MC

Tłumaczenie standardów i rekomendacji
w zakresie cyberbezpieczeństwa

Zabezpieczenia sprzętowe:

Zarządzanie oparte na politykach w zaufanych platformach kontenerowych

NIST IR 8320B_wer. 1.0_PL

NIST IR 8320B_wer. 1.0_PL

29 maja 2025

Zabezpieczenia sprzętowe: Zarządzanie oparte na politykach w zaufanych platformach kontenerowych

Publikacja dostępna pod adresem:

Rekomendacje cyberbezpieczeństwa

NISTIR 8320B

Hardware-Enabled Security:

Policy-Based Governance in Trusted Container Platforms

Michael Bartock
Murugiah Souppaya
Haidong Xia
Raghu Yeluri
Uttam Shetty
Brandon Lum
Mariusz Sabath
Harmeet Singh
Alaa Youssef
Gosia Steinder
Yu Cao
Jayashree Ramanathan

This publication is available free of charge
from: https://doi.org/10.6028/NIST.IR.8320B

National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8320B

Hardware-Enabled Security:

Policy-Based Governance in Trusted Container Platforms

Michael Bartock
Murugiah Souppaya

Computer Security Division
Information Technology Laboratory

Haidong Xia Raghu Yeluri Uttam Shetty

Intel Corporation
Santa Clara, California

Brandon Lum
Mariusz Sabath
Harmeet Singh
Alaa Youssef
Gosia Steinder
IBM
Armonk, New York

Yu Cao
Jayashree Ramanathan

Red Hat
Raleigh, North Carolina

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8320B

April 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Undersecretary of Commerce for Standards and Technology

O PUBLIKACJI

Niniejsze opracowanie **NIST IR 8320B_wer. 1.0_PL, *Zabezpieczenia sprzętowe: Zarządzanie oparte na politykach w zaufanych platformach kontenerowych***, stanowi tłumaczenie publikacji NIST IR 8320B, *Hardware-Enabled Security: Policy-Based Governance in Trusted Container Platforms*, i zostało opracowane za zgodą National Institute of Science and Technology.

Przytaczane i cytowane w publikacji przepisy, okólniki, rozporządzenia wykonawcze, dyrektywy, normy, standardy, polityki, memoranda itp. odnoszą się, o ile nie zaznaczono inaczej, do prawodawstwa i rynku amerykańskiego. Jeżeli cytowany fragment ma przełożenie lub odpowiednik w polskim porządku prawnym lub normalizacyjnym, wówczas informacje te wskazane są bezpośrednio w tekście lub w przypisach.

W publikacji posłużono się pojęciami zdefiniowanymi w oryginalnej (angielskiej) wersji dokumentu, na podstawie którego powstały niniejsze zalecenia.

Tam, gdzie to było możliwe i nie budziło kontrowersji, nazwy ról i kluczowych uczestników procesu zarządzania ryzykiem zostały podane w języku polskim. Pozostałe role i funkcje zostały przedstawione w języku angielskim[1]. Do wszystkich tych ról / funkcji zastosowano akronimy terminologii angielskiej.

Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie ***Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*.**

Podmioty, urządzenia lub materiały o charakterze komercyjnym prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Celem ich wskazania nie jest nakłanianie do korzystania z ww. podmiotów, urządzeń lub materiałów lub ich poparcie. Wskazanie ich nie ma również na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w danej dziedzinie. Taka identyfikacja nie stanowi rekomendacji, poparcia ani nie ma na celu sugerowania, że dane podmioty, materiały lub urządzenia są bezwzględnie najlepsze z dostępnych dla osiągnięcia danego celu.

[1] Kluczowi uczestnicy zarządzania ryzykiem – patrz: Narodowe Standardy Cyberbezpieczeństwa

SPIS TREŚCI

SPIS ILUSTRACJI

SPIS TABEL

STRESZCZENIE

Współczesne centra danych przetwarzające dane w chmurze oraz urządzenia odpowiedzialne za przetwarzanie brzegowe charakteryzują się znacznie większymi powierzchniami ataku. Co więcej, staliśmy się świadkami industrializacji cyberataków, a większość wdrażanych środków bezpieczeństwa charakteryzuje się niską spójnością. Podstawą każdej strategii bezpieczeństwa centrum danych lub urządzeń brzegowych powinno być zabezpieczenie platformy odpowiedzialnej za uruchamianie procesów oraz dostęp do danych. Platforma fizyczna stanowi fundament każdego wielowarstwowego podejścia do bezpieczeństwa, zapewnia bowiem podstawową ochronę gwarantującą zaufanie do środków bezpieczeństwa działających w wyższych warstwach. Niniejsza publikacja stanowi opracowanie wyjaśniające podejście oparte na technikach i technologiach bezpieczeństwa opartych na rozwiązaniach sprzętowych, wykorzystywanych do ochrony kontenerów w środowiskach chmurowych wykorzystywanych przez wielu użytkowników. Opisuje również prototypową implementację podejścia, które powinno stanowić model lub szablon dla przedstawicieli społeczności zajmującej się bezpieczeństwem.

SŁOWA KLUCZOWE

chmura (*ang. cloud*); kontener (*ang. container*); zabezpieczenia sprzętowe (*ang. hardware-enabled security*); sprzętowe źródło zaufania (*ang. hardware root of trust*); bezpieczeństwo platformy (*ang. platform security*); zaufana pula zasobów obliczeniowych (*ang. trusted compute pool*); wirtualizacja (*ang. virtualization*)

ODBIORCY

Głównymi odbiorcami niniejszej publikacji są specjaliści zajmujący się bezpieczeństwem, w tym między innymi inżynierowie i architekci bezpieczeństwa i , administratorzy systemów i inni specjaliści zajmujący się technologią informacyjną, zatrudniani przez dostawców usług chmurowych, a także producenci sprzętu, twórcy oprogramowania układowego i aplikacji, którzy mogą być w stanie wykorzystać sprzętowe techniki i technologie bezpieczeństwa w celu usprawnienia wykorzystywania kontenerów w środowiskach chmurowych wykorzystywanych przez wielu użytkowników.

INFORMACJE O ZNAKACH TOWAROWYCH

Wszystkie zastrzeżone znaki towarowe lub inne znaki towarowe stanową własność organizacji, do których należą.

INFORMACJA O UJAWNIENIU PATENTÓW

INFORMACJA: Laboratorium informatyczne (ITL) NIST zwróciło się do właścicieli patentów, których wykorzystanie może być wymagane w celu zapewnienia zgodności z wytycznymi lub wymogami określonymi w treści niniejszej publikacji, o udostępnienie stosownych zastrzeżeń patentowych. Należy jednak pamiętać o tym, że właściciele patentów nie są zobowiązani do ujawnienia ich na prośbę ITL; co więcej, ITL nie przeprowadziło badań patentowych w celu określenia patentów, które mogą mieć zastosowanie do niniejszej publikacji.

W dniu publikacji i po wystosowaniu prośby (próśb) o wskazanie zastrzeżeń patentowych, których wykorzystanie może być wymagane w celu zapewnienia zgodności z wytycznymi lub wymogami zawartymi w niniejszej publikacji, ITL nie otrzymało informacji o takich zastrzeżeniach patentowych.

Niniejszy dokument nie stanowi oświadczenia ani zapewnienia ze strony ITL, że w celu uniknięcia naruszeń ochrony patentowej przy korzystaniu z niniejszej publikacji nie jest wymagane uzyskanie licencji.

1. WPROWADZENIE

1.1. CEL I ZAKRES

Celem niniejszej publikacji jest opisanie podejścia do zabezpieczania kontenerów aplikacji w środowiskach chmurowych wykorzystywanych przez wielu użytkowników. Niniejsza publikacja opisuje szereg wyzwań związanych z bezpieczeństwem środowisk oferujących infrastrukturę jako usługę (IaaS) omówionych w sprawozdaniu Narodowego Instytutu Standaryzacji i Technologii (IR) NIST IR 8320A[2] [1], który dotyczy technologii przetwarzania w chmurze i geolokalizacji na podstawie znaczników zasobów. Niniejsza publikacja wykorzystuje trzy etapy procesu wdrożenia opisane w rozdziałach 3, 4 oraz 5 poradnika NIST IR 8320A, a ponadto opisuje dwa dodatkowe etapy obejmujące szyfrowanie obrazów kontenerów i opracowywanie zasad dostępu do danych dla kontenerów. Dokument opisuje także przykładowe wdrożenie, które zostało opracowane w celu sprostania opisanym wyzwaniom. Zawiera dostateczną liczbę szczegółowych informacji na temat przykładowego wdrożenia, by umożliwić organizacjom jego odtworzenie w razie potrzeby. Niniejszą publikację należy traktować jako plan lub szablon opracowany z myślą o specjalistach zajmujących się bezpieczeństwem, dzięki któremu mogą zweryfikować lub wdrożyć opisany przykład.

Należy wziąć pod uwagę, że przykładowe wdrożenie przedstawione w niniejszej publikacji jest tylko jednym z możliwych sposobów rozwiązania problemów związanych z bezpieczeństwem. Nie ma ono także na celu wyłączenia możliwości stosowania innych produktów, usług, technik oraz innych rozwiązań, które mogą posłużyć do rozwiązania określonych problemów, ani także wyłączenia możliwości stosowania jakichkolwiek produktów lub usług, które nie zostały wymienione w niniejszej publikacji.

Publikacja NSC RT 8320B opiera się na terminologii i koncepcjach opisanych w dokumencie NIST IR 8320 *Hardware-Enabled Security*: *Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases*[3] [2]. Zapoznanie się

[2] Publikacja w języku polskim NIST IR 8320A.
[3] Publikacja w języku polskim NIST IR 8320.

z treścią powyższego dokumentu jest wymagane przed przeczytaniem niniejszej publikacji, gdyż znajdują się w nim objaśnienia pojęć oraz kluczowych terminów wykorzystywanych w treści przedstawionego opracowania.

1.2. TERMINOLOGIA

W celu zachowania spójności z powiązanymi publikacjami NIST, w treści niniejszego dokumentu zastosowano następujące definicje pojęć związanych z zaufaniem:

- **Zaufanie (*ang. Trust*):** „Przekonanie, że inny element zachowa się zgodnie z oczekiwaniami" [3].
- **Zaufany (*ang. Trusted*):** Element, na którym polega inny element w celu spełnienia krytycznych wymagań w jego imieniu.
- **Zaufane uruchamianie (*ang. Trusted boot*):** Proces uruchamiania systemu, w którym różne parametry urządzeń oraz oprogramowania układowego są mierzone i porównywane ze znanymi prawidłowymi wartościami w celu zweryfikowania ich integralności, a tym samym wiarygodności.
- **Godny zaufania (*ang. Trustworthy*):** Rozwiązanie zasługujące na zaufanie, że będzie w stanie spełnić wszelkie kluczowe wymagania[4].

1.3. STRUKTURA DOKUMENTU

Niniejszy dokument został podzielony na następujące rozdziały i obejmuje następujące załączniki:

- Rozdział 2 określa cel przykładowego wdrożenia oraz cele pośrednie, które należy osiągnąć, aby osiągnąć cel podstawowy.
- Rozdziały od 3 do 7 opisują pięć etapów przykładowego wdrożenia:
  - ✓ Etap 0: Zapewnienie, że platforma, na której uruchamiane są kontenery, jest godna zaufania.

[4] Na podstawie definicji zawartej w publikacji specjalnej NIST (SP) 800-160, tom 2, wersja 1. https://doi.org/10.6028/NIST.SP.800-160v2r1

- ✓ Etap 1: Orkiestracja rozmieszczania obciążeń w celu uruchamiania ich wyłącznie na zaufanych platformach.
- ✓ Etap 2: Możliwość ciągłego monitorowania i egzekwowania ograniczeń dotyczących znaczników zasobów.
- ✓ Etap 3: Umożliwienie użytkownikom końcowym szyfrowania obrazów obciążeń (*ang. workload images*).
- ✓ Etap 4: Możliwość przyznawania obciążeniom dostępu do poufnych informacji za pomocą mechanizmów uwierzytelniania.

- Rozdział Referencje zawiera listę źródeł cytowanych w całym dokumencie.
- Załącznik A zawiera omówienie wysokopoziomowej architektury sprzętowej, na której opiera się przykładowe wdrożenie, a także szczegółowe informacje na temat implementacji modułów sprzętowych i ulepszonych sprzętowych funkcji bezpieczeństwa na platformach opartych na procesorach spółki Intel.
- Załącznik B zawiera dodatkowe informacje dostarczone przez spółki IBM oraz Red Hat opisujące elementy i kroki wymagane do konfiguracji rozwiązań OpenShift i Multi-Cloud Manager.
- Załącznik C zawiera dodatkowe informacje opisujące wszystkie wymagane elementy i kroki wymagane do skonfigurowania implementacji szyfrowania obciążeń.
- Załącznik D zawiera informacje uzupełniające opisujące wszystkie wymagane elementy i kroki wymagane do skonfigurowania przykładowego wdrożenia w celu wykorzystania rozwiązania Trusted Service Identity.
- Załącznik E zawiera wykaz głównych zabezpieczeń wymienionych w publikacji specjalnej NIST (SP) 800-53 Rev. 5[5], które wpływają na przykładowe wdrożenie, a także na zdolność do ochrony zapewniana przez prototypowe rozwiązanie. Dodatkowo załącznik łączy możliwości prototypu do mechanizmów zabezpieczeń opisanych w publikacji specjalnej NIST SP 800-53.

[5] Publikacja w języku polskim NSC 800-53 wer. 2.

- Załącznik F łączy główne funkcje bezpieczeństwa prototypowego rozwiązania z podkategoriami ram cyberbezpieczeństwa.
- Załącznik G zawiera glosariusz objaśniający akronimy użyte w treści niniejszego sprawozdania.

2. PRZYKŁADOWE WDROŻENIE

W tym rozdziale został przedstawiony opis przykładowego wdrożenia.
W podrozdziale 2.1 został omówiony cel. Podrozdział 2.2 zawiera dodatkowe szczegóły oraz omawia wszystkie cele pośrednie, które muszą zostać zrealizowane, aby przykładowe wdrożenie zakończyło się sukcesem. Wymagania te zostały podzielone na pięć etapów dotyczących przypadku użycia. Poszczególne etapy zostały omówione bardziej szczegółowo w podrozdziałach od 2.2.1 do 2.2.5.

