden Sie den Rechtspfeil, um eine Gruppe zu erweitern, damit eine Liste aller Endpunkte in der Gruppe angezeigt wird. Wählen Sie das Kontrollkästchen jedes Endpunkts der Gruppe aus, auf den Sie die Überwachungsoptionen kopieren möchten.
   - Erweitern Sie die Liste der Endpunkte in der Gruppe **Alle Systeme**. Wählen Sie das Kontrollkästchen jedes Endpunkts der Gruppe aus, auf den Sie die Konfigurationsoptionen kopieren möchten.

4. Klicken Sie auf **OK**. Daraufhin werden die Überwachungsoptionen in die ausgewählte Gruppe bzw. auf die ausgewählten Endpunkte kopiert.

RTC-Prüfung (Real Time Compliance) durchführen

Über die Seite "Sicherheit" können Sie eine RTC-Prüfung (Real Time Compliance) durchführen, um sich zu vergewissern, ob ein Endpunkt noch konform ist.

1. Klicken Sie auf die Ellipse rechts von dem Endpunkt, für den Sie eine RTC-Prüfung (Real Time Compliance) durchführen möchten.
2. Klicken Sie auf **Konformitätsprüfung durchführen**. Daraufhin wird die Seite **Konformität** geöffnet, auf der die Zeile für den jeweiligen Endpunkt blinkend angezeigt wird, um darauf hinzuweisen, dass die Prüfung momentan durchgeführt wird.
3. Sollten Regeln nicht angewendet werden können, erscheint eine Fehlernachricht in der Spalte **Anzahl nicht eingehaltener Regeln**. Verwenden Sie den Abwärtspfeil links neben dem Endpunkt, um die Regel anzuzeigen, für die die Prüfung fehlgeschlagen ist.

Trusted Execution (TE) konfigurieren

Auf der Seite **Sicherheit** können Sie das Produkt Trusted Execution (TE) für einen bestimmten Endpunkt oder eine Gruppe von Endpunkten konfigurieren.

1. Klicken Sie auf die Ellipse rechts von dem Endpunkt, für den Sie die TE-Konfigurationsoptionen bearbeiten möchten.
2. Klicken Sie auf **TE konfigurieren**. Daraufhin wird das Fenster "TE-Richtlinienkonfiguration" geöffnet.
3. Alle TE-Konfigurationsoptionen werden mit einer Erläuterung aufgelistet. Zum Ändern einer oder mehrerer TE-Konfigurationsoptionen wählen Sie das entsprechende Kontrollkästchen aus bzw. ab. In manchen Fällen werden die geänderten Optionen erst nach einem Neustart des Servers wirksam.
4. Klicken Sie auf **Speichern**.

Konfigurationsoptionen für Trusted Execution (TE) in andere Gruppen kopieren

Sie können die Konfigurationsoptionen für Trusted Execution (TE) in eine andere Gruppe von Endpunkten oder in einen bestimmten Satz von Endpunkten kopieren.

1. Klicken Sie auf die Ellipse rechts von dem Endpunkt, dessen Konfigurationsoptionen Sie in eine andere Gruppe von Endpunkten oder in einen bestimmten Satz von Endpunkten kopieren möchten.
2. Klicken Sie auf **TE-Konfiguration kopieren**. Jede Gruppe von Endpunkten, einschließlich der Gruppe **Alle Systeme**, werden aufgelistet.
3. Wählen Sie die Endpunktgruppe bzw. die speziellen Endpunkte auf eine der folgenden Arten aus:
   - Wählen Sie das Kontrollkästchen für die Gruppe von Endpunkten in der Liste verfügbarer Gruppen aus. Die Konfigurationsoptionen werden auf jeden Endpunkt in der Gruppe kopiert.
   - Erweitern Sie eine Gruppe, damit eine Liste aller Endpunkte in der Gruppe angezeigt wird. Wählen Sie das Kontrollkästchen jedes Endpunkts der Gruppe aus, auf den Sie die Konfigurationsoptionen kopieren möchten.
   - Erweitern Sie die Liste der Endpunkte in der Gruppe **Alle Systeme**. Wählen Sie das Kontrollkästchen jedes Endpunkts der Gruppe aus, auf den Sie die Konfigurationsoptionen kopieren möchten.
4. Klicken Sie auf **OK**. Daraufhin werden die Konfigurationsoptionen in die ausgewählte Gruppe bzw. auf die ausgewählten Endpunkte kopiert.

Trusted Execution-Dateiliste bearbeiten

Sie können die Überwachungsoptionen von Trusted Execution (TE) für jede Datei auf einem Endpunkt anzeigen und bearbeiten.

1. Klicken Sie auf die Ellipse rechts von dem Endpunkt, der die Dateien hostet, deren TE-Überwachungsoptionen Sie anzeigen oder bearbeiten möchten.

2. Klicken Sie auf **TE-Dateiliste bearbeiten**. Daraufhin wird die Seite **Konfiguration der TE-Dateiliste** geöffnet, auf der alle Verzeichnisse und Dateien aufgelistet werden, die sich auf dem Endpunkt befinden. Ein Häkchen im Symbol für den jeweiligen Verzeichnisordner zeigt an, dass mindestens eine Datei in diesem Verzeichnis überwacht wird.
3. Wenn die Datei, deren Optionen Sie anzeigen oder bearbeiten möchten, in einem Verzeichnis enthalten ist, klicken Sie doppelt auf das Verzeichnis, um die Dateien aufzulisten. Daraufhin werden alle Dateien in dem Verzeichnis aufgelistet.
4. Die Überwachungsoptionen für jede Datei auf dem Endpunkt werden in den Spalten **TE** und **Flüchtig** aufgelistet. Das Kontrollkästchen in der Spalte **TE** ist ausgewählt, wenn die Datei auf Inhaltsänderungen hin überwacht wird. Das Kontrollkästchen in der Spalte **Flüchtig** ist ausgewählt, wenn die Datei nur auf Berechtigungsänderungen hin überwacht wird. Zum Ändern der Überwachungsoptionen wählen Sie die Kontrollkästchen für die gewünschten Dateien auf dem Endpunkt aus bzw. ab.
5. Klicken Sie auf **Speichern**.

Überwachungsoptionen für Trusted Execution-Dateilisten in andere Gruppen kopieren

Sie können die Überwachungsoptionen von Trusted Execution (TE) in eine andere Gruppe von Endpunkten oder in einen bestimmten Satz von Endpunkten kopieren.

1. Klicken Sie auf die Ellipse rechts von dem Endpunkt, dessen Überwachungsoptionen Sie in eine andere Gruppe von Endpunkten oder in einen bestimmten Satz von Endpunkten kopieren möchten.
2. Klicken Sie auf **TE-Dateiliste kopieren**. Jede Gruppe von Endpunkten, einschließlich der Gruppe **Alle Systeme**, werden aufgelistet.
3. Wählen Sie die Endpunktgruppe bzw. die speziellen Endpunkte auf eine der folgenden Arten aus:
   - Wählen Sie das Kontrollkästchen für die Gruppe von Endpunkten in der Liste verfügbarer Gruppen aus. Die Überwachungsoptionen werden auf jeden Endpunkt in der Gruppe kopiert.
   - Erweitern Sie eine Gruppe, damit eine Liste aller Endpunkte in der Gruppe angezeigt wird. Wählen Sie das Kontrollkästchen jedes Endpunkts der Gruppe aus, auf den Sie die Überwachungsoptionen kopieren möchten.
   - Erweitern Sie die Liste der Endpunkte in der Gruppe **Alle Systeme**. Wählen Sie das Kontrollkästchen jedes Endpunkts der Gruppe aus, auf den Sie die Konfigurationsoptionen kopieren möchten.
4. Klicken Sie auf **OK**. Daraufhin werden die Überwachungsoptionen in die ausgewählte Gruppe bzw. auf die ausgewählten Endpunkte kopiert.

Status anderer PowerSC-Features anzeigen

Auf der Seite "Sicherheit" können Sie den Status der PowerSC-Features Trusted Boot, Trusted Firewall und Trusted Logging anzeigen. Außerdem können Sie den Status von TNC-Aktualisierungen (Trusted Network Connect) auf einem Endpunkt anzeigen.

1. Wählen Sie auf der Hauptseite das Register **Sicherheit** aus. Die Seite **Sicherheit** wird geöffnet.
2. Die TNC-Komponente von PowerSC wird verwendet, um Sicherheitspatches auf jedem Endpunkt zu überprüfen und zu aktualisieren. In der Spalte **Aktuell über TNC** der Endpunkttabelle wird angezeigt, ob der Endpunkt aus der Sicht des TNC-Servers auf dem neuesten Stand ist. Im Abschnitt **Aktuell über TNC** im Dashboard-Banner wird der Prozentsatz der Endpunkte in der Gruppe angezeigt, die auf dem neuesten Stand sind. Führen Sie die folgenden Schritte aus, um die Anzeige von TNC-Aktualisierungsinformationen auf der Seite **Sicherheit** zu unterdrücken:
   a. Klicken Sie in der Menüleiste der Hauptseite auf das Symbol **Sprache und Einstellungen**.
   b. Klicken Sie auf **Unterproduktnutzung**.
   c. Setzen Sie **Aktuell über TNC** auf "Aus".
   d. Damit die Informationen wieder angezeigt werden, schieben Sie den Schalter für **Aktuell über TNC** auf "Ein".

3. In der Spalte **TB** der Endpunkttabelle wird angezeigt, ob das PowerSC-Feature Trusted Boot auf dem Endpunkt verfügbar ist. Im Abschnitt **Trusted Boot** im Dashboard-Banner wird der Prozentsatz der Endpunkte in der momentan ausgewählten Gruppe angezeigt, auf denen das PowerSC-Feature Trusted Boot aktiviert ist. Führen Sie die folgenden Schritte aus, um die Anzeige von PowerSC-Trusted-Boot-Informationen auf der Seite **Sicherheit** zu unterdrücken:
   a. Klicken Sie in der Menüleiste der Hauptseite auf das Symbol **Sprache und Einstellungen**.
   b. Klicken Sie auf **Unterproduktnutzung**.
   c. Schieben Sie den Schalter für **Trusted Boot** auf "Aus".
   d. Damit die Informationen wieder angezeigt werden, schieben Sie den Schalter auf "Ein".
4. In der Spalte **TF** der Endpunkttabelle wird angezeigt, ob das PowerSC-Feature Trusted Firewall auf dem Endpunkt verfügbar ist. Im Abschnitt **Trusted Firewall** im Dashboard-Banner wird der Prozentsatz der Endpunkte in der momentan ausgewählten Gruppe angezeigt, auf denen das PowerSC-Feature Trusted Firewall aktiviert ist. Führen Sie die folgenden Schritte aus, um die Anzeige von Trusted-Firewall-Informationen auf der Seite **Sicherheit** zu unterdrücken:
   a. Klicken Sie in der Menüleiste der Hauptseite auf das Symbol **Sprache und Einstellungen**.
   b. Klicken Sie auf **Unterproduktnutzung**.
   c. Schieben Sie den Schalter für **Trusted Firewall** auf "Aus".
   d. Damit die Informationen wieder angezeigt werden, schieben Sie den Schalter auf "Ein".
5. In der Spalte **TL** der Endpunkttabelle wird angezeigt, ob das PowerSC-Feature Trusted Logging auf dem Endpunkt verfügbar ist. Im Abschnitt **Trusted Logging** im Dashboard-Banner wird der Prozentsatz der Endpunkte in der momentan ausgewählten Gruppe angezeigt, auf denen das PowerSC-Feature Trusted Logging aktiviert ist. Führen Sie die folgenden Schritte aus, um die Anzeige von Trusted-Logging-Informationen auf der Seite **Sicherheit** zu unterdrücken:
   a. Klicken Sie in der Menüleiste der Hauptseite auf das Symbol **Sprache und Einstellungen**.
   b. Klicken Sie auf **Unterproduktnutzung**.
   c. Schieben Sie den Schalter für **Trusted Logging** auf "Aus".
   d. Damit die Informationen wieder angezeigt werden, schieben Sie den Schalter auf "Ein".

Trusted Execution-Überwachung aktivieren und inaktivieren

Sie können die TE-Überwachung (Trusted Execution) aktivieren und inaktivieren. Sie können die TE-Überwachung auch inaktivieren und planen, dass sie in einem bestimmten Zeitintervall aktiviert wird.

