MC

Tłumaczenie standardów i rekomendacji
w zakresie cyberbezpieczeństwa

Zabezpieczenia sprzętowe:

Prototyp zabezpieczeń platformy kontenerowej

NIST IR 8320A_wer. 1.0_PL

NIST IR 8320A_wer. 1.0_PL

26 marca 2025

Zabezpieczenia sprzętowe: Prototyp zabezpieczeń platformy kontenerowej

Publikacja dostępna pod adresem:

Narodowe Standardy Cyberbezpieczeństwa

NISTIR 8320A

Hardware-Enabled Security:

Container Platform Security Prototype

Michael Bartock
Murugiah Souppaya
Jerry Wheeler
Tim Knoll
Uttam Shetty
Ryan Savino
Joseprabu Inbaraj
Stefano Righi
Karen Scarfone

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

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

NISTIR 8320A

Hardware-Enabled Security:

Container Platform Security Prototype

Michael Bartock
Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

Jerry Wheeler
Tim Knoll
Uttam Shetty
Ryan Savino
Intel Corporation
Santa Clara, CA

Joseprabu Inbaraj
Stefano Righi
AMI
Atlanta, GA

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

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

June 2021

U.S. Department of Commerce
Gina Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

O PUBLIKACJI

Niniejsze opracowanie **NIST IR 8320A_wer. 1.0_PL *Zabezpieczenia sprzętowe: Prototyp zabezpieczeń platformy kontenerowej***, stanowi tłumaczenie publikacji NIST IR 8320A, *Hardware-Enabled Security: Container Platform Security Prototype*, i zostało opracowana 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

Tłumaczenie

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

SPIS TREŚCI

Tłumaczenie

SPIS ILUSTRACJI

SPIS TABEL

STRESZCZENIE

W czasach centrów danych w chmurze oraz przetwarzania brzegowego, przestrzenie ataków znacząco wzrosły. Jednocześnie hakerstwo stało się powszechne, a większość implementacji środków bezpieczeństwa nie jest spójna ani koherentna. Podstawą każdej strategii bezpieczeństwa centrum danych lub przetwarzania brzegowego powinno być zabezpieczenie platformy, na której dane i obciążenia będą wykonywane i dostępne. Platforma fizyczna stanowi pierwszą warstwę dla każdego warstwowego podejścia do bezpieczeństwa i zapewnia wstępną ochronę, która umożliwia zaufanie zabezpieczeniom wyższego poziomu.

W niniejszej publikacji omówiono techniki i technologie zabezpieczeń sprzętowych, które umożliwiają poprawę bezpieczeństwa wdrożeń kontenerów z wieloma podmiotami je wynajmującymi. Opisano również implementację tego podejścia — prototyp, który w założeniu ma być schematem lub szablonem dla ogólnej społeczności specjalistów ds. bezpieczeństwa.

SŁOWA KLUCZOWE

Kontener (*ang. container*); zabezpieczenia sprzętowe (*ang. hardware-enabled security*); sprzętowe źródło zaufania (*ang. hardware root of trust*); bezpieczeństwo platformy (*ang. platform security*); zaufane zasoby obliczeniowe (*ang. trusted compute pool*); wirtualizacja (*ang. virtualization*)

ODBIORCY

Głównymi odbiorcami tego raportu są specjaliści ds. bezpieczeństwa dostawców usług w chmurze, tacy jak inżynierowie i architekci bezpieczeństwa; administratorzy systemów i inni specjaliści ds. technologii informacyjnych (IT), a także deweloperzy sprzętu, oprogramowania układowego i oprogramowania, którzy mogą być w stanie wykorzystać sprzętowe techniki i technologie zabezpieczeń do poprawy bezpieczeństwa platform dla wdrożeń kontenerów w środowiskach chmurowych z wieloma podmiotami wynajmującymi.

INFORMACJA O ZNAKACH TOWAROWYCH

Wszystkie zastrzeżone znaki towarowe lub inne znaki towarowe należą do odpowiednich organizacji.

INFORMACJA O UJAWNIENIU PATENTÓW

UWAGA: Laboratorium informatyczne (ang. Information Technology Laboratory – ITL) zwróciło się do właścicieli zastrzeżeń patentowych, których wykorzystanie może być konieczne w celu zapewnienia zgodności z wytycznymi lub wymogami niniejszej publikacji, o ujawnienie ITL takich zastrzeżeń patentowych. Jednak posiadacze patentów nie są zobowiązani do odpowiadania na wezwania ITL dotyczące patentów, a ITL nie podjęło się wyszukiwania patentów w celu zidentyfikowania, które z nich, jeśli w ogóle, mogą mieć zastosowanie w niniejszej publikacji.

Na dzień publikacji i po wystosowaniu wezwania (wezwań) do wskazania zastrzeżeń patentowych, których wykorzystanie może być konieczne w celu zapewnienia zgodności z wytycznymi lub wymogami niniejszej publikacji, ITL nie zidentyfikowało żadnych takich zastrzeżeń patentowych.

ITL nie gwarantuje ani nie sugeruje, że w celu uniknięcia naruszenia patentów przy korzystaniu z niniejszej publikacji nie są konieczne licencje.

1. WPROWADZENIE

1.1. CEL I ZAKRES

Celem niniejszej publikacji jest opisanie podejścia do zabezpieczania wdrożeń kontenerów aplikacji w środowiskach chmurowych z wieloma podmiotami wynajmującymi. Niniejsza publikacja w pierwszej kolejności opisuje wybrane problemy z zakresu bezpieczeństwa związane z technologiami chmury obliczeniowej IaaS (*ang. Infrastructure as a Service*) i geolokalizacją w postaci tagów zasobów. Następnie opisano rozwiązanie prototypowe „dowodu słuszności koncepcji" (*ang. proof-of-concept*), który został zaprojektowany w celu sprostania tym wyzwaniom. Publikacja zawiera wystarczającą ilość szczegółów na temat prototypowej implementacji, aby organizacje mogły je w razie potrzeby odtworzyć. Niniejsza publikacja ma być planem lub szablonem, który może być wykorzystany przez ogólną społeczność bezpieczeństwa do walidacji i wdrożenia opisanej implementacji.

Należy zauważyć, że prototypowa implementacja przedstawiona w niniejszej publikacji jest tylko jednym z możliwych sposobów rozwiązania problemów związanych z bezpieczeństwem. Nie ma ona na celu zniechęcenia do korzystania z innych produktów, usług, technik itp., które również mogą odpowiednio rozwiązać problem, ani do korzystania z usług w chmurze, które nie zostały wyraźnie wymienione w niniejszej publikacji.

Niniejsza publikacja opiera się na terminologii i koncepcjach opisanych w raporcie NIST Interagency oraz Internal Report (IR) 8320, *Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases*[2] [1]. Zapoznanie się z tym dokumentem jest warunkiem wstępnym do zapoznania się z niniejszą publikacją, ponieważ wyjaśnia on pojęcia i definiuje podstawową terminologię używaną w niniejszej publikacji.

[2] Patrz: polskojęzyczna publikacja NIST IR 8320_wer. 1.0_PL. Przypis odnosi się do całego dokumentu.

1.2. TERMINOLOGIA

Aby zachować spójność z powiązanymi raportami NIST, w niniejszym raporcie zastosowano następujące definicje terminów związanych z zaufaniem:

- Zaufanie: „Zaufanie, występuje wtedy, gdy jeden element ufa, że drugi element zachowa się zgodnie z oczekiwaniami”[3].
- Zaufany: Element, na którym polega inny element, że ten spełni krytyczne wymagania w jego imieniu.
- Zaufany rozruch systemu: Rozruch systemu, w którym pewne aspekty sprzętu i oprogramowania układowego są mierzone i porównywane ze znanymi prawidłowymi wartościami w celu zweryfikowania ich integralności, a tym samym wiarygodności.
- Godny zaufania: Element godny zaufania to taki element, który spełnia wszelkie niezbędne wymagania[4].

1.3. STRUKTURA DOKUMENTU

Niniejszy dokument został podzielony na następujące rozdziały i załączniki:

- Rozdział 2 zawiera definicję problemu (przypadek użycia), który ma zostać rozwiązany.
- Rozdziały 3, 4 i 5 zawierają opisy trzech etapów wdrażania prototypu:
  - ✓ Etap 0: Atestacja platformy i przetestowane uruchomienie węzła roboczego.
  - ✓ Etap 1: Zaufane rozmieszczanie obciążeń roboczych.
  - ✓ Etap 2: Tagowanie zasobów i zaufanych lokalizacji.
- Załącznik Referencje zawiera wykaz wykorzystanych i polecanych dokumentów.

[3] Software Assurance in Acquisition: Mitigating Risks to the Enterprise, https://apps.dtic.mil/dtic/tr/fulltext/u2/a495389.pdf

[4] W oparciu o definicję z publikacji specjalnej NIST (SP) 800-160 tom 2, https://doi.org/10.6028/NIST.SP.800-160v2

- Załącznik A zawiera przegląd wysokopoziomowej architektury sprzętowej, która została wykorzystana w prototypowej implementacji, a także szczegółowe informacje na temat wdrażania przez platformy Intel modułów sprzętowych i ulepszonych sprzętowych funkcji bezpieczeństwa.
- Załącznik B zawiera dodatkowe informacje dostarczone przez AMI opisujące wszystkie wymagane komponenty i kroki niezbędne do skonfigurowania prototypowej implementacji.
- Załącznik C zawiera dodatkowe informacje opisujące wszystkie wymagane komponenty i kroki niezbędne do skonfigurowania prototypowej implementacji dla Kubernetes.
- Załącznik D zawiera listę głównych mechanizmów środków bezpieczeństwa z publikacji specjalnej NIST (SP) 800-53 Rev. *5*, *Security and Privacy Controls for Information Systems and Organizations*[5], które wpływają na implementację prototypu zabezpieczeń platformy kontenerowej.
- Załącznik E mapuje główne funkcje bezpieczeństwa z prototypowej implementacji do odpowiednich podkategorii z ram cyberbezpieczeństwa (*ang. Cybersecurity Framework*).
- Załącznik F zawiera listę i definicje akronimów i innych skrótów użytych w dokumencie.

[5] Patrz: polskojęzyczna publikacja NSC 800-53 wer. 2. Przypis odnosi się do całego dokumentu.

2. WDROŻENIE PROTOTYPU

W rozdziale tym zdefiniowano wdrożenie prototypu. Rozdział 2.1 wyjaśnia cele podstawowe. Rozdział 2.2 zawiera uszczegółowienia opisujące wszystkie cele pośrednie, które muszą zostać spełnione, aby osiągnąć pożądaną implementację prototypu. Wymagania te są pogrupowane w trzy etapy przypadku użycia, z których każdy został dokładnie przeanalizowany odpowiednio w rozdziałach od 2.2.1 do 2.2.3.

2.1. CEL

Technologie współdzielonego przetwarzania w chmurze są zaprojektowane tak, aby były wysoce zwinne i elastyczne, w przejrzysty sposób wykorzystując wszelkie dostępne zasoby do przetwarzania wdrożeń kontenerów dla swoich klientów [2]. Istnieją jednak obawy dotyczące bezpieczeństwa i prywatności związane z umożliwieniem nieograniczonej orkiestracji wdrażania kontenerów. Za każdym razem, gdy na jednym serwerze w chmurze znajduje się wiele wdrożeń kontenerów, istnieje potrzeba oddzielenia tych wdrożeń od siebie, aby nie zakłócały się wzajemnie, nie uzyskiwały dostępu do wrażliwych danych ani w inny sposób nie zagrażały bezpieczeństwu lub prywatności kontenerów. Wyobraźmy sobie dwie rywalizujące ze sobą organizacje, które wdrożyły kontenery na tym samym serwerze. Każda z nich chciałaby mieć pewność, że serwerowi można zaufać, że nie udostępni informacji drugiej organizacji. Podobnie, pojedyncza organizacja może mieć wdrożonych wiele kontenerów, które muszą być oddzielone ze względu na różne wymagania bezpieczeństwa i potrzeby każdej aplikacji.

Inną obawą związaną ze współdzieloną chmurą obliczeniową jest to, że zadania mogą być przenoszone z serwerów chmurowych zlokalizowanych w jednym kraju na serwery zlokalizowane w innym kraju. Każdy kraj ma własne przepisy dotyczące bezpieczeństwa danych, prywatności i innych aspektów technologii informacyjnej (IT). Ponieważ wymagania tych przepisów mogą być sprzeczne z zasadami lub przepisami organizacji (np. przepisami prawa, wykonawczymi), organizacja może zdecydować, że musi ograniczyć liczbę serwerów w chmurze, z których korzysta, w oparciu o ich lokalizację. Powszechnym zwyczajem jest korzystanie wyłącznie z serwerów w chmurze fizycznie zlokalizowanych w tym samym kraju co organizacja lub fizycznie zlokalizowanych w tym

samym kraju, z którego pochodzą informacje. Określenie przybliżonej fizycznej lokalizacji obiektu, takiego jak serwer obliczeniowy w chmurze, jest ogólnie znane jako geolokalizacja. Geolokalizację można uzyskać na wiele sposobów, z różnym stopniem dokładności, ale typowe metody geolokalizacji nie są zabezpieczone i są egzekwowane poprzez środki bezpieczeństwa — zarządzane i operacyjne — których nie można zautomatyzować ani skalować. Dlatego nie można ufać typowym metodom geolokalizacji, aby spełnić wymagania bezpieczeństwa w chmurze.

Motywacją stojącą za tym przypadkiem użycia jest poprawa bezpieczeństwa i przyspieszenie wdrażania technologii przetwarzania w chmurze poprzez ustanowienie zautomatyzowanego sprzętowego źródła zaufania do egzekwowania i monitorowania integralności platformy oraz ograniczeń geolokalizacyjnych dla serwerów w chmurze. *Sprzętowe źródło zaufania* to z natury zaufana kombinacja sprzętu i oprogramowania układowego odpowiedzialna za pomiar integralności platformy i informacji geolokalizacyjnych w postaci tagu zasobu. Pomiary dokonywane przez sprzętowe źródło zaufania są przechowywane w odpornych na naruszenia urządzeniach i bezpiecznie przesyłane przy użyciu kluczy kryptograficznych unikatowych dla tych urządzeń. Dostęp do tych informacji uzyskują narzędzia do zarządzania i zabezpieczeń wykorzystujące protokoły kryptograficzne w celu zapewnienia integralności platformy i potwierdzenia lokalizacji hosta.

Ten przypadek użycia opiera się na wcześniejszych pracach udokumentowanych w NIST IR 7904, *Trusted Geolocation in the Cloud*: *Proof of Concept Implementation* [3].

2.2. CELE

Korzystanie z zaufanych zasobów obliczeniowych (opisanych w punkcie 3) jest wiodącym podejściem do agregowania zaufanych systemów i oddzielania ich od niezaufanych zasobów, co skutkuje oddzieleniem obciążeń o większym znaczeniu, bardziej wrażliwych od obciążeń aplikacji i danych. Zasady działania są następujące:

1. Utworzenie w chmurze obszaru, który będzie spełniać specyficzne i zróżnicowane wymagania użytkowników w zakresie bezpieczeństwa.
2. Kontrola dostępu do tego obszaru chmury i wdrożenie w nim odpowiednich aplikacji (zadań).
3. Włączenie audytów tego obszaru chmury, aby użytkownicy mogli weryfikować zgodność.

Te zaufane zasoby obliczeniowe pozwalają działom IT czerpać korzyści z dynamicznego środowiska chmurowego, jednocześnie wymuszając wyższy poziom ochrony bardziej krytycznych obciążeń.

Ostatecznym celem jest możliwość wykorzystania „zaufania" jako logicznej granicy podczas wdrażania obciążeń na platformach serwerowych w chmurze. Cel ten zależy od mniejszych celów wstępnych opisanych jako etapy. Można je traktować jako wymagania, które rozwiązanie musi spełnić. Ponieważ warunków wstępnych jest dużo, zostały one podzielone na trzy grupy — etapy:

0. Atestacja platformy i mierzone uruchomienie węzła roboczego. Zapewnia to, że integralność platformy serwera w chmurze jest mierzona i dostępna dla kolejnych etapów.
1. Zaufane lokowanie obciążeń. Ten etap umożliwia orkiestrację wdrożeń kontenerów w celu uruchamiania ich wyłącznie na zaufanych platformach serwerowych w chmurze.
2. Tagowanie zasobów i zaufana lokalizacja Ten etap umożliwia uruchamianie wdrożeń kontenerów tylko na zaufanych platformach serwerowych w chmurze, biorąc pod uwagę jakościowe ograniczenia tagów zasobów (na przykład informacje o lokalizacji).