2.1. CEL

Brak ograniczeń dotyczących orkiestracji uruchamiania kontenerów wiąże się z obawami dotyczącymi prywatności oraz bezpieczeństwa. Powszechnym oczekiwaniem wielu podmiotów jest możliwość korzystania wyłącznie z serwerów chmurowych zlokalizowanych fizycznie w kraju pochodzenia organizacji lub fizycznie zlokalizowanych w tym samym kraju, z którego pochodzą informacje. Każdorazowo, gdy na jednym serwerze chmurowym działa wiele rozwiązań opartych na kontenerach, konieczne jest rozdzielenie ich od siebie, by zagwarantować, że ich działanie nie będzie wpływało negatywnie na inne rozwiązania, że nie będą uzyskiwały dostępu do poufnych danych lub w inny sposób zagrażały bezpieczeństwu lub prywatności kontenerów. Raport NIST IR 8320A, *Hardware-Enabled Security: Container Platform Security Prototype* [1] omawia wyzwania, przed którymi mogą stanąć organizacje podczas korzystania z rozwiązań kontenerowych w chmurze, a także techniki pozwalające na poprawę bezpieczeństwa przetwarzania w chmurze i przyspieszenia wdrażania technologii przetwarzania w chmurze poprzez ustanowienie zautomatyzowanej sprzętowej metody opartej na sprzętowym źródle zaufania w celu zapewniania i monitorowania integralności platformy oraz ograniczeń geolokalizacyjnych dla serwerów chmurowych.

Opracowanie tego przypadku użycia stanowi rozwinięcie etapów opisanych w raporcie NIST IR 8320A oraz przykład wdrożenia dodatkowych technik wykorzystujących sprzętowe źródło zaufania w ramach platform serwerowych. Dane dotyczące integralności i lokalizacji każdego hosta są wykorzystywane w procesach

orkiestracji i zabezpieczania obciążeń, a także zapewniają obciążeniom dostęp do określonych danych. Orkiestracja obciążeń może zapewnić, że kontenery są uruchamiane tylko na platformach serwerowych, które spełniają wymagania dotyczące wiarygodności i znajdują się w dopuszczalnych lokalizacjach. Orkiestracja może również obejmować wstępne szyfrowanie obrazów kontenerów i udostępnianie kluczy deszyfrujących tylko zaufanym serwerom. Co więcej, na podstawie zaufanych atrybutów związanych z fizycznymi serwerami, poszczególnym obciążeniom można przypisać tożsamości powiązane z serwerami, na których są uruchamiane, a następnie na tej podstawie przyznawać im dostęp do wrażliwych informacji.

2.2. CELE

Korzystanie z zaufanych zasobów obliczeniowych opisanych w rozdziałach od 3 do 5 dokumentu NIST IR 8320A, jest dominującym podejściem w zakresie łączenia zaufanych systemów oraz oddzielania ich od niezaufanych zasobów, czego skutkiem jest oddzielenie bardziej wrażliwych i narażonych obciążeń o wyższej wartości od powszechnych procesów, aplikacji i danych. Podstawowe zasady postępowania obejmują:

1. Konfigurację części środowiska chmurowego, która spełnia konkretne i zróżnicowane wymagania bezpieczeństwa stawiane przez użytkowników.
2. Ograniczenie dostępu do tej części chmury, dzięki czemu będą w niej uruchamiane wyłącznie właściwe aplikacje (obciążenia).
3. Umożliwienie przeprowadzania kontroli i audytów wyznaczonej części chmury, aby użytkownicy mogli weryfikować zgodność z ustalonymi zasadami.

Po utworzeniu zaufanych zasobów obliczeniowych można zastosować dodatkowe techniki w celu ochrony aplikacji, które są na nich uruchamiane, lub informacji, do których te aplikacje mają dostęp. Obejmują one:

4. Szyfrowanie obrazów obciążeń i upewnianie się, że zaszyfrowane obrazy mogą zostać odszyfrowane wyłącznie przez wyznaczone serwery.
5. Zapewnienie, że tylko określone aplikacje z ograniczeniami opartymi na lokalizacji mogą uzyskać dostęp do poufnych danych.

Zaufane zasoby obliczeniowe pozwalają personelowi IT czerpać korzyści z dynamicznego środowiska chmurowego przy jednoczesnym zapewnieniu wyższych poziomów ochrony dla najbardziej krytycznych aplikacji.

Celem jest możliwość wykorzystania zaufania w roli granicy logicznej dla uruchamiania aplikacji chmurowych na platformach serwerowych w ramach chmur obliczeniowych. Realizacja tego celu jest uzależniona od uprzedniej realizacji poszczególnych celów pośrednich opisanych w ramach etapów, które należy traktować jako wymagania, które musi spełnić dane rozwiązanie.

2.2.1. ETAP 0: ATESTACJA[6] PLATFORMY I POMIAR URUCHOMIENIA WĘZŁA ROBOCZEGO

Jedną z podstaw wdrożenia rozwiązania jest zapewnienie, że platforma, na której uruchamiane są kontenery, jest godna zaufania. Jeśli platforma nie jest godna zaufania, skutkiem jest nie tylko narażenie aplikacji i danych użytkownika na większe ryzyko naruszenia zasad ochrony, lecz także brak pewności, że podany znacznik zasobu serwera w chmurze jest dokładny i zgodny ze stanem faktycznym. Zapewnienie podstawowych gwarancji wiarygodności stanowi pierwszy etap rozwiązania.

Podrozdział 2.2.1 dokumentu NIST IR 8320A zawiera opis konkretnych celów do zrealizowania na etapie 0.

2.2.2. ETAP 1: ROZMIESZCZENIE APLIKACJI NA ZAUFANYCH ZASOBACH

Po pomyślnym zakończeniu realizacji etapu 0, kolejnym celem jest umożliwienie orkiestracji rozmieszczania obciążeń w celu uruchamiania ich wyłącznie na zaufanych platformach. Rozmieszczenie obciążeń jest jednym z najważniejszych aspektów przetwarzania w chmurze, który pozwala na zwiększanie skalowalności oraz niezawodności. Głównym celem tego etapu jest zapewnienie, że każdy serwer, na którym wykonywane są poszczególne procesy, spełnia minimalne wymagane poziomy zabezpieczeń na podstawie zasad bezpieczeństwa poszczególnych aplikacji.

[6] Wydanie zaświadczenia na podstawie decyzji, że wykazano spełnienie określonych wymagań.

Podrozdział 2.2.2 dokumentu NIST IR 8320A zawiera opis konkretnych celów do zrealizowania na etapie 1.

2.2.3. ETAP 2: OZNACZANIE ZASOBÓW I ZAUFANA LOKALIZACJA

Działania w ramach etapu 2 opierają się na rezultatach poprzedniego etapu i zakładają dodanie możliwości ciągłego monitorowania i egzekwowania ograniczeń związanych z oznaczeniami zasobów.

Podrozdział 2.2.3 dokumentu NIST IR 8320A zawiera opis konkretnych celów do zrealizowania na etapie 2.

2.2.4. ETAP 3: SZYFROWANIE OBCIĄŻEŃ OPARTE NA ZAUFANIU

Działania w ramach etapu 2 opierają się na rezultatach poprzedniego etapu i zakładają uwzględnienie możliwości szyfrowania obrazów kontenerów przez użytkowników końcowych, co zapewnia izolację kryptograficzną danych w spoczynku i pomaga chronić dane i własność intelektualną konsumentów. Aby węzeł obliczeniowy mógł uruchomić instancję aplikacji z zaszyfrowanego obrazu, musi pobrać klucz pozwalający na deszyfrowanie obrazu. Celem tego etapu jest zapewnienie, że tylko węzły obliczeniowe charakteryzujące się stosowną wiarygodnością platformy oraz oznaczone odpowiednimi znacznikami zasobów będą mogły otrzymać klucze deszyfrujące dotyczące określonych obrazów obciążeń.

Etap 3 obejmuje następujące cele wstępne:

1. **Opatrzenie wszystkich instancji zaufanej platformy zaufanymi informacjami oraz oznaczeniami zasobów.** Zakończenie etapu 2 umożliwia wykorzystanie pomiarów zaufania wobec platformy oraz informacji zawartych w oznaczeniach zasobów podczas uruchamiania aplikacji i obciążeń.
2. **Szyfrowanie obrazów aplikacji oraz ochrona kluczy deszyfrowania za pomocą menedżera kluczy.** Klucze deszyfrujące powinny być przechowywane w menedżerze kluczy, dzięki czemu autoryzowane węzły należące do zaufanych zasobów obliczeniowych będą w stanie pobierać i uruchamiać odpowiednie instancje obrazów aplikacji.

3. **Udostępnianie kluczy deszyfrujących obrazy aplikacji wyłącznie serwerom z zaufanymi platformami i w zaufanych lokalizacjach.** Klucze deszyfrujące powinny być udostępniane wyłącznie serwerom charakteryzującym się odpowiednią wiarygodnością platformy i znajdują się w dozwolonych lokalizacjach określonych na podstawie znaczników zasobów.

2.2.5. ETAP 4: DOSTĘP APLIKACJI DO INFORMACJI OPARTY NA ZAUFANIU

Ostatni etap opiera się na rezultatach etapu 3. i dodaje możliwość przyznawania aplikacjom i obciążeniom dostępu do poufnych informacji. Większość aplikacji i obciążeń działających w chmurze wymaga pewnego dostępu do źródeł danych lub innych usług, uwierzytelniając się za pomocą hasła, klucza interfejsu programistycznego aplikacji (API) lub certyfikatu. Obecnie odbywa się to zazwyczaj poprzez sekrety, które z założenia powinny być przechowywane w sposób bezpieczny. Celem tego etapu jest zapewnienie, że tylko określone aplikacje i obciążenia uruchamiane na zaufanych zasobach obliczeniowych mogą korzystać z tych mechanizmów uwierzytelniania w celu uzyskania dostępu do wrażliwych informacji.

Etap 4 obejmuje następujące cele wstępne:

1. **Uruchamianie aplikacji i obciążeń wyłącznie na serwerach w chmurze z zaufanymi platformami i znajdujących się w zaufanych lokalizacjach.** Oznacza to zasadniczo zakończenie prac w ramach etapu 2. i uruchamianie aplikacji oraz obciążeń na stosownym hoście należącym do zaufanych zasobów obliczeniowych.
2. **Utworzenie tożsamości dla aplikacji lub obciążenia podpisanej przy pomocy źródła zaufania węzła obliczeniowego.** Każda instancja aplikacji lub obciążenia uruchamiana na węźle obliczeniowym powinna mieć wyjątkową tożsamość podpisywaną przy pomocy źródła zaufania węzła obliczeniowego, aby było możliwe wykazanie, gdzie jest uruchomiona.
3. **Przyznawanie aplikacjom i obciążeniom stosownego dostępu do wrażliwych informacji w oparciu o ich tożsamość.** Podczas uzyskiwania dostępu do wrażliwych informacji aplikacja lub obciążenie musi przedstawić swoją

tożsamość z powyższego celu i na jej podstawie uzyskuje odpowiedni poziom dostępu do wrażliwych informacji. Poziom dostępu jest wstępnie zdefiniowany i zależy od funkcji aplikacji lub obciążenia, wiarygodności platformy i lokalizacji węzła obliczeniowego, na którym są uruchomione.

2.3. DODATKOWE MATERIAŁY ŹRÓDŁOWE

Dodatkowe informacje na temat zagadnień technicznych, z którymi są związane przedstawione etapy, można znaleźć w następujących publikacjach NIST:

- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems* https://doi.org/10.6028/NIST.SP.800-128;
- NIST SP 800-137[7], *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* https://doi.org/10.6028/NIST.SP.800-137;
- NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing* https://doi.org/10.6028/NIST.SP.800-144;
- NIST SP 800-147B, *BIOS Protection Guidelines for Servers* https://doi.org/10.6028/NIST.SP.800-147B;
- Draft NIST SP 800-155, *BIOS Integrity Measurement Guidelines* https://csrc.nist.gov/publications/detail/sp/800-155/draft;
- NIST IR 8320, Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases https://doi.org/10.6028/NIST.IR.8320;
- NIST IR 8320A, Hardware-Enabled Security: Container Platform Security Prototype https://doi.org/10.6028/NIST.IR.8320A.

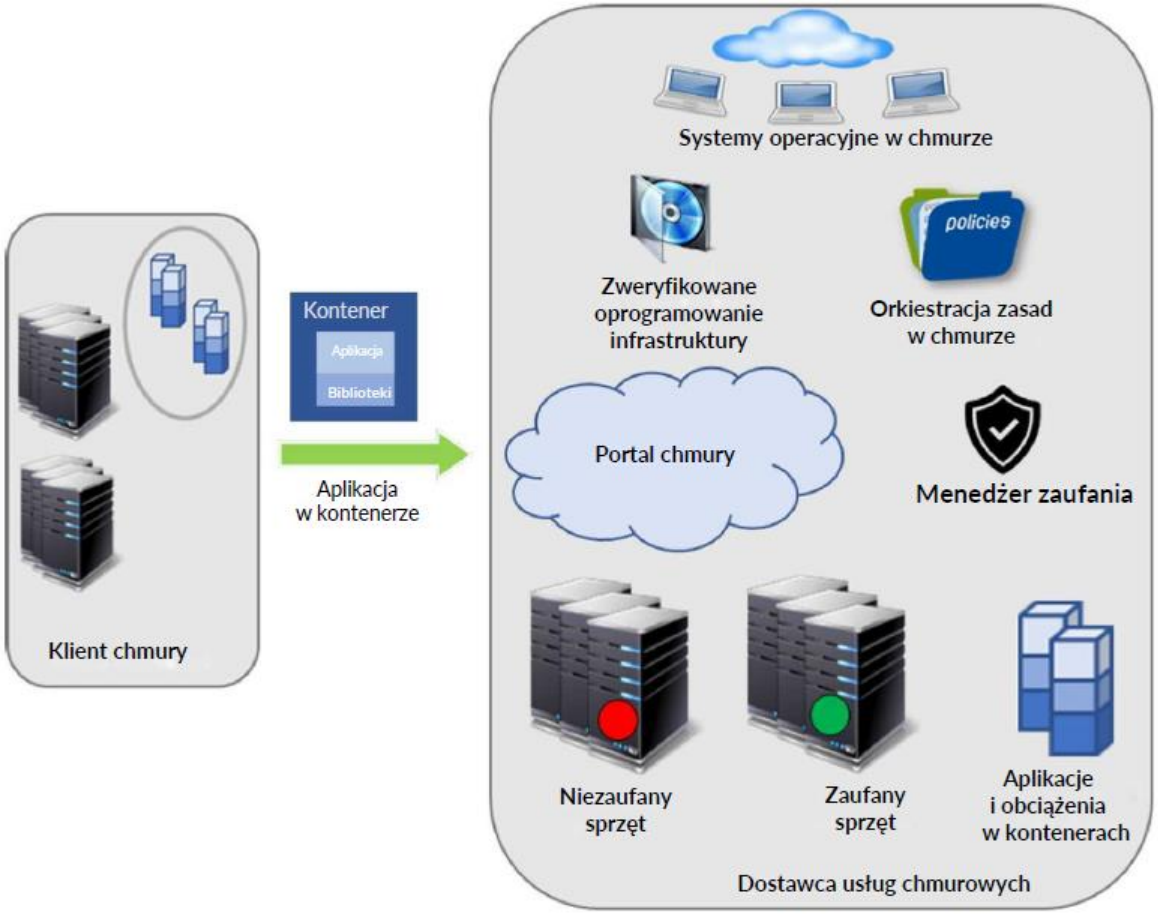
[7] Publikacja w języku polskim NSC 800-137.