1. Klicken Sie auf das Symbol **Trusted Execution aktivieren und inaktivieren**.
2. Wählen Sie im Dropdown-Menü eine der folgenden Optionen aus:
   - **Für alle Endpunkte aktivieren**: Aktiviert die TE-Überwachung für jeden Endpunkt.
   - **Für alle Endpunkte inaktivieren**: Inaktiviert die TE-Überwachung für jeden Endpunkt.
3. Wenn die TE-Überwachung inaktiviert ist, sind die Optionen zum Festlegen einer Zeit für den Neustart der TE-Überwachung verfügbar. Sie können eine der folgenden Neustartzeiten auswählen:
   - **1 Stunde**
   - **5 Stunden**
   - **1 Tag**
   - **1 Woche**
   - **Nie**
4. Klicken Sie auf **Speichern**.

E-Mail-Benachrichtigung beim Eintreten eines Sicherheitsereignisses senden

Über die Seite "Sicherheit" können Sie eine E-Mail-Benachrichtigung an einen oder mehrere Empfänger senden, wenn ein Sicherheitsereignis eintritt.

1. Wählen Sie auf der Hauptseite das Register **Sicherheit** aus. Die Seite **Sicherheit** wird geöffnet.
2. Klicken Sie rechts in der Menüleiste auf das Symbol **E-Mail-Einstellungen**. Daraufhin wird das Fenster **E-Mail-Einstellungen** geöffnet.
3. Wählen Sie das Kontrollkästchen **E-Mails an mich senden** aus.
4. Geben Sie die E-Mail-Adressen der gewünschten Empfänger in Form einer durch Kommas getrennten Liste im Feld **Adressen (durch Kommas getrennt)** ein.

Mit Berichten arbeiten

Über die Seite "Berichte" in der PowerSC-GUI können Sie auf mehrere Berichte zugreifen.

Die folgenden Berichte sind verfügbar:

- Der Bericht **Konformitätsübersicht** enthält eine Momentaufnahme der allgemeinen Informationen, die auf der Seite **Konformität** der Schnittstelle angezeigt werden.
- Der Bericht **Konformitätsdetails** enthält eine Momentaufnahme der allgemeinen und Detailinformationen, die auf der Seite **Konformität** angezeigt werden.
- Der Bericht **Dateiintegritätsübersicht** enthält eine Momentaufnahme der allgemeinen Informationen, die auf der Seite **Sicherheit** angezeigt werden.
- Der Bericht **Dateiintegritätsdetails** enthält eine Momentaufnahme der allgemeinen und Detailinformationen, die auf der Seite **Sicherheit** angezeigt werden.
- **Konformität und FIM kombiniert**

Standardmäßig werden auf der Seite **Berichte** die Berichte **Konformitätsübersicht** und **Dateiintegritätsübersicht** für die Gruppe **Alle Systeme** angezeigt. Es sind keine Standardgruppen für die Berichte **Konformitätsdetails**, **Dateiintegritätsdetails** und **Konformität und FIM kombiniert** angegeben.

Sie können jeden Typ von Bericht für die Gruppe **Alle Systeme** und jede definierte Gruppe erzeugen. Sie können den Bericht für alle Endpunkte in einer Gruppe oder für einen Teil der Endpunkte in der Gruppe erzeugen. Nach der Generierung eines Berichts können Sie die bedarfsgesteuerte oder tägliche Verteilung des Berichts im HTML-Format oder als CSV-Datei an einen oder mehrere E-Mail-Empfänger planen.

Die Liste der Berichte, die auf der Seite **Berichte** angezeigt werden, variiert je nach Benutzeranmelde-ID. Sie können nur Berichte für die Endpunkte generieren, die Sie mit Ihrer Anmelde-ID verwalten. Jeder Bericht, den Sie in einer bestimmten Sitzung generieren, wird beim Öffnen der nächsten Sitzung aufgelistet.

Berichtsgruppe auswählen

Sie können jeden der Berichte für die Gruppe **Alle Systeme** und jede Gruppe, die Sie definiert haben, ausführen. Sie können einen Bericht für alle Endpunkte, die in eine Gruppe eingeschlossen wurden, oder für einen Teil der Endpunkte in der Gruppe ausführen.

1. Klicken Sie auf der Hauptseite auf das Register **Berichte**. Die Seite **Berichte** wird geöffnet.
2. Klicken Sie auf die Ellipse rechts von dem Typ von Bericht, den Sie ausführen möchten.
3. Klicken Sie auf **Gruppe ändern**.
4. Es wird ein Auswahlfeld geöffnet, in dem alle verfügbaren Gruppen aufgelistet werden. Wählen Sie das Optionsfeld neben der Gruppe aus, für die Sie den Bericht ausführen möchten. Klicken Sie auf **Bestätigen**. Der Bericht wird ausgeführt und der Inhalt des Hauptfensters wird mit den Informationen für die ausgewählte Gruppe aktualisiert.
5. Wenn Sie einen Bericht für einen Teil von Endpunkten ausführen möchten, erweitern Sie die Gruppe **Alle Systeme**. Es wird eine Liste mit allen verfügbaren Endpunkten angezeigt. Wählen Sie das Kontrollkästchen neben jedem Endpunkt aus, den Sie in den Bericht einschließen möchten. Klicken Sie auf **Bestätigen**, um den Bericht auszuführen.

Anmerkung: Wenn Sie einen Bericht für eine bestimmte Gruppe von Endpunkten ausführen möchten, können Sie eine Gruppe erstellen, die diese Endpunkte enthält. Die Erstellung der Gruppe spart Zeit und die Gruppe kann von allen Benutzern verwendet werden, weil Gruppen global sind (d. h. für alle Benutzer der Schnittstelle sichtbar sind).

6. Sie können einen bestimmten Endpunkt suchen, indem Sie den Namen des Endpunkts im Feld für den Suchbegriff eingeben. Klicken Sie auf **Bestätigen**, um den Bericht für diesen Endpunkt auszuführen.

Bericht per E-Mail verteilen

Nachdem Sie die Gruppe für einen Bericht festgelegt haben, können Sie die Verteilung des Berichts in Form einer HTML-formatierten E-Mail und einer CSV-Datei planen. Sie können planen, dass die E-Mail sofort oder täglich an einen oder mehrere E-Mail-Empfänger gesendet wird.

Der Einschluss der CSV-Version des Berichts ermöglicht den Empfängern, die Berichtsdaten in ein Spreadsheet oder in eine andere Softwareanwendung zu importieren, die CSV-Dateien verarbeiten kann. CSV-Dateien haben keine Grafik- oder Dashboardkonzepte. Eine aus einem Übersichtsbericht generierte CSV-Datei enthält in der erste Zeile die einzelnen Spaltenüberschriften in Form einer durch Kommas getrennten Liste. In den nachfolgenden Zeilen sind der Endpunkt und die Werte für die einzelnen Spalten aufgelistet.

Aus den Detailberichten werden mehrere CSV-Dateien generiert. Die erste CSV-Datei ist ähnlich formatiert wie der Übersichtsbericht. Für die einzelnen Detailebenen des Berichts wird jeweils eine separate CSV-Datei generiert. Im Bericht "Dateiintegritätsdetails" wird beispielsweise für die folgenden Detailstufen eine separate CSV-Datei generiert:

- **TE-Konfiguration**
- **RTC-Konfiguration**
- **Unterproduktstatus**

1. Klicken Sie auf der Hauptseite auf das Register **Berichte**. Die Seite **Berichte** wird geöffnet.
2. Wählen Sie in der Liste der verfügbaren Berichte den Bericht aus, den Sie verteilen möchten. Der Bericht wird ausgeführt und der Inhalt der Hauptseite wird aktualisiert.
3. Klicken Sie auf die Ellipse rechts neben dem Bericht, den Sie ausführen möchten.
4. Klicken Sie auf **E-Mail-Optionen**. Daraufhin wird das Fenster "Berichte per E-Mail senden" geöffnet.
5. Geben Sie die E-Mail-Adresse jedes Empfängers im Feld **Adressen** ein. Trennen Sie die einzelnen Empfängeradressen durch ein Semikolon (;) voneinander.
6. Geben Sie eine Beschreibung der E-Mail im Feld **Betreff** ein.
7. Wählen Sie eine der folgenden Optionen aus:
   - Wählen Sie das Kontrollkästchen **Jeden Tag um** aus, um den Bericht täglich an die Empfänger zu senden. Geben Sie die lokale Zeit für das Versenden des Berichts an, indem Sie die Zeit in Stunden und Minuten auswählen. Klicken Sie auf **Speichern und Schließen**. Der Bericht wird jeden Tag zur angegebenen Zeit versendet.
   - Klicken Sie auf **Sofort senden**, um den Bericht zu senden. Der Bericht wird gesendet und das Fenster wird geschlossen.

PowerSC Standard Edition-Befehle

PowerSC Standard Edition stellt Befehle für die Kommunikation mit der Komponente Trusted Firewall und der Komponente Trusted Network Connect über die Befehlszeile bereit.

Befehl chvfilt

Zweck

Ändert die Werte für die vorhandene VLAN-übergreifende Filterregel.

Syntax

chvfilt [**-v** <**4**|**6**>] **-n Filter-ID** [**-a** <**D**|**P**>] [**-z** <**Quellen-VLAN**>] [**-Z** <**Ziel-VLAN**>] [**-s** <**Quellenadresse**>] [**-d** <**Zieladresse**>] [**-o** <**Quellenport_Quellenoperation**>] [**-p** <**Quellenport**>] [**-O** <**Zielport_Zieloperation**>] [**-P** <**Zielport**>] [**-c** <**Protokoll**>]

Beschreibung

Der Befehl **chvfilt** wird verwendet, um die Definition einer VLAN-übergreifenden Filterregel in der Filterregeltabelle zu ändern.

Flags

-a Gibt die Aktion an. Gültige Werte:
- D (Deny): Blockiert den Datenverkehr.
- P (Permit): Lässt den Datenverkehr zu.

-c Gibt verschiedene Protokolle an, für die die Filterregel gilt. Gültige Werte:
- udp
- icmp
- icmpv6
- tcp
- any

-d Gibt die Zieladresse im IPv4- oder IPv6-Format an.

-m Gibt die Quellenadressmaske an.

-M Gibt die Zieladressmaske an.

-n Gibt die Filter-ID der zu ändernden Filterregel an.

-o Gibt den Quellenport oder die ICMP-Typoperation (Internet Control Message Protocol) an. Gültige Werte:
- lt
- gt
- eq
- any

-O Gibt den Zielport oder die ICMP-Codeoperation an. Gültige Werte:
- lt
- gt

- eq
- any

-p Gibt den Quellenport oder den ICMP-Typ an.

-P Gibt den Zielport oder den ICMP-Code an.

-s Gibt die Quellenadresse im IPv4- oder IPv6-Format an.

-v Gibt die IP-Version der Filterregeltabelle an. Die gültigen Werte sind 4 und 6.

-z Gibt die VLAN-ID der logischen Quellenpartition an.

-Z Gibt die VLAN-ID der logischen Zielpartition an.

Exitstatus

Dieser Befehl gibt die folgenden Exitwerte zurück:

0 Erfolgreiche Ausführung.

>0 Es ist ein Fehler aufgetreten.

Beispiele

1. Geben Sie den Befehl wie folgt ein, um eine gültige Filterregel im Kernel zu ändern:
   ```
   chvfilt -n 1 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```
2. Die Ausgabe ist wie folgt, wenn keine Filterregel (n=2) im Kernel vorhanden ist:
   ```
   chvfilt -n 2 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

   Das System zeigt die Ausgabe folgendermaßen an:
   ```
   ioctl(QUERY_FILTER) failed no filter rule err=2
   Die Filterregel kann nicht geändert werden.
   ```

Befehl genvfilt

Zweck

Fügt eine VLAN-übergreifende Filterregel zwischen logischen Partitionen auf demselben IBM Power Systems-Server hinzu.

Syntax

genvfilt -v <**4**|**6**> **-a** <**D**|**P**> **-z** <**Quellen-VLAN**> **-Z** <**Ziel-VLAN**> [**-s** <**Quellenadresse**>] [**-d** <**Zieladresse**>] [**-o** <**Quellenport_Operation**>] [**-p** <**Quellenport**>] [**-O** <**Zielport_Operation**>] [**-P** <**Zielport**>] [**-c** <**Protokoll**>]

Beschreibung

Der Befehl **genvfilt** fügt eine VLAN-übergreifende Filterregel zwischen logischen Partitionen (LPARs) auf demselben IBM Power Systems-Server hinzu.

Flags

-a Gibt die Aktion an. Gültige Werte:
- D (Deny): Blockiert den Datenverkehr.
- P (Permit): Lässt den Datenverkehr zu.

-c Gibt verschiedene Protokolle an, für die die Filterregel gilt. Gültige Werte:
- udp

- icmp
- icmpv6
- tcp
- any

-d Gibt die Zieladresse im IPv4- oder IPv6-Format an.

-m Gibt die Quellenadressmaske an.

-M Gibt die Zieladressmaske an.

