



## Rekomendacje Dell Technologies w zakresie konfiguracji urządzeń, oprogramowania i usług w sposób maksymalizujący skuteczność mechanizmów zabezpieczających dla urządzeń serwerowych

### Wprowadzenie

„Najważniejszym zasobem na świecie nie jest już ropa, ale są nim dane”, trudno nie zgodzić się z tą tezą pochodzącą z artykułu z gazety The Economist z maja 2017 roku. Dotyczy to wszystkich organizacji, firm różnych wielkości. Dane stały się najważniejszym zasobem dla wielu organizacji. Ochrona danych i infrastruktury IT, która je obsługuje, to jedno z najważniejszych celów CIO, CISO oraz kierowników IT i dyrektorów centrów danych. Coraz większe wyzwania związane z ochroną infrastruktury IT są pochodną złożoności i ilości złośliwego oprogramowania.

Każdy cyberatak niesie za sobą ryzyko utraty danych, przestoju w pracy i nadszarpnięcia wizerunku firmy. Dlatego od lat globalne wydatki na ochronę przed atakami nieustannie rosną, a w 2021 roku przekroczą zawrotną sumę 1 biliona dolarów. Jednak choć świadomość zewnętrznych i wewnętrznych zagrożeń stale wzrasta, nadal najwięcej uwagi poświęca się tylko zabezpieczeniu systemów operacyjnych i aplikacji. Tymczasem dla bezpieczeństwa infrastruktury nie mniej ważne jest też zabezpieczenie sprzętu i oprogramowania układowego. Infrastruktura serwerów ma kluczowe znaczenie dla bezpieczeństwa centrum danych, ponieważ cyberataki skierowane na oprogramowanie układowe mogą wywoływać trwałe skutki i są trudne do wykrycia.

W miarę jak wzrasta rola serwerów w architekturze centrum danych definiowanej programowo, bezpieczeństwo serwera staje się podstawą ogólnego bezpieczeństwa przedsiębiorstwa. Należy pamiętać, że bezpieczeństwo danych zaczyna się w momencie i w miejscu ich wytworzenia.

### SDL – Security Development Lifecycle

Dostarczenie architektury serwerowej odpornej na ataki i włamania wymaga zapewnienia bezpieczeństwa i szczególnej troski na każdym etapie użytkowania serwera, począwszy od jego produkcji aż do wycofania z użycia. Proces zapewniający taką architekturę nazywa się modelem cyklu utrzymania bezpieczeństwa (Security Development Lifecycle - SDL), w którym cyberbezpieczeństwo stanowi integralną część całego procesu projektowania serwera.

Proces ten obejmuje cały cykl życia serwera, składający się z:

- Opracowania funkcjonalności, projektu, przygotowania prototypu, implementacji, wdrożenia do produkcji, utrzymania, zapewniając cyberbezpieczeństwo na każdym z tych etapów.
- Zastosowania oprogramowania układowego serwera (firmware), które posiada funkcje blokujące i uniemożliwiające wstrzykiwanie złośliwego kodu na każdym etapie cyklu rozwoju produktu. Oprogramowanie układowe już podczas projektowania przechodzi proces modelowania zagrożeń i testy penetracyjne. Na etapie tworzenia oprogramowania układowego stosowane są bezpieczne praktyki kodowania. W przypadku technologii krytycznych, zewnętrzne audyty bezpieczeństwa uzupełniają wewnętrzny proces SDL, aby zapewnić zgodność oprogramowania układowego z najlepszymi praktykami bezpieczeństwa.
- Ciągłych testów i oceny nowych potencjalnych luk w zabezpieczeniach przy użyciu najnowszych narzędzi oceny bezpieczeństwa.
- Szybkiej reakcji na krytyczne podatności i narażenia (CVE), w tym wprowadzenie zaleceń odnośnie środków zaradczych, jeśli jest to uzasadnione.

### Cyberodporna architektura serwerowa

Kluczowe aspekty architektury serwerowej, która zapewnia odporność na cyberataki, wykrywanie cyberataków i przywracanie do bezpiecznego statusu po cyberatakach:

- Skuteczna ochrona przed cyberatakami
- Łańcuch zaufania z weryfikacją autentyczności uruchamianego BIOS, oprogramowania układowego i plików wykonywalnych, porównywanie z kluczem kryptograficznym zaimplementowanym w sprzęcie na etapie produkcji serwera
- Podpisane kryptograficznie aktualizacje oprogramowania układowego
- Blokowanie modyfikacji ustawień systemu (System Lockdown)
- Niezawodne wykrywanie ataków
- Wykrywanie odchyłeń konfiguracji i oprogramowania układowego
- Trwałe rejestrowanie zdarzeń
- Alarmowanie o odchyleniach
- Szybkie odzyskiwanie z minimalizacją wpływu na ciągłość biznesową
- Automatyczne odtworzenie BIOS
- Szybkie odzyskiwanie systemu operacyjnego
- Przywracanie oprogramowania układowego

## Dzisiejsze zagrożenia

Obecnie istnieje wiele wektorów zagrożeń. Poniżej przedstawiamy omówienie wektorów zagrożeń i sposoby przeciwdziałania.