Cele wymagane dla każdego etapu, wraz z bardziej ogólnymi informacjami na temat każdego z etapów, zostały wyjaśnione poniżej.

2.2.1. ETAP 0: ATESTACJA PLATFORMY I MIERZONE URUCHOMIENIE WĘZŁA ROBOCZEGO

Podstawowym elementem rozwiązania jest zapewnienie, że platforma, na której jest wdrażany kontener, jest godna zaufania. Jeśli platforma nie jest godna zaufania, to nie tylko naraża aplikację i dane klienta na większe ryzyko naruszenia bezpieczeństwa, ale także nie ma pewności, że deklarowany tag zasobu serwera w chmurze jest poprawny. Zapewnienie podstawowej gwarancji wiarygodności jest początkowym etapem tego rozwiązania.

Etap 0 obejmuje następujące cele wstępne:

1. **Skonfigurowanie platformy serwera w chmurze jako zaufanej.** „Platforma serwera w chmurze" obejmuje konfigurację sprzętu (np. integralność systemu

BIOS), konfigurację systemu operacyjnego (konfigurację i integralność programu rozruchowego i jądra systemu operacyjnego) oraz integralność środowiska uruchomieniowego kontenera. Obejmuje również różne technologie zabezpieczeń sprzętowych aktywowanych na serwerze. Te technologie łańcucha zaufania *(ang. chain-of-trust – CoT)* zapewniają integralność platformy. Dodatkowe technologie i szczegóły można znaleźć we wspomnianym wcześniej dokumencie NISTIR 8320 [1]. Zostały również omówione w podrozdziale 3.2.

2. **Przed każdym uruchomieniem kontenera węzła roboczego należy zweryfikować (zmierzyć) wiarygodność platformy serwera w chmurze.** Przed uruchomieniem środowiska uruchomieniowego kontenera należy porównać konfiguracje elementów skonfigurowanych w celu 1 (BIOS, system operacyjny, środowisko uruchomieniowe kontenera) z wcześniejszymi pomiarami, aby się upewnić, że zakładany poziom zaufania został utrzymany.
3. **Podczas uruchamiania kontenera należy okresowo sprawdzać wiarygodność platformy serwera w chmurze.** Ten okresowy audyt jest zasadniczo tym samym audytem, który został przeprowadzony w ramach celu 2, z wyjątkiem tego, że często jest wykonywany podczas działania środowiska uruchomieniowego kontenera. Wskazanym jest, ażeby audyt ten był częścią stałego monitorowania.

Osiągnięcie wszystkich tych celów nie zapobiegnie skutecznym atakom, ale sprawi, że nieautoryzowane zmiany w platformie chmurowej zostaną wykryte szybciej niż w innym przypadku. Zapobiega to uruchamianiu nowych wdrożeń kontenerów z wymaganiami zaufania na niezaufanej platformie.

Więcej informacji na temat zagadnień technicznych, do których odnoszą się te cele, 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, *Information Security Continuous Monitoring 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;
- Wersja robocza NIST SP 800-155, *BIOS Integrity Measurement Guidelines* https://csrc.nist.gov/publications/detail/sp/800-155/draft;
- NIST SP 800-190, *Application Container Security Guide* https://doi.org/10.6028/NIST.SP.800-190.

2.2.2. ETAP 1: ZAUFANE ROZMIESZCZANIE OBCIĄŻEŃ

Po pomyślnym zakończeniu etapu 0 kolejnym celem jest możliwość orkiestracji rozmieszczenia obciążeń w celu uruchamiania ich tylko na zaufanych platformach. Rozmieszczenie obciążeń jest kluczowym atrybutem chmury obliczeniowej, poprawiającym skalowalność i niezawodność. Celem tego etapu jest zapewnienie, że każdy serwer, na którym jest uruchamiane obciążenie, będzie spełniał wymagany poziom zabezpieczeń zgodny z zasadami bezpieczeństwa.

Etap 1 obejmuje następujący cel wstępny:

1. **Wdrażanie obciążeń tylko na serwerach w chmurze z zaufanymi platformami.** Zasadniczo oznacza to, że użytkownik wykonuje etap 0, cel 3 (audyt wiarygodności platformy) i wdraża obciążenie na serwerze w chmurze tylko wtedy, gdy audyt wykaże, że platforma jest godna zaufania.

Osiągnięcie tego celu gwarantuje, że obciążenia są wdrażane na zaufanych platformach, zmniejszając w ten sposób ryzyko ich naruszenia.

Więcej informacji na temat zagadnień technicznych, do których odnoszą się te cele, można znaleźć w następujących publikacjach NIST:

- Publikacja robocza 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-draft;
- NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*[6] https://doi.org/10.6028/NIST.SP.800-137;

[6] Patrz: polskojęzyczna publikacja NSC 800-137. Przypis odnosi się do całego dokumentu.

- 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.

2.2.3. ETAP 2: TAGOWANIE ZASOBÓW I ZAUFANA LOKALIZACJA

Etap 2 opiera się na etapie 1., Rozbudowany jest o możliwość ciągłego monitorowania i egzekwowania ograniczeń dotyczących tagów zasobów.

Etap 2 obejmuje następujące cele wstępne:

1. **Informacje o zaufanych tagach zasobów dla każdego przypadku zaufanej platformy.** Informacje te byłyby przechowywane w module kryptograficznym serwera w chmurze (jako skrót kryptograficzny w sprzętowym module kryptograficznym), aby można je było łatwo zweryfikować i poddać audytowi.
2. **Zapewnienie mechanizmów zarządzania konfiguracją i egzekwowania polityk dla zaufanych platform, które obejmują egzekwowanie ograniczeń dotyczących tagów zasobów.** Cel ten opiera się na etapie 1, cel 1 (wdrażanie obciążeń tylko na serwerach w chmurze z zaufanymi platformami); ulepsza etap 2, cel 1 poprzez dodanie sprawdzania tagu zasobu do serwera, na którym ma zostać uruchomione obciążenie.
3. **Podczas orkiestracji obciążeń należy okresowo przeprowadzać audyt tagów zasobów platformy serwera w chmurze pod kątem ograniczeń obowiązujących w politykach dotyczących tagów zasobów.** Cel ten opiera się na etapie 0, celu 3 (audyt wiarygodności platformy), ale w szczególności sprawdza informacje o tagach zasobów pod kątem zasad dotyczących tagów zasobów, aby się upewnić, że tagowanie zasobów przez serwer nie narusza tych polityk.

Osiągnięcie tych celów gwarantuje, że obciążenia nie zostaną uruchomione na serwerze w nieodpowiedniej lokalizacji brzegowej. Pozwala to uniknąć problemów spowodowanych przez chmury znajdujące się w różnych lokalizacjach fizycznych (np.

przepisy, poziomy wrażliwości, kraje lub stany z różnymi przepisami dotyczącymi bezpieczeństwa danych i prywatności).

Więcej informacji na temat zagadnień technicznych, do których odnoszą się te cele, 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, Information Security Continuous Monitoring for Federal Information Systems and Organizations https://doi.org/10.6028/NIST.SP.800-137;
- 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.

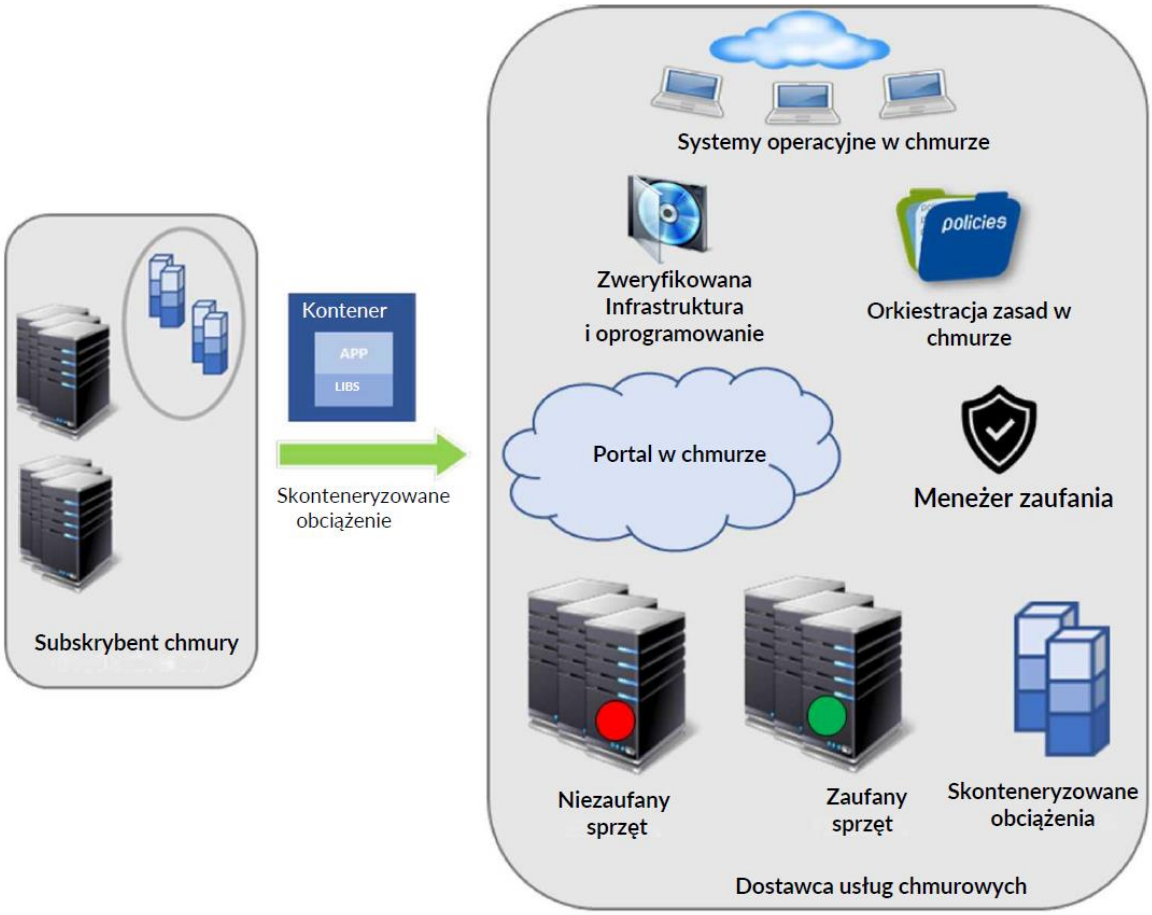
3. PROTOTYPOWANIE — ETAP 0

W tym punkcie opisano etap 0 implementacji prototypu (atestacja platformy i mierzone uruchomienie węzła roboczego).

3.1. OMÓWIENIE ROZWIĄZANIA

Ten etap przypadku użycia umożliwia tworzenie tak zwanych *zaufanych pul (zasobów) obliczeniowych*. Znane również jako *zaufane pule (zasoby)*, są to fizyczne lub logiczne grupy sprzętu obliczeniowego w centrum danych, które są tagowane określonymi i zmiennymi politykami bezpieczeństwa, a dostęp i wykonywanie aplikacji oraz obciążeń są monitorowane, kontrolowane, audytowane itp. W tej fazie rozwiązania atestowane uruchomienie platformy jest uznawane za zaufany węzeł i dodawane do zaufanej puli.

Rysunek 1 przedstawia koncepcję zaufanych pul. Zasoby oznaczone kolorem zielonym wskazują zaufane zasoby. Krytyczne polityki można zdefiniować w taki sposób, aby wrażliwe pod względem bezpieczeństwa usługi w chmurze mogły być uruchamiane tylko na tych zaufanych zasobach.



Rysunek 1: Koncepcja zaufanych pul obliczeniowych

Aby uruchomić platformę w sposób godny zaufania, należy odpowiedzieć sobie na trzy pytania:

1. Skąd podmiot potrzebujący tych informacji miałby wiedzieć, że dana platforma ma włączone niezbędne rozszerzone funkcje zabezpieczeń sprzętowych? Czy dana platforma ma zdefiniowane / zgodne oprogramowanie sprzętowe systemu operacyjnego / platformy oraz uruchomione na niej środowisko wykonawcze kontenera?
2. Dlaczego podmiot żądający tych informacji, którym w środowisku chmurowym byłby koordynator próbujący zaplanować obciążenie na zestawie dostępnych węzłów/serwerów, miałby wierzyć w uzyskaną z platformy odpowiedź?

Atestacja dostarcza ostatecznych odpowiedzi na te pytania. Atestacja to proces dostarczania podpisu cyfrowego oraz zestawu pomiarów bezpiecznie przechowywanych w sprzęcie, które następnie są zatwierdzane przez osobę wnioskującą. Atestacja wymaga źródła zaufania. Platforma musi mieć źródło zaufania

do pomiaru (*ang. Root-of-Trust for Measurement — RTM*), które jest domyślnie wiarygodne, żeby zapewnić dokładny pomiar. Ulepszone funkcje bezpieczeństwa oparte na sprzęcie zapewnia RTM. Platforma musi również mieć źródło zaufania dla raportowania (*ang. Root-of-Trust for Reporting — RTR*) i źródło zaufania dla pamięci masowej (*ang. Root-of-Trust for Storage — RTS*), które zapewniają te same ulepszone funkcje bezpieczeństwa oparte na sprzęcie.

Podmiot, który chce uzyskać z platformy te informacje, może teraz wysłać zapytanie o zaufanie do zainicjowanej platformy, porównując dostarczony zestaw pomiarów z pomiarami, które są na pewno prawidłowe. Zarządzanie prawidłowymi pomiarami dla różnych platform oraz systemów operacyjnych i różnego oprogramowania BIOS, a także zapewnienie ich ochrony przed manipulacją i spoofingiem jest kluczowym wyzwaniem dla operacji IT. Ta zdolność do ochrony może być wewnętrzną zdolnością dostawcy usług lub być dostarczana jako usługa przez zaufaną stronę trzecią, z której mogą korzystać dostawcy usług i organizacje.

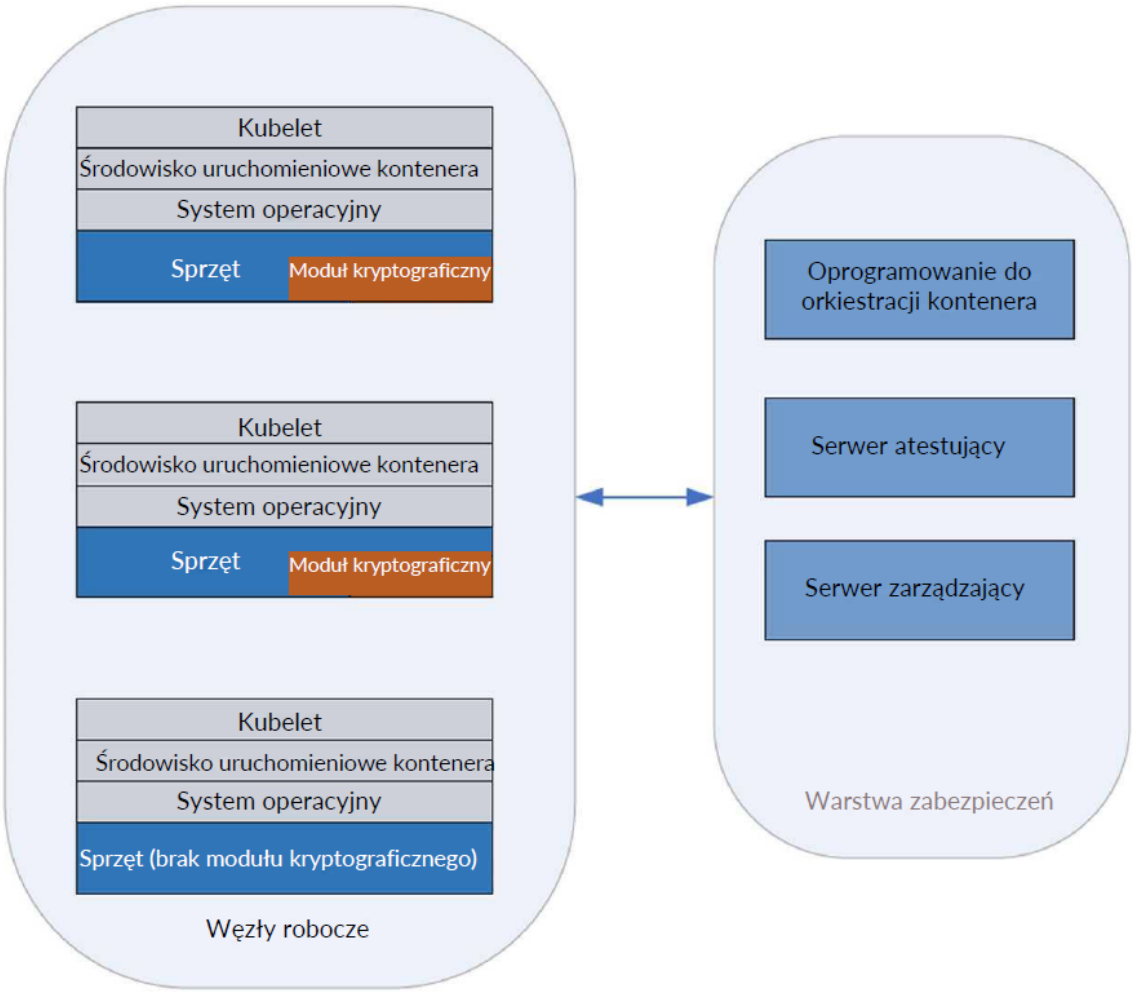
3.2. ARCHITEKTURA ROZWIĄZANIA

Rysunek 2 przedstawia warstwowy widok architektury systemu rozwiązania. Wskazane serwery w puli zasobów posiadają moduł sprzętowy do przechowywania wrażliwych kluczy i pomiarów. Wszystkie serwery widoczne na diagramie są konfigurowane przez serwer zarządzający.