3. ETAP ZEROWY PRZYKŁADOWEGO WDROŻENIA

Niniejszy rozdział zawiera przegląd etapu zerowego przykładowego wdrożenia – atestacji platformy oraz analizy uruchomienia węzła roboczego.

Ten etap umożliwia tworzenie tak zwanych *zaufanych pul zasobów obliczeniowych*. Pojęcie to określa fizyczne lub logiczne grupy sprzętu komputerowego w centrum danych, które wykorzystują określone i zróżnicowane zasady bezpieczeństwa, a zarówno dostęp, jak i uruchamianie aplikacji i obciążeń są monitorowane, kontrolowane i audytowane. Na tym etapie rozwiązania zaświadczone uruchomienie platformy, obejmujące także środowisko uruchomieniowe kontenerów, powoduje jej uznanie za zaufany węzeł i dodanie do puli zaufanych zasobów.

Rysunek 1 przedstawia założenia koncepcji pul zaufanych zasobów obliczeniowych. Zasoby oznaczone kolorem zielonym są zasobami zaufanymi. Kluczowe zasady mogą zostać określone w taki sposób, by usługi chmurowe, dla których bezpieczeństwo ma kluczowe znaczenie, mogły być uruchamiane wyłącznie na zaufanych zasobach. Bardziej szczegółowe informacje i architektura rozwiązania znajdują się w rozdziale 3. dokumentu NIST IR 8320A.



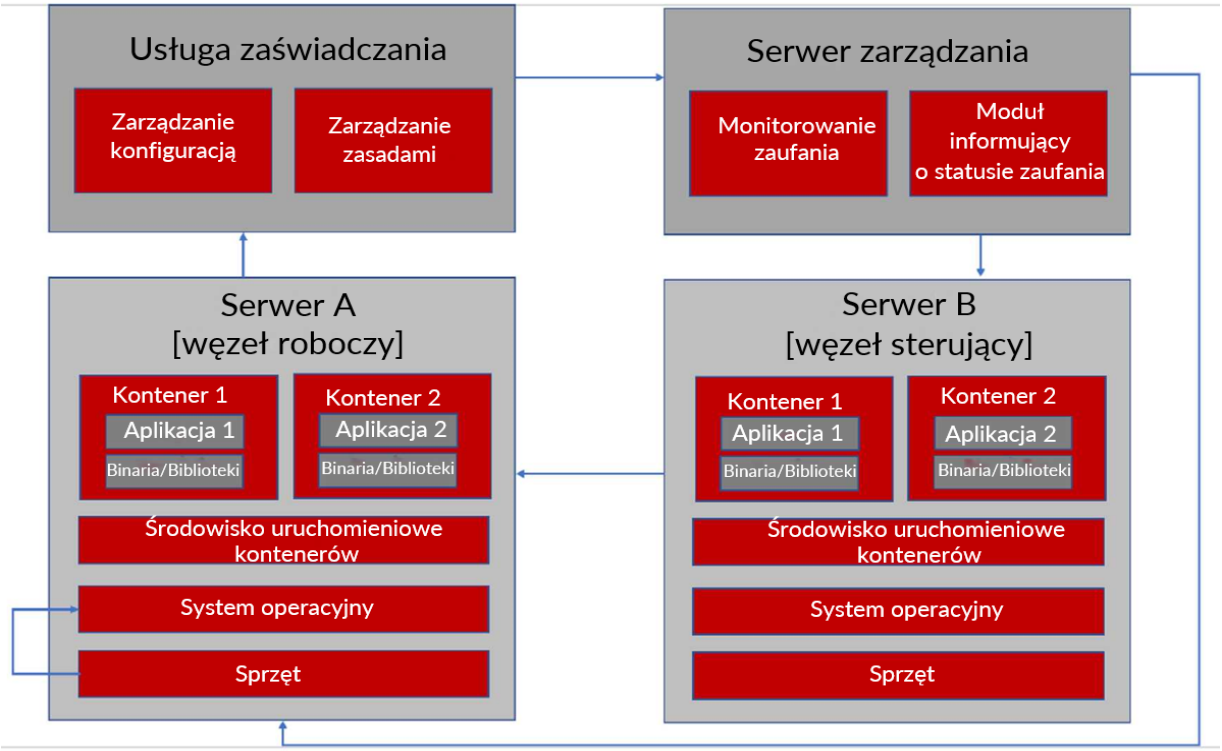
Rysunek 1: Koncepcja zaufanych pul zasobów obliczeniowych

Tłumaczenie

4. ETAP PIERWSZY PRZYKŁADOWEGO WDROŻENIA

Rozdział obejmuje omówienie pierwszego etapu przykładowego wdrożenia (rozmieszczenie aplikacji na zaufanych zasobach). Działania realizowane w ramach tego etapu opierają się na działaniach zrealizowanych w poprzedzającym etapie i dodają elementy, które umożliwiają orkiestrację rozmieszczania aplikacji w celu ich uruchamiania na zaufanych platformach.

Rysunek 2 przedstawia elementy rozwiązania będącego skutkiem etapu pierwszego. Całość opiera się na założeniu, że serwer A i serwer B to dwa serwery działające w ramach tej samej chmury.



Rysunek 2: Przegląd rozwiązania etapu pierwszego

Rozwiązanie składa się z czterech głównych elementów – węzła sterującego, węzła roboczego, usługi atestacji i serwera zarządzania. Każdy z tych elementów współpracuje z pozostałymi, aby umożliwić uruchamianie aplikacji i obciążeń w kontenerach wyłącznie na węzłach roboczych należących do puli zaufanych zasobów obliczeniowych. Szczegółowe omówienie rozwiązania oraz informacje na temat interakcji jego elementów znajdują się w rozdziale 4. dokumentu NIST IR 8320A.

5. ETAP DRUGI PRZYKŁADOWEGO WDROŻENIA

Ten rozdział omawia drugi etap przykładowego wdrożenia (bezpieczne rozmieszczanie aplikacji i obciążeń na podstawie zaufania oraz znaczników zasobów). Działania realizowane w ramach tego etapu opierają się na działaniach zrealizowanych w poprzedzającym etapie i dodają elementy uwzględniające ograniczenia związane z oznaczeniami zasobów. Architektura rozwiązania nie zmienia się w żaden sposób względem poprzedniego etapu, wykorzystuje jednak dodatkowy mechanizm weryfikacji oznaczeń zasobów przy pomocy sprzętowego źródła zaufania serwera i uwzględnia go podczas wykonywania aplikacji i uruchamiania obciążeń.

Ponadto na etapie drugim pojawia się możliwość monitorowania pomiarów w ramach pulpitu nawigacyjnego zarządzania, ryzyka i zgodności. Szczegółowe informacje na temat przeglądu rozwiązania i przykładowy wygląd pulpitu nawigacyjnego znajdują się w rozdziale 4. dokumentu NIST IR 8320A.

6. ETAP TRZECI PRZYKŁADOWEGO WDROŻENIA

Ten rozdział omawia trzeci etap przykładowego wdrożenia (odszyfrowywanie obciążeń oparte na zaufaniu). Działania realizowane w ramach tego etapu opierają się na działaniach zrealizowanych w poprzedzającym etapie i dodają elementy, które umożliwiają odszyfrowywanie zaszyfrowanych obrazów kontenerów przez serwery po wykonaniu pomiarów platformy, oznaczonych zaufanymi znacznikami zasobów.

6.1. OMÓWIENIE ROZWIĄZANIA

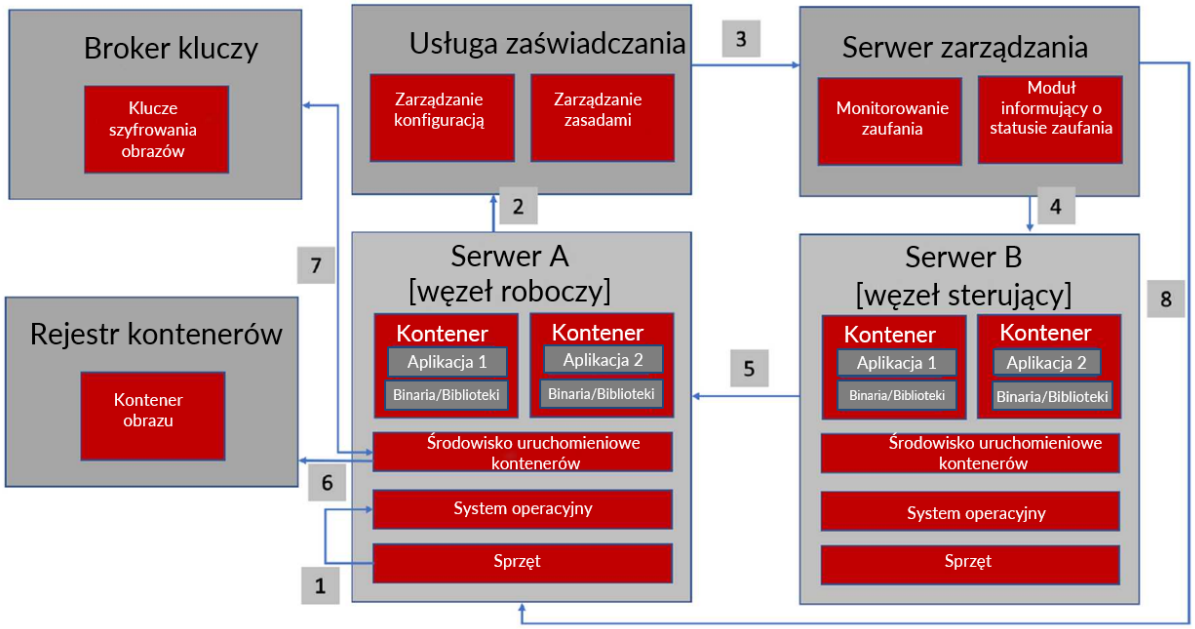
Użytkownicy uruchamiający swoje aplikacje oraz obciążenia w chmurze lub na urządzeniach brzegowych zwykle muszą godzić się z faktem, że ich aplikacje są zabezpieczane przez dostawców usług, jednak nie mają żadnych informacji ani wiedzy na temat stosowanych mechanizmów zabezpieczeń. Możliwość szyfrowania obrazów przez użytkowników końcowych zapewnia użytkownikom końcowym izolację kryptograficzną danych w spoczynku i pomaga chronić dane i własność intelektualną konsumentów.

Gdy usługa węzła uruchomieniowego otrzyma żądanie uruchomienia, może wykryć, że obraz jest zaszyfrowany i wysłać żądanie pobrania klucza deszyfrowania. Żądanie to może zostać przekazane za pośrednictwem usługi atestacji, co pozwoli na przeprowadzenie wewnętrznej oceny zaufania platformy. Żądanie klucza jest przekazywane do brokera kluczy wraz z dowodem zaświadczenia zaufania danej platformy. Broker kluczy może następnie zweryfikować zaświadczony raport platformy i zwolnić klucz z powrotem do dostawcy usług w chmurze i przekazać go usłudze uruchomieniowej węzła. W tym czasie środowisko uruchomieniowe węzła może odszyfrować obraz i kontynuować normalną orkiestrację aplikacji. Podsystem szyfrowania dysków w jądrze może zapewnić szyfrowanie aplikacji oraz danych w spoczynku na platformie.

6.2. ARCHITEKTURA ROZWIĄZANIA

Rysunek 3 przedstawia koncepcję działania rozwiązania wdrożonego na etapie trzecim. Całość opiera się na założeniu, że serwer A i serwer B to dwa serwery działające w ramach tej samej chmury. Rozwiązanie opiera się na tej samej podstawowej architekturze, co rozwiązania w poprzednich etapach, jednak

wprowadza dwa dodatkowe elementy – rejestr kontenerów i brokera kluczy. Rejestr kontenerów to miejsce, w którym przechowywane są zaszyfrowane obrazy kontenerów, a broker kluczy przechowuje ich klucze deszyfrujące i może zapewnić zaufanym serwerom dostęp do nich.



Rysunek 3: Architektura rozwiązania etapu trzeciego

Działanie przykładowego rozwiązania etapu trzeciego obejmuje osiem ogólnych kroków wykonywanych w czasie pracy, które zostały opisane poniżej oraz oznaczone cyframi na rys. 3:

1. Serwer A realizuje proces uruchomienia z pomiarami, a ulepszone funkcje zabezpieczeń sprzętowych zapisują dane pomiarów do modułu sprzętowego.
2. Serwer A wysyła sprawozdanie do usługi zaświadczającej. Sprawozdanie obejmuje podpisane skróty różnych elementów oprogramowania układowego platformy i systemu operacyjnego.
3. Organ zaufania weryfikuje podpis i skróty kryptograficzne, a następnie wysyła zaświadczenie stanu integralności platformy do serwera zarządzania.
4. Serwer zarządzania wymusza przestrzeganie zasad dotyczących aplikacji lub obciążenia na serwerze B w oparciu o wymagania użytkownika.

5. Serwer B uruchamia aplikacje lub obciążenia wymagające zaufanej infrastruktury tylko na platformach serwerowych, które zostały zaświadczone jako zaufane.
6. Serwer A pobiera zaszyfrowany obraz z rejestru kontenerów, dzięki czemu może uruchomić instancję aplikacji lub obciążenia.
7. Broker kluczy wydaje klucz deszyfrujący serwerowi A tylko wtedy, gdy dysponuje zaufanym zaświadczeniem. Serwer A uruchamia instancję aplikacji lub obciążenia.
8. Każda platforma serwerowa jest okresowo poddawana audytowi w celu weryfikacji wartości pomiarów.

7. ETAP CZWARTY PRZYKŁADOWEGO WDROŻENIA

Ten rozdział omawia czwarty etap przykładowego wdrożenia (dostęp aplikacji do informacji oparty na zaufaniu. Działania w ramach tego etapu opierają się na wynikach działań zrealizowanych w poprzednich etapach i dodają elementy, które pozwalają na utworzenie tożsamości dla poszczególnych aplikacji i obciążeń, dzięki czemu możliwe staje się przyznawanie im odpowiedniego dostępu do wrażliwych informacji.