-o Gibt den Quellenport oder die ICMP-Typoperation (Internet Control Message Protocol) an. Gültige Werte:
- lt
- gt
- eq
- any

-O Gibt den Zielport oder die ICMP-Codeoperation an. Gültige Werte:
- lt
- gt
- eq
- any

-p Gibt den Quellenport oder den ICMP-Typ an.

-P Gibt den Zielport oder den ICMP-Code an.

-s Gibt die Quellenadresse im IPv4- oder IPv6-Format an.

-v Gibt die IP-Version der Filterregeltabelle an. Die gültigen Werte sind 4 und 6.

-z Gibt die VLAN-ID der Quellen-LPAR an. Die VLAN-ID muss zwischen 1 und 4096 liegen.

-Z Gibt die VLAN-ID der Ziel-LPAR an. Die VLAN-ID muss zwischen 1 und 4096 liegen.

Exitstatus

Dieser Befehl gibt die folgenden Exitwerte zurück:

0 Erfolgreiche Ausführung.

>0 Es ist ein Fehler aufgetreten.

Beispiele

1. Geben Sie den Befehl wie folgt ein, um eine Filterregel hinzuzufügen, um die Weiterleitung von TCP-Daten aus dem Quellen-VLAN mit der ID 100 an ein Ziel-VLAN mit der ID 200 an bestimmten Ports zuzulassen:

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

Zugehörige Verweise:

„Befehl mkvfilt" auf Seite 168

„Befehl vlantfw" auf Seite 188

Befehl lsvfilt

Zweck

Listet die VLAN-übergreifenden Filterregeln aus der Filtertabelle auf.

Syntax

lsvfilt [**-a**]

Beschreibung

Der Befehl **lsvfilt** wird verwendet, um die VLAN-übergreifenden Filterregeln und deren Status aufzulisten.

Flags

-a Listet nur die aktiven Filterregeln auf.

Exitstatus

Dieser Befehl gibt die folgenden Exitwerte zurück:

0 Erfolgreiche Ausführung.

>0 Es ist ein Fehler aufgetreten.

Beispiele

1. Geben Sie den Befehl wie folgt ein, um alle aktiven Filterregeln im Kernel aufzulisten:
   ```
   lsvfilt -a
   ```

Zugehörige Konzepte:

„Regeln inaktivieren" auf Seite 122
Sie können Regeln, die das VLAN-übergreifende Routing im Feature Trusted Firewall aktivieren, inaktivieren.

Befehl mkvfilt

Zweck

Aktiviert die vom Befehl **genvfilt** definierten VLAN-übergreifenden Filterregeln.

Syntax

mkvfilt -u

Beschreibung

Der Befehl **mkvfilt** aktiviert die vom Befehl **genvfilt** definierten VLAN-übergreifenden Filterregeln.

Flags

-u Aktiviert die Filterregeln in der Filterregeltabelle.

Exitstatus

Dieser Befehl gibt die folgenden Exitwerte zurück:

0 Erfolgreiche Ausführung.

>0 Es ist ein Fehler aufgetreten.

Beispiele

1. Geben Sie den Befehl wie folgt ein, um die Filterregeln im Kernel zu aktivieren:
   ```
   mkvfilt -u
   ```

Zugehörige Verweise:
„Befehl genvfilt" auf Seite 166

Befehl pmconf

Zweck

Erstellt Berichte und verwaltet den TNCPM-Server (Trusted Network Connect Patch Management) durch Registrierung der Technology Levels und TNC-Server für neue Fixes und Generierung von Berichten zum TNCPM-Status.

Anmerkung: Der TNCPM-Server darf nur unter AIX Version 7.2 mit Technology Level 7100-02 Technology Level ausgeführt werden, um den Download der Service-Pack-Metadaten zuzulassen.

Syntax

pmconf mktncpm [**pmport=**<*Port*>] **tncserver=***IP-Adresse* | Hostname **:** <*Port*>

pmconf rmtncpm

pmconf start

pmconf stop

pmconf init -i <*Downloadintervall*> **-l** <*TL-Liste*> **-A** [**-P** <*Downloadpfad*>] [**-x** <*Intervall für vorläufige Fixes*>] [**-K** <*Schlüssel für vorläufige Fixes*>]

pmconf add -l *TL-Liste*

pmconf add -o <*Paketname*> -V <*Version*> -T [installp|rqm] -D <*benutzerdefinierter Pfad*>

pmconf add -p <*SP-Liste*> [**-U** <*benutzerdefinierter SP-Pfad*>]

pmconf add -p <*SP*> **-e** <*Datei mit vorläufigen Fixes*>

pmconf add -y <*Empfehlungsdatei*> **-v** <*Signaturdatei*> **-e**

pmconf chtncpm Attribut = *Wert*

pmconf delete -l <*TL-Liste*>

pmconf delete -o <*Paketname*> -V <*Version*>

pmconf delete -p <*SP-Liste*>

pmconf delete -p <*SP*>**-e** *Datei mit vorläufigen Fixes*

pmconf export -f *Dateiname*

pmconf get -o <Paket> -V <Version> -T <installp | rpm> -D <Downloadverzeichnis>

pmconf get -L -o <Paket> -V <Version | all> -T <installp | rpm>

pmconf get -L -p <SP>

pmconf get -p <SP> -D <Downloadverzeichnis>

pmconf hist -d

pmconf hist -u

pmconf import -f *Name_der_Zertifikatsdatei* **-k** *Name_der_Schlüsseldatei*

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

pmconf list -a *SP*

pmconf list -C

pmconf list -l *SP*

pmconf list -o <*Paketname*> -V <*Version*>

pmconf list -o [-c] [-q]

pmconf log loglevel = info | error | none

pmconf modify -i < *Downloadintervall*>

pmconf modify -P <*Downloadpfad*>

pmconf modify -g <*yes oder no, um alle Lizenzen zu akzeptieren*>

pmconf modify -t <*Liste der APAR-Typen*>

pmconf modify -x <*Intervall_für_vorläufigen_Fix*>

pmconf modify -K <*Schlüssel für vorläufige Fixes*>

| **pmconf proxy** display

| **pmconf proxy** [enable=yes | no] [host=<Hostname>] [port=<Portnummer>]

pmconf restart

pmconf status

Beschreibung

Der Befehl **pmconf** hat die folgenden Funktionen:

Fix-Repository-Management
: Registriert Technology Levels bzw. hebt deren Registrierung auf. Hebt die Registrierung von TNC-Servern auf. TNCPM erstellt für jeden Technology Level ein Fix-Repository, das die neuesten Fixes, **lslpp**-Informationen (z. B. Informationen zu den installierten Dateigruppen oder Dateigruppenaktualisierungen) und Informationen zu den Sicherheitsfixes für diesen Technology Level enthält.

Berichterstellung
: Generiert Berichte zum Status von TNCPM.

Die folgenden Operationen können mit dem Befehl **pmconf** ausgeführt werden:

Element	Beschreibung
add	Registriert einen neuen Technology Level mit TNCPM.
chtncpm	Ändert die Attribute in der Datei "tnccs.conf". Damit die Änderungen im TNCPM-Server wirksam werden, muss ein expliziter Befehl **start** abgesetzt werden.
delete	Hebt die Registrierung eines Technology Levels mit TNCPM auf.
get	Zeigt Informationen zu verfügbaren Sicherheitsfixes und Open Source-Paketen an oder lädt diese herunter.
history	Zeigt den Aktualisierungs- und Downloadverlauf an.
list	Zeigt die Informationen zu TNCPM an.
log	Legt die Protokollstufe für die TNC-Komponenten fest.
mktncpm	Erstellt den TNCPM-Server.
modify	Ändert die Attribute in der Datei "tncpm.conf".
proxy	Verwaltet die Konfiguration der Proxy-Server-Parameter.
rmtncpm	Entfernt den TNCPM-Server.
start	Startet den TNCPM-Server.
stop	Stoppt den TNCPM-Server.

Flags

Element	Beschreibung
-A	Akzeptiert bei der Durchführung von Clientaktualisierungen alle Lizenzvereinbarungen.
-a <Empfehlungsdatei>	Gibt die Empfehlungsdatei an, die dem Parameter **ifix** entspricht. Wenn Sie keine Empfehlungsdatei angeben, wird der Parameter **ifix** nicht als CVE-Adresse Common Vulnerabilities and Exposures) des vorläufigen Fix betrachtet.
-a *SP*	Generiert einen Bericht mit Informationen zu den Sicherheits-APARs (Authorized Program Analysis Report) für das Service-Pack. *SP* wird im Format REL00-TL-SP angegeben (`6100-01-04` stellt beispielsweise Service-Pack 04 für Technology Level 01 und Version 6.1 dar).
-e <Datei mit vorläufigen Fixes>	Gibt die vorläufigen Fixes an, die TNCPM hinzugefügt werden.
-i *Downloadintervall*	Gibt das Intervall an, in dem TNCPM nach neuen Service-Packs für die registrierten Technology Levels sucht. Das Intervall ist ein ganzzahliger Wert, der Minuten oder das folgende Format darstellt: **d** (Anzahl Tage): **h** (Stunden): **m** (Minuten). Der unterstützte Bereich für das *Downloadintervall* ist 30-525600 Minuten.
-K <Schlüssel für vorläufige Fixes>	Gibt den öffentlichen Schlüssel (Public Key) von IBM AIX Product Security Incident Response Tool (PSIRT) an, der für die Authentifizierung der heruntergeladenen Empfehlungen und vorläufigen Fixes verwendet wird. Dieser öffentliche Schlüssel kann von einem PGP-Public-Key-Server unter Verwendung der ID **0x28BFAA12** heruntergeladen werden.
-L	Gibt den Listen- oder reinen Suchmodus an.
o *Paketname*	Der Name des Open Source-Pakets, das gesucht oder heruntergeladen werden soll.
-P *Fix-Repository-Pfad*	Gibt das Downloadverzeichnis für die Fix-Repositorys an, die von TNCPM heruntergeladen werden. Das Standardverzeichnis ist **/var/tnc/tncpm/fix_repository**.
-p *SP-Liste*	Gibt die Liste der herunterzuladenden Service-Packs an. Die Liste ist eine durch Kommas getrennte Liste von SPs im Format REL00-TL-SP (`6100-01-04` stellt beispielsweise Service-Pack 04 für Technology Level 01 und Version 6.1 dar). Wenn Sie das Flag -U verwenden, geben Sie nur einen einzigen SP an.
-t *Liste_der_APAR-Typen*	Gibt die APAR-Typen an, die TNCPM für die Liste der Clientaktualisierungen und TNC-Server unterstützt. Sicherheits-APARs werden immer unterstützt. "Liste_der_APAR-Typen" steht für eine durch Kommas getrennte Liste der folgenden Typen: HIPER, FileNet Process Engine, Enhancement.
T *Pakettyp*	Gibt den Open-Source-Pakettyp an, der gesucht bzw. heruntergeladen werden soll.
-U *benutzerdefiniertes Fix-Repository*	Gibt den Pfad des benutzerdefinierten Fix-Repository an. Geben Sie das Release, den Technology Level und das Service-Pack für das Fix-Repository an, das für die Überprüfung und Aktualisierungen von Clients verwendet wird.
-s	Generiert einen Bericht über die registrierten Service-Packs.
-l *SP*	Generiert einen Bericht mit **lslpp**-Informationen für das Service-Pack. *SP* wird im Format REL00-TL-SP angegeben (`6100-01-04` stellt beispielsweise Service-Pack 04 für Technology Level 01 und Version 6.1 dar).
-u	Generiert einen Bericht mit dem Verlauf der Clientaktualisierungen.
V *Version*	Die Version des Open Source-Pakets, die gesucht oder heruntergeladen werden soll. Im Suchmodus (-L) kann der Wert "all" angegeben werden, um nach allen verfügbaren Versionen des angegebenen Pakets zu suchen.
-d	Generiert einen Bericht über den Downloadverlauf des Service-Packs.
-C	Generiert einen Bericht für das Serverzertifikat.
-f *Dateiname*	Gibt den Namen der Zertifikatsdatei an.
-k *Name_der_Schlüsseldatei*	Gibt die Datei an, aus der der Zertifikatsschlüssel bei einer Importoperation gelesen werden muss.

-c	Zeigt die Benutzerattribute in Form von durch Doppelpunkten getrennten Datensätzen an:
	`# name: Attribut1: Attribut2: ...`
	`policy: Wert1: Wert2: ...`

Element	Beschreibung
-v <*Signaturdatei*>	Gibt die Signaturdatei für die Empfehlung zu den Schwachstellen in IBM AIX an.
-y <*Empfehlungsdatei*>	Gibt eine Empfehlungsdatei für die Schwachstellen in IBM AIX an.
-q	Unterdrückt die Headerinformationen.
-x <*Intervall für vorläufige Fixes*>	Gibt das Intervall (in Minuten) an, in dem nach neuen herunterladbaren vorläufigen Fixes gesucht wird. Wenn Sie diesen Parameter auf 0 setzen, werden der automatische Download vorläufiger Fixes und die automatische Benachrichtigung inaktiviert. Das Standardintervall ist 24 Stunden. Der unterstützte Bereich für das <*Intervall für vorläufige Fixes*> ist 30-525600 Minuten.