Pierwszy krok w implementacji architektury wymaga zapewnienia serwerowi ulepszonych funkcji bezpieczeństwa opartych na sprzęcie. Wymaga to fizycznego lub zdalnego dostępu do serwera w celu uzyskania dostępu do systemu BIOS, włączenia zestawu opcji konfiguracyjnych w celu korzystania z modułu sprzętowego (w tym przejęcia własności modułu) i aktywowania ulepszonych funkcji zabezpieczeń sprzętowych. Proces ten jest w znacznym stopniu zależny od systemu BIOS i producenta oryginalnego sprzętu (*ang. original equipment manufacturer - OEM*). Ten krok jest obowiązkowy dla mierzonego uruchomienia platformy.

Konsola zarządzania zapewnia zdalne monitorowanie i zarządzanie wszystkimi serwerami w architekturze tego rozwiązania. Umożliwia także zdalną konfigurację BIOS-u, która jest wymagana do pomiaru i zabezpieczenia serwera. Okresowo

sprawdza pomiary wszystkich monitorowanych serwerów i porównuje je ze wzorcowymi pomiarami, które zostały wykonane w idealnych warunkach. Gdy którykolwiek z takich pomiarów nie jest zgodny, sygnalizując naruszenie bezpieczeństwa platformy, powiadamia administratora za pośrednictwem wiadomości e-mail lub wiadomości tekstowej. Administrator może następnie użyć konsoli zarządzania do podjęcia działań naprawczych, które mogą obejmować wyłączenie zasilania serwera, ponowną konfigurację lub aktualizację oprogramowania układowego serwera.



Rysunek 2: Etap 0 — Architektura systemu rozwiązania

Platforma jest uruchamiana z pomiarami, a komponenty BIOS i OS są mierzone (kryptograficznie) i umieszczane w sprzętowym module zabezpieczeń serwera. Te wartości pomiarowe są dostępne za pośrednictwem serwera zarządzania w chmurze przy pomocy interfejsu programistycznego aplikacji (API). Gdy hosty są wstępnie

skonfigurowane z serwerem zarządzania w chmurze, odpowiednie wartości pomiarowe są buforowane w bazie danych zarządzania w chmurze.

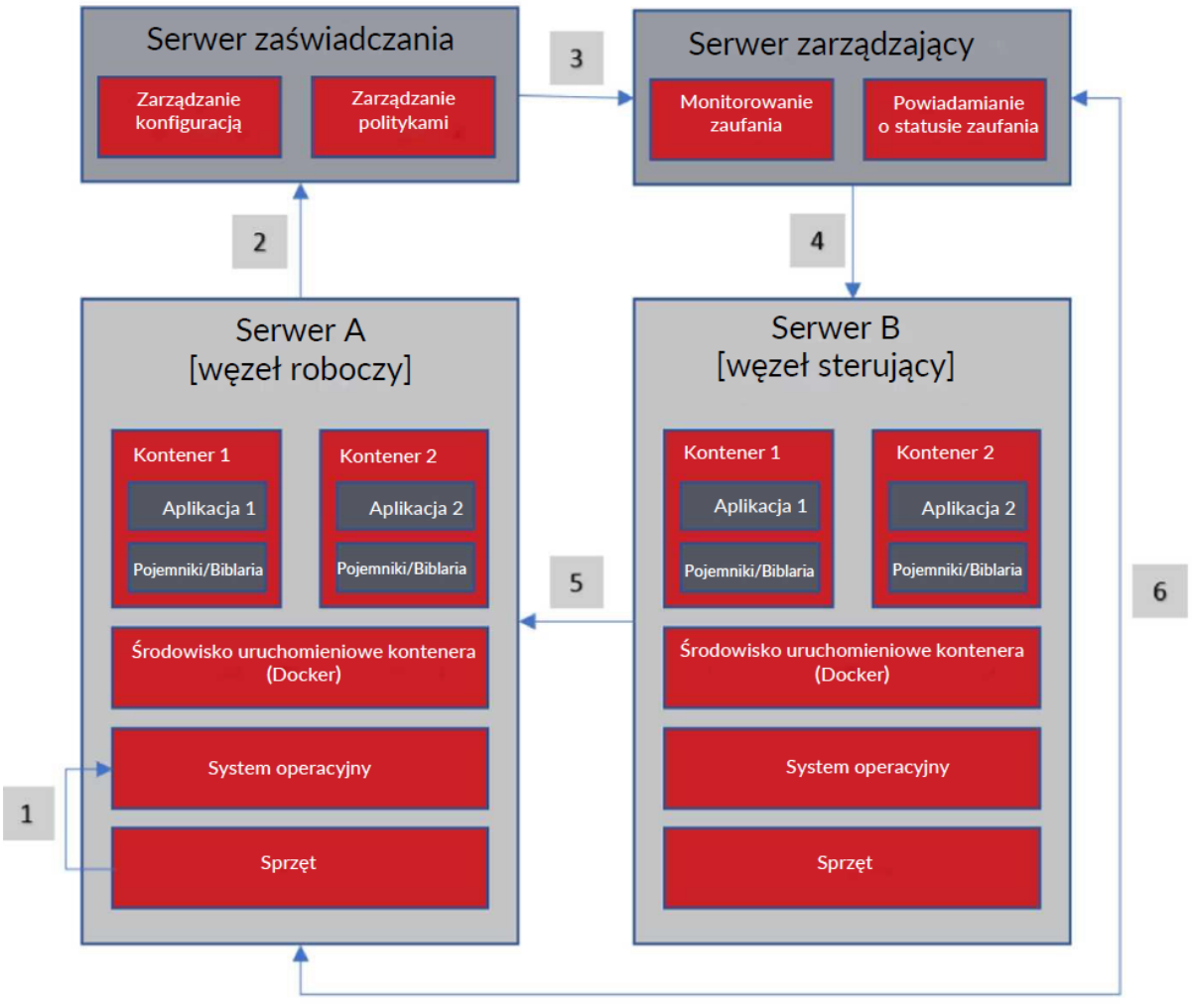
Oprócz mierzonego uruchomienia, ta architektura rozwiązania zapewnia również możliwość przypisania tagów zabezpieczeń zasobów do każdego serwera na etapie procesu zabezpieczania. Tag zasobu jest przypisywany do stabilnego indeksu w module sprzętowym za pośrednictwem mechanizmu pozapasmowego, a podczas uruchamiania platformy zawartość indeksu jest wstawiana / rozszerzana do modułu sprzętowego. Ulepszone funkcje zabezpieczeń sprzętowych zapewniają interfejs i atestację informacji o tagu zasobu, w tym wyszukiwanie tagu zasobu oraz opis czytelny dla użytkownika.

4. PROTOTYPOWANIE — ETAP 1

W tym punkcie przedstawiono etap 1 implementacji prototypu (zaufane rozmieszczanie obciążeń). Do etapu 0 dodano komponenty koordynujące orkiestrację obciążeń w celu uruchomienia ich na zaufanych platformach.

4.1. OMÓWIENIE ROZWIĄZANIA

Rysunek 3 pokazuje sposób działania etapu 1. Przyjęto, że serwer A i serwer B to dwa serwery znajdujące się w tej samej chmurze.



Rysunek 3: Etap 1 — omówienie rozwiązania

Podczas działania prototypu w etapie 1 jest wykonywanych sześć ogólnych kroków, które ponumerowano poniżej i opisano na Rysunku 3:

1. Serwer A wykonuje mierzone uruchomienie, a rozszerzone funkcje zabezpieczeń sprzętowych uzupełniają pomiary w module sprzętowym.
2. Serwer A wysyła zapytanie do źródła zaufania (*ang. Trust Authority*). Zapytanie zawiera podpisane skróty różnych komponentów oprogramowania układowego i systemu operacyjnego platformy.
3. Źródło zaufania weryfikuje podpis i wartości skrótu, a następnie wysyła poświadczenie stanu integralności platformy do serwera zarządzania.
4. Serwer zarządzający wymusza polityki dotyczące obciążeń na serwerze B w oparciu o wymagania użytkowników.
5. Serwer B uruchamia obciążenia wymagające zaufanej infrastruktury tylko na platformach serwerowych, które zostały zatwierdzone jako zaufane.
6. Każda platforma serwerowa jest regularnie poddawana audytowi w oparciu o wartości pomiarowe.

4.2. ARCHITEKTURA ROZWIĄZANIA

Architektura etapu 1 jest taka sama jak etapu 0 (zob. Rysunek 2), z uwzględnieniem dodatkowych pomiarów związanych z orkiestracją rozmieszczenia obciążeń między zaufanymi hostami.

5. PROTOTYPOWANIE — ETAP 2

W tym punkcie omówiono 2 etap implementacji prototypu (bezpieczne umieszczanie obciążeń oparte na zaufaniu i tagach zasobów). Do etapu 1 dodano komponenty uwzględniające ograniczenia tagów zasobów.

5.1. OMÓWIENIE ROZWIĄZANIA

W etapie 2 dodano możliwość monitorowania pomiarów przy użyciu pulpitu nawigacyjnego do zarządzania ryzykiem i zgodnością. Jeden z wykresów, który może pojawić się na takim pulpicie nawigacyjnym, może odzwierciedlać względną wielkość pul zaufanych i niezaufanych serwerów w chmurze. Wartości mogą być wyświetlane jako wartości procentowe lub liczby.

Tabela 1 to strona rozwijana w widoku pulpitu nawigacyjnego wysokiego poziomu. Dostarcza więcej szczegółów na temat wszystkich serwerów w chmurze. W tym przykładzie przedstawiono trzy serwery. Dla każdego serwera podano następujące informacje: adres IP serwera, identyfikator UUID oraz status pomiarów (zaufana walidacja rozruchu i walidacja kondycji systemu).

Tabela 1: Widok zgodności zaufanego rozruchu

IP hosta w chmurze	Identyfikator UUID sprzętu	Weryfikacja zaufanego rozruchu	Sprawdzanie kondycji systemu
<Host 1>	<UUID 1>	Tak/Nie	Tak/Nie
<Host 2>	<UUID 2>	Tak/Nie	Tak/Nie
<Host 3>	<UUID 3>	Tak/Nie	Tak/Nie

Rysunek 4 przedstawia analizę z Tabeli 1 dla pojedynczego serwera. Zawiera on szczegółowe dane pomiarowe dotyczące weryfikacji zaufanego rozruchu, wraz ze statusem połączenia oraz listą tagów zasobów, która może zawierać wartość tagu zasobu. Pokazuje również, kiedy serwer został zmierzony oraz kiedy wygasa ważność tego pomiaru. Częste pomiary charakterystyki serwera (np. co pięć minut) pomagają zapewnić ciągłe monitorowanie serwerów.

Informacje ogólne			
Host Info:	<adres IP lub nazwa hosta>	UUID:	<Unikalny identyfikator>
Trust Report Created On:	<Znacznik czasu>	Trust Report Expires On:	<Znacznik czasu>
Asset Tag Status:	<Deployed/Not Deployed>	Asset Tag List:	<Nazwa-1/wartość-1> <Nazwa-N/wartość-N>
Flavor Group Name:	<Nazwa>	Connection Status:	<Connected / Not connected>

Informacje o zaufaniu			
Overall System Trust:	<Trusted/Untrusted>		
Software Trust:	<Trusted/Untrusted>	Platform Trust:	<Trusted/Untrusted>
Asset Tag Trust:	<Trusted/Untrusted>	Host Unique Trust:	<Trusted/Untrusted>

Rysunek 4: Omówienie pojedynczego serwera

REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[7]	
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
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

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

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[7]	
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[8]

W tym dokumencie odwoływano się do następujących publikacji.

[1] Bartock MJ, Souppaya MP, Savino R, Knoll T, Shetty U, Cherfaoui M, Yeluri R, Malhotra A, Scarfone KA (2021) 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), Draft NIST Interagency or Internal Report (IR) 8320.

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

[2] Souppaya MP, Scarfone KA, Morello J (2017) Application Container Security Guide.

(National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-190. https://doi.org/10.6028/NIST.SP.800-190

[3] Bartock MJ, Souppaya MP, Yeluri R, Shetty U, Greene J, Orrin S, Prafullchandra H, McLeese J, Scarfone KA (2015) Trusted Geolocation in the Cloud: Proof of Concept Implementation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7904. https://doi.org/10.6028/NIST.IR.7904

[4] Greene J (2012) Intel Trusted Execution Technology: Hardware-based Technology for Enhancing Server Platform Security. (Intel Corporation). Available at http://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution- technology/trusted-execution-technology-security-paper.html

[5] AMI (2020) AMI TruE Trusted Environment. Available at https://ami.com/en/products/security-services-and-solutions/ami-true-trusted-environment/

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

[6] 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. https://doi.org/10.6028/NIST.SP.800-53r5

[7] 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

ZAŁĄCZNIK A – ARCHITEKTURA SPRZĘTU I WYMAGANIA WSTĘPNE

Dodatek zawiera przegląd wysokopoziomowej architektury sprzętowej, która została wykorzystana w prototypowej implementacji, a także szczegółowe informacje na temat wdrażania przez platformy Intel® modułów sprzętowych i ulepszonych sprzętowych funkcji bezpieczeństwa [4].

