



Wzmocnienie
bezpieczeństwa
**3,5 razy
więcej funkcji
bezpieczeństwa**

W tym uwierzytelnianie
dwuskładnikowe i zarządzanie
kluczami zewnętrznymi za
pomocą kontrolera iDRAC9



Optymalizacja
efektywności energetycznej
**6 razy więcej
raportów o zużyciu
energii**

20 raportów w Dell OME i 3
raporty w Supermicro SSM



**Wzrost efektywności
operacyjnej poprzez
zaoszczędzenie
1 godz.
i 50 min czasu
administracyjnego
na 100 serwerów**

Automatyczne aktualizacje
w kontrolerze Dell iDRAC9
w porównaniu z brakiem
automatycznych aktualizacji
w przypadku interfejsu IPMI
Supermicro

Zwiększenie bezpieczeństwa i wydajności zgodnie z zasadami zrównoważonego rozwoju dzięki narzędziom do zarządzania serwerami Dell

W porównaniu z ofertą rozwiązań Supermicro do zarządzania

Inwestując w nowe serwery do centrum danych, dokonujesz czegoś więcej niż tylko wyboru sprzętu — wybierasz także rozwiązanie do zarządzania. Gdy administratorzy mają do dyspozycji wydajne, wysoce funkcjonalne narzędzia do wdrażania, monitorowania, utrzymywania i zabezpieczania infrastruktury przy jednoczesnej poprawie jej efektywności energetycznej, mogą łatwo poradzić sobie z codziennym zarządzaniem i poświęcić więcej czasu na innowacje, które stymulują rozwój organizacji. Decydując się na zakup niezawodnych narzędzi do zarządzania, możesz zaoszczędzić czas i pieniądze w przyszłości.

Oceniliśmy ofertę firm Dell™ i Supermicro® w zakresie zarządzania serwerami, porównując trzy narzędzia Dell z dwoma narzędziami Supermicro.

Tabela 1. Testowane przez nas narzędzia do zarządzania. *Dell CloudIQ to oparte na chmurze narzędzie do monitorowania i analizy; Supermicro nie oferuje równoważnego narzędzia.

Źródło: Principled Technologies.

	Dell	Supermicro
Wbudowane/zdalne zarządzanie serwerem	iDRAC9 (Integrated Dell Remote Access Controller)	Supermicro Intelligent Management (IPMI)
Konsola zarządzania urządzeniami typu jeden-do-wielu	Dell OpenManage™ Enterprise (OME) Dell CloudIQ*	Supermicro Server Manager (SSM)

Jeśli chodzi o zrównoważony rozwój, bezpieczeństwo i codzienne zarządzanie, stwierdziliśmy, że firma Dell konsekwentnie dostarcza bardziej funkcjonalne zestawy narzędzi, które zapewniają administratorom więcej opcji i możliwości.

Więcej bardziej rozbudowanych funkcji automatyzacji ułatwiających zarządzanie serwerem

Twoje zespoły IT potrzebują nowoczesnych, wysoce funkcjonalnych narzędzi do zarządzania, które pozwolą im zaoszczędzić czas w codziennej pracy i dotrzymać kroku standardom bezpieczeństwa oraz wydajności. Oceniane przez nas narzędzia do zarządzania firmy Dell obejmują szereg funkcji i możliwości, które nie są dostępne w ofercie rozwiązań do zarządzania firmy Supermicro.

Materiały przyjazne dla środowiska

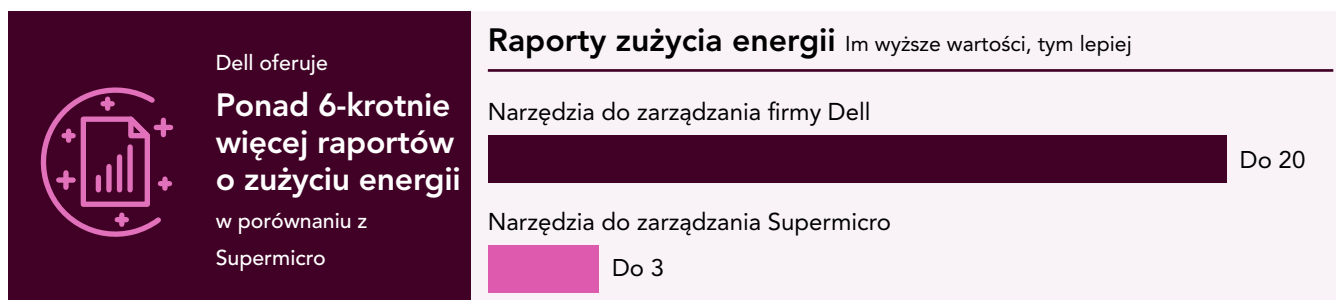
Wraz ze wzrostem kosztów energii i zaostrzającymi się przepisami dotyczącymi ochrony środowiska wiele organizacji skupia się na zrównoważonym rozwoju. Centra danych z natury wymagają dużych ilości energii, ale staranne zarządzanie temperaturą i zasilaniem może pozwolić organizacjom na zmniejszenie ilości zużywanych zasobów. Oprogramowanie Dell OpenManage Enterprise zawiera kilka funkcji, które umożliwiają ściśle monitorowanie i zarządzanie zużyciem energii, pomagając w ten sposób w osiągnięciu celów związanych ze zrównoważonym rozwojem. Tabele 2 i 3 przedstawiają najważniejsze zalety tych funkcji, które opiszemy bardziej szczegółowo poniżej.