### Warstwy platformy serwerowej

Warstwa bezpieczeństwa	Wektor zagrożenia	Strategia przeciwdziałania
Fizyczny serwer	Fizyczna ingerencja	Zapobieganie włamaniom i wykrywanie fizycznej ingerencji
Firmware i oprogramowanie	Uszkodzenie/kompromitacja firmware, wstrzykiwanie złośliwego oprogramowania	Łańcuch zaufania z weryfikacją autentyczności uruchamianego oprogramowania, Intel Boot Guard, AMD Secure, Kryptograficznie podpisany i zwalidowany firmware
Oprogramowanie układowe	Oprogramowanie	Uaktualnianie oprogramowania zgodnie z zaleceniami
Funkcje zaufania poświadczeń	Falszowanie tożsamości	TPM, TXT, łańcuch zaufania
System zarządzania	Modyfikacja ustawień i aktualizacji, nieautoryzowane ataki typu open-port	Zabezpieczenia w interfejsie zarządzającym serwerem (w tym ze zdalnym dostępem)
System zarządzania	Naruszenie danych	SED (Self Encrypting Drives) - FIPS lub Opal / TCG Dyski typu ISE (Instant Secure Erase) Bezpieczne Zarządzanie Kluczami Bezpieczne Uwierzytelnianie Użytkowników
Dane	Sfałszowane komponenty Zagrożenia złośliwym oprogramowaniem	Certyfikat ISO9001 dla wszystkich globalnych miejsc produkcji serwerów. Środki bezpieczeństwa wdrożone w ramach procesu bezpiecznego rozwoju cyklu życia (SDL)
Bezpieczeństwo łańcucha dostaw	Bezpieczeństwo fizyczne w zakładach produkcyjnych Kradzież i naruszenia bezpieczeństwa podczas logistyki	Zgodność z Wymaganiami Bezpieczeństwa Przewozu TAPA (Technology Asset Protection Association) <a href="https://www.iso.org.pl/uslugi-zarzadzania/wdrazanie-systemow/inne-systemy-i-standardy/tapa/">https://www.iso.org.pl/uslugi-zarzadzania/wdrazanie-systemow/inne-systemy-i-standardy/tapa/</a> Partnerstwo celno-handlowe przeciwko terroryzmowi (C-TPAT)

## Ochrona

Funkcja „ochrony” jest kluczowym elementem wytycznych dotyczących cyberbezpieczeństwa organizacji NIST (Amerykańskiego Narodowy Instytut Standaryzacji i Technologii) i zasad ochrony przed cyberatakami.

Te wytyczne składają się z kilku kategorii, w tym kontroli dostępu, bezpieczeństwa danych, utrzymania i przeciwdziałaniu. Kluczową filozofią leżącą u podstaw tych wytycznych i zgodności z nimi

jest to, że zasoby infrastruktury muszą zapewniać pewną ochronę przed nieautoryzowanym dostępem do zasobów i danych w ramach kompleksowo bezpiecznego środowiska instalacyjnego i obliczeniowego. Obejmuje to ochronę przed nieautoryzowanymi modyfikacjami kluczowych komponentów, takich jak BIOS i oprogramowanie układowe. Platforma serwerów proponowana przez Dell EMC spełnia aktualne zalecenia NIST SP 800-193 („Wytyczne dotyczące odporności oprogramowania układowego platformy / Draft Platform Firmware Resiliency Guidelines”).

Odporna na cyberataki architektura serwerowa zapewnia wysoki poziom ochrony platformy obliczeniowej, który obejmuje następujące możliwości:

- Zweryfikowane kryptograficzne bezpieczne uruchamianie
- Zabezpieczenie Dostępu dla Użytkownika
- Podpisane kryptograficznie aktualizacje oprogramowania układowego
- Szyfrowane przechowywanie danych
- Bezpieczeństwo fizyczne
- Integralność i bezpieczeństwo łańcucha dostaw

### Zweryfikowane kryptograficzne bezpieczne uruchamianie

Jednym z najbardziej krytycznych aspektów bezpieczeństwa serwera jest zapewnienie weryfikacji bezpiecznego procesu rozruchu serwera. Ten proces zapewnia łańcuch zaufania dla wszystkich kolejnych operacji, takich jak uruchamianie systemu operacyjnego lub aktualizowanie oprogramowania układowego. Serwery PowerEdge od kilku generacji stosują zabezpieczenia oparte na układach scalonych dla takich funkcji jak iDRAC Credential Vault, zaszyfrowana bezpieczna pamięć w iDRAC do przechowywania wrażliwych danych. Proces rozruchu jest weryfikowany przy użyciu opartego na implementacji w platformę sprzętową łańcucha zaufania, aby spełnić zalecenia NIST SP 800-147B („Wytyczne ochrony BIOS-u dla serwerów”) i NIST SP 800-155 („Wytyczne pomiaru integralności BIOS-u”).

### Łańcuch zaufania

Obecnie produkowane serwery PowerEdge (zarówno te oparte na procesorach Intel jak i AMD) wykorzystują niezmienny, zaimplementowany w sprzęt Root-of-Trust (łańcuch zaufania), aby kryptograficznie poświadczyć integralność oprogramowania BIOS i iDRAC. Podstawa zaufania oparta jest na jednorazowych programowalnych jednokierunkowych kluczach publicznych, które zapewniają ochronę przed manipulacją złośliwym oprogramowaniem. Proces rozruchu systemu BIOS wykorzystuje technologię Intel Boot Guard lub technologię AMD Root-of-Trust, która weryfikuje, czy podpis cyfrowy kryptograficznego skrótu (hash) obrazu rozruchowego jest zgodny z podpisem przechowywanym fabrycznie w układzie scalonym serwera Dell EMC. Niepowodzenie weryfikacji powoduje zamknięcie serwera oraz stosowny komunikat dla użytkownika w dzienniku kontrolera zarządzania oraz może zostać zainicjowany przez użytkownika proces przywracania systemu BIOS. Jeśli Boot Guard sprawdzi się pomyślnie, pozostałe moduły BIOS są sprawdzane przy użyciu procedury łańcucha zaufania, dopóki sterowanie nie zostanie przekazane do systemu operacyjnego lub hiperwizora.

## Wsparcie dla UEFI Secure Boot

Serwery PowerEdge wykorzystują standard branżowy - UEFI Secure Boot, który sprawdza podpisy kryptograficzne sterowników UEFI i innego kodu załadowanego przed uruchomieniem systemu operacyjnego. Producenci systemów komputerowych, dostawcy kart rozszerzeń i dostawcy systemów operacyjnych współpracują w zakresie tej specyfikacji, aby promować ich bezkolizyjną współpracę.

Po włączeniu UEFI Secure Boot, funkcjonalność ta zapobiega ładowaniu niepodpisanych (tzn. niezauważalnych) sterowników urządzeń UEFI, wyświetla komunikat o błędzie i nie pozwala serwerowi na działanie. Ponadto serwery PowerEdge oferują klientom wyjątkową elastyczność korzystania z niestandardowego certyfikatu modułu ładującego, który nie jest podpisany przez Microsoft. Jest to przede wszystkim funkcja dla administratorów środowisk Linux, którzy chcą podpisać własne programy ładujące system operacyjny. Certyfikaty niestandardowe można przesyłać za pośrednictwem preferowanego interfejsu API karty zdalnego zarządzania (iDRAC), w celu uwierzytelnienia programu ładującego system operacyjny klienta.