7.1. OMÓWIENIE ROZWIĄZANIA

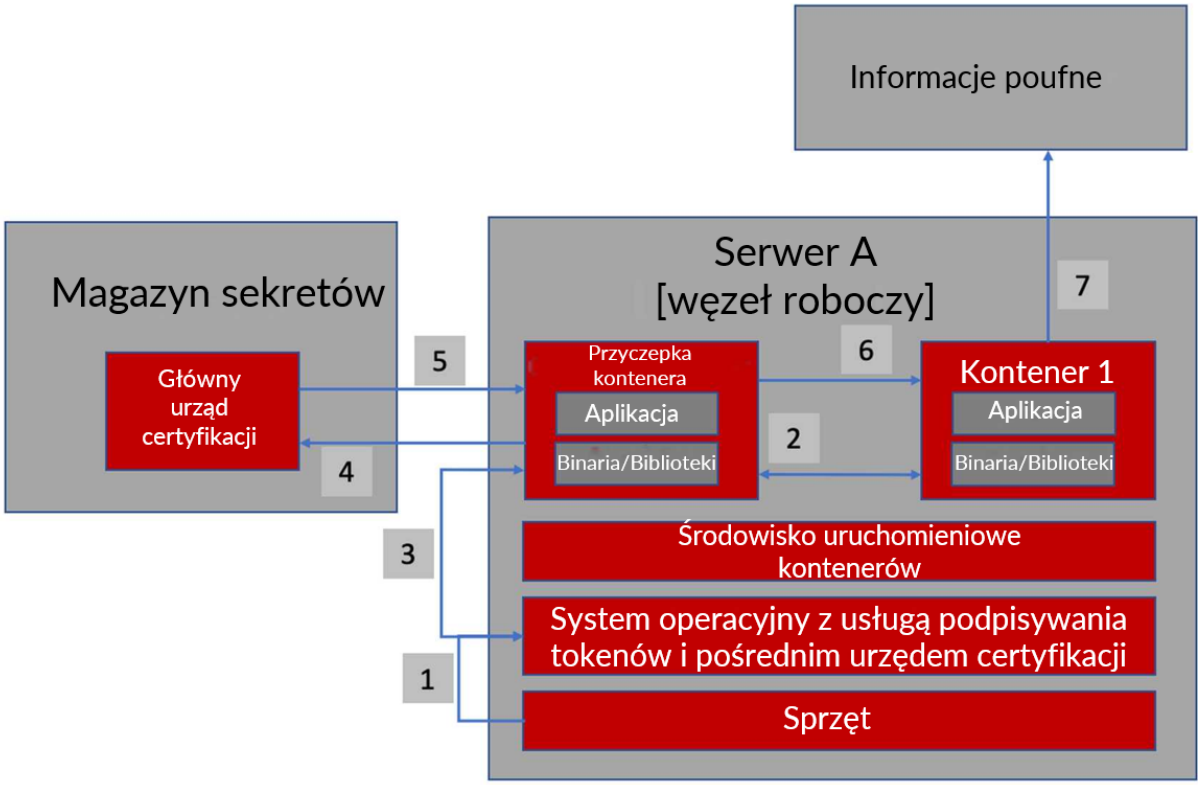
Większość aplikacji oraz obciążeń uruchamianych w chmurze wymaga określonego dostępu do źródeł danych lub innych usług. W tym celu muszą one uwierzytelnić się za pomocą hasła, klucza API lub certyfikatu. Obecnie takie rozwiązania są zwykle realizowane za pośrednictwem sekretów. Mimo że sekrety zostały zaprojektowane z myślą o ich bezpiecznym przechowywaniu (na przykład dzięki szyfrowaniu w spoczynku), na etapie orkiestracji mogą zostać podłączone do dowolnego kontenera oraz odczytane przez każdy podmiot posiadający dostęp do przestrzeni nazw, w tym administratorów chmury. Osoby znające sekrety mogą również uzyskać dostęp do wrażliwych danych, które powinny być chronione. Problem z sekretami polega na tym, że po ich zapisaniu są one również dostępne dla administratorów, operatorów środowisk chmurowych oraz innych podmiotów posiadających dostęp do przestrzeni nazw, niezależnie od tego, czy są one uprawnione do uzyskiwania dostępu do danych chronionych przez sekrety.

Udzielanie aplikacjom i obciążeniom dostępu do informacji opartego na zaufaniu zapewnia ochronę dostępu do wrażliwych danych, zapewniając, że tylko zaświadczone usługi objęte ograniczeniami dotyczącymi lokalizacji mogą uzyskać dostęp do sekretów. Proces opiera się na wykorzystaniu tożsamości aplikacji lub obciążenia, w skład której wchodzą dane na temat tożsamości zaufanego urządzenia, które zostały w pełni zaświadczone, w tym lokalizacji i regionu centrum danych oraz różnych pomiarów dokonywanych w środowisku uruchomieniowym w celu identyfikacji aplikacji. Pomiary te są bezpiecznie podpisywane przez usługę działającą na każdym węźle roboczym, w oparciu o łańcuch zaufania utworzonego podczas

bezpiecznego uruchamiania środowiska, a następnie stale atestowane i weryfikowane. Uruchomienie środowiska wymaga skonfigurowania magazynu sekretów, który obsługuje główny urząd certyfikacji (*ang. Certificate Authority - CA*), oraz zainstalowania pośredniego urzędu certyfikacji i usługi podpisywania tokenów na każdym węźle roboczym. Każdy węzeł roboczy z uruchomioną usługą podpisywania tokenów wykorzystuje swoje sprzętowe źródło zaufania w celu ochrony swojego indywidualnego klucza prywatnego.

7.2. ARCHITEKTURA ROZWIĄZANIA

Rozwiązanie zakłada, że wszystkie kroki opisane w ramach etapu trzeciego zostały pomyślnie wykonane, a aplikacja lub obciążenie zostały uruchomione na węźle roboczym przed rozpoczęciem jakichkolwiek kroków tego etapu. Rysunek 4 przedstawia koncepcję działania rozwiązania wdrożonego na etapie czwartym przy założeniu, że aplikacja lub obciążenie zostały uruchomione na zaufanym węźle roboczym, a dodatkowo zostały określone zasady pomiarów aplikacji, które mogą uzyskać dostęp do sekretów. Pomiary te składają się na tożsamość aplikacji.



Rysunek 4: Architektura rozwiązania etapu czwartego

Działanie przykładowego rozwiązania etapu czwartego obejmuje siedem ogólnych kroków wykonywanych w czasie pracy, które zostały opisane poniżej oraz oznaczone cyframi na rys. 4:

1. Uruchomienie serwera A obejmowało instalację pośredniego urzędu certyfikacji zawierającego mechanizm podpisujący, który wykorzystuje sprzętowe źródło zaufania serwera w celu ochrony swojego klucza prywatnego.
2. Gdy serwer A uruchamia instancję aplikacji lub obciążenia wraz z odpowiednią przyczepką (*ang. sidecar*), przyczepka zbiera pomiary zwane *oświadczeniami* (*ang. claims*), które określają tożsamość danej aplikacji.
3. Przyczepka przesyła pomiary do usługi podpisywania tokenów na serwerze A, a usługa podpisywania podpisuje oświadczenia używając w tym celu pośredniego urzędu certyfikacji, a następnie zwraca token do przyczepki.
4. Przyczepka przesyła żądanie przesłania oznaczonych sekretów do magazynu sekretów, przekazując podpisany token wraz z żądaniem.

5. Magazyn sekretów weryfikuje podpis i datę wygaśnięcia tokena. Jeśli wszystkie dane się zgadzają, przekazane oświadczenia są zestawiane z politykami w celu uzyskania sekretu. Jeśli pomiary są zgodne z politykami, sekret jest udostępniany aplikacji.
6. Przyczepka przekazuje sekret uruchomionej instancji aplikacji.
7. Uruchomiona instancja aplikacji może z łatwością uzyskać dostęp do lokalnych sekretów i użyć ich w celu uzyskania dostępu do wrażliwych danych.

REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[8]	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53

[8] Narodowe Standardy Cyberbezpieczeństwa - Baza wiedzy - Portal Gov.pl (www.gov.pl)

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[8]	
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60
NSC 800-61	Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61

PUBLIKACJE ANGLOJĘZYCZNE[9]

[1] Bartock M, Souppaya M, Wheeler J, Knoll T, Shetty U, Savino R, Inbaraj J, Righi S, Scarfone K (2021) Hardware-Enabled Security: Container Platform Security Prototype. **(National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8320A.** https://doi.org/10.6028/NIST.IR.8320A

[2] Bartock M, Souppaya M, Savino R, Knoll T, Shetty U, Cherfaoui M, Yeluri R, Malhotra A, Banks D, Jordan M, Pendarakis D, Rao JR, Romness P, Scarfone KA (2022) Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8320.

https://doi.org/10.6028/NIST.IR.8320

[3] Polydys ML, Wisseman S (2009) Software Assurance in Acquisition: Mitigating Risks to the Enterprise. https://apps.dtic.mil/dtic/tr/fulltext/u2/a495389.pdf

[4] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[5] National Institute of Standards and Technology (2018), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[9] Publikacje angielski zostały podane w celach uzupełniających dla osób zainteresowanych.

ZAŁĄCZNIK A – WDROŻENIE SPRZĘTOWEGO ŹRÓDŁA ZAUFANIA

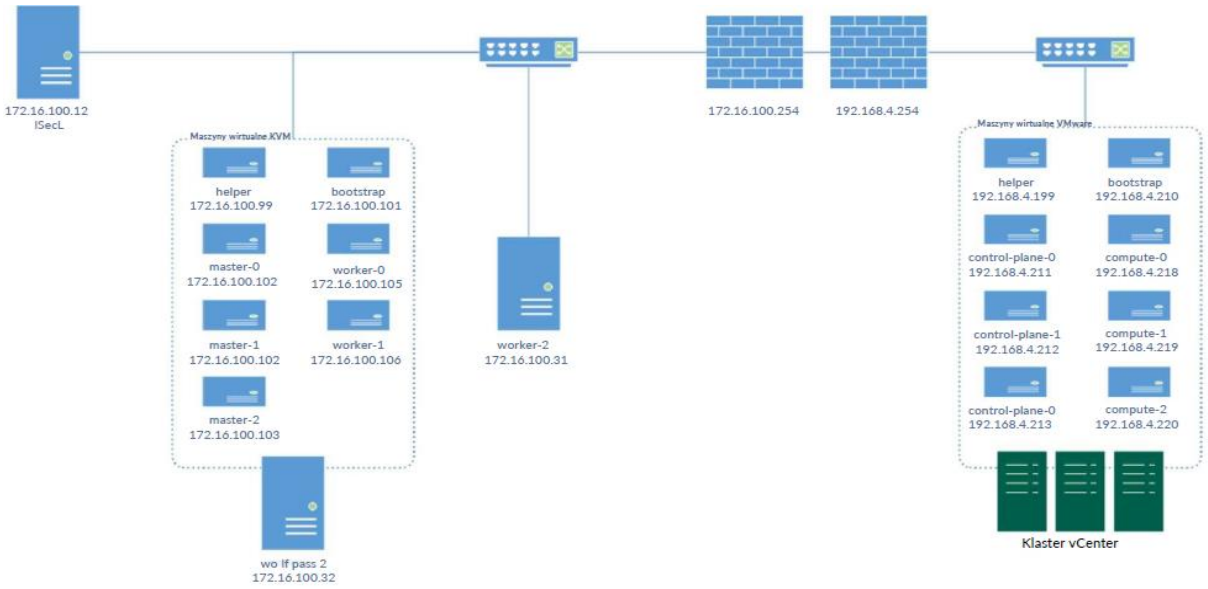
Niniejszy załącznik zawiera omówienie wysokopoziomowej architektury sprzętowej, na której opiera się przykładowe wdrożenie, a także szczegółowe informacje na temat implementacji modułów sprzętowych i ulepszonych sprzętowych funkcji bezpieczeństwa na platformach opartych na procesorach spółki Intel.

A.1 WYSOKOPOZIOMOWA ARCHITEKTURA WDROŻENIA

Rysunek 5 przedstawia wysokopoziomową architekturę wdrożenia. Serwer Intel Security Libraries for Data Center (ISecL-DC - w lewym górnym rogu rysunku) obejmuje usługę brokera kluczy, usługę atestacji i narzędzia do atestacji sprzętowego źródła zaufania i pomiarów hosta. Opisy każdego elementu i kolejne etapy instalacji znajdują się w instrukcji produktu ISecL-DC.

Istnieją dwa klastry OpenShift. Pierwszy z nich obejmuje maszyny wirtualne uruchomione na klastrze VMware, z kolei drugi obejmuje maszyny wirtualne oparte na środowisku Kernel-based Virtual Machine (KVM) oraz jednego hosta uruchamiającego aplikacje bez wirtualizacji. Pierwszy klaster pełni rolę klastra zarządzającego, z kolei drugi klaster jest klastrem zarządzanym.

- Klaster zarządzany to klaster, w którym będą uruchamiane zaufane aplikacje i obciążenia. Może istnieć wiele klastrów zarządzanych przez rozwiązanie IBM Cloud Pak for Multicloud Management (MCM).
- Klaster zarządzający obejmuje płaszczyznę sterowania MCM, a także narzędzia związane z DevOps.



Rysunek 5: Architektura przykładowego wdrożenia

A.2 SPRZĘTOWE ŹRÓDŁO ZAUFANIA: TECHNOLOGIE INTEL TXT I TRUSTED PLATFORM MODULE (TPM)

Sprzętowe źródło zaufania w połączeniu z odpowiednio przygotowanym systemem BIOS, systemem operacyjnym i poszczególnymi elementami, stanowi podstawę bezpieczeństwa platformy obliczeniowej. Bezpieczna platforma zapewnia integralność systemu BIOS i systemu operacyjnego podczas rozruchu, zabezpiecza je przed programami typu rootkit oraz innymi atakami niskopoziomowymi. Zapewnia także zaufanie wobec serwera i platformy hosta.

Zaufana platforma obejmuje trzy źródła zaufania – źródło zaufania do pomiarów (*ang. root of trust for measurement - RTM*), źródło zaufania do raportowania (*ang. root of trust for reporting - RTR*) i źródło zaufania do magazynu (*ang. root of trust for storage* - RTS). Każdy z tych elementów stanowi podstawę platformy. Są to elementy systemu, co do których zaufanie jest wymagane, ponieważ ich nieprawidłowe działanie nie jest wykrywalne na poziomie wyższych warstw. W przypadku platformy obsługującej technologię Intel Trusted Execution Technology (TXT) źródłem zaufania do pomiarów jest mikrokod Core-RTM (*ang. Core-RTM - CRTM*). Źródło zaufania do pomiarów jest pierwszym elementem, który wysyła informacje istotne dla integralności (pomiary) do

źródła zaufania do magazynu. Zaufanie wobec tego elementu jest podstawą zaufania wobec wszystkich innych pomiarów. Źródło zaufania do magazynu obejmuje tożsamości elementów (pomiary) i inne poufne informacje. Moduł Trusted Platform Module (TPM) realizuje funkcje źródeł zaufania do magazynu oraz raportowania w zaufanej platformie obliczeniowej.

Technologia Intel TXT stanowi przykład źródła zaufania do pomiarów, a zarazem jest mechanizmem zapewniającym widoczność, zaufanie i kontrolę rozwiązań chmurowych. Technologia Intel TXT to zestaw elementów sprzętowych zaprojektowanych w celu ochrony wrażliwych informacji przed atakami programowymi. Elementy rozwiązania Intel TXT obejmują funkcje mikroprocesora, chipsetu, podsystemów wejścia/wyjścia oraz innych elementów platformy. W połączeniu z przystosowanym systemem operacyjnym i aplikacjami wykorzystującymi możliwości tej technologii, Intel TXT skutecznie chroni poufność i integralność danych w coraz bardziej wrogich środowiskach.