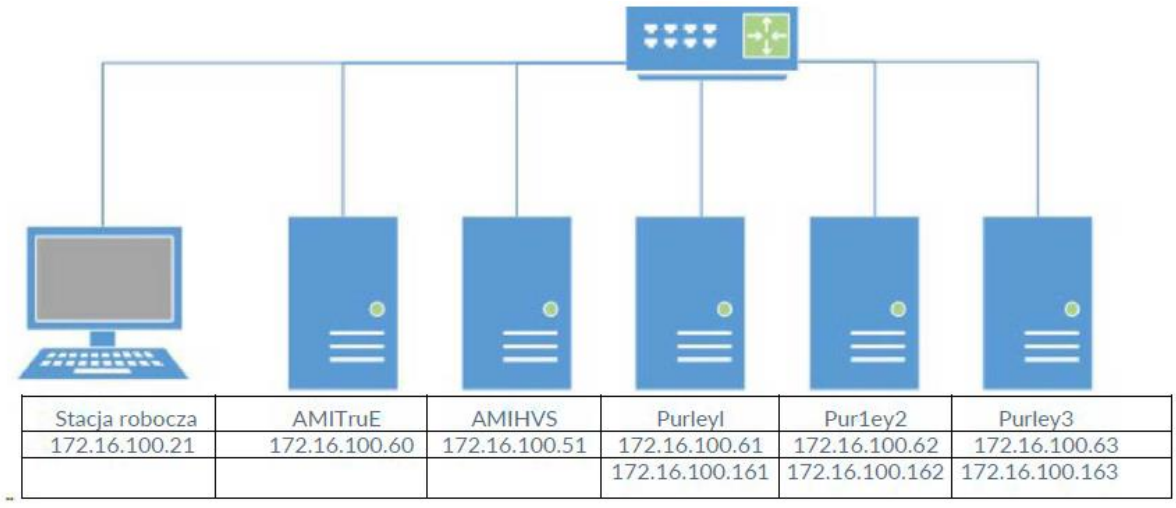
A.1 ARCHITEKTURA IMPLEMENTACJI WYSOKIEGO POZIOMU

Sieć z prototypową implementacją to płaska sieć zarządzania dla komponentów AMI i serwerów obliczeniowych Intel z laptopem używanym jako stacja robocza. Serwery Intel wykorzystują sieci nakładkowe do komunikacji między kontenerami, które w nich działają. Każdy serwer Intel ma gniazdo BIOS i kontroler zarządzania płytą główną (*ang. Baseboard Management Controller - BMC*), dzięki czemu do układu BIOS i BMC można załadować oprogramowanie układowe AMI i zainstalować je na serwerze. Więcej szczegółów technicznych na temat komponentów AMI oraz konfiguracji i instalacji serwerów Intel można znaleźć w dodatkach B i C.

Tabela 2 przedstawia nazwę hosta wraz z konfiguracją IP każdego systemu, a Rysunek 5 przedstawia logiczną architekturę sieci implementacji.

Tabela 2: Nazwy hostów systemów i konfiguracje IP

Nazwa hosta	Adres IP zarządzania	Adres IP BMC
AMI-TruE	172.16.100.50	Nd.
AMI-HVS	172.16.100.51	Nd.
Purley1	172.16.100.61	172.16.100.161
Purley2	172.16.100.62	172.16.100.162
Purley3	172.16.100.63	172.16.100.163
Stacja robocza	172.16.100.21	Nd.



Stacja robocza	AMITruE	AMIHVS	Purleyl	Pur1ey2	Purley3
172.16.100.21	172.16.100.60	172.16.100.51	172.16.100.61	172.16.100.62	172.16.100.63
			172.16.100.161	172.16.100.162	172.16.100.163

Rysunek 5: Architektura sieci logicznej prototypowej implementacji

A.2 TECHNOLOGIA INTEL TXT I MODUŁ TPM

Sprzętowe źródło zaufania, w połączeniu z aktywnym BIOS-em, systemem operacyjnym i komponentami, stanowi podstawę bezpieczniejszej platformy obliczeniowej. Ta zabezpieczona platforma zapewnia integralność BIOS-u i systemu operacyjnego na poziomie rozruchu z atakami typu rootkit i innymi atakami niskiego poziomu. Ustanawia wiarygodność serwera i platformy hosta.

W zaufanej platformie są trzy źródła zaufania: RTM, RTR i RTS. Są to podstawowe elementy platformy. Muszą być zaufane, ponieważ niewłaściwe postępowanie z nimi nie byłoby wykrywalne w wyższych warstwach. Na platformie Intel TXT RTM jest mikrokodem Intel: Core-RTM (CRTM). RTM jest głównym komponentem wysyłającym do RTS informacje (pomiary), które są ważne dla zapewnienia integralności. Zaufanie do tego komponentu jest podstawą zaufania do reszty pomiarów. RTS zawiera dane komponentów (pomiary) i inne wrażliwe informacje. Moduł platformy zaufanej (ang. *Trusted Platform Module – TPM*) zapewnia funkcje ochrony RTS i RTR dla zaufanej platformy obliczeniowej.

Technologia Intel TXT (ang. *Trusted Execution Technology*) to RTM, czyli mechanizm zapewniający widoczność, zaufanie oraz środki bezpieczeństwa w chmurze. Intel TXT to zestaw ulepszonych komponentów sprzętowych zaprojektowanych w celu ochrony poufnych informacji przed atakami. Funkcje Intel TXT obejmują zdolności do ochrony mikroprocesora, chipsetu, podsystemów wejścia / wyjścia oraz innych komponentów

platformy. W połączeniu z włączonym systemem operacyjnym i aplikacjami możliwości te zapewniają poufność oraz integralność danych w obliczu coraz bardziej wrogich środowisk.

Intel TXT zawiera szereg innowacji z zakresu bezpiecznego przetwarzania danych, w tym:

- **Wykonywanie chronione:** Pozwala aplikacjom działać w odizolowanych środowiskach, dzięki czemu żadne nieautoryzowane oprogramowanie na platformie nie może monitorować informacji operacyjnych ani nimi manipulować. Każde z tych odizolowanych środowisk działa z wykorzystaniem dedykowanych zasobów zarządzanych przez platformę.
- **Zabezpieczona pamięć:** Zapewnia możliwość szyfrowania i przechowywania kluczy, danych oraz innych wrażliwych informacji w sprzęcie. Może zostać odszyfrowana tylko w środowisku, w którym została zaszyfrowana.
- **Atestacja:** Jest dla systemu gwarancją, że chronione środowisko zostało poprawnie uruchomione, i pozwala na pomiar oprogramowania działającego w chronionym obszarze. Służy do tego proces atestacji opisany w podrozdziale 3.1. Informacje wymieniane podczas tego procesu są znane jako atestacja klucza tożsamości i służą do ustanowienia wzajemnego zaufania między stronami.
- **Uruchomienie chronione:** Zapewnia kontrolowane uruchamianie wraz z rejestrowaniem krytycznych komponentów oprogramowania systemowego w chronionym środowisku wykonawczym.

Seria procesorów Intel Xeon® Platinum Scalable oraz procesory poprzedniej generacji z serii Xeon Procesor E3, Xeon Procesor E5 i Xeon Procesor E7 obsługują Intel TXT.

Działanie Intel TXT polega na stworzeniu mierzonego środowiska uruchomieniowego (*ang. measured launch environment - MLE*) umożliwiającego dokładne porównanie wszystkich krytycznych elementów środowiska uruchomieniowego z dobrze znanym źródłem. Intel TXT tworzy kryptograficznie unikalny identyfikator dla każdego komponentu zatwierdzonego do uruchamiania. Następnie wprowadza sprzętowy mechanizm egzekwowania, który blokuje uruchamianie niezgodnego kodu albo wskazuje, kiedy spodziewane zaufane uruchomienie nie nastąpiło poprzez proces

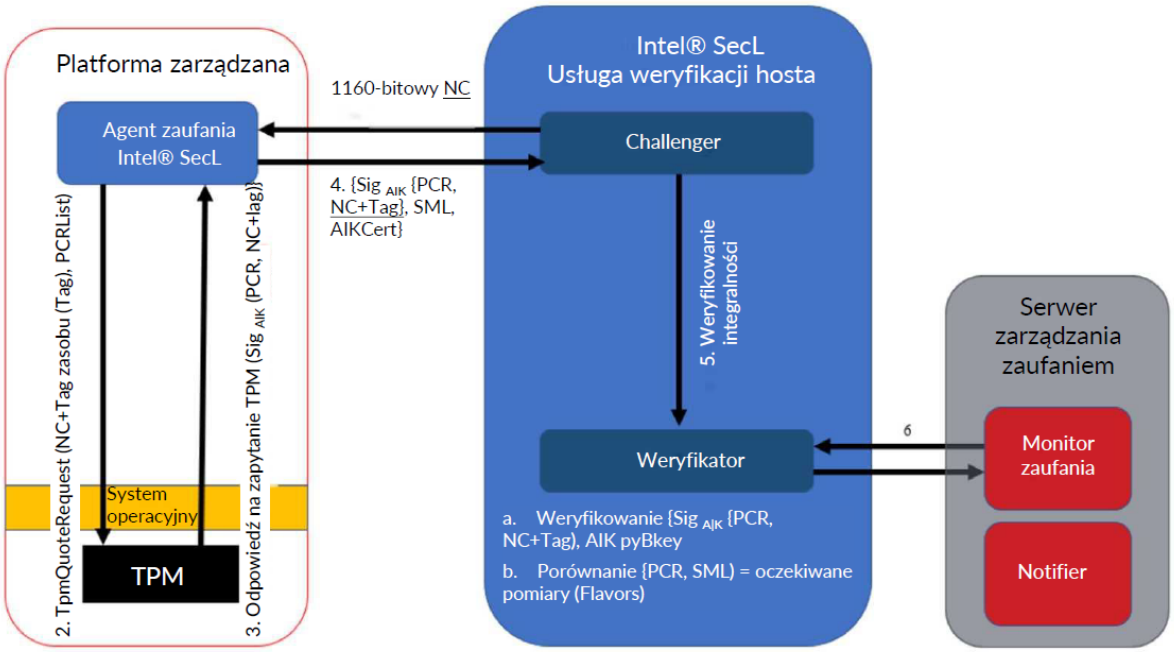
bezpiecznej zdalnej atestacji. Jeśli atestacja wskazuje, że jeden lub więcej zmierzonych komponentów w MLE nie spełnia oczekiwań, może to skutkować zablokowaniem orkiestracji obciążeń na podejrzanej platformie, nawet jeżeli sama platforma nadal jest uruchamiana. To rozwiązanie sprzętowe stanowi podstawę, na której administratorzy IT mogą budować zaufane rozwiązania platformowe w celu ochrony przed agresywnymi atakami programowymi oraz lepszej kontroli środowisk wirtualnych lub chmurowych. Dodatkowe informacje na temat TXT oraz innych technologii RTM, znajduje się w dokumentacji NISTIR 8320, *Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases* [1].

A.3 ATESTACJA

Rozważmy dwa główne problemy związane z inicjowaniem i dostarczaniem do chmury:

- Skąd podmiot potrzebujący tych informacji miałby wiedzieć, czy konkretna platforma ma włączoną funkcję Intel TXT? Czy konkretny serwer ma zgodny BIOS lub system operacyjny (tj. czy można mu zaufać)?
- Dlaczego podmiot żądający tych informacji (w środowisku chmury może to być na przykład harmonogram zasobów lub orkiestrator próbujący zaplanować usługę na zestawie dostępnych węzłów lub serwerów) miałby ufać odpowiedzi z platformy?

Organ atestacji udziela odpowiedzi na te pytania. Atestacja zapewnia kryptograficzny dowód zgodności, wykorzystując koncepcję źródła zaufania w celu zapewnienia środków bezpieczeństwa poprzez złożenie informacji z różnych źródeł zaufania w sposób przejrzysty i możliwy do wykorzystania przez inne podmioty. Rysunek 6 przedstawia protokół atestacji zapewniający środki do przekazywania pomiarów do challengera. Urządzenie atestujące punkt końcowy musi mieć możliwość pomiaru oprogramowania układowego BIOS, niskopoziomowych sterowników urządzeń oraz systemu operacyjnego i innych mierzonych komponentów, a także przekazywania tych pomiarów do organu atestującego. Urządzenie atestujące musi to zrobić jednocześnie chroniąc integralność, autentyczność, niezaprzeczalność, a w niektórych przypadkach, także poufność tych pomiarów.



Rysunek 6: Protokół zdalnej atestacji

Kroki przedstawione na rysunku 6 dotyczą protokołu zdalnego poświadczania:

1. Challenger, na prośbę osoby zgłaszającej żądanie, tworzy NC i wysyła je do agenta atestującego w węźle atestacji wraz z wybraną listą rejestrów konfiguracji platformy (PCR).
2. Agent atestujący wysyła to żądanie do TPM jako TPMQuoteRequest z NC i listą PCR.
3. W odpowiedzi na żądanie TPMQuote moduł TPM ładuje klucz tożsamości atestacji z zabezpieczonej pamięci w module TPM przy użyciu głównego klucza pamięci (SRK) oraz wykonuje polecenie *TPM Quote*, które służy do podpisania wybranych PCR i NC kluczem prywatnym *AIKpriv*. Dodatkowo agent atestacji pobiera dziennik pomiarów (*ang. stored measurement log - SML*).
4. W kroku *odpowiedzi na integralność* agent atestujący wysyła do challengera odpowiedź składającą się z podpisanego zapytania, podpisanego NC i SML. Agent atestujący dostarcza również poświadczenie AIK (*ang. Attestation Identity Key*), które składa się z AIKpub podpisanego przez urząd certyfikacji (*ang. certificate authority - CA*) prywatności.

5. Na etapie *weryfikacji integralności*:
    a. Challenger sprawdza, czy dane uwierzytelniające AIK zostały podpisane przez zaufany urząd certyfikacji prywatności, a tym samym należą do prawdziwego TPM. Challenger weryfikuje również, czy AIKpub jest nadal ważny, sprawdzając listę unieważnień certyfikatów zaufanej strony wydającej.
    b. Challenger weryfikuje podpis zapytania i sprawdza jego aktualność.
    c. Na podstawie otrzymanego SML i wartości PCR, challenger przetwarza SML, porównuje skróty poszczególnych modułów, które są rozszerzone na PCR, z „prawidłowymi znanymi lub wzorcowymi wartościami" i ponownie przelicza otrzymane wartości PCR. Jeśli poszczególne wartości są zgodne z wzorcowymi wartościami oraz jeśli obliczone wartości są zgodne z podpisanym zestawem, wtedy zdalny węzeł jest uznawany za zaufany.
6. Weryfikator informuje serwer zarządzania zaufaniem o stanie zaufania zdalnego węzła. Rejestruje stan zaufania w swojej bazie danych zarządzania, a następnie używa go do wszelkich indywidualnych lub zagregowanych żądań stanu urządzenia. Jeśli administrator subskrybuje zdarzenia związane z bezpieczeństwem, serwer będzie również wysyłał powiadomienia e-mail, gdy zarządzany węzeł zdalny zostanie rozpoznany jako niezaufany.

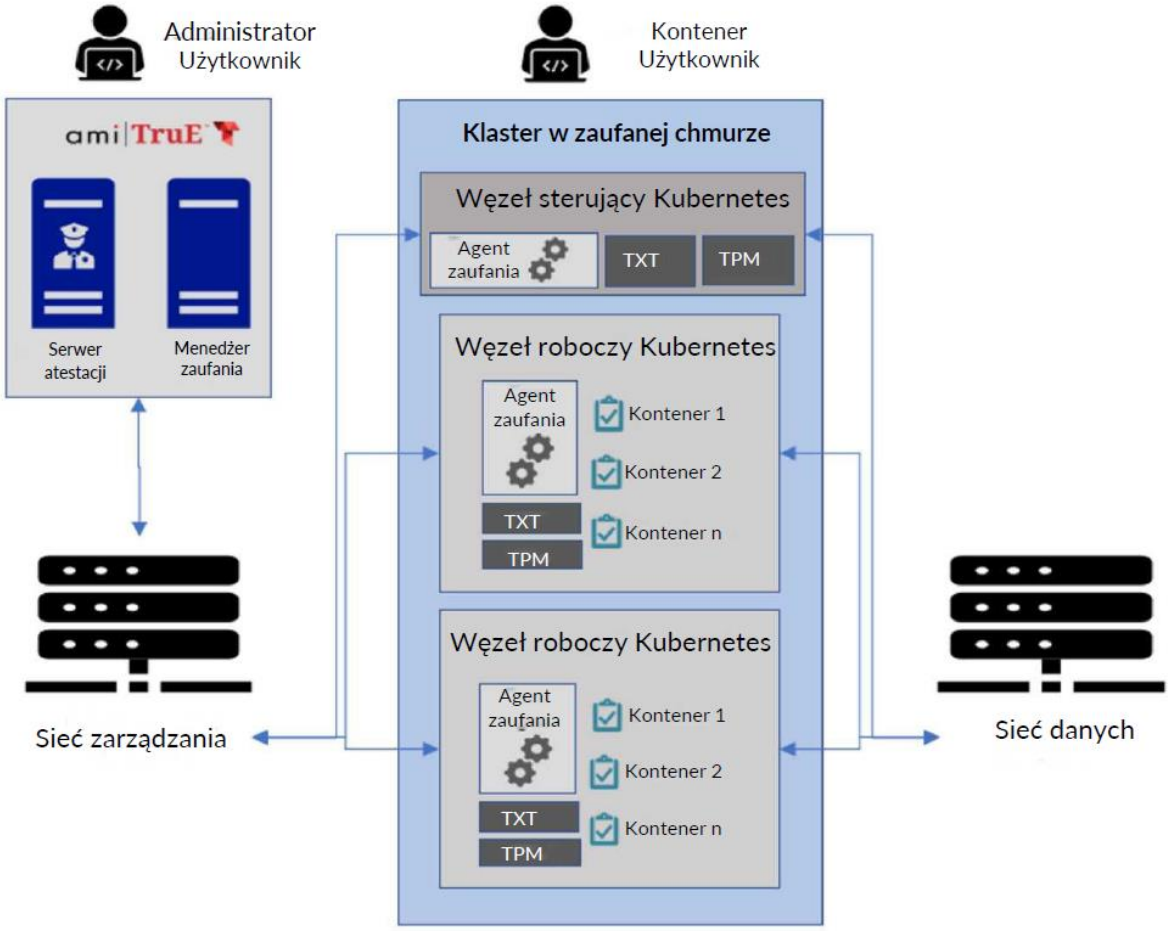
Protokół ten może pomóc w ograniczeniu ataków typu replay, tampering i masquerading.

