IBM PowerSC

Standard Edition

wersja 1.1.6

PowerSC Standard Edition

IBM PowerSC

Standard Edition

wersja 1.1.6

PowerSC Standard Edition

Uwaga

Przed wykorzystaniem informacji znajdujących się w tym podręczniku oraz produktu, którego one dotyczą, należy przeczytać informacje, które zawiera sekcja “Uwagi” na stronie 179.

Niniejsze wydanie dotyczy systemu IBM PowerSC Standard Edition 1.1.6 i wszystkich późniejszych wersji i modyfikacji, o ile nowe wydania nie wskazują inaczej.

Spis treści

Informacje o podręczniku

Ten dokument zawiera informacje dla administratorów systemów plików, systemu i bezpieczeństwa sieci.

Tekst wyróżniony

W dokumencie przyjęto następujące konwencje wyróżnienia tekstu:

Pogrubienie	Wyróżnia komendy, procedury, słowa kluczowe, pliki, struktury, katalogi i inne obiekty o nazwach predefiniowanych w systemie. Wyróżnia także obiekty graficzne, takie jak przyciski, etykiety i ikony, które wybiera użytkownik.
Kursywa	Wyróżnia parametry, których bieżące nazwy lub wartości mają zostać podane przez użytkownika.
Czcionka o stałej szerokości	Oznacza przykłady określonych wartości danych, przykłady tekstu podobnego do tego, który można zobaczyć na ekranie, przykłady fragmentów kodu programu, który mogą napisać programiści, komunikaty systemowe lub informacje, które należy wpisać.

Rozróżnianie wielkości liter w systemie AIX

W systemie AIX rozróżniane są wielkości liter, co oznacza, że system odróżnia wielkie litery od małych. Na przykład do przeglądania plików można użyć komendy **ls**. Jeśli wprowadzona zostanie komenda LS, system zwróci komunikat not found (nie znaleziono). Podobnie PLIK_A, Plik_A i plik_a są trzema różnymi plikami, nawet jeśli znajdują się w tym samym katalogu. Aby uniknąć niepożądanego działania systemu, należy zawsze upewnić się, że używana jest poprawna wielkość liter.

ISO 9000

Podczas tworzenia i rozwijania tego produktu używano systemów z certyfikatem jakości ISO 9000.

Nowości w produkcie PowerSC Standard Edition

Zapoznaj się z nowymi lub znacząco zmodyfikowanymi informacjami na temat produktu PowerSC Standard Edition.

W plikach PDF dla nowych i zmienionych informacji na lewym marginesie umieszczany jest znacznik modyfikacji (|).

Wrzesień 2017

W interfejsie graficznym PowerSC dodano następujące funkcje:

- Dodano panel kontrolny zabezpieczeń i zgodności na najwyższym poziomie pozwalający na szybkie określenie podsumowania statusu zgodności i integralności plików w czasie rzeczywistym.
- Dodano integrację z menedżerami wirtualizacji, takimi jak PowerVC, za pośrednictwem integracji Open Stack, co pozwala na zautomatyzowane i bezpieczne wykrywanie punktów końcowych. Dodatkowo integracja obsługuje środowisko w chmurze, z myślą o bezpieczeństwie od chwili utworzenia maszyny wirtualnej.
- Dodano funkcje raportowania, aby zapewnić obsługę kontroli. Raporty ogólne i szczegółowe dotyczące zgodności i integralności plików są obecnie dostępne zarówno w formacie HTML, jak i w formacie CSV. Raporty te mogą być rozsyłane na żądanie lub w regularnych odstępach czasu.
- Rozszerzony edytor profili zwiększa możliwość dostosowania reguł zgodności i profili. Teraz można łączyć reguły z wielu źródeł i edytować je w interfejsie graficznym.
- Dodano integrację z menedżerami informacji zdarzeń bezpieczeństwa, na przykład QRadar. Udostępnienie wpisów w dzienniku syslog w celu zachowania zgodności i zdarzeń integralności plików ułatwia integrację.
- Udoskonalona funkcja cofania zmian ułatwia wykonywanie złożonego zadania, jakim jest wycofywanie wdrożonego profilu. Produkt PowerSC 1.1.6 znacznie udoskonalono w celu zapewnienia bezproblemowej funkcji cofania dla profilu PCI.
- Poprawiono skalowalność interfejsu graficznego. Serwer interfejsu GUI jest teraz skalowalny horyzontalnie, każda instancja może obsłużyć 1000 lub więcej punktów końcowych.

Dodano następujące funkcje do komponentu TNCPM (Trusted Network Connect Patch Management):

- Wprowadzono obsługę serwera proxy, który zapewnia dodatkową warstwę bezpieczeństwa umożliwiającą odizolowanie TNCPM od sieci Internet.
- Integracja poprawek tymczasowych (iFixes) w TNCPM jest teraz w pełni automatyczna. TNCPM może monitorować i łatać błędy w systemie operacyjnym bez interwencji użytkownika.
- Pobieranie pakietów Open Source jest teraz zintegrowane z TNCPM.

Dodano następującą funkcję zwiększającą opcje zgodności:

- Dodano opcję raportowania, która udostępnia szczegółowe informacje na temat reguł w profilu w momencie jego zastosowania.

PowerSC Standard Edition - pliki PDF

Dokumentacja PowerSC Standard Edition dostępna jest w postaci plików PDF.

- PowerSC Standard Edititon
- PowerSC Standard Edition - Uwagi do wydania

Pojęcia dotyczące PowerSC Standard Edition

Ten przegląd produktu PowerSC Standard Edition zawiera opis jego funkcji, komponentów i obsługi sprzętu.

Produkt PowerSC Standard Edition umożliwia zabezpieczanie i kontrolę systemów operacyjnych znajdujących się w chmurze lub w wirtualnym centrum przetwarzania danych, udostępnia widok dla całego przedsiębiorstwa i udostępnia funkcje zarządzania. PowerSC Standard Edition jest zestawem składników, które obejmują automatyzację zabezpieczania i zgodności, zaufany start, zaufany firewall, zaufane rejestrowanie oraz zaufane połączenia z siecią i zarządzanie poprawkami. Technologia zabezpieczeń, która jest umieszczona w obrębie warstwy wirtualizacji, zapewnia dodatkowe zabezpieczenia dla systemów autonomicznych.

Poniższa tabela zawiera szczegółowe informacje na temat edycji, składników zawartych w edycjach, komponentów, a także sprzętu i procesorów, na którym każdy komponent jest dostępny.

Tabela 1. Komponenty produktu PowerSC Standard Edition, opisy, obsługa systemów operacyjnych i obsługiwany sprzęt

Komponenty	Opis	Obsługiwany system operacyjny	Obsługiwany sprzęt
Automatyzacja zabezpieczeń i zapewniania zgodności	Automatyzuje konfigurowanie, monitorowanie i kontrolowanie zabezpieczeń oraz zgodności dla następujących standardów: • Payment Card Industry Data Security Standard (PCI DSS) • Ustawa Sarbanes-Oxley i zgodność z COBIT (SOX/COBIT) • Departament Obrony USA (DoD) STIG • Ustawa Health Insurance Portability and Accountability Act (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
Zaufany start	Sprawdza kod startowy, system operacyjny i aplikacje oraz wykonuje atestację ich wiarygodności, wykorzystując wirtualny moduł TPM (Trusted Platform Module).	• AIX 6 z pakietem 6100-07 lub nowszy. • AIX 7 z pakietem 7100-01 lub nowszy.	POWER7 z oprogramowaniem wbudowanym eFW7.4 lub nowszym.
Zaufany firewall	Pozwala oszczędzić czas i zasoby umożliwiając bezpośredni routing ruchu sieciowego między wybranymi sieciami VLAN, którymi zarządza ten sam serwer serwer VIOS.	• AIX 6.1 • AIX 7.1 • AIX 7.2 • VIOS w wersji 2.2.1.4 lub nowszy.	• POWER6 • POWER7 • POWER8 • serwer VIOS wersja 6.1S lub nowszy.
Zaufane rejestrowanie	Dzienniki systemu AIX są w czasie rzeczywistym zapisywane na centralnym serwerze VIOS. Ten składnik pozwala na rejestrowanie zabezpieczone przed manipulacją i umożliwia wygodne zarządzanie dziennikami oraz tworzenie ich kopii zapasowych.	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8

Tabela 1. Komponenty produktu PowerSC Standard Edition, opisy, obsługa systemów operacyjnych i obsługiwany sprzęt (kontynuacja)

Komponenty	Opis	Obsługiwany system operacyjny	Obsługiwany sprzęt
Sieć zaufana (TNC) i zarządzanie poprawkami	Sprawdza, czy wszystkie systemy AIX w środowisku wirtualnym mają wymagane poziomy oprogramowania oraz poprawek i udostępnia narzędzia do zarządzania umożliwiające zapewnienie, że wszystkie systemy AIX mają określony poziom oprogramowania. Wysyła alerty, jeśli do sieci jest podłączany system z nieaktualnym oprogramowaniem lub jeśli wydano poprawka dotyczącą zabezpieczeń, która dotyczy używanych systemów.	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
Klient połączenia z zaufaną siecią	Klient zaufanej sieci wymaga w systemie operacyjnym jednego z następujących komponentów:	• AIX 6.1 z pakietem 6100-06 lub nowszy. • Konsola systemowa SUMA (Service Update Management Assistant) dla systemu AIX w wersji 7.1, jeśli do zarządzania poprawkami jest używane środowisko SUMA. • Konsola systemowa SUMA (Service Update Management Assistant) dla systemu AIX w wersji 7.2.1, jeśli do zarządzania poprawkami jest używane środowisko SUMA.	

instalowanie produktu PowerSC Standard Edition 1.1.3

Należy zainstalować zestaw plików dla każdej z wybranych funkcji produktu PowerSC Standard Edition.

Poniższe zestawy plików są dostępne dla produktu PowerSC Standard Edition i graficznego interfejsu użytkownika produktu PowerSC:

- powerscStd.ice: Instalowany w systemach AIX, które wymagają funkcji automatyzacji zabezpieczeń i zgodności produktu PowerSC Standard Edition. Program zgodności wymaga co najmniej 5 MB wolnego miejsca na dysku w systemie plików "/".
- powerscStd.vtpm: Instalowany w systemach AIX, które wymagają funkcji zaufanego startu produktu PowerSC Standard Edition. Zestaw plików powerscStd.vtpm można skopiować z podstawowego nośnika systemu AIX albo z serwisu https://www-01.ibm.com/marketing/iwm/iwm/web/preLogin.do?source=aixbp&S_PKG=vtpm.
- powerscStd.vlog: Instalowany w systemach AIX, które wymagają funkcji zaufanego rejestrowania produktu PowerSC Standard Edition.
- powerscStd.tnc_pm: Instalowany w systemach AIX wersja 7.1 TL4 lub nowszych za pomocą systemu konsoli SUMA (Service Update Management Assistant) w środowisku SUMA do zarządzania poprawkami na poziomie 7.2.1.0. Program curl 7.52.1-1 powinien być zainstalowany w programie TNC Patch Manager w celu umożliwienia bezpiecznego przesyłania poprawek ifixes z serwisu IBM Security Site.
- powerscStd.svm: Instalowany w systemach AIX, które mogą wymagać funkcji routingu obsługiwanej przez produkt PowerSC Standard Edition.
- powerscStd.rtc: Instalowany w systemach AIX, które wymagają funkcji RTC (Real Time Compliance) produktu PowerSC Standard Edition.
- powerscStd.uiAgent.rte: Instalowany w systemach AIX, które będą zarządzane z użyciem graficznego interfejsu użytkownika produktu PowerSC. Zestaw plików powerscStd.ice 115 lub nowszy jest wymagany do zainstalowania install powerscStd.uiAgent.rte 116.
- powerscStd.uiServer.rte: Instalowany w systemie AIX skonfigurowanym do uruchamiania serwera graficznego interfejsu użytkownika produktu PowerSC.

Produkt PowerSC Standard Edition i graficzny interfejs użytkownika produktu PowerSC można zainstalować, używając jednego z następujących interfejsów:

- Komenda **installp** w interfejsie wiersza komend (CLI).
- Interfejs SMIT.

Aby zainstalować produkt PowerSC Standard Edition za pomocą interfejsu SMIT, wykonaj następujące kroki:

1. Wprowadź następującą komendę:
   ```
   % smitty installp
   ```
2. Wybierz opcję **Instalacja oprogramowania**.
3. Wybierz urządzenie wejściowe lub katalog dla oprogramowania, aby wskazać plik instalacyjny w obrazie instalacyjnym produktu IBM Compliance Expert. Na przykład, jeśli obraz instalacyjny zawiera ścieżkę katalogu i nazwę pliku /usr/sys/inst.images/powerscStd.vtpm, należy podać tę ścieżkę pliku w polu **INPUT**.
4. Wyświetl i zaakceptuj umowę licencyjną. Zaakceptuj umowę licencyjną, przewijając ją za pomocą strzałki w dół i wybierając opcję **ZAAKCEPTUJ nową umowę licencyjną**, a następnie naciskając klawisz Tab, aby zmienić wartość na **Tak**.
5. Naciśnij klawisz **Enter**, aby rozpocząć instalację.
6. Sprawdź po zakończeniu instalacji, czy statusem komendy jest **OK**.

Więcej informacji na temat instalowania graficznego interfejsu użytkownika produktu PowerSC zawiera sekcja “Instalowanie interfejsu GUI produktu PowerSC” na stronie 135.

Wyświetlanie licencji na oprogramowanie

Licencję na oprogramowanie można wyświetlić w interfejsie CLI za pomocą następującej komendy:

```
% installp –lE –d ścieżka/nazwa_pliku
```

Gdzie *ścieżka/nazwa_pliku* określa obraz instalacyjny produktu PowerSC Standard Edition.

Na przykład można wpisać następującą komendę przy użyciu interfejsu CLI, aby określić informacje dotyczące licencji powiązanych z produktem PowerSC Standard Edition:

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

Pojęcia pokrewne:

“Pojęcia dotyczące PowerSC Standard Edition” na stronie 5
Ten przegląd produktu PowerSC Standard Edition zawiera opis jego funkcji, komponentów i obsługi sprzętu.

“Instalowanie zaufanego startu” na stronie 101
Istnieją wymagane konfiguracje sprzętu i oprogramowania, które są niezbędne do zainstalowania zaufanego startu.

Zadania pokrewne:

“Instalowanie zaufanego firewalla” na stronie 109
Instalowanie mechanizmu zaufanego firewalla w systemie PowerSC jest podobne do instalowania innych funkcji w tym systemie.

“Instalowanie zaufanego rejestrowania” na stronie 116
Funkcję zaufanego rejestrowania PowerSC można zainstalować za pomocą interfejsu wiersza komend lub narzędzia SMIT.

“Konfigurowanie komponentów TNC” na stronie 122
Każdy komponent TNC (Trusted Network Connect) wymaga pewnej konfiguracji, aby mógł działać w danym środowisku.

Automatyzacja zabezpieczeń i zapewniania zgodności

AIX Profile Manager zarządza predefiniowanymi profilami na potrzeby bezpieczeństwa i zgodności. PowerSC Real Time Compliance w sposób ciągły monitoruje włączone systemy AIX, aby zapewnić, że są one skonfigurowane w sposób spójny i bezpieczny.

Profile XML automatyzują rekomendowaną konfigurację systemu AIX firmy IBM w celu zapewnienia spójności ze standardami Payment Card Data Security Standard, Sarbanes-Oxley Act, U.S. Department of Defense UNIX Security Technical Implementation Guide i Health Insurance Portability and Accountability Act (HIPAA). Organizacje, które przestrzegają standardów bezpieczeństwa, muszą używać predefiniowanych ustawień zabezpieczeń systemów.

AIX Profile Manager działa jako wtyczka programu IBM® Systems Director, która upraszcza stosowanie ustawień zabezpieczeń, monitorowanie ustawień zabezpieczeń i kontrolę ustawień zabezpieczeń dla systemu operacyjnego AIX i systemów serwer VIOS (VIOS). Aby używać funkcji zapewniania zgodności, aplikacja PowerSC musi być zainstalowana w systemach zarządzanych AIX, które spełniają standardy bezpieczeństwa. Funkcja automatyzacji zabezpieczeń i zapewniania zgodności znajduje się w komponencie PowerSC Standard Edition.

Pakiet instalacyjny komponentu PowerSC Standard Edition, 5765-PSE, musi być zainstalowany w systemach zarządzanych AIX. Ten pakiet instalacyjny instaluje zestaw plików powerscStd.ice, który można zaimplementować w systemie za pomocą programu AIX Profile Manager lub komendy **pscxpert**. Program PowerSC z programem IBM Compliance Expert Express (ICEE) obsługują zarządzanie profilami XML i ich rozwijanie. Profilami XML zarządza program AIX Profile Manager.

Uwaga: Przed zastosowaniem profilu bezpieczeństwa w systemie należy zainstalować wszystkie aplikacje.

Koncepcje automatyzacji zabezpieczeń i zapewniania zgodności

Funkcja zabezpieczeń i zapewniania zgodności należąca do programu PowerSC to zautomatyzowana metoda konfigurowania i kontrolowania systemów AIX zgodnie ze standardami Security Technical Implementation Guide (STIG) Departamentu Obrony Stanów Zjednoczonych (DoD), standardem bezpieczeństwa danych Data Security Standard (DSS) Payment Card Industry (PCI), standardem zgodności Sarbanes-Oxley Act i COBIT (SOX/COBIT) i standardem Health Insurance Portability and Accountability Act (HIPAA).

Program PowerSC ułatwia automatyzację konfigurowania i monitorowania systemów, które muszą być zgodne ze standardem bezpieczeństwa danych (DSS) Payment Card Industry (PCI) w wersji 1.2, 2.0 lub 3.0. Dlatego funkcja zabezpieczeń i zapewniania zgodności należąca do programu PowerSC jest dokładną i kompletną metodą automatyzacji konfiguracji zabezpieczeń, która jest używana w celu spełnienia wymagań zgodności IT ze standardem STIG departamentu DoD w systemie UNIX, standardem PCI DSS, standardem Sarbanes-Oxley Act i COBIT (SOX/COBIT), a także standardem Health Insurance Portability and Accountability Act (HIPAA).

Uwaga: Funkcja zabezpieczeń i zapewniania zgodności programu PowerSC aktualizuje istniejące profile XML, które są używane przez program IBM Compliance Expert Express (ICEE). Profili XML programu PowerSC Standard Edition można używać za pomocą komendy **pscxpert** – podobnie do programu ICEE.

Wstępnie skonfigurowane profile zgodności dostarczane z programem PowerSC Standard Edition zmniejszają nakład pracy administracyjnej związanej z interpretowaniem dokumentacji dotyczącej zgodności i implementowaniem standardów jako konkretnych parametrów konfiguracji systemów. Technologia ta zmniejsza koszty konfigurowania zgodności i kontroli poprzez automatyzację procesów. IBMPowerSC Standard Edition zaprojektowano do efektywnego zarządzania wymaganiami systemu dotyczącymi zgodności ze standardami zewnętrznymi, co potencjalnie obniża koszty i zwiększa zgodność.

Zgodność z normą STIG Departamentu Obrony

Departament Obrony USA (DoD) wymaga bardzo bezpiecznych systemów komputerowych. Jakość i obsługa klienta systemu AIX na serwerze Power Systems spełniają poziom bezpieczeństwa i jakości zdefiniowane przez Departament Obrony.

Bezpieczny system operacyjny, taki jak AIX, musi być odpowiednio skonfigurowany w celu osiągnięcia określonych celów zabezpieczeń. Departament Obrony ujął niezbędne konfiguracje bezpieczeństwa wszystkich systemów operacyjnych w dyrektywie 8500.1. W tej dyrektywie określono strategie i przypisano odpowiedzialność agencji ochrony informacji obrony USA (DISA) za zapewnienie wytycznych dotyczących konfiguracji bezpieczeństwa.

Agencja DISA opracowała zasady i wytyczne w procedurach STIG systemu UNIX (Security Technical Implementation Guide), udostępniającego środowisko co najmniej spełniające wymagania w zakresie bezpieczeństwa systemów Departamentu Obrony działających na poziomie poufności II kategorii MAC, które zawiera informacje poufne. Departament Obrony USA ma rygorystyczne wymagania w zakresie bezpieczeństwa informatycznego i wyliczone szczegóły dotyczące wymaganych ustawień konfiguracji, aby zapewnić bezpieczne działanie systemu. Użytkownik może wykorzystać wymagane porady eksperta. Produkt PowerSC Standard Edition pomaga zautomatyzować proces konfigurowania ustawień zgodnie z definicją Departamentu Obrony.

Uwaga: Wszystkie niestandardowe pliki skryptowe dostarczone w celu zachowania zgodności z wymaganiami Departamentu Obrony znajdują się w katalogu /etc/security/pscexpert/dodv2.

PowerSC Standard Edition obsługuje wymagania wersji 1 wydania 2 procedur STIG Departamentu Obrony systemu AIX. Podsumowanie wymagań oraz sposób zapewnienia tej zgodności są przedstawione w tabelach poniżej.

Tabela 2. Ogólne wymagania Departamentu Obrony

Identyfikator punktu kontrolnego STIG Departamentu Obrony	**Kategoria reguły STIG**	**Opis**	**Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność**
AIX00020	2	Musi zostać zaimplementowane oprogramowanie Zaufana Baza Przetwarzania AIX.	**Położenie** /etc/security/pscexpert/dodv2/trust **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
AIX00040	2	Musi zostać użyta komenda **securetcpip**.	**Położenie** /etc/security/pscexpert/dodv2/dodsecuretcpip **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
AIX00060	2	Co tydzień należy sprawdzać system pod kątem nieautoryzowanych plików setuid oraz nieautoryzowanych modyfikacji autoryzowanych plików setuid.	**Położenie** /etc/security/pscexpert/dodv2/trust **Działanie zgodności** Sprawdza co tydzień, aby zidentyfikować zmiany podanych plików.
AIX00080	1	Dla żadnego konta nie można ustawić atrybutu SYSTEM na wartość *none*.	**Położenie** /etc/security/pscexpert/dodv2/SYSattr **Działanie zgodności** Zapewnia, że podany atrybut jest ustawiany na wartość inną niż *none*. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	**Kategoria reguły STIG**	**Opis**	**Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność**
AIX00200	2	System nie może zezwolić na przejście przez bramę bezpośredniego rozgłaszania.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej direct_broadcast na *0*.
AIX00210	2	System musi zapewnić ochronę przed atakami ICMP w połączeniach TCP.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej tcp_icmpsecure na *1*.
AIX00220	2	System musi zapewnić ochronę stosu TCP przed atakami resetowania połączenia, synchronizacji (SYN) i wprowadzania danych.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Zapewnia, że wartość opcji sieciowej tcp_tcpsecure jest ustawiona na wartość *7*.
AIX00230	2	System musi zapewnić ochronę przed atakami fragmentacji IP.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej ip_nfrag na *200*.
AIX00300	1,2,3	System nie może mieć aktywnej usługi bootp.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza podaną usługę.
AIX00310	2	Musi istnieć plik /etc/ftpaccess.ctl.	**Położenie** /etc/security/pscexpert/dodv2/dodv2loginherald **Działanie zgodności** Zapewnia, że plik istnieje.
GEN000020	2	System musi wymagać uwierzytelniania podczas uruchamiania w trybie pojedynczego użytkownika.	**Położenie** /etc/security/pscexpert/dodv2/rootpasswd_home **Działanie zgodności** Zapewnia, że konto użytkownika root każdej partycji startowej ma hasło w pliku /etc/security/passwd. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN000100	1	System operacyjny musi być w obsługiwanej wersji.	**Położenie** /etc/security/pscexpert/dodv2/dodv2cat1 **Działanie zgodności** Wyświetla wyniki testów podanej reguły.
GEN000120	2	Muszą zostać zainstalowane najbardziej aktualne poprawki dotyczące bezpieczeństwa systemu i aktualizacje.	**Położenie** /usr/sbin/instfix -i /etc/security/pscexpert/dodv2/dodv2cat1 **Działanie zgodności** Skonfiguruj za pomocą funkcji Trusted Network Connect.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN000140	2	Co tydzień należy sprawdzać system pod kątem nieautoryzowanych plików setuid oraz nieautoryzowanych modyfikacji autoryzowanych plików setuid.	**Położenie** /etc/security/pscexpert/dodv2/trust **Działanie zgodności** Sprawdza co tydzień, aby zidentyfikować zmiany podanych plików.
GEN000220	2	Co tydzień należy sprawdzać system pod kątem nieautoryzowanych plików setuid oraz nieautoryzowanych modyfikacji autoryzowanych plików setuid.	**Położenie** /etc/security/pscexpert/dodv2/trust **Działanie zgodności** Sprawdza co tydzień, aby zidentyfikować zmiany podanych plików.
GEN000240	2	Zegar systemowy musi być zsynchronizowany z autorytatywnym źródłem czasu Departamentu Obrony USA.	**Położenie** /etc/security/pscexpert/dodv2/dodv2cmntrows **Działanie zgodności** Zapewnia, że zegar systemowy jest zgodny.
GEN000241	2	Zegar systemowy musi być synchronizowany w sposób ciągły lub przynajmniej raz dziennie.	**Położenie** /etc/security/pscexpert/dodv2/dodv2cmntrows **Działanie zgodności** Zapewnia, że zegar systemowy jest zgodny.
GEN000242	2	Do synchronizacji zegara system musi używać co najmniej dwóch źródeł czasu.	**Położenie** /etc/security/pscexpert/dodv2/dodv2netrules **Działanie zgodności** Zapewnia, że do synchronizacji zegara jest używane więcej niż jedno źródło czasu.
GEN000280	2	Nie mogą być dozwolone bezpośrednie operacje logowania na następujące typy kont: • aplikacji • domyślnych • współużytkowanych • programów narzędziowych	**Położenie** /etc/security/pscexpert/dodv2/lockacc_rlogin **Działanie zgodności** Zapobiega bezpośrednim operacjom logowania na podane konta.
GEN000290	2	System nie może zawierać zbędnych kont.	**Położenie** /etc/security/pscexpert/dodv2/lockacc_rlogin **Działanie zgodności** Zapewnia, że nie ma nieużywanych kont.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	**Kategoria reguły STIG**	**Opis**	**Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność**
GEN000300 (dotyczy GEN000320, GEN000380, GEN000880)	2	Wszystkie konta w systemie muszą mieć unikalne nazwy użytkowników lub kont oraz unikalne hasła użytkowników lub kont.	**Położenie** /etc/security/pscexpert/dodv2/grpusrpass_chk **Działanie zgodności** Zapewnia, że wszystkie konta spełniają określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN000320 (dotyczy GEN000300, GEN000380, GEN000880)	2	Wszystkie konta w systemie muszą mieć unikalne nazwy użytkowników lub kont oraz unikalne hasła użytkowników lub kont.	**Położenie** /etc/security/pscexpert/dodv2/grpusrpass_chk **Działanie zgodności** Zapewnia, że wszystkie konta spełniają określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN000340	2	Identyfikatory użytkowników (UID) i identyfikatory grup (GID), które są zastrzeżone dla kont systemowych, nie mogą zostać przypisane do kont innych niż systemowe lub grup innych niż systemowe.	**Położenie** /etc/security/pscexpert/dodv2/account **Działanie zgodności** To ustawienie jest automatycznie włączone, aby wymusić tę regułę.
GEN000360	2	Identyfikatory UID i identyfikatory GID, które są zastrzeżone dla kont systemowych, nie mogą zostać przypisane do kont innych niż systemowe lub grup innych niż systemowe.	**Położenie** /etc/security/pscexpert/dodv2/account **Działanie zgodności** To ustawienie jest automatycznie włączone, aby wymusić tę regułę.
GEN000380 (dotyczy GEN000300, GEN000320, GEN000880)	2	Wszystkie konta w systemie muszą mieć unikalne nazwy użytkowników lub kont oraz unikalne hasła użytkowników lub kont.	**Położenie** /etc/security/pscexpert/dodv2/grpusrpass_chk **Działanie zgodności** Zapewnia, że wszystkie konta spełniają określone wymagania.
GEN000400	2	Baner logowania Departamentu Obrony musi zostać wyświetlony bezpośrednio przed zachętami logowania konsoli lub jako ich część.	**Położenie** /etc/security/pscexpert/dodv2/dodv2loginherald **Działanie zgodności** Wyświetla wymagany baner.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN000402	2	Baner logowania Departamentu Obrony musi zostać wyświetlony bezpośrednio przed zachętami logowania graficznego środowiska pulpitu lub jako ich część.	**Położenie** /etc/security/pscexpert/dodv2/dodv2loginherald **Działanie zgodności** Baner logowania jest ustawiony na baner Departamentu Obrony.
GEN000410	2	Usługa FTPS (File Transfer Protocol over SSL) lub FTP (File Transfer Protocol) w systemie musi być skonfigurowana z banerem logowania Departamentu Obrony.	**Położenie** /etc/security/pscexpert/dodv2/dodv2loginherald **Działanie zgodności** Wyświetla baner, gdy używany jest protokół FTP.
GEN000440	2	Konieczne jest rejestrowanie zakończonych powodzeniem i zakończonych niepowodzeniem prób logowania i wylogowania.	**Położenie** /etc/security/pscexpert/dodv2/loginout **Działanie zgodności** Włącza wymagane rejestrowanie.
GEN000452	2	W momencie logowania system musi wyświetlić datę i godzinę ostatniego pomyślnego logowania na konto.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Wyświetla wymagane informacje.
GEN000460	2	Ta reguła powoduje wyłączenie konta po trzech kolejnych nieudanych próbach logowania.	**Położenie** /etc/security/pscexpert/dodv2/chusrattrdod **Działanie zgodności** Ustawia limit prób logowania na podaną wartość.
GEN000480	2	Ta reguła ustawia czas opóźnienia logowania na 4 sekundy.	**Położenie** /etc/security/pscexpert/dodv2/chdefstanzadod **Działanie zgodności** Ustawia czas opóźnienia logowania na wymaganą wartość.
GEN000540	2	Ta reguła zapewnia, że globalne pliki konfiguracyjne haseł w systemie są konfigurowane zgodnie z wymaganiami dotyczącymi haseł.	**Położenie** /etc/security/pscexpert/dodv2/chusrattrdod **Działanie zgodności** Ustawia wymagane ustawienia haseł.
GEN000560	1	Wszystkie konta w systemie muszą mieć poprawne hasła.	**Położenie** /etc/security/pscexpert/dodv2/grpusrpass_chk **Działanie zgodności** Zapewnia, że konta mają hasła.
GEN000580	2	Ta reguła zapewnia, że wszystkie hasła zawierają przynajmniej 14 znaków.	**Położenie** /etc/security/pscexpert/dodv2/chusrattrdod **Działanie zgodności** Ustawia minimalną długość hasła na 14 znaków.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN000585	2	W systemie do generowania zakodowanych haseł kont musi być używany szyfrujący algorytm mieszający zgodny ze standardem FIPS 140-2.	**Położenie** /etc/security/pscexpert/dodv2/fipspasswd **Działanie zgodności** Zapewnia, że kodowanie mieszające haseł używa zatwierdzonego algorytmu mieszającego.
GEN000590	2	W systemie do generowania zakodowanych haseł kont musi być używany szyfrujący algorytm mieszający zgodny ze standardem FIPS 140-2.	**Położenie** /etc/security/pscexpert/dodv2/fipspasswd **Działanie zgodności** Zapewnia, że kodowanie mieszające haseł używa zatwierdzonego algorytmu mieszającego.
GEN000595	2	Podczas generowania zakodowanych haseł przechowywanych w systemie musi być używany algorytm mieszający zgodny ze standardem FIPS 140-2.	**Położenie** /etc/security/pscexpert/dodv2/fipspasswd **Działanie zgodności** Zapewnia, że kodowanie mieszające haseł używa zatwierdzonego algorytmu mieszającego.
GEN000640	2	Ta reguła wymaga w haśle co najmniej jednego znaku spoza alfabetu.	**Położenie** /etc/security/pscexpert/dodv2/chusrattrdod **Działanie zgodności** Ustawia minimalną liczbę znaków spoza alfabetu, które musi zawierać hasło, na wartość 1.
GEN000680	2	Ta reguła zapewnia, że hasła nie zawierają więcej niż trzy kolejno powtarzające się znaki.	**Położenie** /etc/security/pscexpert/dodv2/chusrattrdod **Działanie zgodności** Ustawia maksymalną liczbę powtarzających się znaków w haśle na wartość 3.
GEN000700	2	Ta reguła zapewnia, że globalne pliki konfiguracyjne haseł w systemie są konfigurowane zgodnie z wymaganiami dotyczącymi haseł.	**Położenie** /etc/security/pscexpert/dodv2/chusrattrdod **Działanie zgodności** Zapewnia, że pliki konfiguracyjne hasła spełniają wymagania.
GEN000740	2	Wszystkie hasła kont przetwarzania innego niż interaktywne i przetwarzania zautomatyzowanego muszą być zablokowane (GEN000280). Bezpośrednie logowania nie mogą być dozwolone do kont współużytkowanych, domyślnych, aplikacji lub programów narzędziowych. (GEN002640) Domyślne konta systemowe muszą być wyłączone lub usunięte.	**Położenie** /etc/security/pscexpert/dodv2/loginout /etc/security/pscexpert/dodv2/lockacc_rlogin **Działanie zgodności** To ustawienie jest automatycznie włączone.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN000740	2	Wszystkie hasła kont przetwarzania innego niż interaktywne i przetwarzania zautomatyzowanego muszą być zmieniane co najmniej raz na rok lub zostać zablokowane.	**Położenie** /etc/security/pscexpert/dodv2/lockacc_rlogin **Działanie zgodności** Zapewnia, że podane hasła są zmieniane raz w roku lub zablokowane.
GEN000750	2	Ta reguła wymaga, aby nowe hasła zawierały przynajmniej 4 znaki, które nie znajdowały się w starym haśle.	**Położenie** /etc/security/pscexpert/dodv2/chusrattrdod **Działanie zgodności** Ustawia minimalną liczbę nowych znaków wymaganych w nowym haśle na wartość 4.
GEN000760	2	Konta muszą zostać zablokowane po 35 dniach nieaktywności.	**Położenie** /etc/security/pscexpert/dodv2/disableacctdod **Działanie zgodności** Blokuje konta po 35 dniach braku aktywności.
GEN000790	2	System musi uniemożliwić użycie jako haseł słów ze słownika.	**Położenie** /etc/security/pscexpert/dodv2/chuserstanzadod **Działanie zgodności** Zapewnia, że ustawiane domyślne hasło nie jest słabe.
GEN000800	2	Ta reguła zapewnia, że ostatnich pięć haseł nie może zostać ponownie wykorzystane.	**Położenie** /etc/security/pscexpert/dodv2/chusrattrdod **Działanie zgodności** Zapewnia, że nowe hasło nie jest takie samo, jak którekolwiek z ostatnich 5 haseł.
GEN000880 (dotyczy GEN000300, GEN000320, GEN000380)	2	Wszystkie konta w systemie muszą mieć unikalne nazwy użytkowników lub kont oraz unikalne hasła użytkowników lub kont.	**Położenie** /etc/security/pscexpert/dodv2/grpusrpass_chk **Działanie zgodności** Zapewnia, że wszystkie konta spełniają określone wymagania.
GEN000900	3	Katalogiem osobistym użytkownika root nie może być katalog główny (/).	**Położenie** /etc/security/pscexpert/dodv2/rootpasswd_home **Działanie zgodności** Zapewnia, że system spełnia określone wymaganie. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN000940	2	Ścieżka wyszukiwania plików wykonywalnych konta użytkownika root musi być ścieżką domyślną dostawcy i może zawierać tylko ścieżki bezwzględne.	**Położenie** /etc/security/pscexpert/dodv2/fixpathvars **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	**Kategoria reguły STIG**	**Opis**	**Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność**
GEN000945	2	Ścieżka wyszukiwania biblioteki konta użytkownika root musi być domyślną ścieżką systemową i może zawierać tylko ścieżki bezwzględne.	**Położenie** /etc/security/pscexpert/dodv2/fixpathvars **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN000950	2	Lista wstępnie ładowanych bibliotek konta użytkownika root musi być pusta.	**Położenie** /etc/security/pscexpert/dodv2/fixpathvars **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN000960 (dotyczy GEN003000, GEN003020, GEN003160, GEN003360, GEN003380)	2	Konto użytkownika nie może zawierać w swojej ścieżce wyszukiwania kodu wykonywalnego katalogów dostępnych do zapisu przez wszystkich.	**Położenie** /etc/security/pscexpert/dodv2/rmwwpaths **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN000980	2	System musi uniemożliwić bezpośrednie logowanie na y konto użytkownika root z wyjątkiem konsoli systemowej.	**Położenie** /etc/security/pscexpert/dodv2/chuserstanzadod **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN001000	2	Konsole zdalne muszą być wyłączone lub zabezpieczone przed dostępem bez uprawnień.	**Położenie** /etc/security/pscexpert/dodv2/remoteconsole **Działanie zgodności** Zapewnia, że podane konsole są wyłączone.
GEN001020	2	Nie można użyć konta użytkownika root do bezpośredniego logowania.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Wyłącza bezpośrednie logowanie na konto użytkownika root.
GEN001060	2	System musi rejestrować w dzienniku zakończone powodzeniem i niepowodzeniem próby uzyskania dostępu do konta użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/loginout **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN001100	1	Hasła użytkownika root nie mogą być nigdy przekazywane w sieci w postaci tekstowej.	**Położenie** /etc/security/pscexpert/dodv2/chuserstanzadod **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN001120	2	System nie może zezwolić na logowanie użytkownika root za pomocą protokołu SSH.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Wyłącza logowanie użytkownika root dla protokołu SSH.
GEN001440	3	Wszyscy interaktywni użytkownicy muszą mieć przypisany katalog osobisty w pliku /etc/passwd.	**Położenie** /etc/security/pscexpert/dodv2/grpusrpass_chk **Działanie zgodności** Zapewnia, że wszyscy użytkownicy interaktywni mają podane katalogi.
GEN001475	2	Plik /etc/group nie może zawierać żadnych zakodowanych haseł grup.	**Położenie** /etc/security/pscexpert/dodv2/passwdhash **Działanie zgodności** Zapewnia, że nie ma żadnych zakodowanych haseł grup w podanym pliku. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001600	2	Ścieżki wyszukiwania kodu wykonywalnego skryptów sterujących uruchamianiem muszą zawierać jedynie ścieżki bezwzględne.	**Położenie** /etc/security/pscexpert/dodv2/fixpathvars **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001605	2	Ścieżki wyszukiwania biblioteki skryptów sterujących uruchamianiem muszą zawierać jedynie ścieżki bezwzględne.	**Położenie** /etc/security/pscexpert/dodv2/fixpathvars **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001610	2	Listy wstępnie ładowanych bibliotek skryptów sterujących uruchamianiem muszą zawierać jedynie ścieżki bezwzględne.	**Położenie** /etc/security/pscexpert/dodv2/fixpathvars **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN001840	2	Ścieżki wyszukiwania kodu wykonywalnego wszystkich globalnych plików inicjowania muszą zawierać jedynie ścieżki bezwzględne.	**Położenie** /etc/security/pscexpert/dodv2/fixpathvars **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001845	2	Ścieżki wyszukiwania biblioteki wszystkich globalnych plików inicjowania muszą zawierać jedynie ścieżki bezwzględne.	**Położenie** /etc/security/pscexpert/dodv2/fixpathvars **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001850	2	Listy wstępnie ładowanych bibliotek wszystkich globalnych plików inicjowania muszą zawierać jedynie ścieżki bezwzględne.	**Położenie** /etc/security/pscexpert/dodv2/fixpathvars **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001900	2	Ścieżki wyszukiwania kodu wykonywalnego wszystkich lokalnych plików inicjowania muszą zawierać jedynie ścieżki bezwzględne.	**Położenie** /etc/security/pscexpert/dodv2/fixpathvars **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001901	2	Ścieżki wyszukiwania biblioteki wszystkich lokalnych plików inicjowania muszą zawierać jedynie ścieżki bezwzględne.	**Położenie** /etc/security/pscexpert/dodv2/fixpathvars **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001902	2	Listy wstępnie ładowanych bibliotek wszystkich lokalnych plików inicjowania muszą zawierać jedynie ścieżki bezwzględne.	**Położenie** /etc/security/pscexpert/dodv2/fixpathvars **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN001940	2	Pliki inicjowania użytkowników nie mogą uruchamiać programów dostępnych do zapisu przez wszystkich.	**Położenie** /etc/security/pscexpert/dodv2/rmwwpaths **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN001980	2	Pliki .rhosts, .shosts, hosts.equiv, shosts.equiv, /etc/passwd, /etc/shadow i /etc/group nie mogą zawierać znaku plus (+) bez zdefiniowania wpisów dla grup sieciowych NIS+.	**Położenie** /etc/security/pscexpert/dodv2/dodv2netrules **Działanie zgodności** Zapewnia, że podane pliki spełniają podane wymagania.
GEN002000	2	W systemie nie może być żadnych plików .netrc.	**Położenie** /etc/security/pscexpert/dodv2/dodv2netrules **Działanie zgodności** Zapewnia, że w systemie nie ma żadnego z podanych plików. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN002020	2	Wszystkie pliki .rhosts, .shosts i hosts.equiv muszą zawierać tylko zaufane pary host-użytkownik.	**Położenie** /etc/security/pscexpert/dodv2/dodv2netrules **Działanie zgodności** Zapewnia, że podane pliki spełniają to wymaganie.
GEN002040	1	Ta reguła wyłącza pliki .rhosts, .shosts i hosts.equiv lub shosts.equiv.	**Położenie** /etc/security/pscexpert/dodv2/mvhostsfilesdod **Działanie zgodności** Wyłącza podane pliki.
GEN002120	1,2	Ta reguła sprawdza i konfiguruje powłoki użytkownika.	**Położenie** /etc/security/pscexpert/dodv2/usershells **Działanie zgodności** Tworzy wymagane powłoki. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN002140	1,2	Wszystkie powłoki, które są przywoływane na liście /etc/passwd, muszą być wymienione w pliku /etc/shells. Wyjątkiem są powłoki podane w celu uniemożliwienia logowania.	**Położenie** /etc/security/pscexpert/dodv2/usershells **Działanie zgodności** Zapewnia, że powłoki są wymienione w odpowiednich plikach. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN002280	2	Pliki i katalogi urządzenia muszą być dostępne do zapisu tylko dla użytkowników z kontem systemowym lub tak jak system jest skonfigurowany przez dostawcę.	**Położenie** /etc/security/pscexpert/dodv2/wwdevfiles **Działanie zgodności** Wyświetla pliki, katalogi i inne pozostałe pliki w systemie znajdujące się w katalogach innych niż publiczne, które są dostępne do zapisu przez wszystkich.
GEN002300	2	Pliki urządzeń używane do tworzenia kopii zapasowych muszą być dostępne do odczytu, zapisu lub odczytu i zapisu tylko przez użytkownika root lub użytkownika kopii zapasowej.	**Położenie** /etc/security/pscexpert/dodv2/wwdevfiles **Działanie zgodności** Wyświetla pliki, katalogi i inne pozostałe pliki w systemie znajdujące się w katalogach innych niż publiczne, które są dostępne do zapisu przez wszystkich.
GEN002400	2	Co tydzień należy sprawdzać system pod kątem nieautoryzowanych plików setuid oraz nieautoryzowanych modyfikacji autoryzowanych plików setuid.	**Położenie** /etc/security/pscexpert/dodv2/trust **Działanie zgodności** Sprawdza co tydzień, aby zidentyfikować zmiany podanych plików. **Uwaga:** Porównanie dwóch najnowszych dzienników tygodniowych, które są tworzone w katalogu /var/security/pscexpert, w celu zweryfikowania, że nie miało miejsce żadne nieuprawnione działanie.
GEN002420	2	Nośniki wymienne, zdalne systemy plików i wszystkie systemy plików, które nie zawierają zatwierdzonych plików setuid, muszą być podłączane z użyciem opcji *nosuid*.	**Położenie** /etc/security/pscexpert/dodv2/fsmntoptions **Działanie zgodności** Zapewnia, że zdalnie podłączane systemy plików mają podane opcje. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN002430	2	Nośniki wymienne, zdalne systemy plików i wszystkie systemy plików, które nie zawierają zatwierdzonych plików urządzenia, muszą być podłączane z użyciem opcji *nodev*.	**Położenie** /etc/security/pscexpert/dodv2/fsmntoptions **Działanie zgodności** Zapewnia, że zdalnie podłączane systemy plików mają podane opcje. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN002480	2	Katalogi publiczne muszą być jedynymi katalogami dostępnymi do zapisu dla wszystkich, a pliki dostępne do zapisu dla wszystkich muszą znajdować się tylko w katalogach publicznych.	**Położenie** /etc/security/pscexpert/dodv2/wwdevfiles /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zgłasza raport, jeśli pliki dostępne do zapisu dla wszystkich znajdują się poza katalogami publicznymi.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN002640	2	Domyślne konta systemowe muszą być wyłączone lub usunięte.	**Położenie** /etc/security/pscexpert/dodv2/lockacc_rlogin /etc/security/pscexpert/dodv2/loginout **Działanie zgodności** Wyłącza domyślne konta systemowe.
GEN002660	2	Kontrola musi być włączona.	**Położenie** /etc/security/pscexpert/dodv2/dodaudit **Działanie zgodności** Włącza komendę dodaudit, która włącza kontrolę.
GEN002720	2	System kontroli musi być tak skonfigurowany, aby kontrolował zakończone niepowodzeniem próby dostępu do plików i programów.	**Położenie** /etc/security/pscexpert/dodv2/dodaudit **Działanie zgodności** Automatycznie włącza podaną kontrolę.
GEN002740	2	System kontroli musi być skonfigurowany w taki sposób, aby kontrolować usunięcia plików.	**Położenie** /etc/security/pscexpert/dodv2/dodaudit **Działanie zgodności** Automatycznie włącza podaną kontrolę.
GEN002750	3	System kontroli musi być skonfigurowany w taki sposób, aby kontrolować tworzenie kont.	**Położenie** /etc/security/pscexpert/dodv2/dodaudit **Działanie zgodności** Automatycznie włącza podaną kontrolę.
GEN002751	3	System kontroli musi być skonfigurowany w taki sposób, aby kontrolować modyfikowanie kont.	**Położenie** /etc/security/pscexpert/dodv2/dodaudit **Działanie zgodności** Automatycznie włącza podaną kontrolę.
GEN002752	3	System kontroli musi być skonfigurowany w taki sposób, aby kontrolować konta, które są wyłączone.	**Położenie** /etc/security/pscexpert/dodv2/dodaudit **Działanie zgodności** Automatycznie włącza podaną kontrolę.
GEN002753	3	System kontroli musi być skonfigurowany w taki sposób, aby kontrolować kończenie kont.	**Położenie** /etc/security/pscexpert/dodv2/dodaudit **Działanie zgodności** Automatycznie włącza podaną kontrolę.
GEN002760	2	System kontroli musi być skonfigurowany w taki sposób, aby kontrolować wszystkie działania administracyjne, uprzywilejowane oraz związane z bezpieczeństwem.	**Położenie** /etc/security/pscexpert/dodv2/dodaudit **Działanie zgodności** Automatycznie włącza podaną kontrolę.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN002800	2	System kontroli musi być skonfigurowany w taki sposób, aby kontrolować logowanie, wylogowywanie i inicjowanie sesji.	**Położenie** /etc/security/pscexpert/dodv2/dodaudit **Działanie zgodności** Automatycznie włącza podaną kontrolę.
GEN002820	2	System kontroli musi być skonfigurowany w taki sposób, aby kontrolować wszystkie modyfikacje uprawnień indywidualnej kontroli dostępu.	**Położenie** /etc/security/pscexpert/dodv2/dodaudit **Działanie zgodności** Automatycznie włącza podaną kontrolę.
GEN002825	2	System kontroli musi być skonfigurowany w taki sposób, aby kontrolować ładowanie i usuwanie z pamięci dynamicznych modułów jądra.	**Położenie** /etc/security/pscexpert/dodv2/dodaudit **Działanie zgodności** Automatycznie włącza podaną kontrolę.
GEN002860	2	Rotacja dzienników kontroli musi być wykonywana codziennie.	**Położenie** /etc/security/pscexpert/dodv2/rotateauditdod **Działanie zgodności** Zapewnia, że jest wykonywana rotacja dzienników kontroli.
GEN002960	2	Dostęp do programu narzędziowego cron musi być kontrolowany za pomocą pliku cron.allow, cron.deny lub obu tych plików.	**Położenie** /etc/security/pscexpert/dodv2/limitsysacc **Działanie zgodności** Zapewnia, czy są włączone limity zgodności.
GEN003000 (dotyczy GEN000960, GEN003020, GEN003160, GEN003360, GEN003380)	2	Demon Cron nie może uruchamiać programów z prawem zapisu dla grupy ani z prawem zapisu dla wszystkich.	**Położenie** /etc/security/pscexpert/dodv2/rmwwpaths **Działanie zgodności** Zapewnia, czy są włączone limity zgodności. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN003020 (dotyczy GEN000960, GEN003000, GEN003160, GEN003360, GEN003380)	2	Demon Cron nie może uruchamiać programów w katalogach dostępnych do zapisu dla wszystkich ani w ich katalogach podrzędnych.	**Położenie** /etc/security/pscexpert/dodv2/rmwwpaths **Działanie zgodności** Usuwa uprawnienie do zapisu dla wszystkich z katalogów programu cron. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN003060	2	Domyślne konta systemowe (oprócz użytkownika root) nie mogą być wymienione w pliku cron.allow lub muszą być dołączone do pliku cron.deny, jeśli nie istnieje plik cron.allow.	**Położenie** cron.allow lub cron.deny **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN003160 (dotyczy GEN000960, GEN003000, GEN003020, GEN003360, GEN003380)	2	Musi działać rejestrowanie programu Cron.	**Położenie** /etc/security/pscexpert/dodv2/rmwwpaths **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN003280	2	Dostęp do programu narzędziowego at musi być kontrolowany za pomocą plików at.allow i at.deny.	**Położenie** /etc/security/pscexpert/dodv2/chcronfilesdod **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN003300	2	Jeśli istnieje plik at.deny, nie może być on pusty.	**Położenie** /etc/security/pscexpert/dodv2/chcronfilesdod **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN003320	2	Domyślne konta systemowe, które nie są kontem użytkownika root, nie mogą być wymienione w pliku at.allow lub muszą być dołączone do pliku at.deny, jeśli nie istnieje plik at.allow.	**Położenie** /etc/security/pscexpert/dodv2/chcronfilesdod **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN003360 (dotyczy GEN000960, GEN003000, GEN003020, GEN003160, GEN003380)	2	Demon at nie może uruchamiać programów z prawem zapisu dla grupy ani z prawem zapisu dla wszystkich.	**Położenie** /etc/security/pscexpert/dodv2/rmwwpaths **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN003380 (dotyczy GEN000960, GEN003000, GEN003020, GEN003160, GEN003360)	2	Demon at nie może uruchamiać programów w katalogach dostępnych do zapisu dla wszystkich ani w ich katalogach podrzędnych.	**Położenie** /etc/security/pscexpert/dodv2/rmwwpaths **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN003510	2	Zrzuty pamięci jądra muszą być wyłączone, jeśli nie są potrzebne.	**Położenie** /etc/security/pscexpert/dodv2/coredumpdev **Działanie zgodności** Wyłącza zrzuty pamięci jądra.
GEN003540	2	System musi używać niewykonywalnych stosów programów.	**Położenie** /etc/security/pscexpert/dodv2/sedconfigdod **Działanie zgodności** Wymusza użycie niewykonywalnych stosów programów.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN003600	2	System nie może przekazywać pakietów IPv4 z opcją source-routing.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej ipsrcforward na *0*.
GEN003601	2	Konieczne jest odpowiednie ustawienie wielkości kolejek zaległości protokołu TCP.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej clean_partial_conns na *1*.
GEN003603	2	System nie może odpowiadać na echa protokołu ICMP w wersji 4 (ICMPv4), które zostały wysłane na adres rozgłaszania.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej bcastping na *0*.
GEN003604	2	System nie może odpowiadać na żądania datownika protokołu ICMP, które zostały wysłane na adres rozgłaszania.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej bcastping na *0*.
GEN003605	2	System nie może zastosować odwróconego routingu źródłowego do odpowiedzi TCP.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej nonlocsrcroute na *0*.
GEN003606	2	System musi uniemożliwić generowania pakietów z opcją source-routing przez aplikacje lokalne.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej ipsrcroutesend na *0*.
GEN003607	2	System nie może akceptować pakietów IPv4 z opcją source-routing.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Wyłącza możliwość akceptowania pakietów IPv4 z opcją source-routing.
GEN003609	2	System musi ignorować komunikaty przekierowania ICMP IPv4.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej ipignoreredirects na *1*.
GEN003610	2	System nie może wysyłać komunikatów przekierowania ICMP IPv4.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej ipsendredirects na *0*.
GEN003612	2	System musi być skonfigurowany do używania mechanizmu TCP SYN cookies w przypadku wystąpienia ataku TCP SYN flood.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej clean_partial_conns na *1*.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN003640	2	System plików root musi korzystać z kronikowania lub innej metody zapewniania spójności systemu plików.	**Położenie** /etc/security/pscexpert/dodv2/chkjournal **Działanie zgodności** Włącza kronikowania w systemie plików root.
GEN003660	2	System musi rejestrować dane informacyjne uwierzytelniania.	**Położenie** /etc/security/pscexpert/dodv2/chsyslogdod **Działanie zgodności** Włącza rejestrowanie danych auth i info.
GEN003700	2	Demony inetd i xinetd muszą zostać wyłączone lub usunięte, jeśli nie używają ich żadne usługi sieciowe.	**Położenie** /etc/security/pscexpert/dodv2/dodv2services **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN003810	2	Usługi portmap lub rpcbind nie mogą być uruchomione, jeśli nie są potrzebne.	**Położenie** /etc/security/pscexpert/dodv2/dodv2services **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN003815	2	Usługi portmap lub rpcbind nie mogą być zainstalowane, jeśli nie mają być używane.	**Położenie** /etc/security/pscexpert/dodv2/dodv2services **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN003820-3860	1,2,3	Nie mogą być uruchomione demony rsh, rexexec oraz telnet ani usługa rlogind.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN003865	2	Nie mogą być zainstalowane narzędzia do analizy sieci.	**Położenie** /etc/security/pscexpert/dodv2/dodv2services **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN003900	2	Plik hosts.lpd (lub jego odpowiednik) nie może zawierać znaku dodawania (+).	**Położenie** /etc/security/pscexpert/dodv2/printers **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN004220	1	Konta administracyjne nie mogą uruchamiać przeglądarki WWW, z wyjątkiem sytuacji, gdy jest to potrzebne do administrowania lokalnymi usługami.	**Położenie** /etc/security/pscexpert/dodv2/dodv2cat1 **Działanie zgodności** Wyświetla wyniki testów podanej reguły.
GEN004460	2	Ta reguła rejestruje dane auth i info.	**Położenie** /etc/security/pscexpert/dodv2/chsyslogdod **Działanie zgodności** Włącza rejestrowanie danych auth i info.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN004540	2	Ta reguła wyłącza komendę pomocy sendmail.	**Położenie** /etc/security/pscexpert/dodv2/sendmailhelp /etc/security/pscexpert/dodv2/dodv2cmntrows **Działanie zgodności** Wyłącza podaną komendę.
GEN004580	2	W systemie nie można używać plików .forward.	**Położenie** /etc/security/pscexpert/dodv2/forward **Działanie zgodności** Wyłącza podane pliki. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN004600	1	Usługa SMTP musi być w najnowszej wersji.	**Położenie** /etc/security/pscexpert/dodv2/SMTP_ver **Działanie zgodności** Gwarantuje, że jest uruchomiona najnowsza wersja podanej usługi. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN004620	2	Serwer sendmail musi mieć wyłączoną funkcję debugowania.	**Położenie** /etc/security/pscexpert/dodv2/SMTP_ver **Działanie zgodności** Wyłącza funkcję debugowania programu sendmail.
GEN004640	1	Usługa SMTP nie może mieć aktywnego aliasu uudecode.	**Położenie** /etc/security/pscexpert/dodv2/SMTPuucode **Działanie zgodności** Wyłącza alias uudecode.
GEN004710	2	Przekazywanie poczty musi być ograniczone.	**Położenie** /etc/security/pscexpert/dodv2/sendmaildod **Działanie zgodności** Ogranicza przekazywania poczty elektronicznej.
GEN004800	1,2,3	W systemie nie można używać niezaszyfrowanego protokołu FTP.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN004820	2	Anonimowe FTP nie może być aktywne w systemie, chyba że zastosowano autoryzację.	**Położenie** /etc/security/pscexpert/dodv2/anonuser **Działanie zgodności** Wyłącza anonimowe FTP w systemie. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN004840	2	Jeśli w systemie jest anonimowy serwer FTP, musi on zostać zlokalizowany w strefie zdemilitaryzowanej (DMZ) sieci.	**Położenie** /etc/security/pscexpert/dodv2/anonuser **Działanie zgodności** Zapewnia, że anonimowy serwer FTP w systemie znajduje się w strefie zdemilitaryzowanej sieci.
GEN004880	2	Musi istnieć plik ftpusers.	**Położenie** /etc/security/pscexpert/dodv2/chdodftpusers **Działanie zgodności** Zapewnia, że podany plik znajduje się w systemie.
GEN004900	2	Plik ftpusers musi zawierać nazwy kont, które nie mogą używać protokołu FTP.	**Położenie** /etc/security/pscexpert/dodv2/chdodftpusers **Działanie zgodności** Zapewnia, że plik zawiera wymagane nazwy kont.
GEN005000	1	Konta anonimowe FTP nie mogą mieć powłoki funkcjonalnej.	**Położenie** /etc/security/pscexpert/dodv2/usershells **Działanie zgodności** Usuwa powłoki z kont anonimowych FTP. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN005080	1	Demon TFTP musi działać w trybie bezpiecznym, który zapewnia dostęp tylko do pojedynczego katalogu w systemie plików hosta.	**Położenie** /etc/security/pscexpert/dodv2/tftpdod **Działanie zgodności** Zapewnia, że demon spełnia określone wymagania.
GEN005120	2	Demon TFTP musi zostać skonfigurowany zgodnie ze specyfikacją dostawcy, włącznie z dedykowanym kontem użytkownika TFTP, powłoką bez możliwości logowania, na przykład /bin/false, oraz katalogiem osobistym należącym do użytkownika TFTP.	**Położenie** /etc/security/pscexpert/dodv2/tftpdod **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005140	1,2,3	Każdy aktywny demon TFTP musi mieć autoryzację i zostać zatwierdzony w systemowym pakiecie akredytacji.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Zapewnia autoryzację demona.
GEN005160	1,2	Każdy host systemu X Window System musi zapisywać pliki .Xauthority.	**Położenie** /etc/security/pscexpert/dodv2/dodv2disableX **Działanie zgodności** Zapewnia, że host zapisał podane pliki.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN005200	1,2	Żaden z ekranów systemu X Window System nie może być eksportowany publicznie.	**Położenie** /etc/security/pscexpert/dodv2/dodv2disableX **Działanie zgodności** Wyłącza rozpowszechnianie podanych programów.
GEN005220	1,2	Pliki .Xauthority lub X*.hosts (albo ich odpowiednik) muszą być używane do ograniczenia dostępu do serwera X-Windows System.	**Położenie** /etc/security/pscexpert/dodv2/dodv2disableX **Działanie zgodności** Zapewnia, że są dostępne podane pliki w celu ograniczenia dostępu do serwera.
GEN005240	1,2	Program narzędziowy .Xauthority musi umożliwiać dostęp tylko do autoryzowanych hostów.	**Położenie** /etc/security/pscexpert/dodv2/dodv2disableX **Działanie zgodności** Zapewnia, że dostęp jest ograniczony do autoryzowanych hostów.
GEN005260	2	Ta reguła wyłącza połączenia z systemem X Window System i menedżer logowania XServer.	**Położenie** /etc/security/pscexpert/dodv2/dodv2cmntrows **Działanie zgodności** Wyłącza wymagane połączenia i menedżer logowania.
GEN005280	1,2,3	System nie może mieć aktywnej usługi UUCP.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN005300	2	Muszą zostać zmienione domyślne ustawienia wspólnot SNMP.	**Położenie** /etc/security/pscexpert/dodv2/chsnmp **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005305	2	Usługa SNMP musi używać tylko protokołu SNMPv3 lub nowszej wersji.	**Położenie** /etc/security/pscexpert/dodv2/chsnmp **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005306	2	Usługa SNMP musi wymagać użycia FIPS 140-2.	**Położenie** /etc/security/pscexpert/dodv2/chsnmp **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005440	2	System musi używać zdalnego serwera syslog (host protokołów).	**Położenie** /etc/security/pscexpert/dodv2/EnableTrustedLogging **Działanie zgodności** Zapewnia, że system używa zdalnego serwera syslog.
GEN005450	2	System musi używać zdalnego serwera syslog (host protokołów).	**Położenie** /etc/security/pscexpert/dodv2/ EnableTrustedLogging **Działanie zgodności** Zapewnia, że system używa zdalnego serwera syslog.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN005460	2	System musi używać zdalnego serwera syslog (host protokołów).	**Położenie** /etc/security/pscexpert/dodv2/ EnableTrustedLogging **Działanie zgodności** Zapewnia, że system używa zdalnego serwera syslog.
GEN005480	2	System musi używać zdalnego serwera syslog (host protokołów).	**Położenie** /etc/security/pscexpert/dodv2/EnableTrustedLogging **Działanie zgodności** Zapewnia, że system używa zdalnego serwera syslog.
GEN005500	2	Demon SSH musi być skonfigurowany w taki sposób, aby używać tylko wersji 2 protokołu SSH (SSHv2).	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005501	2	Klient SSH musi być skonfigurowany w taki sposób, aby używać tylko protokołu SSHv2.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005504	2	Demon SSH musi nasłuchiwać tylko z użyciem sieciowych adresów zarządzania, chyba że udzielono autoryzacji na potrzeby inne niż zarządzania.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005505	2	Demon SSH musi zostać skonfigurowany do używania tylko algorytmów szyfrowania zgodnych ze standardami FIPS 140-2.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005506	2	Demon SSH musi zostać skonfigurowany do używania tylko algorytmów szyfrowania zgodnych ze standardami FIPS 140-2.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005507	2	Demon SSH musi być skonfigurowany w taki sposób, aby używał wyłącznie kodów uwierzytelniania komunikatów (Message Authentication Code - MAC) z zastosowaniem szyfrujących algorytmów mieszających zgodnych ze standardami FIPS 140-2.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN005510	2	Klient SSH musi być skonfigurowany w taki sposób, aby używał wyłącznie kodów uwierzytelniania komunikatów (Message Authentication Code - MAC) z zastosowaniem algorytmów szyfrujących zgodnych ze standardami FIPS 140-2.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005511	2	Klient SSH musi być skonfigurowany w taki sposób, aby używał wyłącznie kodów uwierzytelniania komunikatów (Message Authentication Code - MAC) z zastosowaniem algorytmów szyfrujących zgodnych ze standardami FIPS 140-2.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005512	2	Demon SSH musi być skonfigurowany w taki sposób, aby używał wyłącznie kodów uwierzytelniania komunikatów (Message Authentication Code - MAC) z zastosowaniem szyfrujących algorytmów mieszających zgodnych ze standardami FIPS 140-2.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005521	2	Demon SSH musi ograniczać logowanie do konkretnych użytkowników, grup lub obu tych elementów.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005536	2	Demon SSH musi wykonywać sprawdzanie trybu ścisłego plików konfiguracyjnych katalogu osobistego.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005537	2	Demon SSH musi używać separacji uprawnień.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005538	2	Demon SSH nie może zezwalać na uwierzytelnianie rhosts z użyciem kryptosystemu RSA (Rivest-Shamir-Adleman).	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN005539	2	Demon SSH nie może zezwalać na kompresję lub musi zezwalać na kompresję tylko po pomyślnym uwierzytelnieniu.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005550	2	Demon SSH musi zostać skonfigurowany z banerem logowania Departamentu Obrony.	**Położenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005560	2	Sprawdź, czy jest dostępna brama domyślna skonfigurowana dla protokołu IPv4.	**Położenie** /etc/security/pscexpert/dodv2/chkgtway **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie. **Uwaga:** Jeśli w systemie jest uruchomiony protokół IPv6, należy upewnić się, że ustawienie *ipv6_enabled* w pliku /etc/security/pscexpert/ipv6.conf ma wartość yes. Jeśli w systemie nie jest używany protokół IPv6, należy upewnić się, że wartość ustawienia *ipv6_enabled* wynosi no.
GEN005570	2	Sprawdź, czy jest dostępna brama domyślna skonfigurowana dla protokołu IPv6.	**Położenie** /etc/security/pscexpert/dodv2/chkgtway **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie. **Uwaga:** Jeśli w systemie jest uruchomiony protokół IPv6, należy upewnić się, że ustawienie *ipv6_enabled* w pliku /etc/security/pscexpert/ipv6.conf ma wartość yes. Jeśli w systemie nie jest używany protokół IPv6, należy upewnić się, że wartość ustawienia *ipv6_enabled* wynosi no.
GEN005590	2	W systemie nie mogą być uruchomione żadne demony protokołu routingu, chyba że system jest routerem.	**Położenie** /etc/security/pscexpert/dodv2/dodv2cmntrows **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005590	2	W systemie nie mogą być uruchomione żadne demony protokołu routingu, chyba że system jest routerem.	**Położenie** /etc/security/pscexpert/dodv2/dodv2cmntrows **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN005600	2	Nie może być włączone przekazywanie IP dla protokołu IPv4, chyba że system jest routerem.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej ipforwarding na *0*.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	**Kategoria reguły STIG**	**Opis**	**Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność**
GEN005610	2	W systemie nie może być włączone przekazywanie IP dla protokołu IPv6, chyba że system jest routerem IPv6.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej ip6forwarding na *1*.
GEN005820	2	Należy skonfigurować anonimowy identyfikator UID i GID dla NFS, używając wartości bez uprawnień.	**Położenie** /etc/security/pscexpert/dodv2/nfsoptions **Działanie zgodności** Zapewnia, że podane identyfikatory nie mają uprawnień.
GEN005840	2	Serwer NFS musi być skonfigurowany pod kątem ograniczenia dostępu systemu plików do hostów lokalnych.	**Położenie** /etc/security/pscexpert/dodv2/nfsoptions **Działanie zgodności** Konfiguruje serwer NFS pod kątem ograniczenia dostępu do hostów lokalnych.
GEN005880	2	Serwer NFS nie może zezwalać na zdalny dostęp użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/nfsoptions **Działanie zgodności** Wyłącza zdalny dostęp użytkownika root na serwerze NFS.
GEN005900	2	Opcję *nosuid* należy włączyć we wszystkich podłączeniach klientów NFS.	**Położenie** /etc/security/pscexpert/dodv2/nosuid **Działanie zgodności** Włącza opcję *nosuid* we wszystkich podłączeniach klientów NFS.
GEN006060	2	W systemie nie może być uruchomiony program Samba, chyba że jest potrzebny.	**Położenie** /etc/security/pscexpert/dodv2/dodv2services **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN006380	1	W systemie nie można używać protokołu UDP dla NIS ani NIS+.	**Położenie** /etc/security/pscexpert/dodv2/dodv2cat1 **Działanie zgodności** Wyświetla wyniki testów podanej reguły.
GEN006400	2	Nie można używać protokołu NIS (Network Information System).	**Położenie** /etc/security/pscexpert/dodv2/nisplus **Działanie zgodności** Wyłącza podany protokół. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN006420	2	Mapy NIS muszą być zabezpieczone za pomocą trudnych do odgadnięcia nazw domen.	**Położenie** /etc/security/pscexpert/dodv2/nisplus **Działanie zgodności** Zapewnia, że nazwy domen nie są łatwe do określenia.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN006460	2	Każdy serwer NIS+ musi działać na drugim poziomie bezpieczeństwa.	**Położenie** /etc/security/pscexpert/dodv2/nisplus **Działanie zgodności** Zapewnia, że serwer działa na podanym minimalnym poziomie bezpieczeństwa. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN006480	2	Co tydzień należy sprawdzać system pod kątem nieautoryzowanych plików setuid oraz nieautoryzowanych modyfikacji autoryzowanych plików setuid.	**Położenie** /etc/security/pscexpert/dodv2/trust **Działanie zgodności** Sprawdza co tydzień, aby zidentyfikować zmiany podanych plików.
GEN006560	2	Co tydzień należy sprawdzać system pod kątem nieautoryzowanych plików setuid oraz nieautoryzowanych modyfikacji autoryzowanych plików setuid.	**Położenie** /etc/security/pscexpert/dodv2/trust **Działanie zgodności** Sprawdza co tydzień, aby zidentyfikować zmiany podanych plików.
GEN006580	2	W systemie musi być używany program kontroli dostępu.	**Położenie** /etc/security/pscexpert/dodv2/checktcpd **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN006600	2	Program kontroli dostępu systemu musi rejestrować każdą próbę dostępu do systemu.	**Położenie** /etc/security/pscexpert/dodv2/chsyslogdod **Działanie zgodności** Zapewnia, że są rejestrowane próby dostępu.
GEN006620	2	Program kontroli dostępu systemu musi być skonfigurowany w taki sposób, aby nadawać lub odbierać uprawnienia dostępu do systemu określonym hostom.	**Położenie** /etc/security/pscexpert/dodv2/chetchostsdod **Działanie zgodności** Konfiguruje pliki hosts.deny i hosts.allow do wymaganych ustawień.
GEN007020	2	Musi być wyłączony protokół SCTP (Stream Control Transmission Protocol).	**Położenie** /etc/security/pscexpert/dodv2/dodv2netrules **Działanie zgodności** Wyłącza podany protokół.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	**Kategoria reguły STIG**	**Opis**	**Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność**
GEN007700	2	Procedura obsługi protokołu IPv6 nie może być powiązana ze stosem sieci, chyba że jest potrzebna.	**Położenie** /etc/security/pscexpert/dodv2/rminet6 **Działanie zgodności** Wyłącza procedurę obsługi protokołu IPv6 w stosie sieci, chyba że program obsługi został podany w pliku /etc/ipv6.conf. **Uwaga:** Jeśli w systemie jest uruchomiony protokół IPv6, należy upewnić się, że ustawienie *ipv6_enabled* w pliku /etc/security/pscexpert/ipv6.conf ma wartość yes. Jeśli w systemie nie jest używany protokół IPv6, należy upewnić się, że wartość ustawienia *ipv6_enabled* wynosi no.
GEN007780	2	W systemie nie może być włączonych tuneli 6to4.	**Położenie** /etc/security/pscexpert/dodv2/rmiface **Działanie zgodności** Wyłącza podane tunele. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN007820	2	System nie może mieć skonfigurowanych tuneli IP.	**Położenie** /etc/security/pscexpert/dodv2/rmtunnel **Działanie zgodności** Wyłącza tunele IP. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN007840	2	Klient DHCP musi być wyłączony, jeśli nie jest używany.	**Położenie** /etc/security/pscexpert/dodv2/dodv2services **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN007850	2	Klient DHCP nie może wysyłać dynamicznych aktualizacji DNS.	**Położenie** /etc/security/pscexpert/dodv2/dodv2services **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN007860	2	System musi ignorować komunikaty przekierowania ICMP IPv6.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej ipignoreredirects na *1*.
GEN007880	2	System nie może wysyłać przekierowań ICMP IPv6.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej ipsendredirects na *0*.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN007900	2	W systemie musi być używany odpowiedni filtr ścieżki zwrotnej dla ruchu w sieci IPv6, jeśli system używa protokołu IPv6.	**Położenie** /etc/security/pscexpert/dodv2/chuserstanzadod **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN007920	2	System nie może przekazywać pakietów IPv6 z opcją source-routing.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej ip6srcrouteforward na *0*.
GEN007940: GEN003607	2	System nie może akceptować pakietów IPv4 lub IPv6 z opcją source-routing.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej ipsrcrouterecv na *0*.
GEN007950	2	System nie może odpowiadać na żądania echa protokołu ICMPv6, które zostały wysłane na adres rozgłaszania.	**Położenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Działanie zgodności** Ustawia wartość opcji sieciowej bcastping na *0*.
GEN008000	2	Jeśli w systemie do uzyskania informacji uwierzytelniania lub informacji o koncie jest używany protokół LDAP, certyfikaty służące do uwierzytelniania na serwerze LDAP muszą być udostępnione przez PKI Departamentu Obrony lub metodę zatwierdzoną przez Departament Obrony.	**Położenie** /etc/security/pscexpert/dodv2/ldap_config **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN008020	2	Jeśli w systemie do uzyskania informacji uwierzytelniania lub informacji o koncie jest używany protokół LDAP, połączenie TLS LDAP musi wymagać, aby serwer udostępnił certyfikat z poprawną zaufaną ścieżką.	**Położenie** /etc/security/pscexpert/dodv2/ldap_config **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN008050	2	Jeśli w systemie do uzyskania informacji uwierzytelniania lub informacji o koncie jest używany protokół LDAP, plik /etc/ldap.conf (lub jego odpowiednik) nie może zawierać haseł.	**Położenie** /etc/security/pscexpert/dodv2/ldap_config **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	**Kategoria reguły STIG**	**Opis**	**Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność**
GEN008380	2	Co tydzień należy sprawdzać system pod kątem nieautoryzowanych plików setuid oraz nieautoryzowanych modyfikacji autoryzowanych plików setuid.	**Położenie** /etc/security/pscexpert/dodv2/trust **Działanie zgodności** Sprawdza co tydzień, aby zidentyfikować zmiany podanych plików.
GEN008520	2	System musi implementować lokalny firewall, który chroni host przed skanowaniem portów. Firewall musi odrzucać połączenia na wrażliwe porty przez 5 minut w celu ochrony przed skanowaniem portów.	**Położenie** /etc/security/pscexpert/dodv2/ipsecshunports **Działanie zgodności** Zapewnia, że system spełnia określone wymagania.
GEN008540	2	Lokalny firewall systemu musi implementować strategię *deny-all* (odmów wszystkim), *allow-by-exception* (zezwól na zasadzie wyjątków).	**Położenie** /etc/security/pscexpert/dodv2/ipsecshunhosthls **Działanie zgodności** Zapewnia, że system spełnia określone wymagania. **Uwaga:** Do pliku /etc/security/aixpert/bin/filter.txt można dodać dodatkowe reguły filtrowania. Reguły te są połączone w skrypcie ipsecshunhosthls.sh w przypadku stosowania profilu. Pozycje powinny być podane w następującym formacie: *numer_portu*:*adres_ip*: *działanie* Parametr *działanie* może mieć następujące wartości: Allow (zezwól) albo Deny (odmów).
GEN008600	1	System musi być skonfigurowany do uruchamiania tylko z konfiguracji startowej systemu.	**Położenie** /etc/security/pscexpert/dodv2/dodv2cat1 **Działanie zgodności** Zapewnia, że podczas uruchamiania systemu używana jest tylko konfiguracja startowa systemu.
GEN008640	1	System nie może używać nośnika wymiennego jako programu startowego.	**Położenie** /etc/security/pscexpert/dodv2/dodv2cat1 **Działanie zgodności** Zapewnia, że system nie jest uruchamiany z napędu wymiennego.
GEN009140	1,2,3	System nie może mieć aktywnej usługi chargen.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN009160	1,2,3	System nie może mieć aktywnej usługi Calendar Management Service Daemon (CMSD).	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009180	1,2,3	System nie może mieć aktywnej usługi tool-talk database server (ttdbserver).	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009190	1,2,3	System nie może mieć aktywnej usługi comsat.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009200-9330	1,2,3	System nie może mieć aktywnych pozostałych usług i demonów.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009210	2	System nie może mieć aktywnej usługi discard.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009220	2	System nie może mieć aktywnej usługi dtspc.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009230	2	System nie może mieć aktywnej usługi echo.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009240	2	System nie może mieć aktywnej usługi Internet Message Access Protocol (IMAP).	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009250	2	System nie może mieć aktywnej usługi PostOffice Protocol (POP3).	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.