Technologia Intel TXT obejmuje szereg innowacji w zakresie bezpiecznego przetwarzania, w tym:

- **Wykonywanie chronione:** Pozwala aplikacjom działać w odizolowanych środowiskach, dzięki czemu żadne nieautoryzowane oprogramowanie na platformie nie może obserwować informacji operacyjnych ani wprowadzać do nich zmian. Każde z tych odizolowanych środowisk uruchamia aplikacje przy pomocy dedykowanych zasobów zarządzanych przez platformę.
- **Bezpieczne magazynowanie:** Zapewnia możliwość szyfrowania i przechowywania kluczy, danych i innych wrażliwych informacji w warstwie sprzętowej. Magazynowane dane mogą zostać odszyfrowane wyłącznie przez środowisko, które zaszyfrowało dane.
- **Atestacja:** Umożliwia systemowi zapewnienie, że chronione środowisko zostało poprawnie wywołane, a także dokonanie pomiaru oprogramowania działającego w chronionej przestrzeni. Osiąga się to w ramach procesu zaświadczenia opisanego w kolejnym podrozdziale. Informacje wymieniane podczas tego

procesu są znane jako klucze tożsamości atestacji i służą do zapewnienia wzajemnego zaufania między stronami.

- **Uruchomienie chronione:** Zapewnia kontrolowane uruchamianie i rejestrowanie krytycznych elementów oprogramowania systemowego w chronionym środowisku wykonawczym.

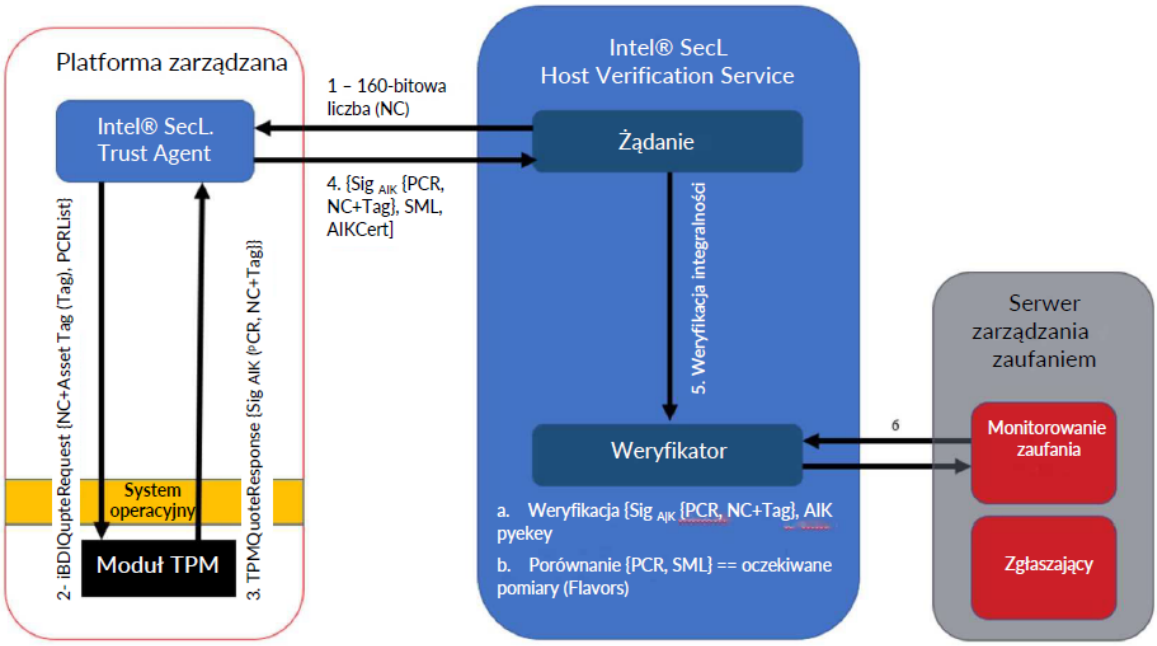
Rozwiązanie Intel TXT jest obsługiwane przez procesory Intel Xeon® Platinum Scalable oraz procesory poprzedniej generacji z serii Xeon E3, Xeon E5 i Xeon E7.

Działanie rozwiązania Intel TXT opiera się na stworzeniu mierzalnego środowiska startowego (*ang. measured launch environment – MLE*) umożliwiającego dokładne porównanie wszystkich krytycznych elementów środowiska startowego ze znanym wzorcem. Rozwiązanie Intel TXT tworzy kryptograficznie wyjątkowy identyfikator dla każdego zatwierdzonego elementu, a następnie zapewnia sprzętowy mechanizm egzekwowania zasad, który blokuje uruchamianie dowolnego niezgodnego kodu lub wskazuje sytuacje, w których oczekiwane zaufane uruchomienie nie nastąpiło w procesie bezpiecznej zdalnej atestacji. W tym drugim przypadku, gdy zaświadczenie wskazuje, że jeden lub więcej elementów poddanych pomiarom w ramach MLE nie spełnia oczekiwań, platforma jest uznawana za podejrzaną, a orkiestracja aplikacji może zostać wstrzymana, nawet jeśli sama platforma zostanie uruchomiona. To rozwiązanie sprzętowe stanowi podstawę, na której administratorzy IT mogą budować zaufane rozwiązania platformowe w celu ochrony przed agresywnymi atakami programowymi i zapewnienia lepszej kontroli nad środowiskami zwirtualizowanymi oraz chmurowymi.

A.3 ATESTACJA: BIBLIOTEKI INTEL SECURITY LIBRARIES (ISECL)

Organ przeprowadzający atestację udziela ostatecznych odpowiedzi na te pytania. Atestacja zapewnia kryptograficzny dowód zgodności, wykorzystując koncepcję źródła zaufania w celu zapewnienia skutecznych środków bezpieczeństwa dzięki zapewnieniu widoczności i użyteczności informacji z różnych źródeł zaufania. Rysunek 6 ilustruje protokół atestacji zapewniający możliwość przekazywania pomiarów na żądanie. Urządzenie zaświadczające musi mieć możliwość dokonania pomiarów

oprogramowania układowego BIOS, niskopoziomowych sterowników urządzeń oraz systemu operacyjnego i innych elementów, a także przekazania tych pomiarów do organu zaświadczającego. Urządzenie zaświadczające musi być w stanie dokonać tych pomiarów jednocześnie chroniąc integralność, autentyczność, wiarygodność, a w wybranych przypadkach także poufność tych pomiarów.



Rysunek 6: Protokół zdalnej atestacji

Poniżej zostały przedstawione kroki znajdujące się na rysunku 6 dotyczące protokołu zdalnej atestacji:

1. Na żądanie żądającego, system tworzy nieprzewidywalną liczbę jednorazową (*ang. non-predictable nonce – NC*) i wysyła ją do agenta zaświadczającego w węźle zaświadczającym wraz z wybraną listą rejestrów konfiguracji platformy (ang. *platform configuration registers – PCR*).
2. Agent zaświadczający przesyła to żądanie do modułu TPM jako TPMQuoteRequest wraz z liczbą jednorazową oraz listą PCR.
3. W odpowiedzi na żądanie TPMQuoteRequest moduł TPM ładuje klucz tożsamości zaświadczenia (*ang. attestation identity key - AIK*) z chronionej pamięci masowej w module TPM przy użyciu klucza głównego magazynu (*ang. storage*

root key - SRK), a następnie wykonuje polecenie TPM Quote, które jest używane do podpisywania wybranych rejestrów PCR i NC kluczem prywatnym AIKpriv. Dodatkowo agent zaświadczający pobiera dziennik zapisanych pomiarów (*ang. stored measurement log - SML*).

4. W kroku odpowiedzi agent zaświadczający wysyła odpowiedź składającą się z podpisanego sprawozdania, NC i SML. Agent zaświadczający dostarcza również poświadczenie AIK, w skład którego wchodzi klucz AIKpub podpisany przez Privacy-CA.
5. Na etapie weryfikacji integralności:
    a. Następuje weryfikacja, czy poświadczenie AIK zostało podpisane przez zaufany Privacy-CA, a tym samym pochodzi z prawdziwego modułu TPM. Żądający weryfikuje również, czy klucz AIKpub jest nadal ważny, sprawdzając listę unieważnień certyfikatów zaufanego wystawcy.
    b. Żądający weryfikuje podpis cytatu i sprawdza jego świeżość.
    c. Na podstawie otrzymanego SML i wartości PCR, żądający przetwarza SML, porównuje indywidualne skróty modułów ze znanymi prawidłowymi wartościami i wzorcami, a następnie ponownie oblicza otrzymane wartości PCR. Jeśli poszczególne wartości są zgodne ze znanymi prawidłowymi wartościami i jeśli obliczone wartości są zgodne z podpisaną wartością zbiorczą, zdalny węzeł jest uznawany za zaufany.
6. Weryfikator informuje menedżera o stanie zaufania zdalnego węzła. Menedżer rejestruje stan zaufania w swojej bazie danych zarządzania i używa go do obsługi wszelkich indywidualnych lub zagregowanych żądań dotyczących statusu urządzenia. Jeśli administrator obserwuje zdarzenia związane z zaufaniem, menedżer będzie również wysyłał powiadomienia e-mail, gdy zarządzany węzeł zdalny zostanie uznany za niezaufany.

Protokół ten może pomóc w ograniczeniu ataków powtórzeniowych, maskarady oraz manipulacji.

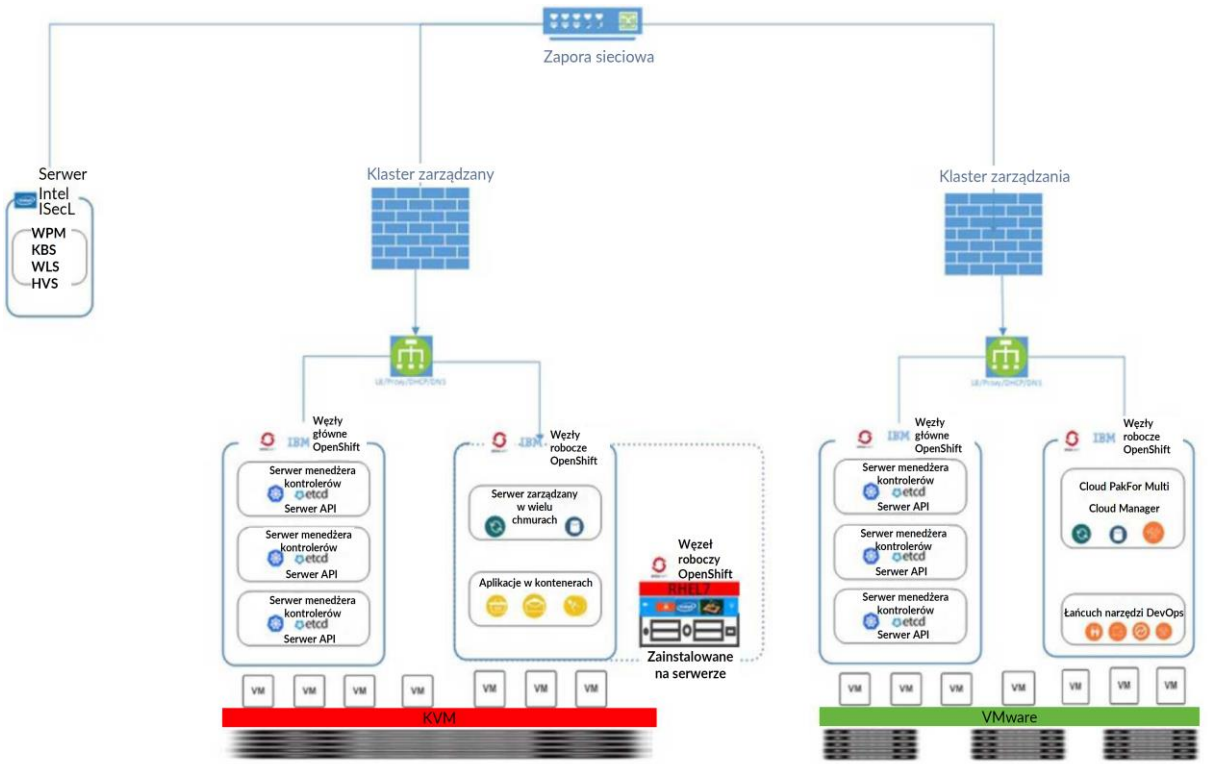
Po pomyślnym zainstalowaniu agenta zaufania ISecL i usługi weryfikacji hosta można utworzyć znaczniki zasobów i przydzielić je każdemu zarządzanemu serwerowi. Rozdział 6.4 instrukcji obsługi ISecL-DC v1.6 opisuje procedurę tworzenia i przydzielania oznaczeń zasobów.

ZAŁĄCZNIK B – WDROŻENIE ORKIESTRACJI APLIKACJI: OPENSHIFT

Załącznik zawiera dodatkowe informacje uzupełniające opisujące wszystkie niezbędne elementy i kroki wymagane do skonfigurowania przykładowego wdrożenia z wykorzystaniem rozwiązania OpenShift.

B.1 ARCHITEKTURA PRZYKŁADOWEGO WDROŻENIA

Kubernetes jest obecnie popularnym rozwiązaniem wykorzystywanym w celu budowania infrastruktur internetowych na szeroką skalę, które umożliwiają podmiotom korzystanie z innowacji, takich jak analityka, sztuczna inteligencja, uczenie maszynowe czy usługi dostępne w chmurze. Obsługa zaawansowanych technologii i tworzenie aplikacji natywnych dla chmury wymaga wykorzystania platform klasy korporacyjnej, takich jak Red Hat OpenShift. W tym załączniku znajduje się opis procesu tworzenia oraz konfiguracji klastrów OpenShift. Rysunek 7 ilustruje, w jaki sposób węzły przedstawione na rysunku 5 (w załączniku A) zostały logicznie wdrożone w formie dwóch klastrów OpenShift i serwera zdalnej atestacji.



Rysunek 7: Architektura przykładowego wdrożenia

W celu realizacji zadanych przypadków użycia, rozwiązanie OpenShift zostało wdrożone w formie dwóch oddzielnych klastrów – klastra zarządzającego opartego na rozwiązaniach VMWare i klastra zarządzanego opartego na infrastrukturze KVM. Każdy klaster dysponuje trzema węzłami płaszczyzny kontrolnej oraz trzema węzłami roboczymi, a także maszyną wirtualną obsługującą load balancer i system nazw domen (DNS) w celu symulacji zaufanego środowiska pracy kontenerów. Elementy MCM (*ang. Multicloud Management*) zostały zainstalowane na obu klastrach OpenShift. Klaster zarządzany (*ang. Multicloud Management*) jest wyposażony w element MCM Hub, który agreguje informacje z wielu klastrów przy użyciu asynchronicznego modelu żądań pracy. Klaster-hub (klaster zarządzający) zbiera informacje na temat statusu klastrów i aplikacji, a także zapewnia zestaw interfejsów API dla różnych funkcji jako centralny kontroler. Klaster zarządzany (*ang. Managed Cluster*) jest wyposażony w element MCM managed-cluster, który jest wykorzystywany w celu definiowania klastra. Z kolei inne zasoby, takie jak MCM Klusterlet są wykorzystywane i skonfigurowane w celu inicjowania połączenia z klastrem–koncentratorem. Klaster zarządzany odbiera żądania pracy i wykonuje je, a następnie zwraca wyniki.