Exitstatus

Dieser Befehl gibt die folgenden Exitwerte zurück:

Element	Beschreibung
0	Der Befehl wurde erfolgreich ausgeführt und alle angeforderten Änderungen wurden vorgenommen.
>0	Es ist ein Fehler aufgetreten. Die ausgegebene Fehlernachricht enthält weitere Details zum Typ des Fehlers.

Beispiele

1. Geben Sie den folgenden Befehl ein, um TNCPM zu initialisieren:
   ```
   pmconf init -f 10080 -l 5300-11,6100-00
   ```
2. Geben Sie den folgenden Befehl ein, um den TNCPM-Dämon zu erstellen:
   ```
   mktncpm pmport=55777 tncserver=11.11.11.11:77555
   ```
3. Geben Sie den folgenden Befehl ein, um den Server zu starten:
   ```
   pmconf start
   ```
4. Geben Sie den folgenden Befehl ein, um den Server zu stoppen:
   ```
   pmconf stop
   ```
5. Geben Sie die folgenden Befehl ein, um einen neuen Technology Level mit TNCPM zu registrieren:
   ```
   pmconf add -l 6100-01
   ```
6. Geben Sie den folgenden Befehl ein, um die Registrierung eines Technology Levels in TNCPM aufzuheben:
   ```
   pmconf delete -l 6100-01
   ```
7. Geben Sie den folgenden Befehl ein, um die Registrierung eines TNC-Servers mit der Adresse 11.11.11.11 in TNCPM aufzuheben:
   ```
   pmconf delete -t 11.11.11.11
   ```
8. Geben Sie den folgenden Befehl ein, um eine neuere Version eines früheren Service-Packs in TNCPM zu registrieren:
   ```
   pmconf add -s 6100-01-04
   ```
9. Geben Sie den folgenden Befehl ein, um die Registrierung eines früheren Service-Packs in TNCPM aufzuheben:
   ```
   pmconf delete -s 6100-01-04
   ```
10. Geben Sie den folgenden Befehl ein, um einen Bericht über die Fix-Repositorys für jeden registrierten Technology Level zu generieren:
    ```
    pmconf list -s
    ```
11. Geben Sie den folgenden Befehl ein, um einen Bericht mit den **lslpp**-Informationen für einen registrierten Technology Level zu generieren:
    ```
    pmconf list -l 6100-01-02
    ```
12. Geben Sie den folgenden Befehl ein, um einen Bericht über den Aktualisierungsverlauf zu generieren:
    ```
    pmconf hist -u
    ```
13. Geben Sie den folgenden Befehl ein, um einen Bericht über den Downloadverlauf zu generieren:
    ```
    pmconf hist -d
    ```

14. Geben Sie den folgenden Befehl ein, um einen Bericht über das Serverzertifikat zu generieren:
    ```
    pmconf list -C
    ```
15. Geben Sie den folgenden Befehl ein, um einen Bericht mit den Sicherheits-APAR-Informationen für ein Service-Pack zu generieren:
    ```
    pmconf list -a 6100-01-02
    ```
16. Geben Sie den folgenden Befehl ein, um ein Serverzertifikat zu importieren:
    ```
    pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt
    ```
17. Geben Sie den folgenden Befehl ein, um das Serverzertifikat zu exportieren:
    ```
    pmconf export -f /tmp/server.txt
    ```
18. Geben Sie den folgenden Befehl ein, um alle verfügbaren Versionen des Open-Source-Pakets für emacs im RPM-Format anzuzeigen:
    ```
    pmconf get -L -o emacs -V all -T rpm
    ```
19. Geben Sie die folgenden Befehle ein, um Version 4.5.1 des Open-Source-Pakets für lsof im RPM-Format in das Verzeichnis /tmp/new_lsof herunterzuladen:
    ```
    mkdir /tmp/new_lsof
    pmconf get -o lsof -V 4.5.1 -T rpm -D /tmp/new_lsof
    ```
20. Geben Sie den folgenden Befehl ein, um alle verfügbaren Versionen von OpenSSH im installp-Format anzuzeigen:
    ```
    pmconf get -o openssh -T installp -L -V all
    ```
21. Geben Sie den folgenden Befehl ein, um die aktuellen Proxy-Konfigurationseinstellungen anzuzeigen, die cURL beim Download von Open-Source-Paketen oder Sicherheitsfixes verwendet:
    ```
    pmconf proxy display
    ```
22. Geben Sie den folgenden Befehl ein, um die zu inaktivierende Proxy-Konfiguration festzulegen:
    ```
    pmconf proxy enable=no
    ```
23. Geben Sie den folgenden Befehl ein, um den Proxy zu aktivieren und den Host auf 'myProxyServer' an Port 9876 zu setzen:
    ```
    pmconf proxy enable=yes host=myProxyServer port=9876
    ```
24. Geben Sie den folgenden Befehl ein, um den zu verwendenden Proxy-Server-Port zu ändern:
    ```
    pmconf proxy port=1234
    ```
25. Geben Sie den folgenden Befehl ein, um bekannte Schwachstellen anzuzeigen, die mit Sicherheitsfixes für Service-Pack-Level 7100-03-02 behoben werden:
    ```
     pmconf get -L -p 7100-03-02
    ```
26. Geben Sie die folgenden Befehle ein, um Sicherheitsfixes für Service-Pack-Level 7200-00-01 in das Verzeichnis /tmp/ifixes_for_7.2.0.1 herunterzuladen, aber nicht anzuwenden:
    ```
    mkdir /tmp/ifixes_for_7.2.0.1
    pmconf get -p 7200-00-01 -D /tmp/ifixes_for_7.2.0.1
    ```

Befehl psconf

Zweck

Berichtet und verwaltet den TNC-Server (Trusted Network Connect), den TNC-Client, den TNC-IP-Referrer (IPRef) und Service Update Management Assistant (SUMA). Der Befehl verwaltet Dateigruppen- und Patch-Management-Richtlinien für die Endpunktintegrität (Server und Client) beim oder nach dem Herstellen einer Netzverbindung zum Schutz des Netzes vor Sicherheitsrisiken und Attacken.

Syntax

TNC-Serveroperationen:

psconf mkserver [tncport=<*Port*> **] pmserver=**<*Host:Port*> [tsserver=<Host>] [**recheck_interval=**<*Zeit_in_Minuten*> | **d** (Tage) : **h** (hours) : **m** (Minuten)] [**dbpath** = <*benutzerdefiniertes Verzeichnis*>] [**default_policy=**<*yes* | *no* >] [**clientData_interval=**<*Zeit_in_Minuten*> | **d** (Tage) : **h** (Stunden) : **m** (Minuten)] [**clientDataPath=**<*vollständiger_Pfad*>]

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

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

psconf chserver attribute = *Wert*

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

psconf add -F <*Name_der_Dateisystemrichtlinie*> -r <*Buildinformationen*> [**apargrp= [±]**<*APAR-Gruppe1, APAR-Gruppe2.. >*] [*Gruppe vorläufiger Fixes*=[+|-]<*Gruppe vorläufiger Fixes1,Gruppe vorläufiger Fixes2...>*]

psconf add { **-G** <*Name der IP-Gruppe*> **ip=[±]**<*Host1, Host2...>* | {**-A**<*APAR-Gruppe*> [**aparlist**=[**±**]*APAR1, APAR2...* | {**-V** <*Gruppe vorläufiger Fixes*> [*ifixlist*=[+|-]*vorläufiger Fix1,vorläufiger Fix2...*]}

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

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

psconf add -I ip= [±]<*Host1, Host2...>*

psconf delete { **-F** <*Name der Dateisystemrichtlinie*> | **-G** <*Name der IP-Gruppe*> | **-P** <*Richtlinienname*> | **-A** <*APAR-Gruppe*> | **-V** <*Gruppe vorläufiger Fixes*>}

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

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

psconf certdel -i <*Host*>

psconf verify -i <*Host*> | **-G** <*IP-Gruppe*>

psconf update [-p] {-i<*Host*>| **-G** <*IP-Gruppe*>[**-r** <*Buildinformationen*> | **-a** <*APAR1, APAR2...*> | **[-u] -v** <*vorläufiger Fix1, vorläufiger Fix2,...*> | **-O** <*openpkggrp1, openkggrp2,...*>}

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

psconf import -C -i <*Host*> **-f** <*Dateiname*> | **–d** <*Dateiname für Importdatenbank*>

psconf { **import -k** <*Name der Schlüsseldatei*> | **export**} **-S -f** <*Dateiname*>

psconf list { **-S** | **-G** < *Name der IP-Gruppe* | **ALL** > | **-F** < *Name der Dateisystemrichtlinie* | **ALL** > | **-P** < *Richtlinienname* | **ALL** > | **-r** < *Nuildinformationen* | **ALL** > | **-I -i** < *IP-Adresse* | **ALL** > | **-A** < *APAR-Gruppe* | **ALL** > | **-V** <*Gruppe vorläufiger Fixes*> | -O <*openpkggrp*|*ALL*>} **[-c] [-q]**

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

psconf export -d <Pfad zum Exportverzeichnis>

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

psconf report -A <Empfehlungsname>

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

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

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

psconf clientData {-l | -g} -i <*IP-Adresse|Host***>**

psconf add -O <*openpkggrp***> <***openpkgname:Version***>**

psconf delete -O <*openpkggrp***> <***openpkgname:version***>**

psconf delete -O <*openpkggrp***>**

psconf delete -O ALL

psconf add -O <*openpkggrp***> fspolicy=<***Name der Dateisystemrichtlinie***>**

psconf report -O ALL -o TEXT

| **psconf add -V <***Gruppe vorläufiger Fixes***> autoupdate=<yes|no>**

| **psconf reboot -i <***Host***> last one**

TNC-Clientoperationen:

psconf mkclient [tncport=<*Port*> **] tncserver=**<*Host:Port*>

psconf mkclient tncport=<<*Port*>> -T

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

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

psconf chclient attribute = *Wert*

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

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

psconf import { **-S** | **-C -k** <*Name_der_Schlüsseldatei*> } **-f** <*Dateiname*>

TNC-IPRef-Operationen:

psconf mkipref [tncport=<*Port*> **] tncserver=**<*Host:Port*>

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

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

psconf chipref attribute = *Wert*

psconf { **import -k** <*Name_der_Schlüsseldatei*> | **export** } **-R -f** <*Dateiname*>

psconf list -R

Beschreibung

Die TNC-Technologie ist eine auf offenen Standards basierende Architektur für die Endpunktauthentifizierung, die Ermittlung der Plattformintegrität und die Integration von Sicherheitssystemen. Die TNC-Architektur überprüft Endpunkte (Netzclients und -server) auf ihre Konformität mit Sicherheitsrichtlinien, bevor sie im geschützten Netz zugelassen werden. Der TNC-IP-Referrer benachrichtigt den TNC-Server über alle neuen IP-Adressen, die in Virtual I/O Server (VIOS) erkannt werden.

SUMA befreit Systemadministratoren von der Aufgabe, Wartungsaktualisierungen manuell aus dem Web abrufen zu müssen. SUMA bietet flexible Optionen, mit denen der Systemadministrator eine automatisierte Schnittstelle zum Herunterladen von Fixes von einer Website für Fixverteilung auf ihre Systeme einrichten können.

Der Befehl **psconf** verwaltet den Netzserver und die Netzclients, indem er Sicherheitsrichtlinien hinzufügt oder löscht, Clients als vertrauenswürdig oder nicht vertrauenswürdig validiert, Berichte generiert und den Server und die Clients aktualisiert.