Tabela 2. Ogólne wymagania Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Kategoria reguły STIG	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN009260	2	System nie może mieć aktywnej usługi talk ani ntalk.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009270	2	System nie może mieć aktywnej usługi netstat w procesie InetD.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009280	2	System nie może mieć aktywnej usługi PCNFS.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009290	2	System nie może mieć aktywnej usługi systat.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009300	2	Usługa inetd time nie może być aktywna w systemie w demonie inetd.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009310	2	System nie może mieć aktywnej usługi rusersd.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009320	2	System nie może mieć aktywnej usługi sprayd.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009330	2	System nie może mieć aktywnej usługi rstatd.	**Położenie** /etc/security/pscexpert/dodv2/inetdservices **Działanie zgodności** Wyłącza wymagane demony i usługi, przekształcając w komentarz pozycje w pliku /etc/inetd.conf.
GEN009340	2	Menedżery logowania serwera X-Windows nie mogą działać, chyba że są potrzebne do zarządzania sesją X11.	**Położenie** /etc/security/pscexpert/dodv2/dodv2cmntrows **Działanie zgodności** Ta reguła wyłącza połączenia z systemem X Window System i menedżer logowania XServer.

Tabela 3. Wymagania dotyczące prawa własności Departamentu Obrony

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
AIX00085	Plik /etc/netsvc.conf musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
AIX00090	Plik /etc/netsvc.conf musi należeć do grupy bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, sys lub system.
AIX00320	Plik /etc/ftpaccess.ctl musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
AIX00330	Plik /etc/ftpaccess.ctl musi należeć do grupy bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, sys lub system.
GEN000250	Właścicielem pliku konfiguracyjnego synchronizacji czasu (na przykład /etc/ntp.conf) musi być użytkownik root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN000251	Właścicielem pliku konfiguracyjnego synchronizacji czasu (na przykład /etc/ntp.conf) musi być grupa bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, sys lub system.
GEN001160	Wszystkie pliki i katalogi muszą mieć poprawnego właściciela.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że wszystkie pliki i katalogi mają poprawnego właściciela.
GEN001170	Wszystkie pliki i katalogi muszą mieć poprawnego właściciela grupy.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że wszystkie pliki i katalogi mają poprawnego właściciela.
GEN001220	Wszystkie systemowe pliki, programy i katalogi muszą być własnością konta system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że systemowe pliki, programy i katalogi są własnością konta system.

Tabela 3. Wymagania dotyczące prawa własności Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	**Opis**	**Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność**
GEN001240	Systemowe pliki, programy i katalogi muszą być własnością grupy system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Wszystkie systemowe pliki, programy i katalogi są własnością grupy system.
GEN001320	Pliki NIS/NIS+/yp muszą być własnością użytkownika root, sys lub bin.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki są własnością użytkownika root, sys lub bin.
GEN001340	Pliki NIS/NIS+/yp muszą być własnością grupy sys, bin, other lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki są własnością użytkownika sys, bin, other lub system.
GEN001362	Plik /etc/resolv.conf musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN001363	Plik /etc/resolv.conf musi należeć do grupy bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, sys lub system.
GEN001366	Plik /etc/hosts musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN001367	Plik /etc/hosts musi należeć do grupy bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, sys lub system.
GEN001371	Plik /etc/nsswitch.conf musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN001372	Plik /etc/nsswitch.conf musi należeć do grupy root, bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy root, bin, sys lub system.

Tabela 3. Wymagania dotyczące prawa własności Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	**Opis**	**Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność**
GEN001378	Plik /etc/passwd musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN001379	Plik /etc/passwd musi należeć do grupy bin, security, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, security, sys lub system.
GEN001391	Plik /etc/group musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN001392	Plik /etc/group musi należeć do grupy bin, security, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, security, sys lub system.
GEN001400	Plik /etc/security/passwd musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN001410	Plik /etc/security/passwd musi należeć do grupy bin, security, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, security, sys lub system.
GEN001500	Wszystkie katalogi osobiste użytkowników interaktywnych muszą być własnością odpowiednich użytkowników.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że wszystkie katalogi osobiste użytkowników interaktywnych muszą być własnością odpowiednich użytkowników.
GEN001520	Wszystkie katalogi osobiste użytkowników interaktywnych muszą należeć do grupy podstawowej właściciela katalogu osobistego.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że wszystkie katalogi osobiste użytkowników interaktywnych należą do grupy podstawowej właściciela katalogu osobistego.

Tabela 3. Wymagania dotyczące prawa własności Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN001540	Wszystkie pliki i katalogi, które są zawarte w katalogu osobistym użytkownika interaktywnego, muszą być własnością tego właściciela katalogu osobistego.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że wszystkie pliki i katalogi, które są zawarte w katalogu osobistym użytkownika interaktywnego, są własnością tego właściciela katalogu osobistego.
GEN001550	Wszystkie pliki i katalogi zawarte w katalogu osobistym użytkownika muszą być własnością grupy, do której należy właściciel tego katalogu osobistego.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że wszystkie pliki i katalogi zawarte w katalogu osobistym użytkownika muszą być własnością grupy, do której należy właściciel tego katalogu osobistego.
GEN001660	Wszystkie pliki startowe systemu muszą być własnością użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki należą do użytkownika root.
GEN001680	Wszystkie pliki startowe systemu muszą być własnością grupy sys, bin, other lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki są własnością grupy sys, bin, other lub system.
GEN001740	Wszystkie globalne pliki inicjowania muszą być własnością użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki należą do użytkownika root.
GEN001760	Wszystkie globalne pliki inicjowania muszą być własnością grupy sys, bin, system lub security.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki są własnością grupy sys, bin, system lub security.
GEN001820	Wszystkie szkieletowe pliki i katalogi (zwykle w katalogu /etc/skel) muszą być własnością użytkownika root lub bin.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki i katalogi należą do użytkownika root lub bin.
GEN001830	Wszystkie szkieletowe pliki (zwykle w katalogu /etc/skel) muszą być własnością grupy security.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki należą do grupy security.

Tabela 3. Wymagania dotyczące prawa własności Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN001860	Wszystkie lokalne pliki inicjowania muszą być własnością użytkownika lub użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki należą do użytkownika lub użytkownika root.
GEN001870	Lokalne pliki inicjowania muszą należeć do grupy użytkownika root lub grupy podstawowej użytkownika.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że lokalne pliki inicjowania muszą należeć do grupy użytkownika root lub grupy podstawowej użytkownika.
GEN002060	Wszystkie pliki .rhosts, .shosts, .netrc lub hosts.equiv muszą być dostępne tylko dla użytkownika root lub właściciela.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że tylko użytkownik root lub właściciel może uzyskać dostęp do podanych plików.
GEN002100	Plik .rhosts nie może być obsługiwany przez moduł PAM (Pluggable Authentication Module).	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik nie jest dostępny przy użyciu modułu PAM.
GEN002200	Wszystkie pliki powłoki muszą być własnością użytkownika root lub bin.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki należą do użytkownika root lub bin.
GEN002210	Wszystkie pliki powłoki muszą być własnością grupy root, bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki są własnością grupy root, bin, sys lub system.
GEN002340	Urządzenia audio muszą być własnością użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że wszystkie urządzenia audio są własnością użytkownika root.
GEN002360	Urządzenia audio muszą być własnością grupy root, sys, bin lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że wszystkie urządzenia audio należą do grupy root, sys, bin lub system.
GEN002520	Wszystkie katalogi publiczne muszą należeć do użytkownika root lub konta aplikacji.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że wszystkie katalogi publiczne należą do użytkownika root lub konta aplikacji.

Tabela 3. Wymagania dotyczące prawa własności Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN002540	Wszystkie katalogi publiczne muszą należeć do grupy system lub grupy aplikacji.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że wszystkie katalogi publiczne należą do grupy system lub grupy aplikacji.
GEN002680	Dzienniki kontroli systemu muszą być własnością użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki należą do użytkownika root.
GEN002690	Dzienniki kontroli systemu muszą należeć do grupy bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki są własnością grupy bin, sys lub system.
GEN003020	Demon Cron nie może uruchamiać programów w katalogach dostępnych do zapisu dla wszystkich ani w ich katalogach podrzędnych.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapobiega uruchamianiu przez demon cron programów w katalogach dostępnych do zapisu dla wszystkich lub ich katalogach podrzędnych.
GEN003040	Pliki crontab muszą być własnością użytkownika root lub twórcy pliku crontab.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że pliki crontab są własnością użytkownika root lub twórcy pliku crontab.
GEN003050	Pliki crontab muszą być własnością grupy system, cron lub grupy podstawowej twórcy pliku crontab.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że pliki crontab są własnością grupy system, cron lub grupy podstawowej twórcy pliku crontab.
GEN003110	Katalogi cron i crontab nie mogą mieć rozszerzonych list kontroli dostępu.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane katalogi nie mają rozszerzonych list kontroli dostępu.
GEN003120	Katalogi cron i crontab muszą być własnością użytkownika root lub bin.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia że katalogi cron i crontab należą do użytkownika root lub bin.
GEN003140	Katalogi cron i crontab muszą należeć do grupy system, sys, bin lub cron.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane katalogi należą do grupy system, sys, bin lub cron.

Tabela 3. Wymagania dotyczące prawa własności Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN003160	Musi zostać zaimplementowane rejestrowanie cron.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że jest zaimplementowane rejestrowanie cron.
GEN003240	Plik cron.allow musi należeć do użytkownika root, bin lub sys.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root, bin lub sys.
GEN003250	Plik cron.allow musi należeć do grupy system, bin, sys lub cron.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy system, bin, sys lub cron.
GEN003260	Plik cron.deny musi należeć do użytkownika root, bin lub sys.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root, bin lub sys.
GEN003270	Plik cron.deny musi należeć do grupy system, bin, sys lub cron.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy system, bin, sys lub cron.
GEN003420	Katalog at musi należeć do użytkownika root, bin, sys, daemon lub cron.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany katalog należy do użytkownika root, sys, daemon lub cron.
GEN003430	Katalog at musi należeć do grupy system, bin, sys lub cron.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany katalog należy do grupy system, bin, sys lub cron.
GEN003460	Plik at.allow musi należeć do użytkownika root, bin lub sys.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root, bin lub sys.
GEN003470	Plik at.allow musi należeć do grupy system, bin, sys lub cron.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy system, bin, sys lub cron.

Tabela 3. Wymagania dotyczące prawa własności Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN003480	Plik at.deny musi należeć do użytkownika root, bin lub sys.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root, bin lub sys.
GEN003490	Plik at.deny musi należeć do grupy system, bin, sys lub cron.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy system, bin, sys lub cron.
GEN003720	Plik inetd.conf, plik xinetd.conf oraz katalog xinetd.d muszą należeć do użytkownika root lub bin.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki i katalog należą do użytkownika root lub bin.
GEN003730	Plik inetd.conf, plik xinetd.conf oraz katalog xinetd.d muszą należeć do grupy bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki i katalog są własnością grupy bin, sys lub system.
GEN003760	Plik services musi należeć do użytkownika root lub bin.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root lub bin.
GEN003770	Plik services musi należeć do grupy bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, sys lub system.
GEN003920	Plik hosts.lpd (lub jego odpowiednik) musi należeć do użytkownika root, bin, sys lub lp.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root, bin, sys lub lp.
GEN003930	Plik hosts.lpd (lub jego odpowiednik) musi należeć do grupy bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, sys lub system.
GEN003960	Właścicielem komendy **traceroute** musi być użytkownik root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że właścicielem tej komendy jest użytkownik root.

Tabela 3. Wymagania dotyczące prawa własności Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN003980	Właścicielem komendy **traceroute** musi być grupa sys, bin lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że właścicielem komendy jest grupa sys, bin lub system.
GEN004360	Plik alias musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN004370	Właścicielem pliku aliases musi być grupa sys, bin lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że właścicielem podanego pliku jest grupa sys, bin lub system.
GEN004400	Pliki uruchamiane za pomocą pliku aliases poczty muszą należeć do użytkownika root i znajdować się w katalogu należącym do użytkownika root i dostępnym do zapisu tylko przez użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że pliki uruchamiane za pomocą pliku aliases poczty należą do użytkownika root i znajdują się w katalogu należącym do użytkownika root i dostępnym do zapisu tylko przez użytkownika root.
GEN004410	Pliki uruchamiane za pomocą pliku aliases poczty muszą należeć do grupy root, bin, sys lub other. Ponadto muszą znajdować się w katalogu należącym do grupy root, bin, sys lub other.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że pliki uruchamiane za pomocą pliku aliases poczty należą do grupy root, bin, sys lub other i znajdują się w katalogu, który należy do grupy root, bin, sys lub other.
GEN004480	Plik dziennika usługi SMTP musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN004920	Plik ftpusers musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN004930	Plik ftpusers musi należeć do grupy bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, sys lub system.

Tabela 3. Wymagania dotyczące prawa własności Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN005360	Plik snmpd.conf musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN005365	Plik snmpd.conf musi należeć do grupy bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, sys lub system.
GEN005400	Plik /etc/syslog.conf musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN005420	Plik /etc/syslog.conf musi należeć do grupy bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, sys lub system.
GEN005610	W systemie nie może być włączone przekazywanie IP dla protokołu IPv6, chyba że system jest routerem IPv6.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że przekazywanie IP dla protokołu IPv6 nie jest włączone, chyba że system jest używany jako router IPv6.
GEN005740	Plik konfiguracyjny eksportu NFS musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN005750	Plik konfiguracyjny eksportu NFS musi należeć do grupy root, bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy root, bin, sys lub system.
GEN005800	Wszystkie pliki i katalogi systemowe wyeksportowane przez NFS muszą należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN005810	Wszystkie pliki i katalogi systemowe wyeksportowane przez NFS muszą należeć do grupy root, bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki i katalogi są własnością grupy root, bin, sys lub system.

Tabela 3. Wymagania dotyczące prawa własności Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN006100	Plik /usr/lib/smb.conf musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN006120	Plik /usr/lib/smb.conf musi należeć do grupy bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, sys lub system.
GEN006160	Plik /var/private/smbpasswd musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN006180	Plik /var/private/smbpasswd musi należeć do grupy sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że właścicielem podanego pliku jest grupa sys lub system.
GEN006340	Pliki w katalogu /etc/news muszą należeć do użytkownika root lub news.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany katalog należy do użytkownika root lub news.
GEN006360	Pliki w katalogu /etc/news muszą należeć do grupy system lub news.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podane pliki należą do grupy system lub news.
GEN008080	Jeśli w systemie do uzyskania informacji uwierzytelniania lub informacji o koncie jest używany protokół LDAP, plik /etc/ldap.conf (lub jego odpowiednik) musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.
GEN008100	Jeśli w systemie do uzyskania informacji uwierzytelniania lub informacji o koncie jest używany protokół LDAP, plik /etc/ldap.conf (lub jego odpowiednik) musi należeć do grupy security, bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, sys lub system.
GEN008140	Jeśli w systemie do uzyskania informacji uwierzytelniania lub informacji o koncie jest używany protokół LDAP, plik lub katalog ośrodka certyfikacji TLS musi należeć do użytkownika root.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do użytkownika root.

Tabela 3. Wymagania dotyczące prawa własności Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN008160	Jeśli w systemie do uzyskania informacji uwierzytelniania lub informacji o koncie jest używany protokół LDAP, plik lub katalog ośrodka certyfikacji TLS musi należeć do grupy root, bin, sys lub system.	**Położenie** /etc/security/pscexpert/dodv2/chowndodfiles **Działanie zgodności** Zapewnia, że podany plik należy do grupy bin, sys lub system.

Tabela 4. Standardy Departamentu Obrony dotyczące uprawnień do plików

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
AIX00100	Plik /etc/netsvc.conf musi mieć tryb 0644 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
AIX00340	Plik /etc/ftpaccess.ctl musi mieć tryb 0640 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN000252	Plik konfiguracyjny synchronizacji czasu (na przykład /etc/ntp.conf) musi mieć tryb 0640 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN000920	Katalog osobisty konta użytkownika root (inny niż /) musi mieć tryb 0700.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że katalog jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN001140	Systemowe pliki i katalogi nie mogą mieć nierównomiernych uprawnień dostępu.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia spójność uprawnień dostępu.
GEN001180	Wszystkie pliki demonów usług sieciowych muszą mieć tryb 0755 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.

Tabela 4. Standardy Departamentu Obrony dotyczące uprawnień do plików (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN001200	Wszystkie pliki komend systemowych muszą mieć tryb 0755 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN001260	Pliki dzienników systemowych muszą mieć tryb 0640 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN001280	Pliki stron podręcznika muszą mieć tryb 0644 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN001300	Pliki bibliotek muszą mieć tryb 0755 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN001360	Pliki NIS/NIS+/yp muszą mieć tryb 0755 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN001364	Plik /etc/resolv.conf musi mieć tryb 0644 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN001368	Plik /etc/hosts musi mieć tryb 0644 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN001373	Plik /etc/nsswitch.conf musi mieć tryb 0644 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.

Tabela 4. Standardy Departamentu Obrony dotyczące uprawnień do plików (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN001380	Plik /etc/passwd musi mieć tryb 0644 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN001393	Plik /etc/group musi mieć tryb 0644 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN001420	Plik /etc/security/passwd musi mieć tryb 0400.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN001480	Wszystkie katalogi osobiste użytkowników muszą mieć tryb 0750 lub dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN001560	Wszystkie pliki i katalogi, które są zawarte w katalogach osobistych użytkowników muszą mieć tryb 0750 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN001580	Wszystkie skrypty sterujące uruchamianiem muszą mieć tryb 0755 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN001640	Skrypty sterujące uruchamianiem nie mogą uruchamiać programów ani skryptów dostępnych do zapisu przez wszystkich.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Sprawdza programy, takie jak cron, pod kątem programów lub skryptów dostępnych do zapisu przez wszystkich.
GEN001720	Wszystkie globalne pliki inicjowania muszą mieć tryb 0644 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.

Tabela 4. Standardy Departamentu Obrony dotyczące uprawnień do plików (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN001800	Wszystkie pliki szkieletowe (na przykład pliki w katalogu /etc/skel) muszą mieć tryb 0644 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN001880	Wszystkie lokalne pliki inicjowania muszą mieć tryb 0740 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN002220	Wszystkie pliki powłoki muszą mieć tryb 0755 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN002320	Urządzenia audio muszą mieć tryb 0660 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że urządzenia audio są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia,
GEN002560	Domyślna wartość **umask** systemu i użytkownika musi wynosić 077.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że podane ustawienie ma wartość *077*.
GEN002700	Dzienniki kontroli systemu muszą mieć tryb 0640 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN002717	Pliki wykonywalne narzędzia kontroli systemu muszą mieć tryb 0750 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN002980	Plik cron.allow musi mieć tryb 0600 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.

Tabela 4. Standardy Departamentu Obrony dotyczące uprawnień do plików (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN003080	Pliki crontab muszą mieć tryb 0600 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN003090	Pliki crontab nie mogą mieć rozszerzonych list kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że podane pliki nie mają rozszerzonych list ACL.
GEN003100	Katalogi cron i crontab muszą mieć tryb 0755 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że podane katalogi są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN003180	Plik cronlog musi mieć tryb 0600 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN003200	Plik cron.deny musi mieć tryb 0600 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN003252	Plik at.deny musi mieć tryb 0640 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN003340	Plik at.allow musi mieć tryb 0600 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN003400	Katalog at musi mieć tryb 0755 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że katalog jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.

Tabela 4. Standardy Departamentu Obrony dotyczące uprawnień do plików (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN003440	Dla zadań at nie można ustawiać parametru **umask** na wartość mniej restrykcyjną niż 077.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że parametr jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN003740	Pliki inetd.conf i xinetd.conf muszą mieć tryb 0440 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN003780	Plik services musi mieć tryb 0444 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN003940	Plik hosts.lpd (lub jego odpowiednik) musi mieć tryb 0644 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN004000	Plik traceroute musi mieć tryb 0700 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN004380	Plik alias musi mieć tryb 0644 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN004420	Pliki uruchamiane za pomocą pliku aliases muszą mieć tryb 0755 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN004500	Plik dziennika usługi SMTP musi mieć tryb 0644 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.

Tabela 4. Standardy Departamentu Obrony dotyczące uprawnień do plików (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN004940	Plik ftpusers musi mieć tryb 0640 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN005040	Wszyscy użytkownicy FTP muszą mieć domyślne ustawienie **umask** o wartości 077.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że ustawienie jest poprawne.
GEN005100	Demon TFTP musi mieć tryb 0755 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że demon jest ustawiany na podany tryb lub na ten, który daje mniejsze uprawnienia.
GEN005180	Wszystkie pliki .Xauthority muszą mieć tryb 0600 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN005320	Plik snmpd.conf musi mieć tryb 0600 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN005340	Pliki bazy MIB muszą mieć tryb 0640 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN005390	Plik /etc/syslog.conf musi mieć tryb 0640 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN005522	Pliki kluczy publicznych hosta SSH muszą mieć tryb 0644 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.

Tabela 4. Standardy Departamentu Obrony dotyczące uprawnień do plików (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN005523	Pliki kluczy prywatnych hosta SSH muszą mieć tryb 0600 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że pliki są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN006140	Plik /usr/lib/smb.conf musi mieć tryb 0644 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN006200	Plik /var/private/smbpasswd musi mieć tryb 0600 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN006260	Plik /etc/news/hosts.nntp (lub jego odpowiednik) musi mieć tryb 0600 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN006280	Plik /etc/news/hosts.nntp.nolimit (lub jego odpowiednik) musi mieć tryb 0600 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN006300	Plik /etc/news/nnrp.access (lub jego odpowiednik) musi mieć tryb 0600 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN006320	Plik /etc/news/passwd.nntp (lub jego odpowiednik) musi mieć tryb 0600 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.
GEN008060	Jeśli w systemie do uzyskania informacji uwierzytelniania lub informacji o koncie jest używany protokół LDAP, plik /etc/ldap.conf (lub jego odpowiednik) musi mieć tryb 0644 lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że plik jest ustawiany na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.

Tabela 4. Standardy Departamentu Obrony dotyczące uprawnień do plików (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN008180	Jeśli w systemie do uzyskania informacji uwierzytelniania lub informacji o koncie jest używany protokół LDAP, plik i/lub katalog ośrodka certyfikacji TLS musi mieć tryb 0644 (0755 w przypadku katalogów) lub tryb dający mniejsze uprawnienia.	**Położenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Działanie zgodności** Zapewnia, że podane pliki i/lub katalogi są ustawiane na podany tryb uprawnień lub na ten, który daje mniejsze uprawnienia.

Tabela 5. Wymagania listy kontroli dostępu Departamentu Obrony

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
AIX00110	Plik /etc/netsvc.conf nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
AIX00350	Plik /etc/ftpaccess.ctl nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN000253	Plik konfiguracyjny synchronizacji czasu (na przykład /etc/ntp.conf) nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN000930	Katalog osobisty konta użytkownika root nie może mieć rozszerzonej listy ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 5. Wymagania listy kontroli dostępu Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN001190	Żadne pliki demona usług sieciowych nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001210	Żadne pliki komend systemowych nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001270	Pliki dziennika systemowego nie mogą mieć rozszerzonych list ACL, chyba że są one potrzebne do obsługi autoryzowanego oprogramowania.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001310	Żadne pliki bibliotek nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001361	Pliki komend NIS/NIS+/yp nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 5. Wymagania listy kontroli dostępu Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN001365	Plik /etc/resolv.conf nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001369	Plik /etc/hosts nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001374	Plik /etc/nsswitch.conf nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001390	Plik /etc/passwd nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001394	Plik /etc/group nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 5. Wymagania listy kontroli dostępu Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN001430	Plik /etc/security/passwd nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001570	Żadne pliki i katalogi zawarte w katalogach osobistych użytkowników nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001590	Żadne skrypty sterujące uruchamianiem nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001730	Żadne globalne pliki inicjowania nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN001810	Pliki szkieletowe nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 5. Wymagania listy kontroli dostępu Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN001890	Lokalne pliki inicjowania nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN002230	Żadne pliki powłoki nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN002330	Urządzenia audio nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN002710	Żadne systemowe pliki audio nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN002990	Rozszerzone listy ACL powinny być wyłączone dla plików cron.allow i cron.deny.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 5. Wymagania listy kontroli dostępu Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN003090	Pliki crontab nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN003110	Katalogi cron i crontab nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN003190	Pliki dziennika cron nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN003210	Plik cron.deny nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN003245	Plik at.allow nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 5. Wymagania listy kontroli dostępu Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN003255	Plik at.deny nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN003410	Katalog at nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN003745	Pliki inetd.conf i xinetd.conf nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN003790	Plik services nie może mieć rozszerzonej listy ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN003950	Plik hosts.lpd (lub jego odpowiednik) nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 5. Wymagania listy kontroli dostępu Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN004010	Plik traceroute nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN004390	Plik alias nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN004430	Pliki uruchamiane za pomocą pliku aliases poczty nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN004510	Plik dziennika usługi SMTP nie może mieć rozszerzonej listy ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN004950	Plik ftpusers nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 5. Wymagania listy kontroli dostępu Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN005190	Pliki .Xauthority nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN005350	Pliki MIB nie mogą mieć rozszerzonych list ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN005375	Plik snmpd.conf nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN005395	Plik /etc/syslog.conf nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN006150	Plik /usr/lib/smb.conf nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 5. Wymagania listy kontroli dostępu Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN006210	Plik /var/private/smbpasswd nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN006270	Plik /etc/news/hosts.nntp nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN006290	Plik /etc/news/hosts.nntp.nolimit nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN006310	Plik /etc/news/nnrp.access nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN006330	Plik /etc/news/passwd.nntp nie może mieć rozszerzonej listy kontroli dostępu (ACL).	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Wyłącza podaną rozszerzoną listę ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Tabela 5. Wymagania listy kontroli dostępu Departamentu Obrony (kontynuacja)

Identyfikator punktu kontrolnego STIG Departamentu Obrony	Opis	Położenie skryptu, w którym jest zdefiniowane działanie, oraz wyniki działania, które umożliwia zgodność
GEN008120	Jeśli w systemie do uzyskania informacji uwierzytelniania lub informacji o koncie jest używany protokół LDAP, plik /etc/ldap.conf (lub jego odpowiednik) nie może mieć rozszerzonej listy ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Zapewnia, że podane pliki nie mają rozszerzonej listy ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.
GEN008200	Jeśli w systemie do uzyskania informacji uwierzytelniania lub informacji o koncie jest używany protokół LDAP, odpowiednio plik lub katalog ośrodka certyfikacji TLS nie może mieć rozszerzonej listy ACL.	**Położenie** /etc/security/pscexpert/dodv2/acldodfiles **Działanie zgodności** Zapewnia, że podany plik lub katalog nie ma rozszerzonej listy ACL. **Uwaga:** To ustawienie nie jest automatycznie zmieniane, gdy strategia jest resetowana do domyślnej strategii systemu AIX za pomocą pliku DoDv2_to_AIXDefault.xml. Użytkownik musi ręcznie zmienić to ustawienie.

Informacje pokrewne:

Zgodność z normą Department of Defense STIG

Branża kart płatniczych - zgodność ze standardami bezpieczeństwa danych (DSS)

Branża kart płatniczych (Payment Card Industry - PCI) w standardzie bezpieczeństwa danych (Data Security Standard - DSS) dzieli zagadnienia związane z bezpieczeństwem informatycznym na 12 sekcji. Są one nazywane procedurami wymagań i oceny bezpieczeństwa.

Procedury oceny bezpieczeństwa i wymagań zdefiniowane przez PCI - DSS zawierają następujące elementy:

Wymaganie 1: należy zainstalować i utrzymywać konfigurację firewalla w celu ochrony danych posiadaczy kart płatniczych.

Udokumentuj listę usług i portów niezbędnych do prowadzenia działalności biznesowej. To wymaganie jest implementowane przez wyłączenie zbędnych lub niebezpiecznych usług.

Wymaganie 2: nie należy używać domyślnych haseł systemowych ani innych parametrów zabezpieczeń zdefiniowanych przez dostawcę.

Przed zainstalowaniem systemu w sieci należy zawsze zmienić wartości domyślne zdefiniowane przez dostawcę. To wymaganie jest implementowane przez wyłączenie demona SNMP (Simple Network Management Protocol).

Wymaganie 3: należy chronić przechowywane dane posiadaczy kart płatniczych.

To wymaganie jest implementowane przez włączenie szyfrowanego systemu plików EFS (Encrypted File System), który jest składnikiem systemu operacyjnego AIX.

Wymaganie 4: należy szyfrować dane posiadaczy kart płatniczych podczas przesyłania przez sieci publiczne.

To wymaganie jest implementowane przez włączenie funkcji IPSEC, która jest składnikiem systemu operacyjnego AIX.

Wymaganie 5: należy korzystać z oprogramowania antywirusowego i regularnie je aktualizować.
To wymaganie jest implementowane przez użycie programu Trusted Execution. Program Trusted Execution jest zalecanym oprogramowaniem antywirusowym, który jest przeznaczony dla systemu operacyjnego AIX. PCI wymaga przechwytywania dzienników z programu Trusted Execution przez włączenie komponentu SIEM (Security Information and Event Management) do monitorowania alertów. Gdy program Trusted Execution działa w trybie tylko rejestrowania, nie zatrzymuje sprawdzania, gdy błąd zostanie spowodowany przez niezgodność sumy kontrolnej.

Wymaganie 6: należy rozwijać i obsługiwać bezpieczne systemy i aplikacje.
To wymaganie jest implementowane przez ręczne zainstalowanie wymaganych poprawek w systemie. Klienci, którzy zakupili program PowerSC Standard Edition, mogą użyć funkcji TNC (Trusted Network Connect).

Wymaganie 7: tylko niezbędny personel może mieć dostęp do danych posiadaczy kart płatniczych.
Rozbudowaną kontrolę dostępu można zastosować, stosując funkcje RBAC działającą z użyciem ról i reguł. Funkcja RBAC nie może być zautomatyzowana, ponieważ wymaga wprowadzania danych przez administratora.

Skrypt RbacEnablement sprawdza, czy w systemie istnieją właściwości isso, so, oraz sa dla ról. Jeśli właściwości te nie istnieją, skrypt tworzy je. Ten skrypt jest również uruchamiany, gdy pscexpert sprawdza kompletność uruchamianych komend, na przykład pscxpert -c.

Wymaganie 8: każda osoba, która ma dostęp do komputera, musi mieć unikalny identyfikator.
To wymaganie można spełnić przez włączenie profili PCI. Do profilu PCI mają zastosowanie następujące reguły:

- Hasło użytkownika jest zmieniane przynajmniej raz na 90 dni.
- Wymagana minimalna długość hasła wynosi 7 znaków.
- Używane hasło musi zawierać cyfry i litery.
- Użytkownik nie może podać jako nowego hasła, które było używane wcześniej (ostatnie cztery hasła).
- Należy ograniczać nieudane próby zalogowania się przez blokowanie użytkownika po sześciu nieudanych próbach zalogowania.
- Czas blokowania należy ustawić na 30 minut albo na ręczne odblokowanie użytkownika przez administratora.
- Jeśli terminal nie był używany przez 15 minut, użytkownik musi ponownie podać swoje hasło, aby reaktywować terminal.

Wymaganie 9: należy ograniczyć fizyczny dostęp do danych posiadaczy kart płatniczych.
Repozytoria, które zawierają dane posiadaczy kart płatniczych, muszą być zainstalowane w pomieszczeniu o ograniczonym dostępie.

Wymaganie 10: należy śledzić i monitorować dostęp do wszystkich zasobów sieciowych i danych posiadaczy kart płatniczych.
To wymaganie jest implementowane przez włączenie automatycznego rejestrowanie dostępu do komponentów systemu.

Wymaganie 11: należy regularnie testować systemy i procesy zabezpieczeń.
To wymaganie jest implementowane przez zastosowanie funkcji Real-Time Compliance.

Wymaganie 12: należy opracować strategię bezpieczeństwa, która obejmuje bezpieczeństwo informacji dla pracowników i podwykonawców.
Modemy dostępowe dla dostawców należy aktywować tylko wtedy, gdy są potrzebne. Należy je dezaktywować natychmiast po użyciu. To wymaganie jest implementowane przez wyłączanie zdalnego logowania użytkownika root, aktywowanie go tylko na żądanie przez administratora systemu, a następnie dezaktywowanie, gdy dostęp nie jest już potrzebny.

