IBM PowerSC

Standard Edition

Wersja 1.1.3

PowerSC Standard Edition

IBM PowerSC

Standard Edition

Wersja 1.1.3

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 47.

Niniejsze wydanie dotyczy systemu IBM PowerSC wersja 1.1.3 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.

IBM PowerSC Standard Edition 1.1.3

Produkt IBM® PowerSC Standard Edition zawiera następujące opcje: automatyzacja zabezpieczania i zgodności, zaufany start, zaufany firewall, zaufane rejestrowanie, zaufane połączenia z siecią i zarządzanie poprawkami.

Nowości w produkcie PowerSC Standard Edition 1.1.3

Zapoznaj się z nowymi lub znacząco zmodyfikowanymi informacjami na temat produktu PowerSC Standard Edition w wersji 1.1.3.

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

Grudzień 2013

- Aktualizacja wymagań systemowych w sekcji “Pojęcia dotyczące PowerSC Standard Edition 1.1.3”.
- Opis wymaganego zastąpienia pliku zaufanego startu przy ponownej instalacji systemu AIX w sekcji “Wymagania wstępne zaufanego startu” na stronie 5.
- Dodano informacje na temat funkcji monitorowania zaufanego firewalla w sekcji “Monitorowanie zaufanego firewalla” na stronie 13.
- Dodano informacje na temat funkcji rejestrowania zaufanego firewalla w sekcji “Rejestrowanie dla zaufanego firewalla” na stronie 13.
- Dodano sekcję “Instalowanie zaufanego rejestrowania” na stronie 18.
- Dodano informacje na temat aktualizacji poprawek tymczasowych dla zaufanej sieci w sekcji “Konfigurowanie serwera zarządzania poprawkami” na stronie 24.
- Dodano informacje na temat raportowania dla serwera sieci zaufanej w sekcji “Raportowanie dla serwera TNC” na stronie 29.
- Dodano informacje na temat instalowania weryfikatora zaufanej sieci w sekcji “Instalowanie weryfikatora” na stronie 6.
- Dodano listę komend zaufanego firewalla w sekcji “Komendy PowerSC Standard Edition” na stronie 31.
- Zmieniono nazwę komendy **tscpmconsole** na **pmconf** i dodano odpowiednie informacje w sekcji “Komenda pmconf” na stronie 35.
- Zmieniono nazwę komendy **tscconsole** na **psconf** i dodano odpowiednie informacje w sekcji “Komenda psconf” na stronie 38.
- Zaktualizowane informacje na temat opcji komendy **vlantfw** w sekcji “Komenda vlantfw” na stronie 44.

Listopad 2012

Zaktualizowano informacje podane w sekcji “Sieć zaufana (TNC) i zarządzanie poprawkami” na stronie 20.

Maj 2012

Dodano dokumentację dla nowego składnika w sekcji “Zaufany firewall” na stronie 10.

Pojęcia dotyczące PowerSC Standard Edition 1.1.3

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	• POWER5 • POWER6 • POWER7
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 Virtual I/O Server.	• AIX 6.1 • AIX 7.1 • VIOS w wersji 2.2.1.4 lub nowszy.	• POWER6 • POWER7 • Virtual I/O Server 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	• POWER5 • POWER6 • POWER7
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 Klient zaufanej sieci wymaga 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.	• POWER5 • POWER6 • POWER7

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:

- powerscExp.ice: Instalowany w systemach AIX, które wymagają funkcji automatyzacji zabezpieczeń i zgodności produktu PowerSC Standard Edition.
- powerscStd.vtpm: Instalowany w systemach AIX, które wymagają funkcji zaufanego startu produktu PowerSC Standard Edition.
- powerscStd.vlog: Instalowany w systemach AIX, które wymagają funkcji zaufanego rejestrowania produktu PowerSC Standard Edition.
- powerscstd.tnc_pm: Instalowany w systemach AIX wersja 6.1 z pakietem Technology Level 6100-06 lub nowszych lub w środowisku SUMA (Service Update Management Assistant) zarządzającym poprawkami dla systemu AIX wersja 7.1.
- powerscStd.svm: Instalowany w systemach AIX, które mogą wymagać funkcji routingu obsługiwanej przez produkt PowerSC Standard Edition.