ZAŁĄCZNIK B – IMPLEMENTACJA PLATFORMY: AMI TRUE

Ten rozdział zawiera dodatkowe informacje dostarczone przez AMI Trusted Environment (AMI TruE) opisujące wszystkie komponenty i kroki wymagane do skonfigurowania prototypowej implementacji [5].

B.1 ARCHITEKTURA ROZWIĄZANIA

Rysunek 7 pokazuje architekturę przedstawioną w Załączniku A, ale z określonymi produktami używanymi w implementacji platformy AMI TruE.



Rysunek 7: Implementacja prototypu AMI TruE

B.2 OPIS SPRZĘTU

Zaimplementowana architektura składa się z dwóch jednostek obliczeniowych Intel NUC (Next Units of Computing) działających jako węzły zarządzające oraz jednej jednostki Intel NUC z dwiema platformami serwerowymi z obsługą Intel TXT służącymi jako klaster zaufanej chmury. Sprzęt został szczegółowo opisany w Tabeli 3.

Tabela 3: Sprzęt zastosowany we wdrażanej architekturze

Sprzęt	Procesor	Pamięć	Przestrzeń dyskowa	System operacyjny
Jeden Intel NUC działający jako „węzeł sterujący Kubernetes”	Intel i5-7300U @ 2,60 GHz	8 GB	250 GB	Red Hat Enterprise Linux (RHEL) 8.1
Dwie platformy serwerów (z włączonym modułem Intel TXT) działające jako „węzły robocze Kubernetes”	Intel Xeon Platinum 8260L @ 2,40 GHz	96 GB	250 GB	RHEL 8.1
Intel NUC działający jako menedżer zaufania	Intel i5-7300U @ 2,60 GHz	8 GB	250 GB	RHEL 7.6
Intel NUC działający jako serwer atestacji	Intel i5-7300U @ 2,60 GHz	8 GB	250 GB	RHEL 8.1

B.3 INSTALOWANIE I KONFIGUROWANIE AMI TRUE

AMI TruE oferuje rozwiązania bezpieczeństwa dla centrów danych wykorzystujące technologie i biblioteki zabezpieczeń firmy Intel. Dzięki AMI TruE centra danych mogą osiągnąć wymagany poziom zaufania i bezpieczeństwa. Poniżej znajduje się lista zaawansowanych funkcji dostępnych w AMI TruE do zarządzania i zabezpieczania serwerów. Niektóre z nich zostały dokładniej omówione w dalszej części tego rozdziału.

- Automatyczne wykrywanie serwerów
- Zbieranie informacji o inwentaryzacji zasobów
- Monitorowanie stanu serwera
- Monitorowanie statusu zaufania dla wszystkich wykrytych serwerów

- Aprowizacja agenta TruE
- Korygowanie niezaufanych serwerów
- Powiadomienia e-mail o zdarzeniach związanych z kondycją lub zaufaniem
- Zdalne sterowanie zasilaniem
- Zdalna konsola (przekierowanie klawiatury, wideo, myszy [KVM])
- Konfiguracja oraz aktualizacja oprogramowania sprzętowego BIOS/BMC
- Aprowizacja systemu operacyjnego i oprogramowania
- Interfejs sieciowy oparty na języku znaczników hipertekstowych w wersji 5 (HTML5)
- Interfejsy API REST (*Representational State Transfer*) do automatyzacji lub integracji

AMI TruE składa się z dwóch komponentów: menadżera zaufania i serwera atestacji, dlatego do wdrożenia AMI TruE wymagane są dwa systemy fizyczne lub wirtualne. Tabela 4 przedstawia minimalne wymagania dla tych systemów.

Tabela 4: Minimalne wymagania systemowe do zainstalowania AMI TruE

Element systemu	Menedżer zaufania	Serwer atestacji
Procesor	CPU 4-rdzeniowy 2,66 GHz	CPU 4-rdzeniowy 2,66 GHz
Pamięć	8 GB	8 GB
Miejsce na dysku	100 GB	100 GB
System operacyjny	RHEL 7.6, 64-bitowy	RHEL 8.1, 64-bitowy

B.3.1. Instalowanie menedżera zaufania AMI TruE

Aby zainstalować menedżer zaufania w swoim systemie, należy wykonać następujące kroki:

1. Zalogować się do systemu menedżera zaufania jako użytkownik root.
2. Pobrać i rozpakować plik amitrue_trustmanager_artifacts.zip do folderu /root.
3. Uruchomić poniższe polecenia jako użytkownik root:

a. Ustawić uprawnienia do wykonywania skryptu instalacyjnego:

```
# chmod +x ./install.sh
```

b. Zainstalować menedżer zaufania AMI TruE, uruchamiając poniższy skrypt instalacyjny:

```
#./install.sh
```

B.3.2. Instalowanie serwera atestacji AMI TruE

Aby zainstalować serwer atestacji w swoim systemie, należy wykonać następujące czynności:

1. Zalogować się do systemu serwera atestacji jako użytkownik root.
2. Pobrać i rozpakować plik amitrue_attestationserver_artifacts.zip do folderu /root.
3. Edytować plik amitrue_security.env, aby skonfigurować następujące elementy:

   ```
   NAZWA HOSTA

   IP_HOSTNAME_ARRAY
   ```

4. Uruchomić poniższe polecenia jako użytkownik root:
   a. Ustawić uprawnienia do wykonywania skryptu instalacyjnego:

   ```
   # chmod +x ./install.sh
   ```

   b. Zainstalować serwer atestacji AMI TruE, uruchamiając poniższy skrypt instalacyjny:

   ```
   #./install.sh
   ```

B.3.3. Konfigurowanie zapory sieciowej dla AMI True

AMI True wykorzystuje kilka portów sieciowych do zarządzania i zabezpieczania platform. Skrypt instalacyjny automatycznie konfiguruje zaporę sieciową, aby zezwalała na użycie tych portów. Upewnij się, że żadne inne oprogramowanie lub narzędzie nie wyłącza żadnego z portów wymienionych w Tabeli 5 oraz Tabeli 6.

Tabela 5: Porty sieciowe dla menedżera zaufania

Port	Cel	Kierunek
9090	Port HTTP dla NGINX	Przychodzące/wychodzące
9443	Port HTTPS dla NGINX	Przychodzące/wychodzące
6379	Baza danych Redis	Wewnętrzny
5432	Baza danych PostgreSQL	Wewnętrzny
1900	Moduł Simple Service Discovery Protocol (SSDP) Discovery	Przychodzące/wychodzące
25/625	Podstawowa usługa powiadamiania (Simple Mail Transfer Protocol [SMTP])	Wychodzące
9089	Menedżer usług podstawowych	Wewnętrzny
9075	Core Discovery	Wewnętrzny
9065	Bezpieczeństwo platformy podstawowej	Wewnętrzny
9055	Core API Server	Wewnętrzny
9080	Serwer Redfish	Wewnętrzny
9091	Server Manager – KVM	Przychodzące/wychodzące

Tabela 6: Porty sieciowe dla serwera atestacji

Port	Cel	Kierunek
5432	Baza danych PostgreSQL	Wewnętrzny
8443	Usługa weryfikacji hosta (*ang. Host Verification Service – HVS*)	Przychodzące/wychodzące
8444	Usługa AAS (*ang. Authentication and Authorization Service*)	Przychodzące/wychodzące
8445	Usługa CMS (*ang. Certificate Management Service*)	Przychodzące/wychodzące
5000	Usługa obciążenia (WLS)	Przychodzące/wychodzące
9443	Usługa zarządzania kluczami (*ang. Key Management Service – KMS*)	Przychodzące/wychodzące
1443	Agent zaufania (*ang. Trust Agent – TA*)	Przychodzące/wychodzące
19082	Centrum integracji (*ang. Integration Hub – HUB*)	Przychodzące/wychodzące
19445	Centrum integracji (*ang. Integration Hub – HUB*)	Przychodzące/wychodzące

B.3.4. Konfigurowanie kluczy dostępu do urządzenia

AMI TruE potrzebuje poświadczeń, aby bezpiecznie komunikować się z wykrytymi urządzeniami, którymi może zarządzać. Aby skonfigurować klucze dostępu, należy wykonać następujące kroki:

1. W podmenu Settings (Ustawienia) w menu głównym wybrać Authentication Keys (Klucze uwierzytelniające).
2. Na stronie Keys (Klucze) użyć opcji Add (Dodaj) lub Edit (Edytuj), aby dodać poświadczenia dostępu dla różnych typów zasobów.

B.3.5. Konfigurowanie zakresu wykrywanie i zakresu zarządzania

Aby umożliwić AMI TruE wyszukiwanie i wykrywanie urządzeń w sieci, należy skonfigurować ją z zakresami adresów IP. Aby skonfigurować zakres wykrywania, należy wykonać następujące kroki:

1. Kliknąć ikonę menu głównego w lewym górnym rogu.
2. W grupie menu Settings (Ustawienie) kliknąć Discovery Settings (Ustawienia wykrywania).
3. Wybrać kartę Global (Globalne) w części Discovery Ranges (Zakresy ustawień).
4. Kliknąć przycisk Add (Dodaj) z prawej strony, aby dodać nowy zakres wykrywania.

Można wykluczyć z zarządzania niektóre wykryte urządzenia. Można skonfigurować zakres zarządzanych urządzeń, tak aby usługa AMI TruE zarządzała tylko urządzeniami mieszczącymi się w tym zakresie. Aby skonfigurować zakres zarządzania, należy wykonać następujące kroki:

1. Na stronie Discovery Settings (Ustawienia wykrywania) w obszarze Discovery Ranges (Zakresy wykrywania) wybrać kartę Manageability (Możliwość zarządzania).
2. Kliknąć przycisk Add (Dodaj), aby dodać zakres zarządzania. Rysunek 8 przedstawia przykładowy zestaw zakresów.

Range	Range Type	Effective Range	Manageability
10.2.0.0/15	CIDR	10.2.0.0 - 10.3.255.255	rmm
10.2.0.0/15	CIDR	10.2.0.0 - 10.3.255.255	rss
10.2.1.0/15	CIDR	10.2.0.0 - 10.3.255.255	fpx
10.2.1.0/15	CIDR	10.2.0.0 - 10.3.255.255	psme
10.2.1.0/24	CIDR	10.2.1.0 - 10.2.1.255	osm
10.2.3.3	Static	10.2.3.3	redfish
10.2.3.4	Static	10.2.3.4	redfish

Rysunek 8: Przykłady zakresów zarządzania

B.4 INSTALOWANIE I KONFIGUROWANIE KLASTRA W ZAUFANEJ CHMURZE

Wszystkie trzy węzły w klastrze w zaufanej chmurze muszą być skonfigurowane do zarządzania i zabezpieczania przez AMI TruE. Obejmuje to konfigurację ustawień BIOS, instalację agenta TruE i rejestrację tych agentów w AMI TruE. Operacje te można wykonać zdalnie za pomocą AMI TruE lub ręcznie. Załącznik B.4.1 zawiera instrukcje operacji zdalnych, a Załącznik B.4.2 zawiera instrukcje operacji ręcznych.

Wymagania wstępne dotyczące zabezpieczenia przez AMI TruE.

Aby można było włączyć atestowanie i monitorowanie statusu zaufania, zarządzane platformy muszą mieć:

- Procesor Intel Xeon lub Intel Xeon Scalable Family z obsługą Intel TXT
- Moduł TPM (wersja 1.2 lub 2.0) zainstalowany i wdrożony do użycia z Intel TXT, zgodnie ze specyfikacją Trusted Compute Group. Jeśli zostanie użyty moduł TPM w wersji 2.0, należy włączyć 256-bitowy algorytm PCR Secure Hash Algorithm (SHA256).
- Moduły TPM i Intel TXT włączone w BIOS
- Wyczyszczone uprawnienia TPM przed instalacją

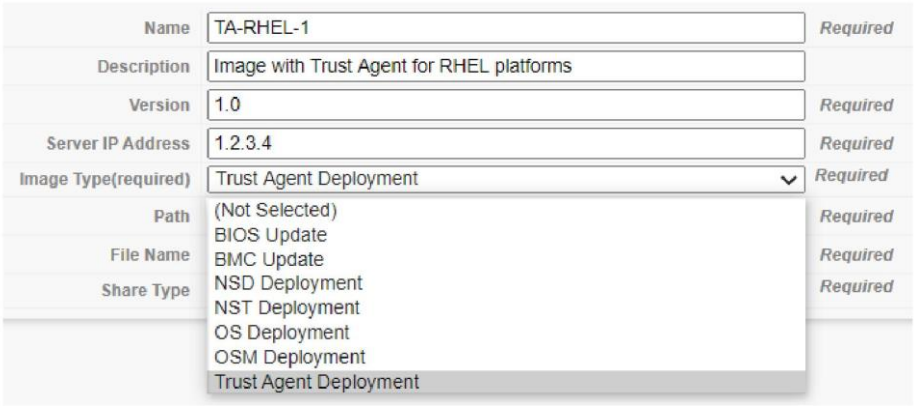
Aby można było naprawić lub odzyskać dane po naruszeniu zaufania, zarządzane platformy powinny mieć następujące funkcjonalności:

- BMC z obsługą Redfish
- BIOS z obsługą Redfish Host Interface
- Secure shell (SSH) włączona w systemie operacyjnym hosta

B.4.1. Zdalna aprowizacja agenta TruE

Aby aprowizować agenta TruE zdalnie za pomocą AMI TruE, należy wykonać następujące kroki:

1. Zalogować się do interfejsu WWW usługi AMI TruE.
2. W menu Provisions (Aprowizacje) użyć opcji Images (Obrazy), aby przejść do strony Images List (Lista obrazów).
3. Kliknąć opcję Add Image (Dodaj obraz) w górnym menu. Wprowadzić szczegóły dotyczące obrazu, jak pokazano na Rysunku 9. Po zakończeniu kliknąć przycisk Save (Zapisz).