Die folgenden Operationen können mit dem Befehl **psconf** ausgeführt werden:

Element	Beschreibung
add	Fügt eine Richtlinie, einen Client oder E-Mail-Informationen auf dem TNC-Server hinzu.
apargrp	Gibt die APAR-Gruppennamen im Rahmen der Dateigruppenrichtlinie an, die für die Verifizierung von TNC-Clients verwendet werden.
aparlist	Gibt die Liste der APARs in der APAR-Gruppe an.
certadd	Markiert das Zertifikat als vertrauenswürdig oder nicht vertrauenswürdig.
certdel	Löscht die Clientinformationen.
chclient	Ändert die Attribute in der Datei `tnccs.conf`. Es muss ein expliziter Befehl **start** abgesetzt werden, damit die Änderungen im TNC-Client wirksam werden. Die Attribut=Wert-Syntax ist dieselbe wie bei **mkclient**.
chipref	Ändert die Attribute in der Datei `tnccs.conf`. Damit die Änderungen in IPRef wirksam werden, muss ein expliziter Befehl **start** abgesetzt werden. Die Attribut=Wert-Syntax ist dieselbe wie bei **mkipref**.
chserver	Ändert die Attribute in der Datei `tnccs.conf`. Es muss ein expliziter Befehl **start** abgesetzt werden, damit die Änderungen im TNC-Server wirksam werden. Die Attribut=Wert-Syntax ist dieselbe wie bei **mkserver**. **Anmerkung:** Das Attribut **dbpath** kann mit dem Befehl **chserver** nicht geändert werden. Es kann nur mit **mkserver** gesetzt werden.
clientData	Erstellt eine Momentaufnahme der Informationen (Betriebssystemversion und installierte Dateigruppen) für den TNC-Client. Der *Clientdatenpfad* gibt an, wo die erfassten Momentaufnahmedaten gespeichert werden. Die Standardposition ist das Verzeichnis `/var/tnc/clientData/` auf dem TNC-Server. Sie können den *Clientdatenpfad* mit dem Unterbefehl **chserver** oder **mkserver** ändern oder festlegen. Sie können die Erfassung der Momentaufnahme für den TNC-Client über die Befehlszeile einleiten, indem Sie den Unterbefehl **clientData** über den TNC-Server ausführen. Der über die Befehlszeile ausgeführte Unterbefehl **clientData** ist vom **clientData_interval**-Intervall unabhängig.

Element	Beschreibung
clientData_interval	Mit dem Unterbefehl **chserver** oder **mkserver** können Sie eine regelmäßige Erfassung der Momentaufnahme konfigurieren, indem Sie einen Wert für das **clientData_interval**-Intervall festlegen. Die Erfassung der Momentaufnahme wird automatisch gestartet, wenn das **clientData_interval**-Intervall einen anderen Wert als 0 (null) hat. Standardmäßig wird die Erfassung der Momentaufnahme vom Scheduler inaktiviert. Zum Aktivieren des Schedulers geben Sie einen Wert für **clientData_interval** an, der größer-gleich 30 ist. Zum Inaktivieren des Schedulers geben Sie den Wert 0 (null) für **clientData_interval** an. Der unterstützte Bereich für das **clientData_interval**-Intervall ist 30-525600 Minuten.
dbpath	Gibt die Position der TNC-Datenbank an. Der Standardwert ist `/var/tnc`.
default_policy	Aktiviert oder inaktiviert die automatische Verifizierung der TNC-Clients für die vorläufigen Fixes und APARs, die dieselbe Version haben wie der Client. Geben Sie *yes* an, um die automatische Verifizierung zu aktivieren. Geben Sie *no* an, um die automatische Verifizierung zu inaktivieren. Weitere Informationen zum Unterbefehl **default_policy** finden Sie in der Tabelle default_policy.
delete	Löscht eine Richtlinie oder die Clientinformationen.
export	Exportiert das Client- oder Serverzertifikat oder die Datenbank auf dem TNC-Server.
fspolicy	Gibt die Dateigruppenrichtlinie des Release, des Technology-Levels und des Service-Packs an, die für die Verifizierung der TNC-Clients verwendet wird.
import	Importiert ein Zertifikat in den Client oder Server oder in die Datenbank des TNC-Servers.
ipgroup	Gibt die IP-Gruppe (Internet Protocol) an, die mehrere Client-IP-Adressen oder Hostnamen enthält.
list	Zeigt Informationen zum TNC-Server, zum TNC-Client oder zu SUMA an.
log	Legt die Protokollstufe für die TNC-Komponenten fest.
mkclient	Konfiguriert den TNC-Client.
mkipref	Konfiguriert den TNC-IP-Referrer.
mkserver	Konfiguriert den TNC-Server.
Openpkggrp	Gibt den Namen der Open-Package-Gruppe im Rahmen der Dateigruppenrichtlinie an, die zur Verifizierung der Clients verwendet wird.
pmport	Gibt die Nummer des Ports an, an dem der **pmserver** empfangsbereit ist. Der Standardwert ist 38240.
pmserver	Gibt den Hostnamen oder die IP-Adresse des Befehls **suma** an, der die neuesten Service-Packs und Sicherheitsfixes herunterlädt, die auf der IBM® ECC-Website und auf der IBM Fix Central-Website verfügbar sind.
reboot	Startet den mit der IP-Adresse in der Variablen <*Host*> angegebenen TNC-Client neu.
recheck_interval	Gibt das Intervall in Minuten oder im Format d (Tage) : h (Stunden) : m (Minuten) an, in dem der TNC-Server die TNC-Clients verifizieren soll. Der unterstützte Bereich für das **recheck_interval**-Intervall ist 30-525600 Minuten. **Hinweis:** Der Wert **recheck_interval=0** bedeutet, dass der Scheduler keine regelmäßige Verifizierung der Clients einleitet und die registrierten Clients automatisch verifiziert werden, wennn sie gestartet werden. In solchen Fällen kann der Client manuell verifiziert werden.
report	Generiert einen Bericht mit der Dateierweiterung .txt oder .csv.
restart	Startet den TNC-Client, den TNC-Server oder den TNC-IP-Referrer erneut.
rmclient	Dekonfiguriert den TNC-Client.
rmipref	Dekonfiguriert den TNC-IP-Referrer.

Element	Beschreibung
rmserver	Dekonfiguriert den TNC-Server.
start	Startet den TNC-Client, den TNC-Server oder den TNC-IP-Referrer.
status	Zeigt den Status der TNC-Konfiguration an.
stop	Stoppt den TNC-Client, den TNC-Server oder den TNC-IP-Referrer.
tncport	Gibt die Nummer des Ports an, an dem der TNC-Server empfangsbereit ist. Der Standardwert ist 42830.
tncserver	Gibt den TNC-Server an, der die TNC-Clients verifiziert oder aktualisiert.
tssserver	Gibt die IP-Adresse oder den Hostnamen des Trusted Surveyor-Servers an.
update	Installiert Patches auf dem Client.
verify	Leitet die manuelle Verifizierung des Clients ein.

In der folgenden Tabelle sind die Ergebnisse der Konfiguration des Unterbefehls **default_policy** mit *yes* oder *no* aufgeführt:

Tabelle 16. Ergebnisse des Unterbefehls "default_policy"

FSpolicy (Dateigruppenrichtlinie)	**default policy=***yes*	**default policy=***no*
Der TNC-Client gehört zu einer Dateigruppenrichtlinie mit definierten Gruppen vorläufiger Fixes und APARs.	Die Standardrichtlinie wird mit den vorläufigen Fixes und APARs überschrieben, die in der Dateigruppenrichtlinie angegeben sind.	Die Standardrichtlinie wird nicht verwendet. Die in der Dateigruppenrichtlinie angegebenen vorläufigen Fixes und APARs werden während des Verifizierungsprozesses für den TNC-Client berücksichtigt.
Der TNC-Client gehört zu einer Dateigruppenrichtlinie ohne definierte vorläufige Fixes und APARs.	Die Standardrichtlinie wird mit den vorläufigen Fixes und APARs während des Verifizierungsprozesses für den TNC-Client verwendet. Es werden nur die vorläufigen Fixes und APARs verwendet, die der Version des TNC-Clients entsprechen.	Die Standardrichtlinie wird nicht verwendet.

Flags

Element	Beschreibung
-A <Empfehlungsname>	Gibt den Empfehlungsnamen für den Bericht an.
-B <Buildinformationen>	Gibt die Buildinformationen für die Vorbereitung eines Patchberichts an.

-c	Zeigt die Benutzerattribute wie folgt in durch Doppelpunkten getrennten Datensätzen an:
	`# name: Attribut1: Attribut2: ...`
	`policy: Wert1: Wert2: ...`

-C	Gibt an, dass die Operation für die Clientkomponente bestimmt ist.
-d *Position der Datenbankdatei/ Verzeichnispfad der Datenbank*	Gibt die Dateipfadposition für den Import der Datenbank bzw. die Verzeichnispfadposition für den Export der Datenbank an.
-D *yyyy-mm-dd*	Gibt das Datum für einen bestimmten Clienteintrag im Protokollverlauf an, wobei *yyyy* für das Jahr, *mm* für den Monat und *dd* für den Tag stehen.
-e *E-Mail-ID* **ipgroup=[±]***g1, g2...*	Gibt die E-Mail-ID gefolgt von einer durch Kommas getrennten Liste mit IP-Gruppennamen an.
-E | **FAIL** | **COMPLIANT** | **ALL** |	Gibt das Ereignis an, für das die E-Mails an die konfigurierte E-Mail-ID gesendet werden sollen. FAIL - Es werden E-Mails gesendet, wenn der Verifizierungsstatus des Clients FAILED (Fehlgeschlagen) lautet. COMPLIANT - Es werden E-Mails gesendet, wenn der Verifizierungsstatus des Clients COMPLIANT (Kompatibel) lautet. ALL - Es werden E-Mails für alle Status der Clientverifizierung gesendet.

Element	Beschreibung
-f *Dateiname*	Gibt die Datei an, aus der das Zertifikat im Fall einer Importoperation gelesen werden muss, bzw. gibt die Position an, an die das Zertifikat im Fall einer Exportoperation geschrieben werden muss.
-F *Dateisystemrichtlinie Buildinfo*	Gibt den Namen der Dateisystemrichtlinie gefolgt von den Buildinformationen an. Die Buildinformationen können im folgenden Format angegeben werden: `6100-04-01`, wobei `6100` für Version 6.1, `04` für die Wartungsstufe und `01` für das Service-Pack stehen.
-g	Führt den Unterbefehl **clientData** für den angegebenen TNC-Client aus. Dieses Flag ist nur für den Unterbefehl **clientData** verfügbar.
-G *IP-Gruppenname* **ip=[±]***ip1, ip2...*	Gibt den Namen der IP-Gruppe gefolgt von einer durch Kommas getrennten Liste von IP-Adressen an.
-H	Listet das Systemprotokoll auf.
-i *Host*	Gibt die IP-Adresse oder den Hostnamen an.
-I ip=[±]*ip1, ip2...* | [±] host1,host2...	Gibt die IP-Adresse bzw. den Hostnamen an, die bzw. der während der Verifizierung ignoriert werden muss.
-k *Dateiname*	Gibt die Datei an, aus der der Zertifikatsschlüssel bei einer Importoperation gelesen werden muss.
-l	Listet die Momentaufnahmedetails auf dem TNC-Server für den angegebenen TNC-Client auf. Dieses Flag ist nur für den Unterbefehl **clientData** verfügbar.
-O <Open-Package-Gruppe>	Gibt den Open-Package-Gruppennamen für die Richtlinie an.
-p	Zeigt eine Vorschau der TNC-Clientaktualisierung an.
-P <Richtlinienname>	Gibt den Richtliniennamen für die Vorbereitung eines Clientrichtlinienberichts an.
-q	Unterdrückt die Headerinformationen.
-r *Buildinfo*	Generiert den Bericht basierend auf den Buildinformationen. Die Buildinformationen können im folgenden Format angegeben werden: `6100-04-01`, wobei `6100` für Version 6.1, `04` für die Wartungsstufe und `01` für das Service-Pack stehen.
-R	Gibt an, dass die Operation für die IPRef-Komponente bestimmt ist.
-s COMPLIANT | IGNORE | FAILED | ALL	Zeigt die Clients wie folgt nach Status an: **COMPLIANT** Zeigt die aktiven Clients an. **IGNORE** Zeigt die von der Verifizierung ausgeschlossenen Clients an. **FAILED** Zeigt die Clients an, deren Verifizierung gemäß konfigurierter Richtlinie fehlgeschlagen ist. **ALL** Zeigt alle Clients unabhängig von deren Status an.
-S <Host>	Gibt den Hostnamen für die Vorbereitung eines Berichts über Clientsicherheitsfixes an.
-t TRUSTED | UNTRUSTED	Markiert den Client als vertrauenswürdig oder nicht vertrauenswürdig. **Anmerkung:** Nur Systemadministratoren können den Server oder Client als vertrauenswürdig oder nicht vertrauenswürdig verifizieren.
-T	Gibt an, dass der Client Anforderungen von jedem TS-Server akzeptieren kann, der ein gültiges Zertifikat hat.
-u	Deinstalliert einen vorläufigen Fix, der auf einem TNC-Client installiert ist.
-v<*CVEid|ALL*>	Zeigt die allgemeinen Sicherheitslücken und Schwachstellen für die registrierten Service-Packs an. **CVEid** **All** Zeigt alle allgemeinen Sicherheitslücken und Schwachstellen für die registrierten Service-Packs an.
-v<*ifix1, ifix2,...*>	Gibt eine durch Kommas getrennte Liste mit vorläufigen Fixes an.
-V<*ifixgrp*>	Gibt den Namen der Gruppe vorläufiger Fixes an.
-V *<ifixgrp>* autoupdate=<yes|no>	Gibt an, ob die vorläufigen Fixes in der angegebenen Gruppe vorläufiger Fixes automatisch aktualisiert werden. **Yes** Aktualisiert die als Dateisystemrichtlinie definierte Richtlinie, wenn neue vorläufige Fixes auf dem TNC-Server empfangen werden. **No** Gibt an, dass neue vorläufige Fixes, die auf dem TNC-Server empfangen werden, der Richtlinie manuell zugewiesen werden. No ist der Standardwert.