Zainstaluj produkt PowerSC Standard Edition za pomocą 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**.

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 1.1.3” na stronie 1
Ten przegląd produktu PowerSC Standard Edition zawiera opis jego funkcji, komponentów i obsługi sprzętu.

“Instalowanie zaufanego startu” na stronie 6
Istnieją wymagane konfiguracje sprzętu i oprogramowania, które są niezbędne do zainstalowania zaufanego startu.

“Instalowanie zaufanej sieci (TNC)” na stronie 22
Instalowanie komponentów zaufanej sieci (TNC) wymaga wykonania opisanych poniżej czynności.

Zadania pokrewne:

“Instalowanie zaufanego firewalla” na stronie 12
Instalowanie mechanizmu zaufanego firewalla w systemie PowerSC jest podobne do instalowania innych funkcji w tym systemie.

“Instalowanie zaufanego rejestrowania” na stronie 18
Funkcję zaufanego rejestrowania PowerSC można zainstalować za pomocą interfejsu wiersza komend lub narzędzia SMIT.

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 Hardware Management Console (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 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 8
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 8
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 Virtual I/O Server (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 3
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 2. 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 5
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 4
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.

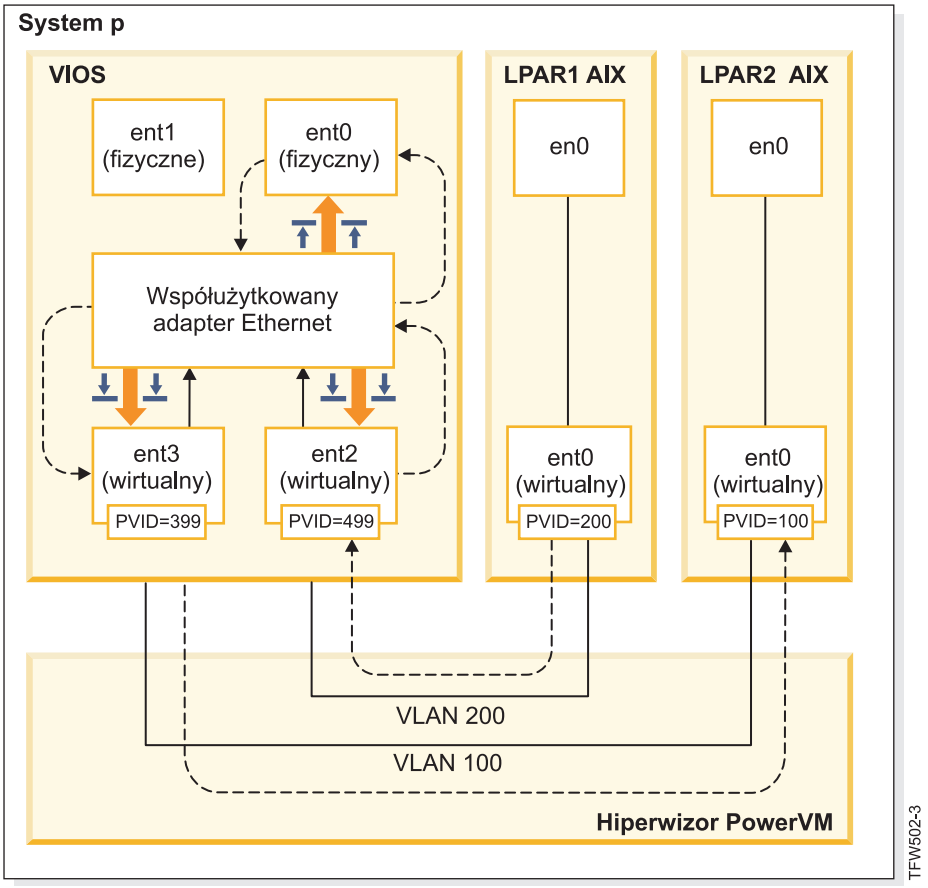
Pojęcia dotyczące zaufanego firewalla

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.