PowerSC Standard Edition zmniejsza zarządzanie konfiguracją, które jest niezbędne do spełnienia wytycznych zamieszczonych w dokumencie PCI DSS w wersji 2.0 i PCI DSS w wersji 3.0. Nie można jednak zautomatyzować całego procesu.

Na przykład ograniczanie dostępu do danych posiadaczy kart płatniczych na podstawie potrzeb biznesowych nie może być zautomatyzowane. System operacyjny AIX udostępnia silne technologie bezpieczeństwa, takie jak kontrola dostępu na podstawie roli (Role Based Access Control - RBAC). Program PowerSC Standard Edition nie może jednak zautomatyzować tej konfiguracji, ponieważ nie może określić, kto potrzebuje dostępu do danych, a kto nie. IBM Compliance Expert może zautomatyzować konfigurowanie innych ustawień zabezpieczeń wymaganych przez PCI.

Gdy profil PCI jest stosowany w środowisku bazy danych, blokowanych jest kilka portów TCP i UDP używanych przez oprogramowanie. Konieczne może być włączenie tych portów i wyłączenie funkcji Trusted Execution, aby umożliwić działanie aplikacji. Uruchom następujące komendy, aby usunąć ograniczenia portów i wyłączyć funkcję Trusted Execution:

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

Uwaga: Wszystkie pliki skryptów niestandardowych, które są udostępniane w celu zapewnienia zgodności z PCI - DSS, znajdują się w katalogu /etc/security/pscexpert/bin.

W poniższej tabeli przedstawiono sposób, w jaki sposób program PowerSC Standard Edition spełnia wymagania standardu PCI DSS za pomocą narzędzia AIX Security Expert:

Tabela 6. Ustawienia dotyczące zgodności ze standardem PCI DSS 2.0 i 3.0

Implementuje następujące standardy PCI DSS	Specyfikacja implementacji	Implementacja narzędzia AIX Security Expert	Skrypt, który modyfikuje wartość
2.1	Przed zainstalowaniem systemu w sieci należy zawsze zmienić wartości domyślne zdefiniowane przez dostawcę. Na przykład hasła i łańcuchy społeczności SNMP. Należy też usunąć zbędne konta.	Ustawia minimalną liczbę tygodni, która musi upłynąć, aby można było zmienić hasło, na 0 (przez ustawienie wartości parametru **minage** na 0).	/etc/security/pscexpert/bin/chusrattr
PCI v2 8.5.9 **PCI v3** 8.2.4	Hasło użytkownika jest zmieniane przynajmniej raz na 90 dni.	Ustawia maksymalną liczbę tygodni, przez które hasło jest ważne, na 13 tygodni (przez ustawienie wartości parametru **maxage** na 13).	/etc/security/pscexpert/bin/chusrattr
2.1	Przed zainstalowaniem systemu w sieci należy zawsze zmienić wartości domyślne zdefiniowane przez dostawcę. Na przykład hasła i łańcuchy społeczności SNMP. Należy też usunąć zbędne konta.	Ustawia liczbę tygodni, przez które konto z przedawnionym hasłem pozostaje w systemie, na wartość 8 (przez ustawienie wartości parametru **maxexpired** na 8).	/etc/security/pscexpert/bin/chusrattr
PCI v2 8.5.10 **PCI v3** 8.2.3	Wymagana minimalna długość hasła wynosi 7 znaków.	Ustawia minimalną długość hasła na 7 znaków przez ustawienie wartości parametru **minlen** na 7.	/etc/security/pscexpert/bin/chusrattr
PCI v2 8.5.11 **PCI v3** 8.2.3	Należy używać haseł, które zawierają zarówno cyfry, jak i litery.	Ustawia minimalną liczbę wymaganych liter w haśle na 1. Zapewnia to, że hasło zawiera przynajmniej jedną literę, ustawiając wartość parametru **minalpha** na 1.	/etc/security/pscexpert/bin/chusrattr

Tabela 6. Ustawienia dotyczące zgodności ze standardem PCI DSS 2.0 i 3.0 (kontynuacja)

Implementuje następujące standardy PCI DSS	Specyfikacja implementacji	Implementacja narzędzia AIX Security Expert	Skrypt, który modyfikuje wartość
PCI v2 8.5.11 **PCI v3** 8.2.3	Należy używać haseł, które zawierają zarówno cyfry, jak i litery.	Ustawia minimalną liczbę wymaganych znaków specjalnych w haśle na 1. Zapewnia to, że hasło zawiera przynajmniej jeden znak inny niż litera, ustawiając wartość parametru **minother** na 1.	/etc/security/pscexpert/bin/chusrattr
PCI v2 2.1 **PCI v3** 8.2.2	Przed zainstalowaniem systemu w sieci należy zawsze zmienić wartości domyślne zdefiniowane przez dostawcę. Na przykład hasła i łańcuchy społeczności SNMP. Należy też usunąć zbędne konta.	Ustawia maksymalną liczbę powtórzeń znaku w haśle na 8, ustawiając wartość parametru **maxrepeats** na 8. To ustawienie oznacza, że znak w haśle może być powtórzony nieograniczoną liczbę razy, gdy spełnione są inne ograniczenia hasła.	/etc/security/pscexpert/bin/chusrattr
PCI v2 8.5.12 **PCI v3** 8.2.5	Użytkownik nie może podać jako nowego hasła, które było używane wcześniej (ostatnie cztery hasła).	Ustawia liczbę tygodni, które muszą upłynąć, aby hasło mogło zostać ponownie wykorzystane, na 52 tygodnie (przez ustawienie wartości parametru **histexpire** na 52).	/etc/security/pscexpert/bin/chusrattr
PCI v2 8.5.12 **PCI v3** 8.2.5	Użytkownik nie może podać jako nowego hasła, które było używane wcześniej (ostatnie cztery hasła).	Ustawia liczbę poprzednich haseł, których nie można wykorzystać, na 4 (ustawiając wartość parametru **histsize** na 4).	/etc/security/pscexpert/bin/chusrattr
PCI v2 8.5.13 **PCI v3** 8.1.6	Należy ograniczać nieudane próby zalogowania się przez blokowanie użytkownika po sześciu nieudanych próbach zalogowania.	Ustawia liczbę kolejnych nieudanych operacji logowania, które powodują zablokowanie konta nieadministracyjnego, na 6 prób (przez ustawienie wartości parametru **loginentries** na 6).	/etc/security/pscexpert/bin/chusrattr
PCI v2 8.5.13 **PCI v3** 8.1.6	Należy ograniczać nieudane próby zalogowania się przez blokowanie użytkownika po sześciu nieudanych próbach zalogowania.	Ustawia liczbę kolejnych nieudanych operacji logowania, które powodują zablokowanie port, na 6 prób (przez ustawienie wartości parametru **logindisable** na 6).	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg
PCI v2 8.5.14 **PCI v3** 8.1.7	Czas blokowania należy ustawić przynajmniej na 30 minut albo na ręczne odblokowanie użytkownika przez administratora.	Określa czas, przez który port będzie zablokowany po tym, jak został wyłączony na 30 minut przez działanie atrybutu *logindisable* przez ustawienie wartości parametru **loginreenable** na 30.	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg
12.3.9	Aktywowanie zdalnego dostępu dla dostawców i partnerów biznesowych tylko wtedy, gdy jest to niezbędne. Dostęp ten należy wyłączyć natychmiast po użyciu.	Wyłącza funkcję zdalnego logowania administratora (root), ustawiając wartość parametru na false. Administrator systemu może aktywować funkcję zdalnego logowania, jeśli zajdzie taka potrzeba, a następnie dezaktywować ją po wykonaniu zadania.	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user

Tabela 6. Ustawienia dotyczące zgodności ze standardem PCI DSS 2.0 i 3.0 (kontynuacja)

Implementuje następujące standardy PCI DSS	**Specyfikacja implementacji**	**Implementacja narzędzia AIX Security Expert**	**Skrypt, który modyfikuje wartość**
8.1.1	Należy wszystkim użytkownikom przypisać unikalne identyfikatory przed umożliwieniem im dostępu do komponentów systemu lub danych posiadaczy kart płatniczych.	Włącza funkcję, która zapewnia, że wszyscy użytkownicy mają unikalną nazwę, zanim będą oni mogli uzyskać dostęp do komponentów systemu lub danych posiadaczy karty płatniczych (przez ustawienie wartości funkcji na true (prawda)).	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user
10.2	Należy włączyć kontrolę w systemie.	Włącza kontrolę plików binarnych w systemie.	/etc/security/pscexpert/bin/pciaudit
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć środowisko CDE (Common Desktop Environment).	Wyłącza środowisko CDE, gdy narzędzie LFT (layer four traceroute) nie jest skonfigurowane.	/etc/security/pscexpert/bin/comntrows
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona timed.	Zatrzymuje pracę demona timed i przekształca w komentarz odpowiednią instrukcję w pliku /etc/rc.tcpip, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/rctcpip
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona rwhod.	Zatrzymuje pracę demona rwhod i przekształca w komentarz odpowiednią instrukcję w pliku /etc/rc.tcpip, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/rctcpip
PCI v2 2.1 **PCI v3** 2.1.1	Przed zainstalowaniem systemu w sieci należy zawsze zmienić wartości domyślne zdefiniowane przez dostawcę. Należy też wyłączyć demona SNMP.	Zatrzymuje pracę demona SNMP i przekształca w komentarz odpowiednią instrukcję w pliku /etc/rc.tcpip, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/rctcpip
PCI v2 2.1 **PCI v3** 2.1.1	Przed zainstalowaniem systemu w sieci należy zawsze zmienić wartości domyślne zdefiniowane przez dostawcę. Należy też wyłączyć demona SNMPMIBD.	Wyłącza demona SNMPMIBD i przekształca w komentarz odpowiednią instrukcję w pliku /etc/rc.tcpip, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/rctcpip
2.1	Przed zainstalowaniem systemu w sieci należy zawsze zmienić wartości domyślne zdefiniowane przez dostawcę. Należy też wyłączyć demona AIXMIBD.	Wyłącza demona AIXMIBD i przekształca w komentarz odpowiednią instrukcję w pliku /etc/rc.tcpip, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/rctcpip
2.1	Przed zainstalowaniem systemu w sieci należy zawsze zmienić wartości domyślne zdefiniowane przez dostawcę. Należy też wyłączyć demona HOSTMIBD.	Wyłącza demona HOSTMIBD i przekształca w komentarz odpowiednią instrukcję w pliku /etc/rc.tcpip, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/rctcpip
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona DPID2.	Zatrzymuje pracę demona DPID2 i przekształca w komentarz odpowiednią instrukcję w pliku /etc/rc.tcpip, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/rctcpip

Tabela 6. Ustawienia dotyczące zgodności ze standardem PCI DSS 2.0 i 3.0 (kontynuacja)

Implementuje następujące standardy PCI DSS	Specyfikacja implementacji	Implementacja narzędzia AIX Security Expert	Skrypt, który modyfikuje wartość
PCI v2 2.1 **PCI v3** 2.2.2	Przed zainstalowaniem systemu w sieci należy zawsze zmienić wartości domyślne zdefiniowane przez dostawcę. Należy też zatrzymać serwer DHCP.	Wyłącza serwer DHCP.	/etc/security/pscexpert/bin/rctcpip
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć agenta DHCP.	Zatrzymuje pracę agenta przekazywania DHCP i przekształca w komentarz odpowiednią instrukcję w pliku /etc/rc.tcpip, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/rctcpip
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona rshd.	Zatrzymuje i wyłącza wszystkie instancje demona rshd i usługi powłoki. Przekształca w komentarz odpowiednie instrukcje w pliku /etc/inetd.conf, aby zapobiec ich automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona rlogind.	Zatrzymuje i wyłącza wszystkie instancje demona rlogind i usługi rlogin. Narzędzie AIX Security Expert przekształca w komentarz odpowiednie instrukcje w pliku /etc/inetd.conf, aby zapobiec ich automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona rexecd.	Zatrzymuje i wyłącza wszystkie instancje demona rexecd. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona comsat.	Zatrzymuje i wyłącza wszystkie instancje demona comsat. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona fingerd.	Zatrzymuje i wyłącza wszystkie instancje demona fingerd. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona systat.	Zatrzymuje i wyłącza wszystkie instancje demona systat. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf

Tabela 6. Ustawienia dotyczące zgodności ze standardem PCI DSS 2.0 i 3.0 (kontynuacja)

Implementuje następujące standardy PCI DSS	**Specyfikacja implementacji**	**Implementacja narzędzia AIX Security Expert**	**Skrypt, który modyfikuje wartość**
2.1	Przed zainstalowaniem systemu w sieci należy zawsze zmienić wartości domyślne zdefiniowane przez dostawcę. Należy też zablokować komendę netstat.	Wyłącza komendę netstat, przekształcając w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.3	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona tftp.	Zatrzymuje i wyłącza wszystkie instancje demona tftp. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona talkd.	Zatrzymuje i wyłącza wszystkie instancje demona talkd. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona rquotad.	Zatrzymuje i wyłącza wszystkie instancje demona rquotad. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona rstatd.	Zatrzymuje i wyłącza wszystkie instancje demona rstatd. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona rusersd.	Zatrzymuje i wyłącza wszystkie instancje demona rusersd. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona rwalld.	Zatrzymuje i wyłącza wszystkie instancje demona rwalld. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf

Tabela 6. Ustawienia dotyczące zgodności ze standardem PCI DSS 2.0 i 3.0 (kontynuacja)

Implementuje następujące standardy PCI DSS	Specyfikacja implementacji	Implementacja narzędzia AIX Security Expert	Skrypt, który modyfikuje wartość
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona sprayd.	Zatrzymuje i wyłącza wszystkie instancje demona sprayd. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć demona pcnfsd.	Zatrzymuje i wyłącza wszystkie instancje demona pcnfsd. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć usługę TCP echo.	Zatrzymuje i wyłącza wszystkie instancje usługi echo(tcp). Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jej automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć usługę TCP discard.	Zatrzymuje i wyłącza wszystkie instancje usługi discard(tcp). Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jej automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć usługę TCP chargen.	Zatrzymuje i wyłącza wszystkie instancje usługi chargen(tcp). Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jej automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć usługę TCP daytime.	Zatrzymuje i wyłącza wszystkie instancje usługi daytime(tcp). Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jej automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć usługę TCP time.	Zatrzymuje i wyłącza wszystkie instancje usługi timed(tcp). Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jej automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć usługę UDP echo.	Zatrzymuje i wyłącza wszystkie instancje usługi echo(udp). Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jej automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf

Tabela 6. Ustawienia dotyczące zgodności ze standardem PCI DSS 2.0 i 3.0 (kontynuacja)

Implementuje następujące standardy PCI DSS	Specyfikacja implementacji	Implementacja narzędzia AIX Security Expert	Skrypt, który modyfikuje wartość
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć usługę UDP discard.	Zatrzymuje i wyłącza wszystkie instancje usługi discard(udp). Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jej automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć usługę UDP chargen.	Zatrzymuje i wyłącza wszystkie instancje usługi chargen(udp). Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jej automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć usługę UDP daytime.	Zatrzymuje i wyłącza wszystkie instancje usługi daytime(udp). Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jej automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć usługę UDP time.	Zatrzymuje i wyłącza wszystkie instancje usługi timed(udp). Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jej automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.3	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć usługę FTP.	Zatrzymuje i wyłącza wszystkie instancje demona ftpd. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.3	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć usługę telnet.	Zatrzymuje i wyłącza wszystkie instancje demona telnetd. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jego automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć usługę dtspc.	Zatrzymuje i wyłącza wszystkie instancje demona dtspc. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inittab, aby zapobiec automatycznemu uruchamianiu demona, gdy narzędzie LFT nie jest skonfigurowane i gdy środowisko CDE jest wyłączone w pliku /etc/inittab.	/etc/security/pscexpert/bin/cominetdconf

Tabela 6. Ustawienia dotyczące zgodności ze standardem PCI DSS 2.0 i 3.0 (kontynuacja)

Implementuje następujące standardy PCI DSS	Specyfikacja implementacji	Implementacja narzędzia AIX Security Expert	Skrypt, który modyfikuje wartość
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć usługę ttdbserver.	Zatrzymuje i wyłącza wszystkie instancje usługi ttdbserver. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jej automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 1.1.5 2.2.2 **PCI v3** 2.2.2	Należy wyłączyć zbędne i niebezpieczne usługi, w tym należy wyłączyć usługę cmsd.	Zatrzymuje i wyłącza wszystkie instancje usługi cmsd. Narzędzie AIX Security Expert przekształca w komentarz odpowiednią instrukcję w pliku /etc/inetd.conf, aby zapobiec jej automatycznemu uruchamianiu.	/etc/security/pscexpert/bin/cominetdconf
PCI v2 2.2.3 **PCI v3** 2.2.4	Należy skonfigurować parametry zabezpieczeń systemu, aby zapobiec niewłaściwemu użytkowaniu.	Usuwa komendy z ustawionym bitem SUID, przekształcając w komentarz odpowiednią pozycję w pliku /etc/inetd.conf, która automatycznie włącza komendy.	/etc/security/pscexpert/bin/rmsuidfrmrcmds
PCI v2 2.2.3 **PCI v3** 2.2.4	Należy skonfigurować parametry zabezpieczeń systemu, aby zapobiec niewłaściwemu użytkowaniu.	Włącza najniższy poziom bezpieczeństwa dla programu File Permissions Manager.	/etc/security/pscexpert/bin/filepermgr
PCI v2 2.2.3 **PCI v3** 2.2.4	Należy skonfigurować parametry zabezpieczeń systemu, aby zapobiec niewłaściwemu użytkowaniu.	Modyfikuje protokół NFS z użyciem ograniczających ustawień, które są zgodne z wymaganiami bezpieczeństwa PCI. Te ustawienia obejmują wyłączenie ograniczonego dostępu zdalnego użytkownika root i dostępu z użyciem anonimowego identyfikatora UID i GID.	/etc/security/pscexpert/bin/nfsconfig
PCI v2 2.2.2 **PCI v3** 2.2.3	Należy włączyć tylko niezbędne i bezpieczne usługi, protokoły, demony, itp. wymagane do poprawnej pracy systemu. Należy zastosować zabezpieczenia dla wszystkich wymaganych usług, protokołów i demonów, które są uważane za niebezpieczne.	Wyłącza demony rlogind, rshd i tftpd, które nie są bezpieczne.	/etc/security/pscexpert/bin/disrmtdmns
PCI v2 2.2.2 **PCI v3** 2.2.3	Należy włączyć tylko niezbędne i bezpieczne usługi, protokoły, demony, itp. wymagane do poprawnej pracy systemu. Należy zastosować zabezpieczenia dla wszystkich wymaganych usług, protokołów i demonów, które są uważane za niebezpieczne.	Wyłącza demony rlogind, rshd i tftpd, które nie są bezpieczne.	/etc/security/pscexpert/bin/rmrhostsnetrc

Tabela 6. Ustawienia dotyczące zgodności ze standardem PCI DSS 2.0 i 3.0 (kontynuacja)

Implementuje następujące standardy PCI DSS	Specyfikacja implementacji	Implementacja narzędzia AIX Security Expert	Skrypt, który modyfikuje wartość
PCI v2 2.2.2 **PCI v3** 2.2.3	Należy włączyć tylko niezbędne i bezpieczne usługi, protokoły, demony, itp. wymagane do poprawnej pracy systemu. Należy zastosować zabezpieczenia dla wszystkich wymaganych usług, protokołów i demonów, które są uważane za niebezpieczne.	Wyłącza demony logind, rshd i tftpdpci_rmetchostsequiv, które nie są bezpieczne.	/etc/security/pscexpert/bin/rmetchostsequiv
PCI v2 1.3.6 **PCI v3** 2.2.3	Należy zastosować inspekcję stanową lub filtrowanie pakietów, aby możliwe było nawiązywanie tylko dozwolonych połączeń sieciowych.	Włącza opcję sieciową **clean_partial_conns**, ustawiając jej wartość na 1.	/etc/security/pscexpert/bin/ntwkopts
PCI v2 2.2.2 **PCI v3** 2.2.3	Należy zastosować inspekcję stanową lub filtrowanie pakietów, aby możliwe było nawiązywanie tylko dozwolonych połączeń sieciowych.	Włącza zabezpieczenia TCP, ustawiając wartość opcji sieciowej **tcp_tcpsecure** na 7. To ustawienie zabezpiecza przed atakami polegającymi na wstawianiu fałszywych pakietów RST i SYN oraz danych w ustanowionych połączeniach.	/etc/security/pscexpert/bin/ntwkopts
1.2	Należy zabezpieczyć przed nieuprawnionym dostępem do nieużywanych portów.	Konfiguruje system do unikania hostów przez 5 minut, aby uniemożliwić innym systemom dostęp do nieużywanych portów.	/etc/security/pscexpert/bin/ipsecshunhosthls **Uwaga:** Do pliku /etc/security/aixpert/bin/filter.txt można dodać dodatkowe reguły filtrowania. Reguły te są połączone w skrypcie ipsecshunhosthls.sh w przypadku stosowania profilu. Pozycje powinny być podane w następującym formacie: *numer_portu*:*adres_ip*: *działanie* Parametr *działanie* może mieć następujące wartości: Allow (zezwól) albo Deny (odmów).
1.2	Należy chronić host przed skanowaniem portów.	Konfiguruje system do wyłączania narażonych portów na 5 minut, co zapobiega skanowaniu portów.	/etc/security/pscexpert/bin/ipsecshunports **Uwaga:** Do pliku /etc/security/aixpert/bin/filter.txt można dodać dodatkowe reguły filtrowania. Reguły te są połączone w skrypcie ipsecshunhosthls.sh w przypadku stosowania profilu. Pozycje powinny być podane w następującym formacie: *numer_portu*:*adres_ip*: *działanie* Parametr *działanie* może mieć następujące wartości: Allow (zezwól) albo Deny (odmów).
7.1.1	Należy ograniczać uprawnienia do tworzenia obiektów.	Ustawia domyślne ustawienia tworzenia obiektów na 22, ustawiając wartość parametru **umask** na 22.	/etc/security/pscexpert/bin/chusrattr
7.1.1	Należy ograniczać dostęp do systemu.	Zapewnia, że identyfikator użytkownika root jest jedynym umieszczonym w pliku cron.allow i usuwa plik cron.deny z systemu.	/etc/security/pscexpert/bin/limitsysacc

Tabela 6. Ustawienia dotyczące zgodności ze standardem PCI DSS 2.0 i 3.0 (kontynuacja)

Implementuje następujące standardy PCI DSS	Specyfikacja implementacji	Implementacja narzędzia AIX Security Expert	Skrypt, który modyfikuje wartość
6.5.8	Należy usnąć kropkę ze ścieżki użytkownika root.	Usuwa kropkę ze zmiennej środowiskowej PATH w następujących plikach w katalogu osobistym użytkownika root: • .cshrc • .kshrc • .login • .profile	/etc/security/pscexpert/bin/rmdotfrmpathroot
6.5.8	Należy usnąć kropkę ze ścieżki użytkownika innego niż root.	Usuwa kropkę ze zmiennej środowiskowej *PATH* w następujących plikach w katalogach osobistych użytkowników: • .cshrc • .kshrc • .login • .profile	/etc/security/pscexpert/bin/rmdotfrmpathnroot
2.2.3	Należy ograniczać dostęp do systemu.	Dodaje użytkownika root i nazwę użytkownika do pliku /etc/ftpusers.	/etc/security/pscexpert/bin/chetcftpusers
2.1	Należy usunąć konto gościa.	Usuwa konto użytkownika guest wraz z jego plikami.	/etc/security/pscexpert/bin/execmds
6.5.2	Należy zapobiegać uruchamianiu programów w segmentach danych.	Włącza funkcję SED (Stack Execution Disable).	/etc/security/pscexpert/bin/sedconfig
8.2	Należy zadbać o to, aby hasło użytkownika root nie było słabe.	Uruchamia sprawdzanie integralności hasła użytkownika root, zapewniając, że stosowane będzie tylko silne hasło.	/etc/security/pscexpert/bin/chuserstanza
PCI v2 8.5.15 **PCI v3** 8.1.8	Należy ograniczyć dostęp do systemu, ustawiając maksymalny czas bezczynności sesji.	Ustawia limit czasu bezczynności na 15 minut. Gdy sesja będzie bezczynna przez dłużej, niż 15 minut, użytkownik będzie musiał ponownie wprowadzić hasło.	/etc/security/pscexpert/bin/autologoff
1.3.5	Należy ograniczyć dostęp do informacji na temat posiadaczy kart płatniczych.	Ustawia wysokie ustawienia regulacji ruchu TCP, co wymusza ochronę przed atakami typu DOS.	/etc/security/pscexpert/bin/tcptr_pscexpert
1.3.5	Należy używać bezpiecznego połączenia podczas migrowania danych.	Włącza automatyczny tunel IPSec między serwerami VIOS podczas migrowania partycji.	/etc/security/pscexpert/bin/cfgsecmig
1.3.5	Należy ograniczać pakiety z nieznanych źródeł.	Zezwala na pakiety z konsoli HMC.	/etc/security/pscexpert/bin/ipsecpermithostorport
5.1.1	Należy stosować oprogramowanie antywirusowe.	Utrzymuje integralność systemu, wykrywając, usuwając i chroniąc przed znanymi typami złośliwego oprogramowania.	/etc/security/pscexpert/bin/manageITsecurity
PCI v2 Sekcja 7 **PCI v3** Sekcja 7	Należy nadawać dostęp tylko wtedy, gdy jest to niezbędne.	Należy włączyć kontrolę dostępu opartą na rolach (RBAC), tworząc role operatora systemu, administratora systemu i kierownika ds. bezpieczeństwa. Każda z tych ról powinna mieć tylko niezbędne uprawnienia.	/etc/security/pscexpert/bin/EnableRbac

Tabela 6. Ustawienia dotyczące zgodności ze standardem PCI DSS 2.0 i 3.0 (kontynuacja)

Implementuje następujące standardy PCI DSS	**Specyfikacja implementacji**	**Implementacja narzędzia AIX Security Expert**	**Skrypt, który modyfikuje wartość**
PCI v2 Nieuwzględnione w profilu w wersji 2, dodano w wersji 3. **PCI v3** 2.3	Należy zastosować dodatkowe zabezpieczenia dla wszystkich wymaganych usług, protokołów i demonów, które są uważane za niebezpieczne.	Używa bezpiecznych technologii, takich jak SSH (Secure Shell), S-FTP (SSH File Transfer Protocol), SSL (Secure Sockets Layer) lub IPsec VPN (Internet Protocol Security Virtual Private Network), aby chronić niebezpieczne usługi, takie jak NetBIOS, udostępnianie plików, Telnet oraz FTP. Konfiguruje on również demon SSH do używania wyłącznie protokołu SSHv2.	/etc/security/pscexpert/bin/sshPCIconfig
PCI v2 Nieuwzględnione w profilu w wersji 2, dodano w wersji 3. **PCI v3** 2.3	Klient SSH musi być skonfigurowany do używania tylko protokołu SSHv2.	Konfiguruje klienta SSH, aby używał tylko protokołu SSHv2.	/etc/security/pscexpert/bin/sshPCIconfig
PCI v2 Nieuwzględnione w profilu w wersji 2, dodano w wersji 3. **PCI v3** 2.3	Demon SSH musi nasłuchiwać tylko na sieciowych adresach używanych do zarządzania, chyba że udzielono osobnej autoryzacji.	Zapewnia, że demon SSH jest skonfigurowany tylko do nasłuchiwania.	/etc/security/pscexpert/bin/sshPCIconfig
PCI v2 Nieuwzględnione w profilu w wersji 2, dodano w wersji 3. **PCI v3** 2.3	Demon SSH musi być skonfigurowany tak, aby używał wyłącznie szyfrów zgodnych ze standardem FIPS 140-2	Zapewnia, że demon SSH używa tylko szyfrów zgodnych z FIPS 140-2.	/etc/security/pscexpert/bin/sshPCIconfig
PCI v2 Nieuwzględnione w profilu w wersji 2, dodano w wersji 3. **PCI v3** 2.3	Demon SSH musi być skonfigurowany tak, aby używał wyłącznie algorytmów MAC (Message Authentication Code), które korzystają z kryptograficznych algorytmów mieszających zgodnych ze standardem1 FIPS 140-2.	Zapewnia, że używane są tylko zatwierdzone algorytmy MAC.	/etc/security/pscexpert/bin/sshPCIconfig
PCI v2 Nieuwzględnione w profilu w wersji 2, dodano w wersji 3. **PCI v3** 2.3	Demon SSH musi ograniczać możliwość logowania tylko do konkretnych użytkowników lub grup.	Ogranicza logowanie w systemie do konkretnych użytkowników i grup.	/etc/security/pscexpert/bin/sshPCIconfig

Tabela 6. Ustawienia dotyczące zgodności ze standardem PCI DSS 2.0 i 3.0 (kontynuacja)

Implementuje następujące standardy PCI DSS		Specyfikacja implementacji	Implementacja narzędzia AIX Security Expert	Skrypt, który modyfikuje wartość
PCI v2	Nieuwzględnione w profilu w wersji 2, dodano w wersji 3.	System musi wyświetlać datę i godzinę ostatniego pomyślnego logowania po pomyślnym zalogowaniu się do konta.	Przechowuje informacje o ostatnim logowaniu się użytkownika i wyświetla je po następnym zalogowaniu.	/etc/security/pscexpert/bin/sshPCIconfig
PCI v3	2.3			
PCI v2	Nieuwzględnione w profilu w wersji 2, dodano w wersji 3.	Demon SSH musi wykonać ścisłe sprawdzanie plików konfiguracyjnych w katalogu osobistym.	Zapewnia, że pliki konfiguracyjne w katalogu osobistym mają ustawione poprawne tryby dostępu.	/etc/security/pscexpert/bin/sshPCIconfig
PCI v3	2.3			
PCI v2	Nieuwzględnione w profilu w wersji 2, dodano w wersji 3.	Demon SSH musi używać separacji uprawnień.	Zapewnia, że demon SSH ma odpowiednią separację uprawnień.	/etc/security/pscexpert/bin/sshPCIconfig
PCI v3	2.3			
PCI v2	Nieuwzględnione w profilu w wersji 2, dodano w wersji 3.	Demon SSH nie może zezwalać na uwierzytelnianie RSA przez hosty zdalne.	Wyłącza uwierzytelnianie RSA dla hostów zdalnych, gdy używany jest demon SSH.	/etc/security/pscexpert/bin/sshPCIconfig
PCI v3	2.3			
PCI v2	1.1.5 2.2.2	Należy sprawdzić standardy konfiguracji i procesy, aby upewnić się, że zaimplementowana została i jest na bieżąco aktualizowana technologia synchronizacji czasu (wymagania PCI DSS 6.1 oraz 6.2).	Włącza demona ntp.	/etc/security/pscexpert/bin/rctcpip
PCI v3	10.4			
PCI v2	Nieuwzględnione w profilu w wersji 2, dodano w wersji 3.	Należy wyłączyć konto użytkownika, gdy nie jest ono używane.	Wyłącza konta użytkowników po 35 dniach nieaktywności.	/etc/security/pscexpert/bin/disableacctpci
PCI v3	8.1.5			
PCI v3	2.2.3	Należy w aplikacjach wyłączyć używanie protokołów SSL v3 i TLS v1.0.	Wyłącza protokoły SSLv3 i TLS v1.0 w konfiguracji demona Courier POP3 (Pop3d).	/etc/security/pscexpert/bin/disableSSL
PCI v3	2.2.3	Należy w aplikacjach wyłączyć używanie protokołów SSL v3 i TLS v1.0.	Wyłącza protokoły SSLv3 i TLS v1.0 w konfiguracji demona Courier IMAP (imapd).	/etc/security/pscexpert/bin/disableSSL

Tabela 6. Ustawienia dotyczące zgodności ze standardem PCI DSS 2.0 i 3.0 (kontynuacja)

Implementuje następujące standardy PCI DSS	Specyfikacja implementacji	Implementacja narzędzia AIX Security Expert	Skrypt, który modyfikuje wartość
PCI v3 8.2.1	Należy w aplikacjach wyłączyć używanie protokołów SSL v3 i TLS v1.0.	Sprawdza plik konfiguracyjny NTP (Network Time Protocol) w celu zastosowania protokołu TLS 1.1 lub nowszego.	/etc/security/pscexpert/bin/checkNTP
PCI v3 2.2.3	Należy w aplikacjach wyłączyć używanie protokołów SSL v3 i TLS v1.0.	Sprawdza plik konfiguracyjny FTPD (File Transfer Protocol Daemon) w celu zastosowania protokołu TLS 1.1 lub nowszego.	/etc/security/pscexpert/bin/secureFTP
PCI v3 2.2.3	Należy w aplikacjach wyłączyć używanie protokołów SSL v3 i TLS v1.0.	Sprawdza plik konfiguracyjny FTP (File Transfer Protocol) w celu zastosowania protokołu TLS 1.1 lub nowszego.	/etc/security/pscexpert/bin/secureFTP
PCI v3 2.2.3	Należy w aplikacjach wyłączyć używanie protokołów SSL v3 i TLS v1.0.	Wyłącza protokoły SSLv3 i TLS v1.0 w konfiguracji demona sendmail.	/etc/security/pscexpert/bin/sendmailPCIConfig
PCI v3 2.2.3	Należy w aplikacjach wyłączyć używanie protokołów SSL v3 i TLS v1.0.	Sprawdza, czy wersja protokołu SSL w systemie AIX jest nowsza od 1.0.2.	/etc/security/pscexpert/bin/sslversion
PCI v3 8.2.1	Należy wymusić uwierzytelnianie dwuskładnikowe.	Należy wymusić uwierzytelnianie dwuskładnikowe, na przykład SHA-256 lub SHA-512.	/etc/security/pscexpert/bin/pwdalgchk

Informacje pokrewne:

Branża kart płatniczych - zgodność ze standardami bezpieczeństwa danych (DSS)

Zgodność z Sarbanes-Oxley Act i COBIT

Ustawa Sarbanes-Oxley (SOX) Act z 2002 r. opracowana na 107. Kongresie Stanów Zjednoczonych nadzoruje kontrolę przedsiębiorstw publicznych, które podlegają ustawodawstwu w zakresie papierów wartościowych i spraw pokrewnych, w celu zabezpieczenia interesów inwestorów.

W sekcji 404 ustawy SOX wprowadzono ocenę zarządzania nad kontrolami wewnętrznymi. W przypadku większości organizacji kontrola wewnętrzna obejmuje systemy informatyczne, które przetwarzają i raportują dane finansowe przedsiębiorstwa. Ustawa SOX zawiera konkretne szczegóły dotyczące zagadnień informatycznych i bezpieczeństwa informatycznego. Wielu rewidentów SOX korzysta ze standardów, takich jak COBIT, jako metod mierzenia i kontrolowania właściwego nadzoru i kontroli nad zasobami informatycznymi. Opcja konfiguracyjna XML standardu SOX/COBIT w programie PowerSC Standard Edition udostępnia konfigurację zabezpieczeń systemów AIX i serwer VIOS (VIOS), która jest wymagana do spełnienia wytycznych dotyczących zgodności ze standardem COBIT.

Program IBM Compliance Expert Express Edition działa w następujących wersjach systemu operacyjnego AIX:

- AIX 6.1
- AIX 7.1
- AIX 7.2

Za zgodność ze standardami zewnętrznymi odpowiada administrator systemu AIX. Program IBM Compliance Expert Express Edition został zaprojektowany po to, aby uprościć zarządzanie ustawieniami systemów operacyjnych i raportami wymaganymi na potrzeby zgodności ze standardami.

Wstępnie skonfigurowane profile zgodności dostarczane z programem IBM Compliance Expert Express Edition zmniejszają obciążenie administratora związane z interpretowaniem dokumentacji dotyczącej zgodności i implementowaniem tych standardów jako konkretnych parametrów konfiguracji systemu.

Możliwości programu IBM Compliance Expert Express Edition zaprojektowano w taki sposób, aby ułatwić klientom efektywne zarządzanie wymaganiami systemowymi powiązanymi ze zgodnością ze standardami zewnętrznymi, co może obniżyć koszty, jednocześnie usprawniając zachowanie zgodności. Wszystkie zewnętrzne standardy bezpieczeństwa obejmują aspekty inne niż ustawienia konfiguracji systemu. Użycie programu IBM Compliance Expert Express Edition nie może zapewnić zgodności z tymi standardami. Program Compliance Expert został zaprojektowany w taki sposób, aby uprościć zarządzanie ustawieniami konfiguracji systemów, dzięki czemu administratorzy mogą skupić się na pozostałych aspektach zgodności ze standardami.

Informacje pokrewne:

Zgodność z COBIT

Ustawa Health Insurance Portability and Accountability Act (HIPAA)

Ustawa Health Insurance Portability and Accountability Act (HIPAA) to profil zabezpieczeń skupiający się na ochronie danych EPHI (Electronically Protected Health Information - Elektronicznie chronione informacje dotyczące zdrowia).

Reguła zabezpieczeń HIPAA skupia się w szczególności na ochronie informacji EPHI i tylko niektóre agencje mają podlegać regule zabezpieczeń HIPAA w oparciu o ich funkcję i korzystanie z informacji EPHI.

Wszystkie obsługiwane obiekty HIPAA, podobnie jak niektóre instytucje rządowe, muszą być zgodne z regułą zabezpieczeń HIPAA.

Reguła zabezpieczeń HIPAA skupia się na ochronie poufności, integralności i dostępności informacji EPHI zgodnie z definicją w regule zabezpieczeń.

Informacje EPHI, którą obsługiwany obiekt tworzy, odbiera, przechowuje lub wysyła, muszą być chronione przed przewidywalnymi zagrożeniami, narażeniem na niedozwolone użycie oraz ujawnienie.

Wymagania, standardy i specyfikacje implementacji reguły bezpieczeństwa HIPAA dotyczą następujących obsługiwanych obiektów:

- Świadczący opiekę zdrowotną
- Plany zdrowia
- Izby rozrachunkowe służby zdrowia
- Recepty opieki zdrowotnej i sponsorzy kart leków

Poniższa tabela zawiera szczegóły dotyczące kilku sekcji reguły zabezpieczeń HIPAA, a każda sekcja zawiera kilka standardów i specyfikacji implementacji.

Uwaga: Wszystkie niestandardowe pliki skryptowe dostarczone w celu zachowania zgodności z wymaganiami ustawy HIPAA znajdują się w katalogu /etc/security/pscexpert/bin.

Tabela 7. Reguły i szczegóły implementacji ustawy HIPAA

Sekcje reguły bezpieczeństwa HIPAA	Specyfikacja implementacji	Implementacja w interfejsie aixpert	Komendy i wartości zwracane
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 164.312 (b)	Implementuje procedury regularnego sprawdzania rekordów aktywności systemu informacyjnego, takich jak dzienniki kontroli, raporty dostępu i raporty incydentów bezpieczeństwa.	Określa, czy w systemie jest włączona kontrola.	**Komenda**: **#audit query**. **Wartość zwracana**: w przypadku powodzenia komenda kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z wartością 1.

Tabela 7. Reguły i szczegóły implementacji ustawy HIPAA (kontynuacja)

Sekcje reguły bezpieczeństwa HIPAA	Specyfikacja implementacji	Implementacja w interfejsie aixpert	Komendy i wartości zwracane
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 166.312 (b)	Implementuje procedury regularnego sprawdzania rekordów aktywności systemu informacyjnego, takich jak dzienniki kontroli, raporty dostępu i raporty incydentów bezpieczeństwa.	Włącza kontrolę w systemie. Ponadto konfiguruje zdarzenia do przechwytywania.	**Komenda**: **# audit start >/dev/null 2>&1**. **Wartość zwracana**: w przypadku powodzenia komenda kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z wartością 1. Kontrolowane są następujące zdarzenia: **FILE_Mknod, FILE_Open, FS_Mkdir, PROC_Execute, DEV_Create, FILE_Acl, FILE_Chpriv, FILE_Fchpriv, FILE_Mode, INIT_Start, PASSWORD_Change, PASSWORD_Check, PROC_Adjtime, PROC_Kill, PROC_Privilege, PROC_Setpgid, USER_SU, USER_Change, USER_Create, USER_Login, USER_Logout, USER_Reboot, USER_Remove, USER_SetEnv, USER_SU, FILE_Acl,FILE_Fchmod, FILE_Fchown**
164.312 (a) (2) (iV)	Szyfrowanie i deszyfrowanie (A):Implementuje mechanizm do szyfrowania i deszyfrowania informacji EPHI.	Określa, czy w systemie jest włączony szyfrowany system plików (EFS).	**Komenda**: **# efskeymgr -V >/dev/null 2>&1**. **Wartość zwracana**: jeśli włączono już system EFS, komenda kończy działanie z wartością 0. Jeśli nie włączono systemu EFS, komenda kończy działanie z wartością 1.
164.312 (a) (2) (iii)	Automatyczne wylogowanie (A): Implementuje procedury elektroniczne do zakończenia sesji elektronicznej po upływie predefiniowanego czasu nieaktywności.	Konfiguruje system w celu wylogowania się z procesów interaktywnych po 15 minutach braku aktywności.	**Komenda**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1** **echo "TMOUT=900 ; TIMEOUT=900; export TMOUT TIMEOUT**. **Wartość zwracana**: jeśli nie powiedzie się znalezienie przez komendę wartości **TMOUT=15**, skrypt kończy działanie z wartością 1. W przeciwnym razie komenda kończy działanie z wartością 0.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Zapewnia, że wszystkie hasła zawierają przynajmniej 14 znaków.	**Komenda**: **chsec -f /etc/security/user -s user -a minlen=8**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia skrypt kończy działanie z kodem błędu 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Zapewnia, że wszystkie hasła zawierają przynajmniej dwa znaki alfabetu, z których jeden musi być wielką literą.	**Komenda**: **chsec -f /etc/security/user -s user –a minalpha=4**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z kodem błędu 1.

Tabela 7. Reguły i szczegóły implementacji ustawy HIPAA (kontynuacja)

Sekcje reguły bezpieczeństwa HIPAA	Specyfikacja implementacji	Implementacja w interfejsie aixpert	Komendy i wartości zwracane
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Określa minimalną liczbę znaków niealfabetycznych w haśle na 2.	**Komenda**: **#chsec –f /etc/security/user –s user –a minother=2**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z kodem błędu 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Zapewnia, że żadne hasła nie zawierają powtarzających się znaków.	**Komenda**: **#chsec –f /etc/security/user –s user –a maxrepeats=1**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z kodem błędu 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Zapewnia, że hasło nie zostanie ponownie wykorzystane wcześniej niż po pięciu zmianach.	**Komenda**: **#chsec –f /etc/security/user –s user –a histsize=5**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z kodem błędu 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Określa maksymalną liczbę tygodni, przez jaką hasło pozostanie ważne, na 13.	**Komenda**: **#chsec –f /etc/security/user –s user –a maxage=8**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z kodem błędu 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Usuwa wszystkie wymagania dotyczące minimalnej liczby tygodni, przed upływem których hasło nie może zostać zmienione.	**Komenda**: **#chsec –f /etc/security/user –s user –a minage=2**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z kodem błędu 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Określa na 4 maksymalną liczbę tygodni do zmiany hasła, które utraciło ważność, po utracie ważności wartości parametru **maxage** ustawionego przez użytkownika.	**Komenda**: **#chsec –f /etc/security/user –s user –a maxexpired=4**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z kodem błędu 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Określa minimalną liczbę znaków, które nie mogą zostać powtórzone ze starego hasła, na 4.	**Komenda**: **#chsec –f /etc/security/user –s user –a mindiff=4**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z kodem błędu 1.

Tabela 7. Reguły i szczegóły implementacji ustawy HIPAA (kontynuacja)

Sekcje reguły bezpieczeństwa HIPAA	Specyfikacja implementacji	Implementacja w interfejsie aixpert	Komendy i wartości zwracane
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Określa, że liczba dni oczekiwania zanim system wyśle ostrzeżenie o wymaganej zmianie hasła wynosi 5.	**Komenda**: **#chsec –f /etc/security/user –s user –a pwdwarntime = 5**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z kodem błędu 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Powoduje sprawdzenie poprawności definicji użytkowników i naprawia błędy.	**Komenda**: **/usr/bin/usrck -y ALL** **/usr/bin/usrck –n ALL**. **Wartość zwracana**: komenda nie zwraca wartości. Komenda sprawdza i naprawia błędy, jeśli istnieją.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Blokuje konto po trzech kolejnych zakończonych niepowodzeniem próbach logowania.	**Komenda**: **#chsec –f /etc/security/user –s user –a loginretries=3**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z kodem błędu 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Określa opóźnienie między jednym logowaniem zakończonym niepowodzeniem a drugim na 5 sekund.	**Komenda**: **chsec -f /etc/security/login.cfg -s default -a logindelay=5**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z kodem błędu 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Określa liczbę nieudanych prób logowania na porcie, po wystąpieniu których port zostanie zablokowany, na 10 sekund.	**Komenda**: **chsec -f /etc/security/lastlog -s username -a \ unsuccessful_login_count=10**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z kodem błędu 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Określa przedział czasu w porcie dla nieudanych prób logowania zanim port zostanie wyłączony na 60 sekund.	**Komenda**: **#chsec -f /etc/security/lastlog -s user –a time_last_unsuccessful_ login=60**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z kodem błędu 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Określa przedział czasu, po upływie którego port zostaje odblokowany po wyłączeniu, na 30 minut.	**Komenda**: **#chsec -f /etc/security/login.cfg -s default -a loginreenable = 30**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z kodem błędu 1.

Tabela 7. Reguły i szczegóły implementacji ustawy HIPAA (kontynuacja)

Sekcje reguły bezpieczeństwa HIPAA	Specyfikacja implementacji	Implementacja w interfejsie aixpert	Komendy i wartości zwracane
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Określa przedział czasu na wpisanie hasła na 30 sekund.	**Komenda**: **chsec -f /etc/security/login.cfg -s usw -a logintimeout=30**. **Wartość zwracana**: w przypadku powodzenia skrypt kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z kodem błędu 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Zarządzanie hasłami (A):Implementuje procedury tworzenia, zmiany i zabezpieczania haseł.	Zapewnia, że konta są blokowane po 35 dniach nieaktywności.	**Komenda**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1if TMOUT = (35x24x60x60){#chsec -f /etc/security/user -s user -aaccount_locked = true}**. **Wartość zwracana**: jeśli nie powiedzie się ustawienie przez komendę wartości **account_locked** na **true**, skrypt kończy działanie z wartością 1. W przeciwnym razie komenda kończy działanie z wartością 0.
164.312 (c) (1)	Implementuje strategie i procedury w celu zabezpieczenia informacji EPHI przed niepoprawną zmianą lub zniszczeniem.	Ustawia strategie zaufanego wykonywania na ON (włączone).	**Komenda**: Włącza: **CHKEXEC, CHKSHLIB, CHKSCRIPT, CHKKERNEXT, STOP_ON_CHKFAIL,TE=ON, na przykład: trustchk –p TE=ON CHKEXEC = ON, CHKSHLIB,=ON, CHKSCRIPT=ON, CHKKERNEXT = ON**. **Wartość zwracana**: w przypadku niepowodzenia skrypt kończy działanie z wartością 1.
164.312 (e) (1)	Implementuje środki bezpieczeństwa technicznego, aby uniemożliwić nieautoryzowany dostęp do informacji EPHI podczas ich przesyłania przez sieć komunikacji elektronicznej.	Określa, czy są zainstalowane zestawy plików **ssh**. Jeśli nie są, wyświetlany jest komunikat o błędzie.	**Komenda**: **# lslpp –l | grep openssh > /dev/null 2>&1**. **Wartość zwracana**: jeśli kod powrotu dla tej komendy wynosi 0, skrypt kończy działanie z wartością 0. Jeśli zestawy plików ssh nie są zainstalowane, skrypt kończy działanie z wartością 1 i wyświetla komunikat o błędzie Zainstaluj zestawy plików ssh dla bezpiecznej transmisji.

Poniższa tabela zawiera szczegóły dotyczące kilku funkcji reguły zabezpieczeń HIPAA, a każda funkcja zawiera kilka standardów i specyfikacji implementacji.

Tabela 8. Funkcje i szczegóły implementacji ustawy HIPAA

Funkcje HIPAA	Specyfikacja implementacji	Implementacja w interfejsie aixpert	Komendy i wartości zwracane
Rejestrowanie błędów	Konsoliduje błędy z różnych dzienników i wysyła je pocztą elektroniczną do administratora.	Określa, czy istnieją jakiekolwiek błędy sprzętu. Określa, czy istnieją błędy nienaprawialne, na podstawie pliku **trcfile** z katalogu /var/adm/ras/trcfile. Wysyła błędy na adres **root@<nazwa_hosta>**.	**Komenda**: **errpt -d H**. **Wartość zwracana**: w przypadku powodzenia komenda kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z wartością 1.

Tabela 8. Funkcje i szczegóły implementacji ustawy HIPAA (kontynuacja)

Funkcje HIPAA	Specyfikacja implementacji	Implementacja w interfejsie aixpert	Komendy i wartości zwracane
Włączenie FPM	Zmienia uprawnienia do plików.	Zmienia uprawnienia plików na podstawie listy uprawnień i plików za pomocą komendy **fpm**.	**Komenda**: **# fpm -l <poziom> -f <plik komend>**. **Wartość zwracana**: w przypadku powodzenia komenda kończy działanie z wartością 0. W przypadku niepowodzenia komenda kończy działanie z wartością 1.
Włączenie RBAC	Tworzy użytkowników **isso**, **so** oraz **sa** i przypisuje odpowiednie role do tych użytkowników.	Sugeruje utworzenie użytkowników **isso**, **so** oraz **sa**. Przypisuje odpowiednie role do tych użytkowników.	**Komenda**: **/etc/security/pscexpert/bin/RbacEnablement**.

Informacje pokrewne:

Ustawa Health Insurance Portability and Accountability Act (HIPAA)

Zgodność z normami NERC (North American Electric Reliability Corporation)

North American Electric Reliability Corporation (NERC) jest organizacją niekomercyjną, która opracowuje standardy na potrzeby branży energetycznej. Program PowerSC Standard Edition zawiera wstępnie skonfigurowany profil NERC zawierający standardy, które mogą być używane do ochrony krytycznych systemów energetycznych.

Profil NERC jest zgodny ze standardami CIP (Critical Infrastructure Protection).

Profil NERC jest zapisany w pliku /etc/security/aixpert/custom/NERC.xml. Można zresetować wymagania CIP, które są stosowane w profilu NERC, do stanu domyślnego, stosując profil NERC_to_AIXDefault.xml z katalogu /etc/security/aixpert/custom. Ten proces nie jest tożsamy z wycofaniem profilu NERC.

Poniższa tabela zawiera informacje na temat standardów CIP, które zostały zastosowane w systemie operacyjnym AIX, oraz sposób, w jaki produkt PowerSC Standard Edition obsługuje standardy CIP:

Tabela 9. Standardy CIP dla produktu PowerSC Standard Edition

Standard CIP	Implementacja narzędzia AIX Security Expert	Skrypt, który modyfikuje wartość
CIP-003-3 R5.1	Służy do konfigurowania parametrów zabezpieczeń systemu, aby zapobiec problemom, usuwając bity SUID i SGID z plików binarnych.	• /etc/security/pscexpert/bin/filepermgr • /etc/security/pscexpert/bin/rmsuidfrmrcmds
CIP-003-3 R5.1.1	Włącza kontrolę dostępu opartą na rolach (RBAC), tworząc role operatora systemu, administratora systemu i kierownika ds. bezpieczeństwa. Każda z tych ról powinna mieć tylko niezbędne uprawnienia.	/etc/security/pscexpert/bin/EnableRbac
CIP-005-3a R2.1-R2.4	Włącza bezpieczny dostęp przez używanie bezpiecznej powłoki SSH.	/etc/security/pscexpert/bin/sshstart
CIP-005-3a R2.5 CIP-007-5 R1.1	Wyłącza następujące zbędne i niebezpieczne usługi: • demon **lpd** • uniwersalne środowisko graficzne (CDE)	/etc/security/pscexpert/bin/comntrows

Tabela 9. Standardy CIP dla produktu PowerSC Standard Edition (kontynuacja)

Standard CIP	Implementacja narzędzia AIX Security Expert	Skrypt, który modyfikuje wartość
CIP-005-3a R2.5 CIP-007-5 R1.1	Wyłącza następujące zbędne i niebezpieczne usługi: • demon **timed** • demon **NTP** • demon **rwhod** • demon **DPID2** • agent DHCP	/etc/security/pscexpert/bin/rctcpip
CIP-005-3a R2.5 CIP-007-5 R1.1	Wyłącza następujące zbędne i niebezpieczne usługi: • demon **comsat** • demon **dtspcd** • demon **fingerd** • demon **ftpd** • demon **rshd** • demon **rlogind** • demon **rexecd** • demon **systat** • demon **tfptd** • demon **talkd** • demon **rquotad** • demon **rstatd** • demon **rusersd** • demon **rwalld** • demon **sprayd** • demon **pcnfsd** • demon **telnet** • usługa cmsd • usługa ttdbserver • usługa TCP echo • usługa TCP discard • usługa TCP chargen • usługa TCP daytime • usługa TCP time • usługa UDP echo • usługa UDP discard • usługa UDP chargen • usługa UDP daytime • usługa UDP time	/etc/security/pscexpert/bin/cominetdconf
CIP-005-3a R2.5 CIP-007-5 R1.1	Wymusza ochronę przed żądaniami odmowy usługi dla portów.	/etc/security/pscexpert/bin/tcptr_aixpert
CIP-005-3a R3 CIP-007-3a R5, R6.5 CIP-007-5 R4.4	Włącza kontrolę plików binarnych w systemie.	/etc/security/pscexpert/bin/pciaudit
CIP-007-3a R3 CIP-007-5 R2.1	Wyświetla komunikat o włączeniu TNC (Trusted Network Connect).	/etc/security/pscexpert/bin/GeneralMsg

Tabela 9. Standardy CIP dla produktu PowerSC Standard Edition (kontynuacja)

Standard CIP	Implementacja narzędzia AIX Security Expert	Skrypt, który modyfikuje wartość
CIP-007-3a R4 CIP-007-5 R3.3	Utrzymuje integralność systemu, wykrywając, usuwając i chroniąc przed znanymi typami złośliwego oprogramowania.	/etc/security/pscexpert/bin/manageITsecurity
CIP-007-3a R5.2.1	Włącza zmianę hasła po pierwszym logowaniu dla wszystkich domyślnych użytkowników, którzy nie są zablokowani.	/etc/security/pscexpert/bin/pwdchg
CIP-007-3a R5.2.2-R5.2.3	Blokuje wszystkie domyślne konta użytkowników.	/etc/security/pscexpert/dodv2/lockacc_rlogin
CIP-007-3a R5.3.1	Ustawia minimalną długość hasła na 6 znaków.	/etc/security/pscexpert/bin/chusrattr
CIP-007-5 R5.5.1	Ustawia minimalną długość hasła na 8 znaków.	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R5.3.2 CIP-007-5 R5.5.2	Ustawia wymaganie, aby hasło zawierało cyfry, litery i znaki specjalne.	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R5.3.3 CIP-007-5 R5.6	Wymusza zmianę hasła raz w roku.	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R7	Wyświetla komunikat o włączeniu systemu plików EFS (Encrypted File System).	/etc/security/pscexpert/bin/GeneralMsg
CIP-007-5 R5.7	Ogranicza liczbę nieudanych prób uwierzytelniania.	/etc/security/pscexpert/bin/chusrattr
CIP-010-1 CIP-010-2 R2.1	Wyświetla komunikat o włączeniu RTC (Real Time Compliance).	/etc/security/pscexpert/bin/GeneralMsg

Informacje pokrewne:

Zgodność z normami NERC (North American Electric Reliability Corporation)

Zarządzanie automatyzacją zabezpieczeń i zapewniania zgodności

W tej sekcji zawarto informacje na temat procesu planowania i wdrażania zabezpieczeń PowerSC oraz profili automatyzacji zapewniania zgodności dla grup systemów, zgodnie z dopuszczalnymi procedurami nadzoru informatycznego i zgodności.