Rysunek 9: Przykład dodawania obrazu

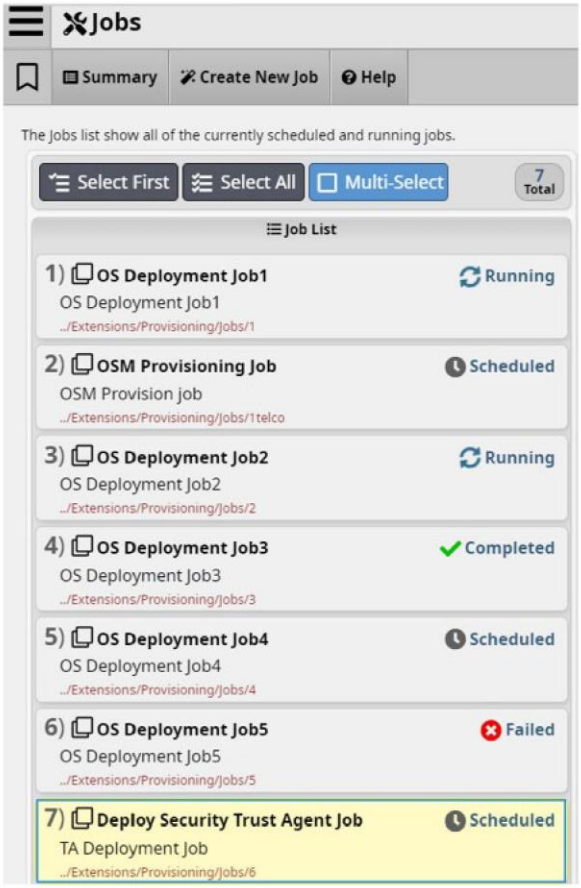
4. Przejść na stronę Create Job Wizard (Kreator tworzenia zadania) wybierając opcję Create Job (Utwórz zadanie) w menu Provisions (Aprowizacje). Następnie należy podać nazwę i opis tworzonego zadania, a jako jego typ wybrać TA Deployment.
5. Kliknąć Next (Dalej), aby przejść na stronę Select Image (Wybór obrazu). Ta strona zawiera listę wszystkich obrazów, które zostały wcześniej przesłane przez administratora. Wybrać obraz, który ma zostać użyty do wdrożenia.
6. Kliknąć Next (Dalej), aby przejść na stronę Targets (Cele). Wybrać jedną lub więcej platform z listy platform docelowych, na których ma zostać wdrożony agent zaufania.
7. Kliknąć Next (Dalej), aby przejść na stronę Schedule (Harmonogram). Można zdecydować się na wykonanie wdrożenia teraz lub zaplanować je w przyszłości. Należy ustawić opcję wymaganą dla tego wdrożenia.
8. Kliknąć przycisk Next (Dalej), aby przejść do karty Review Job Settings (Przejrzyj ustawienia zadań). Na tej stronie znajduje się podsumowanie informacji wprowadzonych dla danego zadania. Korzystając z przycisku Previous (Poprzedni), można wrócić do dowolnej strony kreatora i w razie potrzeby wprowadzić zmiany. Gdy ustawienia są odpowiednie, należy kliknąć przycisk Start, aby zainicjować proces wdrażania.

9. Można sprawdzić status zadania, klikając opcję Jobs (Zadania) w menu Provisioning (Aprowizacja). Na tej stronie wyświetlane są wszystkie zaplanowane zadania wraz z ich bieżącymi statusami, jak w przykładzie na Rysunku 10.
   W razie potrzeby zaplanowane zadanie można anulować za pomocą przycisku Cancel Job (Anuluj zadanie).

B.4.2. Ręczna aprowizacja agenta TruE

Aby aprowizować agenta TruE ręcznie, należy wykonać następujące kroki:

1. Rejestracja menedżera subskrypcji RedHat jest obowiązkowa. Aby go zarejestrować, należy skorzystać z poniższych instrukcji:



Rysunek 10: Przykład listy zadań:

   a. Utworzyć konto RedHat.

   b. Upewnić się, że system ma dostęp do Internetu.

   c. Rozpocząć dostęp do terminala, logując się jako użytkownik root.

d. Wpisać “subscription-manager-gui”. Wyświetli się okienko Subscription Manager.

e. Kliknąć przycisk Register (Zarejestruj) i wpisać poświadczenia dostępu, aby się zarejestrować.

2. Wyłączyć zaporę sieciową w systemie docelowym, uruchamiając następujące polecenia:

```
$ sudo systemctl stop firewalld
$ sudo systemctl disable firewalld
```

3. Przejść do ustawień systemu BIOS. Włączyć moduł TPM2 i wyczyścić własność.

4. Aby korzystać z opcji Unified Extensible Firmware Interface (UEFI) SecureBoot dla zaufanego rozruchu, należy ją włączyć w ustawieniach BIOS-u i pominąć następny krok, w przeciwnym razie zostanie użyty tboot i nie należy włączać opcji SecureBoot.

5. Aby używać tboot, należy wykonać następujące kroki:

   a. Uruchomić to polecenie, aby zainstalować tboot:

   ```
   # yum install tboot
   ```

   b. Utworzyć kopię zapasową bieżącego pliku grub.cfg:

   ```
   # cp /boot/grub2/grub.cfg /boot/grub2/redhat/grub.bak
   ```

   c. Wygenerować nowy plik grub.cfg z opcją rozruchu tboot:

   ```
   # grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

   d. Zaktualizować domyślną opcję rozruchu. Upewnić się, że wartość GRUB_DEFAULT jest ustawiona na opcję tboot. Opcję rozruchu tboot można znaleźć w pliku „/boot/redhat/grub.cfg”.

6. Ponownie uruchomić system. Ponieważ pomiar odbywa się podczas uruchamiania systemu, ponowny rozruch jest wymagany do uruchomienia opcji rozruchu tboot i wypełnienia pomiarów w module TPM.

7. Aby sprawdzić, czy zaufany rozruch z opcją tboot przebiegł pomyślnie, uruchomić polecenie `txt-stat` i wyświetlić plik dziennika tboot. Sprawdzić, czy parametry TXT measured launch i secrets flag set mają wartość TRUE.

```
**********************************************************
TXT measured launch: TRUE
secrets flag set: TRUE
**********************************************************
```

8. Zainstalować agenty AMI TruE, wykonując następujące kroki:
   a. Zalogować się jako użytkownik root i uruchomić wszystkie poniższe polecenia jako użytkownik root.
   b. Skopiować plik „pkgs/platform-security-agent-artifacts.zip do folderu /root.
   c. Rozpakować artefakty w folderze „/root".
   d. Skopiować z „platform-security-agent-artifacts" pliki „install_agent.sh" I „install_agent.env" do folderu „/root".
   e. Skonfigurować plik „install_agent.env" w następujący sposób:
      I. Zmienna HOSTNAME nie może być pusta. Ta zmienna służy do ustawienia nazwy hosta dla systemu (np. demo, demo-name-one, demo2).

      Uwaga: Zmienna HOSTNAME nie może zawierać podkreśleń.

      II. Zmienna IP_HOSTNAME_ARRAY nie może być pusta. Należy podać pary IP i HOSTNAME oddzielone spacjami. Ta zmienna służy do edycji pliku „/etc/hosts" za pomocą podanych adresów IP i nazw hostów.

      Na przykład: `IP_HOSTNAME_ARRAY=(10.0.0.0 demo 10.0.0.1 demo-name-one 10.0.0.2 demo2)`

      Uwaga: Najpierw należy podać adres IP, a następnie nazwę hosta dla tego adresu IP. Należy uważać, aby nie pomylić adresów IP i nazw hostów.

III. Należy zastąpić wszystkie wystąpienia „127.0.0.1” adresem IP systemu, wszystkie wystąpienia „localhost” w adresach URL adresem IP systemu, a wszystkie inne wystąpienia „localhost” nazwą hosta systemu.

IV. Należy wygenerować BEARER_TOKEN i CMS_TLS_CERT_SHA384 za pomocą skryptu instalacyjnego usługi z opcją „populate-users” na komputerze, na którym są uruchomione wszystkie usługi. Następnie należy skopiować i wkleić wartości do pliku env.

V. Dla NO_PROXY i HTTPS_PROXY należy podać odpowiednio registry_ip i proxy_url.

Uwaga: W pliku env nie należy używać niepotrzebnych spacji.

Uwaga: Są to podstawowe wytyczne. Jeśli użytkownicy mają odpowiednią wiedzę na temat tych zmiennych środowiskowych, mogą je modyfikować zgodnie z własnymi potrzebami.

f. Ustawić uprawnienia do wykonywania skryptu instalacyjnego.

```
# chmod +x install agent.sh
```

g. Uruchomić skrypt instalacyjny.

```
# ./install agent.sh install
```

h. Skrypt wyświetli kilka komunikatów o zależnościach i zapyta, czy kontynuować instalację. Wpisać „yes”, aby kontynuować instalację.

i. Po zainstalowaniu TA skrypt ponownie uruchomi system. Po ponownym uruchomieniu należy się zalogować jako użytkownik root i ponownie uruchomić skrypt.