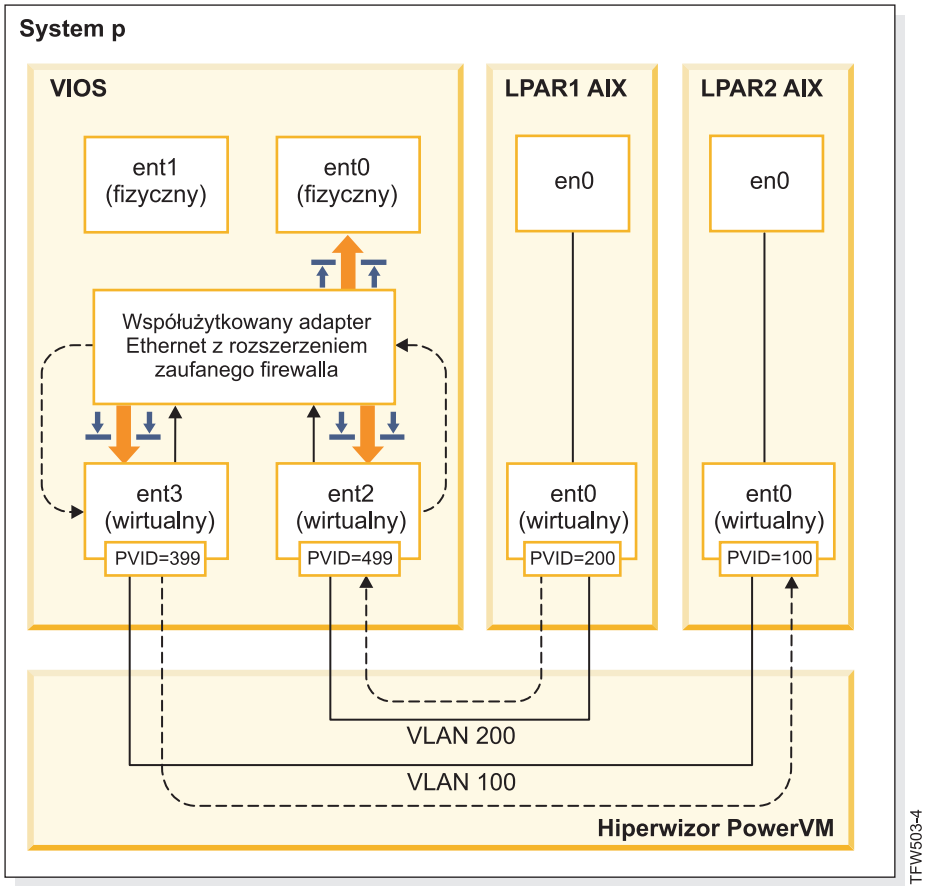
Zaufany firewall pozwala na skonfigurowanie reguł umożliwiających przesyłanie niektórych typów ruchu bezpośrednio z jednej sieci VLAN na serwerze Virtual I/O Server (VIOS) do innej sieci VLAN na tym samym serwerze VIOS, przy zachowaniu wysokiego poziomu bezpieczeństwa dzięki ograniczeniu innych typów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

Rys. 1 na stronie 11 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 12.



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 Virtual I/O Server (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 3
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.

Monitorowanie zaufanego firewalla

Monitorowanie zaufanego firewalla analizuje ruch generowany przez różne partycje logiczne (LPAR) i pozwala na określenie, czy uruchomiony zaufany firewall poprawia wydajność systemu.