Tabela 2. Różnice w zakresie zrównoważonego rozwoju między oprogramowaniem Dell OpenManage Enterprise a SSM. Źródło: Principled Technologies.

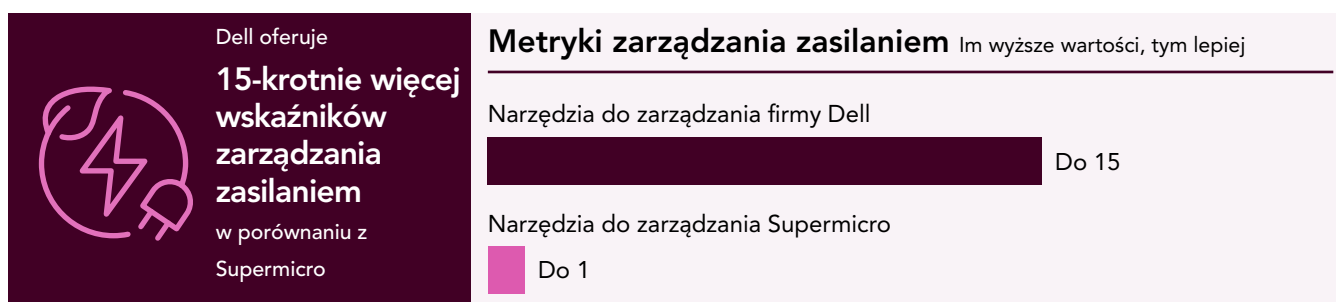
Funkcja	Narzędzia do zarządzania firmy Dell	Narzędzia do zarządzania Supermicro
Kalkulator zużycia emisji dwutlenku węgla i narzędzie do planowania pojemności	✓	x
Analiza śladu węglowego	✓	x
Zasady zarządzania zasilaniem wyzwalane temperaturą	✓	x
Zasady zarządzania zasilaniem statycznym	✓	✓

Tabela 3. Podsumowanie naszego porównania między Dell OME i Supermicro SSM i IPMI. Źródło: Principled Technologies.

Funkcja	Najważniejsze korzyści płynące z narzędzi do zarządzania firmy Dell	Wady narzędzi do zarządzania Supermicro
 Kalkulator zużycia emisji dwutlenku węgla i narzędzie do planowania pojemności	Możliwość oszacowania emisji gazów cieplarnianych za pomocą konfigurowalnych wartości, które pomogą Ci osiągnąć cele w zakresie zrównoważonego rozwoju	Brak porównywalnej funkcji ; utrudnia planowanie osiągnięcia celów w zakresie zrównoważonego rozwoju
 Analiza śladu węglowego	Dostępny za pośrednictwem oprogramowania OpenManage Enterprise Power Manager; dostarcza dane o emisji dwutlenku węgla, które mogą pomóc w osiągnięciu celów zrównoważonego rozwoju	Brak porównywalnej funkcji ; brak możliwości śledzenia śladu węglowego, który pomógłby monitorować realizację celów w zakresie zrównoważonego rozwoju
 Zautomatyzowane zarządzanie zasilaniem i temperaturą	Opcje zasad wyzwalane statycznie i temperaturowo z opcją wyzwalania, gdy serwer przekroczy próg zużycia energii lub temperatury	Jeden statyczny typ zasad bez skojarzonych opcji wyzwalania
 Raporty zużycia energii	Ponad 6 razy więcej raportów, z 20 wbudowanymi raportami z zaplanowaną dystrybucją wiadomości e-mail i opcjami dostosowywania	2 wbudowane raporty w SSM; 1 raport w Supermicro IPMI, którego nie można eksportować
 Wskaźniki zarządzania zasilaniem	Nawet 15 razy więcej wskaźników zapewniającym bardziej szczegółowy wgląd w zarządzanie zużyciem energii	Tylko 1 wskaźnik , co daje mniejszy wgląd i gorszą kontrolę nad zużyciem energii



Rysunek 1. Liczba raportów o zużyciu energii dostępnych w rozwiązaniach Dell OME i Supermicro SSM. Źródło: Principled Technologies.



Rysunek 2. Liczba wskaźników zarządzania zasilaniem dostępnych w rozwiązaniach Dell OME i Supermicro SSM. Źródło: Principled Technologies.

Zautomatyzowane zarządzanie zasilaniem i temperaturą

OpenManage Enterprise Power Manager zapewnia zautomatyzowane zarządzanie zasilaniem i temperaturą za pomocą opcji zasad zarówno statycznych, jak i wyzwalanych temperaturą, które umożliwiają administratorom ustawianie wartości granicznych zużycia energii lub progów temperatury w celu obniżenia kosztów chłodzenia. Z kolei w SSM obowiązuje jedna zasada, czyli statyczny limit zużycia energii, który nie jest automatycznie uruchamiany przez serwer przekraczający wartość graniczną, co może prowadzić do wyższych kosztów energii.

Organizacje, które chcą dogłębnie analizować zużycie energii w centrum danych z myślą o optymalizacji, mogą skorzystać z **20 różnych wbudowanych raportów zużycia energii** zapewnianych przez OpenManage Enterprise Power Manager. Te raporty są przydatne w planowaniu pojemności i zarządzaniu zasilaniem w celu maksymalizacji wydajności. Możliwości w zakresie raportowania w SSM są znacznie bardziej ograniczone. Administratorzy mogą uruchomić tylko jednego hosta z raportem usług lub zobaczyć trend zużycia energii na ekranie monitorowania. Dzięki Supermicro IPMI użytkownicy mogą przeglądać wykres mocy na poziomie podzespołu w BMC; nie mogą jednak eksportować danych z wykresu do analizy i mogą je zapisać tylko jako obraz.