Exitstatus

Dieser Befehl gibt die folgenden Exitwerte zurück:

Element	Beschreibung
0	Der Befehl wurde erfolgreich ausgeführt und alle angeforderten Änderungen wurden vorgenommen.
>0	Es ist ein Fehler aufgetreten. Die ausgegebene Fehlernachricht enthält weitere Details zum Typ des Fehlers.

Beispiele

1. Geben Sie den folgenden Befehl ein, um den TNC-Server zu starten:

   ```
   psconf start server
   ```

2. Geben Sie den folgenden Befehl ein, um eine Dateisystemrichtlinie mit dem Namen `71D_latest` für den Build `7100-04-02` hinzuzufügen:

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

3. Geben Sie den folgenden Befehl ein, um eine Dateisystemrichtlinie mit dem Namen `71D_old` zu löschen:

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

4. Geben Sie den folgenden Befehl ein, um zu prüfen, ob der Client mit der IP-Adresse `11.11.11.11` **vertrauenswürdig** ist:

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

5. Geben Sie den folgenden Befehl ein, um den Client mit der IP-Adresse `11.11.11.11` vom Server zu löschen:

   ```
   psconf certdel -i 11.11.11.11
   ```

6. Geben Sie den folgenden Befehl ein, um die Informationen eines Clients mit der IP-Adresse `11.11.11.11` zu verifizieren:

   ```
   psconf verify -i 11.11.11.11
   ```

7. Geben Sie den folgenden Befehl ein, um die Informationen des Clients mit der IP-Adresse `11.11.11.11` anzuzeigen:

   ```
   psconf list -i 11.11.11.11
   ```

8. Geben Sie den folgenden Befehl ein, um den Bericht für Clients mit dem Status **COMPLIANT** zu generieren:

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

9. Geben Sie den folgenden Befehl ein, um den Bericht für den Build `7100-04-02` zu generieren:

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

10. Geben Sie den folgenden Befehl ein, um den Verbindungsverlauf eines Clients mit der IP-Adresse `11.11.11.11` anzuzeigen:

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

11. Geben Sie den folgenden Befehl ein, um Einträge für einen Client mit der IP-Adresse `11.11.11.11` aus dem Protokollverlauf zu löschen, die ein Datum bis zum 1. Februar 2009 einschließlich aufweisen:

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

12. Geben Sie den folgenden Befehl ein, um das Clientzertifikat eines Clients mit der IP-Adresse `11.11.11.11` vom Server zu importieren:

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

13. Geben Sie den folgenden Befehl ein, um das Serverzertifikat von einem Client zu exportieren:

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

14. Geben Sie den folgenden Befehl ein, um den Client mit der IP-Adresse `11.11.11.11` auf eine entsprechende Version vom Server zu aktualisieren:

    ```
    psconf update -i 11.11.11.11
    ```

15. Geben Sie den folgenden Befehl ein, um die Clientstatus anzuzeigen:

    ```
    psconf status
    ```

16. Geben Sie den folgenden Befehl ein, um das Clientzertifikat anzuzeigen:

```
psconf list -C
```

17. Geben Sie den folgenden Befehl ein, um den Client zu starten:
    ```
    psconf start client
    ```
18. Geben Sie den folgenden Befehl ein, um die Momentaufnahmeinformationen anzuzeigen, die mit dem Unterbefehl **clientData** erfasst wurden:
    ```
    psconf clientData -l [IP-Adresse|Host]
    ```
19. Geben Sie den folgenden Befehl ein, um den Verlauf für den TNC-Client anzuzeigen:
    ```
    psconf list –H –i [IP-Adresse|ALL]
    ```

Sicherheit

Hinweis für RBAC-Benutzer und Trusted AIX-Benutzer:

Mit diesem Befehl können privilegierte Operationen ausgeführt werden. Privilegierte Operationen dürfen nur von privilegierten Benutzern ausgeführt werden. Weitere Informationen zu Berechtigungen und Privilegien finden Sie im Abschnitt "Datenbank mit privilegierten Befehlen" unter "Sicherheit". Eine Liste der Privilegien und Berechtigungen für diesen Befehl finden Sie in den Beschreibungen des Befehls **lssecattr** und des Unterbefehls **getcmdattr**.

Befehl pscuiserverctl

Zweck

Wird verwendet, um die Optionen für den PowerSC-GUI-Server zu konfigurieren.

Syntax

pscuiserverctl -r set [arg1 [arg2 [arg3]]]

pscuiserverctl set [httpPort]

pscuiserverctl set [httpsPort]

pscuiserverctl set [administratorGroupList]

pscuiserverctl set [logonGroupList]

pscuiserverctl set [powervcKeystoneUrl]

pscuiserverctl set [QRadarSyslogResponseEnabled]

pscuiserverctl set [tncServer]

Flags

-r Startet den PowerSC-GUI-Server nach dem Anwenden eines Parameterwerts erneut.

set
Legt eine Option für den PowerSC-GUI-Server fest bzw. ruft diese ab.

Parameter

httpPort ***HTTP-Portnummer***
Zeigt den von der PowerSC-GUI verwendeten Standardport an bzw. legt diesen fest.

httpsPort ***HTTPS-Portnummer***
Zeigt den von der PowerSC-GUI verwendeten sicheren Standardport an bzw. legt diesen fest.

administratorGroupList *UNIX-Gruppe1,UNIX-Gruppe2,...*
Zeigt die UNIX-Gruppen, die Administratorfunktionen in der PowerSC-GUI ausführen dürfen, an bzw. legt diese fest.

logonGroupList *UNIX-Gruppe1,UNIX-Gruppe2,...*
Zeigt die UNIX-Gruppen, die sich an der PowerSC-GUI anmelden dürfen, an bzw. legt diese fest.

powervcKeystoneUrl *URL_für_PowerVC-Keystore*
Zeigt die URL des PowerVC-Keystore-Servers an.

QRadarSyslogResponseEnabled on | off
Zeigt die aktuelle Einstellung der syslog-Protokollierung in der PowerSC-GUI an oder setzt die Syslog-Protokollierung auf on (ein) oder off (aus).

tncServer *tncserver.abc.com*
Zeigt den Hostnamen des TNC-Servers an bzw. legt diesen fest. Wenn Sie den Hostnamen des TNC-Servers ändern, müssen Sie den PowerSC-GUI-Server erneut starten.

Exitstatus

Dieser Befehl gibt die folgenden Exitwerte zurück:

0 Erfolgreiche Ausführung.

>0 Es ist ein Fehler aufgetreten.

Beispiele

1. Geben Sie den folgenden Befehl ein, um den Port anzuzeigen, der momentan als Standardport für die PowerSC-GUI festgelegt ist:
   ```
   pscuiserverctl set httpPort
   ```
2. Geben Sie den folgenden Befehl ein, um den Standardport für die PowerSC-GUI festzulegen:
   ```
   pscuiserverctl set httpPort 80
   ```
3. Geben Sie den folgenden Befehl ein, um den Port anzuzeigen, der momentan als sicherer Standardport für die PowerSC-GUI festgelegt ist:
   ```
   pscuiserverctl set httpsPort
   ```
4. Geben Sie den folgenden Befehl ein, um den sicheren Standardport für die PowerSC-GUI festzulegen:
   ```
   pscuiserverctl set httpsPort 483
   ```
5. Geben Sie den folgenden Befehl ein, um die UNIX-Gruppen anzuzeigen, die Administratorfunktionen in der PowerSC-GUI ausführen dürfen:
   ```
   pscuiserverctl set administratorGroupList
   ```
6. Geben Sie den folgenden Befehl ein, um die UNIX-Gruppen festzulegen, die Administratorfunktionen in der PowerSC-GUI ausführen dürfen:
   ```
   pscuiserverctl set administratorGroupList securitygroup1,admingrp1
   ```
7. Geben Sie den folgenden Befehl ein, um die UNIX-Gruppen anzuzeigen, die sich an der PowerSC-GUI anmelden dürfen:
   ```
   pscuiserverctl set logonGroupList
   ```
8. Geben Sie den folgenden Befehl ein, um die UNIX-Gruppen festzulegen, die sich an der PowerSC-GUI anmelden dürfen:
   ```
   pscuiserverctl set logonGroupList unixgroup1,unixgrp2
   ```
9. Geben Sie den folgenden Befehl ein, um die URL des PowerVC-Keystore-Servers anzuzeigen:
   ```
   pscuiserverctl set powervcKeystoneUrl
   ```
10. Geben Sie den folgenden Befehl ein, um die URL des PowerVC-Keystore-Servers festzulegen:
    ```
    pscuiserverctl set powervcKeystoneUrl https://powervc/server/example/
    ```

11. Geben Sie den folgenden Befehl ein, um anzuzeigen, ob die syslog-Protokollierung in der PowerSC-GUI aktiviert oder inaktiviert ist:

    ```
    pscuiserverctl set QRadarSyslogResponseEnabled
    ```

12. Geben Sie den folgenden Befehl ein, um die syslog-Protokollierung in der PowerSC-GUI zu aktivieren bzw. zu inaktivieren:

    ```
    pscuiserverctl set QRadarSyslogResponseEnabled on
    pscuiserverctl set QRadarSyslogResponseEnabled off
    ```

13. Geben Sie den folgenden Befehl ein, um den Hostnamen des TNC-Servers anzuzeigen:

    ```
    pscuiserverctl set tncServer
    ```

14. Geben Sie den folgenden Befehl ein, um den Hostnamen des TNC-Servers festzulegen:

    ```
    pscuiserverctl set tncServer tncserver.abc.com
    ```

15. Die Festlegung des Hostnamens für den TNC-Server erfordert einen Neustart des PowerSC-GUI-Servers. Geben Sie den folgenden Befehl ein, um den PowerSC-GUI-Server erneut zu starten:

    ```
    pscuiserverctl -r set tncServer tncs1.rs.com
    ```

Befehl pscxpert

Zweck

Hilft dem Systemadministrator bei der Definition der Sicherheitskonfiguration.

Syntax

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

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

pscxpert -f Profile [**-p**] [**-r** | **-R**]

pscxpert -u [**-p**]

pscxpert -c [**-p**] [**-r** | **-R**] [**-P** Profil] [**-l** Stufel]

pscxpert -t

pscxpert -l <Level> [**-p**] <**-a** *Datei1* | **-n** *Datei2* | **-a** *Datei3* **-n** *Datei4*>

pscxpert -f Profil **-a** Datei [**-p**]

pscxpert -d

Beschreibung

Der Befehl **pscxpert** setzt verschiedene Systemkonfigurationseinstellungen, um die angegebene Sicherheitsstufe zu aktivieren.

Wenn der Befehl **pscxpert** nur mit dem Flag **-l** ausgeführt wird, werden die Sicherheitseinstellungen unverzüglich implementiert, ohne dem Benutzer die Konfiguration der Einstellungen zu ermöglichen. Bei der Ausführung des Befehls **pscxpert -l high** werden beispielsweise automatisch alle High-Level-Sicherheitseinstellungen auf das System angewendet. Wird der Befehl**pscxpert -l** jedoch mit den Flags **-n** und **-a** ausgeführt, werden die Sicherheitseinstellungen in einer mit dem Parameter *Datei* angegebenen Datei gespeichert. Das Flag **-f** wendet dann die neuen Konfigurationen an.

Nach der Erstauswahl wird ein Menü angezeigt, das alle Sicherheitskonfigurationsoptionen enthält, die der ausgewählten Sicherheitsstufe zugeordnet sind. Diese Optionen können als Ganzes akzeptiert oder einzeln aktiviert und inaktiviert werden. Nachdem alle sekundären Änderungen angewendet wurden, führt der Befehl **pscxpert** mit dem Anwenden der Sicherheitseinstellungen auf das Computersystem fort.

Führen Sie den Befehl **pscxpert** als Rootbenutzer des Ziel-VIOS (Virtual I/O Server) aus. Wenn Sie nicht als Rootbenutzer des Ziel-VIOS angemeldet sind, führen Sie vor der Ausführung des Befehls den Befehl**oem_setup_env** aus.