Jeśli funkcja monitorowania zaufanego firewalla 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 monitorowanie dla zaufanego firewalla, wpisz następującą komendę:

```
vlantfw -m
```

Aby wyświetlić wyniki monitorowania zaufanego firewalla, wpisz następującą komendę:

```
vlantfw -D
```

Aby wyłączyć monitorowanie dla zaufanego firewalla, 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 system monitoringu zaufanego firewalla określi, że ruch kierowanie ruchu wewnętrznie zwiększy efektywność, mechanizm rejestrowania zaufanego firewalla zapisze listę ścieżek w pliku svm.log. Limitem wielkości pliku svm.log jest 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
```

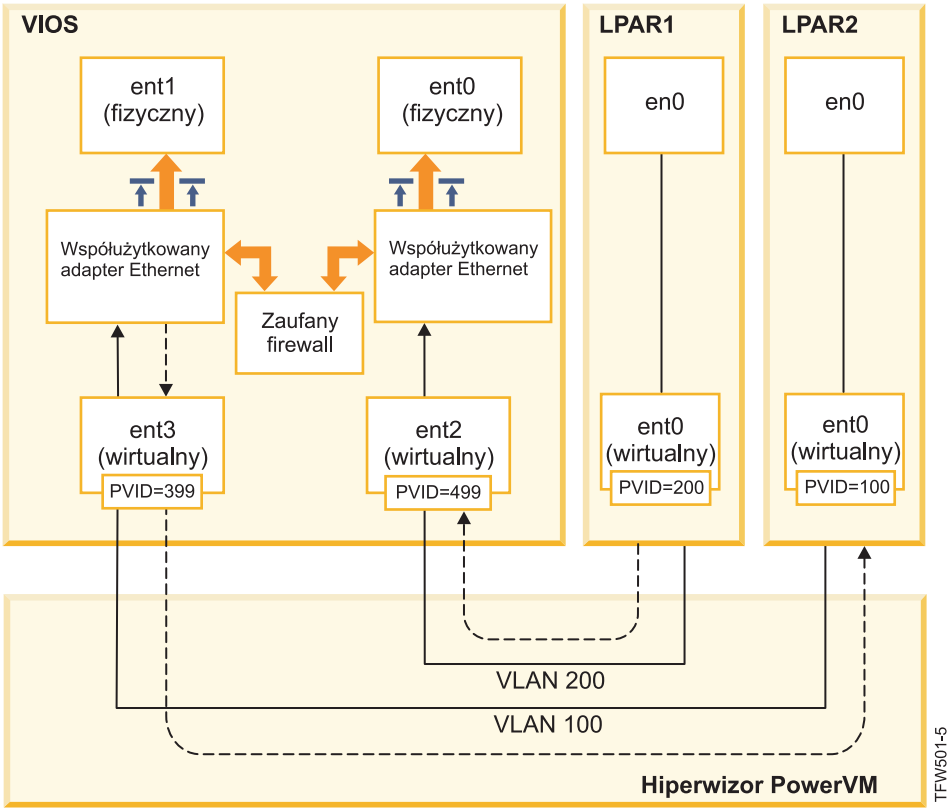
Plik dziennika jest dostępny dla wyświetlania w następującej lokalizacji: /home/padmin/svm/svm.log.

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 Virtual I/O Server (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 Virtual I/O Server (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:
   - `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 32

“Komenda mkvfilt” na stronie 34

“Komenda vlantfw” na stronie 44

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 Virtual I/O Server (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 15
Użytkownik może utworzyć reguły, aby włączyć komunikację między sieciami VLAN za pośrednictwem zaufanego firewalla.

Odsyłacze pokrewne:

“Komenda lsvfilt” na stronie 34

“Komenda rmvfilt” na stronie 43

Zaufane rejestrowanie

Funkcja zaufanego rejestrowania PowerVM pozwala partycjom LPAR systemu AIX na zapisywanie do plików dzienników umieszczonych na przyłączonych serwerach Virtual I/O Server (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 Virtual I/O Server (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 3
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 18.

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 Virtual I/O Server (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 18.

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.

Sieć zaufana (TNC) i zarządzanie poprawkami

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

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 (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:

Serwer zaufanej sieci (TNC) integruje się z SUMA tworząc wszechstronne rozwiązanie do zarządzania poprawkami.

Program AIX SUMA pobiera najnowsze pakiety z poprawkami i poprawki bezpieczeństwa dostępne w serwisie IBM ECC and Fix Central. Demon zarządzania TNC i poprawkami 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 (Service Update Management Assistant) 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.

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 (Virtual I/O Server) 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 38

Instalowanie zaufanej sieci (TNC)

Instalowanie komponentów zaufanej sieci (TNC) wymaga wykonania opisanych poniżej czynności.

Aby przygotować konfigurację do instalacji komponentów sieci TNC, wykonaj następujące czynności:

1. Zidentyfikuj adresy IP systemów do skonfigurowania serwera TNC, serwera TNCPM (Trusted Network Connect and Patch Management) oraz odsyłacza IP w serwerze Virtual I/O Server (VIOS).

   Uwaga: Serwer TNC nie może zostać skonfigurowany jako klient TNC.
2. Skonfiguruj serwer do zarządzania instalacją sieciową (NIM) . System skonfigurowany jako serwer jest nadrzędnym serwerem NIM, a w systemie klienta należy zainstalować zestawy plików sets:bos.sysmgt.nim.master.
3. Skonfiguruj serwer TNCPM. Tę konfigurację można skonfigurować w systemie NIM. Serwer TNCPM używa mechanizmu SUMA w celu pobrania poprawek z serwisów WWW IBM Fix Central i ECC. 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
   ```