Wtyczka OpenManage Enterprise Power Manager umożliwia administratorom **wyświetlanie do 15 różnych wskaźników**, w tym zużycia energii przez poszczególne podzespoły, przepływu powietrza i wykorzystania podzespołów. SSM oferuje tylko raport całkowitego zużycia energii.

Emisja dwutlenku węgla i analiza śladu węglowego

OME zawiera kalkulator emisji dwutlenku węgla i narzędzie do planowania wydajności, które oprócz innych funkcji może pomóc w oszacowaniu własnej emisji gazów cieplarnianych. Podaje domyślne wartości kosztów energii i emisji dwutlenku węgla dla jednostki zużytej energii, ale umożliwia dostosowanie tych wartości do kosztów energii w danym regionie oraz modelu zużycia w centrum danych. SSM nie oferuje porównywalnej funkcji, co może utrudniać organizacjom planowanie i monitorowanie postępów w osiąganiu celów w zakresie zrównoważonego rozwoju.

zabezpieczenia

Cyberprzestępczość rośnie wykładniczo, grożąc firmom „uszkodzeniem i zniszczeniem danych, spadkiem wydajności, kradzieżą pieniędzy, własności intelektualnej, danych osobowych i finansowych, defraudacją, oszustwem, zakłóceniem normalnego toku działalności po ataku, dochodzeniami kryminalistycznymi, problemami związanymi z przywróceniem i usunięciem zhakowanych danych i systemów oraz uszczerbkiem na reputacji”.¹ W tym krajobrazie decydenci powinni uwzględniać bezpieczeństwo przy każdym zakupie serwera. Odkryliśmy, że oprogramowanie Dell OpenManage Enterprise zawiera kilka funkcji ułatwiających bezpieczeństwo danych, których nie mają narzędzia Supermicro (patrz tabele 4 i 5).

Tabela 4. Różnice w zabezpieczeniach między narzędziami do zarządzania firmą Dell a narzędziami do zarządzania Supermicro. Źródło: Principled Technologies.

Funkcja	Narzędzia do zarządzania firmą Dell	Narzędzia do zarządzania Supermicro
Uwierzytelnianie wieloskładnikowe	✓	x
Zewnętrzne zarządzanie kluczami	✓	x
Kontrola dostępu oparta na zakresie	✓	x
Konfiguracja zabezpieczeń oparta na zasadach	✓	x
Ostrzeżenia dotyczące cyberbezpieczeństwa	✓	x
Kontrola dostępu oparta na rolach	✓	✓
Dynamiczne wyłączanie portów USB	✓	✓

Tabela 5. Podsumowanie naszego porównania funkcji zabezpieczeń między narzędziami do zarządzania firmą Dell i Supermicro. Źródło: Principled Technologies.

Funkcja	Najważniejsze korzyści płynące z narzędzi do zarządzania firmą Dell	Wady narzędzi do zarządzania Supermicro
 Uwierzytelnianie wieloskładnikowe (MFA)	Uwierzytelnianie dwuskładnikowe za pomocą kontrolera iDRAC oraz adresu e-mail i identyfikatora RSA SecurID , uniemożliwiające nieautoryzowanym użytkownikom uzyskanie dostępu do poufnych danych	Brak porównywalnej funkcji — pozostawia lukę w zabezpieczeniach, która mogłaby pomóc nieautoryzowanym użytkownikom uzyskać dostęp do poufnych danych
 Zewnętrzne zarządzanie kluczami	Rozwiązanie Secure Enterprise Key Manager w kontrolerze iDRAC umożliwiające dodanie kolejnej warstwy zabezpieczeń w celu ochrony danych przechowywanych na serwerach przy użyciu szyfrowania dysków i scentralizowanego zarządzania	Brak porównywalnej funkcji , co pozostawia kolejną lukę w zabezpieczeniach
 Kontrola dostępu	OME oferuje zarówno kontrolę dostępu opartą na rolach (RBAC), jak i kontrolę dostępu opartą na zakresie (SBAC) w celu ograniczenia grup urządzeń, do których menedżer urządzeń ma dostęp	Tylko RBAC — mniejsze możliwości w zakresie ograniczania dostępu przez administratorów
 Konfiguracja zabezpieczeń oparta na zasadach	Ustawienia konfiguracji zabezpieczeń oparte na zasadach za pośrednictwem CloudIQ, które ostrzegają administratorów o rozbieżnościach	Brak porównywalnej funkcji , co może opóźnić działanie i usunięcie naruszeń
 Ostrzeżenia dotyczące cyberbezpieczeństwa	Raportowanie porad dotyczących zabezpieczeń za pośrednictwem rozwiązania Dell CloudIQ Security ze szczegółowymi informacjami na temat luk w zabezpieczeniach i odpowiednimi sugestiami dotyczącymi środków zaradczych w celu umożliwienia szybkiego działania	Brak porównywalnej funkcji , co pozostawia luki w zabezpieczeniach do wykorzystania przez złośliwe podmioty

Uwierzytelnianie wieloskładnikowe

Uwierzytelnianie wieloskładnikowe (MFA) może pomóc w zapobieganiu uzyskiwaniu dostępu do poufnych danych przez nieautoryzowanych użytkowników i złośliwe podmioty. Potwierdziliśmy, że kontroler Dell iDRAC umożliwia uwierzytelnianie dwuskładnikowe zarówno za pomocą poczty e-mail, jak i identyfikatora RSA SecurID — zestawu zewnętrznych technologii uwierzytelniania wieloskładnikowego używanych w wielu branżach.² Potwierdziliśmy również, że ani Supermicro IPMI, ani SSM nie zapewniają tej funkcji, co pozostawia lukę w zabezpieczeniach.