B.2 INSTALACJA I KONFIGURACJA OPENSHIFT

Zarządzanie platformą OpenShift w wielu lokalizacjach wiąże się z wyzwaniami, takimi jak wysoka złożoność, komplikacja zarządzania oraz wysokie koszty. Niektóre problemy dotyczą między innymi zapewnienia widoczności wszystkich klastrów, by zobaczyć, na których urządzeniach działają elementy aplikacji, wyszukiwania systemów, które uległy awarii, monitorowania wykorzystania zasobów w chmurach i klastrach, a także zarządzania konfiguracją i zmianami w środowiskach. Rozwiązania IBM Cloud Pak for Multicloud Management/Red Hat Advanced Cluster Management for Kubernetes stanowią odpowiedź na te wyzwania. Opierają się na wytycznych społeczności Kubernetes i zawierają zaawansowane funkcje ważne z punktu widzenia tworzenia i obsługi środowisk klasy korporacyjnej.

Repozytorium polityk (*ang. Policies repository*), które jest częścią składnika koncentratora Manager (*ang. Manager hub*), stanowi część klastra zarządzającego. Repozytorium jest dostarczane z domyślnymi szablonami zgodności i polityk, jednak

na potrzeby tego wdrożenia zostały opracowane nowe zasady dotyczące środowiska, które pozwoliły na realizację integracji z węzłem atestacji Intel. Repozytorium stanowi magazyn polityk dotyczących klastra zarządzanego, a dokument zasad jest stosowany przy użyciu powiązania lokacji.

B.2.1. Klaster zarządzający oparty na rozwiązaniach VMware (klaster A)

Wymagania sprzętowe: Konfiguracja platformy OpenShift Container Platform (OCP) w wersji 4.3 w oparciu o rozwiązania VMware wymaga zapewnienia co najmniej jednego serwera ESXi i jednej maszyny wirtualnej pracującej pod kontrolą systemu operacyjnego CentOS/Red Hat w tej samej wirtualnej sieci lokalnej (VLAN) w lokalnym centrum danych. W przypadku przedstawionej konfiguracji, rozwiązanie obejmowało serwer wyposażony w 48-rdzeniowy procesor, 256 GB pamięci RAM i 2 TB pamięci masowej. Na serwerze została zainstalowana platforma ESXi. Maszyna wirtualna z systemem CentOS/Red Hat jest wymagana tylko przez kilka godzin i może zostać usunięta po zakończeniu instalacji.

Konfiguracja sieci: Adresy IP użyte w tym procesie i pliki konfiguracyjne pochodzą ze środowiska National Cybersecurity Center of Excellence (NCCoE) – krajowego centrum doskonalenia w cyberbezpieczeństwie. Zostały wykorzystane na potrzeby niniejszego dokumentu jedynie w celach ilustracyjnych. Oprócz konfiguracji rozwiązania ESXi i serwera vCenter, wymagane jest co najmniej 16 adresów IP, które zostaną przypisane do maszyn wirtualnych. Każdy węzeł obsługujący maszynę wirtualną wymaga jednego adresu IP. Zalecana minimalna liczba 16 adresów IP wynika z konfiguracji rozwiązania: 1 węzeł pomocniczy + 1 węzeł rozruchowy + 3 węzły sterowania + 3 węzły robocze = 8 węzłów. Dodatkowe adresy IP są dostępne na wypadek, gdyby w przyszłości pojawiła się potrzeba uruchomienia dodatkowych węzłów roboczych. W ramach tego wdrożenia, rozwiązanie vCenter zostało uruchomione w tej samej podsieci IP, zatem w sumie wykorzystano 9 adresów IP.

Wymagania dotyczące maszyn wirtualnych VMware OCP: Tabela 1 zawiera listę maszyn wirtualnych utworzonych na serwerze VMware wraz z wymaganiami sprzętowymi i rolami pełnionymi w klastrze.

Tabela 1: Maszyny wirtualne zainstalowane na klastrze zarządzania opartym na oprogramowaniu VMware

Nazwa węzła	Liczba wirtualnych procesorów (vCPU)	Pamięć operacyjna (w GB)	Pamięć masowa (w GB)	Rola
Helper Node (Węzeł Pomocniczy)	4	16	150	Instalator LB/DNS/Proxy/DHCP/OCP
Bootstrap-0	4	16	150	Uruchomienie OCP
Control-plane-0	4	16	150	Kontroler OCP
Control-plane-1	4	16	150	Kontroler OCP
Control-plane-2	4	16	150	Kontroler OCP
compute-0	4	16	150	Węzeł obliczeniowy OCP
compute-1	4	16	150	Węzeł obliczeniowy OCP
compute-2	4	16	150	Węzeł obliczeniowy OCP

Podręczniki wdrożenia OCP w środowisku VMware: Aby wdrożyć OCP 4.3 w środowisku VMware, należy pobrać następujące repozytorium Git: https://github.com/fctoibm/ocpvmware4.3 i postępować zgodnie z instrukcjami, by uruchomić podręczniki (*ang. playbooks*). Należy upewnić się, że informacje w plikach vars.yaml oraz host.yaml są zgodne z informacjami sieciowymi dotyczącymi danego środowiska.

B.2.2. Klaster zarządzany oparty na rozwiązaniu KVM (klaster B)

Drugi klaster OCP jest klastrem zarządzanym. Obejmuje rozwiązanie MCM Klusterlet, które zapewnia, że każdy zarządzany klaster przestrzega obowiązujących polityk.

Wymagania sprzętowe: W przypadku przedstawionej konfiguracji, rozwiązanie obejmowało serwer działający pod kontrolą systemu operacyjnego CentOS z 48-rdzeniowym procesorem, 256 GB pamięci RAM i 1 TB pamięci masowej. Do stworzenia oraz zarządzania maszynami wirtualnymi zostało wykorzystane rozwiązanie KVM. Wykorzystane narzędzie wiersza poleceń KVM to virt-install, z kolei narzędzie graficznego interfejsu użytkownika (GUI) to virt-manager. W celu skorzystania z narzędzia GUI do konfiguracji maszyn wirtualnych KVM, należy zainstalować środowisko graficzne Gnome oraz rozwiązanie VNC na serwerze CentOS. Wszystkie maszyny wirtualne uruchamiane na klastrze zarządzanym zostaną uruchomione na pojedynczym hoście KVM skonfigurowanym z nazwą hosta wolfpass2 – ta sama nazwa została użyta w tabeli oraz w rysunku 5 (w załączniku A).

Konfiguracja sieci: Adresy IP użyte w tym procesie i pliki konfiguracyjne pochodzą ze środowiska NCCoE. Zostały wykorzystane na potrzeby niniejszego dokumentu jedynie w celach ilustracyjnych. Instalacja OCP w środowisku opartym na KVM wymaga co najmniej 16 możliwych do przydzielenia adresów IP. Każdy węzeł obsługujący maszynę wirtualną wymaga jednego adresu IP. Zalecana minimalna liczba 16 przypisywanych adresów IP wynika z konfiguracji rozwiązania: 1 węzeł pomocniczy + 1 węzeł rozruchowy + 3 węzły sterowania + 3 węzły robocze = 8 węzłów. Dodatkowe adresy IP są dostępne na wypadek, gdyby w przyszłości pojawiła się potrzeba uruchomienia dodatkowych węzłów roboczych. Przed rozpoczęciem wdrożenia należy odpowiednio zaplanować przestrzeń adresową IP.

Wymagania dotyczące maszyn wirtualnych KVM OCP: Tabela 2 zawiera listę maszyn wirtualnych utworzonych na serwerze KVM wraz z wymaganiami sprzętowymi i rolami pełnionymi w klastrze.

Tabela 2: Maszyny wirtualne zainstalowane na klastrze zarządzanym opartym na oprogramowaniu KVM

Nazwa węzła	Liczba wirtualnych procesorów (vCPU)	Pamięć operacyjna (w GB)	Pamięć masowa (w GB)	Rola
Helper Node (Węzeł Pomocniczy)	4	16	150	Instalator DNS/Proxy/DHCP/OCP
Bootstrap	4	16	150	Uruchomienie OCP
Master0	4	16	150	Kontroler OCP
Master1	4	16	150	Kontroler OCP
Master2	4	16	150	Kontroler OCP
Worker0	4	16	150	Węzeł obliczeniowy OCP
Worker1	4	16	150	Węzeł obliczeniowy OCP

Uwaga: Klaster OpenShift wymaga trzech węzłów roboczych, jednak ze względu na to, że w przypadku przedstawionego wdrożenia wykorzystywany jest dodatkowy serwer fizyczny dla trzeciego węzła roboczego, uruchamiane są tylko dwie maszyny wirtualne węzłów roboczych.

Podręczniki wdrożenia OCP w środowisku KVM: Aby wdrożyć OCP 4.3 w środowisku KVM, należy pobrać następujące repozytorium Git: https://github.com/fctoibm/ocpkvm4.3 i postępować zgodnie z instrukcjami, by uruchomić podręczniki. Należy upewnić się, że informacje w plikach vars.yaml oraz host.yaml są zgodne z informacjami sieciowymi dotyczącymi danego środowiska.

Podręcznik wdrażania OCP w środowisku KVM tworzy wszystkie węzły robocze jako maszyny wirtualne. Aby utworzyć polityki oparte na sprzętowych źródłach zaufania, do klastra musi zostać dodany serwer fizyczny obsługujący funkcje Intel TXT oraz

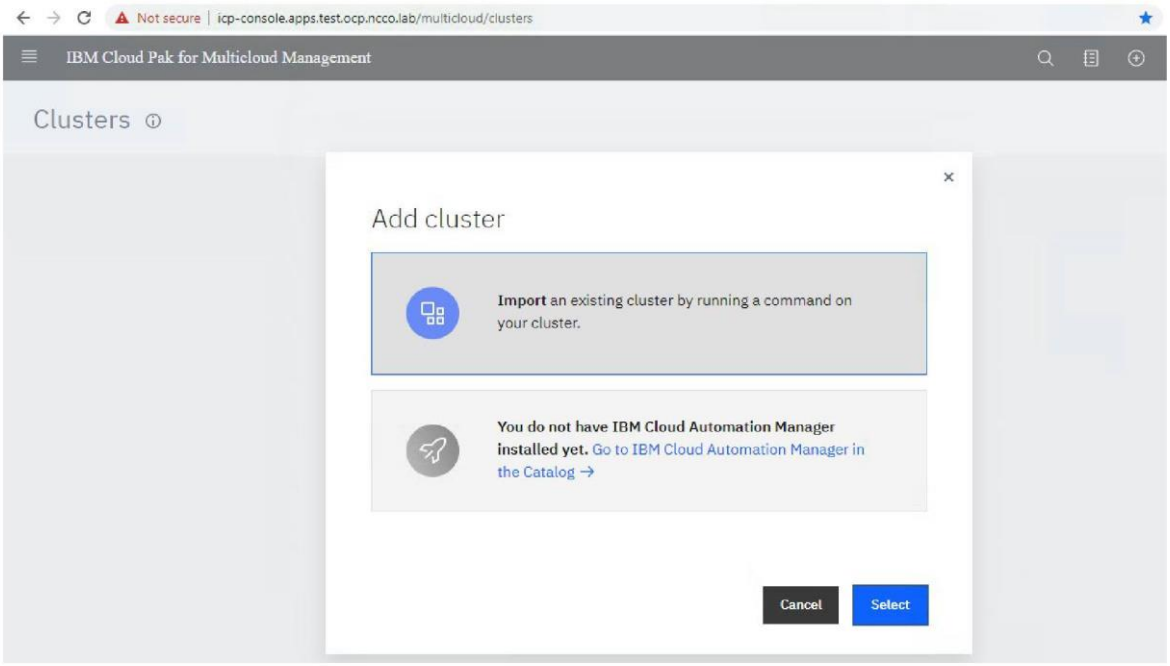
sprzętowy moduł bezpieczeństwa TPM jako dodatkowy węzeł roboczy. Serwer ten musi pracować pod kontrolą systemu operacyjnego Red Hat Enterprise Linux (RHEL) i mieć zainstalowane rozwiązanie Intel Trust Agent, opisane w załączniku A.2. W przypadku serwera fizycznego dokumentacja OpenShift szczegółowo opisuje sposób dodawania węzła obliczeniowego RHEL do istniejącego klastra.

B.2.3. Instalacja rozwiązania MCM Pak 1.3 (MCM HUB – VMware)

Aby zainstalować rozwiązanie MCM Pak 1.3 w środowisku OCP 4.3, konieczne jest zakończenie instalacji OCP 4.3 oraz posiadanie uprawnień dostępu na poziomie administratora. Niniejszy dokument zakłada, że rozwiązanie OCP 4.3 zostało zainstalowane przy użyciu tego samego repozytorium GitHub i z tym samym plikiem vars.yaml.

Wdrażanie rozwiązania MCM Pak: Instalacyjne repozytorium Git obsługuje dwie opcje – instalację w środowisku VMware lub KVM. W razie potrzeby oba te rozwiązania konfigurują maszyny wirtualne. Maszyna wirtualna o nazwie PakHelper node posłuży jako klient w celu instalacji rozwiązania MCM Pak. Nie ma potrzeby wdrażania maszyny wirtualnej, jeśli w tej samej sieci dostępna jest już maszyna wirtualna działająca pod kontrolą systemu operacyjnego CentOS 7. Jeśli maszyna wirtualna CentOS 7 jest już dostępna, należy pominąć opcje 1 i 2. Z kolei, jeśli stosowna maszyna wirtualna nie istnieje, należy wykonać opcje 1 lub 2 oraz 3 z następującego repozytorium Git: https://github.com/fctoibm/mcmpak1.3 i postępować zgodnie z instrukcjami, by uruchomić podręczniki.

Dodawanie klastra OCP opartego na środowisku KVM jako klastra zarządzanego w rozwiązaniu MCM: Po instalacji rozwiązania MCM Pak klaster OCP oparty na środowisku KVM można zaimportować do rozwiązania IBM MCM, co umożliwia zarządzanie. Aby to zrobić, należy przejść do interfejsu użytkownika MCM, a następnie przejść do zakładki zarządzania klastrami (Clusters Management). Jak widać na rysunku 8, rozwiązanie oferuje możliwość zaimportowania istniejącego klastra. Aby zaimportować istniejący klaster OCP oparty na środowisku KVM, należy wykonać kroki opisane w stosownym artykule dostępnym w Centrum wiedzy IBM.