## Obsługa TPM

Serwery PowerEdge obsługują trzy wersje układu szyfrującego TPM:

- TPM 1.2 FIPS + Common Criteria + certyfikat TCG (Nuvoton)
- TPM 2.0 FIPS + Common Criteria + certyfikat TCG (Nuvoton)
- TPM 2.0 Chiny (NationZ)

TPM może być wykorzystywany do wykonywania funkcji kryptograficznych z użyciem klucza publicznego, obliczania funkcji skrótu (hash), generowania, zarządzania i bezpiecznego przechowywania kluczy oraz do ich poświadczania. Obsługiwana jest również funkcja Intel TXT (Trusted Execution Technology) oraz funkcja Microsoft Platform Assurance w systemie Windows Server 2016/2019. Za pomocą modułu TPM można włączyć funkcję szyfrowania dysku twardego BitLocker w systemie Windows Server 2012/2016/2019. TPM jest kompatybilny ze zdalnym rozwiązaniem atestacji HyTrust CloudControl.

Rozwiązania do zdalnej atestacji mogą wykorzystywać moduł TPM do wykonywania pomiarów w czasie uruchamiania sprzętu serwera, hiperwizora, systemu BIOS i systemu operacyjnego oraz porównywania ich w sposób bezpieczny pod względem kryptograficznym z danymi bazowymi przechowywanymi w module TPM. Jeśli nie są identyczne, to bezpieczeństwo serwera mogło zostać naruszone, a administratorzy systemu powinni wyłączyć i odłączyć serwer lokalnie lub zdalnie.

TPM jest włączony poprzez BIOS. Jest oferowany jako rozwiązanie modułu plug-in na płycie głównej.

## Certyfikaty bezpieczeństwa

Dell EMC posiada certyfikaty dla takich jak NIST FIPS 140-2 i Common Criteria EAL-4.

Są one ważne dla umów zgodnych z amerykańską DoD i innych powiązanych rządowych.

Wykaz certyfikatów dla serwerów PowerEdge:

- Platforma serwerowa: Common Criteria EAL4 + z certyfikatem RHEL
- Certyfikacja iDRAC i CMC FIPS 140-2 poziom 1
- Certyfikacja FIPS 140-2 i Common Criteria dla TPM 1.2 i 2.0
- Certyfikat FIPS 140-2 dla dysków SED

## Bezpieczeństwo dostępu użytkownika

Zapewnienie właściwego uwierzytelnienia i autoryzacji jest kluczowym wymogiem każdej nowoczesnej polityki kontroli dostępu. Podstawowymi interfejsami dostępu do serwerów PowerEdge są interfejsy API, CLI lub GUI wbudowanego kontrolera iDRAC. Preferowane interfejsy API i CLI do automatyzacji zarządzania serwerami to:

- iDRAC Restful API z Redfish
- iDRAC WS-MAN API
- RACADM CLI
- SSH CLI

Każdy z nich zapewnia to, że stosowne dane uwierzytelniające, takie jak nazwa użytkownika i hasło, przesyłane są za pomocą szyfrowanego połączenia, takiego jak HTTPS. SSH uwierzytelnia użytkownika za pomocą dopasowanego zestawu kluczy kryptograficznych (tym samym eliminuje potrzebę wprowadzania mniej bezpiecznych haseł). Starsze protokoły, takie jak IPMI, są obsługiwane, ale nie są zalecane w przypadku nowych wdrożeń ze względu na problemy z ich bezpieczeństwem odkryte w ostatnich latach. Zalecamy przejście z IPMI na iDRAC Restful API z protokołem Redfish.

Certyfikaty TLS / SSL można przysyłać do kontrolera iDRAC (karty zdalnego zarządzania) w celu uwierzytelnienia sesji przeglądarki internetowej. Istnieją 3 opcje związane z certyfikatami:

- Samopodpisany certyfikat TLS / SSL Dell EMC – certyfikat jest generowany automatycznie i samopodpisany przez iDRAC. Zaleta: Nie ma potrzeby utrzymywania osobnego urzędu certyfikacji (standard X.509 / IETF PKIX)
- Niestandardowy podpisany certyfikat TLS / SSL – certyfikat jest generowany automatycznie i samopodpisany za pomocą klucza prywatnego, który został już przesłany do iDRAC.
- Certyfikat TLS / SSL podpisany przez CA – Żądanie podpisania certyfikatu (CSR) jest generowane i przesyłane do Twojego wewnętrznego urzędu certyfikacji lub przez zewnętrzny urząd certyfikacji, taki jak VeriSign, Thawte i Go Daddy, w celu podpisania. Zalety: Może korzystać z komercyjnego urzędu certyfikacji (standardy PKIX X.509 / IETF). Jeden zaufany urząd certyfikacji dla wszystkich kontrolerów iDRAC.

Karta zdalnego zarządzania iDRAC9 umożliwia integrację z Active Directory lub LDAP poprzez wykorzystanie istniejących schematów uwierzytelniania i autoryzacji użytkowników, które zapewniają bezpieczny dostęp do serwerów PowerEdge. iDRAC9 obsługuje także kontrolę dostępu opartą na rolach (RBAC), aby zapewnić odpowiedni poziom dostępu - administrator, operator lub obserwator – zależny od funkcji użytkownika w centrum danych. Zdecydowanie zaleca się stosowanie

RBAC w taki sposób, aby nie nadawać najwyższego poziomu uprawnień (tj. Administratora) wszystkim użytkownikom.

Uwierzytelnianie dwuskładnikowe (2FA) jest coraz częściej stosowane ze względu na niewystarczające bezpieczeństwo uwierzytelniania jednoskładnikowego oparte na nazwę użytkownika i hasło. iDRAC9 pozwala na użycie inteligentnych kart zdalnego dostępu do GUI. Dwa elementy autoryzacji to fizyczna obecność karty inteligentnej oraz jej PIN.

iDRAC9 zapewnia również dodatkowe sposoby ochrony przed nieautoryzowanym dostępem, w tym blokowanie i filtrowanie adresów IP. Kontroler dynamicznie bada, kiedy występują błędy logowania z określonego adresu IP i blokuje (lub uniemożliwia) danym adresom/adresowi logowanie się do kontrolera iDRAC9 przez określony czas. Filtrowanie IP ogranicza zakres adresów IP klientów uzyskujących dostęp do kontrolera iDRAC. Porównuje adres IP przychodzącego logowania z określonym zakresem i umożliwia dostęp do kontrolera iDRAC tylko ze stacji zarządzania, której źródłowy adres IP znajduje się w tym zakresie. Wszystkie pozostałe żądania logowania są odrzucane.