Zarządzanie kluczami

Zewnętrzne systemy zarządzania kluczami (KMS) umożliwiają zespołom IT korzystanie z oddzielnego serwera innej firmy do zarządzania kluczami używanymi do blokowania i odblokowywania pamięci masowej, dodając warstwę zabezpieczeń. Kontroler iDRAC zawiera funkcję Local Key Manager (LKM) dla wszystkich nowych serwerów Dell PowerEdge. Niektóre licencje obejmują również funkcję Secure Enterprise Key Manager (SEKM), zapewniając dodatkowe bezpieczeństwo dzięki pełnemu szyfrowaniu dysku i zewnętrznemu zarządzaniu kluczami. SEKM obsługuje standardowy w branży protokół OASIS KMIP, dając organizacjom wybór dowolnego zewnętrznego dostawcy rozwiązań KMS, który korzysta z tego standardu. Supermicro nie oferuje tej funkcji bezpieczeństwa ani jej odpowiednika.

Kontrola dostępu

Kontrola dostępu oparta na rolach (RBAC), w której rola użytkownika określa części systemu, do których ma dostęp, oraz zadania, które może w nich wykonywać, jest integralnym składnikiem wielu strategii zabezpieczeń serwerów. W oprogramowaniu OpenManage Enterprise kontrola dostępu oparta na rolach definiuje uprawnienia użytkownika dla trzech wbudowanych ról: Administrator, Menedżer urządzeń i Przeglądający.³ Zapewnia również kontrolę dostępu opartą na zakresie (SBAC), która umożliwia administratorom ograniczenie grup urządzeń, do

których ma dostęp menedżer urządzeń.⁴ Daje to administratorom możliwość zapewnienia dostępu do podzbioru urządzeń. Supermicro oferuje rozwiązanie RBAC, ale nie SBAC.

Zarządzanie poświadczeniami

Rotacja haseł kontrolera iDRAC służy kilku celom: rotuje dostęp do oprogramowania OpenManage Enterprise zgodnie z zasadami zabezpieczeń, domyślnie w cyklu miesięcznym; współpracuje z zewnętrznym programem obsługi haseł; obsługuje oprogramowanie CyberArk do zarządzania hasłami.^{5,6}

Dzięki oprogramowaniu OpenManage Enterprise administratorzy mogą zarządzać rotacją haseł kontrolera iDRAC, zastępując konieczność korzystania ze statycznego znanego konta administratora kontem usługi zarządzanym przez OME. SSM nie ma takiej możliwości.

Konfiguracja zabezpieczeń oparta na zasadach

Firma Dell oferuje funkcję cyberbezpieczeństwa opartą na zasadach w rozwiązaniu CloudIQ for PowerEdge AIOps. Ta funkcja pobiera konfigurację wdrożonego serwera PowerEdge i porównuje ją z polityką konfiguracji dotyczącą bezpieczeństwa opartą na najlepszych praktykach firmy Dell. W przypadku, gdy CloudIQ wykryje rozbieżność, powiadamia administratora i podaje kroki naprawcze.⁷ SSM nie oferuje równoważnej funkcji, co może oznaczać opóźnienia w wykrywaniu naruszeń.

Ostrzeżenia dotyczące cyberbezpieczeństwa

Poradniki bezpieczeństwa informują opinię publiczną o problemach związanych z zabezpieczeniami. Według firmy Dell strona Dell Security Advisories w CloudIQ zawiera pełną listę odpowiednich porad dotyczących zabezpieczeń wraz z ich znaczeniem, liczbą systemów, których dotyczą, oraz datą publikacji.⁸ Rozwiązanie Dell CloudIQ zawiera raporty z poradami dotyczącymi bezpieczeństwa ze szczegółowymi informacjami na temat luk w zabezpieczeniach i sugestiami dotyczącymi środków zaradczych. SSM nie oferuje podobnej funkcji, co może narazić systemy na ataki.

Informacje o Dell CloudIQ

Dell CloudIQ to oparte na chmurze narzędzie AIOps oferujące „proaktywne monitorowanie, uczenie maszynowe i analitykę predykcijną” dla dużej liczby produktów i usług firmy Dell, w tym serwerów, pamięci masowej, urządzeń do ochrony danych i infrastruktury hiperkonwergentnej.⁹ W badaniu Principled Technologies z 2022 r. dowiedziono, że narzędzie CloudIQ miało znikomy wpływ na przepustowość sieci, a jednocześnie pozwalało monitorować telemetrię, stan, alerty i zasoby z jednej konsoli.¹⁰

Dowiedz się więcej o CloudIQ na stronie <https://www.dell.com/en-us/dt/solutions/cloudiq.htm>.

Dynamiczne wyłączenie portów USB

Wyłączanie i włączanie portów USB daje administratorom kontrolę nad dostępem do serwera przez port USB, zapobiegając w ten sposób ich złośliwemu użyciu i ryzyku instalacji zabronionych aplikacji lub wirusów.