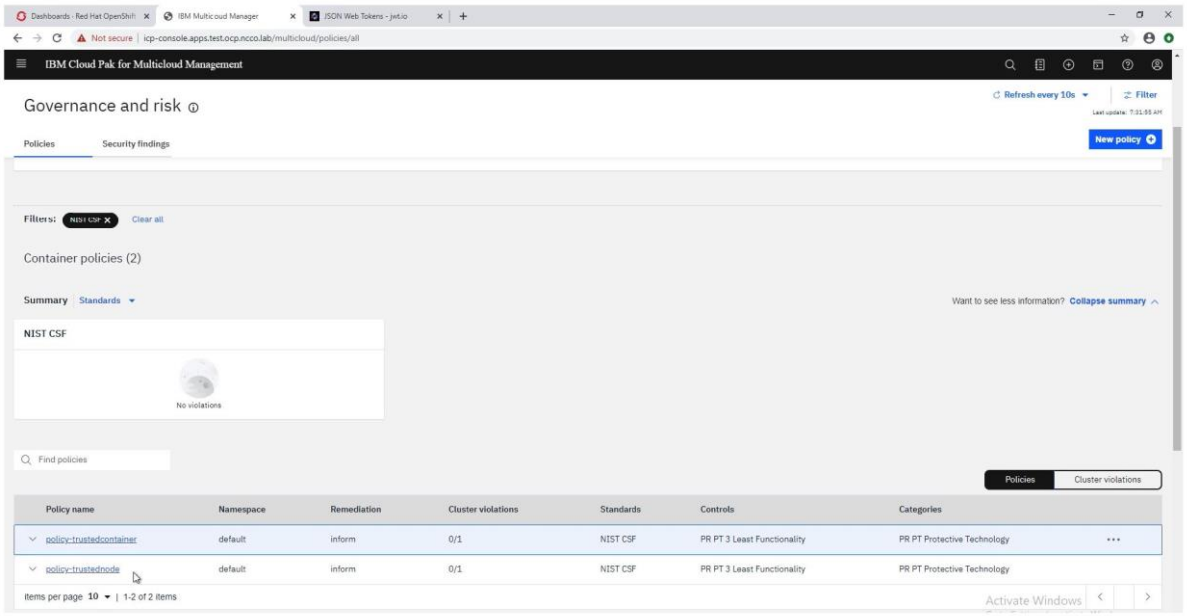


Rysunek 8: Konsola MCM pozwalająca na importowanie klastra

Tworzenie zasad dla klastra zarządzanego: Po pomyślnym zaimportowaniu klastra OCP opartego na środowisku KVM, można utworzyć oraz zastosować określone polityki zarządzające orkiestracją obciążeń. Zasady są tworzone w rozwiązaniu MCM Hub i przesyłane do każdego zarządzanego klastra, gdzie są egzekwowane.
W przykładowym wdrożeniu zostały wprowadzone dwie polityki:

1. Zasada „Trusted Node Policy" pozwala na zagwarantowanie, że wszystkie węzły w klastrze są zaufane i atestowane. W trybie informacyjnym zgodnie z zasadą następuje rejestracja każdego przypadku naruszenia statusu zaufania węzła. W trybie egzekwowania zgodnie z zasadą dany węzeł jest wyłączany i usuwany z klastra.
2. Zasada „Trusted Container Policy" zapewnia, że wszystkie obciążenia uruchamiane w przestrzeni nazw korzystają z zestawu obrazów z określonej ścieżki rejestru. Infrastruktura jest skonfigurowana w taki sposób, że w podanej ścieżce znajdują się jedynie zaszyfrowane obrazy kontenerów. Dzięki temu w przestrzeni nazw uruchamiane są tylko zaszyfrowane obrazy.

Rysunek 9 przedstawia wspomniane dwie zasady w interfejsie użytkownika, utworzone dla zarządzanych klastrów.



Rysunek 9: Zasady dotyczące klastrów zarządzanych

Oprócz tych dwóch polityk, w systemie zostało skonfigurowane zadanie Tekton, które stanowi element środowiska OpenShift, przeprowadzające szereg kontroli oraz szyfrujące obrazy. Ten bezpieczny proces zajmuje się tworzeniem, skanowaniem podatności i szyfrowaniem. Więcej informacji na temat tego procesu znajduje się w Załączniku C.

ZAŁĄCZNIK C – WDROŻENIE SZYFROWANIA APLIKACJI I OBCIĄŻEŃ

Załącznik zawiera dodatkowe informacje uzupełniające opisujące wszystkie wymagane elementy i kroki wymagane do skonfigurowania przykładowego wdrożenia z wykorzystaniem szyfrowania kontenerów.

C.1 ARCHITEKTURA PRZYKŁADOWEGO WDROŻENIA

Stosowny schemat architektury został przedstawiony na rysunku 7 znajdującym się w Załączniku B.

C.2 KONFIGURACJA SZYFROWANIA APLIKACJI I OBCIĄŻEŃ

Poszczególne elementy ekosystemu kontenerów umożliwiają szyfrowanie aplikacji i obciążeń poprzez szyfrowanie obrazów kontenerów. Technologia ta opiera się na specyfikacji obrazu kontenera opracowanego przez zespół Open Container Initiative (OCI). Komponenty, które wspierają korzystanie z tego rozwiązania to:

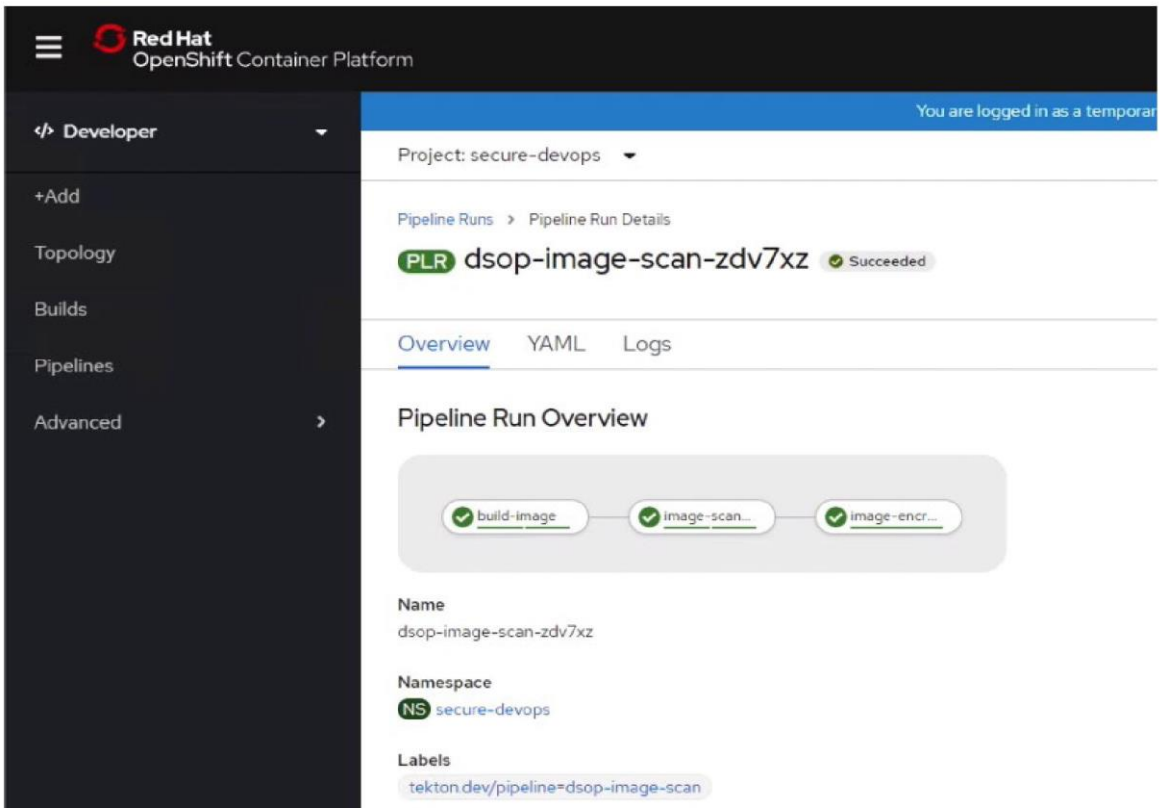
- **Tworzenie:** Narzędzie Skopeo służy do szyfrowania obrazów kontenerów i przesyłania ich do rejestru.
- **Uruchamianie:** Środowisko uruchomieniowe kontenerów Cri-o stanowi element platformy OpenShift i zostało skonfigurowane do odszyfrowywania obrazów. Jest to domyślne środowisko uruchomieniowe węzłów roboczych OpenShift 4.3 i obsługuje odszyfrowywanie obrazów kontenerów zgodnych ze specyfikacją OCI.
- **Rejestr:** Rejestr dystrybucji Docker Distribution Registry służy do przesyłania, pobierania i przechowywania zaszyfrowanych obrazów. W przykładowym wdrożeniu została wykorzystana wersja 2.7.1 rozwiązania.

Te elementy stanowią podstawowe komponenty systemu szyfrowania aplikacji i obciążeń. Na potrzeby przykładu konieczne było skonfigurowanie integracji z interfejsami API rozwiązania ISecL Attestation Hub, aby zaprezentować szyfrowanie obciążeń i obrazów z atestacją sprzętową. Określono także niestandardowy schemat metadanych szyfrowania kontenera do pracy z brokerem kluczy ISecL. Referencyjny kod implementacji i dokumentacja znajdują się w repozytorium https://github.com/lumjjb/seclkeywrap.

Kluczowe punkty integracji to:

- Określenie niestandardowego schematu metadanych szyfrowania kontenera do pracy z brokerem kluczy ISecL.
- Zainstalowanie poprawek elementów CRI-0 i Skopeo, aby umożliwić korzystanie z niestandardowego protokołu ISecL. Poprawki są dostępne w repozytoriach https://github.com/lumjjb/cri-o/tree/sample_integration oraz https://github.com/lumjjb/skopeo/tree/sample_integration.

W ramach cyklu DevSecOps rozwiązania te zostały zintegrowane z procesem Tekton w celu kompilacji, kontroli bezpieczeństwa i szyfrowania obrazów. Odpowiedni proces można podejrzeć za pośrednictwem pulpitu nawigacyjnego OpenShift, przełączając się do roli Developer i wybierając menu „Pipelines" – przedstawione na rysunku 10. Definicje obiektów Tekton są dostępne pod adresem: https://gist.github.com/lumjjb/22191008f849f240851aec8a1ee0304d



Rysunek 10: Tworzenie procesu deszyfrowania obrazów

Tłumaczenie

ZAŁĄCZNIK D – TRUSTED SERVICE IDENTITY (TSI)

Załącznik zawiera informacje uzupełniające opisujące wszystkie wymagane elementy i kroki wymagane do skonfigurowania przykładowej implementacji wykorzystującej rozwiązania Trusted Service Identity (TSI).

D.1 OMÓWIENIE TSI

Rozwiązanie TSI zapewnia ochronę dostępu do wrażliwych danych, zapewniając, że tylko atestowane usługi objęte ograniczeniami dotyczącymi lokalizacji mogą uzyskać dostęp do poświadczeń. Proces opiera się na wykorzystaniu tożsamości aplikacji lub obciążenia, w skład której wchodzą dane na temat tożsamości zaufanego urządzenia, które zostały w pełni zaświadczone przez rozwiązanie Intel TXT, w tym lokalizacji i regionu centrum danych oraz różnych pomiarów dokonywanych w środowisku uruchomieniowym, takich jak nazwa obrazu i klastra, wyjątkowe identyfikatory oraz przestrzeń nazw w celu identyfikacji aplikacji. Pomiary te są bezpiecznie podpisywane przez usługę działającą na każdym węźle hosta, w oparciu o łańcuch zaufania utworzonego podczas bezpiecznego uruchamiania środowiska, a następnie stale atestowane i weryfikowane.

Każdemu kontenerowi, który wymaga dostępu do sekretów w celu uzyskania dostępu do wrażliwych danych, przypisywana jest krótkotrwała zmierzona tożsamość w postaci tokenu JSON Web Token (JWT), który jest podpisywany przy pomocy źródła zaufania przez zaświadczony proces. Ta mierzona tożsamość jest formą *efemerycznej biometrii cyfrowej* o krótkim czasie ważności.

Przykładowe wdrożenie obejmuje klaster Kubernetes oparty na platformie OpenShift rozszerzonej przy pomocy rozwiązania TSI, w którym każdy węzeł dysponuje pośrednim urzędem certyfikacji podpisanym przez główny urząd certyfikacji podczas procesu bezpiecznego uruchamiania klastra.

Podczas uruchamiania proces instalacji uzyskuje raport atestacji (Security Assertion Markup Language [SAML]) z serwera zaświadczającego dla każdego węzła roboczego. Raport jest następnie sprawdzany w celu weryfikacji, czy wszystkie elementy (system operacyjny, platforma i oprogramowanie) są zaufane, a proces uruchamiania pobiera

pola tożsamości węzłów roboczych ze znacznika zasobu w raporcie. Każdy węzeł roboczy uruchamia również usługę podpisywania JWT (JSS), która zawiera organ podpisujący wykorzystujący sprzętowy moduł bezpieczeństwa TPM w celu ochrony swojego indywidualnego klucza prywatnego.

Główny urząd certyfikacji jest bezpiecznie przechowywany w magazynie, który jest rozszerzony o wtyczkę TSI Authentication Vault.

D.2 INSTALACJA I KONFIGURACJA ROZWIĄZANIA TSI

Rozwiązanie TSI wymaga procesu atestacji w celu dokładnego określenia tożsamości węzłów roboczych hostujących kontenery aplikacji. W przykładowym wdrożeniu rozwiązanie TSI opiera się na serwerze ISecL, wdrożonego w celu przypisywania tożsamości węzłom roboczym. Proces szczegółowo opisujący integrację rozwiązania TSI z ISecL można znaleźć w repozytorium: https://github.com/IBM/trusted-service-identity/blob/intel-asset/README.md#attestation.