### Hasło wygenerowane fabrycznie

Domyślnie wszystkie obecnie oferowane serwery PowerEdge są dostarczane z unikatowym, fabrycznie wygenerowanym hasłem dostępu do kontrolera iDRAC, aby zapewnić dodatkowe bezpieczeństwo serwera. Dla ułatwienia hasło jest znajduje się na wysuwanym znaczniku informacyjnym znajdującym się z przodu obudowy, obok etykiety serwera. Użytkownicy, którzy wybiorą tę opcję, muszą użyć go do pierwszego logowania do kontrolera iDRAC. Ze względów bezpieczeństwa Dell EMC zdecydowanie zaleca zmianę hasła domyślnego.

### Blokowanie modyfikacji ustawień systemu (System Lockdown)

iDRAC9 oferuje nową funkcję, która uniemożliwia modyfikację konfiguracji sprzętu i oprogramowania wewnętrznego serwera lub serwerów. Ten tryb można włączyć za pomocą GUI, interfejsów CLI, takich jak RACADM lub jako część profilu konfiguracji serwera. Użytkownicy z uprawnieniami administracyjnymi mogą ustawić tryb blokady systemu, który uniemożliwia użytkownikom z mniejszymi uprawnieniami wprowadzanie zmian na serwerze. Tę funkcję może włączyć / wyłączyć administrator IT. Wszelkie zmiany wprowadzone po wyłączeniu blokady systemu są śledzone w dzienniku kontrolera zarządzającego. Włączając tryb blokady, można zapobiec odchyleniom od zdefiniowanej przez administratora konfiguracji serwera podczas korzystania z narzędzi i agentów Dell EMC, a także zabezpieczyć się przed złośliwymi atakami na osadzone oprogramowanie wewnętrzne podczas korzystania z pakietów aktualizacji Dell EMC.

### Izolacja Domen

Obecnie oferowane serwery PowerEdge z procesorami Intel zapewniają dodatkowe bezpieczeństwo dzięki Domain Isolation (Izolacji Domen). Jest to ważna funkcja w środowiskach hostingowych obsługujących wielu dzierżawców (tenantów). W celu zabezpieczenia konfiguracji sprzętowej serwera, firma hostingowa może zablokować wszelkie rekonfiguracje ustawień sprzętowych przez tenanta. Jest to opcja konfiguracji zapewniająca brak dostępu aplikacjom do zarządzania z poziomu OS hosta do procesora karty iDRAC jak również do funkcji chipsetu takich jak Management Engine (ME) lub Innovation Engine (IE).

## Podpisane kryptograficznie aktualizacje oprogramowania układowego

Serwery PowerEdge od wielu lat używają podpisów cyfrowych przy aktualizacjach oprogramowania, aby zapewnić, że tylko autentyczne oprogramowanie układowe może działać na określonej platformie serwerowej. Podpisujemy kryptograficznie wszystkie nasze pakiety oprogramowania układowego za pomocą hash'a SHA-256 z 2048-bitowym szyfrowaniem RSA. Ta metoda ma zastosowanie dla wszystkich kluczowych komponentów serwera, w tym oprogramowania wewnętrznego dla iDRAC, BIOS, PERC, adapterów wejścia/wyjścia i wbudowanych kart sieciowych, zasilaczy, dysków, CPLD i kontrolerów płyty głównej. iDRAC skanuje aktualizacje oprogramowania układowego i porównuje ich sygnatury za pomocą wbudowanego w sprzęt łańcucha zaufania; każdy pakiet oprogramowania układowego, którego weryfikacja nie powiedzie się, jest przerywany, a komunikat o błędzie jest rejestrowany w dzienniku karty zarządzającej, aby ostrzec administratorów IT.

Uwierzytelnianie dla firmware wbudowane jest również w elementach firm dostarczających je do serwerów Dell EMC. Zapewniają weryfikację podpisu oprogramowania przy użyciu własnych mechanizmów root-of-trust (łańcucha zaufania). Zapobiega to możliwe-mu wykorzystaniu narzędzia aktualizacji innej firmy do załadowania złośliwego oprogramowania układowego, na przykład do karty sieciowej lub dysku (omijając korzystanie z podpisanych pakietów aktualizacji Dell EMC). Wiele zewnętrznych urządzeń PCIe i pamięci masowych dostarczanych z serwerami PowerEdge używa sprzętowego root-of-trust do sprawdzania poprawności odpowiednich aktualizacji oprogramowania układowego.

W przypadku podejrzenia, że oprogramowanie układowe w dowolnym urządzeniu jest niebezpieczne lub zmanipulowane, administratorzy IT mogą przywrócić obrazy oprogramowania układowego do poprzedniej zaufanej wersji przechowywanej w iDRAC. Na serwerze przechowujemy 2 wersje oprogramowania układowego urządzenia - istniejącą wersję produkcyjną („N”) i wcześniejszą zaufaną wersję („N-1”).

## iDRAC Credential Vault

Moduł zarządzający iDRAC posiada wbudowaną bezpieczną pamięć, która chroni różne wrażliwe dane, takie jak poświadczenia użytkownika iDRAC oraz klucze prywatne dla samopodpisanych certyfikatów SSL. Jest to kolejny przykład bezpieczeństwa wbudowanego w sprzęt, pamięć ta jest szyfrowana unikatowym, niezmiennym kluczem głównym, który jest programowany w każdym układzie iDRAC w momencie produkcji. Chroni to przed fizycznymi atakami, w których atakujący demontuje układ, próbując uzyskać dostęp do danych.

## Bezpieczeństwo sprzętu

Bezpieczeństwo sprzętu jest integralną częścią każdego kompleksowego rozwiązania. Niektórzy klienci chcą ograniczyć dostęp do portów wejścia/wyjścia, takich jak USB. Obudowa serwerowa nie musi być zazwyczaj otwierana po wprowadzeniu do eksploatacji. We wszystkich przypadkach klienci przynajmniej chcieliby śledzić i rejestrować takie działania. Ogólnym celem jest zniechęcenie i ograniczenie wszelkich fizycznych ingerencji.