Kontroler iDRAC firmy Dell zapewnia niezależne, dynamiczne wyłączanie portów USB bez przestojów. Choć Supermicro oferuje dynamiczne wyłączanie przedniego i tylnego portu USB w systemie, wymaga to klucza licencyjnego Supermicro DataCenter Management Suite na węzeł. Dział IT może uruchomić tę funkcję, wdrażając polecenie blokady systemu, które można wykonać z poziomu BMC lub konsoli Supermicro IPMI, ale nie jest to niezależne od trybu blokady systemu.¹¹

Jak pokazano na rysunku 3, wyłączanie portów za pomocą kontrolera Dell iDRAC było prostym procesem **wymagającym tylko 41 sekund i 4 kroków**. W przypadku Supermicro IPMI zajęło to **niemal czterokrotnie więcej czasu — 2 minuty i 50 sekund oraz 6 kroków**. Ekstrapolując te oszczędności czasu na 100 systemów, oszczędność czasu wzrosłaby do 3 godzin i 35 minut, co oznacza, że administrator spędziłby prawie połowę dnia pracy przy użyciu interfejsu IPMI Supermicro w porównaniu z nieco ponad godziną przy użyciu kontrolera Dell iDRAC.



Rysunek 3. Czas na wyłączenie przednich portów USB dla pojedynczego serwera i ekstrapolowany czas na wyłączenie przednich portów USB dla 100 serwerów.

Im niższa wartość, tym lepiej. Źródło: Principled Technologies.

Informacje o Dell OpenManage Enterprise

OpenManage Enterprise to konsola zarządzania systemami typu jeden-do-wielu dla centrum danych. Konsola zapewnia nowoczesny interfejs graficzny użytkownika HTML5 i jest wdrażana jako urządzenie wirtualne dla środowisk VMware ESXi™, Microsoft Hyper-V i Kernel-based Virtual Machine (KVM). Oprogramowanie OpenManage Enterprise może wykrywać i inwentaryzować sieci IPv4 i IPv6 zawierające do 8000 urządzeń, w tym serwery do montażu w szafie montażowej Dell, serwerów Dell w obudowie typu tower oraz kaset i obudów Dell.¹² W niedawnym badaniu PT dowiedziono, że środowisko firmy Dell z oprogramowaniem OpenManage Enterprise i OpenManage Enterprise Modular (OME-M) może zaoszczędzić czas na wprowadzaniu zmian w sieciach VLAN i pomóc uniknąć interwencji podczas zaplanowanych aktualizacji oprogramowania sprzętowego.¹³

Dowiedz się więcej o oprogramowaniu OpenManage Enterprise na stronie <https://www.dell.com/en-us/lp/dt/openmanage-enterprise>

Monitorowanie, analityka i łatwość obsługi

Narzędzia do zarządzania różnią się znacznie pod względem sposobu, w jaki wspierają administratorów wykonujących działania związane z monitorowaniem i analizą, a także inne rutynowe zadania, takie jak planowanie aktualizacji. W tej sekcji przyjrzymy się różnicom w tych obszarach między badanymi przez nas narzędziami do zarządzania firmy Dell i Supermicro. Jak odkryliśmy, badając funkcje związane ze zrównoważonym rozwojem i zabezpieczeniami, pakiet narzędzi do zarządzania firmy Dell oferuje wiele funkcji ułatwiających życie administratorów — funkcji, których nie mają narzędzia Supermicro. W tabeli 6 porównano korzyści płynące z zarządzania, jakie zapewniają te narzędzia.

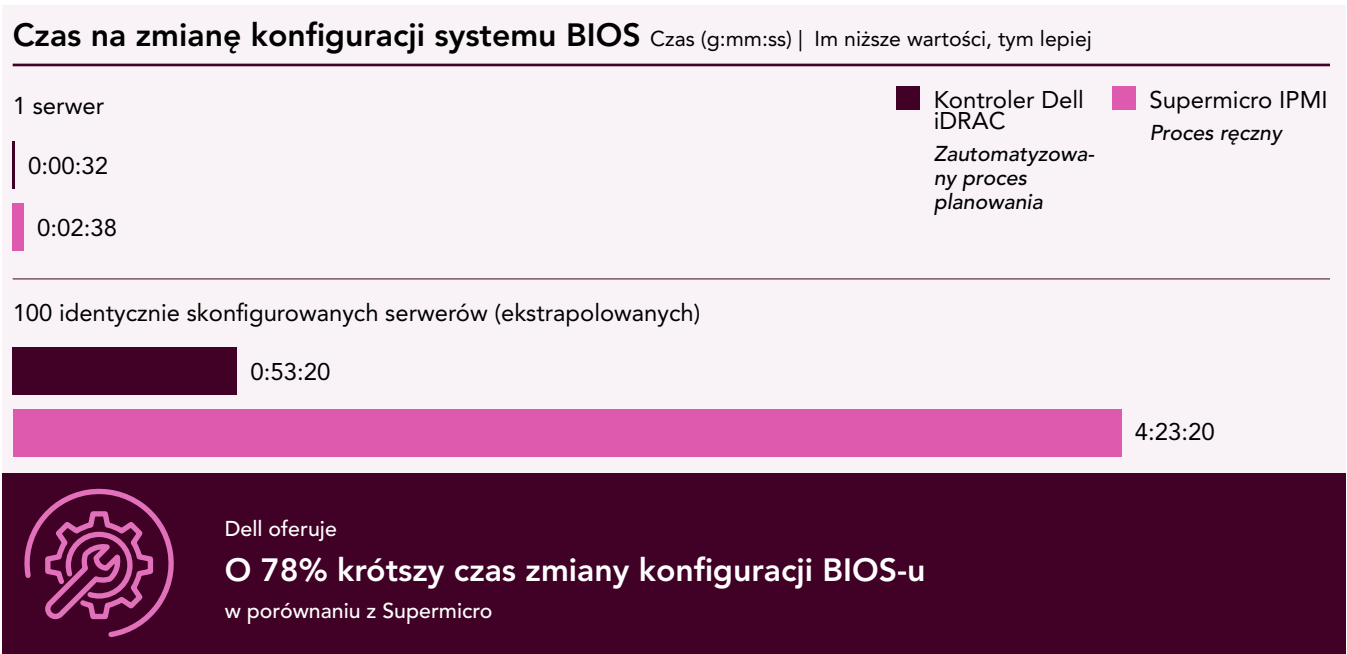
Tabela 6. Podsumowanie naszego porównania między narzędziami do zarządzania firm Dell i Supermicro. Źródło: Principled Technologies.