4. 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 27.
5. 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.
6. 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
   ```

Odsyłacze pokrewne:

“Komenda psconf” na stronie 38

Informacje pokrewne:

“Instalowanie produktu PowerSC Standard Edition 1.1.3” na stronie 3
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 zaufanej sieci (TNC) i zarządzania poprawkami

Należy skonfigurować sieć zaufaną (TNC) jako demona zarządzania poprawkami. Serwer TNC integruje się z SUMA tworząc wszechstronne rozwiązanie do zarządzania poprawkami.

Konfigurowanie 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 4280, a dla portu pmserver wartość domyślna równa 38240.

Odsyłacze pokrewne:

“Komenda psconf” na stronie 38

Konfigurowanie klienta połączenia z zaufaną siecią

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 38

Konfigurowanie serwera zarządzania poprawkami

W sekcji opisano kroki umożliwiające skonfigurowanie systemu jako serwera zarządzania poprawkami.

Należy skonfigurować serwer serwera zarządzania poprawkami zaufanej sieci (TNC) w serwerze zarządzania instalacją sieciową (NIM), aby można było aktualizować klienty TNC.

| Aby zainicjować repozytoria poprawek dla zarządzania poprawkami TNC, wprowadź następującą komendę:

```
| pmconf init -i <odstęp czasu pobierania> -l <TL list> [-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.

| 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

Serwer zarządzania poprawkami TNC obsługuje mechanizm **syslog** do 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 38

Informacje pokrewne:

Zabezpieczenia IBM AIX

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 38

Konfigurowanie odsyłacza IP na serwerze VIOS

Sekcja zawiera informacje na temat konfigurowania odsyłacza IP na serwerze Virtual I/O Server (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.

Odsyłacze pokrewne:

“Komenda psconf” na stronie 38

Zarządzanie zaufaną siecią (TNC) i zarządzaniem poprawkami

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 38

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
```

Uwaga: Jeśli zostanie podane wiele strategie 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 38

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 Virtual I/O Server (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:

  ```
  tncconsole 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 38

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 38

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.