## Alarm otwarcia obudowy

Serwery PowerEdge zapewniają wykrywanie i rejestrowanie włamań sprzętowych. Wykrywanie działa nawet kiedy nie jest dostępne zasilanie. Czujniki obudowy serwera wykrywają, kiedy ktoś otwiera lub manipuluje obudową, m.in. podczas transportu. Serwery, które zostały otwarte podczas transportu, generują wpis w dzienniku karty zarządzającej iDRAC po dostarczeniu zasilania.

## Dynamiczne włączanie i wyłączenie portów USB

Aby zwiększyć bezpieczeństwo, zalecamy całkowicie wyłączyć porty USB. Ewentualnie można wyłączyć tylko porty USB z przodu serwera. Porty USB można wyłączyć do użytku produkcyjnego, a następnie tymczasowo włączyć bez konieczności restartowania serwera, aby udzielić dostępu do debugowania systemu.

## iDRAC Direct

iDRAC Direct to specjalny port USB, który jest podłączony do procesora serwisowego iDRAC w celu debugowania i zarządzania serwerem. Bezpieczny serwer powinien posiadać port zarządzający odseparowany od portów dostępnych dla systemu operacyjnego. iDRAC Direct pozwala administratorowi podłączyć standardowy kabel USB Micro-AB do tego portu, a drugi koniec (typ A) do laptopa. Poprzez przeglądarkę internetową może uzyskać dostęp do interfejsu GUI kontrolera iDRAC w celu szczegółowego debugowania i zarządzania serwerem. Jeśli zainstalowana jest licencja iDRAC Enterprise, użytkownik może nawet uzyskać dostęp do pulpitu systemu operacyjnego za pośrednictwem funkcji wirtualnej konsoli iDRAC.

Ponieważ do logowania używane są standardowe dane uwierzytelniających iDRAC, iDRAC Direct działa jako bezpieczny moduł diagnostyczny z dodatkową zaletą rozbudowanego zarządzania sprzętem. Opcja ta może to być atrakcyjna w przypadku zabezpieczenia fizycznego dostępu do serwera w zdalnych lokalizacjach (w tym przypadku porty USB hosta i wyjścia VGA można wyłączyć).

## Integralność i bezpieczeństwo łańcucha dostaw

Integralność łańcucha dostaw koncentruje się na dwóch kluczowych wyzwaniach:

- Utrzymanie integralności sprzętowej: upewnienie się, że przed wysyłką produktu do klientów nie modyfikuje się produktu ani nie wprowadza niebezpiecznych komponentów.
- Utrzymanie integralności oprogramowania: zapewnienie, że żadne złośliwe oprogramowanie nie zostanie wbudowane do oprogramowania układowego lub sterowników urządzeń przed wysłaniem produktu do klientów, a także zapobieganie lukom w zabezpieczeniach związanych z kodowaniem oprogramowania.

Dell EMC definiuje bezpieczeństwo łańcucha dostaw jako praktykę stosowania środków kontroli w celu zapobiegania i wykrywania potencjalnych zagrożeń, które chronią aktywa fizyczne, komponenty, informacje, własność intelektualną i ludzi. Te środki bezpieczeństwa pomagają również zapewnić bezpieczeństwo i integralność łańcucha dostaw, zmniejszając możliwości złośliwego lub nieintencjonalnego wprowadzania złośliwego oprogramowania i niebezpiecznych komponentów do łańcucha dostaw.

## Integralność sprzętu i oprogramowania

Dell EMC koncentruje się również na procesach kontroli jakości, aby zminimalizować możliwość infiltracji łańcucha dostaw przez niebezpieczne komponenty. Dell EMC wprowadził kontrolę dostawców, procesów produkcyjnych i zarządzania poprzez audyty i testy. Po wybraniu dostawcy weryfikuje, czy wszystkie materiały użyte na kolejnych etapach produkcji pochodzą z listy zatwierdzonych dostawców i czy są zgodne z listą materiałów. Kontrole materiałów podczas produkcji pomagają zidentyfikować komponenty, które są źle oznaczone, odbiegają od parametrów wydajności lub zawierają nieprawidłowy identyfikator elektroniczny.

Części są zamawiane bezpośrednio od oryginalnego producenta projektu (ODM) lub oryginalnego producenta komponentów (OCM). Kontrola materiałowa, która ma miejsce podczas procesu produkcji, stwarza wiele możliwości identyfikacji niebezpiecznych z punktu widzenia cyberbezpieczeństwa lub uszkodzonych komponentów, które mogłyby wejść do łańcucha dostaw.

Ponadto Dell EMC utrzymuje certyfikat ISO 9001 dla wszystkich globalnych zakładów produkcyjnych. Ścisłe przestrzeganie tych procesów i kontroli pomaga zminimalizować ryzyko implementacji niebezpiecznych komponentów w produktach Dell EMC lub wstrzyknięcia złośliwego oprogramowania do oprogramowania układowego lub sterowników urządzeń. Środki te są wdrażane w ramach procesu Software Development Lifecycle (SDL).

## Bezpieczeństwo fizyczne

Dell EMC ma wiele długoletnich praktyk, które ustanawiają i utrzymują bezpieczeństwo w zakładach produkcyjnych i sieciach logistycznych. Wymagamy od fabryk, w których budowane są produkty Dell EMC, aby spełniały określone wymagania bezpieczeństwa obiektu Transported Asset Protection Association (TAPA), w tym stosowanie monitorowanych kamer z obwodem zamkniętym w kluczowych obszarach, kontroli dostępu oraz stale chronionych wejść i wyjść. Wprowadzono również środki w celu ochrony produktów przed kradzieżą i manipulacją podczas transportu w ramach wiodącego w branży programu logistycznego. Centrum dowodzenia monitoruje wybrane przesyłki przychodzące i wychodzące na całym świecie, aby upewnić się, że przesyłki docierają z jednego miejsca do drugiego bez zakłóceń.