Wenn Sie den Befehl **pscxpert** ausführen, während eine andere Instanz des Befehls **pscxpert** aktiv ist, wird der Befehl **pscxpert** mit einer Fehlernachricht beendet.

Anmerkung: Führen Sie den Befehl **pscxpert** nach allen größeren Systemänderungen wie Softwareinstallationen und Softwareaktualisierungen erneut aus. Wenn bei der erneuten Ausführung des Befehls **pscxpert** ein bestimmtes Sicherheitskonfigurationselement nicht ausgewählt ist, wird dieses Konfigurationselement übersprungen.

Flags

Element	Beschreibung
-a	Die Einstellungen mit den zugehörigen Sicherheitsstufenoptionen werden in gekürztem Format in die angegebene Datei geschrieben.
-c	Überprüft die Sicherheitseinstellungen anhand des zuvor angewendeten Regelsatzes. Falls die Prüfung einer Regel fehlschlägt, werden auch die vorherigen Versionen der Regel geprüft. Dieser Prozess wird so lange fortgesetzt, bis die Prüfung erfolgreich ist oder bis alle Instanzen der fehlerhaften Regel in der Datei `/etc/security/aixpert/core/appliedaixpert.xml` geprüft wurden. Sie können diese Prüfung für jedes Standardprofil oder angepasste Profil ausführen.
-d	Zeigt die Dokumenttypdefinition (DTD) an.

Element	Beschreibung
-f	Wendet die Sicherheitseinstellungen an, die in der angegebenen *Profildatei* festgelegt sind. Die Profile sind im Verzeichnis `/etc/security/aixpert/custom` enthalten. Zu den verfügbaren Profilen gehören die folgenden Standardprofile: **DataBase.xml** Diese Datei enthält die Anforderungen für die Standarddatenbankeinstellungen. **DoD.xml** Diese Datei enthält die Anforderungen für die DoD-STIG-Einstellungen (Department of Defense Security Technical Implementation Guide). **DoD_to_AIXDefault.xml** Setzt die Einstellungen auf die AIX-Standardeinstellungen zurück. **DoDv2.xml** Diese Datei enthält die Anforderungen für Version 2 der DoD-STIG-Einstellungen (Department of Defense Security Technical Implementation Guide). **DoDv2_to_AIXDefault.xml** Setzt die Einstellungen auf die AIX-Standardeinstellungen zurück. **Hipaa.xml** Diese Datei enthält die Anforderungen für die HIPAA-Einstellungen (Health Insurance Portability and Accountability Act). **NERC.xml** Diese Datei enthält die Anforderungen für die NERC-Einstellungen (North American Electric Reliability Corporation). **NERC_to_AIXDefault.xml** Diese Datei ändert die NERC-Einstellungen in die AIX-Standardeinstellungen. **PCI.xml** Diese Datei enthält die Anforderungen für die PCI-DSS-Einstellungen (Payment Card Industry Data Security Standard). **PCIv3.xml** Diese Datei enthält die Anforderungen für Version 3 der PCI-DSS-Einstellungen (Payment Card Industry Data Security Standard). **PCI_to_AIXDefault.xml** Diese Datei ändert die Einstellungen in die AIX-Standardeinstellungen. **PCIv3_to_AIXDefault.xml** Diese Datei ändert die Einstellungen in die AIX-Standardeinstellungen. **SOX-COBIT.xml** Diese Datei enthält die Anforderungen für die Sarbanes-Oxley Act and COBIT-Einstellungen. Sie können auch angepasste Profile in demselben Verzeichnis erstellen und diese auf Ihre Einstellungen anwenden, indem Sie die vorhandenen XML-Dateien umbenennen und ändern. Der folgende Befehl wendet beispielsweise das HIPAA-Profil auf Ihr System an: `pscxpert -f /etc/security/aixpert/custom/Hipaa.xml` Wenn Sie das Flag **-f** angeben, werden die Sicherheitseinstellungen konsistent von System auf System angewendet, indem eine Datei **appliedaixpert.xml** sicher von einem System auf ein anderes übertragen und dort angewendet wird. Alle erfolgreich angewendeten Regeln werden in die Datei `/etc/security/aixpert/core/appliedaixpert.xml` geschrieben und die entsprechenden `undo`-Aktionsregeln werden in die Datei `/etc/security/aixpert/core/undo.xml` geschrieben.

Element	Beschreibung
-l	Setzt die Systemsicherheitseinstellungen auf die angegebene Stufe. Dieses Flag hat die folgenden Optionen: **h | high** Gibt Optionen mit hoher Sicherheitsstufe an. **m | medium** Gibt Optionen mit mittlerer Sicherheitsstufe an. **l | low** Gibt Optionen mit niedriger Sicherheitsstufe an. **d | default** Gibt die Optionen auf AIX-Standardsicherheitsstufe an. **s | sox-cobit** Gibt die Sicherheitsoption für Sarbanes-Oxley Act und COBIT an. Wenn Sie das Flag **-l** und das Flag **-n** angeben, werden die Sicherheitseinstellungen nicht im System implementiert, sondern nur in die angegebene Datei geschrieben. Alle erfolgreich angewendeten Regeln werden in die Datei `/etc/security/aixpert/core/appliedaixpert.xml` geschrieben und die entsprechenden Widerrufsaktionsregeln werden in die Datei `/etc/security/aixpert/core/undo.xml` geschrieben. **Achtung:** Wenn Sie das Flag **d | default** verwenden, kann das Flag die Sicherheitseinstellungen, die Sie zuvor mit dem Befehl **pscxpert** oder unabhängig konfiguriert haben, überschreiben und das System mit seiner traditionellen offenen Konfiguration wiederherstellen.
-n	Schreibt die Einstellungen mit den zugehörigen Sicherheitsoptionen in die angegebene Datei.
-p	Gibt an, dass eine ausführliche Ausgabe der Sicherheitsregeln angezeigt wird. Das Flag **-p** protokolliert die verarbeiteten Regeln im Prüfsubsystem, wenn die Option **auditing** aktiviert ist. Diese Flag kann zusammen mit den Optionen **-l**, **-u**, **-c** und **-f** verwendet werden. Das Flag **-p** aktiviert die ausführliche Ausgabe im Terminal und in der Datei "aixpert.log".
-P	Akzeptiert den Profilnamen als Eingabe. Diese Option wird zusammen mit dem Flag **-c** verwendet. Die Flags **-c** und **-P** werden verwendet, um die Kompatibilität des Systems mit dem übergebenen Profil zu prüfen.
-r	Schreibt die vorhandenen Einstellungen des Systems in die Datei `/etc/security/aixpert/check_report.txt`. Sie können die Ausgabe in Sicherheits-oder Kompatibilitätsprüfberichten verwenden. Der Bericht beschreibt jede Einstellung und deren potenzielle Verknüpfung mit einer Voraussetzung zur Einhaltung von Vorschriften und gibt Aufschluss darüber, ob die Prüfung erfolgreich war oder nicht. **Anmerkung:** • Das Flag "-r" unterstützt die Anwendungsoperation nur für Profile. Die Anwendungsoperation für Stufen wird nicht unterstützt. • Die Option "-r" zeigt die vollständige Nachricht (eine oder mehrere Zeilen) für eine Regel an.
-R	Erzeugt dieselbe Ausgabe wie das Flag **-r**. Außerdem fügt dieses Flag eine Beschreibung des Regelscripts oder Regelprogramms hinzu, das zur Implementierung der Konfigurationseinstellung verwendet wird. **Anmerkung:** • Das Flag "-R" unterstützt die Anwendungsoperation nur für Profile. Die Anwendungsoperation für Stufen wird nicht unterstützt.
-t	Zeigt den Typ des auf das System angewendeten Profils an.
-u	Macht die zuletzt angewendeten Sicherheitseinstellungen rückgängig. **Anmerkung:** • Mit dem Flag **-u** kann die Anwendung der DoD-, DoDv2-, NERC-, PCI- und PCIv3-Profile nicht rückgängig gemacht werden. Wenn Sie diese Profile nach dem Hinzufügen wieder entfernen möchten, wenden Sie das Profil an, das mit `_AIXDefault.xml` endet. Um beispielsweise das Profil "NERC.xml" zu entfernen, müssen Sie das Profil "NERC_to_AIXDefault.xml" anwenden. • Nach einer Anwendungsoperation am System vorgenommene Änderungen gehen bei einer Widerrufsoperation verloren. Die Einstellungen werden auf die Werte zurückgesetzt, die vor der Anwendungsoperation wirksam waren.

Parameter

Element	Beschreibung
Datei	Die Ausgabedatei, in der die Sicherheitseinstellungen gespeichert werden. Für den Zugriff auf diese Datei ist Rootberechtigung erforderlich.
Stufe	Die angepasste Stufe, die mit den zuvor angewendeten Einstellungen verglichen wird.
Profil	Der Dateiname des Profils, das die Konformitätsregeln für das System bereitstellt. Für den Zugriff auf diese Datei sind Rootberechtigungen erforderlich.

Sicherheit

Der Befehl **pscxpert** kann nur von Root ausgeführt werden.

Beispiele

1. Geben Sie den folgenden Befehl ein, um alle High-Level-Sicherheitsoptionen in eine Ausgabedatei zu schreiben:

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

   Nach der Ausführung dieses Befehls können Sie die Ausgabedatei bearbeiten und bestimmte Sicherheitsrollen auf Kommentar setzen, indem Sie diese in die XML-Standardkommentarzeichenfolge einschließen. `<--` kennzeichnet den Anfang des Kommentars und `-\>` schließt den Kommentar.
2. Geben Sie den folgenden Befehl ein, um die Sicherheitseinstellungen aus der Department of Defense-STIG-Konfigurationsdatei anzuwenden:

   ```
   pscxpert -f /etc/security/aixpert/custom/DoD.xml
   ```
3. Geben Sie den folgenden Befehl ein, um die Sicherheitseinstellungen aus der HIPAA-Konfigurationsdatei anzuwenden:

   ```
   pscxpert -f /etc/security/aixpert/custom/Hipaa.xml
   ```
4. Geben Sie den folgenden Befehl ein, um die Sicherheitseinstellungen des Systems zu überprüfen und die Regeln, für die die Überprüfung fehlgeschlagen ist, im Prüfsubsystem zu protokollieren:

   ```
   pscxpert -c -p
   ```
5. Geben Sie den folgenden Befehl ein, um die angepasste Stufe der Sicherheitseinstellungen für das NERC-Profil auf dem System zu überprüfen und die Regeln, für die die Überprüfung fehlgeschlagen ist, im Prüfsubsystem zu protokollieren:

   ```
   pscxpert -c -p -l NERC
   ```
6. Geben Sie den folgenden Befehl ein, um Berichte zu generieren und sie in die Datei `/etc/security/aixpert/check_report.txt` zu schreiben:

   ```
   pscxpert -c -r
   ```

Position

Element	Beschreibung
/usr/sbin/pscxpert	Enthält den Befehl **pscxpert**.

Dateien

Element	Beschreibung
/etc/security/aixpert/log/aixpert.log	Enthält ein Traceprotokoll der angewendeten Sicherheitseinstellungen. Diese Datei verwendet den syslog-Standard nicht. Der Befehl **pscxpert** schreibt direkt in die Datei, hat Lese-/Schreibberechtigungen und erfordert Rootsicherheit.
/etc/security/aixpert/log/firstboot.log	Enthält ein Traceprotokoll der Sicherheitseinstellungen, die beim ersten Booten einer SbD-Installation (Secure by Default) angewendet wurden.
/etc/security/aixpert/core/undo.xml	Enthält eine XML-Liste der Sicherheitseinstellungen, die aufgehoben werden können.

Befehl rmvfilt

Zweck

Entfernt die VLAN-übergreifenden Filterregeln aus der Filtertabelle.

Syntax

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

Beschreibung

Der Befehl **rmvfilt** wird verwendet, um die VLAN-übergreifenden Filterregeln aus der Filtertabelle zu entfernen.

Flags

-n Gibt die ID der zu entfernenden Filterregel an. Die Option **all** wird verwendet, um alle Filterregeln zu entfernen.

Exitstatus

Dieser Befehl gibt die folgenden Exitwerte zurück:

0 Erfolgreiche Ausführung.

>0 Es ist ein Fehler aufgetreten.

Beispiele

1. Geben Sie den Befehl wie folgt ein, um alle Filterregeln zu entfernen oder um alle Filterregeln im Kernel zu inaktivieren:

   ```
   rmvfilt -n all
   ```

Zugehörige Konzepte:

„Regeln inaktivieren" auf Seite 122
Sie können Regeln, die das VLAN-übergreifende Routing im Feature Trusted Firewall aktivieren, inaktivieren.