```
# ./install agent.sh install
```

j. Po zainstalowaniu agenta obciążenia skrypt ponownie uruchomi system, aby zakończyć instalację.

B.5 KORZYSTANIE Z AMI TRUE

Po zainstalowaniu i skonfigurowaniu AMI TruE rozpoczyna wykrywanie i monitorowanie kondycji i poziomu zaufania wszystkich zarządzanych platform. W tym punkcie omówiono funkcje dostępne w AMI TruE służące do monitorowania i zabezpieczania platform.

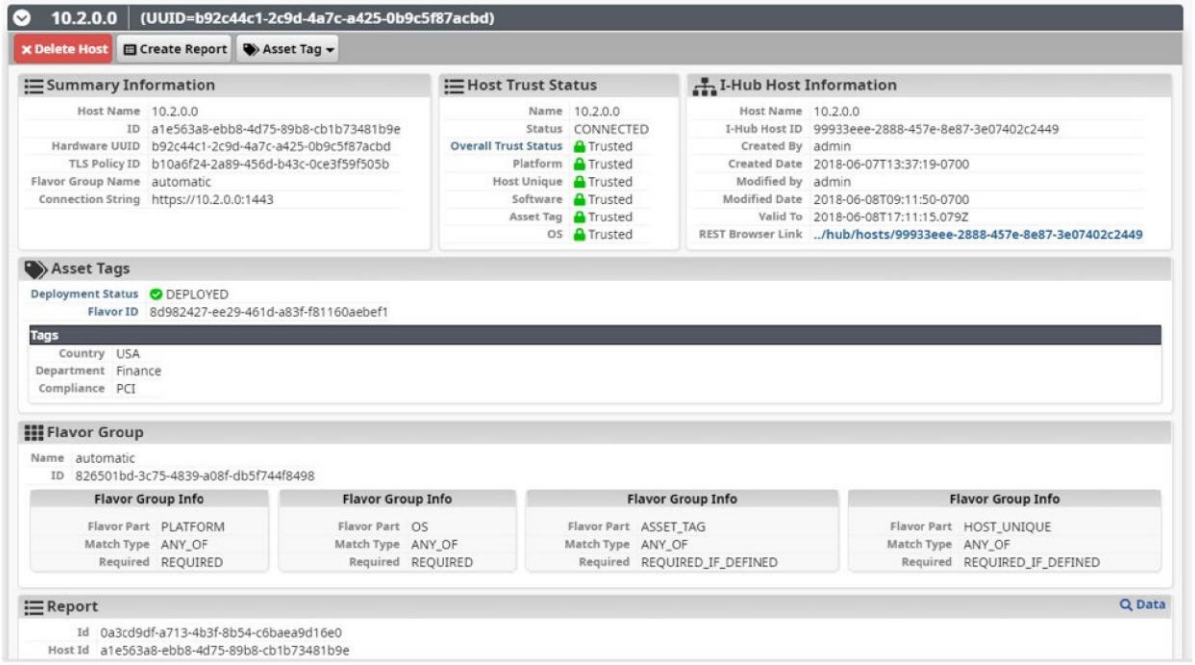
B.5.1. Monitorowanie statusu zaufania za pomocą AMI TruE

Wystarczy połączyć się z AMI TruE z dowolnej standardowej przeglądarki internetowej i użyć poświadczeń do zalogowania się do interfejsu internetowego. Wyświetli się pulpit nawigacyjny z kilkoma widżetami. Do pulpitu nawigacyjnego można również przejść z dowolnej innej strony interfejsu internetowego, klikając ikonę menu hamburgera w lewym górnym rogu i wybierając menu Dashboard (Pulpit nawigacyjny). Rysunek 11 przedstawia pulpit nawigacyjny z wykresem odzwierciedlającym względny rozmiar pul zaufanych (zielony), niezaufanych (czerwony) i nieznanych (szary) serwerów w chmurze. W tym przykładzie w puli zaufanej znajduje się osiem serwerów, a w puli niezaufanej są dwa serwery. Bardziej szczegółowe informacje o zaufaniu, w tym stan bezpieczeństwa węzłów, status zaufania w zależności od wariantu itp. również znajdują się na tym pulpicie nawigacyjnym.

Rysunek 11: Przykład pulpitu nawigacyjnego raportu AMI TruE

Kliknięcie linku Go to Hosts Collection (Przejdź do kolekcji hostów) w prawym górnym rogu pulpitu nawigacyjnego powoduje przejście do bardziej szczegółowej strony zarządzania. Kliknięcie jednego z serwerów wymienionych na stronie Hosts (Hosty) spowoduje wyświetlenie informacji o zaufaniu dla wybranego serwera, jak pokazano na Rysunku 12.

Informacje te zawierają nazwę hosta, identyfikator UUID sprzętu, szczegóły dotyczące wersji, tagowania zasad, adres URL połączenia i status zaufania komponentu.



Rysunek 12: Przykład strony z podsumowaniem informacji dla serwera zaufania

B.5.2. Generowanie raportów dotyczących zaufania

Aby wygenerować nowy raport dla platformy, wybierz tę platformę z listy hostów i kliknij opcję Create Report (Utwórz raport). Pobrany raport jest prezentowany jako część informacji o hoście, jak pokazano na Rysunku 13.

Rysunek 13: Przykład raportu zaufania

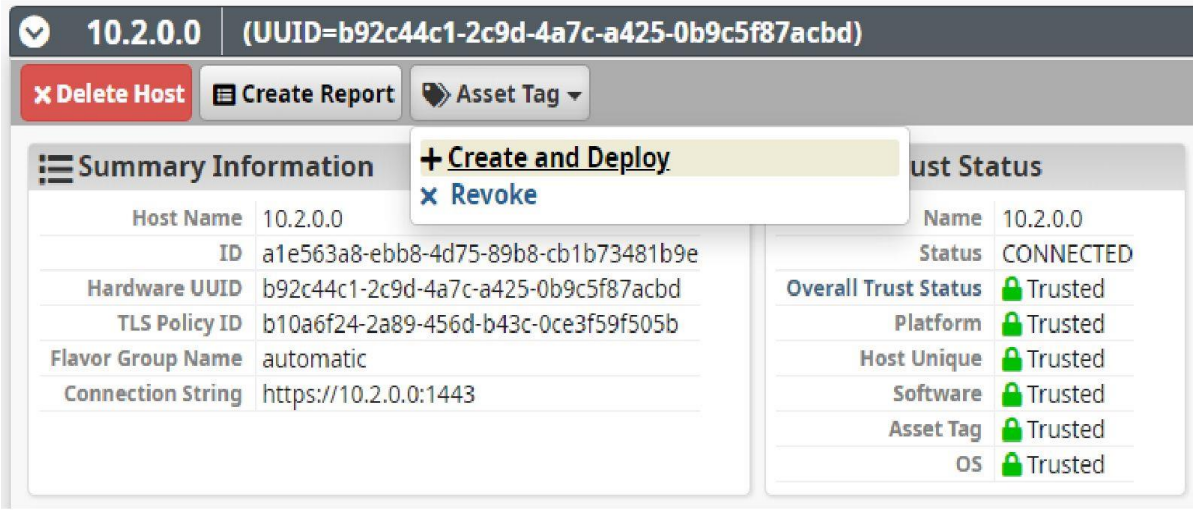
Aby wyświetlić nieprzetworzone dane JSON (*ang. JavaScript Object Notation*) dla dowolnych potrzeb analitycznych, kliknij opcję Data (Dane) w prawym górnym rogu okna report (Raport).

B.5.3. Tagowanie platform za pomocą AMI TruE

Tagi zasobów są używane do tagowania zarządzanych platform za pomocą jednego lub więcej atrybutów zdefiniowanych przez użytkownika, takich jak tag zasobu, informacje o zgodności lub typ klienta. Umożliwia to lokowanie i orkiestrację obciążeń w oparciu o zasady.

AMI TruE zapewnia opcje tworzenia i wdrażania nowych tagów zasobów na jednej lub kilku zarządzanych platformach. Ponadto umożliwia cofnięcie wcześniej utworzonego tagu zasobu. Aby utworzyć i wdrożyć tag zasobu, należy:

1. Otworzyć menu główne i przejść do strony Hosts (Hosty) w grupie menu Security (Bezpieczeństwo).
2. Wybrać jeden lub więcej serwerów z listy hostów, aby wybrać platformy, dla których mają zostać wdrożone tagi zasobów.
3. Kliknąć menu Asset Tag (Tag zasobu) po prawej stronie strony i wybrać opcję Create and Deploy (Utwórz i wdróż), jak pokazano na Rysunku 14.



Rysunek 14: Przykład utworzenia i wdrożenia tagu zasobu

4. Powinno się wyświetlić okno Asset Tag Creation (Tworzenie znacznika zasobu).
   a. Aby dodać tag zasobu do listy, należy wprowadzić jego nazwę i wartość w polach Key Name (Nazwa klucza) i Key Value (Wartość klucza), a następnie kliknąć przycisk Add (Dodaj).
   b. Aby usunąć określony tag z listy, należy kliknąć przycisk „X” obok niego na liście tagów zasobów.
   c. Po dodaniu jednego lub więcej tagów zasobów należy kliknąć przycisk Deploy (Wdróż), aby wdrożyć wszystkie wymienione tagi zasobów na wybranych platformach.

Alternatywnie można kliknąć pozycję menu Asset Tag (Tag zasobu) w górnym menu, będąc na stronie Hosts (Hosty), aby uruchomić stronę Asset Tag (Tag zasobu). Strona ta zawiera opcje filtrowania platform za pomocą opcji Search (Szukaj). Następnie można użyć przefiltrowanej listy platform do wdrożenia tagu zasobów, jak opisano powyżej.

B.5.4. Otrzymywanie powiadomień o zdarzeniach dotyczących zaufania

Powiadomienie, gdy platforma staje się niezaufana, pozwala administratorom szybko podjąć działania naprawcze. AMI TruE udostępnia dwa tryby powiadomień o wszelkich zdarzeniach bezpieczeństwa: alerty e-mail i wpisy w dzienniku zdarzeń.

B.5.4.1. Alerty e-mail

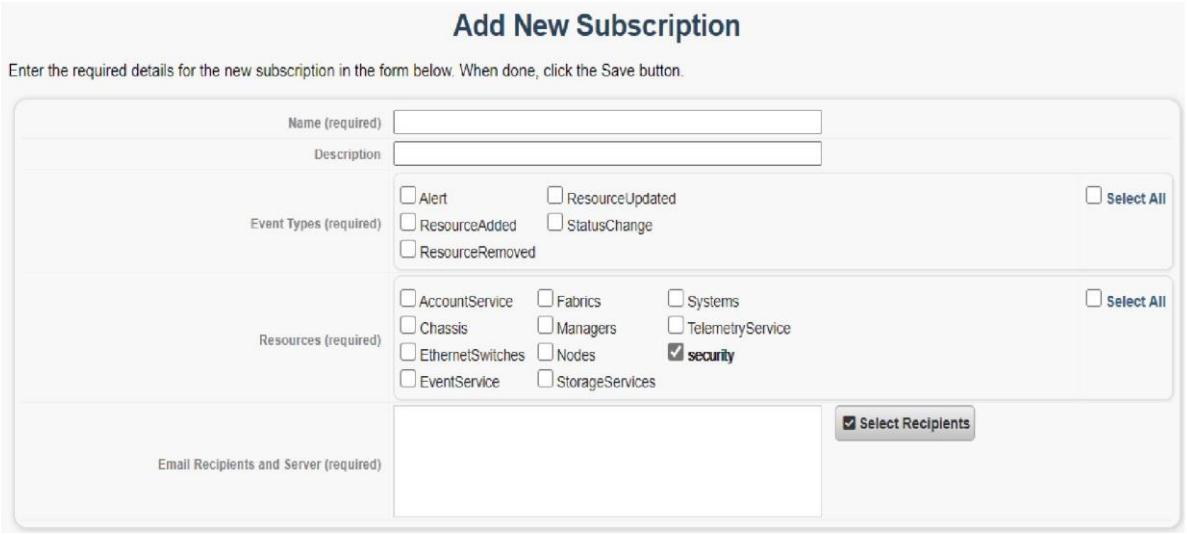
Administratorzy mogą zdecydować się na otrzymywanie powiadomień e-mail o zdarzeniach związanych z bezpieczeństwem. Rozpoczyna się to od dodania informacji o jednym lub kilku serwerach poczty e-mail, które mogą być używane do wysyłania informacji o alertach.

1. Aby dodać serwer e-mail, należy wybrać ikonę menu głównego (ikona hamburgera) w lewym górnym rogu, a następnie wybrać Email Notifications (Powiadomienia e-mail) w grupie menu Notifications (Powiadomienia).
2. W wyświetlonym menu należy wybrać opcję Configure Email Servers (Konfiguruj serwery poczty). Wyświetli się lista skonfigurowanych serwerów poczty e-mail oraz opcje dodawania nowej konfiguracji serwera poczty e-mail, modyfikowania istniejącej konfiguracji serwera poczty e-mail lub usuwania wcześniej skonfigurowanego serwera.
3. Należy kliknąć opcję Add (Dodaj), aby dodać nową pozycję, lub wybrać wiersz i kliknąć Edit (Edytuj), aby edytować istniejącą pozycję. Po wprowadzeniu szczegółów serwera poczty należy kliknąć opcję Save (Zapisz).
4. Po skonfigurowaniu co najmniej jednego serwera e-mail, następnym krokiem jest dodanie adresów e-mail administratorów lub inżynierów wsparcia, którzy mają otrzymywać powiadomienia o wszelkich zdarzeniach związanych z zaufaniem. Aby wyświetlić książkę adresową e-mail, należy kliknąć ikonę menu głównego (ikonę hamburgera) w lewym górnym rogu i wybrać opcję Email Notifications

(Powiadomienia e-mail) w grupie menu Notifications (Powiadomienia). W wyświetlonym menu należy wybrać Email Address Book (Książka adresowa). Do zarządzania adresami e-mail służą opcje Add (Dodaj), Edit (Edytuj) i Delete (Usuń) na karcie Email Addresses (Adresy e-mail). Ponadto grupy e-mail mogą być używane do powiadamiania grupy administratorów o określonych zdarzeniach. Grupami e-mail można zarządzać na karcie Email Groups (Grupy e-mail) na stronie Email Address Book (Książka adresowa).

5. Po dodaniu adresów e-mail lub grup, kolejnym krokiem jest skonfigurowanie subskrypcji powiadomień. Z menu głównego należy wybrać opcję Notification Subscriptions (Subskrypcje powiadomień) w grupie menu Notifications (Powiadomienia).

6. Do skonfigurowania subskrypcji zdarzeń służy opcja Add New Subscriptions (Dodaj nowe subskrypcje) na stronie Notification Subscriptions (Subskrypcje powiadomień). Na stronie Add New Subscriptions (Dodaj nowe subskrypcje), jak to pokazano na Rysunku 15, należy wybrać typy zdarzeń i zasoby (zasoby zdarzeń), dla których mają być wysyłane powiadomienia. Można wybrać Security (Bezpieczeństwo) jako zasób, który ma otrzymywać wszelkie zdarzenia związane z zaufaniem.



Rysunek 15: Przykład strony Add New Subscription (Dodaj nową subskrypcję)

7. Następnie należy kliknąć Select Recipients (Wybierz odbiorców) i wybrać co najmniej jeden adres e-mail lub grupę adresów, na które mają być wysyłane powiadomienia. Po zakończeniu kliknąć przycisk Save (Zapisz), aby dodać subskrypcję.

B.5.4.2. Dzienniki zdarzeń

AMI TruE rejestruje w dzienniku zdarzeń wszystkie zdarzenia związane z platformą, w tym zdarzenia dotyczące bezpieczeństwa. Administratorzy mogą przeglądać te zdarzenia za pośrednictwem interfejsu internetowego.

1. Aby wyświetlić dzienniki zdarzeń, należy wybrać ikonę menu głównego (ikona hamburgera) w lewym górnym rogu i kliknąć opcję Global Event Log (Globalny dziennik zdarzeń) w grupie menu Logs (Dzienniki).
2. Po przejrzeniu dzienników zdarzeń i podjęciu odpowiednich działań administratorzy mogą usunąć zdarzenia za pomocą opcji Clear Log (Wyczyść dziennik) na stronie Global Event Log (Globalny dziennik zdarzeń).

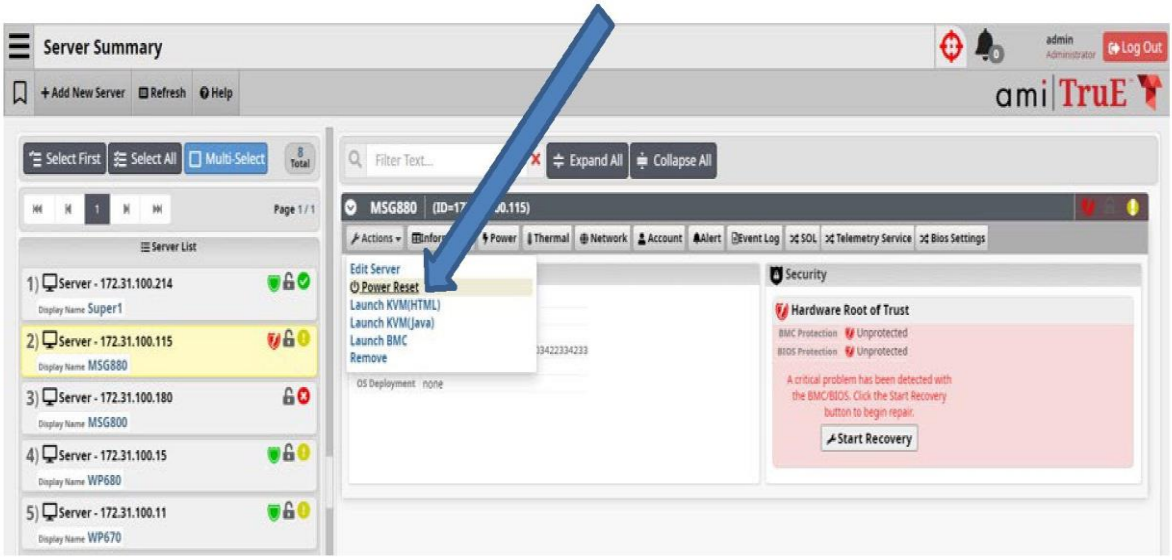
B.5.5. Używanie AMI TruE do usuwania skutków awarii

Zdolność do pełnej naprawy i odzyskania danych jest jedną z kluczowych potrzeb w zakresie odporności platformy. AMI TruE oferuje wiele opcji odzyskiwania zaatakowanej platformy.

B.5.5.1. Zdalne sterowanie zasilaniem

AMI TruE udostępnia funkcje zdalnego zarządzania zasilaniem w celu włączenia / wyłączenia lub zresetowania / ponownego uruchomienia platformy w ramach działań naprawczych.

1. Po kliknięciu ikony menu głównego w lewym górnym rogu należy wybrać opcję Server Summary (Podsumowanie serwera) w menu Server Manager (Menedżer serwerów). Ta strona zawiera listę wszystkich zarządzanych serwerów w lewym panelu z ikonami przedstawiającymi ich status zaufania, kondycję i stan zasilania. Należy wybrać serwer, który ma zostać zamknięty lub wyłączony. W prawym panelu należy kliknąć przycisk Actions (Działania) i wybrać opcję Power Reset (Resetowanie zasilania), jak pokazano na Rysunku 16.



Rysunek 16: Przykład zdalnego sterowania zasilaniem

2. Zostanie wyświetlone wyskakujące okno z opcjami wyboru typu operacji zasilania, która ma zostać wykonana. Aby kontynuować, należy wybrać odpowiednią operację sterowania zasilaniem i kliknąć przycisk OK.

B.5.5.2. Zdalna aktualizacja oprogramowania układowego

Korzystając z AMI TruE, można skonfigurować BIOS/BMC lub zaktualizować całe oprogramowanie układowe BIOS/BMC, jeśli warstwa oprogramowania układowego stanie się niezaufana.

1. Pierwszym krokiem do aktualizacji oprogramowania układowego BIOS lub BMC jest przesłanie obrazów oprogramowania układowego. W menu Provisions (Dostarczanie) należy wybrać opcję Images (Obrazy).
2. Aby dodać nowy obraz dla dowolnej aprowizacji, wystarczy kliknąć przycisk Add Image (Dodaj obraz) w górnym menu. Aby umożliwić AMI TruE filtrowanie i prezentowanie pasujących obrazów dla określonego zadania aprowizacji, należy wprowadzić szczegóły dotyczące lokalizacji obrazu oprogramowania układowego, szczegóły wersji itp.
3. Po przesłaniu obrazu oprogramowania układowego BMC lub BIOS należy utworzyć zadanie, aby zaktualizować oprogramowanie układowe natychmiast lub w zaplanowanym czasie. AMI TruE udostępnia kreator umożliwiający

utworzenie zadania w celu wybrania obrazów, węzłów docelowych i ich natychmiastowej aktualizacji lub zaplanowania aktualizacji na przyszłą datę i godzinę. Aby utworzyć zadanie, na stronie Jobs (Zadania) należy kliknąć opcję Create New Job (Utwórz nowe zadanie).

4. Następnie należy wpisać nazwę zadania, dodać opis i wybrać opcję BIOS Update lub BMC Update jako typ zadania. Kliknąć Next (Dalej), aby przejść do zakładki Image (Obraz).
5. Następnie należy wybrać obraz, który ma zostać użyty, i kliknąć Next (Dalej), aby przejść do strony Targets (Cele). Ta strona zawiera listę wszystkich platform docelowych z BIOS-em lub BMC, które można zaktualizować, w zależności od wybranego typu zadania.
6. Po wybraniu jednej lub więcej platform docelowych, które mają zostać zaktualizowane, należy wybrać przycisk Next (Dalej), aby przejść do karty Schedule (Harmonogram). Na tej karcie dostępne są opcje natychmiastowego uruchomienia zadania lub zaplanowania jego uruchomienia w przyszłości. Po skonfigurowaniu ustawień należy kliknąć przycisk Next (Dalej), aby przejść do karty Review Job Settings (Przejrzyj ustawienia zadań).
7. Można tu przejrzeć informacje wprowadzone dla tego zadania aktualizacji. Używając przycisku Previous (Poprzedni) można przejść do innych kart w tym kreatorze, aby w razie potrzeby zmienić dane. Po zakończeniu można kliknąć przycisk Start, aby rozpocząć lub zaplanować zadanie aktualizacji.
8. Aby sprawdzić status zaplanowanego zadania, należy wybrać opcję Jobs (Zadania) w menu Provisioning (Aprowizacja). Wyświetli się lista wszystkich uruchomionych lub zaplanowanych zadań i będzie można je anulować, jeśli zajdzie taka potrzeba.

B.5.5.3. Zdalne instalowanie systemu operacyjnego

Jeśli system operacyjny zostanie zaatakowany, AMI TruE zapewnia opcje zdalnej ponownej instalacji wersji systemu operacyjnego, która jest uznana za zaufaną przez organizację lub centrum danych. Należy wykonać kroki opisane w Załączniku B.5.5.2, ale w polu Job Type (Typ zadania) wybrać OS Deployment (Wdrożenie systemu operacyjnego).

ZAŁĄCZNIK C – IMPLEMENTACJA PLATFORMY: KUBERNETES

Załącznik zawiera dodatkowe informacje opisujące wszystkie wymagane komponenty i kroki niezbędne do skonfigurowania prototypowej implementacji dla Kubernetes.

C.1 ARCHITEKTURA PROTOTYPU

Diagram architektury znajduje się na Rysunku 7 w Załączniku B.1.

C.2 OPIS SPRZĘTU

Opis sprzętu używanego podczas konfigurowania Kubernetes znajduje się w Załączniku B.2.

C.3 INSTALOWANIE I KONFIGUROWANIE KUBERNETES

Wdrożenia Kubernetes w minimalnym stopniu składają się z węzłów sterujących i węzłów roboczych, które wykorzystują określone środowisko uruchomieniowe kontenera. Istnieje wspólny zestaw wymagań dla obu typów węzłów, a także unikalne konfiguracje dla każdego typu węzła. W tej implementacji zainstalowano Docker 19.3.5 jako środowisko uruchomieniowe kontenera i uruchomiono kubelet w wersji 1.17.0 jako warunek wstępny.

Wstępnie wymagana instalacja:

Poniższe polecenia włączają nakładki ruchu sieciowego dla komunikacji między zasobnikami Kubernetes w klastrze.