Dell EMC bierze również aktywny udział w szeregu dobrowolnych programów i inicjatyw dotyczących bezpieczeństwa łańcucha dostaw. Jedną z takich inicjatyw jest Partnerstwo Celno-Handlowe Przeciwko Terroryzmowi (C-TPAT), wprowadzone przez rząd Stanów Zjednoczonych po 11 września w celu zmniejszenia potencjału terroryzmu, poprzez wzmocnienie środków bezpieczeństwa granic i łańcucha dostaw. W ramach tej inicjatywy amerykańska agencja celna i graniczna prosi członków uczestniczących w tym partnerstwie o zapewnienie integralności praktyk bezpieczeństwa oraz o przekazanie wytycznych dotyczących bezpieczeństwa swoim partnerom biznesowym w łańcuchu dostaw. Dell EMC jest aktywnym uczestnikiem od 2002 roku i utrzymuje najwyższy status członkostwa.

## Kompleksowe monitorowanie za pomocą kontrolera iDRAC

Zamiast polegać na agencie systemu zarządzania i komunikacji z zarządzanymi zasobami na serwerze, zalecamy stosowanie karty zarządzającej iDRAC, która stosuje bezpośrednią ścieżkę out-of-band do każdego urządzenia. Dell EMC wykorzystuje standardowe protokoły branżowe, takie jak MCTP, NC-SI i NVMe-MI do komunikacji z urządzeniami peryferyjnymi, takimi jak kontrolery RAID PERC, karty

sieciowe Ethernet, karty Fibre Channel HBA, SAS HBA i dyski NVMe. Ta architektura jest wynikiem wieloletniej współpracy z wiodącymi w branży dostawcami w celu zapewnienia zarządzania komponentami sprzętowymi bez udziału agenta w naszych serwerach PowerEdge. Operacje konfiguracji i aktualizacji oprogramowania układu wykorzystują również zaawansowane funkcje UEFI i HII obsługiwane przez Dell EMC i naszych partnerów.

Dzięki tej możliwości iDRAC może monitorować system w przypadku zmian konfiguracji, ingerencji fizycznych (takich jak otwarcie obudowy) oraz niestabilnej pracy serwera. Zdarzenia konfiguracji są powiązane bezpośrednio z tożsamością użytkownika, który zainicjował zmianę, niezależnie od tego, czy pochodzi od użytkownika GUI, użytkownika interfejsu API, czy użytkownika konsoli.

## Dziennik cyklu życia

Dziennik cyklu życia to zbiór zdarzeń, które występują na serwerze przez czas jego eksploatacji. Dziennik cyklu życia zawiera opis zdarzeń ze znacznikami czasu, istotnością, identyfikatorem użytkownika lub źródłem, zalecanymi działaniami i innymi informacjami technicznymi, które mogą być bardzo przydatne do celów śledzenia lub alarmowania. Poniżej przedstawiono różne rodzaje informacji zapisanych w Dzienniku cyklu życia (LCL):

- Zmiany konfiguracji elementów sprzętowych systemu
- Zmiany konfiguracji kontrolerów iDRAC, BIOS, NIC i RAID
- Dzienniki wszystkich operacji zdalnych
- Historia aktualizacji oprogramowania układowego na podstawie urządzenia, wersji i daty
- Informacje o wymienianych częściach
- Informacje o uszkodzonych częściach
- Identyfikatory zdarzeń i komunikatów o błędach
- Zdarzenia związane z zasilaniem
- Błędy POST
- Zdarzenia logowania użytkownika
- Zdarzenia zmiany stanu czujników

## Alerty

Rekomendujemy kartę iDRAC, która zapewnia możliwość konfigurowania różnych alertów o zdarzeniach, a także działań, które należy wykonać, gdy wystąpi określone zdarzenie w Dzienniku Cyklu Życia. Po wygenerowaniu zdarzenia jest ono przekazywane do określonych miejsc docelowych przy użyciu wybranych mechanizmów dla typu alertu. Można włączyć lub wyłączyć alerty za pośrednictwem interfejsu internetowego iDRAC, RACADM lub narzędzia do ustawień iDRAC.

iDRAC obsługuje różne typy alertów, takie jak:

- Powiadomienie e-mail lub IPMI
- SNMP trap
- Logi systemu operacyjnego i logi zdalne

- Zdarzenia Redfish
- Zdarzenia WS

Alerty można również podzielić na kategorie według oceny - Krytyczne, Ostrzeżenia lub Informacyjne.

Do alertów można zastosować wybrane filtry:

- Kondycja systemu – np. temperatura, napięcie lub błąd urządzenia
- Kondycja pamięci – np. błędy kontrolera, błędy dysku fizycznego lub wirtualnego
- Zmiany konfiguracji – np. zmiana konfiguracji RAID, usunięcie karty PCIe
- Dzienniki kontroli – np. błąd uwierzytelnienia hasła
- Oprogramowanie układowe / sterownik – np. aktualizacja lub obniżenie wersji oprogramowania. Administrator IT może skonfigurować różne akcje dla tych alertów - np. Uruchom ponownie, Wyłącz zasilanie lub Brak akcji.

### Wykrywanie odchylenia konfiguracji i oprogramowania układowego

Organizacje powinny zmniejszać podatności platformy obliczeniowej na ataki złośliwego oprogramowania poprzez narzucenie standaryzacji w obrębie konfiguracji i ustawień, a także przyjmując zasadę „zero tolerancji” dla wszelkich zmian. Zalecamy stosowanie konsoli zarządzającej Dell EMC OpenManage Enterprise & Modular pozwalającej zdefiniować własną konfigurację bazową serwera, a następnie monitorować odchylenie serwerów od tego wzorca. Profil bazowy może być budowany w oparciu o różne kryteria, aby zapewnić środowisku produkcyjnemu bezpieczeństwo i wydajność.

OpenManage Enterprise może zgłaszać wszelkie odchylenia od wzorca i opcjonalnie naprawiać to odchylenie za pomocą mechanizmów out-of-band wbudowanych w kartę zdalnego zarządzania iDRAC. Zmiany mogą wystąpić w kolejnych oknach konserwacji, podczas ponownego uruchamiania serwerów, aby ponownie zapewnić zgodność środowiska produkcyjnego ze wzorcem. Ten proces umożliwia wdrożenie zmian konfiguracji do produkcji bez żadnych przestoju, tylko w godzinach przeznaczonych do konserwacji. Zwiększa to dostępność serwera bez uszczerbku dla jego użyteczności i bezpieczeństwa.