Funkcja	Najważniejsze korzyści płynące z narzędzi do zarządzania firmy Dell	Wady narzędzi do zarządzania Supermicro
 Streaming telemetrii	Strumieniowe przesyłanie danych telemetrycznych iDRAC9 dostępne dla zdalnych serwerów syslog; pomaga przewidywać awarie i optymalizować wydajność; może przysyłać strumieniowo dane serwera do narzędzi analitycznych, takich jak Grafana i Splunk	Brak automatycznego przesyłania strumieniowego danych telemetrycznych
 Mobilne monitorowanie i zarządzanie	Aplikacja mobilna OpenManage w wieloma funkcjami dla systemów iOS i Android, która integruje się z OME i kontrolerem iDRAC9	Aplikacja Supermicro IPMIView, która nie integruje się z SSM
 Monitorowanie urządzeń i serwerów innych firm	OME obsługuje monitorowanie urządzeń i serwerów, w tym obsługę rozwiązań swoich głównych konkurentów	Obsługuje tylko urządzenia innych firm, które korzystają z ich agentów, kontrolerów BMC, wcześniejszych wersji sprzętu obsługujących IPMI oraz urządzeń obsługujących Redfish
 Monitorowanie nieruchomości	Dostępne za pośrednictwem OME i CloudIQ; OME może przysyłać dane z licencjonowanych serwerów zarządzanych do CloudIQ w celu monitorowania w wielu centrach danych	Brak portalu opartego na chmurze do agregowania danych monitorowania w centrach danych
 Działania oparte na alertach	Zasady w OME, które uruchamiają działania na podstawie danych wejściowych z alertu	Brak dostępnych działań opartych na alertach
 Łatwiejsze wdrażanie serwera (możliwość importu/eksportu konfiguracji systemu)	Może używać kontrolera iDRAC9 do importowania/eksportowania wszystkich elementów konfiguracji serwerów; wymaga jedynie 48 sekund i 5 kroków na import oraz 1 minutę i 9 sekund i 7 kroków na eksport	Może importować/eksportować tylko konfigurację Baseboard Management Controller (BMC), co wymaga poświęcenia czasu na ręczną konfigurację dla każdego serwera
 Mniej czasu na zmianę ustawień konfiguracji BIOS	Może szybko zmienić pełne ustawienia systemu BIOS bezpośrednio z kontrolera iDRAC oraz przygotować aktualizację i uruchomić ponownie system w oknie konserwacji, oszczędzając znaczną ilość czasu potrzebnego na czynności administracyjne	Ograniczone zmiany w systemie BIOS dostępne z poziomu BMC, w przeciwnym razie wymagane jest ponowne uruchomienie serwera; wymaga wykonania większej liczby ręcznych kroków i zajmuje więcej czasu administratora
 Działa jako urządzenie wirtualne	Dostępne w OME, co eliminuje potrzebę aktualizacji systemu operacyjnego	Brak porównywalnej funkcji, musi działać w zarządzanym systemie operacyjnym. Daje to administratorom jeszcze jeden podzespół do aktualizowania
 Widok połączenia	Dostępne w kontrolerze iDRAC; narzędzie do rozwiązywania problemów wykorzystujące protokół LLDP do diagnozowania usterek sieci, takich jak okablowanie, uszkodzone porty przełącznika i inne	Brak widoku połączenia, brak informacji o fizycznej łączności z portami przełącznika nadrzędnego
 Możliwość zaplanowania aktualizacji oprogramowania sprzętowego i sterowników	Dostępne w OME i iDRAC	Może zaplanować aktualizacje systemu BIOS i oprogramowania sprzętowego BMC, ale nie może zaplanować aktualizacji sterowników

Zmiana elementu konfiguracji systemu BIOS

Dell umożliwia pełną zmianę ustawień konfiguracji BIOS bezpośrednio z kontrolera iDRAC z możliwością wprowadzenia tych zmian do następnego ponownego uruchomienia. Supermicro oferuje ograniczony zestaw ustawień systemu BIOS z poziomym BMC. Oprócz tego zmiana ustawień systemu BIOS na serwerach Supermicro dla pojedynczego elementu konfiguracji wymaga od administratora ponownego uruchomienia serwera w celu uzyskania dostępu do menu konfiguracji BIOS z ekranu rozruchowego.