W ramach zapewniania zgodności i prowadzenia nadzoru informatycznego, systemy z podobnym obciążeniem i klasami zabezpieczeń danych muszą być zarządzane i konfigurowane w spójny sposób. Aby zaplanować i wdrożyć zapewnianie zgodności w systemie, wykonaj następujące czynności:

Identyfikowanie grup pracy systemu

Wytyczne zapewniania zgodności i prowadzenia nadzoru informatycznego wskazują, że systemy z podobnym obciążeniem i klasami zabezpieczeń danych muszą być zarządzane i konfigurowane w spójny sposób. Dlatego należy zidentyfikować wszystkie systemy działające z podobnym obciążeniem.

Używanie testowego systemu nieprodukcyjnego w początkowej konfiguracji

Zastosuj odpowiedni profil zgodności produktu PowerSC w systemie testowym.

Rozważ następujące przykłady stosowania profili zgodności w systemie operacyjnym AIX.

Przykład 1: stosowanie profilu DoD.xml

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

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

W tym przykładzie nie ma reguł, które się nie powiodły (Failedrules=0). Oznacza to, że wszystkie reguły zostały pomyślnie zastosowane i można rozpocząć fazę testowania. Jeśli wystąpiłyby błędy, zostałyby wygenerowane szczegółowe informacje na ich temat.

Przykład 2: stosowanie profilu PCI.xml

```
# 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

Niepowodzenie reguły pci_grpck musi zostać zbadane. Możliwe przyczyny niepowodzenia są między innymi następujące:

- Reguła nie ma zastosowania w danym środowisku i musi zostać usunięta.
- Występuje problem z systemem, który należy naprawić.

Badanie nieudanej reguły

W większości przypadków podczas stosowania profilu zabezpieczeń i zgodności PowerSC nie występują błędy. W systemie może jednak brakować niektórych wymagań wstępnych, mogą też wystąpić inne problemy wymagające reakcji ze strony administratora.

Przyczynę błędu można sprawdzić tak jak na następującym przykładzie:

Wyświetl plik /etc/security/aixpert/custom/PCI.xml i odszukaj regułę generującą błąd. W tym przykładzie jest to reguła pci_grpck. Uruchom komendę **fgrep**, odszukaj regułę pci_grpck i sprawdź powiązany plik XML.

```
fgrep -p pci_grpck /etc/security/aixpert/custom/PCI.xml
<AIXPertEntry name="pci_grpck" function="grpck"
<AIXPertRuleType type="DLS"/
<AIXPertDescription&gt;Implements portions of PCI Section 8.2,
Check group definitions: Verifies the correctness of group definitions
and fixes the errors
</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
```

W regule pci_grpck można zauważyć komendę /usr/sbin/grpck.

Aktualizowanie nieudanej reguły

Podczas stosowania profilu zabezpieczeń i zgodności PowerSC mogą zostać wykryte błędy.

W systemie może brakować niektórych wymagań wstępnych, mogą też wystąpić inne problemy wymagające reakcji ze strony administratora. Po określeniu bazowej komendy reguły, która się nie powiodła, sprawdź system, aby określić komendę konfiguracji, która spowodowała błąd. W systemie mogą występować problemy z bezpieczeństwem. Możliwe jest także, że określona reguła nie ma zastosowania w środowisku tego systemu. W takim przypadku należy utworzyć niestandardową regułę zabezpieczeń.

Tworzenie niestandardowego profilu konfiguracji zabezpieczeń

Jeśli reguła nie dotyczy danego środowiska systemu, większość organizacji dopuszcza udokumentowane wyjątki.

Aby usunąć regułę i utworzyć niestandardową strategię zabezpieczeń wraz z plikiem konfiguracyjnym, wykonaj następujące kroki:

1. Skopiuj zawartość następujących plików do jednego pliku /etc/security/aixpert/custom/ *<moja_strategia_zabezpieczeń>*.xml:

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

2. Zmodyfikuj plik *<moja_strategia_zabezpieczeń>*.xml, usuwając z niego regułę, która nie jest odpowiednia. Regułę należy usunąć od otwierającego znacznika XML <AIXPertEntry nazwa... aż do zamykającego znacznika </AIXPertEntry.

Można wstawić dodatkowe reguły. Dodatkowe reguły należy wstawić do schematu XML AIXPertSecurityHardening. Profili produktu PowerSC nie można zmieniać bezpośrednio, można jednak konfigurować profile.

Dla większości środowisk należy utworzyć niestandardową strategię XML. Aby rozdystrybuować profil klienta na inne systemy, należy w bezpieczny sposób skopiować zmodyfikowaną strategię w pliku XML na system wymagający takiej samej konfiguracji. Do przesyłania plików w bezpieczny sposób należy użyć bezpiecznego protokołu, na przykład SFTP. Profil należy zapisać w bezpiecznej lokalizacji /etc/security/aixpert/custom/ *<moja_strategia_zabezpieczeń.xml>*.

Zaloguj się do systemu, w którym niestandardowy profil musi zostać utworzony, następnie uruchom następującą komendę:

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

Testowanie aplikacji za pomocą programu AIX Profile Manager

Konfiguracje zabezpieczeń mogą wpływać na aplikacje i sposób dostępu do systemu zarządzanego oraz zarządzanie nim. Jest istotne, aby przetestować aplikacje i oczekiwane metody zarządzania przed wdrożeniem systemu w środowisku produkcyjnym.

Standardy zgodności z przepisami wymuszają konfigurację zabezpieczeń, które są bardziej rygorystyczne, niż początkowa konfiguracja domyślna systemu. Aby przetestować system, wykonaj następujące kroki:

1. Wybierz opcję **Wyświetl i zarządzaj profilami** w panelu po prawej stronie ekranu powitania programu AIX Profile Manager.
2. Wybierz profil używany jako szablon do wdrażania w monitorowanych systemach.
3. Kliknij opcję **Porównaj**.
4. Wybierz grupę systemów zarządzanych lub wybierz poszczególne systemy w grupie i kliknij przycisk **Dodaj**, aby dodać je do pola wybranych systemów.
5. Kliknij przycisk **OK**.

Zostanie uruchomiona operacja porównywania.

Monitorowanie systemów w celu zapewnienia ciągłej zgodności za pomocą programu AIX Profile Manager

Konfiguracje zabezpieczeń mogą wpływać na aplikacje i sposób dostępu do systemu zarządzanego oraz zarządzanie nim. Jest istotne, aby monitorować aplikacje i oczekiwane metody zarządzania podczas wdrażania systemu w środowisku produkcyjnym.

Aby użyć programu AIX Profile Manager do monitorowania systemu AIX, wykonaj następujące czynności:

1. Wybierz opcję **Wyświetl i zarządzaj profilami** w panelu po prawej stronie ekranu powitania programu AIX Profile Manager.
2. Wybierz profil używany jako szablon do wdrażania w monitorowanych systemach.

3. Kliknij opcję **Porównaj**.
4. Wybierz grupę systemów zarządzanych lub wybierz poszczególne systemy w grupie i dodaj je do pola wybranych systemów.
5. Kliknij przycisk **OK**.

Zostanie uruchomiona operacja porównywania.

Konfigurowanie automatyzacji zabezpieczeń i zapewniania zgodności produktu PowerSC

W tej sekcji opisano procedurę konfigurowania produktu PowerSC dla automatyzacji zabezpieczeń i zapewniania zgodności z wiersza komend i za pomocą programu AIX Profile Manager.

Konfigurowanie ustawień opcji zgodności produktu PowerSC

Sekcja zawiera podstawowe informacje o funkcji automatyzacji i zabezpieczeń produktu PowerSC, testowaniu konfiguracji nieprodukcyjnych systemów testowych i planowaniu oraz wdrażaniu ustawień. Po zastosowaniu konfiguracji zgodności ustawienia te zmieniają liczne ustawienia konfiguracyjne w systemie operacyjnym.

Uwaga: Niektóre standardy i profile zgodności wyłączają usługę Telnet, ponieważ używa ona haseł w postaci jawnego tekstu. Dlatego należy zainstalować, skonfigurować i uruchomić Open SSH. Można użyć dowolnego innego sposobu komunikacji z konfigurowanym systemem. Te standardy zgodności wymagają wyłączenia identyfikatora logowania root. Przed dalszym stosowaniem zmian konfiguracji należy skonfigurować co najmniej jednego użytkownika innego niż root. Ta konfiguracja nie wyłącza użytkownika root i można zalogować się jako użytkownik inny niż root, a następnie uruchomić komendę **su** w celu rozpoczęcia sesji jako root. Należy przetestować, czy można nawiązać połączenie SSH z systemem, zalogować się jako użytkownik inny niż root i uruchomić komendę w celu rozpoczęcia sesji jako root.

Aby uzyskać dostęp do profili konfiguracji DoD, PCI, SOX lub COBIT, użyj następującego katalogu:

- Profile te w systemie operacyjnym AIX znajdują się w katalogu /etc/security/aixpert/custom.
- Profile na serwerze serwer VIOS (VIOS) znajdują się w katalogu /etc/security/aixpert/core.

Konfigurowanie zgodności produktu PowerSC z wiersza komend

Implementowanie lub sprawdzanie profilu zgodności za pomocą komendy **pscxpert** w systemie AIX i komendy **viosecure** na serwerze serwer VIOS (VIOS).

Aby zastosować profile zgodności produktu PowerSC w systemie AIX, wpisz jedną z następujących komend, w zależności od poziomu zgodności zabezpieczeń, który chcesz zastosować.

Tabela 10. Komendy PowerSC dla systemu AIX

Komenda	Standard zgodności
% pscxpert -f /etc/security/aixpert/custom/DoD.xml	*Procedury STIG systemu UNIX Departamentu Obrony Stanów Zjednoczonych*
% pscxpert -f /etc/security/aixpert/custom/Hipaa.xml	*Ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych (Heath Insurance Portability and Accountability Act - HIPAA)*
% pscxpert -f /etc/security/aixpert/custom/PCI.xml	*Payment Card Industry Data Security Standard (PCI DSS)*
% pscxpert -f /etc/security/aixpert/custom/SOX-COBIT.xml	*Ustawa Sarbanes-Oxley Act z 2002 – COBIT IT Governance*

Aby zastosować profile zgodności produktu PowerSC w systemie VIOS, wpisz jedną z następujących komend, w zależności od poziomu zgodności zabezpieczeń, który chcesz zastosować.

Tabela 11. Komendy PowerSC dla systemu serwer VIOS

Komenda	Standard zgodności
% viosecure -file /etc/security/aixpert/custom/DoD.xml	*Procedury STIG systemu UNIX Departamentu Obrony Stanów Zjednoczonych*
% viosecure -file /etc/security/aixpert/custom/Hipaa.xml	*Ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych (Heath Insurance Portability and Accountability Act - HIPAA)*
% viosecure -file /etc/security/aixpert/custom/PCI.xml	*Payment Card Industry Data Security Standard (PCI DSS)*
% viosecure -file /etc/security/aixpert/custom/SOX-COBIT.xml	*Ustawa Sarbanes-Oxley Act z 2002 – COBIT IT Governance*

Działanie komendy **pscxpert** w systemie AIX i komendy **viosecure** na serwerze VIOS może chwilę potrwać, ponieważ sprawdzają one lub ustawiają cały system i wprowadzają zmiany konfiguracji związane z bezpieczeństwem. Dane wyjściowe powinny być podobne do tych, które przedstawiono poniżej:

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

Jednak niektóre reguły mogą zakończyć się niepowodzeniem w zależności od środowiska AIX, zestawu instalacyjnego i wcześniejszej konfiguracji.

Na przykład reguła wymagań wstępnych może się nie powieść, ponieważ system nie ma wymaganego zestawu plików instalacji. Konieczne jest zrozumienie każdego błędu i rozwiązanie go przed wdrożeniem profili zgodności w centrum przetwarzania danych.

Pojęcia pokrewne:

“Zarządzanie automatyzacją zabezpieczeń i zapewniania zgodności” na stronie 91
W tej sekcji zawarto informacje na temat procesu planowania i wdrażania zabezpieczeń PowerSC oraz profili automatyzacji zapewniania zgodności dla grup systemów, zgodnie z dopuszczalnymi procedurami nadzoru informatycznego i zgodności.

Konfigurowanie zgodności produktu PowerSC za pomocą programu AIX Profile Manager

W tej sekcji opisano procedurę konfigurowania profili zabezpieczeń i zgodności produktu PowerSC oraz wdrażania konfiguracji w systemie zarządzanym przez system AIX za pomocą programu AIX Profile Manager.

Aby skonfigurować profile zabezpieczeń i zgodności produktu PowerSC za pomocą programu AIX Profile Manager, wykonaj następujące kroki:

1. Zaloguj się do programu IBM Systems Director i wybierz program AIX Profile Manager.
2. Utwórz szablon, który jest oparty na jednym z profili zabezpieczeń i zgodności produktu PowerSC, wykonując następujące kroki:
   a. Kliknij opcję **Wyświetlanie szablonów i zarządzanie nimi** na prawym panelu strony powitania programu AIX Profile Manager.
   b. Kliknij przycisk **Utwórz**.
   c. Kliknij pozycję **System operacyjny** na liście **Typ szablonu**.
   d. Podaj nazwę szablonu w polu **Nazwa szablonu konfiguracyjnego**.
   e. Kliknij opcję **Kontynuuj > Zapisz**.
3. Wybierz profil do użycia z szablonem, wybierając opcję **Przeglądaj** w opcji **Wybierz profil, który ma zostać użyty dla tego szablonu**. Profile zawierają następujące elementy:
   - ice_DLS.xml jest domyślnym poziomem bezpieczeństwa systemu operacyjnego AIX.
   - ice_DoD.xml to procedury STIG (Security Technical Implementation Guide) Departamentu Obrony dla ustawień UNIX.
   - ice_HLS.xml to ogólne zabezpieczenia na wysokim poziomie dla ustawień AIX.
   - ice_LLS.xml to zabezpieczenia na niskim poziomie dla ustawień AIX.

- ice_MLS.xml to zabezpieczenia na średnim poziomie dla ustawień AIX.
- ice_PCI.xml to ustawienia standardu PCI (Payment Card Industry) dla systemu operacyjnego AIX.
- ice_SOX.xml to ustawienia SOX lub COBIT dla systemu operacyjnego AIX.

4. Usuń profil z wybranego pola.
5. Wybierz opcję **Dodaj**, aby przenieść wymagany profil do wybranego pola.
6. Kliknij przycisk **Zapisz**.

Aby wdrożyć konfigurację w systemie zarządzanym AIX, wykonaj następujące kroki:

1. Wybierz opcję **Wyświetlanie szablonów i zarządzanie nimi** na prawym panelu strony powitania programu AIX Profile Manager.
2. Wybierz wymagany szablon w celu wdrożenia.
3. Kliknij opcję **Wdróż**.
4. Wybierz systemy do wdrożenia profilu i kliknij przycisk **Dodaj**, aby przenieść wymagany profil do wybranego pola.
5. Kliknij przycisk **OK**, aby wdrożyć szablon konfiguracji. System został skonfigurowany zgodnie z wybranym szablonem profilu.

W celu zapewnienia pomyślnego wdrożenia dla standardu DoD, PCI lub SOX, program PowerSC Standard Edition musi być zainstalowany w punkcie końcowym systemu AIX. Jeśli system, który jest wdrażany, nie ma zainstalowanego programu PowerSC, instalacja nie powiedzie się. Program IBM Systems Director wdraża szablon konfiguracji w wybranych punktach końcowych systemu AIX i konfiguruje je zgodnie z wymaganiami zgodności.

Informacje pokrewne:

AIX Profile Manager

IBM Systems Director

PowerSC Real Time Compliance

Funkcja PowerSC Real Time Compliance w sposób ciągły monitoruje włączone systemy AIX, aby zapewnić, że są one skonfigurowane w sposób spójny i bezpieczny.

Funkcja PowerSC Real Time Compliance działa z funkcją automatyzacji zgodności należącą do produktu PowerSC i strategiami programu narzędziowego AIX Security Expert do wysyłania powiadomień, gdy wystąpią naruszenia zgodności lub zostanie zmieniony monitorowany plik. Gdy zostanie naruszona strategia konfiguracji zabezpieczeń, funkcja PowerSC Real Time Compliance wysyła wiadomość e-mail lub wiadomość tekstową, aby poinformować administratora systemu.

Funkcja PowerSC Real Time Compliance to pasywna opcja zabezpieczająca, która obsługuje predefiniowane lub zmienione profile zgodności, w tym: Department of Defense Security Technical Implementation Guide, Payment Card Industry Data Security Standard, Sarbanes-Oxley Act i COBIT. Udostępnia ona domyślną listę plików, dla których mają być monitorowane zmiany, ale do tej listy można dodawać pliki.

Instalowanie funkcji PowerSC Real Time Compliance

Funkcja PowerSC Real Time Compliance jest instalowana z produktem PowerSC Standard Edition w wersji 1.1.4 lub nowszej i nie jest częścią Podstawowego systemu operacyjnego AIX.

Aby zainstalować produkt PowerSC Standard Edition, wykonaj następujące kroki:

1. Upewnij się, że w systemie, w którym instalowana jest funkcja PowerSC Standard Edition, używany jest jeden z następujących systemów operacyjnych AIX:
   - System IBM AIX 6 z pakietem Technology Level 7 lub nowszy z pakietami AIX Event Infrastructure for AIX i AIX Clusters (bos.ahafs 6.1.7.0) lub nowszymi.
   - System IBM AIX 7 z pakietem Technology Level 1 lub nowszy z pakietami AIX Event Infrastructure for AIX i AIX Clusters (bos.ahafs 7.1.1.0) lub nowszymi.
   - System AIX wersja 7.2 lub nowszy z pakietami AIX Event Infrastructure for AIX i AIX Clusters (bos.ahafs 7.2.0.0) lub nowszymi.
2. Aby zaktualizować lub zainstalować zestaw plików funkcji PowerSC Standard Edition, należy zainstalować zestaw plików powerscStd.rtc z pakietu instalacyjnego dla funkcji PowerSC Standard Edition w wersji 1.1.4 nowszej.

Konfigurowanie funkcji PowerSC Real Time Compliance

Funkcję PowerSC Real Time Compliance można skonfigurować pod kątem wysyłania alertów, gdy wystąpi naruszenie profilu zgodności lub zostaną wprowadzone zmiany w monitorowanym pliku. Przykładowe profile: Department of Defense Security Technical Implementation Guide, Payment Card Industry Data Security Standard, Sarbanes-Oxley Act i COBIT.

Funkcję PowerSC Real Time Compliance można skonfigurować, korzystając z jednej z następujących metod:

- Wprowadź komendę **mkrtc**.
- Uruchom narzędzie SMIT, wprowadzając następującą komendę:

  ```
  smit RTC
  ```

Określanie plików monitorowanych przez funkcję PowerSC Real Time Compliance

Funkcja PowerSC Real Time Compliance monitoruje domyślną listę plików zawierających ustawienia zabezpieczeń wysokiego poziomu pod kątem zmian. Lista ta może być dostosowywana przez dodawanie i usuwanie plików w pliku /etc/security/rtc/rtcd_policy.conf.

Istnieją dwie metody określania szablonu zgodności, który został zastosowany w systemie. Jedną z metod jest użycie komendy **pscxpert**. Drugą metodą jest użycie programu AIX Profile Manager z programem IBM Systems Director.

Gdy profil zgodności zostanie określony, można dodawać kolejne pliki do listy plików, które mają być monitorowane, umieszczając dodatkowe pliki w pliku /etc/security/rtc/rtcd_policy.conf. Gdy ten plik zostanie zapisany, nowa lista zostanie natychmiast użyta jako podstawowa i będzie ona monitorowana pod kątem zmian bez restartowania systemu.

Ustawianie alertów dla produktu PowerSC Real Time Compliance

Użytkownik musi skonfigurować powiadamianie w funkcji PowerSC Real Time Compliance, wskazując typ alertów i odbiorców alertów.

Demon rtcd, który jest głównym komponentem funkcji PowerSC Real Time Compliance, otrzymuje informacje o typach alertów i odbiorcach z pliku konfiguracyjnego /etc/security/rtc/rtcd.conf. Plik ten można zmodyfikować w edytorze tekstu, aby go zaktualizować.

Informacje pokrewne:

Format pliku /etc/security/rtc/rtcd.conf dla RTC

Zaufany start

Opcja Zaufany start modułu VTPM (Virtual Trusted Platform Module), który jest wirtualną instancją modułu TPM opracowanego przez organizację Trusted Computing Group. Moduł VTPM służy do bezpiecznego przechowywania parametrów startu systemu na potrzeby ich weryfikacji w przyszłości.

Pojęcia dotyczące zaufanego startu

Ważne jest, aby zrozumieć pojęcia związane z integralnością procesu uruchamiania systemu operacyjnego i sposobu jego klasyfikowania jako zaufanego startu lub niezaufanego startu.

Można skonfigurować maksymalnie partycji logicznych (LPAR) z obsługą VTPM dla każdego systemu fizycznego za pomocą konsoli konsola HMC (HMC). Po zakończeniu konfiguracji każdy moduł VTPM jest unikalny dla każdej partycji LPAR. W przypadku użycia z technologią AIX Trusted Execution moduł VTPM zapewnia bezpieczeństwo i kontrolę dla następujących partycji:

- Kodu startowego na dysku.
- Całego systemu operacyjnego.
- Warstwy aplikacji.

Administrator może wyświetlać zaufane i niezaufane systemy używając centralnej konsoli, na której jest zainstalowany program weryfikatora **openpts**, dostępny w pakiecie rozszerzeń systemu AIX. Konsoli **openpts** zarządza jednym lub wieloma serwerami Power Systems i monitoruje lub atestuje wiarygodność systemów AIX Profile Manager zainstalowanych w centrum przetwarzania danych. Atestacja to proces, w którym weryfikator określa (lub atestuje), czy kolektor wykonał operację zaufanego startu.

Status zaufanego startu

Partycja określana jako zaufany, jeśli weryfikator pomyślnie zweryfikuje integralność kolektora. Weryfikator jest partycją zdalną, która określa, czy kolektor wykonał operację zaufanego startu. Kolektor jest partycją systemu AIX, która ma podłączony moduł VTPM (Virtual Trusted Platform Module) i zaufany stos oprogramowania (TS). Sprawdza on czy pomiary zarejestrowane w obrębie modułu VTPM są zgodne z danymi odniesienia przechowywanymi w weryfikatorze. Stan zaufanego startu wskazuje, czy partycja została uruchomiona w zaufany sposób. Ta deklaracja dotyczy tylko integralności procesu uruchamiania systemu, a nie poziomu jego bieżących zabezpieczeń.

Status niezaufanego startu

Partycja przechodzi do stanu niezaufanego, jeśli weryfikator nie może pomyślnie sprawdzić integralności procesu startu systemu. Stan niezaufany wskazuje, że niektóre aspekty procesu startu są niespójne z informacjami odniesienia posiadanymi przez weryfikatora. Możliwe przyczyny nieudanej atestacji obejmują wykonanie startu z innego urządzenia startowego, uruchomienie innego obrazu jądra i zmianę istniejącego kodu startowego.

Pojęcia pokrewne:

“Rozwiązywanie problemów z zaufanym startem” na stronie 103
W tej sekcji przedstawiono kilka typowych scenariuszy zaradczych, które są wymagane do zidentyfikowania przyczyny niepowodzenia atestacji przy użyciu zaufanego startu.

Planowanie zaufanego startu

Sekcja zawiera informacje na temat wymaganych konfiguracji sprzętu i oprogramowania, które są niezbędne do zainstalowania zaufanego startu.

Wymagania wstępne zaufanego startu

Instalacja zaufanego startu wymaga skonfigurowania modułu gromadzącego dane i weryfikatora.

Podczas przygotowywania do reinstalacji systemu operacyjnego AIX w systemie, w którym jest już zainstalowany zaufany start, należy skopiować plik /var/tss/lib/tpm/system.data i użyć go do zastąpienia pliku w tej samej lokalizacji po zakończeniu reinstalacji. Jeśli nie ten plik nie zostanie skopiowany, należy usunąć zwirtualizowanych moduł TPM (Trusted Platform Module) z konsoli zarządzania i ponownie zainstalować go w partycji.

Kolektor

Wymagania dotyczące konfiguracji do instalacji kolektora obejmują następujące wymagania wstępne:

- Sprzęt POWER7, który ma oprogramowanie wbudowane w wersji 740.
- Zainstaluj system IBM AIX 6 z pakietem Technology Level 7 lub IBM AIX 7 z pakietem Technology Level 1.
- Zainstaluj konsolę HMC (Hardware Management Console) w wersji 7.4 lub nowszej.
- Skonfiguruj dla partycji moduł VTPM i co najmniej 1 GB pamięci.
- Zainstaluj program Secure Shell (SSH), na przykład OpenSSH lub odpowiednik.

Weryfikator

Dostęp do weryfikatora **openpts** można uzyskać z poziomu interfejsu wiersza komend i graficznego interfejsu użytkownika, który jest przeznaczony do uruchamiania na wielu platformach. Wersja weryfikatora OpenPTS dla systemu AIX jest dostępna w pakiecie rozszerzeń dla AIX. Wersje OpenPTS weryfikator dla systemu Linux i innych platform są dostępne do pobrania z sieci WWW. Wymagania konfiguracyjne obejmują następujące wymagania wstępne:

- Zainstaluj program SSH, na przykład OpenSSH lub odpowiednik.
- Nawiąż połączenie sieciowe SSH do kolektora.
- Zainstaluj środowisko Java™ w wersji 1.6 lub nowszej, aby uzyskać dostęp do konsoli **openpts** z poziomu interfejsu graficznego.

Przygotowywanie do naprawy

Opisane w tej sekcji informacje na temat zaufanego startu mogą posłużyć służy jako przewodnik do identyfikowania sytuacji, które mogą wymagać naprawy. Nie wpływa to na proces startu.

Istnieje wiele sytuacji, które mogą spowodować niepowodzenie atestacji i trudno jest przewidzieć, w jakich okolicznościach może ono wystąpić. Należy zdecydować o wykonaniu odpowiednich działań w zależności od okoliczności. Jednak zalecane jest przygotowanie się na pewne często spotykane scenariusze i opracowanie strategii lub przepływu pracy, aby ułatwić obsługę takich incydentów. Naprawianie jest to działanie naprawcze, które należy wykonać gdy podczas atestacji jeden lub więcej kolektorów okaże się niezaufany.

Na przykład, jeśli wystąpił błąd atestacji, ponieważ kod startowy był niezgodny z danymi referencyjnymi weryfikatora, warto zastanowić się nad odpowiedziami na następujące pytania:

- W jaki sposób można sprawdzić, czy zagrożenie jest wiarygodne?
- Czy niedawno były wykonywane planowane prace konserwacyjne, aktualizacja systemu AIX, lub instalacja nowego sprzętu?
- Czy można skontaktować się z administratorem, który ma dostęp do tych informacji?
- Kiedy system był uruchamiany po raz ostatni raz w zaufanym stanie?
- Jeśli zagrożenie bezpieczeństwa jest wiarygodne, jakie czynności należy wykonać? (Sugestie mogą obejmować włączenie gromadzenia dzienników kontroli, odłączania systemu od sieci, wyłączenie zasilania systemu i powiadomienie użytkowników).
- Czy naruszono ochronę innych systemów, które należy sprawdzić?

Pojęcia pokrewne:

“Rozwiązywanie problemów z zaufanym startem” na stronie 103
W tej sekcji przedstawiono kilka typowych scenariuszy zaradczych, które są wymagane do zidentyfikowania przyczyny niepowodzenia atestacji przy użyciu zaufanego startu.

Uwagi dotyczące migracji

Poniżej przedstawiono kwestie, na które należy zwrócić uwagę przy migrowaniu partycji, która ma włączoną obsługę modułu VTPM (Virtual Trusted Platform Module).

Zaletą korzystania z modułu VTPM w porównaniu z fizycznym modułem TPM jest to, że umożliwia przenoszenie partycji między systemami, zachowując dane VTPM. Aby wykonać bezpieczną migrację partycji logicznej, oprogramowanie szyfruje dane VTPM przed ich przesłaniem. Przed wykonaniem migracji należy zaimplementować następujące środki zabezpieczające:

- Włączyć komunikację IPSEC między serwerami serwer VIOS (VIOS), które biorą udział w migracji.
- Skonfigurować zaufany klucz systemowy za pomocą konsoli HMC (Hardware Management Console) do sterowania systemami zarządzanymi, którego można będzie użyć do deszyfrowania danych VTPM po zakończeniu migracji. Aby pomyślnie przeprowadzić migrację danych, system docelowy migracji musi mieć taki sam klucz, jak system źródłowy.

Informacje pokrewne:

Korzystanie z HMC

Migracja serwera VIOS

Instalowanie zaufanego startu

Istnieją wymagane konfiguracje sprzętu i oprogramowania, które są niezbędne do zainstalowania zaufanego startu.

Informacje pokrewne:

“instalowanie produktu PowerSC Standard Edition 1.1.3” na stronie 7
Należy zainstalować zestaw plików dla każdej z wybranych funkcji produktu PowerSC Standard Edition.

Instalowanie kolektora

Należy zainstalować kolektor za pomocą zestawu plików z dysku CD podstawowego systemu AIX.

Aby zainstalować kolektor, zainstaluj pakiety powerscStd.vtpm i openpts.collector, które są na podstawowym dysku CD przy użyciu komend **smit** lub **installp**.

Instalowanie weryfikatora

Komponent weryfikatora OpenPTS działa w systemie operacyjnym AIX i na innych platformach.

Wersję weryfikatora dla systemu AIX można zainstalować z zestawu plików przy użyciu pakietu rozszerzeń AIX. Aby zainstalować weryfikatora w systemie operacyjnym AIX, zainstaluj pakiet openpts.verifier z pakietu rozszerzeń AIX za pomocą komendy **smit** lub **installp**. Spowoduje to zainstalowanie zarówno weryfikatora w wersji dla wiersza komend, jak i dla interfejsu graficznego.

Weryfikatora OpenPTS w wersji dla innych systemów operacyjnych można pobrać z katalogu ###Download Linux OpenPTS Verifier For Use With AIX Trusted Boot.

Informacje pokrewne:

Pobierz weryfikator OpenPTS dla Linux do używania z zaufanym startem systemu AIX

Konfigurowanie zaufanego startu

W sekcji opisano procedurę rejestrowania systemu i jego atestacji do wykonywania zaufanego startu.

Rejestrowanie systemu

W sekcji opisano procedurę rejestrowania systemu w weryfikatorze.

Rejestrowanie systemu to proces udostępniania początkowego zestawu pomiarów dla weryfikatora, które tworzą podstawę dla następnych żądań atestacji. Aby zarejestrować system z wiersza komend, użyj następującej komendy z poziomu weryfikatora:

```
openpts -i <nazwa_hosta>
```

Informacje na temat zarejestrowanych partycji znajdują się w katalogu $HOME/.openpts. Każda nowa partycja podczas procesu rejestrowania ma przypisywany unikalny identyfikator, a informacje dotyczące zarejestrowanych partycji są zapisywane w katalogu odpowiadającym unikalnemu identyfikatorowi.

Aby wykonać rejestrowanie systemu przy użyciu interfejsu graficznego, wykonaj następujące kroki:

1. Uruchom interfejs graficzny za pomocą komendy **/opt/ibm/openpts_gui/openpts_gui.sh**.
2. Wybierz opcję **Rejestrowanie** z menu nawigacyjnego.
3. Wprowadź nazwę hosta i informacje autoryzacyjne SSH dla systemu.
4. Kliknij przycisk **Zarejestruj**.

Pojęcia pokrewne:

"Atestowanie systemu"
W niniejszej sekcji opisano procedurę atestacji systemu z poziomu wiersza komend i za pomocą interfejsu graficznego.

Atestowanie systemu

W niniejszej sekcji opisano procedurę atestacji systemu z poziomu wiersza komend i za pomocą interfejsu graficznego.

Aby wykonać zapytanie o integralność startu systemu, użyj następującej komendy z poziomu weryfikatora:

```
openpts <nazwa_hosta>
```

Aby wykonać atestację systemu przy użyciu interfejsu graficznego, wykonaj następujące kroki:

1. Wybierz kategorię z menu nawigacyjnego.
2. Wybierz jeden lub więcej systemów do atestowania.
3. Kliknij przycisk **Atestuj**.

Rejestrowanie się i atestowanie systemu bez hasła

Żądanie atestacji jest wysyłane za pomocą SSH (Secure Shell). Zainstaluj certyfikat weryfikatora w kolektorze, aby umożliwić nawiązanie połączenia SSH bez podawania hasła.

Aby skonfigurować certyfikat weryfikatora w systemie kolektora, wykonaj następujące kroki:

- W weryfikatorze uruchom następujące komendy:

  ```
  ssh-keygen    # Brak frazy hasła
  scp ~/.ssh/id_rsa.pub <kolektor>:/tmp
  ```

- Na kolektorze uruchom następujące komendy:

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

Zarządzanie zaufanym startem

W sekcji opisano procedurę zarządzania wynikami atestacji zaufanego startu.

Interpretowanie wyników atestacji

W tej sekcji opisano procedurę wyświetlania i sprawdzania wyników atestacji.

Wyniki atestacji mogą przyjmować jeden z następujących stanów:

1. Żądanie atestacji nie powiodło się: żądanie atestacji nie zakończyła się pomyślnie. Sekcja Rozwiązywanie problemów zawiera więcej informacji na temat możliwych przyczyn niepowodzenia.
2. Integralność systemu poprawna: atestacja zakończyła się pomyślnie, a start systemu jest zgodny z informacjami uzupełniającymi, które posiada weryfikator. Ten komunikat wskazuje na włączenie zaufanego startu.
3. Integralność systemu niepoprawna: żądanie atestacji zostało zakończone, ale wykryto rozbieżność między informacjami, które są zbierane podczas startu systemu i informacjami uzupełniającymi, które posiada weryfikator. Oznacza to, że start jest niezaufany.

Atestacja zgłasza również, czy do kolektora została zastosowana aktualizacja za pomocą następującego komunikatu:

Dostępna jest aktualizacja systemu: ten komunikat wskazuje, że w kolektorze została zastosowana aktualizacja i jest dostępny zestaw zaktualizowanych informacji odniesienia, który będzie obowiązywać od następnego startu. Użytkownik jest proszony o zaakceptowanie lub odrzucenie aktualizacji. Na przykład, użytkownik może wybrać zaakceptowanie tych aktualizacji, jeśli ma informacje o trwającym serwisowaniu kolektora.

Aby zbadać problemy z atestacją za pomocą interfejsu graficznego, wykonaj następujące kroki:

1. Wybierz kategorię z menu nawigacyjnego.
2. Wybierz system do zbadania.
3. Kliknij dwukrotnie odpowiednią pozycję dla systemu. Zostanie wyświetlone okno właściwości. To okno zawiera informacje dziennika na temat atestacji, która nie powiodła się.

Usuwanie systemów

W sekcji opisano procedurę usuwanie systemu z weryfikatora bazy danych.

Aby usunąć system z bazy danych weryfikatora, uruchom następującą komendę:

```
openpts -r <nazwa_hosta>
```

Rozwiązywanie problemów z zaufanym startem

W tej sekcji przedstawiono kilka typowych scenariuszy zaradczych, które są wymagane do zidentyfikowania przyczyny niepowodzenia atestacji przy użyciu zaufanego startu.

Komenda **openpts** określa system jako niepoprawny, jeśli bieżący stan uruchomienia systemu nie jest zgodny z informacjami odniesienia, które są przechowywane w systemie weryfikatora. Komenda **openpts** określa prawdopodobne przyczyny braku integralności. Pełny start systemu AIX zawiera wiele zmiennych, a niepowodzenie atestacji wymaga wykonania analizy w celu określenia przyczyny niepowodzenia.

Poniższa tabela zawiera listę typowych scenariuszy zaradczych, które są wymagane do zidentyfikowania przyczyny niepowodzenia:

Tabela 12. Typowe scenariusze rozwiązania problemów w przypadku niepowodzenia

Przyczyna niepowodzenia	Możliwe przyczyny	Sugerowane działania naprawcze

Atestacja nie została zakończona.	• Niepoprawna nazwa hosta.
	• Brak trasy sieciowej między źródłem i miejscem docelowym.
	• Niepoprawne informacje autoryzacyjne.
		Sprawdź działanie połączenia SSH (Secure Shell) za pomocą następującej komendy:
		`ssh ptsc@hostname`
		
		Jeśli połączenie SSH zostanie nawiązane pomyślne, sprawdź poniższe przyczyny niepowodzenia atestacji:
		• W atestowanym systemie nie jest uruchomiony demon **tcsd**.
		• Atestowany system nie został zainicjowany przy użyciu komendy **ptsc**. Ten proces powinien zostać wykonany automatycznie podczas uruchamiania systemu, ale sprawdź obecność katalogu /var/ptsc/ na kolektorze. Jeśli katalog /var/ptsc/ nie istnieje, uruchom następującą komendę na kolektorze:
		`ptsc -i`

Oprogramowanie wbudowane CEC zostało zmodyfikowane.	• Wykonano aktualizację oprogramowania wbudowanego. • Partycja LPAR została zmigrowana do systemu, który ma inną wersję oprogramowania wbudowanego.	Sprawdź wersję oprogramowania wbudowanego systemu, na którym znajduje się partycja LPAR.
Zasoby przydzielone do partycji LPAR zostały zmienione.	Procesor lub pamięć przydzielona do partycji LPAR została zmieniona.	Sprawdź profil partycji w konsoli HMC.
Zmodyfikowano oprogramowanie wbudowane dla adapterów, które są dostępne w partycji LPAR.	Dodano lub usunięto urządzenie sprzętowe z partycji LPAR.	Sprawdź profil partycji w konsoli HMC.
Lista urządzeń przyłączonych do partycji LPAR została zmieniona.	Dodano lub usunięto urządzenie sprzętowe z partycji LPAR.	Sprawdź profil partycji w konsoli HMC.
Kod startowy został zmieniony, co obejmuje jądro systemu operacyjnego.	• W systemie AIX została zastosowana aktualizacja, o której weryfikator nie ma informacji. • Uruchomiono komendę **bosboot**.	• Dowiedz się od administratora kolektora, czy przed ostatnią operacją restartu były wykonywane jakieś prace serwisowe. • Sprawdź w dziennikach kolektora informacje o pracach serwisowych.
Partycja LPAR została uruchomiona z innego urządzenia.	• Rejestracja została wykonana natychmiast po instalacji sieciowej. • System został uruchomiony z urządzenia serwisowego.	Urządzenie startowe i opcje można sprawdzić za pomocą komendy **bootinfo**. Jeśli rejestrowanie zostało wykonane natychmiast po instalacji NIM (Network Installation Management) i przed wykonaniem restartu, szczegóły rejestracji dotyczą instalacji sieciowej, a nie następnego dysku startowego. Tę rejestrację można naprawić przez usunięcie rejestracji i ponowną rejestrację partycji logicznej.
Wywołano usługę zarządzania systemem (SMS) z interaktywnego menu startowego.		Proces startowy musi działać nieprzerwanie bez interakcji użytkownika, aby system mógł zostać uznany za zaufany. Wejście do menu startowego SMS spowoduje, że start będzie niepoprawny.
Zmodyfikowano bazę danych zaufanego wykonywania (TE).	• Do bazy danych TE zostały dodane lub usunięte pliki binarne. • Zostały zaktualizowane pliki binarne w bazie danych.	Uruchom komendę **trustchk**, aby sprawdzić bazę danych.

Pojęcia pokrewne:

“Przygotowywanie do naprawy” na stronie 100

Opisane w tej sekcji informacje na temat zaufanego startu mogą posłużyć służy jako przewodnik do identyfikowania

sytuacji, które mogą wymagać naprawy. Nie wpływa to na proces startu.

“Pojęcia dotyczące zaufanego startu” na stronie 99
Ważne jest, aby zrozumieć pojęcia związane z integralnością procesu uruchamiania systemu operacyjnego i sposobu jego klasyfikowania jako zaufanego startu lub niezaufanego startu.

Informacje pokrewne:

Korzystanie z HMC

Zaufany firewall

Opcji zaufanego firewalla jest mechanizmem zabezpieczającym działającym w warstwie wirtualizacji, który podnosi wydajność i efektywność wykorzystania zasobów podczas komunikacji między różnymi strefami bezpieczeństwa w wirtualnych sieciach LAN (VLAN) działających na tym samym serwerze Power Systems. Zaufany firewall zmniejsza obciążenie sieci zewnętrznej dzięki przesunięciu obsługi filtrowania pakietów przy użyciu reguł firewalla do warstwy wirtualizacji. Funkcja filtrowania jest kontrolowana przez zestaw łatwych do zdefiniowania reguł sieciowych, które umożliwiają przekazywanie zaufanego ruchu sieciowego między strefami bezpieczeństwa sieci VLAN bez opuszczania środowiska wirtualnego. Zaufany firewall zabezpiecza i kieruje ruchem w sieci wewnętrznej między serwerami AIX, IBM i Linux.

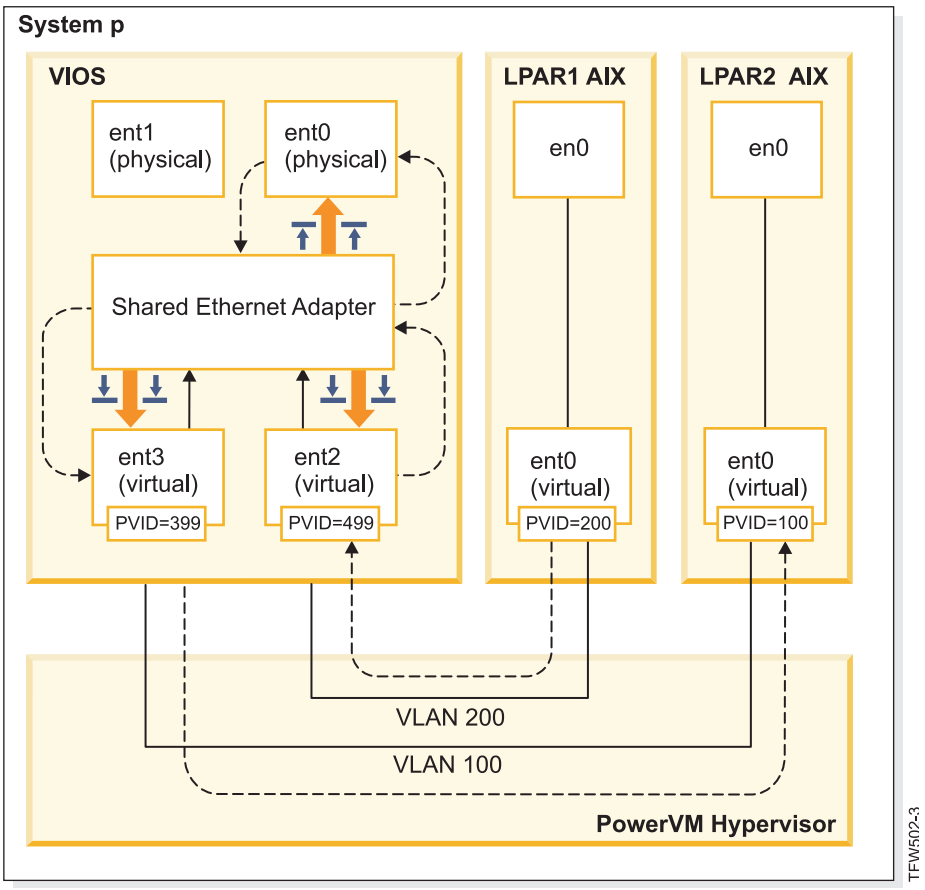
Pojęcia dotyczące zaufanego firewalla

Korzystanie z zaufanego firewalla wymaga zapoznania się z zestawem podstawowych pojęć.

Sprzęt Power Systems może być skonfigurowany do obsługi wielu stref bezpieczeństwa z wirtualnymi sieciami LAN (VLAN). Skonfigurowana przez użytkownika strategia, mająca postać reguły zaufanego firewalla, umożliwia zaufanym składnikom ruchu sieciowego na przechodzenie między strefami bezpieczeństwa sieci VLAN bez opuszczania warstwy wirtualizacji. Jest to podobne do wprowadzenia fizycznego sieciowego firewalla do środowiska wirtualnego, który udostępnia bardziej wydajną obsługę funkcji firewalla dla zwirtualizowanych centrów przetwarzania danych.

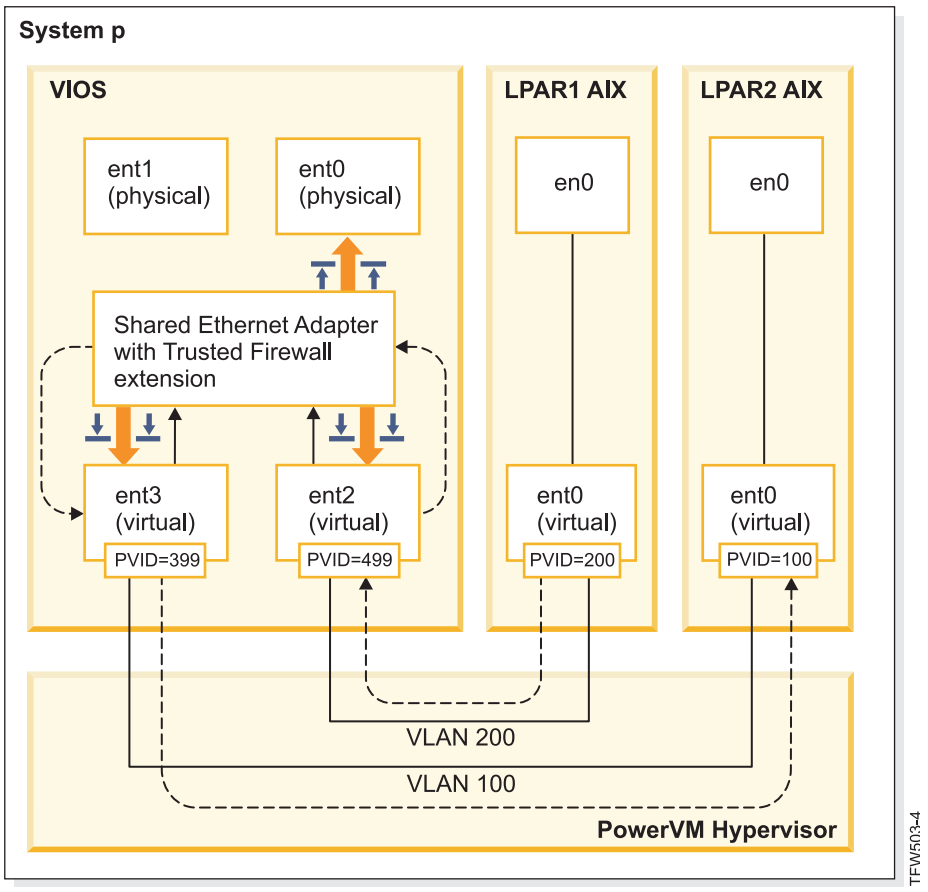
Zaufany firewall pozwala na skonfigurowanie reguł umożliwiających przesyłanie niektórych typów ruchu bezpośrednio z jednej sieci VLAN na serwerze serwer VIOS (VIOS) do innej sieci VLAN na tym samym serwerze VIOS, przy zachowaniu wysokiego poziomu bezpieczeństwa dzięki ograniczeniu innych typów ruchu. Jest to konfigurowalny firewall działający w obrębie warstwy wirtualizacji serwerów Power Systems.

Rys. 1 na stronie 108 przedstawia przykład, w którym celem jest możliwość bezpiecznego i wydajnego przesyłania informacji z VLAN 200 w partycji LPAR1 i z VLAN 100 w partycji z LPAR2. Bez zaufanego firewalla informacje przesyłane z partycji LPAR1 do LPAR2 byłyby wysyłane z sieci wewnętrznej do routera, który kierowałby je z powrotem do LPAR2.



Rysunek 1. Przykład przekazywania informacji między sieciami VLAN bez zaufanego firewalla

Przy użyciu zaufanego firewalla można skonfigurować reguły umożliwiające przekazanie informacji z LPAR1 do LPAR2 bez opuszczania przez nie sieci wewnętrznej. Ścieżkę tę przedstawia Rys. 2 na stronie 109.



Rysunek 2. Przykład przekazywania informacji między sieciami VLAN za pośrednictwem zaufanego firewalla

Reguły konfiguracji, które umożliwiają bezpieczne przesyłanie wybranych informacji pomiędzy sieciami VLAN, skracają ścieżkę od źródła do miejsca docelowego. Zaufany firewall do obsługi tej komunikacji używa rozszerzeń jądra SEA (Shared Ethernet Adapter - współużytkowany adapter Ethernet) i SVM (Security Virtual Machine - maszyna wirtualna zabezpieczeń).

Współużytkowany adapter Ethernet (SEA)
Adapter SEA jest miejscem, w którym rozpoczyna się i kończy routing. Po zarejestrowaniu maszyny SVM adapter SEA odbiera pakiety i przekazuje je do SVM. Jeśli SVM określi, że pakiet jest przeznaczony dla partycji LPAR na tym samym serwerze Power Systems, zaktualizuje nagłówek warstwy 2 pakietu. Pakiet jest zawracany do adaptera SEA w celu przekazania go do miejsca docelowego w systemie lub w sieci zewnętrznej.

Maszyna wirtualna zabezpieczeń (SVM)
Maszyna SVM jest miejscem, w którym są stosowane reguły filtrowania. Reguły filtrowania są niezbędne do zachowania bezpieczeństwa w sieci wewnętrznej. Po zarejestrowaniu maszyny SVM w adapterze SEA, pakiety są przekazywane do SVM przed przesłaniem ich do sieci zewnętrznej. Na podstawie aktywnych reguł filtrowania maszyna SVM określa, czy pakiet pozostanie w sieci wewnętrznej czy zostanie przeniesiony do sieci zewnętrznej.

Instalowanie zaufanego firewalla

Instalowanie mechanizmu zaufanego firewalla w systemie PowerSC jest podobne do instalowania innych funkcji w tym systemie.

Wymagania wstępne:

- Wersje PowerSC wcześniejsze niż 1.1.1.0 nie mają wymaganego zestawu plików do zainstalowania zaufanego firewalla. Upewnij się, że masz instalacyjny dysk CD systemu PowerSC w wersji 1.1.1.0 lub nowszej.
- Aby wykorzystać zaufanego firewalla, należy użyć konsoli HMC lub serwera serwer VIOS (VIOS) do skonfigurowania wirtualnej sieci LAN (VLAN).

Zaufany Firewall jest udostępniany jako dodatkowy zestaw plików na instalacyjnym dysku CD systemu PowerSC Standard Edition. Nazwa pliku to powerscStd.svm.rte. Można dodać zaufanego firewalla do istniejącej instancji produktu PowerSC w wersji 1.1.0.0 lub nowszej, albo zainstalować go w trakcie nowej instalacji tego systemu.

Aby dodać funkcję zaufanego firewalla do istniejącej instancji PowerSC:

1. Upewnij się, że uruchomiony jest serwer VIOS w wersji 2.2.1.4 lub nowszej.
2. Włóż dysk instalacyjny CD produktu PowerSC dla wersji 1.1.1.0 lub pobierz obraz z instalacyjnego dysku CD.
3. Użyj komendy **oem_setup_env**, aby uzyskać dostęp użytkownika root.
4. Użyj komendy **installp** lub narzędzia SMIT, aby zainstalować zestaw plików PowerscStd.svm.rte.

Informacje pokrewne:

“instalowanie produktu PowerSC Standard Edition 1.1.3” na stronie 7
Należy zainstalować zestaw plików dla każdej z wybranych funkcji produktu PowerSC Standard Edition.

Konfigurowanie zaufanego firewalla

Po zainstalowaniu opcji zaufanego firewalla wymaga ona wykonania dodatkowych prac konfiguracyjnych.

Trusted Firewall Advisor

Funkcja Trusted Firewall Advisor analizuje ruch generowany przez różne partycje logiczne (LPAR) i pozwala na określenie, czy uruchomiony zaufany firewall poprawia wydajność systemu.

Jeśli funkcja Trusted Firewall Advisor zarejestruje znaczną ilość ruchu z różnych sieci wirtualnych (VLAN), które są w tym samym zespole CEC, włączenie zaufanego firewalla powinno korzystnie wpłynąć na działanie systemu.

Aby włączyć funkcję Trusted Firewall Advisor, wpisz następującą komendę:

```
vlantfw -m
```

Aby wyświetlić wyniki działania funkcji Trusted Firewall Advisor, wpisz następującą komendę:

```
vlantfw -D
```

Aby wyłączyć funkcję Trusted Firewall Advisor, wpisz następującą komendę:

```
vlantfw -M
```

Rejestrowanie dla zaufanego firewalla

Rejestrowanie zaufanego firewalla kompiluje listę ścieżek ruchu sieciowego w obrębie zespołu CEC (Central Electronics Complex). Lista ta zawiera filtry, które są używane przez zaufany firewall do kierowania ruchem.

Jeśli doradca zaufanego firewalla (Trusted Firewall Advisor) określi, że ruch kierowanie ruchu wewnętrznie zwiększy efektywność, mechanizm rejestrowania zaufanego firewalla zapisze listę ścieżek w pliku svm.log. Wielkość pliku svm.log jest ograniczona do 16 MB. Jeśli pozycje przekraczają limit 16 MB, najstarsze wpisy zostaną usunięte z pliku dziennika.

Aby uruchomić rejestrowanie dla zaufanego firewalla, wpisz następującą komendę:

```
vlantfw -l
```

Aby zatrzymać rejestrowanie dla zaufanego firewalla, wpisz następującą komendę:

```
vlantfw -L
```

Plik dziennika jest dostępny dla wyświetlania w następującej lokalizacji: /home/padmin/svm/svm.log.

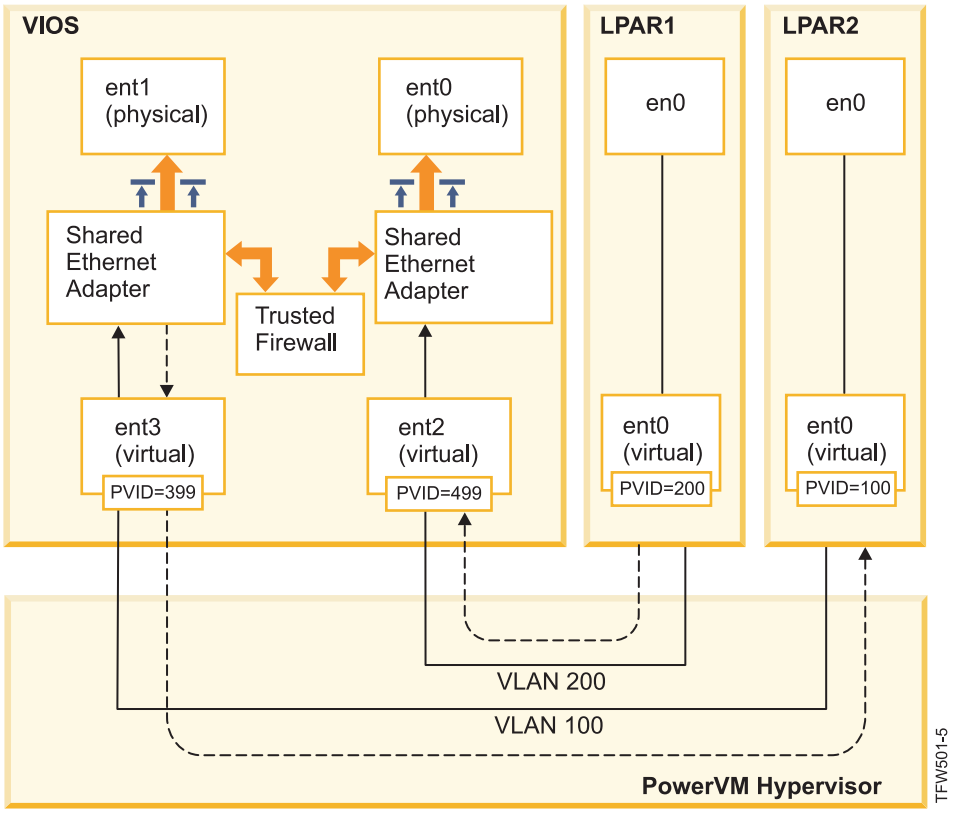
Uwaga: Użytkownik może uruchamiać komendy uruchamiania i zatrzymywania rejestrowania dla zaufanego firewalla tylko wtedy, gdy uwierzytelni się jako użytkownik root.

Wiele współużytkowanych adapterów Ethernet

Można skonfigurować zaufany firewall w systemach, które używają wielu współużytkowanych adapterów Ethernet.

Niektóre konfiguracje używają wielu współużytkowanych adapterów Ethernet (SEA) na tym samym serwerze serwer VIOS (VIOS). Dzięki użyciu wielu adapterów SEA można połączyć zalety przełączania awaryjnego i równoważenia obciążenia. Zaufany firewall obsługuje routing między wieloma adapterami SEA, jeśli są one zainstalowane na tym samym serwerze VIOS.

Rys. 3 przedstawia środowisko z wieloma adapterami SEA.



Rysunek 3. Konfiguracja z wieloma współużytkowanymi adapterami Ethernet na pojedynczym serwerze VIOS

Poniżej przedstawiono przykłady wielu konfiguracji adapterów SEA, które są obsługiwane przez zaufany firewall:

- Adaptery SEA są skonfigurowane przy użyciu adapterów typu trunk na tym samym wirtualnym przełączniku hiperwizora Power. Taka konfiguracja jest obsługiwana, ponieważ każdy adapter SEA odbiera ruch sieciowy z różnymi identyfikatorami sieci VLAN.
- Adaptery SEA są skonfigurowane przy użyciu adapterów typu trunk na różnych przełącznikach wirtualnych hiperwizora Power, a każdy adapter trunk ma skonfigurowany inny identyfikator sieci VLAN. W tej konfiguracji każdy adapter SEA nadal odbiera ruch sieciowy przy użyciu różnych identyfikatorów sieci VLAN.
- Adaptery SEA mają skonfigurowane adaptery typu trunk na różnych przełącznikach w wirtualnych przełącznikach hiperwizora Power, a w przełącznikach wirtualnych są wykorzystywane takie same identyfikatory sieci VLAN. W tym przypadku ruch sieciowy dla obu adapterów SEA ma takie same identyfikatory sieci VLAN.

Przykładem takiej konfiguracji jest posiadanie partycji LPAR2 w sieci VLAN200 z wirtualnym przełącznikiem 10 i partycji LPAR3 z siecią VLAN200 z wirtualnym przełącznikiem 20. Ponieważ obie partycje LPAR i odpowiadające im adaptery SEA używają tego samego identyfikatora sieci VLAN (VLAN200), oba adaptery SEA będą mieć dostęp do pakietów o tym identyfikatorze VLAN.

Nie można włączyć obsługi mostu na więcej niż jednym serwerze VIOS. Z tego powodu poniższe konfiguracje wiele adapterów SEA nie są obsługiwane przez zaufany firewall:

- Wiele serwerów VIOS i wiele sterowników SEA.
- Równoważenie obciążenia dla wielu adapterów SEA: adaptery typu trunk, które mają skonfigurowany routing między sieciami VLAN nie mogą zostać podzielone między serwery VIOS.

Usuwanie współużytkowanych adapterów Ethernet

Czynności wymagane do usunięcia z systemu urządzenia dla współużytkowanego adaptera Ethernet (SEA) należy wykonać w określonej kolejności.

Aby usunąć współużytkowany adapter Ethernet (SEA) z systemu, wykonaj następujące kroki:

1. Usuń maszynę wirtualną zabezpieczeń (SVM), która jest powiązana z SEA, wprowadzając następującą komendę:
   ```
   rmdev -dev svm
   ```
2. Usuń adapter SEA, wprowadzając następującą komendę:
   ```
   rmdev -dev ID współużytkowanego adaptera ethernet
   ```

Uwaga: Usuwanie adaptera SEA przed usunięciem SVM może spowodować awarię systemu.

Tworzenie reguł

Użytkownik może utworzyć reguły, aby włączyć komunikację między sieciami VLAN za pośrednictwem zaufanego firewalla.

Aby włączyć funkcję routingu dla zaufanego firewalla, użytkownik musi utworzyć reguły określające dozwoloną komunikację. Aby zwiększyć bezpieczeństwo, nie istnieje jedna reguła, która umożliwiałaby komunikację między wszystkich sieciami VLAN w systemie. Każde dozwolone połączenie wymaga utworzenia własnej reguły, a każda aktywowana reguła umożliwia komunikację w obu kierunkach między podanymi dla niej punktami końcowymi.

Ponieważ reguły są tworzone w interfejsie serwera serwer VIOS (VIOS), dodatkowe informacje na temat komend są dostępne w zestawie sekcji VIOS w Centrum informacyjnym dla sprzętu Power Systems.

Aby utworzyć regułę, wykonaj następujące działania:

1. Otwórz interfejs wiersza komend serwera VIOS.
2. Zainicjuj sterownik SVM wprowadzając następującą komendę:
   ```
   mksvm
   ```
3. Uruchom zaufany firewall, wprowadzając komendę:
   ```
   vlantfw -s
   ```
4. Aby wyświetlić wszystkie znane adresy IP i MAC partycji LPAR, wprowadź następującą komendę:
   ```
   vlantfw -d
   ```

   Potrzebne będą adresy IP i MAC partycji logicznych (LPAR), dla których tworzone są reguły.
5. Utwórz regułę filtru umożliwiającą komunikację między dwiema partycjami LPAR (LPAR1 i LPAR2) wprowadzając jedną z następujących komend (komendy należy wprowadzać w jednym wierszu):
   ```
   genvfilt -v4 -a P -z [vlanid_lpar1] -Z [vlanid_lpar2] -s [adres_ip_lpar1] -d [adres_ip_lpar2]
   genvfilt -v4 -a P -z [vlanid_lpar1] -Z [vlanid_lpar2] -s [adres_ip_lpar1] -d
        [adres_ip_lpar2] -o any -p 0 -O gt -P 23
   ```

Uwaga: Jedna reguła filtru umożliwia domyślnie komunikację w obu kierunkach, w zależności od portu i protokołu. Na przykład można włączyć komunikację Telnet z partycji LPAR1 do LPAR2 wpisując następującą komendę:

```
genvfilt -v4 -a-P -z [vlanid_lpar1] -Z [vlanid_lpar2] -s [adres_ip_lpar1] -d
    [adres_ip_lpar2] -o any -p 0 -O eq -P 23
```

6. Aktywuj wszystkie reguły filtrowania w jądrze wpisując następującą komendę:

   ```
   mkvfilt -u
   ```

Uwaga: Ta procedura aktywuje tę regułę i wszystkie inne reguły filtrowania, które istnieją w systemie.

Dodatkowe przykłady

Poniższe przykłady przedstawiają inne reguły filtrowania, które można utworzyć za pomocą zaufanego firewalla:

- Aby umożliwić komunikację SSH z partycji LPAR w sieci VLAN 100 do partycji LPAR w sieci VLAN 200, wprowadź następującą komendę:

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

- Aby zezwolić na cały ruch przy użyciu portów 0 - 499, wprowadź następującą komendę:

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

- Aby zezwolić na ruch TCP bez ograniczeń między partycjami LPAR, wprowadź następującą komendę:

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

  Jeśli nie podano żadnych portów, ruch sieciowy może używać wszystkich portów.

- Aby umożliwić przesyłanie pakietów ICMP (Internet Control Message Protocol) między partycjami LPAR, wprowadź następującą komendę:

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

Pojęcia pokrewne:

“Dezaktywowanie reguł”
Można dezaktywować reguły, które umożliwiają routing danych między sieciami VLAN w zaufanym firewallu.

Odsyłacze pokrewne:

“Komenda genvfilt” na stronie 156

“Komenda mkvfilt” na stronie 158

“Komenda vlantfw” na stronie 177

Informacje pokrewne:

VIOS (Virtual I/O Server)

Dezaktywowanie reguł

Można dezaktywować reguły, które umożliwiają routing danych między sieciami VLAN w zaufanym firewallu.

Ponieważ reguły są dezaktywowane w interfejsie serwera serwer VIOS (VIOS), dodatkowe informacje na temat komend i całego procesu są dostępne w zestawie sekcji VIOS w Centrum informacyjnym dla sprzętu Power Systems.

Aby dezaktywować regułę, wykonaj następujące działania:

1. Otwórz interfejs wiersza komend serwera VIOS.
2. Aby wyświetlić wszystkie aktywne reguły filtrowania, wprowadź następującą komendę:

   ```
   lsvfilt -a
   ```

   Możesz pominąć opcję **-a**, aby wyświetlić wszystkie reguły filtrowania przechowywane w menedżerze Object Data Manager.
3. Zanotuj numer identyfikacyjny dla reguły filtru, którą chcesz dezaktywować. W tym przykładzie numer identyfikacyjny reguły filtru jest równy 23.

4. Dezaktywuj regułę filtru nr 23, gdy jest ona aktywna w jądrze, wprowadzając następującą komendę:

```
rmvfilt -n 23
```

Aby dezaktywować wszystkie reguły filtrowania w jądrze, wpisz następującą komendę:

```
rmvfilt -n all
```

Pojęcia pokrewne:

“Tworzenie reguł” na stronie 112
Użytkownik może utworzyć reguły, aby włączyć komunikację między sieciami VLAN za pośrednictwem zaufanego firewalla.

Odsyłacze pokrewne:

“Komenda lsvfilt” na stronie 157

“Komenda rmvfilt” na stronie 177

Zaufane rejestrowanie

Funkcja zaufanego rejestrowania PowerVM pozwala partycjom logicznym systemu AIX na zapisywanie do plików dzienników umieszczonych na przyłączonych serwerach serwer VIOS (VIOS). Dane są transmitowane do serwera VIOS bezpośrednio przez hiperwizor bez konieczności nawiązania połączenia sieciowego między partycją LPAR klienta i serwerem VIOS.

Dzienniki wirtualne

Administrator serwera serwer VIOS (VIOS) tworzy i zarządza plikami dzienników. Są one widziane przez system operacyjny AIX jako wirtualne urządzenia rejestrujące w katalogu /dev, podobnie jak dyski wirtualne lub wirtualne nośniki optyczne.

Zapisywanie plików dzienników jako dzienników wirtualnych zwiększa poziom zaufania dla rekordów, ponieważ nie mogą one zostać zmienione przez użytkownika z uprawnieniami użytkownika root na kliencie LPAR, na którym zostały wygenerowane. Do tej samej partycji klienckiej LPAR można przyłączyć wiele wirtualnych urządzeń rejestrujących, a każde z nich będzie mieć własny plik w katalogu /dev.

Zaufane rejestrowanie umożliwia skonsolidowane danych rejestrowanych z wielu klienckich partycji LPAR w jednym systemie plików, który jest dostępny z poziomu serwera VIOS. Oznacza to, że serwer VIOS stanowi pojedyncze miejsce w systemie umożliwiające analizę i archiwizowanie dzienników. Administrator klienckiej partycji LPAR może skonfigurować aplikacje i system operacyjny AIX do zapisywania danych do wirtualnych urządzeń rejestrujących w sposób podobny do rejestrowania danych przy użyciu lokalnych plików. Podsystem kontroli systemu AIX można skonfigurować do kierowania rekordów kontroli do wirtualnych dzienników, a dla innych usługi AIX, takich jak syslog, można zmodyfikować istniejącą konfigurację w celu kierowania danych do dzienników wirtualnych.

Aby skonfigurować dziennik wirtualny, administrator serwera VIOS musi określić nazwę dziennika wirtualnego, który zawiera następujące oddzielne komponenty:

- Nazwa klienta
- Nazwa dziennika

Nazwy dwóch komponentów mogą być ustawiane przez administratora serwera VIOS na dowolną wartość, ale nazwa klienta jest zwykle taka sama dla wszystkich dzienników wirtualnych, które są przyłączone do danej partycji LPAR (na przykład nazwa hosta partycji LPAR). Nazwa dziennika jest używana do identyfikowania przeznaczenia dziennika (na przykład kontrola lub syslog).

W partycji LPAR z systemem AIX każde urządzenie rejestrujące jest widoczne jako dwa funkcjonalnie równoważne pliki w systemie plików /dev. Pierwszy plik nazywa się tak, jak urządzenie, na przykład /dev/vlog0, a drugi plik ma nazwę łączącą przedrostek vl z nazwą protokołu i numerem urządzenia. Na przykład, jeśli wirtualne urządzenie dziennika vlog0 ma podaną wartość audit jako nazwę dziennika, będzie ono widziane w systemie plików /dev zarówno jako vlog0 i vlaudit0.

Informacje pokrewne:

Tworzenie wirtualnych dzienników

Wykrywanie wirtualnych urządzeń rejestrujących

Po utworzeniu przez administratora serwera VIOS wirtualnych urządzeń rejestrujących i przyłączeniu ich do klienckiej partycji LPAR, należy odświeżyć konfigurację urządzeń klienckiej partycji LPAR dla urządzeń, które mają być widoczne.

Administrator klienckiej partycji LPAR może odświeżyć ustawienia za pomocą jednej z następujących metod:

- Zrestartowanie klienckiej partycji LPAR.
- Uruchomienie komendy **cfgmgr**.

Uruchomienie komendy **lsdev**, aby wyświetlić listę wirtualnych urządzeń rejestrujących. Urządzenia te są domyślnie poprzedzane przedrostkiem vlog. Poniżej przedstawiono przykład danych wyjściowych komendy **lsdev** w systemie AIX partycji LPAR, w którym znajdują się dwa urządzenia dzienników wirtualnych:

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

Sprawdź właściwości poszczególnych urządzeń wirtualnego dziennika za pomocą komendy lsattr El <*nazwa urządzenia*>, które generuje dane wyjściowe podobne do następujących:

```
lsattr –El vlog0
PCM                     Moduł sterowania ścieżkami                Fałsz
client_name    dev-lpar-05 Nazwa klienta                          Fałsz
device_name    vlsyslog0   Nazwa urządzenia                       Fałsz
log_name       syslog      Nazwa dziennika                       Fałsz
max_log_size   4194304     Maksymalna wielkość pliku dziennika   Fałsz
max_state_size 2097152     Maksymalna wielkość pliku stanu protokołu  Fałsz
pvid           brak        Identyfikator fizycznego woluminu     Fałsz
```

Ten raport wyświetla nazwę klienta, nazwę urządzenia i ilość danych dziennika, które można zapisać na serwerze VIOS.

Dziennik wirtualny może zapisywać dwa typy danych:

- Dane dziennika: surowe dane dziennika generowane przez aplikacje w systemie AIX partycji LPAR.
- Dane stanu: informacje o tym, kiedy urządzenia zostały skonfigurowane, otwarte, zamknięte oraz inne operacje, które są używane do analizowania aktywności dziennika.

Administrator serwera VIOS może określić ilość **danych dziennika** i **danych stanu**, które mogą być zapisywane dla każdego dziennika wirtualnego. Jest ona określona przez wartości atrybutów max_log_size i max_state_size. Gdy ilość przechowywanych danych przekroczy podany limit, najwcześniejsze dane dziennika zostaną nadpisane. Administrator serwera VIOS musi upewnić się, że dane dziennika są gromadzone i archiwizowane wystarczająco często, aby je zabezpieczyć.

Instalowanie zaufanego rejestrowania

Funkcję zaufanego rejestrowania PowerSC można zainstalować za pomocą interfejsu wiersza komend lub narzędzia SMIT.

Wymaganiem wstępnym dla instalacji zaufanego rejestrowania jest serwer VIOS w wersji 2.2.1.0 lub nowszej i system IBM AIX 6 z pakietem Technology Level 7 lub IBM AIX 7 z pakietem Technology Level 1.

Nazwą pliku dla instalacji zaufanego rejestrowania jest powerscStd.vlog, który znajduje się na dysku instalacyjnym CD PowerSC Standard Edition.

Aby zainstalować funkcję zaufanego rejestrowania:

1. Upewnij się, że uruchomiony jest serwer VIOS w wersji 2.2.1.0 lub nowszej.
2. Włóż dysk instalacyjny CD produktu PowerSC lub pobierz obraz z instalacyjnego dysku CD.
3. Użyj komendy **installp** lub narzędzia SMIT, aby zainstalować zestaw plików powerscStd.vlog.

Informacje pokrewne:

“instalowanie produktu PowerSC Standard Edition 1.1.3” na stronie 7
Należy zainstalować zestaw plików dla każdej z wybranych funkcji produktu PowerSC Standard Edition.

Konfigurowanie zaufanego rejestrowania

Poniżej przedstawiono procedurę konfigurowania zaufanego rejestrowania w podsystemie kontroli AIX i dla mechanizmu syslog.

Konfigurowanie podsystemu kontroli AIX

Podsystem kontroli AIX można skonfigurować do zapisywania danych binarnych do wirtualnego urządzenia rejestrującego oprócz zapisywania dzienników w lokalnym systemie plików.

Uwaga: Przed skonfigurowaniem podsystemu kontroli systemu AIX, należy wykonać procedurę opisaną w sekcji “Wykrywanie wirtualnych urządzeń rejestrujących” na stronie 115.

Aby skonfigurować podsystem kontroli systemu AIX, wykonaj następujące czynności:

1. Skonfiguruj podsystem kontroli AIX do rejestrowania danych w trybie binarnym (auditbin) .
2. Aktywuj zaufane rejestrowanie dla kontroli AIX, edytując plik konfiguracyjny /etc/security/audit/config.
3. Dodaj parametr virtual_log =/dev/vlog0 do sekcji bin:.

   Uwaga: Ta instrukcja jest poprawna, jeśli administrator LPAR chce, aby dane auditbin były zapisywane w pliku /dev/vlog0.
4. Zrestartuj podsystem kontroli AIX w następującej kolejności:

   ```
   audit shutdown
   audit start
   ```

Rekordy kontroli będą zapisywane w produkcie serwer VIOS (VIOS) za pośrednictwem podanego wirtualnego urządzenia protokołującego oprócz zapisywania dzienników do lokalnego systemu plików. Dzienniki są zapisywane zgodnie z parametrami bin1 i bin2 podanymi w sekcji bin: w pliku konfiguracyjnym /etc/security/audit/config.

Informacje pokrewne:

Podsystem kontrolujący

Konfigurowanie syslog

Można skonfigurować systemowy mechanizm syslog do zapisywania komunikatów do wirtualnych dzienników, dodając odpowiednie reguły do pliku /etc/syslog.conf.

Uwaga: Przed skonfigurowaniem pliku /etc/syslog.conf należy wykonać procedurę opisaną w sekcji “Wykrywanie wirtualnych urządzeń rejestrujących” na stronie 115.

Można zmodyfikować plik /etc/syslog.conf w celu dopasowania komunikatów dziennika w oparciu o następujące kryteria:

- Narzędzie
- Poziom priorytetu

Aby użyć dzienników wirtualnych dla komunikatów syslog, należy skonfigurować reguły w pliku /etc/syslog.conf, aby zapisywać żądane komunikaty do dziennika odpowiedniego wirtualnego w katalogu /dev.

Na przykład, aby wysyłać komunikaty na poziomie debugowania utworzone przez dowolne narzędzie do wirtualnego urządzenia vlog0, dodaj następujący wiersz do pliku /etc/syslog.conf:

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

Uwaga: Nie należy używać funkcji rotacji dziennika, które są dostępne dla demona syslogd dla żadnej z komend, które zapisują dane do dzienników wirtualnych. Pliki w systemie plików /dev nie są zwykłymi plikami i nie można ich zmieniać ani przenosić. Administrator systemu VIOS musi skonfigurować rotację dzienników wirtualnych w ramach serwera VIOS.

Po zakończeniu konfigurowania należy zrestartować demona syslogd za pomocą następującej komendy:

```
refresh -s syslogd
```

Informacje pokrewne:

Demon syslogd

Zapisywanie danych do wirtualnych urządzeń rejestrujących

Do wirtualnego urządzenia rejestrującego można zapisać dowolne dane otwierając odpowiedni plik w katalogu /dev i zapisując dane do tego pliku. Dziennik wirtualny można być otwarty jednocześnie tylko przez jeden proces.

Na przykład:

Aby zapisać komunikaty do wirtualnych urządzeń rejestrujących przy użyciu komendy **echo**, wpisz następującą komendę:

```
echo "Komunikat dziennika" > /dev/vlog0
```

Aby zapisywać pliki w wirtualnych urządzeń rejestrujących przy użyciu komendy **cat**, użyj następującej komendy:

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

Maksymalna wielkość pojedynczego zapisu jest ograniczona do 32 KB, a programy, które spróbują zapisać więcej danych w pojedynczej operacji zapisu otrzymają błąd we/wy (EIO). Programy narzędziowe działające w wierszu komend, takie jak komenda **cat**, automatycznie dzielą przesyłane dane na operacje zapisu o wielkości 32KB.

Zaufana sieć (Trusted Network Connect — TNC)

Zaufana sieć (TNC) jest częścią mechanizmu TCG (Trusted Computing Group), który udostępnia specyfikacje umożliwiające sprawdzanie integralności punktów końcowych. TNC definiuje otwartą architekturę ułatwiającą administratorom wymuszanie strategii pozwalających na efektywną kontrolę dostępu do infrastruktury sieciowej.

Zaufana sieć zawiera cztery komponenty:

- Serwer TNC
- Zarządzanie poprawkami TNC
- Serwer TNC
- Odsyłacz IP dla TNC

Pojęcia dotyczące zaufanej sieci (TNC)

Sekcja zawiera informacje na temat komponentów, konfigurowania bezpiecznej komunikacji oraz systemu zarządzania poprawkami dla zaufanej sieci (TNC).

Komponenty połączenia z zaufaną siecią

Sekcja zawiera informacje na temat komponentów środowiska zaufanej sieci (TNC).

Model sieci TNC składa się z następujących komponentów:

Serwer zaufanej sieci (Trusted Network Connect — TNC)

Serwer zaufanej sieci (TNC) identyfikuje klienty, które są dodawane do sieci i inicjuje ich weryfikację.

Klient TNC udostępnia serwerowi wymagane informacje o wersji zestawu plików w celu wykonania weryfikacji. Serwer określa, czy klient jest we właściwej wersji skonfigurowanej przez administratora. Jeśli klient nie jest zgodny, serwer TNC powiadamia administratora o wymaganych działaniach naprawczych.

Serwer TNC inicjuje weryfikacje klientów, którzy próbują uzyskać dostęp do sieci. Serwer TNC ładuje zestawy weryfikacyjne integralności (IMV), które mogą zażądać od klientów przesłania danych o integralności i ją zweryfikować. System AIX zawiera domyślny zestaw IMV, który weryfikuje zestaw plików o wersje poprawek zainstalowane w systemie. Serwer TNC jest środowiskiem, które ładuje wiele modułów IMV i zarządza nimi. Przy weryfikowaniu klienta wykorzystuje on zestawy IMV do wysyłania żądań informacji do klientów i ich weryfikowania.

Zarządzanie poprawkami TNC

Serwer zaufanej sieci (TNC) integruje się z SUMA (Service Update Management Assistant) i cURL, tworząc wszechstronne rozwiązanie do zarządzania poprawkami.

Menedżer poprawek pobiera najnowsze pakiety z poprawkami i poprawki bezpieczeństwa dostępne w serwisach WWW IBM ECC i Fix Central. Demon zarządzania poprawkami TNC przekazuje ostatnio zaktualizowane informacje do serwera TNC, który obsługuje podstawowy zestaw plików do sprawdzania klientów.

Należy skonfigurować demona **tncpmd** w taki sposób, aby zarządzał pobieraniem za pośrednictwem asystenta SUMA i aby wysyłał informacje o zestawie plików do serwera TNC. Ten demon musi być uruchomiony w systemie, który jest podłączony do Internetu, aby można było automatycznie pobierać aktualizacje. Aby korzystać z serwera zarządzania poprawkami TNC bez podłączania go do Internetu, można zarejestrować zdefiniowane przez użytkownika repozytorium poprawek na serwerze zarządzania poprawkami TNC.

Uwaga: Serwer TNC oraz demon **tncpmd** mogą być zainstalowane w tym samym systemie.

Zarządzanie poprawkami odbywa się za pomocą jednej z następujących metod:

- Za pomocą interfejsu wiersza komend (pmconf)
- Za pomocą demona (tncpmd2)

Używanie interfejsu wiersza komend (pmconf) do zarządzania poprawkami:

Asystent SUMA i narzędzie cURL są wywoływane, gdy poziom pakietu serwisowego jest pobierany za pomocą komendy **pmconf add**.

Gdy poziom pakietu serwisowego jest pobierany za pomocą komendy **pmconf add**, wywoływany jest asystent SUMA w celu pobrania i zarejestrowania tego poziomu pakietu serwisowego w TNC. Ponadto wywoływane jest narzędzie cURL w celu pobrania nowych lub brakujących poprawek bezpieczeństwa.

Następujące argumenty komendy **pmconf get** umożliwiają dodatkowe sterowanie w ramach zarządzania poprawkami bezpieczeństwa:

- **display-only** umożliwia użytkownikowi sprawdzenie opisów słabych punktów zabezpieczeń obsługiwanych przez poprawki bezpieczeństwa, które są stosowane dla tego poziomu pakietu serwisowego. Poprawki bezpieczeństwa nie są pobierane przy użyciu tej komendy.
- **download-only** umożliwia użytkownikowi pobranie, ale nie zastosowanie, poprawek bezpieczeństwa do biblioteki pobierania określonej przez użytkownika. Żadne poprawki nie są stosowane.

Używanie demona (tncpmd2) do zarządzania poprawkami:

Komponent programu planującego demona można skonfigurować do automatycznego sprawdzania aktualizacji wpływających na bezpieczeństwo klientów TNC.

Program planujący szuka nowych poziomów pakietów serwisowych z częstotliwością określoną za pomocą przedziału czasu pobierania. Jeśli dla pakietu Technology Level (TL), który jest w danej chwili zarejestrowany w TNC, zostanie wykryty nowy poziom pakietu serwisowego, do repozytorium zostanie pobrany i dodany ten nowy poziom pakietu serwisowego i wszystkie brakujące nowe poprawki bezpieczeństwa. Przedział czasu pobierania ustawia się za pomocą komendy **pmconf init**. Zalecaną wartością jest co najmniej jeden raz na miesiąc (43200 minut).

Program planujący szuka nowych opublikowanych poprawek tymczasowych bezpieczeństwa z częstotliwością określoną za pomocą parametru ifix_download_interval. Wszystkie nowe poprawki bezpieczeństwa są pobierane i dodawane do repozytorium. Zalecany przedział czasu pobierania poprawek tymczasowych wynosi raz dziennie (1440 minut).

Klient połączenia z zaufaną siecią

Klient zaufanej sieci (TNC) udostępnia informacje, które są wymagane przez serwer TNC dla weryfikacji.

Serwer określa, czy klient jest w wersji skonfigurowanej przez administratora. Jeśli klient nie jest zgodny, serwer TNC powiadamia administratora o aktualizacjach, które są wymagane.

Klient TNC ładuje IMC podczas uruchamiania i używa IMC do gromadzenia wymaganych informacji.

Odsyłacz IP dla zaufanej sieci (TNC)

Serwer zaufanej sieci (TNC) serwer może automatycznie zainicjować weryfikację dla klientów, które są podłączeni do sieci. Odsyłacz IP działający na partycji serwera VIOS (serwer VIOS) wykrywa nowe klienty obsługiwane przez serwer VIOS i wysyła ich adresy IP do serwera TNC. Serwer TNC sprawdza klienta zgodnie ze zdefiniowaną strategią.

Bezpieczna komunikacja w zaufanej sieci

Demony zaufanej sieci (TNC) komunikują się przez zaszyfrowane kanały zestawione przy użyciu protokołu TLS (Transport Layer Security lub SSL (Secure Sockets Layer).

Bezpieczna komunikacja zapewnia, dane i komendy, które są przesyłane w sieci, są uwierzytelnione i bezpieczne. Każdy system musi mieć własny klucz i certyfikat, które są generowane po uruchomieniu komendy inicjowania komponentów. Ten proces jest całkowicie przezroczysty dla administratora i wymaga mniej zaangażowanie z jego strony.

Aby zweryfikować nowego klienta, należy zaimportować certyfikat klienta do bazy danych serwera. Certyfikat jest początkowo oznaczony jako niezaufany, a administrator może użyć komendy **psconf**, aby wyświetlać certyfikaty i oznaczyć je jako zaufane, wprowadzając następującą komendę:

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

Aby można było użyć innego klucza i certyfikatu, komenda **psconf** pozwala również na importowanie kluczy i certyfikatów.

Aby zaimportować certyfikat z serwera, wprowadź następującą komendę:

```
psconf import  -S -k<nazwa pliku klucza> -f<nazwa pliku klucza>
```

Aby zaimportować certyfikat z klienta, wprowadź następującą komendę:

```
psconf import -C -k<nazwa pliku klucza> -f<nazwa pliku klucza>
```

Protokół TNC (Trusted Network Connect)

Środowisko TNC używa protokołu TNC (Trusted Network Connect) w celu zachowania integralności sieci.

Zaufana sieć TNC udostępnia specyfikację umożliwiającą sprawdzenie integralności punktu końcowego. Żądanie dostępu wysyłane przez punkty końcowe są oceniane na podstawie pomiarów integralności najważniejszych komponentów, które mogą mieć wpływ na ich środowiska operacyjne. Środowisko TNC umożliwia administratorom monitorowanie integralności systemów w sieci. TNC jest zintegrowane z infrastrukturą dystrybucji poprawek AIX tworząc kompletne rozwiązanie do zarządzania poprawkami.

Specyfikacja TNC musi spełnić wymagania systemu AIX i architektury systemowej rodziny POWER. Komponenty środowiska TNC zostały zaprojektowane tak, aby powstało kompletne środowisko do zarządzania poprawkami dla systemu operacyjnego AIX. Taka konfiguracja umożliwia administratorom efektywne zarządzanie konfiguracją oprogramowania w instalacjach systemu AIX. Udostępnia ona narzędzia do weryfikowania poziomów poprawek w systemach i generowania raportów dla klientów, które nie spełniają wymagań dotyczących zgodności. Dodatkowo mechanizm zarządzanie poprawkami uprasza proces pobierania i instalowania poprawek.

Moduły IMC i IMV

Serwer lub klient zaufanej sieci (TNC) wewnętrznie korzystają z modułów IMC (Integrity Measurement Collector) i IMV (Integrity Measurement Verifier) do weryfikacji serwera.

Ta struktura umożliwia ładowanie wielu modułów IMC i IMV do serwera i klientów. Moduł, który wykonuje weryfikację systemu operacyjnego (OS) i zestawu plików jest standardowo dostarczany wraz z systemem operacyjnym AIX. Aby uzyskać dostęp do modułów, które są dostarczane z systemem operacyjnym AIX, użyj jednej z następujących ścieżek:

- /usr/lib/security/tnc/libfileset_imc.a: Gromadzi informacje na temat poziom systemu operacyjnego i zestawu plików, który jest zainstalowany w systemie klienta i wysyła je do modułu IMV (serwer TNC) dla weryfikacji.
- /usr/lib/security/tnc/libfileset_imv.a: Żąda od klienta podania informacji o poziomie systemu operacyjnego i zestawie plików i porównuje je z informacjami bazowymi. Ponadto aktualizuje status klienta w bazie danych serwera TNC. Aby wyświetlić status, wprowadź następującą komendę:

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

Odsyłacze pokrewne:

“Komenda psconf” na stronie 163

TNC — wymagania

Aby w pełni korzystać ze wszystkich funkcji każdego komponentu TNC, należy się upewnić, że w danym środowisku spełniono minimalne wymagania.

Zarządzanie poprawkami TNC

AIX	SUMA	OpenSSL	Notes
7.2 TL1	7.2.1.0	1.0.2	Dostarczany z systemem operacyjnym
7.2 TL0	7.2.1.0	1.0.2	Może być konieczna oddzielna instalacja SUMA/Java.
7.1 TL4	7.2.1.0	1.0.2	Może być konieczna oddzielna instalacja SUMA/Java.
7.1 TL1, TL2, TL3			Brak obsługi pobierania poziomów Service Pack systemu AIX 7.2
7.1 TL0			Minimalny obsługiwany poziom wydania TNCPM

Konfigurowanie komponentów TNC

Każdy komponent TNC (Trusted Network Connect) wymaga pewnej konfiguracji, aby mógł działać w danym środowisku.

Do skonfigurowania komponentów TNC należy wykonać każdy krok z poniższej procedury. Opisano również kroki opcjonalne.

1. Określ adresy IP systemów, w których będą konfigurowane: serwer TNC, serwer TNCPM (TNC Patch Management) oraz TNC IP referrer dla serwer VIOS (VIOS).
2. Skonfiguruj serwer do zarządzania instalacją sieciową (NIM). System, który został skonfigurowany jako serwer TNCPM, jest głównym serwerem NIM. W tym systemie musi być zainstalowany zestaw plików sets:bos.sysmgt.nim.master.
3. Należy włączyć komponent AHA (Autonomic Health Advisor) w celu automatycznego powiadamiania serwera TNC o nowych pakietach poprawek i poprawkach. Jeśli komponent AHA nie zostanie włączony, program planujący TNC będzie aktualizować serwer TNC w zaplanowanych odstępach czasu. Aby włączyć automatyczne powiadomienia AHA:

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

4. Aby zainicjować repozytoria poprawek dla TNC Patch Management, wpisz następującą komendę (w jednym wierszu):

   ```
   pmconf init -i <odstęp czasu pobierania> -l <lista TL> [-A] [-P <ścieżka pobierania>]
   [-x <odstęp czasu ifix>] [-K <klucz ifix>]
   ```

   Oto przykład komendy **pmconf**:

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

   Komenda **init** pobiera najnowszy pakiet poprawek dla każdego poziomu poprawek i udostępnia go dla serwera TNC. Zaktualizowane pakiety serwisowe pozwalają serwerowi TNC na uruchomienie podstawowej weryfikacji klienta TNC, a serwerowi zarządzania poprawkami TNC na instalowanie aktualizacji klienta TNC. Podaj opcję **-A**, aby zaakceptować wszystkie umowy licencyjne po uruchomieniu aktualizacji klienta. Domyślnie repozytoria poprawek, które są pobierane przez serwer zarządzania poprawkami TNC, znajdują się w pliku /var/tnc/tncpm/fix_repository. Użyj opcji **-P**, aby określić inny katalog.
5. Skonfiguruj serwer TNCPM. Serwer TNCPM może być skonfigurowany w systemie NIM. Serwer TNCPM używa mechanizmu SUMA do pobierania poprawek z serwisów WWW IBM Fix Central i ECC. Serwer TNCPM używa narzędzia cURL do pobierania poprawek ifiix z serwisu IBM Security. Aby można było pobrać poprawki, system musi być podłączony do Internetu. Wprowadź następującą komendę, aby skonfigurować serwer TNCPM:

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

Na przykład:

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

6. Skonfiguruj strategie na serwerze TNC. Aby utworzyć strategie dla weryfikowania klientów, zapoznaj się z informacjami podanymi w sekcji “Tworzenie strategii dla klienta zaufanej sieci (TNC)” na stronie 127.
7. Skonfiguruj klienty, używając następującej komendy:

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

Na przykład:

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

8. Dokończ konfigurowanie komponentów TNC, wykonując opcjonalne kroki dla każdego z nich.

Odsyłacze pokrewne:

“Komenda psconf” na stronie 163

Informacje pokrewne:

“instalowanie produktu PowerSC Standard Edition 1.1.3” na stronie 7

Należy zainstalować zestaw plików dla każdej z wybranych funkcji produktu PowerSC Standard Edition.

Instalowanie za pomocą NIM

IBM Fix Central

Centrum pomocy Passport Advantage Online

Konfigurowanie opcji dla komponentów TNC

Dla każdego z komponentów TNC można skonfigurować co najmniej jedną opcję.

Konfigurowanie opcji dla serwera zaufanej sieci (TNC)

W sekcji opisano kroki wymagane do skonfigurowania serwera TNC.

Aby skonfigurować serwer TNC, plik /etc/tnccs.conf musi zawierać pozycję podobną do poniższej:

```
component = SERVER
```

Aby skonfigurować system jako serwer, wprowadź następującą komendę:

```
psconf mkserver tncport=<port> pmserver=<ip|nazwa_hosta[,ip2|nazwa_hosta2..]:port>
[recheck_interval=<czas w minutach>]
```

Na przykład:

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

Uwaga: Numery portów tncport i pmserver muszą mieć ustawione różne wartości, a jeśli wartość parametru recheck_interval nie zostanie podana, zostanie użyta wartość domyślna 1440 minut.

Dla portu tncport jest używana wartość domyślna wynosząca 42830, a dla portu pmserver wartość domyślna równa 38240.

Odsyłacze pokrewne:

“Komenda psconf” na stronie 163

Konfigurowanie opcji dodatkowych dla klienta zaufanej sieci (TNC)

W tej sekcji opisano kroki wymagane do skonfigurowania klienta zaufanej sieci (TNC) i wymagane ustawienia konfiguracyjne.

Aby skonfigurować klienta TNC, plik /etc/tnccs.conf musi zawierać pozycję podobną do poniższej:

```
component = CLIENT
```

Aby skonfigurować system jako klienta, wprowadź następującą komendę:

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

Na przykład:

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

Uwaga: Wartości portu serwera i portu klienta tncport muszą być takie same.

Odsyłacze pokrewne:

"Komenda psconf" na stronie 163

Konfigurowanie opcji dla serwera zarządzania poprawkami dla TNC

Serwer zarządzania poprawkami zaufanej sieci (TNCPM) integruje się z narzędziami SUMA i cURL, tworząc wszechstronne rozwiązanie do zarządzania poprawkami.

Należy skonfigurować serwer TNCPM w serwerze zarządzania instalacją sieciową (NIM), aby można było aktualizować klienty TNC.

Aby włączyć automatyczne pobieranie zaleceń IBM dotyczących bezpieczeństwa i poprawek tymczasowych, można określić przedział czasu dla poprawek tymczasowych. Ten składnik udostępnia automatyczne powiadamianie o nowo opublikowanych poprawkach tymczasowych dotyczących zabezpieczeń i powiązanych z nimi identyfikatorach CVE (Common Vulnerabilities and Exposures). Wszystkie porady dotyczące bezpieczeństwa i poprawki tymczasowe są weryfikowane przed ich zarejestrowaniem na serwerze TNC. Klucz publiczny systemu IBM AIX, który jest wymagany do automatycznego pobierania poprawek tymczasowych dotyczących bezpieczeństwa, jest dostępny do pobrania z serwisu WWW IBM AIX Security. Automatyczne pobieranie pakietów serwisowych i poprawek tymczasowych można wyłączyć, ustawiając dla przedziału czasu pobierania i przedziału czasu dla poprawek tymczasowych wartość 0.

Można także samodzielnie zaktualizować rejestrację pakietu serwisowego i poprawki tymczasowej. Aby samodzielnie zarejestrować zalecenie dotyczącymi bezpieczeństwa IBM Security Advisory wraz z odpowiednimi poprawkami tymczasowymi, wprowadź następującą komendę:

```
pmconf add -y <plik zalecenia> -v <plik sygnatury>  -e <plik tar ifix>
```

Aby samodzielnie zarejestrować autonomiczną poprawkę tymczasową, wprowadź następującą komendę:

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

Aby zarejestrować nowy poziom poprawek i pobrać jego najnowszy pakiet serwisowy, wprowadź następującą komendę:

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

Aby pobrać pakiet serwisowy, który nie jest w najnowszej wersji, lub aby pobrać pakiet poprawek, który ma być używany do weryfikacji i aktualizacji klienta, wprowadź następującą komendę:

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

Aby zarejestrować repozytorium pakietów serwisowych lub pakietów poprawek, które istnieje w systemie, wpisz następującą komendę:

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

Aby skonfigurować system jako serwer zarządzania poprawkami, wprowadź następującą komendę:

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

Przykład tej komendy:

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

Serwer zarządzania poprawkami TNC zawsze obsługuje zarządzanie zabezpieczeniami raportami APAR (Authorized Problem Analysis Report) dotyczącymi bezpieczeństwa. Wprowadź następującą komendę, aby skonfigurować serwer zarządzający poprawkami TNC do zarządzania innymi typami raportów APAR:

```
pmconf add -t <lista_typów_APAR>
```

W tym przykładzie <lista_typów_APAR> to rozdzielana przecinkami lista zawierająca następujące typy raportów APAR:

- HIPER
- PE
- Enhancement

Aby zarządzać repozytoriami pakietów TNCPM Open, wpisz jedną lub więcej z następujących komend:

```
pmconf add -o <nazwa pakietu> -V
<wersja> -T [installp|rqm] -D <ścieżka
użytkownika>
pmconf delete -o <nazwa pakietu> -V
<wersja>
pmconf list -o <nazwa pakietu> -V
<wersja>
pmconf list -O [-c] [-q]
```

Pakiety Open są dodawane do tego katalogu domyślnego:

/var/tnc/tncpm/fix_repository/packages.

Ścieżka użytkownika = położenie pakietu w systemie

Aby wyświetlić opisowe informacje dotyczące poprawek bezpieczeństwa dla konkretnej wersji pakietu poprawek bez stosowania poprawek w repozytorium, wpisz następującą komendę:

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

Na przykład:

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

Aby pobrać poprawki bezpieczeństwa dla konkretnej wersji pakietu poprawek bez stosowania poprawek w repozytorium, wpisz następującą komendę:

```
pmconf get -p <SP> -D <katalog
pobierania>
```

Uwaga: Przed wykonaniem tej komendy musi istnieć *katalog pobierania*.

Na przykład:

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

Serwer zarządzania poprawkami TNC obsługuje komendę **syslog** w celu pobierania pakietów serwisowych, pakietów poprawek i aktualizacji klienta. Poziom istotności to user, a priorytet to info. Przykład: user.info.

Serwer zarządzania poprawkami TNC utrzymuje także również dziennik wszystkich aktualizacji klienta w pliku /var/TNC/tncpm/log/update/<ip><znacznik_czasu>.

Odsyłacze pokrewne:

“Komenda psconf” na stronie 163

Informacje pokrewne:

Konfigurowanie powiadomienia e-mail dla serwera połączenia z zaufaną siecią (TNC)

W tej sekcji opisano procedurę konfigurowania powiadomienia e-mail dla serwera zaufanej sieci (TNC).

Serwer TNC sprawdza poziom poprawek klienta TNC i jeśli serwer stwierdzi, że klient nie jest zgodny, wysyła wiadomość e-mail do administratora z wynikami i z wymaganymi działaniami naprawczymi.

Aby skonfigurować adres e-mail administratora, wpisz następującą komendę:

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

Na przykład:

```
psconf add –e abc@firma.pl ipgroup=vayugrp1,vayugrp2
```

W powyższym przykładzie wiadomość e-mail dla grupy IP *vayugrp1* i *vayugrp2* będzie wysłana na adres abc@firma.pl.

Aby wysłać wiadomość e-mail na globalny adres e-mail dla grupy IP, która nie ma przypisanego adresu e-mail, wprowadź następującą komendę:

```
psconf add –e <adres_email>
```

Na przykład:

```
psconf add –e abc@firma.pl
```

W poprzednim przykładzie, jeśli grupa IP nie ma przypisanego adresu e-mail, wiadomość e-mail zostanie wysłana na adres abc@firma.pl. Będzie on działać jako globalny adres e-mail.

Odsyłacze pokrewne:

“Komenda psconf” na stronie 163

Konfigurowanie odsyłacza IP na serwerze VIOS

Sekcja zawiera informacje na temat konfigurowania odsyłacza IP na serwerze serwer VIOS (VIOS) w celu automatycznego inicjowania weryfikacji.

Uwaga: Przed skonfigurowaniem odsyłacza IP na wirtualnym serwerze we/wy (VIOS) należy skonfigurować rozszerzenie jądra SVM.

Aby skonfigurować odsyłacz IP dla serwera TNC, plik konfiguracyjny /etc/tnccs.conf musi zawierać poniższe ustawienie: komponent = IPREF.

Aby skonfigurować system jako klienta, wprowadź następującą komendę:

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

Na przykład:

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

Wartości portu tncserver i portu klienta tncport muszą być takie same.

Skonfiguruj odsyłacz IP dla TNC na serwerze VIOS. Ta konfiguracja w systemie VIOS wyzwala weryfikację klientów podłączających się do sieci. Wprowadź następującą komendę, aby skonfigurować odsyłacz:

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

Na przykład:

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

Uwaga: Wartości portu serwera i portu TNC, który jest portem klienta, muszą być takie same.

Odsyłacze pokrewne:

"Komenda psconf" na stronie 163

Zarządzanie komponentami TNC (Trusted Network Connect)

Sekcja zawiera informacje na temat zarządzania siecią zaufaną (TNC) w celu zaimplementowania zadań, takich jak dodawanie klientów, strategie, dzienniki, wyniki weryfikacji, aktualizowanie klientów oraz certyfikatów dotyczących TNC.

Wyświetlanie dzienników serwera sieci zaufanej

W sekcji opisano procedurę wyświetlania dzienników serwera zaufanej sieci (TNC).

Serwer TNC rejestruje wyniki weryfikacji dla wszystkich klientów. Aby wyświetlić dziennik, uruchom komendę **psconf**:

```
psconf list –H –i <ip |ALL>
```

Odsyłacze pokrewne:

"Komenda psconf" na stronie 163

Tworzenie strategii dla klienta zaufanej sieci (TNC)

Sekcja zawiera informacje na temat konfigurowania strategii dotyczących klienta sieci zaufanej (TNC).

Konsola psconf udostępnia interfejs wymagany do zarządzania strategiami TNC. Każdy klient lub grupa klientów może być powiązany ze strategią.

Można utworzyć następujące strategie:

- Grupa IP zawierająca wiele adresów IP klientów.
- Każdy adres IP klienta może należeć tylko do jednej grupy.
- Grupa IP jest powiązana z grupą strategii.
- Grupa strategii zawiera różne rodzaje strategii. Na przykład strategia zestawu plików określa, jaka musi być wersja systemu operacyjnego klienta (tj. wydanie, poziom poprawek i pakiet serwisowy). W grupie strategii może istnieć wiele strategii zestawu plików i klient, który odwołuje się do tej strategii, musi być w wersji określonej przez jeden z plików strategii.

Następujące komendy pokazują, w jaki sposób można utworzyć grupę IP, grupę strategii oraz strategie zestawu plików.

Aby utworzyć grupę IP, wpisz następującą komendę:

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

Na przykład:

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

Uwaga: Dla grupy należy podać co najmniej jeden adres IP. Wiele adresów IP należy rozdzielić przecinkami.

Aby utworzyć strategię dla zestawu plików, wpisz następującą komendę:

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

Na przykład:

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

Uwaga: Informacje o kompilacji należy podać w formacie <rel00-TL-sp>.

Aby utworzyć strategię i przypisać grupę IP, wpisz następującą komendę:

```
psconf add –P <nazwa_strategii> ipgroup=[±] <grp_ip1, grp_ip2 ...]
```

Na przykład:

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

Aby przypisać strategię dla zestawu plików do strategii, wpisz następującą komendę:

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

Na przykład:

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

Aby dodać strategię OpenPackage, wpisz następującą komendę:

```
pconf add -O <grupa_openpkg>
<nazwa_openpkg:wersja>
```

Poniżej przedstawiono przykład dodawania strategii OpenPackage:

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

Aby przypisać strategię OpenPackage do strategii Fspolicy, wpisz następującą komendę:

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

Uwaga: Jeśli zostanie podane wiele strategii dla plików, system wymusi na kliencie najlepiej pasującą strategię. Na przykład, jeśli klient jest na 6100-02-01 i podano strategię zestawu plików jako 7100-03-04 i 6100-02-03, na kliencie zostanie wymuszona strategia 6100-02-03.

Odsyłacze pokrewne:

"Komenda psconf" na stronie 163

Uruchamianie weryfikacji dla klienta zaufanej sieci (TNC)

Sekcja zawiera informacje na temat weryfikacji klienta zaufanej sieci (TNC).

Użyj jednej z następujących metod w celu zweryfikowania klienta:

- Demon odsyłacza IP w serwerze serwer VIOS (VIOS) przekazuje adres IP klienta do serwera TNC: partycja kliencka LPAR pobiera adres IP i próbuje połączyć się z siecią. Demon odsyłacza IP na serwerze VIOS wykrywa nowy adres IP i przekazuje go do serwera TNC. Następnie serwer TNC inicjuje weryfikację po odebraniu nowego adresu IP.
- Serwer TNC okresowo weryfikuje klienta. Administrator może dodać adres IP klienta do weryfikacji do bazy danych strategii TNC. Serwer TNC weryfikuje klienty, które znajdują się w bazie danych. Ponowna weryfikacja odbywa się automatycznie w regularnych odstępach czasu określonym przez wartość atrybutu recheck_interval, który jest umieszczony w pliku konfiguracyjnym /etc/tnccs.conf.
- Administrator samodzielnie inicjuje weryfikację klienta. Administrator może zainicjować samodzielnie weryfikację, aby sprawdzić, czy klient został dodany do sieci, uruchamiając następującą komendę:

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

Uwaga: Dla zasobów, które nie są podłączone do serwera VIOS można weryfikować i aktualizować klienty podczas ich samodzielnego dodawania do serwera TNC.

Odsyłacze pokrewne:

"Komenda psconf" na stronie 163

Wyświetlanie wyników weryfikacji dla zaufanej sieci

W sekcji opisano procedurę wyświetlania wyników weryfikacji klienta zaufanej sieci (TNC).

Aby wyświetlić wyniki weryfikacji klientów w sieci, wprowadź następującą komendę:

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

Ta komenda wyświetla wszystkie klienty, które mają status **IGNORED**, **COMPLIANT** lub **FAILED**.

- **IGNORED**: Adres IP klienta jest ignorowany na liście adresów IP (oznacza to, że klient może być wyłączone z weryfikacji).
- **COMPLIANT**: Klient przeszedł weryfikację, tzn. jest zgodny ze strategią.
- **FAILED**: Weryfikacja klienta nie powiodła się, oznacza to, że klient nie jest zgodny ze strategią i wymagane są działania administracyjne).

Aby określić przyczynę niepowodzenia, należy uruchomić komendę **psconf** podając adres IP klienta, dla którego wystąpiło niepowodzenie:

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

Odsyłacze pokrewne:

“Komenda psconf” na stronie 163

Aktualizowanie klienta zaufanej sieci

Serwer zaufanej sieci (TNC) weryfikuje klienta i aktualizuje w bazie danych status klienta i wynik weryfikacji. Administrator może wyświetlić wyniki i podjąć działania w celu zaktualizowania klienta.

Aby zaktualizować klienta, który jest we wcześniejszej wersji, wprowadź następującą komendę:

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

Na przykład:

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

Komenda **psconf** aktualizuje klienta przy użyciu odpowiedniej wersji i poprawek APAR, jeśli nie są one zainstalowane.

Aby zaktualizować klienta z pakietami Open:

```
psconf update -i <ip> -O opengrp2
```

Odsyłacze pokrewne:

“Komenda psconf” na stronie 163

Zarządzanie strategiami zarządzania poprawkami

Do konfigurowania strategii zarządzania poprawkami służy komenda **pmconf**.

Strategie zarządzania poprawkami dostarczają informacji, takich jak adres IP serwera TNC i przedział czasu, wymaganych do zainicjowania aktualizacji SUMA.

Aby zarządzać strategią zarządzania poprawkami, wprowadź następującą komendę:

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

Na przykład:

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

Uwaga: Porty pmport i tncserver muszą być różne.

Odsyłacze pokrewne:

“Komenda pmconf” na stronie 159

Importowanie certyfikatów połączenia sieci zaufanej

W sekcji opisano procedurę importowania certyfikatu w celu bezpiecznego przesyłania danych w sieci.

Demony zaufanej sieci (TNC) komunikują się przez zaszyfrowane kanały zestawione przy użyciu protokołu TLS (Transport Layer Security lub SSL (Secure Sockets Layer). Demon ten zapewnia, że dane i komendy, które są przesyłane w sieci, są uwierzytelniane i bezpieczne. Każdy system ma własny klucz i certyfikat, które są generowane po uruchomieniu komendy inicjowania komponentów. Ten proces jest przezroczysty dla administratora i wymaga mniej zaangażowanie z jego strony. Gdy klient jest weryfikowany po raz pierwszy, jego certyfikat jest importowany do bazy danych serwera. Certyfikat jest początkowo oznaczony jako niezaufany, a administrator może użyć komendy **psconf**, aby wyświetlać certyfikaty i oznaczyć je jako zaufane, wprowadzając następującą komendę:

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

Jeśli administrator chce użyć innego klucza i certyfikatu, komenda **psconf** pozwala również na zaimportowanie klucza i certyfikatu.

Aby zaimportować certyfikat z serwera, wprowadź następującą komendę:

```
psconf import -S -k <nazwa pliku
klucza> -f <nazwa pliku>
```

Aby zaimportować certyfikat z klienta, wprowadź następującą komendę:

```
psconf import -C -k <nazwa pliku
klucza> -f <nazwa pliku>
```

Odsyłacze pokrewne:

“Komenda psconf” na stronie 163

Raportowanie dla serwera TNC

Serwer zaufanej sieci (TNC) obsługuje zarówno format CSV (wartości rozdzielone przecinkami), jak i tekstowy format wyjściowy dla raportów dotyczących zagrożeń CVE, zaleceń IBM Security Advisory, strategii serwera TNC, poprawek bezpieczeństwa dla klienta TNC i raportów poprawek tymczasowych.

Raport CVE wyświetla wszystkie często spotykane zagrożenia i narażenia dla zarejestrowanych pakietów serwisowych. Aby wyświetlić wyniki tego raportu, wpisz następującą komendę:

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

Raport IBM Security Advisory wyświetla znane zagrożenia bezpieczeństwa dla zainstalowanego oprogramowania IBM. Aby wyświetlić wyniki tego raportu, wpisz następującą komendę:

```
psconf report -A <nazwa_zalecenia>
```

Raport strategii serwera TNC wyświetla strategie bezpieczeństwa, które są wymuszane na serwerze TNC. Aby wyświetlić wyniki tego raportu, wpisz następującą komendę:

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

Raport poprawek klienta TNC wyświetla zainstalowane i brakujące poprawki tymczasowe dla klienta TNC. Aby wyświetlić wyniki tego raportu, wpisz następującą komendę:

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

Można również uruchomić raport, który generuje listę zarejestrowanych pakietów serwisowych oraz pokrewnych raportów APAR i poprawek tymczasowych. Aby wyświetlić wyniki tego raportu, wpisz następującą komendę:

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

Aby wyświetlić listę zarejestrowanych pakietów Open Source, wprowadź następującą komendę report:

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

Odsyłacze pokrewne:

"Komenda psconf" na stronie 163

Rozwiązywanie problemów z zaufaną siecią i zarządzaniem poprawkami

Poniżej przedstawiono możliwe przyczyny problemów z zaufaną siecią (TNC) i mechanizmami zarządzania poprawkami oraz czynności umożliwiające ich rozwiązanie.

Aby rozwiązać problemy dotyczące TNC i systemu zarządzania poprawkami, sprawdź ustawienia konfiguracyjne, które są wymienione w poniższej tabeli.

Tabela 13. Rozwiązywanie problemów dotyczących ustawień konfiguracyjnych TNC i systemu zarządzania poprawkami

Problem	Rozwiązanie
Serwer TNC nie uruchamia się lub nie odpowiada	Wykonaj następującą procedurę: 1. Sprawdź, czy demon serwera TNC działa, wprowadzając komendę: `ps –eaf | grep tnccsd` 2. Jeśli nie jest on uruchomiony, usuń plik /var/tnc/.tncsock. 3. Zrestartuj serwer. Jeśli to nie rozwiąże problemu, sprawdź czy w pliku konfiguracyjnym /etc/tnccs.conf na serwerze TNC znajduje się pozycja component = SERVER.
Serwer zarządzania poprawkami dla TNC nie uruchamia się lub nie odpowiada	• Sprawdź, czy demon serwera zarządzania poprawkami TNC działa, wprowadzając komendę: `ps –eaf | grep tncpmd` • Sprawdź czy w pliku konfiguracyjnym /etc/tnccs.conf na serwerze zarządzania poprawkami TNC znajduje się pozycja component = TNCPM.
Klient TNC nie uruchamia się lub nie odpowiada	• Sprawdź, czy demon klienta TNC działa, wprowadzając komendę: `ps –eaf | grep tnccsd` • Sprawdź czy w pliku konfiguracyjnym /etc/tnccs.conf na kliencie TNC znajduje się pozycja component = CLIENT.
Odsyłacz IP dla TNC referrer nie jest uruchomiony na serwerze serwer VIOS (VIOS)	• Sprawdź, czy demon odsyłacza IP dla TNC działa, wprowadzając komendę: `ps –eaf | grep tnccsd` • Sprawdź czy w pliku konfiguracyjnym /etc/tnccs.conf na serwerze VIOS znajduje się pozycja component = IPREF.
Nie można skonfigurować systemu jednocześnie jako serwer i klient TNC	Serwer TNC i klient nie może działać jednocześnie w tym samym systemie.
Demony są uruchomione, ale weryfikacja nie jest wykonywana.	Włącz rejestrowanie komunikatów dla demonów. Ustaw poziom rejestrowania level=info w pliku /etc/tnccs.conf. Można przeanalizować komunikaty zarejestrowane w dzienniku.

graficzny interfejs użytkownika produktu PowerSC

W tej sekcji opisano graficzny interfejs użytkownika produktu PowerSC firmy IBM. Podano tu między innymi informacje na temat instalowania, konserwowania i używania tego interfejsu.

Interfejs GUI produktu PowerSC firmy IBM zwiększa użyteczność produktu PowerSC Standard Edition, udostępniając alternatywę dla interakcji za pomocą wiersza komend i plików dzienników. Interfejs GUI produktu PowerSC udostępnia scentralizowaną konsolę zarządzania na potrzeby wirtualizacji punktów końcowych i ich statusu, stosowania, wycofywania i sprawdzania poziomów zgodności, grupowania systemów na potrzeby stosowania działań dotyczących poziomów zgodności, a także wyświetlania i dostosowywania profili konfiguracyjnych zgodności.

Interfejs GUI produktu PowerSC zawiera także funkcję monitorowania integralności plików (File Integrity Monitoring — FIM). Funkcja FIM obejmuje zgodność w czasie rzeczywistym (Real Time Compliance — RTC) i zaufane wykonywanie (Trusted Execution — TE). Za pomocą interfejsu GUI produktu PowerSC można skonfigurować funkcje RTC i TE, a także przeglądać zdarzenia w czasie rzeczywistym. Ponadto interfejs GUI produktu PowerSC udostępnia rozbudowane możliwości edycji profili i raportowania.

Pojęcia dotyczące interfejsu GUI produktu PowerSC

Przed użyciem interfejsu GUI produktu PowerSC należy poznać ogólne pojęcia dotyczące zabezpieczeń i wykrywania punktów końcowych.

interfejs GUI produktu PowerSC — bezpieczeństwo

Interfejs GUI produktu PowerSC zapewnia bezpieczeństwo przy użyciu dwukierunkowej komunikacji HTTPS między serwerem interfejsu GUI produktu PowerSC i agentami interfejsu GUI produktu PowerSC w każdym z punktów końcowych systemu AIX.

Proces uzgadniania TLS korzysta z certyfikatów, które są dostępne na serwerze interfejsu GUI produktu PowerSC i na agentach interfejsu GUI produktu PowerSC. Proces uzgadniania TLS obsługuje pojedyncze uwierzytelnianie w obu kierunkach, ponieważ agent interfejsu GUI produktu PowerSC lub serwer interfejsu GUI produktu PowerSC może inicjować komunikację. Agent tworzy wartość jednorazową (liczbę losową), która jest wysyłana do serwera interfejsu GUI produktu PowerSC przy pierwszym połączeniu. Następnie serwer interfejsu GUI produktu PowerSC dołącza tę wartość jednorazową do każdej komendy wysyłanej do tego agenta. Ta wartość jednorazowa stanowi kolejną warstwę potwierdzania dla agenta punktu końcowego, że uruchamia on komendę, która pochodzi z autentycznego serwera interfejsu GUI produktu PowerSC. Punkt końcowy musi upewnić się, że źródło wywołania usługi WWW jest zaufane. Początkowe uzgadnianie i wartość jednorazowa zapewniają relację zaufania.

Cała komunikacja między agentami interfejsu GUI produktu PowerSC i serwerem interfejsu GUI produktu PowerSC jest szyfrowana przy użyciu protokołów i zestawów algorytmów szyfrowania, które są spójne z wymaganiami w zakresie bezpieczeństwa chronionych systemów. Obecnie poziomem protokołu jest TLS 1.2. Serwer interfejsu GUI produktu PowerSC komunikuje się ze wszystkimi agentami interfejsu GUI produktu PowerSC i ze wszystkimi użytkownikami interfejsu GUI produktu PowerSC. Dlatego serwer interfejsu GUI produktu PowerSC musi mieć certyfikat zaufany przez wszystkie połączenia od przeglądarek WWW użytkowników. Mogą to być na przykład certyfikaty pochodzące od powszechnie znanych ośrodków, takich jak Verisign lub pochodzące od wewnętrznie zaufanego ośrodka certyfikacji.

Podczas instalacji serwer interfejsu GUI produktu PowerSC tworzy certyfikat samopodpisany na własny użytek. Certyfikat ten można używać bezterminowo, ale jest on przeznaczony do użytku tymczasowego i można go zastąpić udostępnionym przez użytkownika szeroko uznanym certyfikatem. Podczas instalacji serwera interfejsu GUI produktu PowerSC także tworzony jest certyfikat podpisujący, który jest używany do podpisywania wszystkich certyfikatów punktów końcowych.

Proces instalowania automatycznie tworzy plik zaufanych certyfikatów dla każdego punktu końcowego. Plik zaufanych certyfikatów jest taki sam dla każdego punktu końcowego i musi zostać skopiowany z serwera interfejsu GUI produktu PowerSC do każdego punktu końcowego. Taka kombinacja certyfikatów na serwerze interfejsu GUI produktu PowerSC i w punktach końcowych zapewnia wysoki poziom zabezpieczenia komunikacji.

Szersze mechanizmy zabezpieczeń udostępniają grupy systemu UNIX. Każdy użytkownik, taki jak użytkownik LDAP lub użytkownik lokalny, który jest definiowany przez system operacyjny, musi być członkiem określonej grupy systemu UNIX, aby zalogować się w interfejsie GUI produktu PowerSC. Administrator może ustawić lub zmienić to przypisanie do grupy za pomocą komendy **pscuiserverctl**.

Dostęp użytkownika po zalogowaniu może być nadal ograniczony do trybu tylko do przeglądania. Można użyć funkcji uprawnień użytkownika do wykonywania działań dla punktów końcowych, które są kontrolowane przez przypisanie do grupy systemu UNIX. Aby wykonać jakiekolwiek działania, użytkownik musi być członkiem grupy UNIX, która ma uprawnienia do zarządzania punktem końcowym. Więcej informacji na ten temat zawiera sekcja Określanie, które grupy mają dostęp.

Domyślnie każdy użytkownik, który jest członkiem grupy zabezpieczeń, może zarządzać każdym punktem końcowym widocznym w interfejsie GUI produktu PowerSC. Administrator funkcji PowerSC może ograniczyć dostęp użytkownika na poziomie indywidualnego punktu końcowego, używając komendy **setGroups.sh**.

Istnieją różne komendy służące do konfigurowania, które mogą być wykonywane tylko przez administratora, na przykład komendy do zmiany globalnych ustawień poczty elektronicznej lub tworzenia nowego profilu. Uprawnienia użytkownika administracyjnego ustawia się za pomocą grup systemu UNIX i można je konfigurować za pomocą komendy **pscuiserverctl**.

Zapełnianie treści dotyczącej punktu końcowego na stronie zgodności

Serwer interfejsu GUI produktu PowerSC i agent interfejsu GUI produktu PowerSC komunikują się z punktem końcowym w celu wykrycia poziomu zgodności.

Agent po uruchomieniu i sporadycznie do osiągnięcia powodzenia próbuje zainicjować połączenie z serwerem interfejsu GUI produktu PowerSC. Po nawiązaniu połączenia jeden raz wykonywane jest uzgadnianie zabezpieczeń między agentem i serwerem. Gdy uzgodnienie zabezpieczeń od agenta do serwera zostanie po raz pierwszy pomyślnie wynegocjowane, serwer tworzy element domeny o unikalnym identyfikatorze (UID) na potrzeby wewnętrznej reprezentacji punktu końcowego i przekazuje ten identyfikator z powrotem do punktu końcowego. Ten identyfikator UID jest następnie dołączany podczas całej komunikacji od agenta do serwera. To działanie powoduje zakończenie procesu wykrywania. Serwer interfejsu GUI produktu PowerSC i punkt końcowy mogą bezpiecznie komunikować się ze sobą w dowolnym kierunku.

Gdy uzgadnianie w ramach początkowego wykrywania zostanie zakończone lub agent interfejsu GUI produktu PowerSC zostanie zrestartowany, agent interfejsu GUI produktu PowerSC próbuje określić informacje o bieżącym statusie zgodności dla punktu końcowego i aktualizuje serwer interfejsu GUI produktu PowerSC. Istnienie punktu końcowego i informacje o bieżącej zgodności są używane do zapełnienia strony statusu zgodności interfejsu GUI produktu PowerSC. Jeśli nie można określić żadnych informacji o statusie zgodności, pozycja nie będzie dostępna na stronie statusu zgodności.

Serwer interfejsu GUI produktu PowerSC zawiera reprezentację wszystkich znanych punktów końcowych, które są automatycznie tworzone w wyniku początkowego połączenia i komunikacji między agentem i serwerem. Gdy agenty punktów końcowych śledzą zmiany w statusie zgodności punktów końcowych, zmiany te są przekazywane do serwera i na nim zapisywane. Wszystkie interakcje użytkownika od interfejsu GUI produktu PowerSC z punktem końcowym są wykonywane za pomocą serwera interfejsu GUI produktu PowerSC. Interfejs użytkownika nie współpracuje bezpośrednio z żadnym punktem końcowym ani agentem punktów końcowych.

Instalowanie interfejsu GUI produktu PowerSC

Komponenty agentów interfejsu GUI produktu PowerSC i serwera interfejsu GUI produktu PowerSC są instalowane podczas instalowania produktu PowerSC Standard Edition. Każdy z nich jest instalowany z zestawów plików installp.

Agent interfejsu GUI produktu PowerSC

Agent interfejsu GUI produktu PowerSC instaluje się na każdym punkcie końcowym systemu AIX. Agent interfejs GUI produktu PowerSC śledzi aktywność w punkcie końcowym i udostępnia informacje na ten temat serwerowi interfejsu GUI produktu PowerSC.

Ponadto agent interfejsu GUI produktu PowerSC uruchamia komendy, które są wyzwalane z interfejsu GUI produktu PowerSC. Cała komunikacja między agentami interfejsu GUI produktu PowerSC i serwerem interfejsu GUI produktu PowerSC jest szyfrowana.

Komenda installp umożliwia zainstalowanie podstawowego produktu PowerSC Standard Edition i agenta interfejsu GUI produktu PowerSC. Do zainstalowania agenta interfejsu GUI produktu PowerSC używany jest zestaw plików installp o nazwie powerscStd.uiAgent.rte. Poniższy przykład przedstawia komendę installp, która jest uruchamiana w każdym punkcie końcowym:

Uwaga: W poniższym przykładzie obrazy instalatora są rozpakowywane w katalogu /tmp/inst.images/.

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

Serwer interfejsu GUI produktu PowerSC

Serwer interfejsu GUI produktu PowerSC może działać w dowolnym systemie AIX. Zalecane jest utworzenie dedykowanej partycji LPAR w systemie AIX, na której serwer interfejsu GUI produktu PowerSC zostanie zainstalowany i uruchomiony.

Komenda **installp** umożliwia zainstalowanie podstawowego produktu PowerSC Standard Edition i serwera interfejsu GUI produktu PowerSC. Do zainstalowania serwera interfejsu GUI produktu PowerSC używany jest zestaw plików **installp** o nazwie powerscStd.uiServer.rte. Poniższy przykład przedstawia komendę **installp**, która jest uruchamiana w punkcie końcowym:

Uwaga: W poniższym przykładzie obrazy instalatora są rozpakowywane w katalogu /tmp/inst.images/.

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

Wymagania dotyczące interfejsu GUI produktu PowerSC

W tym miejscu podano informacje o wymaganiach programowych dla interfejsu GUI produktu PowerSC.

Sprzętowe

- Komponenty serwera interfejsu GUI produktu PowerSC powinny zostać zainstalowane na oddzielnej partycji LPAR lub na maszynie wirtualnej, na której działa system AIX 7.1 lub nowszy.
- Komponenty agenta interfejsu GUI produktu PowerSC muszą zostać zainstalowane w każdym punkcie końcowym systemu AIX.

Programowe

- Serwer interfejsu GUI produktu PowerSC wymaga systemu AIX 7.1 lub nowszego.
- Serwer interfejsu GUI produktu PowerSC wymaga uruchomionego demona sendmail.
- Zestaw plików bos.loc.utf.<LANG> musi być zainstalowany, aby interfejs GUI produktu PowerSC poprawnie wyświetlał opisy reguł profilu w językach innych niż angielski.

Dystrybuowanie certyfikatu bezpieczeństwa magazynu zaufanych certyfikatów do punktów końcowych

Administratorzy systemu muszą wdrożyć certyfikat bezpieczeństwa magazynu zaufanych certyfikatów we wszystkich punktach końcowych.

Podczas instalacji tworzony jest plik zaufanych certyfikatów. Może on być używany przez wszystkie punkty końcowe. Plik ten ma nazwę endpointTruststore.jks i znajduje się w katalogu /etc/security/powersc/uiServer/.

Po instalacji należy umieścić plik endpointtruststore.jks w każdym punkcie końcowym dla agenta interfejsu GUI produktu PowerSC w tym punkcie końcowym, aby skontaktować się z serwerem interfejsu GUI produktu PowerSC i zainicjować proces, w wyniku którego w punkcie końcowym tworzony jest magazyn kluczy.

Plik zaufanych certyfikatów możesz dystrybuować, używając jednej z następujących metod:

- Ręcznie skopiuj plik endpointTruststore.jks do każdego punktu końcowego.
- Jeśli w środowisku używany jest PowerVC (lub inny menedżer wirtualizacji), plik endpointTruststore.jks można umieścić w obrazie PowerVC. Gdy obraz PowerVC jest wdrażany w punkcie końcowym, dołączany jest zarówno agent interfejsu GUI produktu PowerSC, jak i plik zaufanych certyfikatów.

Gdy plik endpointTruststore.jks jest wdrażany za pomocą jednej z tych metod i punkt końcowy zostanie uruchomiony, agent interfejsu GUI produktu PowerSC używa pliku zaufanych certyfikatów do określenia miejsca, w którym uruchomiony jest serwer interfejsu GUI produktu PowerSC. Następnie agent interfejsu GUI produktu PowerSC wysyła komunikat do serwera interfejsu GUI produktu PowerSC z żądaniem dołączenia do listy dostępnych i monitorowanych punktów końcowych.

Ręczne kopiowanie pliku zaufanych certyfikatów do punktów końcowych

Administratorzy systemu muszą ręcznie skopiować plik zaufanych certyfikatów do każdego punktu końcowego istniejącego w środowisku.

Plik zaufanych certyfikatów musi być także skopiowany do każdego nowego punktu końcowego, który jest dodawany.

Uwaga: Jeśli używany jest menedżer wirtualizacji, taki jak PowerVC, plik zaufanych certyfikatów można skopiować do nowego punktu końcowego, tworząc obraz zawierający agenta interfejsu GUI produktu PowerSC i plik zaufanych certyfikatów. Patrz sekcja “Kopiowanie pliku zaufanych certyfikatów do punktów końcowych za pomocą menedżera wirtualizacji”.

1. Aby skopiować plik magazynu zaufanych certyfikatów /etc/security/powersc/uiServer/endpointTruststore.jks punktu końcowego do pliku /etc/security/powersc/uiAgent/endpointTruststore.jks w każdym punkcie końcowym, uruchom następującą komendę **scp**:

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

2. Aby zrestartować agenty punktów końcowych po instalacji certyfikatu bezpieczeństwa, w punkcie końcowym uruchom następujące komendy:

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

3. Powtórz kroki 1 i 2 dla każdego istniejącego punktu końcowego i dla każdego nowego punktu końcowego (jeśli nie jest używany menedżer wirtualizacji danych).

Kopiowanie pliku zaufanych certyfikatów do punktów końcowych za pomocą menedżera wirtualizacji

Administratorzy systemu mogą używać menedżerów wirtualizacji, takich jak PowerVC, aby skopiować plik zaufanych certyfikatów do wszystkich nowych punktów końcowych, używając obrazu, który zawiera agenta PowerSC i plik zaufanych certyfikatów.

1. Skopiuj plik zaufanych certyfikatów /etc/security/powersc/uiServer/endpointTruststore.jks punktu końcowego do obrazu PowerVC.
2. Wdróż obraz PowerVC do każdego nowego punktu końcowego, który został dodany do systemu.

Konfigurowanie kont użytkowników

Domyślnie każdy użytkownik, bez względu na to, czy jest to użytkownik LDAP, czy też użytkownik lokalny, który jest definiowany przez system operacyjny, musi być członkiem grupy zabezpieczeń, aby zalogować się w interfejsie GUI produktu PowerSC.

Administrator może zmienić to wymagane przypisanie do grupy za pomocą komendy **pscuiserverctl**. Po zalogowaniu się do interfejsu GUI produktu PowerSC użytkownik może wyświetlić status punktów końcowych tylko wtedy, gdy jego konto użytkownika należy do grupy systemu UNIX, która ma uprawnienia do zarządzania tymi punktami końcowymi. Administrator może zmienić ustawienia konta użytkownika na poziomie indywidualnego punktu końcowego, używając komendy **setGroups.sh**.

Należy wziąć pod uwagę następujące kwestie:

- Między punktami końcowymi i grupami systemu AIX istnieje relacja wiele-do-wielu.
  - Jedna grupa systemu AIX może być powiązana z wieloma punktami końcowymi.
  - Jeden punkt końcowy może być powiązany z wieloma grupami systemu AIX.
- Gdy użytkownik zaloguje się do interfejsu GUI produktu PowerSC, powiązania grup są używane do określenia, czy ten użytkownik może uruchamiać komendy w konkretnych punktach końcowych, czy też może jedynie wyświetlać ich status.
  - Aby uruchamiać komendy dla konkretnego punktu końcowego za pomocą interfejsu GUI produktu PowerSC, użytkownik musi być powiązany z jedną spośród grup powiązanych z danym punktem końcowym.
  - Przynależność użytkownika do grup jest porównywana z zestawem grup powiązanych z każdym punktem końcowym. Jeśli przynależność użytkownika do grup jest zgodna z grupami powiązanymi z każdym punktem końcowym, użytkownik może uruchamiać komendy, takie jak **Zastosuj profile**, **Cofnij** i **Sprawdź** dla tego punktu końcowego. Jeśli przynależność użytkownika do grup nie jest zgodna z żadnymi grupami powiązanymi z każdym punktem końcowym, użytkownik może tylko wyświetlić status danego punktu końcowego.

Następujące skrypty powłoki są dostępne na serwerze interfejsu GUI produktu PowerSC w katalogu /opt/powersc/uiServer/bin/.

Tabela 14. Skrypty powłoki grupy

Skrypt powłoki	Opis
pscuiserverctl	Określa grupę logowania w systemie AIX (UNIX), do której musi należeć użytkownik, aby zalogować się do interfejsu GUI produktu PowerSC. Użytkownik musi być członkiem tylko jednej z takich grup.
setGroups.sh	Określa jedną lub więcej grup w systemie AIX, do których musi należeć użytkownik, aby uruchamiać komendy w konkretnych punktach końcowych.

Uruchamianie komend i skryptów konfigurowania grup

Administratorzy systemu muszą uruchomić komendę **pscuiserverctl** i skrypt **setGroups**, aby określać, które grupy systemów operacyjnych mogą logować się w interfejsie GUI produktu PowerSC, wykonywać funkcje administratora i wykonywać komendy w konkretnych punktach końcowych.

1. Na serwerze interfejsu GUI produktu PowerSC przejdź do katalogu /opt/powersc/uiServer/bin/.
2. Uruchom następującą komendę, aby określić grupę w systemie AIX, do której musi należeć użytkownik, aby zalogować się do interfejsu GUI produktu PowerSC. Podana grupa jest zapisywana w pliku /etc/security/powersc/uiServer/uiServer.conf.

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

Wskazówka: Przed uruchomieniem tej komendy, można użyć komendy **groups** *nazwa_użytkownika*, aby wyświetlić grupy, do których należy użytkownik.

3. Uruchom następującą komendę, aby określić grupy w systemie UNIX, które mają uprawnienia do wykonywania funkcji administratora za pomocą interfejsu GUI produktu PowerSC.

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

4. Uruchom następującą komendę, aby określić grupy w systemie AIX, do których musi należeć użytkownik, aby uruchamiać komendy w konkretnych punktach końcowych. Należy podać pełne nazwy hostów punktów końcowych. Podane grupy są zapisywane w pliku /etc/security/powersc/uiServer/groups.txt.

   ```
   ./setGroups.sh nazwa_grupy "lista rozdzielonych przecinkami nazw hostów punktów końcowych"
   ```

   Uwaga: Podczas wyszukiwania punktów końcowych w ograniczony sposób obsługiwane są znaki wieloznaczne. Na przykład poprawne są następujące specyfikacje określające wszystkie punkty końcowe, których nazwa rozpoczyna się łańcuchem "Boston_" lub kończy się łańcuchem ".rs.com":

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

   Wskazówka: W tej komendzie gwiazdka (*) jest jedynym obsługiwanym znakiem wieloznacznym. Można jej używać tylko na początku i na końcu łańcucha.

Używanie interfejsu GUI produktu PowerSC

Interfejs GUI produktu PowerSC umożliwia sprawdzanie punktów końcowych wykrytych w systemie, tworzenie niestandardowych grup, tworzenie niestandardowych profili, kopiowanie niestandardowych profili do punktów końcowych i stosowanie profili. Ponadto można sprawdzić komunikację między punktami końcowymi i serwerem interfejsu GUI produktu PowerSC, a także zatrzymać komunikację między punktem końcowym i serwerem interfejsu GUI produktu PowerSC.

Strona główna interfejsu GUI produktu PowerSC zawiera następujące sekcje:

- Pasek **Grupy**: zawiera grupy zdefiniowane dla środowiska. Grupy są kolekcjami punktów końcowych, które są grupowane ze względu na podobieństwo do siebie. Grupa **Wszystkie systemy** jest tworzona automatycznie, gdy w środowisku wykrywane są punkty końcowe. Użytkownik może tworzyć grupy niestandardowe. Na przykład można utworzyć grupę punktów końcowych, których wspólnym elementem jest HIPAA.
- Strona **Zgodność** zawiera trzy sekcje:
  - Na górnym panelu wyświetlane są informacje statystyczne dotyczące grupy wybranej na pasku **Grupy**. Te informacje statystyczne przedstawiają wyniki ostatnich poziomów zgodności zastosowanych do punktów końcowych w wybranej grupie. Dla wybranej grupy można wyświetlić procent systemów poprawnych i z niepowodzeniem, łączną liczbę sprawdzonych reguł i określone reguły, które się nie powiodły.
  - Panel centralny stanowi pasek zadań, którego można używać do wykonywania działań na jednym lub wielu punktach końcowych. Można zastosować, cofnąć i sprawdzić poziom zgodności.
  - Na panelu dolnym wyświetlana jest tabela zawierająca wszystkie punkty końcowe lub grupę punktów końcowych dostępnych w środowisku. Ta tabela zawiera następujące informacje dla każdego punktu końcowego:
    - Nazwa systemu
    - Typ reguły zgodności
    - Data i godzina zastosowania poziomu zgodności do punktu końcowego
    - Data i godzina sprawdzenia poziomu zgodności w punkcie końcowym
    - Status poziomu zgodności
    - Liczba reguł w punkcie końcowym zakończonych niepowodzeniem
    - Liczba reguł w punkcie końcowym zakończonych powodzeniem podczas sprawdzania poziomu zgodności
- Strona **Bezpieczeństwo** zawiera dwie sekcje:
  - Na górnym panelu w czasie rzeczywistym wyświetlane są informacje o bezpieczeństwie dotyczące grupy punktów końcowych wybranej na pasku **Grupy**. Dla wybranej grupy można sprawdzić łączną liczbę zdarzeń

zgodności w czasie rzeczywistym (RTC – Real Time Compliance), łączną liczbę zdarzeń zaufanego wykonywania (Trusted Execution – TE), procent punktów końcowych, które mają aktualne poprawki TNC, procent punktów końcowych, dla których zainstalowano zaufane uruchamianie, liczbę punktów końcowych, które mają zainstalowany zaufany firewall i procent punktów końcowych, które mają zainstalowane zaufane rejestrowanie.

  - Na dolnym panelu wyświetlana jest tabela, która zawiera punkty końcowe systemu znajdujące się w grupie. Ta tabela zawiera następujące informacje dla każdego punktu końcowego:
    - Nazwa punktu końcowego systemu
    - Indykatory zdarzeń integralności plików
    - Status aktywacji funkcji RTC
    - Status aktywacji funkcji TE
    - Status aktualizacji poprawek TNC
- Strona **Raporty** zawiera raporty dotyczące zgodności i integralności plików. Dostępne są raporty ogólne i szczegółowe.
- Strona **Edytor profilu** zawiera trzy sekcje:
  - Na górnym panelu znajduje się menu rozwijane, które zawiera listę dostępnych profili wbudowanych i niestandardowych.
  - Panel centralny stanowi pasek zadań, którego można używać do usuwania profili, tworzenia nowych profili i kopiowania profili do punktów końcowych, które należą do grupy.
  - Na panelu dolnym wyświetlana jest tabela zawierająca wszystkie reguły zawarte w wybranym profilu. Dla każdej reguły wyświetlane są następujące informacje:
    - Nazwa reguły zgodności
    - Typ reguły zgodności
    - Opis reguły

Określanie języka interfejsu GUI produktu PowerSC

Interfejs GUI produktu PowerSC można wyświetlać w różnych językach.

Aby wybrać język interfejsu GUI produktu PowerSC, należy kliknąć ikonę **Język i ustawienia** na pasku menu strony głównej. Bieżący język używany do wyświetlania interfejsu jest wyświetlany w menu. Aby zmienić język, należy kliknąć powiązaną ikonę. Z listy dostępnych języków należy wybrać język dla danej sesji.

Nawigowanie po interfejsie GUI produktu PowerSC

Za pomocą interfejsu GUI produktu PowerSC można konfigurować komunikację między punktami końcowymi i serwerem oraz administrować tą komunikacją, organizować i grupować punkty końcowe, monitorować i stosować wbudowane i niestandardowe poziomy zgodności i profile, monitorować i konfigurować zabezpieczenia punktów końcowych, a także generować i dystrybuować raporty w określonych odstępach czasu.

1. Otwórz interfejs GUI produktu PowerSC. Interfejs GUI produktu PowerSC wyświetli stronę główną.
2. Aby administrować komunikacją między punktami końcowymi i serwerem, kliknij ikonę **Język i ustawienia** na pasku menu strony głównej. Kliknij ikonę **Administrator punktu końcowego**, aby sprawdzić lub zatrzymać komunikację między punktami końcowymi i serwerem interfejsu GUI produktu PowerSC. Więcej informacji na ten temat zawiera sekcja “Administrowanie komunikacją między punktami końcowymi i serwerem” na stronie 140.
3. Kliknij poziomy wielokropek na panelu nawigacyjnym stron Zgodność i Bezpieczeństwo, aby otworzyć Edytor grupy. Edytor grupy umożliwia tworzenie niestandardowych grup punktów końcowych. Więcej informacji na ten temat zawiera sekcja “Tworzenie grup niestandardowych” na stronie 142.
4. Aby utworzyć profile niestandardowe i skopiować te profile do punktów końcowych, kliknij kartę **Edytor profilu**. Więcej informacji na ten temat zawiera sekcja “Praca z profilami zgodności” na stronie 143.
5. Aby monitorować i zastosować wbudowane i niestandardowe poziomy zgodności i profile, kliknij kartę **Zgodność**. Więcej informacji na ten temat zawiera sekcja Stosowanie poziomów zgodności i profili.

6. Aby monitorować i konfigurować bezpieczeństwo punktów końcowych, kliknij kartę **Bezpieczeństwo**. Więcej informacji na ten temat zawiera sekcja Monitorowanie bezpieczeństwa punktów końcowych.
7. Aby generować raporty i dystrybuować je na żądanie lub zgodnie z harmonogramem, kliknij kartę **Raporty**. Więcej informacji na ten temat zawiera sekcja Praca z raportami.

Administrowanie komunikacją między punktami końcowymi i serwerem

Na stronie **Administrator punktu końcowego** można sprawdzić lub zatrzymać komunikację między punktami końcowymi i serwerem interfejsu GUI produktu PowerSC. Można również sprawdzić i wygenerować żądania magazynu kluczy.

Weryfikowanie komunikacji między punktami końcowymi i serwerem

Istnieje możliwość zweryfikowania komunikacji między wykrytymi punktami końcowymi i serwerem interfejsu GUI produktu PowerSC.

1. Kliknij ikonę **Język i ustawienia** na pasku menu strony głównej. Kliknij opcję **Administrator punktu końcowego**. Zostanie otwarta strona administrowania punktem końcowym.
2. Na pasku **Grupy** wybierz grupę zawierającą punkty końcowe, które chcesz zweryfikować. Punkty końcowe dla tej grupy zostaną wyświetlone w tabeli punktów końcowych.
3. Wszystkie punkty końcowe systemu dla wybranej grupy są wyświetlane w tabeli zgodności. Wyświetlane punkty końcowe można filtrować za pomocą pola **Filtruj wg tekstu**. W tym polu wpisz tekst, który ma zostać użyty do filtrowania, i naciśnij klawisz Enter. Lista punktów końcowych z wybranej grupy jest dynamicznie filtrowana w celu wyświetlenia tylko tych wierszy, które zawierają wprowadzony tekst.
4. Aby odświeżyć wyświetlane informacje o statusie, kliknij opcję **Odśwież tabelę**.
5. Zaznacz odpowiednie pole wyboru dla każdego punktu końcowego, który chcesz zweryfikować.
6. Kliknij ikonę **Zweryfikuj**.
7. W kolumnach **Zweryfikowano** i **Diagnoza łączności** zostanie wyświetlony komunikat potwierdzenia dotyczący poprawnego połączenia.

Usuwanie punktów końcowych z monitorowania w interfejsie GUI produktu PowerSC

Gdy punkt końcowy zostanie wykryty, jest on monitorowany w sposób ciągły. Jeśli punkt końcowy został usunięty ze środowiska, należy go także usunąć z serwera interfejsu GUI produktu PowerSC.

Aby usunąć punkty końcowe z monitorowania w interfejsie GUI produktu PowerSC, wykonaj następujące kroki:

1. Kliknij ikonę **Język i ustawienia** na pasku menu strony głównej. Kliknij opcję **Administrator punktu końcowego**. Zostanie otwarta strona administrowania punktem końcowym.
2. Na pasku **Grupy** wybierz grupę zawierającą punkty końcowe, które chcesz usunąć. Punkty końcowe dla tej grupy zostaną wyświetlone w tabeli punktów końcowych.
3. Wszystkie punkty końcowe systemu dla wybranej grupy są wyświetlane w tabeli zgodności. Wyświetlane punkty końcowe można filtrować za pomocą pola **Filtruj wg tekstu**. W tym polu wpisz tekst, który ma zostać użyty do filtrowania, i naciśnij klawisz Enter. Lista punktów końcowych z wybranej grupy jest dynamicznie filtrowana w celu wyświetlenia tylko tych wierszy, które zawierają wprowadzony tekst.
4. Aby odświeżyć wyświetlane informacje o statusie, kliknij opcję **Odśwież tabelę**.
5. Zaznacz odpowiednie pole wyboru dla każdego punktu końcowego, dla którego chcesz zatrzymać monitorowanie.
6. Kliknij ikonę **Usuń**.
7. W kolumnach **Datownik weryfikacji** i **Diagnoza łączności** zostanie wyświetlony komunikat potwierdzenia usunięcia punktu końcowego.

Weryfikowanie żądań magazynu kluczy i generowanie magazynu kluczy

Dla każdego punktu końcowego należy zweryfikować, czy żądanie magazynu kluczy jest poprawne, a jeśli jest poprawne, można wy generować magazyn kluczy dla tego punktu końcowego.

Gdy punkt końcowy zostanie uruchomiony po raz pierwszy, agent interfejsu GUI produktu PowerSC używa pliku zaufanych certyfikatów do określenia miejsca, w którym uruchomiony jest serwer interfejsu GUI produktu PowerSC. Następnie agent interfejsu GUI produktu PowerSC wysyła komunikat do serwera interfejsu GUI produktu PowerSC z żądaniem dołączenia do listy dostępnych i monitorowanych punktów końcowych.

Za pomocą strony **Administrator punktu końcowego Żądania magazynu kluczy** można zweryfikować, czy żądanie magazynu kluczy jest poprawne, a jeśli jest poprawne, można wygenerować magazyn kluczy dla tego punktu końcowego.

1. Kliknij ikonę **Język i ustawienia** na pasku menu strony głównej. Kliknij opcję **Administrator punktu końcowego**. Zostanie otwarta strona administrowania **Punkt końcowy - Wszystkie systemy**.
2. Każdy znany punkt końcowy jest wyświetlany w kolumnie **Nazwa systemu**. Kliknij opcję **Żądania magazynu kluczy**, aby sprawdzić, czy istnieją żądania magazynu kluczy w toku. Zostanie otwarta strona **Administrator punktu końcowego Żądania magazynu kluczy**.
3. Żądania magazynu kluczy dla wszystkich nowych lub dodanych serwerów są wyświetlane w kolumnie **Nazwa hosta**. Po potwierdzeniu, że magazynu kluczy ma zostać rozszerzony do punktu końcowego, zaznacz pole wyboru tego punktu końcowego i kliknij opcję **Zweryfikuj**.
4. Weryfikacja jest wykonywana przez PowerVC. Podaj ID użytkownika i hasło w oknie **Wymagane jest podanie informacji autoryzacyjnych PowerVC**. Kliknij przycisk **OK**. Jeśli nie masz PowerVC, pomiń ten i następny krok.

   Uwaga: Weryfikacja jest procesem użycia funkcji API OpenStack do sprawdzenia, czy produkt PowerVC rozpoznaje nowo zadeklarowany punkt końcowy. Jeśli produkt PowerVC nie znajduje się w środowisku użytkownika lub adres powervcKeystoneUrl nie został poprawnie skonfigurowany (za pomocą komendy pscuiserverctl), produkt PowerSC nie może zweryfikować punktu końcowego.
5. Gdy weryfikacja zostanie zakończona, w kolumnie **Nazwa hosta** wyświetlany jest komunikat w postaci tekstu w dymku. Komunikat ten potwierdza, czy produkt PowerVC rozpoznał nowy punkt końcowy. Na podstawie informacji w komunikacie można podjąć decyzję o tym, czy wygenerować magazyn kluczy.
6. Aby wygenerować magazyn kluczy, kliknij opcję **Wygeneruj magazyn kluczy**. Gdy generowany jest magazyn kluczy, punkt końcowy w tabeli miga. Gdy operacja zostanie zakończona, wartość w kolumnie **Magazyn kluczy został wygenerowany** jest zmieniana z **nie** na **tak**.

   Uwaga: Jeśli nie zweryfikowano punktu końcowego za pomocą produktu PowerVC, wyświetlany jest komunikat z pytaniem, czy kontynuować weryfikację. Kliknij opcję **Kontynuuj**, jeśli rozpoznasz punkt końcowy i chcesz wygenerować magazyn kluczy.

   Agent produktu PowerSC może potrzebować kilku minut, aby wykryć, że magazyn kluczy został wygenerowany. Gdy agent zainstaluje magazyn kluczy, nowy punkt końcowy jest wyświetlany jako w pełni zarządzany punkt końcowy na stronach **Administrator punktu końcowego - Wszystkie systemy**, **Zgodność**, **Bezpieczeństwo** i **Raporty** interfejsie GUI produktu PowerSC.
7. Jeśli nie chcesz generować magazynu kluczy dla punktu końcowego, możesz usunąć żądanie. Zaznacz pole wyboru punktu końcowego, który chcesz usunąć, i kliknij ikonę **Usuń**.
8. Wszystkie punkty końcowe oczekujące na weryfikację magazynu kluczy są wyświetlane w tabeli punktów końcowych. Wyświetlane punkty końcowe można filtrować za pomocą pola **Filtruj wg tekstu**. W tym polu wpisz tekst, który ma zostać użyty do filtrowania, i naciśnij klawisz **Enter**. Lista punktów końcowych jest dynamicznie filtrowana w celu wyświetlenia tylko tych wierszy, które zawierają wprowadzony tekst.
9. Aby odświeżyć informacje w tabeli punktów końcowych, kliknij opcję **Odśwież tabelę**.

Organizowanie i grupowanie punktów końcowych

Administratorzy systemu mogą organizować i grupować punkty końcowe na podstawie wybranej właściwości wspólnej. Można definiować grupy niestandardowe, które mogą zawierać jawnie wybrany zestaw punktów końcowych zarządzanych za pomocą interfejsu GUI produktu PowerSC.

Jeśli na przykład używane są 3 lub 4 środowiska, można utworzyć grupy zawierające produkcyjne punkty końcowe, testowe punkty końcowe i punkty końcowe zapewniania jakości.

Podczas instalowania tworzona jest grupa domyślna o nazwie **Wszystkie systemy**. Grupa ta zawiera wszystkie punkty końcowe wykryte w danym środowisku.

Tworzenie grup niestandardowych

Można utworzyć grupę niestandardową z jawnie wybraną listą określonych punktów końcowych.

1. Na pasku **Grupy** wybierz opcję **Utwórz nową grupę**. Zostanie otwarty pasek **Tworzenie nowej grupy**. Jeśli pasek **Grupy** nie jest rozwinięty, kliknij poziomy wielokropek na lewym panelu na głównej stronie interfejsu.
2. Wprowadź unikalną nazwę nowej grupy i naciśnij klawisz Enter. Nowa grupa zostanie dodana do paska **Grupy**.
3. Dodaj systemy, które mają znajdować się w tej grupie. Z listy **Wszystkie systemy** dostępnych systemów punktów końcowych wybierz te systemy, które chcesz dodać do grupy. Kliknij strzałkę w prawo, aby przenieść wszystkie wybrane systemy do nowej grupy. Aby usunąć systemy punktów końcowych z grupy, podświetl punkty końcowe na liście nowej grupy i kliknij strzałkę w lewo.
4. Po dodaniu lub usunięciu elementów grupy zapisz zmiany, klikając ikonę **Zapisz** na pasku menu panelu treści.
5. Kliknij poziomy wielokropek, aby powrócić do paska **Grupy**. Nowa grupa zostanie umieszczona na liście.

Dodawanie lub usuwanie systemów przypisanych do istniejącej grupy

Można dodawać lub usuwać punkty końcowe, które są przypisane do istniejącej grupy.

1. Na pasku **Grupy** kliknij przycisk wielokropka znajdujący się po prawej stronie grupy, do której chcesz dodać lub z której chcesz usunąć punkt końcowy. Jeśli pasek **Grupy** nie jest rozwinięty, kliknij poziomy wielokropek na lewym panelu na głównej stronie interfejsu.
2. Kliknij opcję **Edytuj grupę**.
3. Aby dodać system punktu końcowego do grupy, wybierz system na liście **Wszystkie systemy** i kliknij strzałkę w prawo. System zostanie dodany do listy ***nazwa_grupy***.
4. Aby usunąć punkt końcowy z grupy, wybierz system na liście **Systemy grupy** i kliknij strzałkę w lewo. System zostanie usunięty z listy ***nazwa_grupy***.
5. Kliknij ikonę **Zapisz zmiany grupy**, aby zapisać zmiany.
6. Aby usunąć system z grupy, wybierz system, a następnie kliknij strzałkę w lewo.
7. Aby anulować zmiany dotyczące grupy, kliknij opcję **Anuluj zmiany grupy**.
8. Kliknij wielokropek **Grupy**, aby powrócić do paska **Grupy**.

Usuwanie grupy

Grupy, które nie są już potrzebne, można usunąć.

1. Na pasku **Grupy** kliknij przycisk wielokropka znajdujący się po prawej stronie grupy, która ma zostać usunięta. Jeśli pasek **Grupy** nie jest rozwinięty, kliknij poziomy wielokropek na panelu nawigacyjnym na głównej stronie interfejsu.
2. Kliknij opcję **Usuń grupę**. Grupa zostanie usunięta z listy grup w pasku **Grupy**.

Zmiana nazwy grupy

Istnieje możliwość zmiany nazwy grupy punktów końcowych.

1. Na pasku **Grupy** kliknij przycisk wielokropka znajdujący się po prawej stronie grupy, której nazwa ma zostać zmieniona. Jeśli pasek **Grupy** nie jest rozwinięty, kliknij poziomy wielokropek na panelu nawigacyjnym na głównej stronie interfejsu.
2. Kliknij opcję **Zmień nazwę grupy**. Podaj nową nazwę grupy w polu **Nazwa grupy**.

Klonowanie grupy

Można sklonować grupę, aby pod nową nazwą utworzyć duplikat składający się z tych samych punktów końcowych.

1. Na pasku **Grupy** kliknij przycisk wielokropka znajdujący się po prawej stronie grupy, która ma zostać usunięta. Jeśli pasek **Grupy** nie jest rozwinięty, kliknij poziomy wielokropek na panelu nawigacyjnym na głównej stronie interfejsu.
2. Kliknij opcję **Sklonuj grupę**. Grupa zostanie skopiowana i zostanie jej przypisana nowa nazwa.

Praca z profilami zgodności

Za pomocą edytora profilu interfejsu GUI produktu PowerSC można wyświetlać wbudowane profile zgodności, tworzyć profile niestandardowe i kopiować profile do punktów końcowych systemu.

Produkt PowerSC Standard Edition jest dostarczany z zestawem wbudowanych profili, których można używać do konfigurowania punktów końcowych systemu, aby każdy punkt końcowy spełniał następujące standardy bezpieczeństwa:

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

Więcej informacji na temat wbudowanych profili zawiera sekcja “Koncepcje automatyzacji zabezpieczeń i zapewniania zgodności” na stronie 9.