### Odzyskiwanie działania systemu

Rozwiązania serwerowe muszą obsługiwać odzyskiwanie do znanego, spójnego stanu w odpowiedzi na różne zdarzenia:

- Nowo odkryte luki w zabezpieczeniach
- Złośliwe ataki i sabotaż danych
- Uszkodzenie oprogramowania wewnętrznego z powodu awarii pamięci lub niewłaściwych procedur aktualizacji

- Wymiana komponentów serwera
- Wycofanie lub zmiana przeznaczenia serwera

Poniżej szczegółowo omawiamy, jak reagujemy na nowe luki w zabezpieczeniach i inne problemy związane z cyberatakami na platformę sprzętową oraz jak w razie potrzeby przywracamy serwer do stanu pierwotnego.

### Szybka reakcja na nowe luki w zabezpieczeniach

Podatności typu CVE to nowo odkryte wektory ataku, które zagrażają oprogramowaniu i produktom. Szybkie reakcje na CVE są kluczowe dla większości firm, aby mogły właściwie ocenić swoją sytuację i podjąć odpowiednie działania. CVE można wydać w odpowiedzi na nowe luki zidentyfikowane w wielu elementach, w tym:

- Otwarty kod źródłowy, taki jak OpenSSL
- Przeglądarki internetowe i inne oprogramowanie zapewniające dostęp do Internetu
- Sprzęt i oprogramowanie układowe dostawcy
- Systemy operacyjne i hiperwizory

Dell EMC natychmiast reaguje na nowe CVE na serwerach PowerEdge i dostarcza aktualne informacje, w tym:

- Których produktów dotyczy problem
- Jakie kroki zaradcze można zastosować
- W razie potrzeby, kiedy będą dostępne aktualizacje w celu rozwiązania problemu CVE.

### Odzyskiwanie BIOS i Systemu Operacyjnego

Dell rekomenduje system umożliwiający dwa rodzaje powrotu do pożądanego stanu: odzyskiwanie systemu BIOS i odzyskiwanie systemu operacyjnego. W obu przypadkach specjalny obszar pamięci jest ukryty przed oprogramowaniem wykonawczym (BIOS, system operacyjny, oprogramowanie układowe urządzenia itp.). Te obszary zawierają pierwotne obrazy, które można wykorzystać jako alternatywę dla uszkodzonego oprogramowania podstawowego.

Rekomendujemy używanie Rapid OS Recovery umożliwiający szybkie odzyskanie systemu z obrazu systemu. Rekomendujemy wewnętrzne karty SD jako nośniki odzyskiwania. To urządzenie może być widoczne na liście rozruchowej i w systemie operacyjnym w celu instalacji systemu. Następnie można je wyłączyć i ukryć na liście rozruchowej i w systemie operacyjnym. W stanie ukrytym system BIOS wyłącza urządzenie, aby system operacyjny nie mógł uzyskać do niego dostępu. W przypadku uszkodzenia obrazu systemu operacyjnego można włączyć urządzenie odzyskiwania w celu rozruchu. Dostęp do tych ustawień można uzyskać poprzez BIOS lub interfejs iDRAC.

W skrajnych przypadkach, jeśli BIOS jest uszkodzony (z powodu złośliwego ataku, utraty zasilania podczas procesu aktualizacji lub innego nieprzewidzianego zdarzenia), ważne jest, aby zapewnić sposób na przywrócenie BIOS-u do jego pierwotnego stanu. Obraz kopii zapasowej BIOS jest przechowywany w iDRAC, więc w razie potrzeby można go użyć do odzyskania obrazu BIOS. Karta zdalnego zarządzania iDRAC steruje procesem przywrócenia.

- Automatyczne przywracanie systemu BIOS jest inicjowane przez sam system BIOS.
- Użytkownicy BIOS mogą inicjować odzyskiwanie systemu BIOS na żądanie, za pomocą komendy RACADM CLI.

### Przywracanie oprogramowania układowego

Zalecamy regularne aktualizowanie oprogramowania układowego, aby zapewnić najnowszą funkcjonalność i aktualizacje zabezpieczeń. Jednak w przypadku wystąpienia problemów po aktualizacji może być konieczne wycofanie aktualizacji lub zainstalowanie wcześniejszej wersji. Jeśli przywrócisz poprzednią wersję, zostanie ona również zweryfikowana pod kątem jej podpisu.

Przywracanie oprogramowania układowego z istniejącej wersji produkcyjnej „N” do poprzedniej wersji „N-1” jest obecnie obsługiwane dla następujących obrazów oprogramowania układowego:

- BIOS
- iDRAC z Lifecycle Controller
- Karty sieciowe (NIC)
- Kontroler RAID (PERC)
- Zasilacz (PSU)
- Płyta główna

Musi istnieć możliwość przywrócenia oprogramowania do poprzednio zainstalowanej wersji („N-1”), korzystając z jednej z następujących metod:

- Interfejs web iDRAC
- Interfejs web CMC
- RACADM CLI - iDRAC i CMC
- Lifecycle Controller - GUI
- Lifecycle Controller-Remote Services

Można przywrócić oprogramowanie wewnętrzne dla kontrolera iDRAC lub dowolnego urządzenia obsługiwane przez Lifecycle Controller, nawet jeśli aktualizacja była wcześniej przeprowadzana przy użyciu innego interfejsu. Jeśli oprogramowanie wewnętrzne zostało zaktualizowane przy użyciu interfejsu GUI Lifecycle Controller, można przywrócić oprogramowanie wewnętrzne za pomocą interfejsu web iDRAC. Możesz wycofać zmianę oprogramowania dla wielu urządzeń wraz z pojedynczym restartem systemu.

Na serwerach PowerEdge, które mają oprogramowanie wewnętrzne kontrolera iDRAC i Lifecycle Controller, wycofanie zmiany oprogramowania wewnętrznego iDRAC powoduje również wycofanie zmiany oprogramowania wewnętrznego kontrolera Lifecycle Controller.