Befehl vlantfw

Zweck

Zeigt die IP- und MAC-Zuordnungsinformationen (Media Access Control) an bzw. löscht diese und steuert die Protokollierungsfunktion.

Syntax

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

Beschreibung

Der Befehl **vlantfw** zeigt die IP- und MAC-Zuordnungseinträge an bzw. löscht sie. Außerdem kann mit diesem Befehl die Protokollierungsfunktion von Trusted Firewall gestartet und gestoppt werden.

Flags

-d Zeigt alle IP-Zuordnungsinformationen an.

-D Zeigt die erfassten Verbindungsdaten an.

-E Zeigt die Daten zu den Verbindungen zwischen logischen Partitionen (LPARs) in verschiedenen Zentralprozessorkomplexen an.

-f Entfernt alle IP-Zuordnungsinformationen.

-F Löscht den Verbindungsdatencache.

-G Zeigt die Filterregeln an, die konfiguriert werden können, um den Datenverkehr intern über Trusted Firewall weiterzuleiten.

-I Zeigt die Daten zu den Verbindungen zwischen LPARs an, die verschiedenen VLAN-IDs zugeordnet sind, aber denselben Zentralprozessorkomplex haben.

-l Startet die Protokollierungsfunktion von Trusted Firewall.

-L Stoppt die Protokollierungsfunktion von Trusted Firewall und leitet den Tracedateiinhalt in die Datei `/home/padmin/svm/svm.log` um.

-m Aktiviert die Trusted Firewall-Überwachung.

-M Inaktiviert die Trusted Firewall-Überwachung.

-q Fragt den Status einer sicheren virtuellen Maschine ab.

-s Startet Trusted Firewall.

-t Stoppt Trusted Firewall.

Parameter

-N *integer*
Zeigt die Filterregel an, die der angegebenen ganzen Zahl entspricht.

Exitstatus

Dieser Befehl gibt die folgenden Exitwerte zurück:

0 Erfolgreiche Ausführung.

>0 Es ist ein Fehler aufgetreten.

Beispiele

1. Geben Sie den Befehl wie folgt ein, um alle IP-Zuordnungen anzuzeigen:
   ```
   vlantfw -d
   ```
2. Geben Sie den Befehl wie folgt ein, um alle IP-Zuordnungen zu entfernen:
   ```
   vlantfw -f
   ```
3. Geben Sie den Befehl wie folgt ein, um die Protokollierungsfunktion von Trusted Firewall zu starten:
   ```
   vlantfw -l
   ```
4. Geben Sie den Befehl wie folgt ein, um den Status einer sicheren virtuellen Maschine zu überprüfen:
   ```
   vlantfw -q
   ```
5. Geben Sie den Befehl wie folgt ein, um Trusted Firewall zu starten:

```
vlantfw -s
```

6. Geben Sie den Befehl wie folgt ein, um Trusted Firewall zu stoppen:

```
vlantfw -t
```

7. Geben Sie den Befehl wie folgt ein, um die Regeln anzuzeigen, die zum Generieren von Filtern verwendet werden können, die Datenverkehr im Zentralprozessorkomplex weiterleiten:

```
vlantfw -G
```

Zugehörige Verweise:

„Befehl genvfilt" auf Seite 166

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Dokuments ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
USA

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Die genannten Leistungsdaten und Clientbeispiele dienen nur der Veranschaulichung. Die tatsächlichen Leistungsergebnisse können je nach Konfiguration und Betriebsbedingung variieren.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Veröffentlichung dient nur zu Planungszwecken. Die in dieser Veröffentlichung enthaltenen Informationen können geändert werden, bevor die beschriebenen Produkte verfügbar sind.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden und jede Ähnlichkeit mit Namen und Adressen tatsächlicher Personen oder Unternehmen ist rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellensprache geschrieben sind und Programmiertechniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle für die Betriebsumgebung konform sind, für die diese Beispielprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten. Die Beispielprogramme werden ohne Wartung (auf "as-is"-Basis) und ohne jegliche Gewährleistung zur Verfügung gestellt. IBM übernimmt keine Haftung für Schäden, die durch die Verwendung der Beispielprogramme entstehen.

Kopien oder Teile der Beispielprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© (Name Ihrer Firma) (Jahr).

Teile des vorliegenden Codes wurden aus Beispielprogrammen der IBM Corporation abgeleitet.

Hinweise zur Datenschutzrichtlinie

IBM Softwareprodukte, einschließlich Software as a Service-Lösungen ("Softwareangebote"), können Cookies oder andere Technologien verwenden, um Informationen zur Produktnutzung zu erfassen, die Endbenutzererfahrung zu verbessern und Interaktionen mit dem Endbenutzer anzupassen oder zu anderen Zwecken. In vielen Fällen werden von den Softwareangeboten keine personenbezogenen Daten erfasst.

Einige der IBM Softwareangebote können Sie jedoch bei der Erfassung personenbezogener Daten unterstützen. Wenn dieses Softwareangebot Cookies zur Erfassung personenbezogener Daten verwendet, sind nachfolgend nähere Informationen über die Verwendung von Cookies durch dieses Angebot zu finden.

Dieses Softwareangebot verwendet keine Cookies oder andere Technologien zur Erfassung personenbezogener Daten.

Wenn die für dieses Softwareangebot genutzten Konfigurationen Sie als Kunde in die Lage versetzen, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen, müssen Sie sich zu allen gesetzlichen Bestimmungen in Bezug auf eine solche Datenerfassung, einschließlich aller Mitteilungspflichten und Zustimmungsanforderungen, rechtlich beraten lassen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in der "IBM Online-Datenschutzerklärung, Schwerpunkte" unter http://www.ibm.com/privacy, in der "IBM Online-Datenschutzerklärung" unter http://www.ibm.com/privacy/details im Abschnitt "Cookies, Web-Beacons und sonstige Technologien" und unter "IBM Software Products and Software-as-a-Service Privacy Statement" unter http://www.ibm.com/software/info/product-privacy.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der International Business Machines Corporation in den USA und/oder anderen Ländern. Andere Produkt- und Servicenamen können Marken von IBM oder anderen Anbietern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite Copyright and trademark information unter www.ibm.com/legal/copytrade.shtml.

Linux ist eine Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Index

A

AIX-Datei syslog 125
AIX-Prüfsubsystem 125
Aktualisierung einer fehlgeschlagenen Regel 100
Attestierungsergebnisse interpretieren 111
Automation von Sicherheit und Konformität verwalten 99, 100

B

Befehl pscxpert 183
Befehle
  chvfilt 165
  genvfilt 166
  lsvfilt 167
  mkvfilt 168
  pscuiserverctl 181
  rmvfilt 188
  vlantfw 188
Berichte
  arbeiten mit 162
  Berichtsgruppe auswählen 162
  verteilen 163
Berichts- und Management-Tool für TNC, SUMA
  Befehl psconf verwenden 173
Berichts- und Management-Tool für TNCPM
  Befehl pmconf verwenden 169

C

chvfilt, Befehl 165
Client konfigurieren 132
Clientrichtlinien 136
Clientverifizierung 137
Collector installieren 109
cURL 127, 130

D

Daten auf virtuelle Protokolleinheiten schreiben 126

E

E-Mail-Benachrichtigung 134

F

Feature
  PowerSC Real Time Compliance 105
Fehler bei TNC und Patch Management beheben 140
Fehlerbehebung 112
Fehlerhebung vorbereiten 108
Fehlgeschlagene Regel aktualisieren 100

G

genvfilt, Befehl 166
Grafische Benutzerschnittstelle
  Endpunkt- und Serverkommunikation 148
GUI-Schnittstelle
  Agent 143
  angepasste Endpunktgruppen 150
  angepasste Profile löschen 153
  Benachrichtigung über Konformitätsereignis 156
  Benachrichtigung über Sicherheitsereignis 162
  Einführung 141
  Endpunkt 142
  Endpunkt- und Serverkommunikation verifizieren 148
  Endpunkte entfernen 148
  Endpunkte gruppieren 150
  Endpunkte zur Gruppe hinzufügen 150
  Endpunktgruppen angeben 145
  Endpunktgruppen klonen 151
  Endpunktgruppen löschen 151
  Endpunktgruppen umbenennen 151
  Endpunktsicherheit überwachen 156
  Gruppenscripts ausführen 145
  installieren 143
  Keystore-Anforderungen generieren 149
  Keystore-Anforderungen verifizieren 149
  Konformitätsprofile 151
  Konformitätsprofile anwenden 153, 154
  Konformitätsprofile anzeigen 152
  Konformitätsprofile erstellen 152
  Konformitätsprofile überprüfen 155, 156
  Konformitätsprofile widerrufen 154
  Navigation 147
  Profile auf Endpunkte kopieren 153
  Rollback von RTC auf frühere Zeitmarke 157
  Rollback von RTC-Dateien auf eine frühere Überwachungskonfiguration durchführen 158
  RTC-Dateiliste bearbeiten 158
  RTC-Konfigurationsoptionen in Gruppen kopieren 157
  RTC konfigurieren 157
  RTC-Prüfung durchführen 159
  Server 143
  Sicherheit 141
  Sicherheitszertifikate ausführen 144
  Sicherheitszertifikate erstellen 143
  Sprache 147
  Status von PowerSC-Produkten anzeigen 160
  TE-Dateiliste bearbeiten 159
  TE-Konfigurationsoptionen in Gruppen kopieren 159
  TE konfigurieren 159
  TE-Überwachung aktivieren und inaktivieren 161
  Überwachungsoptionen für RTC-Dateilisten in andere Gruppen kopieren 158
  Überwachungsoptionen für TE-Dateilisten in andere Gruppen kopieren 160
  verwenden 146
  Voraussetzungen 143

H

Hardware-und Softwarevoraussetzungen 5
Hinweise zur Migration 109

I

IMC- und IMV-Module 129
Installation von PowerSC Standard Edition 7
installieren 7
Installieren 130
IP-Referrer 129
IP-Referrer in VIOS 135

K

Komponenten 127
Konfiguration von Trusted Logging 125
konfigurieren 131
Konformität mit Department of Defense-STIG 10
Konzepte 127

L

lsvfilt, Befehl 167

M

mkvfilt, Befehl 168

P

Patch Management 127
Patch-Management 128, 130
Patch Management-Server konfigurieren 132
Planung 108
pmconf 128
pmconf, Befehl 169
PowerSC 10, 90, 98, 101
  Real-Time Compliance 105
  Trusted Firewall
    gemeinsam genutzte Ethernet-Adapter entfernen 120
    installieren 117
    konfigurieren 118
    mit mehreren gemeinsam genutzten Ethernet-Adaptern konfigurieren 119
    Regeln erstellen 120
    Regeln inaktivieren 122
  Trusted Logging
    installieren 124
PowerSC-Sicherheits- und -Konformitätsautomation konfigurieren 101
PowerSC Standard Edition 5, 7
Protokoll 129
Protokolle anzeigen 135
Prüffunktion installieren 110
psconf, Befehl 173
pscuiserverctl, Befehl 181

R

Real-Time Compliance 105
Richtlinien verwalten 138
rmvfilt, Befehl 188

S

Server 127
Server konfigurieren 131
sichere Kommunikation 129
Sicherheit
  PowerSC
    Real-Time Compliance 105
SOX und COBIT 90
SUMA 127, 128, 130
System attestieren 110
System registrieren 110
Systeme löschen 111

T

Testen der Anwendungen 100
TNC 140
TNC-Client 128
TNC-Client aktualisieren 138
TNC-Komponenten verwalten 135
Trusted Boot 107, 108, 109, 110, 111, 112
Trusted Boot installieren 109
Trusted Boot konfigurieren 110
Trusted Boot-Konzepte 107
Trusted Boot verwalten 111
Trusted Firewall 115
  entfernen
    gemeinsam genutzte Ethernet-Adapter 120
  installieren 117
  konfigurieren 118
    mehrere gemeinsam genutzte Ethernet-Adapter 119
  Regeln erstellen 120
  Regeln inaktivieren 122
Trusted Firewall-Konzepte 115
Trusted Logging 123, 126
  installieren 124
Trusted Network Connect 127, 128, 129, 130, 131, 132, 135, 136, 137, 138
Trusted Network Connect-Server 134, 135
Trusted Network Connect und Patch Management 127

U

Übersicht 5, 127
Übersicht über Trusted Logging 123
Überwachung von Systemen auf kontinuierliche Konformität 101
Untersuchung einer fehlgeschlagenen Regel 99

V

Verifizierungsergebnisse anzeigen 137
Verwaltung der Automation von Sicherheit und Konformität 98, 100, 101
virtuelle Protokolle 123
virtuelle Protokolleinheiten anzeigen 123
vlantfw, Befehl 188
Voraussetzungen 108

Z

Zertifikate importieren 129, 138

Gedruckt in Deutschland