Każdy z wbudowanych profili zawiera reguły, które muszą być stosowane do punktu końcowego, aby spełnić wymagania w zakresie bezpieczeństwa. Aby zastosować tylko podzbiór lub inną kombinację tych reguł albo dostosować poziomy zgodności, można utworzyć profil niestandardowy.

W większości środowisk administratorzy często modyfikują pliki zgodności, aby usunąć problemy dotyczące reguł. Gdy sprawdzenie zgodności zostanie zakończone, pliki reguł zgodności są traktowane jako stabilne i są wdrażane na serwerach produkcyjnych.

Profile niestandardowe można utworzyć za pomocą interfejsu GUI produktu PowerSC przez połączenie reguł z profili wbudowanych lub innych profili niestandardowych.

Wyświetlanie profili zgodności

Użytkownik może wyświetlić reguły, które znajdują się w każdym z profili wbudowanych i niestandardowych.

1. Na stronie głównej wybierz kartę **Edytor profilu**. Zostanie otwarta strona **Edytor profilu**.
2. Kliknij strzałkę w dół, aby wyświetlić listę profili. W menu rozwijanym wyświetlane są dostępne **Profile wbudowane** i **Profile niestandardowe**.
3. Wybierz profil, który chcesz wyświetlić. Wyświetlana jest każda reguła zawarta w profilu, w tym jej nazwa, typ i opis. Więcej informacji na temat reguł zawiera sekcja “Koncepcje automatyzacji zabezpieczeń i zapewniania zgodności” na stronie 9.
4. Wszystkie reguły dla wybranego profilu są wyświetlane w tabeli profili. Wyświetlane profile można filtrować za pomocą pola **Filtruj wg tekstu**. W tym polu tekstowym wpisz tekst, który ma zostać użyty do filtrowania. Lista reguł w wybranym profilu zostanie odświeżona.

Tworzenie profilu niestandardowego

Istnieje możliwość utworzenia profilu opartego na istniejącym profilu, a następnie dostosowania tego nowego profilu, aby zawierał tylko konkretny zestaw reguł.

1. Na stronie głównej wybierz kartę **Edytor profilu**. Zostanie otwarta strona **Edytor profilu**.
2. Kliknij strzałkę w dół, aby wyświetlić listę profili. W menu rozwijanym wyświetlane są dostępne **Profile wbudowane** i **Profile niestandardowe**.
3. Wybierz profil, na którym ma być oparty nowy profil.
4. Kliknij ikonę **Utwórz nowy profil**. Zostanie otwarte okno Nazwa i typ nowego profilu.
5. Wprowadź nazwę nowego profilu w polu **Nazwa profilu**.
6. Wprowadź typ w polu **Typ profilu**. Wprowadzany typ zwykle identyfikuje typ wbudowanej strategii, na której oparty jest nowy profil, a także unikalny identyfikator. Przykład: PCIxx, SOX-COBITxy, DoDxyz, HIPAAwxyz lub NERCabc.
7. Kliknij przycisk **Potwierdź**.
8. Aby dodać regułę do profilu niestandardowego, wybierz regułę z oryginalnego profilu, na podstawie którego tworzysz profil niestandardowy, a następnie kliknij strzałkę w prawo. Reguła jest dodawana do nowego profilu niestandardowego. Powtórz tę czynność dla każdej reguły, którą chcesz dołączyć.
9. Aby usunąć regułę z profilu niestandardowego, wybierz ją z profilu niestandardowego i kliknij strzałkę w lewo. Reguła jest usuwana z nowego profilu niestandardowego. Powtórz tę czynność dla każdej reguły, którą chcesz usunąć.
10. Kliknij przycisk **Zapisz** po zakończeniu dodawania reguł.

Kopiowanie profili do członków grupy

Istnieje możliwość kopiowania profili do grupy punktów końcowych. Gdy profil niestandardowy zostanie skopiowany do punktu końcowego, będzie on dostępny do zastosowania w tym punkcie końcowym. Jest on także dostępny do sprawdzenia, czy można go zastosować do punktu końcowego bez błędów.

1. Na stronie głównej wybierz kartę **Edytor profilu**. Zostanie otwarta strona **Edytor profilu**.
2. Kliknij strzałkę w dół, aby wyświetlić listę profili. W menu rozwijanym wyświetlane są dostępne **Profile wbudowane** i **Profile niestandardowe**.
3. Wybierz profil, który chcesz skopiować do członków grupy.
4. Kliknij ikonę **Skopiuj profil do członków grupy**. Zostanie otwarte okno **Skopiuj *nazwa_profilu* do członków grupy**.
5. Zostanie wyświetlona każda grupa, która została utworzona dla organizacji, wraz z powiązanym z nią polem wyboru. Zaznacz pole wyboru każdej grupy, do której ma zostać skopiowany wybrany profil.
6. Kliknij opcję **Kopiuj**.
7. Aby zastosować lub sprawdzić profil, wróć do strony **Zgodność**, wybierając kartę **Zgodność**.

Usuwanie profilu niestandardowego

Profil niestandardowy można usunąć.

1. Na stronie głównej wybierz kartę **Edytor profilu**. Zostanie otwarta strona **Edytor profilu**.
2. Kliknij strzałkę w dół, aby wyświetlić listę profili. W menu rozwijanym wyświetlane są dostępne **Profile wbudowane** i **Profile niestandardowe**.
3. Rozwiń listę **Profile niestandardowe**.
4. Wybierz profil, który chcesz usunąć.
5. Kliknij ikonę **Usuń profil**. Profil niestandardowy, który został wybrany, zostanie usunięty.

Administrowanie poziomami zgodności i profilami

Administratorzy systemu mogą stosować, sprawdzać i wycofywać wbudowane i niestandardowe poziomy zgodności oraz profile w wielu punktach końcowych.

W poniższej tabeli podano listę predefiniowanych profili i poziomów zgodności obsługiwanych przez produkt PowerSC Standard Edition.

Tabela 15. Predefiniowane profile i poziomy zgodności obsługiwane przez produkt PowerSC Standard Edition

Profile	**Poziomy**
Baza danych	niski
DoD	średni
DoD_to_AIXDefault	wysoki
DoDv2	domyślny
DoDv2_to_AIXDefault	
HIPAA	
NERC	
NERC_to_AIXDefault	
NERCv5	
NERCv5_to_AIXDefault	
PCI	
PCI_to_AIXDefault	
PCIv3	
PCIv3_to_AIXDefault	
SOX-COBIT	

Na stronie **Zgodność** w interfejsie GUI produktu PowerSC można wykonać następujące czynności:

- Wybranie i zastosowanie zdefiniowanego profilu lub poziomu do jednego lub wielu punktów końcowych.
- Wyzwolenie operacji cofnięcia dla jednego lub wielu punktów końcowych.
- Sprawdzenie zdefiniowanego profilu lub poziomu pod kątem bieżącego stanu jednego lub wielu punktów końcowych. Operacja sprawdzenia nie powoduje wprowadzenia żadnych zmian w punkcie końcowym, ale ustawia wartość **Datownik sprawdzenia**, aby wskazać kiedy wykonano ostatnie sprawdzenie.

Stosowanie poziomów zgodności i profili

Istnieje możliwość zastosowania poziomu zgodności lub profilu do jednego lub większej liczby punktów końcowych w wybranej grupie.

1. Na stronie głównej wybierz kartę **Zgodność**. Zostanie otwarta strona **Zgodność**.
2. Na pasku **Grupy** wybierz grupę zawierającą punkty końcowe, do których chcesz zastosować poziomy zgodności i profile.
3. Wszystkie punkty końcowe systemu dla wybranej grupy są wyświetlane w tabeli zgodności. Wyświetlane punkty końcowe można filtrować za pomocą pola tekstowego **Filtruj wg tekstu**. W tym polu tekstowym wpisz tekst, który ma zostać użyty do filtrowania, i naciśnij klawisz Enter. Lista punktów końcowych z wybranej grupy jest dynamicznie filtrowana w celu wyświetlenia tylko tych wierszy, które zawierają wprowadzony tekst.
4. Aby odświeżyć wyświetlane informacje o statusie, kliknij opcję **Odśwież tabelę**. Aby ustawić częstotliwość automatycznego odświeżania ekranu, kliknij opcję **Okres odświeżania**.
5. W kolumnie **Typ reguły zgodności** można sprawdzić poziomy i profile, które zostały skopiowane do powiązanego punktu końcowego. Wybierz poziom lub profil, który chcesz zastosować do punktu końcowego. Zaznacz powiązane z nim pole wyboru.
6. Powtórz krok 5 dla każdego punktu końcowego w grupie, do których mają zostać zastosowane poziomy zgodności i profile.
7. Kliknij ikonę **Zastosuj profile**.
8. Wybrane poziomy zgodności i profile są stosowane do wszystkich wybranych punktów końcowych. Jeśli nie można zastosować jednej lub większej liczby reguł, uważa się, że zakończyły się one niepowodzeniem. W

przypadku niepowodzenia jednej lub większej liczby reguł punkt końcowy jest oznaczany czerwonym paskiem, a w kolumnie **Liczba reguł z niepowodzeniem** wyświetlany jest tekst **Niepowodzenie**.

9. W kolumnie **Liczba reguł z niepowodzeniem** dla każdego oznaczonego punktu końcowego można sprawdzić przyczynę niepowodzenia reguły. Stosowane reguły można dopasować, tworząc lub modyfikując profil niestandardowy.

Wycofywanie poziomów zgodności

Istnieje możliwość wycofania ostatniego poziomu zgodności lub profilu, który został zastosowany do jednego lub większej liczby punktów końcowych w wybranej grupie.

Aby wycofać poziomy zgodności, wykonaj następujące kroki:

1. Na stronie głównej wybierz kartę **Zgodność**. Zostanie otwarta strona **Zgodność**.
2. Na pasku **Grupy** wybierz grupę zawierającą punkty końcowe, dla których chcesz wycofać poziomy zgodności i profile.
3. Wszystkie punkty końcowe dla wybranej grupy są wyświetlane w tabeli zgodności. Wyświetlane punkty końcowe można filtrować za pomocą pola tekstowego **Filtruj wg tekstu**. W tym polu tekstowym wpisz tekst, który ma zostać użyty do filtrowania, i naciśnij klawisz Enter. Lista punktów końcowych z wybranej grupy jest dynamicznie filtrowana w celu wyświetlenia tylko tych wierszy, które zawierają wprowadzony tekst.
4. Aby odświeżyć wyświetlane informacje o statusie, kliknij opcję **Odśwież tabelę**. Aby ustawić częstotliwość automatycznego odświeżania ekranu, kliknij opcję **Okres odświeżania**.
5. Aby wycofać poziom lub profil, który został zastosowany do punktu końcowego:
   a. Zaznacz pole wyboru odpowiedniego punktu końcowego.
   b. Kliknij ikonę **Cofnij**.

Sprawdzanie ostatnio zastosowanego poziomu zgodności i profilu

Istnieje możliwość sprawdzenia ostatniego poziomu zgodności lub profilu, który został zastosowany do jednego lub większej liczby punktów końcowych w wybranej grupie.

1. Na stronie głównej wybierz kartę **Zgodność**. Zostanie otwarta strona **Zgodność**.
2. Na pasku **Grupy** wybierz grupę zawierającą punkty końcowe, dla których chcesz sprawdzić poziomy zgodności i profile.
3. Wszystkie punkty końcowe dla wybranej grupy są wyświetlane w tabeli zgodności. Wyświetlane punkty końcowe można filtrować za pomocą pola tekstowego **Filtruj wg tekstu**. W tym polu tekstowym wpisz tekst, który ma zostać użyty do filtrowania, i naciśnij klawisz Enter. Lista punktów końcowych z wybranej grupy jest dynamicznie filtrowana w celu wyświetlenia tylko tych wierszy, które zawierają wprowadzony tekst.
4. Aby odświeżyć wyświetlane informacje o statusie, kliknij opcję **Odśwież tabelę**. Aby ustawić częstotliwość automatycznego odświeżania ekranu, kliknij opcję **Okres odświeżania**.
5. Zaznacz odpowiednie pole wyboru obok nazwy systemu punktu końcowego, dla którego chcesz sprawdzić ostatni zastosowany poziom lub profil.
6. Powtórz krok 5 na stronie 145 dla każdego punktu końcowego w grupie, dla którego chcesz sprawdzić poziom zgodności i profil.
7. Kliknij ikonę **Sprawdź**.
8. Punkt końcowy jest sprawdzany, aby stwierdzić, czy reguły zawarte w poziomie zgodności lub profilu mogą zostać zastosowane. Punkty końcowe nie są aktualizowane. Jeśli nie można zastosować reguł, uważa się, że zakończą się niepowodzeniem po zastosowaniu. W przypadku niepowodzenia jednej lub większej liczby reguł punkt końcowy jest oznaczany czerwonym paskiem, a w kolumnie **Liczba reguł z niepowodzeniem** wyświetlany jest tekst **Niepowodzenie**.
9. Na liście **Liczba reguł z niepowodzeniem** dla każdego oznaczonego punktu końcowego można wyświetlić komunikat wskazujący przyczynę niepowodzenia reguły. Stosowane reguły można dopasować, tworząc profil niestandardowy.

Sprawdzanie niezastosowanego poziomu zgodności lub profilu

Istnieje możliwość sprawdzenia poziomu zgodności lub profilu, który nie został zastosowany do jednego lub większej liczby punktów końcowych w wybranej grupie.

1. Na stronie głównej wybierz kartę **Zgodność**. Zostanie otwarta strona **Zgodność**.
2. Na pasku **Grupy** wybierz grupę zawierającą punkty końcowe, dla których chcesz sprawdzić wpływ poziomu zgodności lub profilu.
3. Wszystkie punkty końcowe dla wybranej grupy są wyświetlane w tabeli zgodności. Wyświetlane punkty końcowe można filtrować za pomocą pola tekstowego **Filtruj wg tekstu**. W tym polu tekstowym wpisz tekst, który ma zostać użyty do filtrowania, i naciśnij klawisz Enter. Lista punktów końcowych z wybranej grupy jest dynamicznie filtrowana w celu wyświetlenia tylko tych wierszy, które zawierają wprowadzony tekst.
4. Aby odświeżyć wyświetlane informacje o statusie, kliknij opcję **Odśwież tabelę**. Aby ustawić częstotliwość automatycznego odświeżania ekranu, kliknij opcję **Okres odświeżania**.
5. Zaznacz odpowiednie pole wyboru obok nazwy systemu punktu końcowego, dla którego chcesz sprawdzić ostatni zastosowany poziom lub profil. Można wybrać więcej niż jeden punkt końcowy.
6. Otwórz listę rozwijaną **Ostatnio sprawdzony typ**. Wybierz jedną z następujących opcji:
   - **Wszystkie dostępne poziomy** – wyświetla listę wszystkich dostępnych poziomów, które można sprawdzić dla punktu końcowego.
   - **Wszystkie dostępne profile** – wyświetla listę wszystkich dostępnych profili, które można sprawdzić dla punktu końcowego.
7. Wybierz poziom lub profil, który chcesz sprawdzić dla punktu końcowego.
8. Kliknij ikonę **Sprawdź**. Wyniki sprawdzenia zostaną zwrócone i wyświetlone pod punktem końcowym.

Wysłanie powiadamiania e-mail po wystąpieniu zdarzenia dotyczącego zgodności

Na stronie Zgodność można wysłać powiadomienie e-mail do jednego lub większej liczby odbiorców, gdy wystąpi zdarzenie dotyczące zgodności.

1. Na stronie głównej wybierz kartę **Zgodność**. Zostanie otwarta strona **Zgodność**.
2. Kliknij ikonę **Ustawienia poczty elektronicznej** w prawym górnym rogu paska menu. Zostanie otwarte okno **Ustawienia poczty elektronicznej**.
3. Zaznacz pole wyboru **Wysyłaj do mnie wiadomości e-mail**.
4. W polu **Adresy (oddzielone przecinkami)** wprowadź adresy e-mail wszystkich adresatów oddzielone przecinkami.

Monitorowanie bezpieczeństwa punktu końcowego

Za pomocą strony **Bezpieczeństwo** można monitorować bezpieczeństwo punktu końcowego w czasie rzeczywistym.

Na stronie Bezpieczeństwo wyświetlany jest status punktów końcowych monitorowanych przez funkcje zgodności w czasie rzeczywistym (Real Time Compliance — RTC) i zaufanego wykonywanie (Trusted Execution — TE).

Zarówno zgodność RTC (komponent produktu PowerSC), jak i TE (komponent systemu AIX) reprezentują funkcję monitorowania integralności pliku (File Integrity Monitoring — FIM). Funkcja FIM monitoruje zmiany ważnych plików, aby zapewnić, że zdarzenia wpływające na pliki są autoryzowane. Zdarzenia, które mogą wpływać na bezpieczeństwo, to między innymi nieoczekiwana zmiana uprawnienia do pliku, aktualizacja zawartości pliku lub niezaplanowana instalacja aplikacji. Należy rozpoznawać takie zdarzenia, aby zabezpieczyć ważne pliki i aplikacje.

Strona **Bezpieczeństwo** to strona monitorowania w czasie rzeczywistym należąca do interfejsu GUI produktu PowerSC. Wyświetlane są na niej zdarzenia, które są generowane wtedy, gdy zostaną zmienione pliki monitorowane przez funkcje RTC lub TE. Zdarzenia zawierają szczegóły informujące o tym, kiedy zawartość pliku została zmieniona, kiedy uzyskano dostęp do punktu końcowego, a także kiedy została zmieniona konfiguracja.

Za pomocą strony **Bezpieczeństwo** można wykonywać następujące czynności:

- Wyświetlanie informacji monitorowania przez funkcje RTC i TE w czasie rzeczywistym
- Konfigurowanie funkcji RTC i TE dla wszystkich punktów końcowych
- Wyświetlanie statusu innych produktów PowerSC w punktach końcowych
- Włączanie i wyłączanie funkcji TE

Konfigurowanie funkcji RTC (Real Time Compliance)

Na stronie **Bezpieczeństwo** można skonfigurować zgodność w czasie rzeczywistym (Real Time Compliance — RTC) dla konkretnego punktu końcowego lub grupy punktów końcowych.

1. Kliknij przycisk wielokropka znajdujący się po prawej stronie punktu końcowego, dla którego chcesz zmodyfikować opcje konfiguracyjne funkcji RTC.
2. Kliknij opcję **Skonfiguruj RTC**. Zostanie otwarte okno Konfiguracja strategii RTC.
3. Zostaną wyświetlone wszystkie dostępne opcje konfiguracyjne funkcji RTC z objaśnieniem. Aby zmienić jedną lub więcej opcji konfiguracyjnych funkcji RTC, zaznacz lub usuń zaznaczenie pola wyboru znajdującego się po lewej stronie opcji. W niektórych przypadkach zmiany opcji nie zostaną zaimplementowane, dopóki serwer nie zostanie zrestartowany.
4. Kliknij przycisk **Zapisz**.

Przywracanie opcji konfiguracyjnych zgodności RTC (Real Time Compliance) do wartości dla poprzedniej daty i godziny

Istnieje możliwość przywrócenia konfiguracji zgodności RTC do postaci z poprzedniej daty i godziny.

1. Kliknij przycisk wielokropka znajdujący się po prawej stronie punktu końcowego, dla którego chcesz wycofać opcje konfiguracyjne zgodności RTC do poprzedniej wersji.
2. Kliknij opcję **Wycofaj RTC**. Zostaną wyświetlone datowniki dla każdej wersji konfiguracji zgodności RTC.
3. Kliknij datownik dla wersji konfiguracji, która ma zostać przywrócona. Opcje konfiguracyjne zgodności RTC, które obowiązywały dla danej daty i godziny, zostaną przywrócone.

Kopiowanie opcji konfiguracyjnych zgodności RTC (Real Time Compliance) do innych grup

Istnieje możliwość skopiowania opcji konfiguracyjnych zgodności RTC do innej grupy punktów końcowych lub do konkretnego zestawu punktów końcowych.

1. Kliknij przycisk wielokropka znajdujący się po prawej stronie punktu końcowego, którego opcje konfiguracyjne chcesz skopiować do innej grupy punktów końcowych lub do konkretnego zestawu punktów końcowych.
2. Kliknij opcję **Skopiuj konfigurację RTC**. Zostaną wyświetlone wszystkie grupy punktów końcowych, w tym grupa **Wszystkie systemy**.
3. Wybierz grupę lub konkretne punkty końcowe, używając jednej z następujących metod:
   - Na liście dostępnych grup zaznacz pole wyboru grupy punktów końcowych. Opcje konfiguracyjne zostaną skopiowane do wszystkich punktów końcowych znajdujących się w tej grupie.
   - Użyj strzałki w prawo, aby rozwinąć grupę w celu wyświetlenia listy wszystkich punktów końcowych w grupie. Zaznacz pole wyboru każdego punktu końcowego grupy, do którego chcesz skopiować opcje konfiguracyjne.
   - Rozwiń listę punktów końcowych w grupie **Wszystkie systemy**. Zaznacz pole wyboru każdego punktu końcowego grupy, do którego chcesz skopiować punkty końcowe.
4. Kliknij przycisk **OK**. Opcje konfiguracyjne zostaną skopiowane do wybranej grupy lub do wybranych punktów końcowych.

Edytowanie listy plików funkcji RTC (Real Time Compliance)

Użytkownik może wyświetlać i edytować opcje monitorowania funkcji RTC dla każdego pliku w punkcie końcowym.

1. Kliknij przycisk wielokropka znajdujący się po prawej stronie punktu końcowego zawierającego pliki, dla których chcesz wyświetlić lub edytować opcje monitorowania funkcji RTC.

2. Kliknij opcję **Edytuj listę plików RTC**. Zostanie otwarta strona **Konfiguracja listy plików RTC** zawierająca wszystkie katalogi i pliki znajdujące się w punkcie końcowym. Znacznik wyboru na ikonie folderu katalogu wskazuje, że w tym katalogu monitorowany jest przynajmniej jeden plik.
3. Jeśli plik, którego opcje chcesz zmodyfikować, znajduje się w katalogu, dwukrotnie kliknij ten katalog, aby wyświetlić pliki. Wyświetlane są wszystkie pliki znajdujące się w katalogu.
4. Opcje monitorowania każdego pliku w punkcie końcowym są wyświetlane w kolumnach **Zawartość** i **Atrybuty**. Pole wyboru jest zaznaczone w kolumnie **Zawartość**, jeśli plik jest monitorowany pod kątem zmiany zawartości. Pole wyboru jest zaznaczone w kolumnie **Atrybuty**, jeśli plik jest monitorowany pod kątem zmiany atrybutów. Aby zmodyfikować opcje monitorowania, zaznacz lub usuń zaznaczenie pól wyboru dla jednego lub większej liczby plików w punkcie końcowym.
5. Kliknij przycisk **Zapisz**.

Przywracanie opcji monitorowania plików funkcji RTC do wartości dla poprzedniej konfiguracji

Istnieje możliwość przywrócenia poprzedniej wersji plików monitorowanych przez funkcję RTC.

1. Kliknij przycisk wielokropka znajdujący się po prawej stronie punktu końcowego, dla którego chcesz wycofać opcje monitorowania plików funkcji RTC do poprzedniej wersji.
2. Kliknij opcję **Wycofaj listę plików RTC**. Zostaną wyświetlone datowniki dla każdej wersji konfiguracji monitorowanych plików.
3. Kliknij datownik dla wersji konfiguracji opcji monitorowania, która ma zostać przywrócona. Opcje konfiguracyjne, które obowiązywały dla danej daty i godziny, zostaną przywrócone.

Kopiowanie opcji monitorowania listy plików zgodności w czasie rzeczywistym (RTC) do innych grup

Istnieje możliwość skopiowania opcji monitorowania plików funkcji RTC do innej grupy punktów końcowych lub do konkretnego zestawu punktów końcowych.

1. Kliknij przycisk wielokropka znajdujący się po prawej stronie punktu końcowego, którego opcje monitorowania plików chcesz skopiować do innej grupy punktów końcowych lub do konkretnego zestawu punktów końcowych.
2. Kliknij opcję **Skopiuj listę plików RTC**. Zostaną wyświetlone wszystkie grupy punktów końcowych, w tym grupa **Wszystkie systemy**.
3. Wybierz grupę lub konkretne punkty końcowe, używając jednej z następujących metod:
   - Na liście dostępnych grup zaznacz pole wyboru grupy punktów końcowych. Opcje monitorowania listy plików zostaną skopiowane do wszystkich punktów końcowych znajdujących się w tej grupie.
   - Użyj strzałki w prawo, aby rozwinąć grupę w celu wyświetlenia listy wszystkich punktów końcowych w grupie. Zaznacz pole wyboru każdego punktu końcowego grupy, do którego chcesz skopiować opcje monitorowania plików.
   - Rozwiń listę punktów końcowych w grupie **Wszystkie systemy**. Zaznacz pole wyboru każdego punktu końcowego grupy, do którego chcesz skopiować punkty końcowe.
4. Kliknij przycisk **OK**. Opcje monitorowania plików zostaną skopiowane do wybranej grupy lub do wybranych punktów końcowych.

Uruchamianie sprawdzania zgodności RTC (Real Time Compliance)

Na stronie Bezpieczeństwo można uruchomić sprawdzanie zgodności RTC w celu sprawdzenia, czy punkt końcowy jest nadal zgodny.

1. Kliknij przycisk wielokropka znajdujący się po prawej stronie punktu końcowego, dla którego chcesz uruchomić sprawdzanie zgodności RTC (Real Time Compliance).
2. Kliknij opcję **Uruchom sprawdzanie zgodności**. Zostanie otwarta strona **Zgodność**, na której będzie migać wiersz danego punktu końcowego, co oznacza, że trwa sprawdzanie.

3. Jeśli zastosowanie jakiś reguł zakończyło się niepowodzeniem, w kolumnie **Liczba reguł z niepowodzeniem** zostanie wyświetlony komunikat wskazujący niepowodzenie. Użyj przycisku strzałki w dół znajdującego się po lewej stronie punktu końcowego, aby wyświetlić regułę z niepowodzeniem.

Konfigurowanie zaufanego wykonywania

Na stronie **Bezpieczeństwo** można skonfigurować zaufane wykonywanie (Trusted Execution — TE) dla konkretnego punktu końcowego lub grupy punktów końcowych.

1. Kliknij przycisk wielokropka znajdujący się po prawej stronie punktu końcowego, dla którego chcesz zmodyfikować opcje konfiguracyjne zaufanego wykonywania (TE).
2. Kliknij opcję **Skonfiguruj TE**. Zostanie otwarte okno Konfiguracja strategii TE.
3. Zostaną wyświetlone wszystkie opcje konfiguracyjne TE z objaśnieniem. Aby zmienić jedną lub więcej opcji konfiguracyjnych TE, zaznacz lub usuń zaznaczenie odpowiedniego pola wyboru. W niektórych przypadkach zmiany opcji nie zostaną zaimplementowane, dopóki serwer nie zostanie zrestartowany.
4. Kliknij przycisk **Zapisz**.

Kopiowanie opcji zaufanego wykonywania (TE) do innych grup

Istnieje możliwość skopiowania opcji konfiguracyjnych funkcji TE do innej grupy punktów końcowych lub do konkretnego zestawu punktów końcowych.

1. Kliknij przycisk wielokropka znajdujący się po prawej stronie punktu końcowego, którego opcje konfiguracyjne chcesz skopiować do innej grupy punktów końcowych lub do konkretnego zestawu punktów końcowych.
2. Kliknij opcję **Skopiuj konfigurację TE**. Zostaną wyświetlone wszystkie grupy punktów końcowych, w tym grupa **Wszystkie systemy**.
3. Wybierz grupę lub konkretne punkty końcowe, używając jednej z następujących metod:
   - Na liście dostępnych grup zaznacz pole wyboru grupy punktów końcowych. Opcje konfiguracyjne zostaną skopiowane do wszystkich punktów końcowych znajdujących się w tej grupie.
   - Rozwiń grupę w celu wyświetlenia listy wszystkich punktów końcowych w grupie. Zaznacz pole wyboru każdego punktu końcowego grupy, do którego chcesz skopiować opcje konfiguracyjne.
   - Rozwiń listę punktów końcowych w grupie **Wszystkie systemy**. Zaznacz pole wyboru każdego punktu końcowego grupy, do którego chcesz skopiować punkty końcowe.
4. Kliknij przycisk **OK**. Opcje konfiguracyjne zostaną skopiowane do wybranej grupy lub do wybranych punktów końcowych.

Edytowanie listy plików zaufanego wykonywania (TE)

Użytkownik może wyświetlać i edytować opcje monitorowania funkcji TE dla każdego pliku w punkcie końcowym.

1. Kliknij przycisk wielokropka znajdujący się po prawej stronie punktu końcowego zawierającego pliki, dla których chcesz wyświetlić lub edytować opcje monitorowania funkcji TE.
2. Kliknij opcję **Edytuj listę plików TE**. Zostanie otwarta strona **Konfiguracja listy plików TE** zawierająca wszystkie katalogi i pliki znajdujące się w punkcie końcowym. Znacznik wyboru na ikonie folderu katalogu wskazuje, że w tym katalogu monitorowany jest przynajmniej jeden plik.
3. Jeśli plik, którego opcje chcesz wyświetlić lub zmodyfikować, znajduje się w katalogu, dwukrotnie kliknij ten katalog, aby wyświetlić pliki. Wyświetlane są wszystkie pliki znajdujące się w katalogu.
4. Opcje monitorowania każdego pliku w punkcie końcowym są wyświetlane w kolumnach **TE** i **Ulotny**. Pole wyboru jest zaznaczone w kolumnie **TE**, jeśli plik jest monitorowany pod kątem zmiany zawartości. Pole wyboru jest zaznaczone w kolumnie **Ulotny**, jeśli plik jest monitorowany tylko pod kątem zmiany uprawnień. Aby zmienić opcje monitorowania, zaznacz lub usuń zaznaczenie pól wyboru dla jednego lub większej liczby plików w punkcie końcowym.
5. Kliknij przycisk **Zapisz**.

Kopiowanie opcji monitorowania listy plików zaufanego wykonywania (TE) do innych grup

Istnieje możliwość skopiowania opcji monitorowania plików funkcji TE do innej grupy punktów końcowych lub do konkretnego zestawu punktów końcowych.

1. Kliknij przycisk wielokropka znajdujący się po prawej stronie punktu końcowego, którego opcje monitorowania plików chcesz skopiować do innej grupy punktów końcowych lub do konkretnego zestawu punktów końcowych.
2. Kliknij opcję **Skopiuj listę plików TE**. Zostaną wyświetlone wszystkie grupy punktów końcowych, w tym grupa **Wszystkie systemy**.
3. Wybierz grupę lub konkretne punkty końcowe, używając jednej z następujących metod:
   - Na liście dostępnych grup zaznacz pole wyboru grupy punktów końcowych. Opcje monitorowania listy plików zostaną skopiowane do wszystkich punktów końcowych znajdujących się w tej grupie.
   - Rozwiń grupę w celu wyświetlenia listy wszystkich punktów końcowych w grupie. Zaznacz pole wyboru każdego punktu końcowego grupy, do którego chcesz skopiować opcje monitorowania plików.
   - Rozwiń listę punktów końcowych w grupie **Wszystkie systemy**. Zaznacz pole wyboru każdego punktu końcowego grupy, do którego chcesz skopiować punkty końcowe.
4. Kliknij przycisk **OK**. Opcje monitorowania plików zostaną skopiowane do wybranej grupy lub do wybranych punktów końcowych.

Wyświetlanie statusu innych funkcji produktu PowerSC

Na stronie Bezpieczeństwo można wyświetlić status funkcji produktu PowerSC, takich jak Zaufane uruchamianie, Zaufany firewall i Zaufane rejestrowanie. Ponadto można wyświetlić status aktualizacji zaufanej sieci (Trusted Network Connect – TNC) w punkcie końcowym.

1. Na stronie głównej wybierz kartę **Bezpieczeństwo**. Zostanie otwarta strona **Bezpieczeństwo**.
2. Komponent TNC produktu PowerSC służy do sprawdzania i aktualizowania poprawek dotyczących bezpieczeństwa w każdym punkcie końcowym. Kolumna **Aktualizowanie z użyciem TNC** w tabeli punktów końcowych wskazuje, czy punkt końcowy jest aktualny z perspektywy serwera TNC. Sekcja **Aktualizowanie z użyciem TNC** w banerze panelu kontrolnego pokazuje wartość procentową aktualnych punktów końcowych w grupie. Aby usunąć wyświetlanie informacji o aktualizacjach TNC na stronie **Bezpieczeństwo**, wykonaj następujące kroki:
   a. Kliknij ikonę **Język i ustawienia** na pasku menu strony głównej.
   b. Kliknij opcję **Użycie podproduktów**.
   c. Dla opcji **Aktualizowanie z użyciem TNC** ustaw wartość Wyłączone.
   d. Aby przywrócić wyświetlanie przełącz opcję **Aktualizowanie z użyciem TNC** do wartości Włączone.
3. Kolumna **TB** w tabeli punktów końcowych wskazuje, czy funkcja zaufanego uruchamiania (Trusted Boot – TB) PowerSC jest dostępna w punkcie końcowym. Sekcja **Zaufane uruchamianie** w banerze panelu kontrolnego przedstawia wartość procentową punktów końcowych w obecnie wybranej grupie, dla których aktywowano funkcję zaufanego uruchamiania PowerSC. Aby usunąć wyświetlanie informacji funkcji zaufanego uruchamiania PowerSC na stronie **Bezpieczeństwo**, wykonaj następujące kroki:
   a. Kliknij ikonę **Język i ustawienia** na pasku menu strony głównej.
   b. Kliknij opcję **Użycie podproduktów**.
   c. Przesuń przełącznik opcji **Zaufane uruchamianie** do pozycji Wyłączone.
   d. Aby przywrócić wyświetlanie, przesuń przełącznik do pozycji Włączone.
4. Kolumna **TF** w tabeli punktów końcowych wskazuje, czy funkcja zaufanego firewalla (Trusted Firewall – TF) PowerSC jest dostępna w punkcie końcowym. Sekcja **Zaufany firewall** w banerze panelu kontrolnego przedstawia wartość procentową punktów końcowych w obecnie wybranej grupie, dla których aktywowano funkcję zaufanego firewalla PowerSC. Aby usunąć wyświetlanie informacji funkcji zaufanego firewalla na stronie **Bezpieczeństwo**, wykonaj następujące kroki:
   a. Kliknij ikonę **Język i ustawienia** na pasku menu strony głównej.
   b. Kliknij opcję **Użycie podproduktów**.

c. Przesuń przełącznik opcji **Zaufany firewall** do pozycji Wyłączone.
d. Aby przywrócić wyświetlanie, przesuń przełącznik do pozycji Włączone.

5. Kolumna **TL** w tabeli punktów końcowych wskazuje, czy funkcja zaufanego rejestrowania (Trusted Logging – TL) PowerSC jest dostępna w punkcie końcowym. Sekcja **Zaufane rejestrowanie** w banerze panelu kontrolnego przedstawia wartość procentową punktów końcowych w obecnie wybranej grupie, dla których aktywowano funkcję zaufanego rejestrowania PowerSC. Aby usunąć wyświetlanie informacji funkcji zaufanego rejestrowania na stronie **Bezpieczeństwo**, wykonaj następujące kroki:
   a. Kliknij ikonę **Język i ustawienia** na pasku menu strony głównej.
   b. Kliknij opcję **Użycie podproduktów**.
   c. Przesuń przełącznik opcji **Zaufane rejestrowanie** do pozycji Wyłączone.
   d. Aby przywrócić wyświetlanie, przesuń przełącznik do pozycji Włączone.

Przełączanie monitorowania zaufanego wykonywania

Użytkownik może włączać i wyłączać monitorowanie zaufanego wykonywania (TE). Ponadto użytkownik może wyłączyć monitorowanie TE i zaplanować jego włączenie z uwzględnieniem podanego przedziału czasu.

1. Kliknij ikonę **Przełączanie zaufanego wykonywania**.
2. Z paska rozwijanego wybierz jedną z następujących opcji:
   - **WŁĄCZ dla wszystkich punktów końcowych**, aby włączyć monitorowanie TE dla każdego punktu końcowego.
   - **WYŁĄCZ dla wszystkich punktów końcowych**, aby wyłączyć monitorowanie TE dla każdego punktu końcowego.
3. Jeśli monitorowanie TE jest wyłączone, opcje ustawiania czasu restartowania monitorowania TE stają się dostępne. Użytkownik może wybrać jeden z następujących czasów restartowania:
   - **1 godz.**
   - **5 godz.**
   - **1 dzień**
   - **1 tydzień**
   - **Nigdy**
4. Kliknij przycisk **Zapisz**.

Wysłanie powiadamiania e-mail po wystąpieniu zdarzenia dotyczącego bezpieczeństwa

Na stronie Bezpieczeństwo można wysłać powiadomienie e-mail do jednego lub większej liczby odbiorców, gdy wystąpi zdarzenie dotyczące bezpieczeństwa.

1. Na stronie głównej wybierz kartę **Bezpieczeństwo**. Zostanie otwarta strona **Bezpieczeństwo**.
2. Kliknij ikonę **Ustawienia poczty elektronicznej** w prawym rogu paska menu. Zostanie otwarte okno **Ustawienia poczty elektronicznej**.
3. Zaznacz pole wyboru **Wysyłaj do mnie wiadomości e-mail**.
4. W polu **Adresy (oddzielone przecinkami)** wprowadź adresy e-mail wszystkich adresatów oddzielone przecinkami.

Praca z raportami

Na stronie Raporty interfejsu GUI produktu PowerSC dostępnych jest wiele raportów.

Dostępne są następujące raporty:

- Raport **Przegląd zgodności** jest obrazem stanu informacji wysokiego poziomu, który jest wyświetlany na stronie **Zgodność** interfejsu.

- Raport **Szczegóły zgodności** jest obrazem stanu szczegółowych informacji niskiego poziomu, który jest wyświetlany na stronie **Zgodność**.
- Raport **Przegląd integralności pliku** jest obrazem stanu informacji wysokiego poziomu, który jest wyświetlany na stronie **Bezpieczeństwo** interfejsu.
- Raport **Szczegóły integralności pliku** jest obrazem stanu szczegółowych informacji niskiego poziomu, który jest wyświetlany na stronie **Bezpieczeństwo**.
- **Zgodność połączona z FIM**

Domyślnie na stronie **Raporty** wyświetlane są raporty **Przegląd zgodności** i **Przegląd integralności pliku** dla grupy **Wszystkie systemy**. Dla raportów **Szczegóły zgodności**, **Szczegóły integralności pliku** i **Zgodność połączona z FIM** nie określono grup domyślnych.

Użytkownik może wygenerować każdy typ raportu dla grupy **Wszystkie systemy** i dla każdej zdefiniowanej grupy. Użytkownik może wygenerować raport dla wszystkich punktów końcowych w grupie lub dla podzbioru punktów końcowych w grupie. Po wygenerowaniu raportu można zaplanować dystrybucję raportu w wiadomości e-mail sformatowanej za pomocą kodu HTML i jako pliku CSV do jednego lub wielu odbiorców na żądanie lub codziennie.

Lista raportów wyświetlanych na stronie **Raporty** zmienia się w zależności od używanego identyfikatora użytkownika użytego do zalogowania. Raporty można wygenerować tylko dla tych punktów końcowych, którymi użytkownik zarządza na podstawie używanego identyfikatora. Każdy raport, który zostanie wygenerowany w danej sesji, zostanie wyświetlony po otwarciu kolejnej sesji.

Wybieranie grupy raportów

Użytkownik może uruchomić każdy raport dla grupy **Wszystkie systemy** i dla każdej zdefiniowanej grupy. Użytkownik może uruchomić raport dla wszystkich punktów końcowych znajdujących się w grupie lub dla podzbioru punktów końcowych w grupie.

1. Na stronie głównej kliknij kartę **Raporty**. Zostanie otwarta strona **Raporty**.
2. Kliknij przycisk wielokropka znajdujący się po prawej stronie typu raportu, który chcesz uruchomić.
3. Kliknij opcję **Zmień grupę**.
4. Zostanie wyświetlone okno wyboru z wszystkimi dostępnymi grupami. Wybierz przełącznik obok grupy, dla której chcesz uruchomić raport. Kliknij przycisk **Potwierdź**. Raport zostanie uruchomiony, a zawartość panelu głównego zostanie odświeżona z użyciem informacji dla wybranej grupy.
5. Aby uruchomić raport dla podzbioru punktów końcowych, rozwiń grupę **Wszystkie systemy**. Zostanie wyświetlona lista wszystkich dostępnych punktów końcowych. Zaznacz pole wyboru obok każdego punktu końcowego, który ma zostać uwzględniony w raporcie. Kliknij opcję **Potwierdź**, aby uruchomić raport.

   Uwaga: Aby uruchomić raport dla konkretnej grupy punktów końcowych, można utworzyć grupę zawierającą te punkty końcowe. Tworząc grupę, oszczędza się czas, a ponadto grupa może być używana przez wszystkich użytkowników, ponieważ grupy są globalne (są widoczne dla wszystkich użytkowników interfejsu).
6. Można wyszukać konkretny punkt końcowy, wprowadzając nazwę punktu końcowego w polu wyszukiwania. Kliknij opcję **Potwierdź**, aby uruchomić raport dla tego punktu końcowego.

Dystrybuowanie raportów za pomocą wiadomości e-mail

Po ustawieniu grupy dla raportu można zaplanować jego dystrybuowanie w postaci wiadomości e-mail sformatowanej za pomocą kodu HTML i pliku CSV. Można zaplanować wysyłanie wiadomości e-mail do jednego lub wielu odbiorców natychmiast lub codziennie.

Dołączenie wersji CSV raportu umożliwia odbiorcom załadowanie danych raportu do arkusza kalkulacyjnego lub ich zaimportowanie do innej aplikacji wykorzystującej pliki CSV. Pliki CSV nie zawierają grafiki ani elementów paneli kontrolnych. Plik CSV generowany z raportu przeglądowego zawiera w pierwszym wierszu wszystkie nagłówki kolumn rozdzielone przecinkami. W kolejnych wierszach znajdują się punkty końcowe i wartości poszczególnych kolumn.

Na podstawie raportów szczegółowych generowanych jest wiele plików CSV. Pierwszy plik CSV ma format podobny do raportu przeglądowego. Oddzielny plik CSV jest generowany dla każdego poziomu szczegółowości raportu. Na przykład w raporcie Szczegóły integralności pliku następujące poziomy szczegółowości spowodują wygenerowanie oddzielnych plików CSV:

- **Konfiguracja TE**
- **Konfiguracja RTC**
- **Status podproduktu**

1. Na stronie głównej kliknij kartę **Raporty**. Zostanie otwarta strona **Raporty**.
2. Z listy dostępnych raportów wybierz raport, który chcesz dystrybuować. Raport zostanie uruchomiony, a zawartość strony głównej zostanie odświeżona.
3. Kliknij przycisk wielokropka znajdujący się po prawej stronie raportu, który chcesz dystrybuować.
4. Kliknij opcję **Opcje wiadomości e-mail**. Zostanie otwarte okno Wyślij raporty w wiadomości e-mail.
5. Podaj adres e-mail dla każdego odbiorcy w polu **Adresy**. Adresy odbiorców należy oddzielić średnikiem (;).
6. Podaj opis wiadomości e-mail w polu **Temat**.
7. Wybierz jedną spośród następujących opcji:
   - Zaznacz pole wyboru **Wysyłaj codziennie o**, aby codziennie wysyłać raport do odbiorców. Podaj czas miejscowy wysyłania raportu, wybierając godzinę i minuty. Kliknij opcje **Zapisz i Zamknij**. Raport będzie wysyłany codziennie w określonym czasie.
   - Kliknij opcję **Wyślij natychmiast**, aby wysłać raport. Raport zostanie wysłany, a okno zostanie zamknięte.

Komendy PowerSC Standard Edition

Produkt PowerSC Standard Edition udostępnia komendy, które umożliwiają komunikację z komponentem zaufanego firewalla i komponentem zaufanej sieci za pomocą wiersza komend.

Komenda chvfilt

Przeznaczenie

Zmienia wartości dla istniejącej reguły filtrowania komunikacji między wirtualnymi sieciami LAN.

Składnia

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

Opis

Komenda **chvfilt** służy do zmiany definicji reguły filtrowania komunikacji między wirtualnymi sieciami LAN w tabeli reguł filtrowania.

Opcje

-a Określa działanie. Poprawne wartości to:
- D (Deny): blokuje ruch
- P (Permit): zezwala na ruch

-c Określa protokoły, do których ma zastosowanie reguła filtrowania. Poprawne wartości to:
- udp
- icmp
- icmpv6
- tcp
- any

-d Określa adres docelowy w formacie IPv4 lub IPv6.

-m Określa maskę adresu źródłowego.

-M Określa maskę adresu docelowego.

-n Określa identyfikator reguły filtrowania, która ma zostać zmodyfikowana.

-o Określa port źródłowy lub typ operacji dla protokołu ICMP (Internet Control Message Protocol). Poprawne wartości to:
- lt
- gt
- eq
- any

-O Określa port docelowy lub kod ICMP. Poprawne wartości to:
- lt
- gt
- eq

- any

-p Określa port źródłowy lub typ ICMP.

-P Określa port docelowy lub kod ICMP.

-s Określa adres źródłowy w formacie v4 lub v6.

-v Określa wersję protokołu IP dla tabeli reguł filtrowania. Poprawne wartości to 4 i 6.

-z Określa identyfikator sieci VLAN dla źródłowej partycji logicznej.

-Z Określa identyfikator sieci VLAN dla docelowej partycji logicznej.

Status wyjścia

Ta komenda zwraca następujące wartości wyjścia:

0 Pomyślne zakończenie.

>0 Wystąpił błąd.

Przykłady

1. Aby zmienić poprawną regułę filtrowania, która istnieje w jądrze, wpisz następującą komendę:
   ```
   chvfilt -n 1 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```
2. Jeśli reguły filtrowania (n=2) nie ma w jądrze, dane wyjściowe będą następujące:
   ```
   chvfilt -n 2 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

   System wyświetli następujące dane wyjściowe:
   ```
   ioctl(QUERY_FILTER) failed no filter rule err=2
   Cannot Change the filter rule.
   ```

Komenda genvfilt

Przeznaczenie

Dodaje regułę filtrowania dla wirtualnej sieci LAN (VLAN) łączącej partycje logiczne na tym samym serwerze IBM Power Systems.

Składnia

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

Opis

Komenda **genvfilt** dodaje regułę filtrowania dla wirtualnej sieci LAN (VLAN) łączącej partycje logiczne na tym samym serwerze IBM Power Systems server.

Opcje

-a Określa działanie. Poprawne wartości to:
- D (Deny): blokuje ruch
- P (Permit): zezwala na ruch

-c Określa protokoły, do których ma zastosowanie reguła filtrowania. Poprawne wartości to:
- udp
- icmp
- icmpv6

- tcp
- any

-d Określa adres docelowy w formacie v4 lub v6.

-m Określa maskę adresu źródłowego.

-M Określa maskę adresu docelowego.

-o Określa port źródłowy lub typ operacji dla protokołu ICMP (Internet Control Message Protocol). Poprawne wartości to:
- lt
- gt
- eq
- any

-O Określa port docelowy lub kod ICMP. Poprawne wartości to:
- lt
- gt
- eq
- any

-p Określa port źródłowy lub typ ICMP.

-P Określa port docelowy lub kod ICMP.

-s Określa adres źródłowy w formacie IPv4 lub IPv6.

-v Określa wersję protokołu IP dla tabeli reguł filtrowania. Poprawne wartości to 4 i 6.

-z Określa identyfikator sieci wirtualnej dla źródłowej partycji logicznej. Identyfikator wirtualnej sieci LAN musi zawierać się w zakresie od 1 do 4096.

-Z Określa identyfikator sieci wirtualnej dla docelowej partycji logicznej. Identyfikator wirtualnej sieci LAN musi zawierać się w zakresie od 1 do 4096.

Status wyjścia

Ta komenda zwraca następujące wartości wyjścia:

0 Pomyślne zakończenie.

>0 Wystąpił błąd.

Przykłady

1. Aby dodać regułę filtru, która przepuszcza dane TCP ze źródła sieci VLAN o identyfikatorze 100 do docelowej sieci VLAN o identyfikatorze 200 na określonych portach, wpisz następującą komendę:

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

Odsyłacze pokrewne:

“Komenda mkvfilt” na stronie 158

“Komenda vlantfw” na stronie 177

Komenda lsvfilt

Przeznaczenie

Wyświetla listę reguł filtrowania dotyczących komunikacji między wirtualnymi sieciami LAN.

Składnia

lsvfilt [**-a**]

Opis

Komenda **lsvfilt** służy do wyświetlania listy reguł filtrowania dotyczących komunikacji między wirtualnymi sieciami LAN oraz ich statusu.

Opcje

-a Wyświetla tylko aktywne reguły filtrowania.

Status wyjścia

Ta komenda zwraca następujące wartości wyjścia:

0 Pomyślne zakończenie.

>0 Wystąpił błąd.

Przykłady

1. Aby wyświetlić wszystkie aktywne reguły filtrowania w jądrze, wpisz następującą komendę:

   ```
   lsvfilt -a
   ```

Pojęcia pokrewne:

"Dezaktywowanie reguł" na stronie 113
Można dezaktywować reguły, które umożliwiają routing danych między sieciami VLAN w zaufanym firewallu.

Komenda mkvfilt

Przeznaczenie

Aktywuje reguły filtrowania dotyczące komunikacji między wirtualnymi sieciami LAN (VLAN), zdefiniowane za pomocą komendy **genvfilt**.

Składnia

mkvfilt -u

Opis

Komenda **mkvfilt** aktywuje reguły filtrowania dotyczące komunikacji między sieciami VLAN, które zostały zdefiniowane za pomocą komendy **genvfilt**.

Opcje

-u Aktywuje reguły filtrowania w tabeli reguł filtrowania.

Status wyjścia

Ta komenda zwraca następujące wartości wyjścia:

0 Pomyślne zakończenie.

>0 Wystąpił błąd.

Przykłady

1. Aby aktywować reguły filtrowania w jądrze, wpisz następującą komendę:

```
mkvfilt -u
```

Odsyłacze pokrewne:

"Komenda genvfilt" na stronie 156

Komenda pmconf

Przeznaczenie

Raportuje i zarządza serwerem zaufanej sieci i zarządzania poprawkami (TNCPM) serwera, rejestruje wersje oprogramowania i pobiera informacje o najnowszych poprawkach, a także generuje raporty o statusie TNCPM.

| **Uwaga:** Serwer TNCPM może być uruchomiony tylko w systemie AIX wersja 7.2 z pakietem serwisowym 7100-02,
| który umożliwia pobieranie metadanych dla pakietu serwisowego.

Składnia

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

pmconf rmtncpm

pmconf start

pmconf stop

pmconf init -i <*okres pobierania*> **-l** <*TL List*> **-A** [**-P** <*ścieżka pobierania*>] [**-x** <*okres ifix*>] [**-K** <*klucz ifix*>]

pmconf add -l *lista_TL*

pmconf add -o <*nazwa pakietu*> -V <*wersja*> -T [installp|rqm] -D <*ścieżka definiowana przez użytkownika*>

pmconf add -p <*SP List*> [**-U** <*ścieżka SP definiowana przez użytkownika*>]

pmconf add -p <*SP*> **-e** <*plik ifix*>

pmconf add -y <*plik zaleceń*> **-v** <*plik sygnatury*> **-e**

pmconf chtncpm atrybut = *wartość*

pmconf delete -l <*lista TL*>

pmconf delete -o <*nazwa pakietu*> -V <*wersja*>

pmconf delete -p <*lista SP*>

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

pmconf export -f *nazwa_pliku*

| **pmconf get** -o <pakiet> -V <wersja> -T <installp | rpm> -D <katalog pobierania>

| **pmconf get** -L -o <pakiet> -V <wersja | all> -T <installp | rpm>

| **pmconf get** -L -p <SP>

pmconf get -p <SP> -D <katalog pobierania>

pmconf hist -d

pmconf hist -u

pmconf import -f *nazwa_pliku_cert* **-k** *nazwa_pliku_klucza*

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

pmconf list -a *SP*

pmconf list -C

pmconf list -l *SP*

pmconf list -o <*nazwa pakietu*> -V <*wersja*>

pmconf list -o [-c] [-q]

pmconf log loglevel = info | error | none

pmconf modify -i < *okres_pobierania*>

pmconf modify -P <*ścieżka pobierania*>

pmconf modify -g <*yes lub no, aby zaakceptować wszystkie licencje*>

pmconf modify -t <*lista typów APAR*>

pmconf modify -x <*odstęp czasu ifix*>

pmconf modify -K <*klucz ifix*>

pmconf proxy display

pmconf proxy [enable=yes | no] [host=<nazwa hosta>] [port=<port>]

pmconf restart

pmconf status

Opis

Funkcje komendy **pmconf** są następujące:

Zarządzanie repozytorium poprawek
Rejestruje lub wyrejestrowuje poziomy poprawek; wyrejestrowuje serwery TNC. TNCPM tworzy repozytorium poprawek dla każdego poziomu poprawek, w którym są zapisywane najnowsze poprawki, informacje **lslpp** (na przykład informacje o zainstalowanych zestawach plików lub zestawach plików aktualizacji) i informacje o odpowiednich dla tego poziomu poprawkach bezpieczeństwa.

Raportowanie
Generuje raporty na temat statusu TNCPM.

Przy użyciu komendy **pmconf** można wykonać następujące operacje:

Opcja	Opis
add	Rejestruje nowy poziom poprawek za pomocą TNCPM.
chtncpm	Zmienia atrybuty w pliku tnccs.conf. W celu uwzględnienia zmian w serwerze TNCPM wymagane jest jawne podanie komendy **start**.
delete	Wyrejestrowuje poziom poprawek za pomocą TNCPM.
get	Wyświetla lub pobiera informacje na temat dostępnych poprawek bezpieczeństwa i pakietów Open Source.
history	Wyświetla historię aktualizacji i pobierania.
list	Wyświetla informacje na temat TNCPM.
log	Ustawia poziom rejestrowania dla komponentów TNC.
mktncpm	Tworzy serwer TNCPM.
modify	Modyfikuje atrybuty w pliku tncpm.conf.
proxy	Zarządza konfiguracją parametrów serwera proxy.
rmtncpm	Usuwa serwer TNCPM.
start	Uruchamia serwer TNCPM.
stop	Zatrzymuje serwer TNCPM.

Opcje

Opcja	Opis
-A	Akceptuje wszystkie umowy licencyjne podczas wykonywania aktualizacji klienta.
-a <plik zaleceń>	Określa plik zaleceń, który odpowiada parametrowi **ifix**. Jeśli plik zaleceń nie zostanie podany, parametr **ifix** nie jest wyświetlany jako adres CVE (Common Vulnerabilities and Exposures) poprawki tymczasowej.
-a *SP*	Generuje raport poprawek APAR dla pakietu serwisowego. *SP* jest w formacie REL00-TL-SP (na przykład 6100-01-04 reprezentuje pakiet serwisowy 04 dla pakietu poprawek 01 i wersji 6.1).
-e <plik ifix>	Określa poprawki tymczasowe, które zostały dodane do TNCPM.
-i *przedział_czasu_pobierania*	Określa odstęp czasu, co który demon TNCPM sprawdza, czy pojawiły się nowe pakiety serwisowe dla zarejestrowanych pakietów poprawek. Odstęp czasu jest liczbą całkowitą, która reprezentuje czas w następującym formacie: **d** (liczba dni): **h** (godziny): **m** (minuty). Obsługiwany zakres dla *przedziału_czasu_pobierania* wynosi 30 - 525600 minut.
-K <klucz ifix>	Określa klucz publiczny narzędzia IBM AIX Product Security Incident Response Tool (PSIRT), który służy do uwierzytelniania pobranych zaleceń i poprawek tymczasowych. Ten klucz publiczny może zostać pobrany z publicznego serwera kluczy PGP za pomocą identyfikatora **0x28BFAA12**.
-L	Określa tylko tryb listowania lub wyszukiwania.
o *nazwa pakietu*	Nazwa pakietu Open Source, który ma zostać wyszukany lub pobrany.
-P *ścieżka_repozytorium_poprawek*	Określa katalog pobierania dla repozytoriów poprawek, który będą pobierane przez TNCPM. Katalogiem domyślnym jest **/var/tnc/tncpm/repozytorium poprawek**.
-p *lista_SP*	Określa listę pakietów serwisowych do pobrania. Jest to lista rozdzielana przecinkami w formacie REL00-TL-SP (na przykład 6100-01-04 reprezentuje pakiet serwisowy 04 dla pakietu poprawek 01 i wersji 6.1). W przypadku użycia opcji -U należy podać tylko jeden pakiet serwisowy.
-t *lista_typów_APAR*	Określa typy poprawek APAR, które TNCPM obsługuje dla aktualizacji klienta i nasłuchiwania serwera TNC. Poprawki dotyczące bezpieczeństwa są zawsze obsługiwane. lista_typów_APAR to rozdzielona przecinkami lista następujących typów: HIPER, FileNet Process Engine, Enhancement.
T *typ pakietu*	Określa typ pakietu Open Source do wyszukania lub pobrania
-U *repozytorium_poprawek_użytkownika*	Określa ścieżkę do repozytorium poprawek zdefiniowanego przez użytkownika. Określ wersję, poziom poprawek i pakiet serwisowy, które będą powiązane z repozytorium poprawek używanym do sprawdzania i aktualizowania klientów.
-s	Generuje raport dla zarejestrowanych pakietów serwisowych.
-l *SP*	Generuje raport informacji **lslpp** dla pakietu serwisowego. *SP* jest w formacie REL00-TL-SP (na przykład 6100-01-04 reprezentuje pakiet serwisowy 04 dla pakietu poprawek 01 i wersji 6.1).
-u	Generuje raport historii aktualizacji klienta.
V *wersja*	Wersja pakietu Open Source, który ma zostać wyszukany lub pobrany. W trybie wyszukiwania (-L) wartość "all" pozwala wyszukać wszystkie dostępne wersje podanego pakietu.
-d	Generuje raport historii pobierania pakietów serwisowych.
-C	Generuje raport dla certyfikatu serwera.
-f *nazwa_pliku*	Określa nazwę pliku certyfikatu.
-k	Określa plik, z którego ma być zaimportowany klucz certyfikatu.

-c	Wyświetla atrybuty użytkownika w postaci rekordów rozdzielanych dwukropkami, w następujący sposób:
	`# nazwa: atrybut1: atrybut2: ...`
	`strategia: wartość1: wartość2: ...`

-v <*plik_sygnatur*>	Określa plik sygnatury dla zalecenia IBM dotyczącego słabego punktu zabezpieczeń systemu AIX.
-y <*plik_zaleceń*>	Określa plik zaleceń IBM AIX dotyczących słabego punktu zabezpieczeń.
-q	Blokuje informacje nagłówka.

Opcja	Opis
-x <*odstęp czasu ifix*>	Określa odstęp czasu w minutach dla sprawdzania i pobierania nowych poprawek tymczasowych. Jeśli ta wartość zostanie ustawiona na 0, funkcja automatycznego pobierania poprawek tymczasowych i powiadomień będzie wyłączona. Domyślny przedział czasu wynosi 24 godziny. Obsługiwany zakres dla <*odstępu czasu ifix*> wynosi 30 - 525600 minut.

Status wyjścia

Ta komenda zwraca następujące wartości wyjścia:

Opcja	Opis
0	Komenda została pomyślnie wykonana i wszystkie żądane zmiany zostały wprowadzone.
>0	Wystąpił błąd. Wyświetlony komunikat o błędzie zawiera więcej szczegółowych informacji na temat typu niepowodzenia.

Przykłady

1. Aby zainicjować TNCPM, wpisz następującą komendę:
   ```
   pmconf init -f 10080 -l 5300-11,6100-00
   ```
2. Aby utworzyć demona TNCPM, wpisz następującą komendę:
   ```
   mktncpm pmport=55777 tncserver=11.11.11.11:77555
   ```
3. Aby uruchomić serwer, wprowadź następującą komendę:
   ```
   pmconf start
   ```
4. Aby zatrzymać serwer, wprowadź następującą komendę:
   ```
   pmconf stop
   ```
5. Aby zarejestrować nowy pakiet poprawek za pomocą TNCPM, wprowadź następującą komendę:
   ```
   pmconf add -l 6100-01
   ```
6. Aby wyrejestrować pakiet poprawek za pomocą TNCPM, wprowadź następującą komendę:
   ```
   pmconf delete -l 6100-01
   ```
7. Aby wyrejestrować z TNCPM serwer TNC, który ma adres IP 11.11.11.11, wprowadź następującą komendę:
   ```
   pmconf delete -t 11.11.11.11
   ```
8. Aby zarejestrować w TNCPM nowszą wersję wcześniejszego pakietu serwisowego, wprowadź następującą komendę:
   ```
   pmconf add -s 6100-01-04
   ```
9. Aby wyrejestrować z TNCPM wcześniejszą wersję pakietu poprawek, wprowadź następującą komendę:
   ```
   pmconf delete -s 6100-01-04
   ```
10. Aby wygenerować raport dotyczący repozytoriów poprawek dla każdego zarejestrowanego pakietu poprawek, wprowadź następującą komendę:
    ```
    pmconf list -s
    ```
11. Aby wygenerować raport dotyczący informacji **lslpp** dla zarejestrowanego poziomu poprawek, wpisz następującą komendę:
    ```
    pmconf list -l 6100-01-02
    ```
12. Aby wygenerować raport dotyczący historii aktualizacji, wprowadź następującą komendę:
    ```
    pmconf hist -u
    ```
13. Aby wygenerować raport dotyczący historii pobierania, wprowadź następującą komendę:
    ```
    pmconf hist -d
    ```
14. Aby wygenerować raport dotyczący certyfikatu serwera, wprowadź następującą komendę:
    ```
    pmconf list -C
    ```
15. Aby wygenerować raport dla pakietu poprawek APAR dotyczącego zabezpieczeń, wprowadź następującą komendę:
    ```
    pmconf list -a 6100-01-02
    ```

16. Aby zaimportować certyfikat serwera, wprowadź następującą komendę:
    ```
    pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt
    ```
17. Aby wyeksportować certyfikat serwera, wprowadź następującą komendę:
    ```
    pmconf export -f /tmp/server.txt
    ```
18. Aby wyświetlić wszystkie dostępne wersje pakietów rpm programu open source ‘emacs’, wprowadź następującą komendę:
    ```
    pmconf get -L -o emacs -V all -T rpm
    ```
19. Aby pobrać wersję 4.5.1 pakietu open source ‘lsof’ w formacie rpm do katalogu /tmp/new_lsof, wprowadź następującą komendę:
    ```
    mkdir /tmp/new_lsof
    pmconf get -o lsof -V 4.5.1 -T rpm -D /tmp/new_lsof
    ```
20. Aby wyświetlić wszystkie dostępne wersje programu OpenSSH w formacie installp, wprowadź następującą komendę:
    ```
    pmconf get -o openssh -T installp -L -V all
    ```
21. Aby wyświetlić bieżące ustawienia konfiguracji proxy, które będą używane przez program cURL do pobierania pakietów Open Source lub poprawek bezpieczeństwa, wprowadź następującą komendę:
    ```
    pmconf proxy display
    ```
22. Aby wyłączyć konfigurację proxy, wprowadź następującą komendę:
    ```
    pmconf proxy enable=no
    ```
23. Aby włączyć i ustawić proxy na host ‘myProxyServer’ i port 9876, wprowadź następującą komendę:
    ```
    pmconf proxy enable=yes host=myProxyServer port=9876
    ```
24. Aby zmienić port serwera proxy, wprowadź następującą komendę:
    ```
    pmconf proxy port=1234
    ```
25. Aby wyświetlić znane słabe punkty usuwane przez poprawki bezpieczeństwa dla pakietu serwisowego 7100-03-02, wprowadź następującą komendę:
    ```
     pmconf get -L -p 7100-03-02
    ```
26. Aby pobrać do katalogu /tmp/ifixes_for_7.2.0.1 (bez instalowania) poprawki bezpieczeństwa dla pakietu serwisowego 7200-00-01, wprowadź następujące komendy:
    ```
    mkdir /tmp/ifixes_for_7.2.0.1
    pmconf get -p 7200-00-01 -D /tmp/ifixes_for_7.2.0.1
    ```

Komenda psconf

Przeznaczenie

Raportuje i zarządza serwerem zaufanej sieci (TNC), klientem TNC, odsyłaczem IP dla TNC (IPRef) i programem SUMA (Service Update Management Assistant). Zarządza strategiami zarządzania zestawami plików i poprawek w celu zachowania integralności punktu końcowego (serwera i klienta) podczas lub po zakończeniu połączenia sieciowego w celu ich ochrony przed atakami i zagrożeniami sieciowymi.

Składnia

Operacje serwera TNC:

psconf mkserver [**tncport=**<*port*>] **pmserver=**<*host:port*> [tsserver=<host>] [**recheck_interval=**<*czas_w_minutach*> | **d** (dni) : **h** (godziny) : **m** (minuty)] [**dbpath** = <*katalog_zdefiniowany_przez_użytkownika*>] [**default_policy=**<*yes* | *no* >] [**clientData_interval=**<*czas_w_minutach*> | **d** (dni) : **h** (godziny) : **m** (minuty)] [**clientDataPath=**<*pełna_ścieżka*>]

psconf { **rmserver | status** }

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

psconf chserver attribute = *wartość*

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

psconf add -F <*nazwa_strategii_FS*> -r <*inf_wersji*> [**apargrp=** [**±**]<*apargrp1, apargrp2.. >*] [*ifixgrp*=[+|-]<*grupa_popr_tymcz1,grupa_popr_tymcz2...>*]

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

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

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

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

psconf delete { **-F** <*nazwa_strategii_FS*> | **-G** <*nazwa_grp_ip*> | **-P** <*nazwa_strategii*> | **-A** <*grp_apar*> | **-V** <*grp_ifix*>}

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

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

psconf certdel -i <*host*>

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

psconf update [-p] {**-i**<*host*>| **-G** <*grupa_IP*>[**-r** <*informacje_o_kompilacji*> | **-a** <*apar1, apar2...*> | [**-u**] **-v** <*popr_tymcz_1, popr_tymcz_2,...*> | **-O** <*grupa_openpkg1, grupa_openpkg2,...>*}

psconf log loglevel=<info | error | none>

psconf import -C -i <*host*> **-f** <*nazwa_pliku*> | **–d** <*nazwa pliku bazy danych importowania*>

psconf { **import -k** <*nazwa_pliku_klucza*> | **export**} **-S -f** <*nazwa_pliku*>

psconf list { **-S** | **-G** < *nazwa_grupy_IP* | **ALL** > | **-F** < *nazwa_strategii_FS* | **ALL** > | **-P** < *nazwa_strategii* | **ALL** > | **-r** < *informacje_o_kompilacji* | **ALL** > | **-I -i** < *ip* | **ALL** > | **-A** < *grupa_apar* | **ALL** > | **-V** <*grupa_popr_tymcz*> | -O <*grupa_openpkg|ALL*>} [**-c**] [**-q**]

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

psconf export -d <ścieżka do katalogu eksportowania>

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

psconf report -A <nazwa_zalecenia>

psconf report -P <nazwa_strategii|ALL> -o <TEXT|CSV>

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

psconf report -B <inf_wersji|ALL> -o <TEXT|CSV>

psconf clientData {-l | -g} -i <*IP*|*host*>

psconf add -O <*grupa_openpkg*> <*nazwa_openpkg:wersja*>

psconf delete -O <*grupa_openpkg*> <*nazwa_openpkg:wersja*>

psconf delete -O <*grupa_openpkg*>

psconf delete -O ALL

psconf add -O <*grupa_openpkg*> fspolicy=<*nazwa strategii FS*>

psconf report -O ALL -o TEXT

| **psconf add -V <*grupa_popr_tymcz*> autoupdate=<yes|no>**

| **psconf reboot -i <*host*> last one**

Operacje klienta TNC:

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

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

psconf { **rmclient | status** }

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

psconf chclient atrybut = *wartość*

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

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

psconf import { **-S | -C -k** <*nazwa_pliku_klucza*> } **-f** <*nazwa_pliku*>

Operacje IPRef TNC:

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

psconf { **rmipref | status** }

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

psconf chipref attribute = *wartość*

psconf { **import -k** <*nazwa_pliku_klucza*> **| export** } **-R -f** <*nazwa_pliku*>

psconf list -R

Opis

Technologia TNC jest architekturą wykorzystującą otwarte standardy do uwierzytelniania punktu końcowego, określania integralności platformy oraz integracji systemów zabezpieczeń. Architektura TNC sprawdza zgodność punktów końcowych (klientów sieciowych i serwerów) ze strategiami bezpieczeństwa przed zezwoleniem na ich podłączenie do chronionej sieci. Program TNC IPRef powiadamia serwer TNC o wszystkich nowych adresach IP, które zostały wykryte na wirtualnym serwerze we/wy (VIOS).

Mechanizm SUMA zwalnia administratorów systemu z obowiązku ręcznego pobierania aktualizacji i poprawek z sieci WWW. Oferuje on elastyczne opcje, które umożliwiają administratorowi systemu skonfigurowanie zautomatyzowanego interfejsu do pobierania poprawek z dystrybucyjnych serwisów WWW do swoich systemów.

Komenda **psconf** zarządza serwerem sieciowym i klientami umożliwiając dodawanie lub usuwanie strategii bezpieczeństwa, sprawdzanie poprawności klientów jako zaufanych lub niezaufanych, generowanie raportów oraz aktualizowanie serwera i klienta.

Przy użyciu komendy **psconf** można wykonać następujące operacje:

Opcja	Opis
add	Dodaje strategię, klienta, albo informacje e-mail na serwerze TNC.
apargrp	Określa nazwy grup APAR jako część strategii dla zestawu plików, które są używane na potrzeby weryfikacji klientów TNC.
aparlist	Określa listę raportów APAR, które są częścią grupy APAR.
certadd	Zaznacza certyfikat jako zaufany lub niezaufany.
certdel	Usuwa informacje dotyczące klienta.
chclient	Zmienia atrybuty w pliku tnccs.conf. W celu uwzględnienia zmian w kliencie TNC wymagane jest jawne podanie komendy **start**. Składnia atrybut=wartość będzie taka sama, jak dla komendy **mkclient**.
chipref	Zmienia atrybuty w pliku tnccs.conf. W celu uwzględnienia zmian w demonie IPRef wymagane jest jawne podanie komendy **start**. Składnia atrybut=wartość będzie taka sama, jak dla komendy **mkipref**.
chserver	Zmienia atrybuty w pliku tnccs.conf. W celu uwzględnienia zmian w serwerze TNC wymagane jest jawne podanie komendy **start**. Składnia atrybut=wartość będzie taka sama, jak dla komendy **mkserver**. **Uwaga:** Atrybutu **dbpath** nie można zmienić za pomocą komendy **chserver**. Można go ustawić tylko podczas uruchamiania komendy **mkserver**.
clientData	Tworzy obraz stanu informacji (poziom systemu operacyjnego i zainstalowane zestawy plików) na temat klienta TNC. Ścieżka *clientDataPath* określa miejsce, w którym przechowywane są zgromadzone obrazy stanu. Położeniem domyślnym jest katalog /var/tnc/clientData/ na serwerze TNC. Ścieżkę *clientDataPath* można zmienić lub ustawić za pomocą podkomendy **chserver** lub **mkserver**. Gromadzenie obrazów stanu klienta TNC można zainicjować za pomocą wiersza komend lub przez uruchomienie podkomendy **clientData** na serwerze TNC. Podkomenda **clientData** uruchamiana za pomocą wiersza komend nie zależy od przedziału czasu **clientData_interval**.
clientData_interval	Za pomocą podkomendy **chserver** lub **mkserver** można skonfigurować gromadzenie obrazów stanu w regularnych odstępach czasu, podając wartość dla odstępu czasu **clientData_interval**. Gromadzenie obrazów stanu rozpoczyna się automatycznie, gdy odstęp czasu **clientData_interval** ma wartość inną niż 0 (zero). Domyślnie gromadzenie obrazów stanu jest wyłączone przez program planujący. Aby włączyć ten program planujący, dla parametru **clientData_interval** podaj wartość większą lub równą 30. Aby wyłączyć ten program planujący, dla parametru **clientData_interval** podaj wartość 0 (zero). Dla odstępu czasu **clientData_interval** obsługiwane są wartości z zakresu od 30 do 525600 minut.
dbpath	Określa położenie bazy danych TNC. Wartością domyślną jest /var/tnc.
default_policy	Włącza lub wyłącza automatyczne weryfikowanie, czy klienty TNC mają poprawki tymczasowe (ifix) i raporty APAR na tym samym poziomie co klient. Podaj wartość *yes*, aby włączyć automatyczne weryfikowanie. Podaj wartość *no*, aby wyłączyć automatyczne weryfikowanie. Więcej informacji na temat podkomendy **default_policy** zawiera Tabela default_policy.
delete	Usuwa strategię lub informacje dotyczące klienta.

Opcja	Opis
export	Eksportuje certyfikat klienta lub serwera lub bazę danych na serwerze TNC.
fspolicy	Określa strategię zestawu plików dla wydania, poziomu poprawek i pakietu serwisowego, które mają być używane przy weryfikacji klientów TNC.
import	Importuje certyfikat na kliencie lub serwerze, lub bazę danych na serwerze TNC.
ipgroup	Określa grupę IP, która zawiera wiele adresów IP lub nazw hostów klientów.
list	Wyświetla informacje na temat serwera TNC, klienta TNC, lub SUMA.
log	Ustawia poziom rejestrowania dla komponentów TNC.
mkclient	Konfiguruje klienta TNC.
mkipref	Konfiguruje demona TNC IPRef.
mkserver	Konfiguruje serwer TNC.
grupa_openpkg	Określa nazwę grupy openpkg jako część strategii dla zestawów plików używanej do weryfikowania klientów.
pmport	Określa numer portu, na którym nasłuchuje serwer **pmserver**. Wartością domyślną jest 38240.
pmserver	Określa nazwę hosta lub adres IP komendy **suma**, która pobiera najnowsze pakiety poprawek i poprawki bezpieczeństwa dostępnych w serwisie WWW IBM® ECC i serwisie WWW IBM Fix Central.
reboot	Restartuje klienta TNC, który jest identyfikowany za pomocą adresu IP w zmiennej <*host*>.
recheck_interval	Określa odstęp czasu w dniach (d) , godzinach (h) lub minutach (m), co jaki serwer TNC ma weryfikować klienty TNC. Dla odstępu czasu **recheck_interval** obsługiwane są wartości z zakresu od 30 do 525600 minut. **Uwaga:** Wartość **recheck_interval=0** oznacza, że program planujący nie będzie inicjował weryfikacji klientów w regularnych odstępach czasu i zarejestrowane klienty będą automatycznie weryfikowane podczas ich uruchamiania. W takich przypadkach klient może zostać zweryfikowany ręcznie.
report	Generuje raport, który ma rozszerzenie pliku .txt lub .csv.
restart	Restartuje klienta TNC, serwer TNC, lub demon TNC IPRef.
rmclient	Dekonfiguruje klienta TNC.
rmipref	Dekonfiguruje TNC IPRef.
rmserver	Dekonfiguruje serwer TNC.
start	Uruchamia klienta TNC, serwer TNC, lub demon TNC IPRef.
status	Wyświetla status konfiguracji TNC.
stop	Zatrzymuje klienta TNC, serwer TNC, lub demon TNC IPRef.
tncport	Określa numer portu, na którym nasłuchuje serwer TNC. Wartością domyślną jest 42830.
tncserver	Określa serwer TNC, który sprawdza lub aktualizuje klienty TNC.
tssserver	Określa adres IP lub nazwę hosta serwera Trusted Surveyor.
update	Instaluje poprawki na kliencie.
verify	Inicjuje samodzielną weryfikację klienta.

W poniższej tabeli przedstawiono wyniki skonfigurowania wartości *yes* lub *no* dla podkomendy **default_policy**:

Tabela 16. Wyniki dla podkomendy default_policy

FSpolicy (strategia dla zestawów plików)	**default policy=***yes*	**default policy=***no*
Klient TNC należy do strategii dla zestawów plików ze zdefiniowanymi grupami poprawek tymczasowych (iFix) i raportów APAR	Strategia domyślna jest zastępowana przez poprawki tymczasowe (iFix) i raporty APAR udostępnione w strategii dla zestawów plików.	Domyślna strategia nie jest używana. Poprawki tymczasowe (iFix) i raporty APAR dostarczone w strategii dla zestawów plików są brane pod uwagę podczas procesu weryfikowania dla klienta TNC.

Tabela 16. Wyniki dla podkomendy default_policy (kontynuacja)

FSpolicy (strategia dla zestawów plików)	default policy=*yes*	default policy=*no*
Klient TNC należy do strategii dla zestawów plików bez zdefiniowanych grup poprawek tymczasowych (iFix) i raportów APAR	Podczas procesu weryfikowania dla klienta TNC używana jest strategia domyślna z poprawkami tymczasowymi (iFix) i raportami APAR. Podczas procesu weryfikowania używane są tylko te poprawki tymczasowe (iFix) i raporty APAR, które są zgodne z poziomem klienta TNC.	Domyślna strategia nie jest używana.

Opcje

Opcja	Opis
-A <advisoryName>	Określa nazwę zalecenia dla raportu.
-B <inf_wersji>	Określa informacje o kompilacji, aby przygotować raport poprawek.

-c	Wyświetla atrybuty użytkownika w postaci rekordów rozdzielanych dwukropkami, w następujący sposób:
	`# nazwa: atrybut1: atrybut2: ...`
	`strategia: wartość1: wartość2: ...`

-C	Określa, że operacja jest wykonywana dla komponentu klienta.
-d *położenie pliku bazy danych/ścieżka bazy danych*	Określa ścieżkę pliku dla importowania bazy danych/określa położenie ścieżki katalogu dla eksportowania z bazy danych.
-D *rrrr-mm-dd*	Określa datę dla pozycji określonego klienta w dzienniku historii, gdzie *rrrr* oznacza rok, *mm* miesiąc, a *dd* jest dniem.
-e *e-mail* **ipgroup=**[**±**]*g1, g2...*	Określa adres poczty elektronicznej, po którym następuje rozdzielona przecinkami lista nazw grup IP.
-E | FAIL | COMPLIANT | ALL |	Określa zdarzenie, dla którego ma zostać wysłana wiadomość e-mail do skonfigurowanego adresata poczty elektronicznej. FAIL - wiadomości e-mail są wysyłane, gdy statusem weryfikacji klienta jest niepowodzenie. COMPLIANT - wiadomości e-mail są wysyłane, gdy statusem weryfikacji klienta jest zgodność. ALL - wiadomości e-mail są wysyłane dla wszystkich statusów weryfikacja klienta.
-f *nazwa_pliku*	Określa plik, z którego ma zostać odczytany certyfikat w przypadku operacji importowania lub określa miejsce, do którego certyfikat musi być zapisany w przypadku operacji eksportowania.
-F *strategia_fspolicy inf_wersji*	Określa nazwę strategii dla systemu plików, a po niej informacje o kompilacji. Informacje o kompilacji można podać w następującym formacie: 6100-04-01, gdzie 6100 reprezentuje wersję 6.1, 04 jest poziomem konserwacji, a 01 jest pakietem serwisowym.
-g	Uruchom podkomendę **clientData** w określonym kliencie TNC. Ta opcja jest dostępna tylko dla podkomendy **clientData**.
-G*ipgroupname* **ip=**[**±**]*ip1, ip2...*	Określa nazwę grupy IP, po której następuje rozdzielana przecinkami lista adresów IP.
-H	Wyświetla dziennik historii.
-i *host*	Określa adres IP lub nazwę hosta.
-I ip=[**±**]*ip1, ip2...* | [±] host1,host2...	Określa adres IP/nazwę hosta, które muszą zostać zignorowane podczas weryfikacji.
-k *nazwa_pliku*	Określa plik, z którego ma być zaimportowany klucz certyfikatu dla operacji importowania.
-l	Wyświetla szczegóły obrazu stanu na serwerze TNC dla określonego klienta TNC. Ta opcja jest dostępna tylko dla podkomendy **clientData**.
-O <grupa_openpkg>	Określa nazwę grupy openpkg dla strategii.
-p	Podgląd aktualizacji klienta TNC.
-P <nazwaStrategii>	Określa nazwę strategii, dla której należy przygotować raport strategii klienta.
-q	Blokuje informacje nagłówka.
-r *inf_wersji*	Generuje raport przy wykorzystaniu informacji o kompilacji. Informacje o kompilacji można podać w następującym formacie: 6100-04-01, gdzie 6100 reprezentuje wersję 6.1, 04 jest poziomem konserwacji, a 01 jest pakietem serwisowym.
-R	Określa, że operacja jest wykonywana dla komponentu IPRef.

Opcja	Opis
-s COMPLIANT | IGNORE | FAILED | ALL	Wyświetla klienty według statusu w następujący sposób: **COMPLIANT** Wyświetla aktywne klienty. **IGNORE** Wyświetla klienty, które są wykluczone z weryfikacji. **FAILED** Wyświetla klienty, dla których nie powiodły się weryfikacja zgodnie ze skonfigurowaną strategię. **ALL** Wyświetla listę wszystkich klientów, niezależnie od ich statusu.
-S <host>	Określa nazwę hosta, dla którego należy przygotować raport poprawek bezpieczeństwa.
-t TRUSTED | UNTRUSTED	Zaznacza podanego klienta jako zaufanego lub niezaufanego. **Uwaga:** Tylko administratorzy systemu mogą określić serwery lub klienty jako zaufane lub niezaufane.
-T	Określa, że klient może akceptować żądania z dowolnego serwera TS, który ma poprawny certyfikat.
-u	Deinstaluje poprawkę tymczasową, która jest zainstalowana na kliencie TNC.
-v<*CVEid|ALL*>	Wyświetla często spotykane zagrożenia i narażenia dla zarejestrowanych pakietów serwisowych. **CVEid** **All** Wyświetla wszystkie często spotykane zagrożenia i narażenia dla zarejestrowanych pakietów serwisowych.
-v<*popr_tymcz_1, popr_tymcz_2,...*>	Określa rozdzielaną przecinkami listę poprawek tymczasowych.
-V<*grupa_popr_tymcz*>	Określa nazwę grupy poprawek tymczasowych.
-V <*grupa_popr_tymcz*> autoupdate=<yes|no>	Określa, czy poprawki tymczasowe w grupie poprawek tymczasowych o podanej nazwie są aktualizowane automatycznie. **Yes** Automatycznie aktualizuje strategię zdefiniowaną dla strategii FS, gdy na serwerze TNC zostaną odebrane nowe poprawki tymczasowe. **No** Określa, że nowe poprawki tymczasowe będą ręcznie przypisywane do strategii, gdy zostaną odebrane na serwerze TNC. No jest wartością domyślną.

Status wyjścia

Ta komenda zwraca następujące wartości wyjścia:

Opcja	Opis
0	Komenda została pomyślnie wykonana i wszystkie żądane zmiany zostały wprowadzone.
>0	Wystąpił błąd. Wyświetlony komunikat o błędzie zawiera więcej szczegółowych informacji na temat typu niepowodzenia.

Przykłady

1. Aby uruchomić serwer TNC, wprowadź następującą komendę:
   ```
   psconf start server
   ```
2. Aby dodać strategię systemu plików o nazwie 71d_latest dla kompilacji 7100-04-02, wpisz następującą komendę:
   ```
   psconf add -F 71D_latest 7100-04-02
   ```
3. Aby usunąć strategię systemu plików o nazwie 71d_old, wpisz następującą komendę:
   ```
   psconf delete -F 71D_old
   ```
4. Aby sprawdzić, czy klient, który ma adres IP 11.11.11.11 jest **zaufany**, wpisz następującą komendę:
   ```
   psconf certadd -i 11.11.11.11 -t TRUSTED
   ```
5. Aby usunąć z serwera klienta o adresie IP 11.11.11.11, wpisz następującą komendę:
   ```
   psconf certdel -i 11.11.11.11
   ```
6. Aby zweryfikować informacje o kliencie o adresie IP 11.11.11.11, wpisz następującą komendę:
   ```
   psconf verify -i 11.11.11.11
   ```
7. Aby wyświetlić informacje o kliencie o adresie IP 11.11.11.11, wpisz następującą komendę:
   ```
   psconf list -i 11.11.11.11
   ```
8. Aby wygenerować raport dla klientów, które są w stanie **COMPLIANT**, wprowadź następującą komendę:

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

9. Aby wygenerować raport dla kompilacji 7100-04-02, wpisz następującą komendę:
   ```
   psconf list -r 7100-04-02
   ```
10. Aby wyświetlić historię połączeń dla klienta o adresie IP 11.11.11.11, wpisz następującą komendę:
    ```
    psconf list -H -i 11.11.11.11
    ```
11. Aby usunąć z dziennika historii pozycje dla klienta o adresie IP 11.11.11.11 starsze lub równe niż data 1 lutego, 2009, wprowadź następującą komendę:
    ```
    psconf delete -H -i 11.11.11.11 -D 2009-02-01
    ```
12. Aby zaimportować z serwera certyfikat kliencki dla klienta o adresie IP 11.11.11.11, wpisz następującą komendę:
    ```
    psconf import -C -i 11.11.11.11 -f /tmp/client.txt
    ```
13. Aby wyeksportować certyfikat serwera z klienta, wprowadź następującą komendę:
    ```
    psconf export -S -f /tmp/server.txt
    ```
14. Aby zaktualizować z serwera klienta o adresie IP 11.11.11.11 do odpowiedniej wersji, wpisz następującą komendę:
    ```
    psconf update -i 11.11.11.11
    ```
15. Aby wyświetlić statusy klientów, wprowadź następującą komendę:
    ```
    psconf status
    ```
16. Aby wyświetlić certyfikat klienta, wprowadź następującą komendę:
    ```
    psconf list -C
    ```
17. Aby uruchomić klienta, wprowadź następującą komendę:
    ```
    psconf start client
    ```
18. Aby wyświetlić informacje o obrazach stanu zgromadzonych za pomocą podkomendy **clientData**, wprowadź następującą komendę:
    ```
    psconf clientData -l [IP|host]
    ```
19. Aby wyświetlić historię klienta TNC, wprowadź następującą komendę:
    ```
    psconf list –H –i [IP|ALL]
    ```

Zabezpieczenia

Uwaga dla użytkowników RBAC i użytkowników Trusted AIX:

Ta komenda umożliwia wykonanie operacji uprzywilejowanych. Operacje uprzywilejowane mogą wykonywać tylko użytkownicy uprzywilejowani. Więcej informacji na temat autoryzacji i uprawnień zawiera baza danych komend uprzywilejowanych w publikacji Privileged Command Database in Security. Listę uprawnień i autoryzacji powiązanych z tą komendą zawiera opisy komendy **lssecattr** lub **getcmdattr**.

Komenda pscuiserverctl

Przeznaczenie

Służy do konfigurowania opcji serwera interfejsu GUI produktu PowerSC.

Składnia

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]

Opcje

-r Restartuje serwer interfejsu GUI produktu PowerSC po zastosowaniu wartości parametru.

set
Ustawia lub pobiera wartość opcji serwera interfejsu GUI produktu PowerSC.

Parametry

httpPort *numer_portu_http*
Wyświetl lub określ domyślny port używany przez interfejs GUI produktu PowerSC.

httpsPort *numer_portu_https*
Wyświetl lub określ domyślny port chroniony używany przez interfejs GUI produktu PowerSC.

administratorGroupList *grupa_unix1,grupa_unix2,...*
Wyświetl lub podaj grupy w systemie UNIX, które mają uprawnienia do wykonywania funkcji administratora za pomocą interfejsu GUI produktu PowerSC.

logonGroupList *grupa_unix1,grupa_unix2,...*
Wyświetl lub podaj grupy w systemie UNIX, które mają uprawnienia do logowania się do interfejsu GUI produktu PowerSC.

powervcKeystoneUrl *adres_URL_magazynu_kluczy_powervc*
Wyświetl lub podaj adres URL serwera magazynu kluczy PowerVC.

QRadarSyslogResponseEnabled on | off
Wyświetl bieżące ustawienie rejestrowania Syslog z interfejsu GUI produktu PowerSC lub ustaw wartość on lub off dla rejestrowania Syslog.

tncServer *serwer_tnc.abc.com*
Wyświetl lub podaj nazwę hosta serwera TNC. Jeśli zostanie zmieniona nazwa hosta serwera TNC, należy zrestartować serwer interfejsu GUI produktu PowerSC.

Status wyjścia

Ta komenda zwraca następujące wartości wyjścia:

0 Pomyślne zakończenie.

>0 Wystąpił błąd.

Przykłady

1. Aby poznać domyślny port używany przez interfejs GUI produktu PowerSC:
   ```
   pscuiserverctl set httpPort
   ```
2. Aby ustawić domyślny port używany przez interfejs GUI produktu PowerSC:
   ```
   pscuiserverctl set httpPort 80
   ```
3. Aby poznać domyślny port chroniony używany przez interfejs GUI produktu PowerSC:
   ```
   pscuiserverctl set httpsPort
   ```
4. Aby ustawić domyślny port chroniony używany przez interfejs GUI produktu PowerSC:
   ```
   pscuiserverctl set httpsPort 483
   ```

5. Aby wyświetlić grupy w systemie UNIX, które mają uprawnienia do wykonywania funkcji administratora za pomocą interfejsu GUI produktu PowerSC:
   ```
   pscuiserverctl set administratorGroupList
   ```
6. Aby ustawić grupy w systemie UNIX, które mają uprawnienia do wykonywania funkcji administratora za pomocą interfejsu GUI produktu PowerSC:
   ```
   pscuiserverctl set administratorGroupList securitygroup1,admingrp1
   ```
7. Aby wyświetlić grupy w systemie UNIX, które mają uprawnienia do logowania się do interfejsu GUI produktu PowerSC:
   ```
   pscuiserverctl set logonGroupList
   ```
8. Aby ustawić grupy w systemie UNIX mające uprawnienia do logowania się do interfejsu GUI produktu PowerSC:
   ```
   pscuiserverctl set logonGroupList unixgroup1,unixgrp2
   ```
9. Aby sprawdzić adres URL serwera magazynu kluczy PowerVC:
   ```
   pscuiserverctl set powervcKeystoneUrl
   ```
10. Aby ustawić adres URL serwera magazynu kluczy PowerVC:
    ```
    pscuiserverctl set powervcKeystoneUrl https://powervc/server/example/
    ```
11. Aby sprawdzić, czy rejestrowanie Syslog z interfejsu GUI produktu PowerSC jest włączone, czy też wyłączone:
    ```
    pscuiserverctl set QRadarSyslogResponseEnabled
    ```
12. Aby ustawić rejestrowanie Syslog z interfejsu GUI produktu PowerSC na włączone lub wyłączone:
    ```
    pscuiserverctl set QRadarSyslogResponseEnabled on
    pscuiserverctl set QRadarSyslogResponseEnabled off
    ```
13. Aby sprawdzić nazwę hosta serwera TNC:
    ```
    pscuiserverctl set tncServer
    ```
14. Aby ustawić nazwę hosta serwera TNC:
    ```
    pscuiserverctl set tncServer tncserver.abc.com
    ```
15. Ustawienie nazwy hosta serwera TNC wymaga zrestartowania serwera interfejsu GUI produktu PowerSC. Aby zrestartować serwer interfejsu GUI produktu PowerSC:
    ```
    pscuiserverctl -r set tncServer tncs1.rs.com
    ```

Komenda pscxpert

Przeznaczenie

Pomaga administratorowi systemu w ustawieniu konfiguracji zabezpieczeń.

Składnia

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

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

pscxpert -f profil [**-p**] [**-r**|**-R**]

pscxpert -u [**-p**]

pscxpert -c [**-p**] [**-r**|**-R**] [**-P** profil] [**-l** poziom]

pscxpert -t

pscxpert -l <poziom> [**-p**] <**-a** *plik1* | **-n** *plik2* | **-a** *plik3* **-n** *plik4*>

pscxpert -f profil **-a** plik [**-p**]

pscxpert -d

Opis

Komenda **pscxpert** ustawia różne ustawienia konfiguracji systemu w celu włączenia określonego poziomu bezpieczeństwa.

Uruchomienie komendy **pscxpert** wyłącznie z opcją **-l** implementuje ustawienia zabezpieczeń natychmiast bez pozwolenia użytkownikowi na skonfigurowanie tych ustawień. Na przykład uruchomienie komendy **pscxpert -l high** powoduje automatyczne zastosowanie w systemie wszystkich ustawień zabezpieczeń wysokiego poziomu. Uruchomienie komendy **pscxpert -l** z opcjami **-n** i **-a** powoduje zapisanie ustawień zabezpieczeń w pliku określonym za pomocą parametru *plik*. Następnie opcja **-f** powoduje zastosowanie tych nowych konfiguracji.

Po dokonaniu początkowego wyboru wyświetlane jest menu zawierające wszystkie opcje konfiguracyjne zabezpieczeń powiązane z wybranym poziomem zabezpieczeń. Opcje te można zaakceptować w całości albo włączać lub wyłączać je indywidualnie. Po wprowadzeniu wszystkich dodatkowych zmian komenda **pscxpert** kontynuuje stosowanie ustawień zabezpieczeń w systemie komputerowym.

Komendę **pscxpert** należy uruchamiać jako użytkownik root docelowego serwera VIOS. Gdy użytkownik nie jest zalogowany jako użytkownik root docelowego serwera VIOS, przed uruchomieniem tej komendy należy uruchomić komendę **oem_setup_env**.

Jeśli komenda **pscxpert** zostanie uruchomiona, gdy inna instancja komendy **pscxpert** jest już uruchomiona, komenda **pscxpert** kończy działanie z komunikatem o błędzie.

Uwaga: Należy ponownie uruchomić komendę **pscxpert** po wprowadzeniu większych zmian w systemie, takich jak instalacja lub aktualizacja oprogramowania. Jeśli konkretny element konfiguracyjny nie zostanie wybrany przy ponownym uruchomieniu komendy **pscxpert**, ten element konfiguracyjny zostanie pominięty.

Opcje

Opcja	Opis
-a	Ustawienia z powiązanymi opcjami poziomu zabezpieczeń są zapisywane do podanego pliku w formacie skróconym.
-c	Sprawdza ustawienia zabezpieczeń w odniesieniu do wcześniej zastosowanego zestawu reguł. Jeśli sprawdzenie w odniesieniu do reguły nie powiedzie się, sprawdzane są także poprzednie wersje tej reguły. Ten proces jest kontynuowany aż sprawdzenie powiedzie się lub do momentu, gdy zostaną sprawdzone wszystkie instancje reguły zakończonej niepowodzeniem w pliku /etc/security/aixpert/core/appliedaixpert.xml. To sprawdzenie można uruchomić dla każdego profilu domyślnego lub niestandardowego.
-d	Wyświetla definicję typu dokumentu (DTD).

Opcja	Opis
-f	Stosuje ustawienia zabezpieczeń udostępnione w podanym pliku *profil*. Profile znajdują się w katalogu /etc/security/aixpert/custom. Wśród dostępnych profili znajdują się następujące profile standardowe: **DataBase.xml** Ten plik zawiera wymagania dla ustawień domyślnej bazy danych. **DoD.xml** Ten plik zawiera wymagania dla ustawień procedur STIG (Security Technical Implementation Guide) Departamentu Obrony. **DoD_to_AIXDefault.xml** Zmienia ustawienia na domyślne ustawienia systemu AIX. **DoDv2.xml** Ten plik zawiera wymagania dla ustawień drugiej wersji procedur STIG (Security Technical Implementation Guide) Departamentu Obrony. **DoDv2_to_AIXDefault.xml** Zmienia ustawienia na domyślne ustawienia systemu AIX. **Hipaa.xml** Ten plik zawiera wymagania dla ustawień HIPAA (Health Insurance Portability and Accountability Act). **NERC.xml** Ten plik zawiera wymagania dla ustawień NERC (North American Electric Reliability Corporation). **NERC_to_AIXDefault.xml** TEn plik zmienia ustawienia NERC na domyślne ustawienia systemu AIX. **PCI.xml** Ten plik zawiera wymagania dla ustawień standardu PCI DSD (Payment Card Industry Data Security Standard). **PCIv3.xml** Ten plik zawiera wymagania dla ustawień trzeciej wersji standardu PCI DSD (Payment Card Industry Data Security Standard). **PCI_to_AIXDefault.xml** TEn plik zmienia ustawienia na domyślne ustawienia systemu AIX. **PCIv3_to_AIXDefault.xml** TEn plik zmienia ustawienia na domyślne ustawienia systemu AIX. **SOX-COBIT.xml** Ten plik zawiera wymagania dla ustawień Sarbanes-Oxley Act i COBIT. Można także utworzyć profile niestandardowe w tym samym katalogu i zastosować je do ustawień, zmieniając nazwy i zawartość istniejących plików XML. Na przykład następująca komenda ma zastosowanie do profilu HIPAA w systemie: `pscxpert -f /etc/security/aixpert/custom/Hipaa.xml` Gdy zostanie podana opcja **-f**, ustawienia zabezpieczeń są stale stosowane z systemu do systemu przez bezpieczne przesyłanie i stosowanie pliku **appliedaixpert.xml** z systemu do systemu. Wszystkie pomyślnie zastosowane reguły są zapisywane w pliku /etc/security/aixpert/core/appliedaixpert.xml, a odpowiadające im reguły działania wycofywania są zapisywane w pliku /etc/security/aixpert/core/undo.xml.

Opcja	Opis
-l	Ustawia określony poziom bezpieczeństwa systemu. Dostępne są następujące opcje: **h|high** Określa opcje zabezpieczeń na wysokim poziomie. **m|medium** Określa opcje zabezpieczeń na średnim poziomie. **l|low** Określa opcje zabezpieczeń na niskim poziomie. **d|default** Określa opcje zabezpieczeń na standardowym poziomie systemu AIX. **s|sox-cobit** Określa opcje zabezpieczeń Sarbanes-Oxley Act i COBIT. Jeśli zostanie podana zarówno opcja **-l**, jak i opcja **-n**, ustawienia zabezpieczeń nie zostaną zaimplementowane w systemie. Zostaną one tylko zapisane w określonym pliku. Wszystkie pomyślnie zastosowane reguły są zapisywane w pliku /etc/security/aixpert/core/appliedaixpert.xml, a odpowiadające im reguły działania wycofywania są zapisywane w pliku /etc/security/aixpert/core/undo.xml. **Ważne:** Gdy zostanie użyta opcja **d|default**, może ona nadpisać skonfigurowane ustawienia zabezpieczeń, które zostały wcześniej ustawione za pomocą komendy **pscxpert** lub niezależenie, i przywrócić system do jego tradycyjnej, otwartej konfiguracji.
-n	Zapisuje ustawienia z powiązanymi opcjami poziomu zabezpieczeń w określonym pliku.
-p	Określa, że dane wyjściowe reguł zabezpieczeń są wyświetlane jako szczegółowe dane wyjściowe. Opcja **-p** rejestruje przetworzone reguły w podsystemie kontrolującym, jeśli włączono opcję **kontrola**. Tej opcji można używać z dowolną z następujących opcji: **-l**, **-u**, **-c** i **-f**. Opcja **-p** włącza szczegółowe dane wyjściowe w terminalu i pliku aixpert.log.
-P	Akceptuje nazwę profilu jako wejście. Ta opcja jest używana wraz z opcjami **-c**. Opcje **-c** i **-P** są używane do sprawdzania kompatybilności systemu z przekazanym profilem.
-r	Zapisuje istniejące ustawienia systemu do pliku /etc/security/aixpert/check_report.txt. Danych wyjściowych można używać w raportach kontroli zabezpieczeń lub zgodności. Ten raport opisuje każde ustawienie, jego możliwe powiązanie z wymaganiami zgodności z przepisami i informację o tym, czy sprawdzenie zakończyło się niepowodzeniem. **Uwaga:** • Opcja -r obsługuje tylko operację stosowania dla profili. Nie obsługuje operacji stosowania dla poziomów. • Opcja -r wyświetla cały komunikat (jeden lub więcej wierszy) dla reguły.
-R	Generuje te same dane wyjściowe co opcja **-r**. Ponadto flaga ta dodaje opis skryptu lub programu reguły używanego do zaimplementowania ustawienia konfiguracyjnego. **Uwaga:** • Opcja -R obsługuje tylko operację stosowania dla profili. Nie obsługuje operacji stosowania dla poziomów.
-t	Wyświetla typ profilu zastosowanego w systemie.
-u	Wycofuje zastosowane ustawienia zabezpieczeń. **Uwaga:** • Nie można użyć opcji **-u** do wycofania zastosowanego profilu DoD, DoDv2, NERC, PCI lub PCIv3. Aby usunąć te profile po ich dodaniu, zastosuj profil, który kończy się łańcuchem _AIXDefault.xml. Aby na przykład usunąć profil NERC.xml, należy zastosować profil NERC_to_AIXDefault.xml. • Zmiany w systemie wprowadzone po operacji zastosowania są tracone, gdy wykonywana jest operacja cofnięcia. Ustawienia są przywracane do wartości, która istniała przed operacją zastosowania.

Parametry

Opcja	Opis
plik	Plik wyjściowy, w którym zapisane są ustawienia zabezpieczeń. Aby uzyskać dostęp do tego pliku, wymagane są uprawnienia użytkownika root.
poziom	Poziom niestandardowy, który ma zostać użyty do sprawdzenia poprzednio zastosowanych ustawień.
profil	Nazwa pliku profilu, który udostępnia systemowi reguły zgodności. Aby uzyskać dostęp do tego pliku, wymagane są uprawnienia użytkownika root.

Zabezpieczenia

Komenda **pscxpert** może być uruchamiana tylko przez użytkownika root.

Przykłady

1. Aby zapisać wszystkie opcje zabezpieczeń wysokiego poziomu w pliku wyjściowym, wprowadź następującą komendę:

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

   Po uruchomieniu tej komendy można edytować plik wyjściowy, a konkretne role zabezpieczeń można przekształcić w komentarz przez ujęcie ich w standardowy łańcuch komentarza XML (<-- rozpoczyna komentarz, a -\> zamyka komentarz).
2. Aby zastosować ustawienia zabezpieczeń z pliku konfiguracyjnego STIG Departamentu Obrony, wprowadź następującą komendę:

   ```
   pscxpert -f /etc/security/aixpert/custom/DoD.xml
   ```
3. Aby zastosować ustawienia zabezpieczeń z pliku konfiguracyjnego HIPAA, wprowadź następującą komendę:

   ```
   pscxpert -f /etc/security/aixpert/custom/Hipaa.xml
   ```
4. Aby sprawdzić ustawienia zabezpieczeń w systemie i zarejestrować reguły, które nie powiodły się w podsystemie kontrolującym, wprowadź następującą komendę:

   ```
   pscxpert -c -p
   ```
5. Aby sprawdzić poziom niestandardowy ustawień zabezpieczeń dla profilu NERC w systemie i zarejestrować reguły, które nie powiodły się w podsystemie kontrolującym, wprowadź następującą komendę:

   ```
   pscxpert -c -p -l NERC
   ```
6. Aby wygenerować raporty i zapisać je w pliku /etc/security/aixpert/check_report.txt, wprowadź następującą komendę:

   ```
   pscxpert -c -r
   ```

Położenie

Opcja	Opis
/usr/sbin/pscxpert	Zawiera komendę **pscxpert**.

Pliki

Opcja	Opis
/etc/security/aixpert/log/aixpert.log	Zawiera protokół śledzenia zastosowanych ustawień zabezpieczeń. Ten plik nie używa standardowego syslog. Komenda **pscxpert** zapisuje dane bezpośrednio w tym pliku, ma uprawnienia do odczytu/zapisu i wymaga zabezpieczeń na poziomie użytkownika root.
/etc/security/aixpert/log/firstboot.log	Zawiera dziennik śledzenia ustawień zabezpieczeń, które zostały zastosowane podczas pierwszego startu instalacji SbD (Secure by Default).
/etc/security/aixpert/core/undo.xml	Zawiera listing XML ustawień zabezpieczeń, które można wycofać.

Komenda rmvfilt

Przeznaczenie

Usuwa z tabeli filtrów reguły filtrowania dotyczące komunikacji między wirtualnymi sieciami LAN.

Składnia

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

Opis

Komenda **rmvfilt** służy do usuwania z tabeli filtrów reguł filtrowania dotyczących komunikacji między wirtualnymi sieciami LAN.

Opcje

-n Określa identyfikator reguły filtrowania, która ma zostać usunięta. Opcja **all** pozwala na usunięcie wszystkich reguł filtrowania.

Status wyjścia

Ta komenda zwraca następujące wartości wyjścia:

0 Pomyślne zakończenie.

>0 Wystąpił błąd.

Przykłady

1. Aby usunąć wszystkie reguły filtrowania lub aby wyłączyć wszystkie reguły filtrowania w jądrze, wpisz następującą komendę:

   ```
   rmvfilt -n all
   ```

Pojęcia pokrewne:

“Dezaktywowanie reguł” na stronie 113
Można dezaktywować reguły, które umożliwiają routing danych między sieciami VLAN w zaufanym firewallu.

Komenda vlantfw

Przeznaczenie

Wyświetla lub usuwa informacje o powiązaniu adresów IP i MAC (Media Access Control) i steruje funkcją rejestrowania.

Składnia

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

Opis

Komenda **vlantfw** wyświetla lub usuwa pozycje powiązania adresów IP i MAC. Pozwala także na uruchamianie lub zatrzymywanie narzędzia rejestrowania dla zaufanego firewalla.

Opcje

-d Wyświetla wszystkie informacje dotyczące powiązań IP.

-D Wyświetla zgromadzone dane na temat połączeń.

-E Wyświetla informacje o połączeniach między partycjami logicznymi (LPAR) umieszczonymi w różnych zespołach CEC.

-f Usuwa wszystkie informacje dotyczące powiązań IP.

-F Powoduje wyczyszczenie pamięci podręcznej danych o połączeniach.

-G Wyświetla reguły filtrowania, które mogą być skonfigurowane do kierowania ruchu wewnętrznie za pośrednictwem zaufanego firewalla.

-I Wyświetla dane o połączeniach między partycjami LPAR, które są powiązane z różnymi identyfikatorami sieci VLAN, ale współużytkują ten sam zespół CEC.

-l Uruchamia narzędzie rejestrowania dla zaufanego firewalla.

-L Zatrzymuje narzędzia rejestrowania dla zaufanego firewalla i przekierowuje zawartość pliku śledzenia do pliku /home/padmin/svm/svm.log.

-m Włącza monitorowanie zaufanego firewalla.

-M Wyłącza monitorowanie zaufanego firewalla.

-q Wysyła zapytanie o status bezpiecznej maszyny wirtualnej.

-s Uruchamia zaufany firewall.

-t Zatrzymuje zaufany firewall.

Parametry

-N *liczba całkowita*
Wyświetla regułę filtrowania, która odpowiada podanej liczbie całkowitej.

Status wyjścia

Ta komenda zwraca następujące wartości wyjścia:

0 Pomyślne zakończenie.

>0 Wystąpił błąd.

Przykłady

1. Aby wyświetlić wszystkie przypisania adresów IP, wpisz następującą komendę:
   ```
   vlantfw -d
   ```
2. Aby usunąć wszystkie przypisania adresów IP, wpisz następującą komendę:
   ```
   vlantfw -f
   ```
3. Aby uruchomić funkcję rejestrowania zaufanego firewalla, wpisz następującą komendę:
   ```
   vlantfw -l
   ```
4. Aby sprawdzić status bezpiecznej maszyny wirtualnej, wpisz następującą komendę:
   ```
   vlantfw -q
   ```
5. Aby uruchomić zaufany firewall, wpisz następującą komendę:
   ```
   vlantfw -s
   ```
6. Aby zatrzymać zaufany firewall, wpisz następującą komendę:
   ```
   vlantfw -t
   ```
7. Aby wyświetlić odpowiednie reguły, których można użyć do wygenerowania filtrów kierujących ruchem sieciowym w zespole CEC, wpisz następującą komendę:
   ```
   vlantfw -G
   ```

Odsyłacze pokrewne:

“Komenda genvfilt” na stronie 156

Uwagi

Niniejsza publikacja została przygotowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych.

IBM może nie oferować w innych krajach produktów, usług lub opcji omawianych w tej publikacji. Informacje o produktach i usługach dostępnych w danym kraju/regionie można uzyskać od lokalnego przedstawiciela IBM. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi IBM. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie niniejszej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przesyłać na adres:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Zapytania w sprawie licencji dotyczących informacji kodowanych przy użyciu dwubajtowych zestawów znaków (DBCS) należy kierować do lokalnych działów IBM Intellectual Property Department lub zgłaszać na piśmie pod adresem:

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

INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W STANIE, W JAKIM SIĘ ZNAJDUJE ("AS IS") BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ GWARANCJI, ŻE PUBLIKACJA NIE NARUSZA PRAW OSÓB TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy drukarskie. Informacje te są okresowo aktualizowane, a zmiany te zostaną uwzględnione w kolejnych wydaniach tej publikacji. Firma IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Jakiekolwiek wzmianki na temat stron internetowych nienależących do firmy IBM zostały podane jedynie dla wygody użytkownika i nie oznaczają, że IBM w jakikolwiek sposób firmuje te strony. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych do tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do używania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Informacje na temat możliwości stosowania tego programu, takie jak: (i) wymiana informacji między niezależnie tworzonymi programami a innymi programami (włącznie z tym programem) czy (ii) wspólne używanie wymienianych informacji, można uzyskać pod adresem:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, uiszczenie odpowiedniej opłaty.

Licencjonowany program opisany w niniejszej publikacji oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie LicencyjnejIBM na Program lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Dane o wydajności i przytoczone przykłady klientów mają charakter wyłącznie ilustracyjny. Rzeczywista wydajność w konkretnych konfiguracjach i środowiskach operacyjnych może być inna.

Informacje dotyczące produktów firm innych niż IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące możliwości produktów innych podmiotów należy kierować do dostawców tych produktów.

Stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Wszelkie ceny podawane przez IBM są propozycjami cen detalicznych; ceny te są aktualne i podlegają zmianom bez wcześniejszego powiadomienia. Ceny podawane przez dealerów mogą być inne.

Przedstawione tu informacje służą tylko do planowania. Informacja ta podlega zmianom do chwili, gdy produkty, których ona dotyczy, staną się dostępne.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennych operacjach działalności gospodarczej. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy/nazwiska są fikcyjne i jakiekolwiek podobieństwo do istniejących nazw/nazwisk jest całkowicie przypadkowe.

LICENCJA W ZAKRESIE PRAW AUTORSKICH:

Niniejsza publikacja zawiera przykładowe aplikacje w języku źródłowym, ilustrujące techniki programowania w różnych systemach operacyjnych. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM, w celu projektowania, używania, sprzedaży lub dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tego systemu operacyjnego, dla którego napisane zostały programy przykładowe. Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować ani sugerować niezawodności, użyteczności i funkcjonalności tych programów. Programy przykładowe są oferowane w stanie, w jakim się znajdują („AS IS”), bez jakiejkolwiek gwarancji. IBM nie ponosi odpowiedzialności za jakiekolwiek szkody wynikające z używania programów przykładowych.

Każda kopia lub dowolna część programów przykładowych, albo też dowolna praca pochodna, musi zawierać poniższą informację o prawach autorskich:

© (nazwa przedsiębiorstwa) (rok).

Fragmenty niniejszego kodu pochodzą z przykładowych programów IBM Corp.

Uwagi dotyczące strategii ochrony prywatności

Oprogramowanie IBM, w tym rozwiązanie SaaS (Software as a Service), zwane dalej "Oferowanym Oprogramowaniem" może korzystać z informacji cookie lub z innych technologii do gromadzenia danych o używaniu produktów, do poprawienia jakości usług dla użytkowników końcowych, do dopasowania interakcji do ich oczekiwań oraz do innych celów. W wielu przypadkach Oferowane Oprogramowanie nie gromadzi informacji umożliwiających identyfikację osób. Część Oferowanego Oprogramowania może jednak umożliwiać gromadzenie informacji umożliwiających identyfikację osób. Jeśli Oferowane Oprogramowanie korzysta z informacji cookie do gromadzenia informacji umożliwiających identyfikację osób, poniżej znajdują się szczegółowe informacje na temat takiego korzystania.

Oferowane Oprogramowanie nie korzysta z informacji cookie ani z innych technologii do gromadzenia informacji umożliwiających identyfikację osób.

Jeśli konfiguracje Oferowanego Oprogramowania umożliwiają gromadzenie informacji umożliwiających identyfikację użytkowników końcowych za pośrednictwem informacji cookie lub innych technologii, należy wystąpić o poradę prawną w zakresie prawa obowiązującego przy takim gromadzeniu danych, w tym wymagań dotyczących powiadomienia i zgody.

Więcej informacji na temat korzystania z różnych technologii, w tym z informacji cookie, do opisanych wyżej celów znajduje się w sekcji Ochrona prywatności w IBM pod adresem http://www.ibm.com/privacy oraz Oświadczenie IBM o Ochronie Prywatności w Internecie, pod adresem http://www.ibm.com/privacy/details, a także w sekcji zatytułowanej "Cookies, Web Beacons and Other Technologies" oraz "IBM Software Products and Software-as-a-Service Privacy Statement", pod adresem http://www.ibm.com/software/info/product-privacy.

Znaki towarowe

IBM, logo IBM oraz ibm.com są znakami towarowymi lub zastrzeżonymi znakami towarowymi International Business Machines Corp. zarejestrowanymi w wielu różnych krajach. Nazwy innych produktów lub usług mogą być znakami towarowymi IBM lub innych podmiotów. Aktualna lista znaków towarowych IBM jest dostępna w serwisie WWW Copyright and trademark information (Informacje o prawach autorskich i znakach towarowych) pod adresem www.ibm.com/legal/copytrade.shtml.

Linux jest zastrzeżonym znakiem towarowym Linusa Torvaldsa w Stanach Zjednoczonych i/lub w innych krajach.

Java oraz wszystkie znaki towarowe i logo dotyczące języka Java są znakami towarowymi lub zastrzeżonymi znakami towarowymi Oracle i/lub przedsiębiorstw afiliowanych Oracle.

Indeks

M

N

O

P

R

S

T

U

W

Z

Drukowane w USA