Proces ten wymaga realizacji dwóch niezależnych etapów:

- **Rejestracja zasobów za pomocą serwera Intel Verification Server**: Zaufany proces uruchamiania odpowiedzialny za instalację środowiska musi poprawnie ustawić atrybuty tożsamości każdego węzła roboczego. Te wartości tożsamości w postaci oznaczeń zasobów są bezpiecznie przechowywane w modułach TPM hostów. W rezultacie są one uwzględniane w raporcie SAMLattestation, który zawiera również wszystkie wyniki atestacji dla systemu operacyjnego, platformy oraz zaufanego oprogramowania. Proces ten został przeprowadzony w ramach kroków opisanych w Załączniku A.
- **Wdrożenie rozwiązania TSI z zaświadczeniem**: Przykładowe wdrożenie opisane w niniejszym dokumencie pozwala na wykorzystanie serwera atestacji Intel Attestation Server w celu uzyskania tożsamości węzłów roboczych. W celu skonfigurowania instalacji TSI do współpracy z serwerem Intel Attestation Server wymagane jest wprowadzenie kilku zmian. Co więcej, sprzętowy moduł bezpieczeństwa TPM jest współdzielony przez rozwiązania Intel Trust Agent oraz usługę podpisywania JWT rozwiązania TSI, przez co wymaga zastosowania

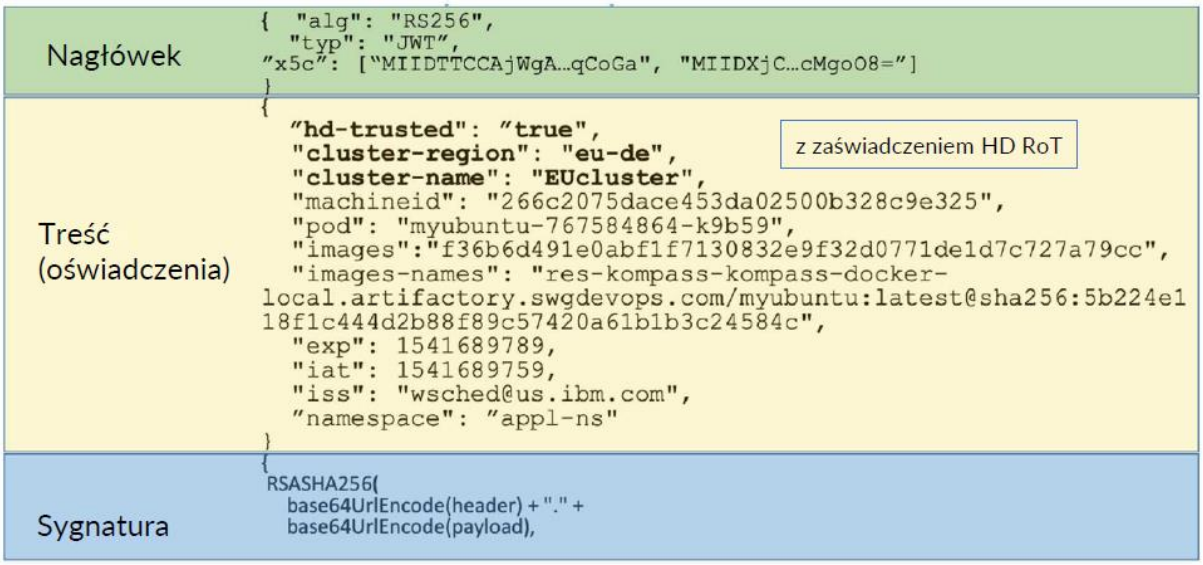
proxy TPM. Szczegółowe informacje na temat sugerowanych zmian konfiguracji można znaleźć w repozytorium https://github.com/IBM/trusted-service-identity/blob/intel- asset/README.md#attestation.

W wyniku tych zmian rozwiązanie TSI zostanie zainstalowane w klastrze, wykorzystując raport atestacji z usługi atestacji Intel Attestation Service w celu zapewnienia tożsamości węzłów roboczych i utrzymania procesu atestacji.

Zanim sekrety będą mogły zostać przekazane do kontenera aplikacji, najpierw muszą zostać utworzone w magazynie Secret Store (Vault). W celu przekazania sekretów należy postępować zgodnie z instrukcją w repozytorium: https://github.com/IBM/trusted-service-identity/blob/master/examples/vault/README.md#secrets.

Po uruchomieniu aplikacji sekrety zostaną przekazane na podstawie tożsamości aplikacji, a także jej środowiska uruchomieniowego oraz lokalizacji. W rezultacie sekret zostanie dostarczony do pamięci kontenera i w żadnym momencie nie będzie przechowywany w klastrze Kubernetes, jednocześnie z punktu widzenia aplikacji nie są wymagane żadne dodatkowe zmiany.

Rysunek 11 przedstawia przykładowy token JWT utworzony przez rozwiązanie TSI. Warto zwrócić uwagę na to, że składa się z trzech części: nagłówka, treści zawierającej twierdzenia oraz sygnaturę do weryfikacji.



Rysunek 11: Przykładowy token JWT utworzony przez rozwiązanie TSI

Treść zawiera pomiary dotyczące tożsamości aplikacji. Zawierają one pewne wartości statyczne, takie jak cluster-region (np. Niemcy, eu-de), cluster-name, indywidualny identyfikator urządzenia (*ang. machineid*), który stanowi wyjątkowy identyfikator węzła roboczego, a także szereg pomiarów, takich jak przestrzeń nazw, unikalny identyfikator oraz lista obrazów. Obrazy te zawierają sygnaturę obrazu, dzięki czemu możliwa jest weryfikacja obrazu i zagwarantowanie, że aplikacja uruchamia kod, który ma być uruchomiony oraz że kod nie został zmodyfikowany. Wartość hd-trusted określa, czy wszystkie zaświadczone elementy są zaufane.

Wartości parametrów cluster-name, cluster-region i hd-trusted są niezbędne w celu określenia tożsamości zasobów obliczeniowych i są odczytywane z serwera atestacji Intel Attestation Server. Token zawiera również znacznik czasu wygaśnięcia tokena, zwykle ustawiony na jedną minutę, co zapewnia ich tymczasowość i krótkotrwałość, a także ochronę przed wyciekiem. Są to pomiary środowiska uruchomieniowego, które reprezentują tożsamość aplikacji, podpisane przy pomocy źródła zaufania i wykorzystywane do oceny pod kątem zasad udostępniania sekretów.

Sekrety przechowywane w magazynie są chronione na podstawie ustalonych polityk. Zasady obejmują rodzaj (*ang. policytype*) oraz atrybuty – te same, które są wykorzystywane do tworzenia twierdzeń, wskazujące ścieżkę do sekretu. Jeśli twierdzenia podane w żądaniu są zgodne ze ścieżką atrybutu zasady, sekret zostanie udostępniony aplikacji.

ZAŁĄCZNIK E – NAZEWNICTWO ZABEZPIECZEŃ ZGODNE Z OPUBLIKOWANYM DOKUMENTEM NSC 800-53 ORAZ INNYMI PUBLIKACJAMI

Główne zabezpieczenia z katalogu środków bezpieczeństwa opisanych w dokumencie NSC 800-53, wpływające na przykładowe wdrożenie zabezpieczeń platformy kontenerowej, obejmują:

- AU-2, Audyt zdarzeń
- CA-2, Ocena zabezpieczeń
- CA-7, Ciągłe monitorowanie
- CM-2, Konfiguracja bazowa
- CM-3, Zabezpieczanie zmian konfiguracji
- CM-8, Inwentaryzacja komponentów systemu
- IR-4, Obsługa incydentów
- SA-9, Usługi systemu zewnętrznego
- SC-1, Polityka i procedury [dot. kategorii ochrony systemów i sieci telekomunikacyjnych]
- SC-7, Ochrona połączeń brzegowych
- SC-29, Heterogeniczność systemu
- SC-32, Dzielenie systemu na partycje
- SC-36, Przetwarzanie i przechowywanie rozproszone
- SI-3, Zabezpieczenie przed złośliwym kodem
- SI-4, Monitorowanie systemu
- SI-6, Weryfikacja funkcji bezpieczeństwa i ochrony prywatności
- SI-7, Aplikacje, oprogramowanie układowe i integralność informacji

Tabela 3 obejmuje listę funkcji bezpieczeństwa zapewnianych przez przykładowe wdrożenie:

Tabela 3: Funkcje bezpieczeństwa zapewniane przez przykładowe wdrożenie

Kategoria funkcji	Numer funkcji	Nazwa funkcji
IC1 – Pomiary	IC1.1	Mierzalny rozruch systemu BIOS
	IC1.2	Ustalenie poziomu bazowego dla pomiarów systemu BIOS (lista dopuszczalnych wartości)
	IC1.3	Zdalne zatwierdzenie pomiarów wykonanych w czasie rozruchu
	IC1.4	Zdolność do ochrony i wykrywania konfiguracji
IC2 – Weryfikacja oznaczeń	IC2.1	Weryfikacja oznaczeń zasobów
IC3 – Realizacja polityk	IC3.1	Przekazywanie obciążeń w oparciu o polityki
	IC3.2	Migracja obciążeń w oparciu o polityki
	IC3.3	Odszyfrowywanie obciążeń w oparciu o polityki
	IC3.4	Dostęp do obciążeń w oparciu o polityki
IC4 – Sprawozdawczość	IC4.1	Obsługa ciągłego monitorowania
	IC4.2	Obsługa przygotowywania sprawozdań na żądanie
	IC4.3	Obsługa wysyłania powiadomień o zdarzeniach dotyczących zaufania

Tabela 4 zestawia funkcje oraz możliwości w zakresie ochrony wymienione w tabeli 3 ze środkami bezpieczeństwa określonymi w dokumencie NSC 800-53, które zostały wymienione w formie listy na początku niniejszego załącznika.

Tabela 4: Zestawienie funkcji i możliwości w zakresie ochrony ze środkami bezpieczeństwa określonymi w dokumencie NSC 800-53

Środek bezpieczeństwa określony w dokumencie NSC 800-53	Pomiary				Weryfikacja znaczników	Egzekwowanie polityk				Raportowanie		
	IC1.1	IC1.2	IC1.3	IC1.4	IC2.1	IC3.1	IC3.2	IC3.3	IC3.4	IC4.1	IC4.2	IC4.3
AU-2										X	X	X
CA-2				X						X	X	
CA-7										X	X	
CM-2		X		X	X							
CM-3	X		X		X							
CM-8				X	X							
IR-4												X
SA-9						X	X					
SC-1						X	X					
SC-7	X			X		X	X					
SC-29						X	X					
SC-32					X	X	X					
SC-36					X	X	X					
SI-3	X	X		X						X	X	
SI-4		X	X	X						X	X	
SI-6	X	X	X	X								
SI-7	X	X	X			X	X					

ZAŁĄCZNIK F – ZESTAWIENIE PODKATEGORII RAM CYBERBEZPIECZEŃSTWA

Niniejszy załącznik stanowi zestawienie głównych funkcji oraz możliwości w zakresie cyberbezpieczeństwa przykładowego wdrożenia opartego na zaufanej lokalizacji geograficznej do następujących podkategorii wymienionych w ramach cyberbezpieczeństwa [5]:

- ID.GV-1: Opracowana jest strategia bezpieczeństwa informacji w organizacji.
- ID.GV-3: Wymagania prawne i ustawowe cyberbezpieczeństwa, w tym zobowiązania dotyczące prywatności i swobód obywatelskich, zostały zrozumiane i są kontrolowane.
- PR.DS-6: Mechanizmy kontroli integralności służą do weryfikacji oprogramowania, oprogramowania układowego i integralności informacji.
- PR.IP-5: Strategia i przepisy dotyczące fizycznego środowiska roboczego względem aktywów organizacyjnych są wypełnione.

ZAŁĄCZNIK G – AKRONIMY I INNE ZASTOSOWANE SKRÓTY

Wybrane akronimy i skróty użyte w treści niniejszego sprawozdania rozwinięte i zdefiniowane poniżej.

Dodatkowo patrz: NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.*

Akronim	Terminologia angielska	Terminologia polska
AIK	Attestation Identity Key	Klucz tożsamości atestacji
API	Application Programming Interface	Interfejs programistyczny aplikacji
BIOS	Basic Input/Output System	Podstawowy system wejścia/wyjścia
CA	Certificate Authority	Urząd certyfikacji
CPU	Central Processing Unit	Procesor
CRTM	Core Root of Trust for Measurement	Główne źródło zaufania do pomiarów
DHCP	Dynamic Host Configuration Protocol	Protokół DHCP; protokół dynamicznego konfigurowania hostów
DNS	Domain Name System	System DNS; system nazw domen
GB	Gigabyte	Gigabajt
HD	Hard Drive	Dysk twardy
HDD	Hard Disk Drive	Napęd dysku twardego
IaaS	Infrastructure as a Service	Infrastruktura jako usługa
Intel TXT	Intel Trusted Execution Technology	Technologia Intel Trusted Execution
I/O	Input/Output	Wejście/wyjście

Akronim	Terminologia angielska	Terminologia polska
IP	Internet Protocol	Internet Protocol (nazwa protokołu)
IR	Interagency or Internal Report	Sprawozdanie międzyresortowe lub Sprawozdanie wewnętrzne
ISecL	Intel Security Libraries	Biblioteki zabezpieczeń Intel
ISecL-DC	Intel Security Libraries for Data Center	Nazwa własna rozwiązania Intel
IT	Information Technology	Technologia informacyjna
ITL	Information Technology Laboratory	Laboratorium informatyczne
JSON	JavaScript Object Notation	JavaScript Object Notation – nazwa formatu danych
JSS	JWT Signing Service	Usługa podpisywania JWT
JWT	JSON Web Token	JSON Web Token – nazwa własna otwartego standardu
KVM	Kernel-Based Virtual Machine	Maszyna wirtualna oparta na jądrze, także nazwa własna środowiska maszyn wirtualnych w systemie GNU/Linux
MCM	Multicloud Management	Zarządzanie wieloma chmurami
MLE	Measured Launch Environment	Mierzalne środowisko startowe
NC	Nonce	Liczba jednorazowa
NCCoE	National Cybersecurity Center of Excellence	Krajowe centrum doskonalenia cyberbezpieczeństwa
NIST	National Institute of Standards and Technology	Narodowy Instytut Standaryzacji i Technologii

Akronim	Terminologia angielska	Terminologia polska
OCI	Open Container Initiative	Nazwa własna projektu
OCP	OpenShift Container Platform	Nazwa własna platformy kontenerowej OpenShift
OS	Operating System	System operacyjny
PCR	Platform Configuration Register	Rejestr konfiguracji platformy
RAM	Random-Access Memory	Pamięć o dostępie swobodnym
RHEL	Red Hat Enterprise Linux	Nazwa własna dystrybucji systemu operacyjnego GNU/Linux
RTM	Root of Trust for Measurement	Źródło zaufania do pomiarów
RTR	Root of Trust for Reporting	Źródło zaufania do raportowania
RTS	Root of Trust for Storage	Źródło zaufania do magazynu
SAML	Security Assertion Markup Language	Security Assertion Markup Language (nazwa protokołu)
SML	Stored Measurement Log	Dziennik zapisanych pomiarów
SP	Special Publication	Publikacja specjalna
SRK	Storage Root Key	Klucz główny magazynu
TB	Terabyte	Terabajt – jednostka używana w informatyce między innymi do określania rozmiaru największych pamięci masowych, zasobów plików i baz danych
TPM	Trusted Platform Module	Sprzętowy moduł bezpieczeństwa, moduł TPM

Akronim	Terminologia angielska	Terminologia polska
TSI	Trusted Service Identity	Identyfikacja zaufanych usług
VLAN	Virtual Local Area Network	VLAN – Wirtualna sieć lokalna
VM	Virtual Machine	VM – Maszyna wirtualna