Rysunek 4 przedstawia czas potrzebny do zmiany konfiguracji systemu BIOS na pojedynczym serwerze przy użyciu kontrolera Dell iDRAC i interfejsu IPMI Supermicro. Proces ręczny przy użyciu **narzędzia Supermicro trwa dodatkowo 2 minuty i 6 sekund, czyli niemal 5 razy dłużej** niż ustawienie procesu automatycznego w kontrolerze iDRAC. Jeśli ekstrapolujemy te czasy na 100 serwerów, które są skonfigurowane identycznie, oszczędność czasu dzięki kontrolerowi iDRAC wyniosłaby 3,5 godziny. (Gdyby serwery nie były skonfigurowane identycznie, nie zauważylibyśmy tych oszczędności czasu).



Rysunek 4. Czas wykonania zmiany konfiguracji BIOS zarówno na pojedynczym serwerze, jak i na 100 identycznie skonfigurowanych serwerach (ekstrapolacja).
Im niższa wartość, tym lepiej. Źródło: Principled Technologies.

Informacje o kontrolerze iDRAC9

Serwery Dell PowerEdge™ są wyposażone w zintegrowany kontroler Dell Remote Access Controller 9 z kontrolerem cyklu eksploatacji firmy Dell, który zapewnia funkcje administrowania systemem, w tym alerty i funkcje zdalnego zarządzania. Według firmy Dell najważniejsze zalety kontrolera iDRAC9 obejmują:

- możliwość zarządzania tysiącami serwerów za pomocą interfejsów API i narzędzi skryptowych;
- wbudowaną obsługę oferującą wgląd w stan i kondycję serwera oraz monitorowanie tysięcy parametrów;
- zaawansowane funkcje i opcje związane z bezpieczeństwem.¹⁴

Aby dowiedzieć się więcej o funkcjach kontrolera iDRAC9, odwiedź stronę <https://www.dell.com/en-us/lp/dt/open-manage-idrac>.

Automatyczne aktualizacje oprogramowania sprzętowego i sterowników

iDRAC

W przeciwieństwie do Supermicro IPMI kontroler Dell iDRAC umożliwia zaplanowanie automatycznych aktualizacji oprogramowania sprzętowego. Oznacza to, że skonfigurowanie automatycznych aktualizacji zgodnie z harmonogramem jest jednorazowym zadaniem, które pozwoli zaoszczędzić czas przy każdym cyklu aktualizacji. Rysunek 5 przedstawia ekstrapolowany czas do zaplanowania automatycznych aktualizacji oprogramowania sprzętowego po raz pierwszy dla 100 serwerów, korzystając z kontrolera Dell iDRAC i Supermicro IPMI. Proces ręczny przy użyciu narzędzia Supermicro trwa **13 minut dłużej** niż ustawienie procesu automatycznego w kontrolerze iDRAC.

Jeśli założymy, że administrator konfiguruje miesięczny harmonogram w pierwszą sobotę wieczorem każdego miesiąca, administrator korzystający z kontrolera iDRAC będzie musiał jednorazowo poświęcić 58 sekund na serwer. W przypadku 100 serwerów jest to jednorazowa konfiguracja trwająca 1 godzinę, 36 minut i 40 sekund. Dla porównania administrator korzystający z Supermicro IPMI musiałby poświęcić 1 godzinę i 50 minut na 100 serwerów w każdej przerwie konserwacyjnej. Jeśli porównamy jednorazową konfigurację za pomocą kontrolera iDRAC i pierwszą z wielu konfiguracji w przypadku IPMI Supermicro, narzędzie do zarządzania firmy Dell pozwala zaoszczędzić około 13 minut i 20 sekund. (Patrz Rysunek 5).

Jednak za drugim razem i za każdym kolejnym razem **rozwiązanie Dell oszczędza 110 minut, ponieważ administrator nie musi już wykonywać tego zadania.** (Patrz Rysunek 6). Ta oszczędność czasu występuje nawet wtedy, gdy 100 serwerów nie jest identycznie skonfigurowanych. Należy pamiętać, że czasy te obejmują tylko przesłanie oprogramowania układowego do kontrolera BMC i nie uwzględniają czasu pobierania ani wyodrębniania oprogramowania sprzętowego Supermicro.

OME

Dell OME obsługuje **aktualizacje oprogramowania wewnętrznego dla wszystkich podzespołów**, a także aktualizacje sterowników systemu Windows. Program SSM obsługuje aktualizację oprogramowania sprzętowego systemu BIOS i kontrolera BMC, ale **nie aktualizacje sterowników ani innych składników systemu.**

Ekstrapolowany czas zaplanowania automatycznej aktualizacji oprogramowania wewnętrznego za pierwszym razem (100 serwerów)

Czas (g:mm:ss) | Im niższe wartości, tym lepiej

Dell iDRAC *Zautomatyzowany proces planowania*



Supermicro IPMI *Proces ręczny*



 **Oszczędność do 13 minut przy pierwszym planowaniu automatycznych aktualizacji oprogramowania wewnętrznego dla 100 serwerów**

Rysunek 5. Ekstrapolowany czas aktualizacji oprogramowania sprzętowego na 100 serwerach za pierwszym razem. Im niższa wartość, tym lepiej. Źródło: Principled Technologies.

Ekstrapolowany czas zaplanowania automatycznej aktualizacji oprogramowania wewnętrznego za każdym kolejnym razem (100 serwerów)

Czas (g:mm:ss) | Im niższe wartości, tym lepiej

Dell iDRAC *Zautomatyzowany proces planowania*

Brak dodatkowego czasu

Supermicro IPMI *Proces ręczny*



 **Oszczędność czasu administratora dzięki automatycznym aktualizacjom, BEZ konieczności poświęcania czasu na aktualizację po początkowej konfiguracji**

Rysunek 6. Ekstrapolowany czas aktualizacji oprogramowania wewnętrznego na 100 serwerach za każdym razem. Im niższa wartość, tym lepiej. Źródło: Principled Technologies.