### Przywracanie konfiguracji serwera po serwisowaniu sprzętu

Przywracanie serwera do działania po naprawach serwisowych jest krytyczną częścią każdej akcji informatycznej. Zdolność do osiągnięcia krótkiego czasu odzyskiwania danych wiarygodnych danych konfiguracyjnych ma bezpośredni wpływ na bezpieczeństwo systemów. Przywrócenie właściwej

konfiguracji serwera i oprogramowania wewnętrznego zapewnia, że zasady bezpieczeństwa dotyczące działania serwera są automatycznie spełnione.

Serwery powinny zapewniać funkcjonalność, która szybko przywraca konfigurację serwera w następujących sytuacjach:

- Wymiana pojedynczych części
- Wymiana płyty głównej (pełne tworzenie kopii zapasowej i przywracanie profilu serwera)
- Wymiana płyty głównej (Easy Restore).

## Wymiana części

Zalecamy używanie technologii iDRAC, która automatycznie zapisuje obraz oprogramowania układowego i ustawienia konfiguracji dla kart sieciowych, kontrolerów RAID i zasilaczy (PSU). W przypadku wymiany tych części iDRAC automatycznie wykrywa nowy element i przywraca konfigurację oraz oprogramowanie układowe. Ta funkcja oszczędza czas i zapewnia bezpieczeństwo. Aktualizacja następuje automatycznie po wymianie części i ponownym uruchomieniu systemu.

## Easy Restore (do wymiany płyty głównej)

Wymiana płyty głównej może być czasochłonna i wpływać na produktywność systemów. Musi istnieć możliwość tworzenia kopii zapasowych i przywracania konfiguracji i oprogramowania wewnętrznego serwera, aby zminimalizować wysiłek potrzebny do wymiany uszkodzonej płyty głównej.

Istnieją dwa sposoby tworzenia kopii zapasowych i przywracania przez serwer PowerEdge:

1. Serwery PowerEdge automatycznie wykonują kopię zapasową ustawień konfiguracji systemu (BIOS, iDRAC, NIC), service tag'a, aplikacji diagnostycznej UEFI i innych licencjonowanych danych do pamięci flash. Po wymianie płyty głównej na serwerze narzędzie Easy Restore monitoruje o automatyczne przywrócenie tych danych.
2. Użytkownik może wykonać kopię zapasową konfiguracji systemu, w tym zainstalowanych obrazów oprogramowania układowego na różnych komponentach, takich jak BIOS, RAID, NIC, iDRAC, Lifecycle Controller i karty sieciowe typu NDC oraz ustawienia konfiguracji tych komponentów. Operacja tworzenia kopii zapasowej obejmuje również dane konfiguracyjne dysku twardego, płytę główną i wymienione części. Kopia zapasowa tworzy pojedynczy plik, który można zapisać na udziale sieciowym (CIFS, NFS, HTTP lub HTTPS). Kopię zapasową profilu można przywrócić w dowolnym momencie. Dell EMC zaleca wykonanie operacji tworzenia kopii zapasowej dla każdego profilu systemu.

## Wymazywanie systemu

Pod koniec cyklu życia systemu należy go wycofać z produkcji lub zmienić przeznaczenie. Celem procedury wymazywania systemu jest usunięcie poufnych danych i ustawień. Jest to funkcjonalność narzędzia Lifecycle Controller – czyli składowej karty iDRAC, które zostało zaprojektowane do

usuwania dzienników, danych konfiguracyjnych, danych z pamięci wewnętrznej, pamięci podręcznej i wszelkich aplikacji.

Następujące urządzenia, ustawienia konfiguracji i aplikacje należy usunąć za pomocą funkcji wymazywania systemu:

- iDRAC jest resetowany do wartości domyślnych
- Dane kontrolera LifeCycle Controller (LC)
- BIOS
- Wbudowane pakiety diagnostyczne i sterowniki systemu operacyjnego
- iSM
- Raporty dotyczące kolekcji SupportAssist

Dodatkowo należy również usunąć następujące komponenty:

- Sprzętową pamięć podręczna (wymazanie PERC NVCache)
- Karta SD vFlash (inicjalizacja karty)

Dane dotyczące następujących komponentów są usuwane kryptograficznie przez system Erase, jak opisano poniżej:

- SED (dyski samoszyfrujące)
- Dyski ISE (dyski Instant Secure Erase)
- Urządzenia NVM (Apache Pass, NVDIMM)

Ponadto dyski twarde inne niż ISE SATA należy usunąć za pomocą nadpisywania danych.

Należy pamiętać, iż Instant Secure Erase (ISE) niszczy wewnętrzny klucz szyfrowania używany w dyskach obecnej generacji serwerów Dell EMC, przez co danych użytkownika nie można odzyskać. ISE jest uznaną metodą usuwania danych na dyskach pamięci, o której mowa w specjalnej publikacji NIST 800-88 „Guidelines for Media Sanitization”.

Zalety nowej funkcji ISE z System Erase są następujące:

- **Szybkość:** znacznie szybsza niż techniki nadpisywania danych, takie jak DoD 5220.22-M (sekundy względem godzin)
- **Skuteczność:** ISE sprawia, że wszystkie dane na dysku, w tym zarezerwowane bloki, są całkowicie nieczytelne
- **Lepszy całkowity koszt posiadania:** urządzenia do przechowywania mogą być ponownie użyte zamiast zostać w sposób fizyczny zniszczone

Do kasowania systemu można uzyskać dostęp z interfejsu GUI Lifecycle Controller, interfejsu API WS-Man lub interfejsu CLI RACADM.



## Restart serwera

W czasie restartu zasilania serwer oraz wszystkie jego komponenty są uruchamiane ponownie. Wszystkie dane w pamięci ulotnej są również usuwane. Fizyczny restart serwera wymaga wyciągnięcia kabla zasilającego, odczekania 30 sekund, a następnie włożenia kabla z powrotem. Stanowi to wyzwanie podczas pracy ze zdalnym systemem. Nowa funkcja w serwerach Dell EMC pozwala na wykonanie efektywnego restartu zasilania z iSM, iDRAC GUI, BIOS lub skryptu. Pełny restart zasilania włącza się przy następnym restarcie zasilania.

Funkcja restartu zasilania eliminuje potrzebę fizycznej obecności w centrum danych, co skraca czas rozwiązywania problemów.

W ten sposób może wyeliminować wszelkie złośliwe oprogramowanie, które nadal rezyduje w pamięci.