Odsyłacze pokrewne:

“Komenda psconf” na stronie 38

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 35

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 38

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}
```

Odsyłacze pokrewne:

“Komenda psconf” na stronie 38

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 3. 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 Virtual I/O Server (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.

Tabela 3. Rozwiązywanie problemów dotyczących ustawień konfiguracyjnych TNC i systemu zarządzania poprawkami (kontynuacja)

Problem	Rozwiązanie
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.

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”

“Komenda vlantfw” na stronie 44

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 16
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 32

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 7.1 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** <*ifix okres*>] [**-K** <*ifix klucz*>]

pmconf add -l *lista_TL*

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** <*plik tar ifix*>

pmconf delete -l *lista_TL*

pmconf delete -p <*lista SP*>

| **pmconf delete -p** <*SP*>**-e** *plik ifix*

pmconf list -s [**-c**] [**-q**]

pmconf list -l *SP*

pmconf list -C

pmconf list -a *SP*

pmconf hist -u

pmconf hist -d

pmconf import -f *nazwa_pliku_cert* **-k** *nazwa_pliku_klucza*

pmconf export -f *nazwa_pliku*

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 delete -l <*lista TL*>

pmconf restart

pmconf status

pmconf log loglevel = info | error | none

pmconf chtncpm atrybut = *wartość*

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.
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.
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.
-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).
-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**.
-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.
-P *ścieżka_repozytorium_poprawek*	Określa katalog pobierania dla repozytoriów poprawek, który będą pobierane przez TNCPM. Katalogiem domyślnym jest **/var/tnc/tncpm/repozytorium poprawek**.
-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.
-d	Generuje raport historii pobierania pakietów serwisowych.
-C	Generuje raport dla certyfikatu serwera.
-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).
-f *nazwa_pliku*	Określa nazwę pliku certyfikatu.
-k *nazwa_pliku_klucza*	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.
-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.

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
    ```

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 użytkownika*>]

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

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

| **psconf chserver** attribute = *wartość*

| **psconf add -F** <*nazwa_strategii_FS*> -r <*inf_wersji*> [**apargrp=** [**±**]<*apargrp1, apargrp2.. >*] [*ifixgrp*=[+|-
|]<*ifixgrp1*,*ifixgrp2...>*]

| **psconf add** { **-G** <*nazwa_grp_ip*> **ip=**[**±**]<*host1, host2...*> | {**-A**<*grp_apar*> [**lista_apar**=[**±**]*apar1, apar2...* | {**-V**
| <*grp_ifix*> [*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** <*grp_ip*> [**-r** <*inf_wersji*> | **-a** <*apar1, apar2...*> | [**-u**] **-v** <*ifix1*, *ifix2*,...>}

| **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_grp_ip* | **ALL** > | **-F** < *nazwa_strategii_FS* | **ALL** > | **-P** < *nazwa_strategii* | **ALL** > | **-r** <
| *inf_wersji* | **ALL** > | **-I -i** < *ip* | **ALL** > | **-A** < *grp_apar* | **ALL** > | **-V** <*grp_ifix*>} [**-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>**

| 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**.

Opcja	Opis
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**.
dbpath	Określa położenie bazy danych TNC. Wartością domyślną jest /var/tnc.
delete	Usuwa strategię lub informacje dotyczące klienta.
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.
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.
recheck_interval	Określa odstęp czasu w dniach (d) , godzinach (h) lub minutach (m), co jaki serwer TNC ma weryfikować klienty TNC. **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 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.

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 listę nazw grupy IP.

Opcja	Opis
-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 *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.
-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.
-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	Określa rozdzielaną przecinkami listę poprawek tymczasowych.
-V	Określa nazwę grupy poprawek tymczasowych.

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**, wpisz 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