```
# cat > /etc/modules-load.d/containerd.conf <<EOF overlay
br netfilter
EOF
# modprobe overlay
# modprobe br netfilter
# cat > /etc/sysctl.d/99-kubernetes-cri.conf <<EOF
net.bridge.bridge-nf-call-iptables = 1
net.ipv4.ip forward  =    1
net.bridge.bridge-nf-call-ip6tables = 1
EOF
# sysctl --system
# systemctl enable containerd
```

Poniższe polecenia dodają repozytorium Kubernetes potrzebne do instalacji pakietów oprogramowania.

```
# cat <<EOF > /etc/yum.repos.d/kubernetes.repo
[kubernetes]
name=Kubernetes
baseurl=https://packages.cloud.google.com/yum/repos/kubernetes-el7- x86_64
enabled=1
gpgcheck=1
repo gpgcheck=1
gpgkey=https://packages.cloud.google.com/yum/doc/yum-key.gpghttps://packages.cloud.google.com/yum/doc/rpm-package-key.gpg
EOF
```

Poniższe polecenia instalują i uruchamiają niezbędne pakiety oprogramowania Kubernetes.

```
# dnf install -y kubeadm-1.17.0 kubelet-1.17.0 kubectl-1.17.0
# systemctl enable kubelet
# echo 'KUBELET_EXTRA_ARGS="—fail-swap-on=false"' >
/etc/sysconfig/kubelet
# systemctl start kubelet
```

Uruchomienie poniższego polecenia spowoduje wyświetlenie danych wyjściowych pokazanych na Rysunku 17:

```
# kubectl describe nodes
```

```
System Info:
  Machine ID:                 8a2900f0e5ff4c1fa525e609cf9f7514
  System UUID:                237accad-ab12-03ce-1000-bfde6a6dc4e0
  Boot ID:                    24a26a03-d512-4cd4-85fd-e2e8a35a985a
  Kernel Version:             4.18.0-193.14.3.el8_2.x86_64
  OS Image:                   Red Hat Enterprise Linux 8.2 (Ootpa)
  Operating System:           linux
  Architecture:               amd64
  Container Runtime Version:  docker://19.3.5
  Kubelet Version:            v1.17.0
  Kube-Proxy Version:         v1.17.0
PodCIDR:                      10.10.20.0/24
PodCIDRs:                     10.10.20.0/24
```

Rysunek 17: Wersje Kubelet i Docker

C.3.1. Konfiguracja węzła sterującego Kubernetes

Poniższe polecenie jest wykonywane w celu ukończenia konfiguracji węzła sterującego Kubernetes w tej implementacji poprzez ustanowienie sieci nakładkowej warstwy zabezpieczeń.

```
# kubeadm init --pod-network-cidr=10.10.20.0/24
```

Uruchom następujące polecenia, aby umożliwić bieżącemu użytkownikowi, w tym przypadku root, korzystanie z klastra.

```
# mkdir -p $HOME/.kube
# sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
# sudo chown $(id -u):$(id -g) $HOME/.kube/config
```

Uruchom następujące polecenie, aby włączyć Calico jako interfejs CNI (*ang. Container Network Interface*).

```
# kubectl apply -f
https://docs.projectcalico.org/manifests/calico.yaml
```

C.3.2. Konfiguracja węzła roboczego Kubernetes

Po uruchomieniu węzła sterującego do wdrożenia Kubernetes można dołączyć węzły robocze. Do dołączenia węzłów roboczych do klastra Kubernetes

wymagany jest token. Aby uzyskać token, należy uruchomić w węźle sterującym poniższe polecenie.

```
# kubeadm token create --print-join-command
```

Poniższe polecenie jest wykonywane w celu dołączenia węzłów roboczych do wdrożenia Kubernetes, które zostało uzyskane w wyniku wykonania poprzedniego polecenia.

```
# kubeadm join 172.16.100.61:6443 --token <token redacted>
--discovery- token-ca-cert-hash \
                        sha256:<hash redacted>
```

Po dołączeniu węzła roboczego do klastra Kubernetes należy uruchomić następujące polecenie w węźle sterującym, aby sprawdzić, czy węzły w klastrze są gotowe:

```
# kubectl get nodes
```

C.3.3. Orkiestracja Kubernetes

Aby klaster Kubernetes mógł wykorzystywać pomiary zaufania i tagi zasobów hostów w swoich politykach planowania, węzeł sterujący Kubernetes musi być skonfigurowany do komunikacji z usługą centrum atestacji w instalacji AMI. Na serwerze weryfikacji hosta AMI pod adresem `/root/binaries/k8s/isecl-k8s-extensions-v2.0.0.bin` znajduje się instalacyjny plik binarny, który należy skopiować i uruchomić w węźle sterującym Kubernetes. Spowoduje to utworzenie niestandardowych definicji zasobów (*ang. Custom Resource Definitions - CRD*), które umożliwią wykorzystanie pomiarów zaufania ISecL i tagów zasobów przez harmonogram Kubernetes.

Dla hostów Kubernetes należy utworzyć tenant[9], do którego należy je dodać w kliencie internetowym AMI TruE. Podczas tworzenia tenantu użytkownik może wybrać powiązanie hostów, które są już w usłudze weryfikacji hostów. Po dodaniu hostów do tenantu ich pomiary zaufania i tagi zasobów mogą być używane w zasadach planowania Kubernetes. Aby włączyć pomiary zaufania używane przez harmonogram Kubernetes, należy wprowadzić kilka modyfikacji w konfiguracji harmonogramu Kubernetes, a klucze

[9] Inna nazwa: dzierżawca, najemca.

dostępu muszą być współdzielone między węzłem sterującym Kubernetes a serwerem weryfikacji hosta AMI TruE. Serwer weryfikacji hosta AMI TruE jest zbudowany z bazy kodu ISecL; pełny opis kroków można znaleźć w punkcie 6.13.3.2 dokumentacji produktu ISecL pod adresem https://01.org/sites/default/files/documentation/intelr secl-dc v1.6 ga productguide 1.pdf

ZAŁĄCZNIK D – WSPARCIE ŚRODKÓW BEZPIECZEŃSTWA

Główne środki bezpieczeństwa zawarte są w publikacji NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*[10] [6]. Katalog środków bezpieczeństwa, które mają wpływ na implementację prototypu bezpieczeństwa platformy kontenerowej to:

- AU-2, Rejestrowanie zdarzeń,
- CA-2, Oceny środków bezpieczeństwa,
- CA-7, Ciągłe monitorowanie,
- CM-2, Konfiguracja zabezpieczenia bazowego,
- CM-3, Zabezpieczenie zmian konfiguracji,
- CM-8, Wykaz komponentów systemu,
- IR-4, Obsługa incydentów,
- SA-9, Zewnętrzne usługi systemowe,
- SC-1, Zasady i procedury [dla rodziny ochrony systemu i komunikacji],
- SC-7, Ochrona granic,
- SC-29, Różnorodność,
- SC-32, Partycjonowanie systemu,
- SC-36, Rozproszone przetwarzanie i magazynowanie,
- SI-2, Korygowanie przepływu,
- SI-3, Ochrona przed złośliwym kodem,
- SI-4, Monitorowanie systemu,
- SI-6, Weryfikacja funkcji zabezpieczeń i prywatności,
- SI-7, Integralność informacji, oprogramowania układowego i oprogramowania.

[10] Patrz: polskojęzyczna publikacja NSC 800-53 wer. 2. Przypis odnosi się do całego dokumentu.

Tabela 7 zawiera listę funkcji zabezpieczeń zapewnianych przez prototyp zaufanego tagu zasobów:

Tabela 7: Funkcje zabezpieczeń zapewnianych przez prototyp zaufanego tagu zasobów

Kategoria zdolności do ochrony	Numer zdolności do ochrony	Nazwa zdolności do ochrony
IC1 — Pomiary	IC1.1	Mierzony rozruch systemu BIOS
	IC1.2	Zabezpieczenie bazowe dla pomiarów BIOS (lista dozwolonych)
	IC1.3	Zdalna atestacja pomiarów rozruchu
	IC1.4	Zdolność do ochrony i wykrywanie konfiguracji
IC2 — Weryfikowanie tagów	IC2.1	Weryfikacja tagów zasobów
IC3 — Egzekwowanie zasad	IC3.1	Aprowizacja obciążenia oparta na zasadach
	IC3.2	Migrowanie obciążenia opartego na zasadach
IC4 — Raportowanie	IC4.1	Obsługa ciągłego monitorowania
	IC4.2	Obsługa raportów na żądanie
	IC4.3	Obsługa powiadomień o zdarzeniach związanych z zaufaniem
IC5 — Korygowanie	IC5.1	Zdalne wyłączenie zaatakowanej platformy
	IC5.2	Aktualizacja zaatakowanego systemu BIOS oprogramowania układowego
	IC5.3	Ponowna instalacja zaatakowanego systemu operacyjnego

Tabela 8 odwzorowuje zdolności do ochrony z Tabeli 7 na środki bezpieczeństwa NIST SP 800-53 z listy znajdującej się na początku tego dodatku.

Tabela 8: Odwzorowanie środków ochrony na środki bezpieczeństwa NSC 800-53

Środki bezpieczeństwa NSC 800-53	**Pomiary**				**Weryfikacja tagów**	**Egzekwowanie polityk**		**Raportowanie**			**Korygowanie**		
	IC1.1	IC1.2	IC1.3	IC1.4	IC2.1	IC3.1	IC3.2	IC4.1	IC4.2	IC4.3	IC5.1	IC5.2	IC5.3
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	X	X	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-2											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				X	X	X

ZAŁĄCZNIK E – MAPOWANIE PODKATEGORII RAM CYBERBEZPIECZEŃSTWA

Niniejszy dodatek przedstawia główne funkcje zabezpieczeń implementacji prototypu zabezpieczeń platformy kontenerowej w odniesieniu do następujących podkategorii z ram cyberbezpieczeństwa [7]:

- DE.CM-4: Wykryto złośliwy kod.
- DE.CM-6: Aktywność zewnętrznych dostawców usług jest monitorowana w celu wykrywania potencjalnych zdarzeń związanych z cyberbezpieczeństwem.
- ID.GV-1: Ustanowiono i ogłoszono zasady cyberbezpieczeństwa organizacji.
- ID.GV-3: Wymogi prawne i ustawowe dotyczące cyberbezpieczeństwa, w tym obowiązki w zakresie prywatności i swobód obywatelskich, są zrozumiałe i zarządzane.
- ID.RA-1: Podatności zasobów są identyfikowane i dokumentowane.
- PR.DS-6: Do weryfikowania integralności oprogramowania, oprogramowania układowego i informacji wykorzystywane są mechanizmy sprawdzania integralności.
- PR.IP-3: Wdrożono procesy zabezpieczania zmian konfiguracji.
- PR.IP-5: Przestrzegane są polityki i przepisy dotyczące fizycznego środowiska operacyjnego dla aktywów organizacyjnych.
- PR.IP-12: Opracowano i wdrożono plan zarządzania podatnościami na zagrożenia.
- PR.PT-1: Zapisy audytu/rejestrowania są określane, dokumentowane, wdrażane i przeglądane zgodnie z zasadami.
- RS.MI-1: Incydenty są kontrolowane.
- RS.MI-2: Incydenty są mitygowane.

Tabela 9 pokazuje mapowanie zdolności do ochrony (przedstawionych w Tabeli 7 załącznika D) na podkategorie ram cyberbezpieczeństwa.

Tabela 9: Mapowanie zdolności do ochrony na podkategorie ram cyberbezpieczeństwa NIST

Podkategoria ram cyberbezpieczeństwa	**Pomiary**				**Weryfikacja tagów**	**Egzekwowanie zasad**		**Raportowanie**			**Korygowanie**		
	IC1.1	IC1.2	IC1.3	IC1.4	IC2.1	IC3.1	IC3.2	IC4.1	IC4.2	IC4.3	IC5.1	IC5.2	IC5.3
DE.CM-4	X							X					
DE.CM-6	X		X			X	X	X	X	X			
ID.GV-1						X	X						
ID.GV-3					X	X	X						
ID.RA-1											X	X	X
PR.DS-6	X	X	X			X	X				X	X	X
PR.IP-3	X		X	X	X								
PR.IP-5					X	X	X						
PR.IP-12											X	X	X
PR.PT-1	X		X					X	X	X			
RS.MI-1											X	X	X
RS.MI-2												X	X

ZAŁĄCZNIK F – AKRONIMY

Wybrane akronimy i skróty użyte w niniejszej publikacji zostały rozwinięte poniżej.

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

Akronim	Terminologia angielska	Terminologia polska
AAS	Authentication and Authorization Service	Usługa uwierzytelniania i autoryzacji
AIK	Attestation Identity Key	Klucz identyfikacji i atestacji
AMI TruE	AMI Trusted Environment	Zaufane środowisko AMI
API	Application Programming Interface	Interfejs programistyczny aplikacji
BIOS	Basic Input/Output System	Podstawowy system wejścia/wyjścia
BMC	Board Management Controller	Kontroler BMC
CA	Certification Authority	Urząd (organ) certyfikacji
CMS	Certificate Management Service	Usługa zarządzania certyfikatami
CNI	Container Network Interface	Interfejs sieciowy kontenera
CoT	Chain of Trust	Łańcuch zaufania
CPU	Central Processing Unit	Procesor
CRD	Custom Resource Definition	Niestandardowa definicja zasobu
CRTM	Core Root of Trust for Measurement	Główny aparat zaufanych pomiarów
GB	Gigabyte	Gigabajt
GHz	Gigahertz	Gigahertz

HTML5	Hypertext Markup Language (version 5)	HTML, hipertekstowy język znaczników (wersja 5)
HVS	Host Verification Service	Usługa weryfikacji hosta
IaaS	Infrastructure as a Service	Infrastruktura jako usługa
Intel TXT	Intel Trusted Execution Technology	Technologia Intel TXT
I/O	Input/Output	Wejście/wyjście
IP	Internet Protocol	Protokół internetowy
IR	Integracy or Internal Report	Sprawozdanie międzyresortowe lub wewnętrzne
IT	Information Technology	Technologia informacyjna
ITL	Information Technology Laboratory	Laboratorium informatyczne
JSON	JavaScript Object Notation	Notacja JSON
KMS	Key Management Service	Usługa zarządzania kluczami
KVM	Keyboard, Video, Mouse	Klawiatura, wideo, mysz
MLE	Measured Launch Environment	Mierzone środowisko uruchomieniowe
NC	Nonce	Nieoczekiwane
NIST	National Institute of Standards and Technology	Narodowy Instytut Standaryzacji i Technologii
NISTIR	National Institute of Standards and Technology Interagency or Internal Report	Integracyjny lub wewnętrzny raport NIST

NUC	Next Unit of Computing	Następna jednostka obliczeniowa
OEM	Original Equipment Manufacturer	Producent oryginalnego sprzętu
System operacyjny	Operating System	System operacyjny
PCR	Platform Configuration Register	Rejestr konfiguracji platformy
REST	Representational State Transfer	Transfer REST
RHEL	Red Hat Enterprise Linux	Linux, wersja Red Hat Enterprise
RTM	Root of Trust for Measurement	Pomiar źródła zaufania
RTR	Root of Trust for Reporting	Raportowanie źródła zaufania
RTS	Root of Trust for Storage	Źródło zaufania dla pamięci masowej
SHA256	Secure Hash Algorithm 256-bit	256-bitowy bezpieczny algorytm haszujący
SML	Stored Measurement Log	Dziennik pomiarów
SMTP	Simple Mail Transfer Protocol	Protokół SMPT, protokół transmisji danych w Internecie
SP	Special Publication	Publikacja specjalna
SRK	Storage Root Key	Klucz główny składowania
SSDP	Simple Service Discovery Protocol	Protokół SSDP, prosty protokół do wykrywania usług

SSH	Secure Shell	Powłoka (rodzina protokołów) SSH
TA	Trust Agent	Agent zaufania
TPM	Trusted Platform Module	Moduł TPM
UEFI	Unified Extensible Firmware Interface	Interfejs UEFI
URL	Uniform Resource Locator	Adres URL
UUID	Universally Unique Identifier	Identyfikator UUID, uniwersalny unikatowy identyfikator
WLS	Workload Service	Usługa obciążenia