    ```

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 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 16
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 32

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 tego dokumentu nie daje żadnych uprawnień licencyjnych do tychże patentów. Zapytania dotyczące licencji można wysłać na piśmie na adres:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA.

Zapytania w sprawie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (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

Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego: 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 ORAZ PRZYDATNOŚCI DO OKREŚLONEGO CELU LUB GWARANCJI, ŻE PUBLIKACJA TA 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 niniejszym dokumencie mogą zawierać nieścisłości techniczne lub błędy drukarskie. Podane w niej informacje są okresowo aktualizowane; zmiany te zostaną ujęte w jej kolejnych wydaniach. 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.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych firm zostały wprowadzone wyłącznie dla wygody użytkownika i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. 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 Corporation
Dept. LRAS/Bldg. 903
11501 Burnet Road
Austin, TX 78758-3400
USA

Informacje takie mogą być udostępniane na odpowiednich warunkach, w niektórych przypadkach za opłatą.

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 Licencyjnej IBM na Program lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Wszelkie dane dotyczące wydajności zostały zebrane w kontrolowanym środowisku. W związku z tym rezultaty uzyskane w innych środowiskach operacyjnych mogą się znacząco różnić. Niektóre pomiary mogły być dokonywane na systemach będących w fazie rozwoju i nie ma gwarancji, że pomiary te wykonane na ogólnie dostępnych systemach dadzą takie same wyniki. Niektóre z pomiarów mogły być estymowane przez ekstrapolację. Rzeczywiste wyniki mogą być inne. Użytkownicy powinni we własnym zakresie sprawdzić odpowiednie dane dla ich środowisk.

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 produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Wszelkie stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Wszelkie ceny podawane przez IBM są sugerowanymi cenami detalicznymi; ceny te są aktualne i podlegają zmianom bez wcześniejszego powiadomienia. Ceny podawane przez dealerów mogą być inne.

Niniejsza informacja służy jedynie do celów planowania. Informacja ta podlega zmianom do chwili, gdy produkty, których ona dotyczy, staną się dostępne.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennej 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 i adresów jest całkowicie przypadkowe.

LICENCJA NA PRAWA AUTORSKIE:

Publikacja ta zawiera przykładowe aplikacje w kodzie źródłowym, które ilustrują techniki programowania na różnych platformach systemowych. 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 czy funkcjonalności tych programów. Programy przykładowe są dostarczane w stanie, w jakim się znajdują ("AS IS"), bez udzielania jakichkolwiek gwarancji. IBM nie ponosi odpowiedzialności za żadne szkody wynikłe z użycia programów przykładowych.

Każdy egzemplarz i fragmenty programów przykładowych oraz jakichkolwiek prac pochodnych muszą zawierać następujące uwagi dotyczące praw autorskich:

© (nazwa przedsiębiorstwa użytkownika, rok). Fragmenty niniejszego kodu pochodzą z przykładowych programów IBM Corp. © Copyright IBM Corp. (wpisać rok lub lata).

W przypadku przeglądania niniejszych informacji w formie elektronicznej, zdjęcia i kolorowe ilustracje mogą nie być wyświetlane.

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 pozwalających na identyfikację osoby. Część Oferowanego Oprogramowania może jednak umożliwiać gromadzenie informacji pozwalających na identyfikację osoby. Jeśli Oferowane Oprogramowanie korzysta z informacji cookie do gromadzenia informacji pozwalających na identyfikację osoby, poniżej znajdują się szczegółowe informacje na temat takiego korzystania.

To Oferowane Oprogramowanie nie używa informacji cookie ani innych technologii do gromadzenia informacji pozwalających na identyfikację osoby.

Jeśli konfiguracje Oferowanego Oprogramowania umożliwiają gromadzenie informacji pozwalających na 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 i ibm.com są znakami towarowymi lub zastrzeżonymi znakami towarowymi International Business Machines Corp. w wielu krajach świata. Nazwy innych produktów i usług mogą być znakami towarowymi IBM lub innych firm. 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 i wszystkie znaki towarowe i logo związane z językiem Java są znakami towarowymi lub zastrzeżonymi znakami towarowymi Oracle i/lub przedsiębiorstw afiliowanych Oracle.

Indeks

W

Z

Drukowane w USA