Wnioski

Wybór dostawcy do zakupu serwerów to coś więcej niż tylko platforma sprzętowa. Osoby podejmujące decyzje muszą również wziąć pod uwagę bardziej długoterminowe kwestie, w tym bezpieczeństwo systemu/danych, wydajność energetyczną i łatwość zarządzania. Te obawy sprawiają, że narzędzia do zarządzania systemami oferowane przez dostawcę są równie ważne jak sprzęt.

Przetestowaliśmy funkcje i możliwości narzędzi do zarządzania serwerami firm Dell i Supermicro, porównując kontroler Dell iDRAC9 z interfejsem IPMI Supermicro do zarządzania serwerami wbudowanymi oraz rozwiązanie Dell OpenManage Enterprise i CloudIQ z oprogramowaniem Supermicro Server Manager do zarządzania i monitorowania urządzeń i konsol typu „jeden do wielu”. Okazało się, że narzędzia do zarządzania firmy Dell zapewniają bardziej kompleksowe funkcje i możliwości w zakresie bezpieczeństwa, zrównoważonego rozwoju oraz zarządzania/monitorowania niż serwery Supermicro. Ponadto narzędzia firmy Dell zautomatyzowały więcej zadań, aby ułatwić zarządzanie serwerami, co przyniosło administratorom znaczną oszczędność czasu w porównaniu z koniecznością ręcznego wykonywania tych samych zadań za pomocą narzędzi Supermicro.

Podczas zakupu serwera powiązane produkty do zarządzania dostawcy mają kluczowe znaczenie dla ochrony danych, wspierania bardziej zrównoważonego środowiska i ułatwiania konserwacji systemów. Nasze testy i badania wykazały, że oferta firmy Dell do zarządzania serwerami PowerEdge zapewnia więcej funkcji ułatwiających organizacjom osiągnięcie tych celów niż porównywalne produkty do zarządzania Supermicro.

1. Steve Morgan, „Cybercrime To Cost The World \$10.5 Trillion Annually By 2025”, dostęp 15 lutego 2024 r., <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>.
2. Dell, „Using iDRAC9 RSA SecurID 2FA”, dostęp 15 lutego 2024 r., <https://dl.dell.com/Manuals/Common/dellemc-idrac9-rsa-securid-2fa.pdf>.
3. Dell, „Dell EMC OpenManage Enterprise SupportAssist Version 1.1 User's Guide”, dostęp 15 lutego 2024 r., <https://www.dell.com/support/manuals/en-us/openmanage-enterprise-supportassist/omesapuserguide11/role-and-scope-based-access-control-in-openmanage-enterprise?>.
4. Dell, „Dell EMC OpenManage Enterprise SupportAssist Version 1.1 User's Guide”.
5. Dell, „OpenManage Enterprise 4.0: iDRAC Password Management and Rotation”, dostęp 15 lutego 2024 r., <https://www.dell.com/support/kbdoc/en-us/000219279/openmanage-enterprise-4-0-idrac-password-management-and-rotation>.
6. Dell, „OpenManage Portfolio Software Licensing Guide”, dostęp 3 kwietnia 2024 r., <https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/openmanage-portfolio-software-licensing-guide.pdf>.
7. Mark Maclean i Kyle Shannon, „Dell CloudIQ Cybersecurity For PowerEdge: The Benefits Of Automation”, dostęp 15 lutego 2024 r., <https://infohub.delltechnologies.com/en-US/p/dell-cloudiq-cybersecurity-for-poweredge-the-benefits-of-automation/>.
8. Dell, „Security Advisories”, dostęp 15 lutego 2024 r., <https://infohub.delltechnologies.com/en-US/l/cloudiq-a-detailed-review/security-advisories/>.
9. Dell, „Dell CloudIQ - AIOps for Intelligent IT Infrastructure Insights”, dostęp 15 lutego 2024 r., <https://www.dell.com/en-us/dt/solutions/cloudiq.htm>.
10. Principled Technologies, „Dell CloudIQ provides a single console for proactive monitoring and had negligible impact on network bandwidth in our tests”, dostęp 17 stycznia 2024 r., <https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf>.
11. Supermicro, „X13DEM User's Manual”, dostęp 16 lutego 2024 r., <https://www.supermicro.com/manuals/motherboard/X13/MNL-2407.pdf>.
12. Dell, „OpenManage Enterprise”, dostęp 20 grudnia 2023 r., <https://www.dell.com/en-us/work/learn/openmanage-enterprise>.
13. Principled Technologies, „A Dell PowerEdge MX environment using OpenManage Enterprise and OpenManage Enterprise Modular can make life easier for administrators”, dostęp 17 stycznia 2024 r., <https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf>.
14. „Integrated Dell Remote Access Controller (iDRAC)”, dostęp 16 stycznia 2024 r., <https://www.dell.com/en-us/lp/dt/openmanage-idrac>.

Przeczytaj informacje naukowe zawarte w tym raporcie



Facts matter.®

Principled Technologies jest zarejestrowanym znakiem towarowym firmy Principled Technologies, Inc. Pozostałe nazwy produktów są znakami towarowymi odpowiednich właścicieli. Aby uzyskać dodatkowe informacje, zapoznaj się z danymi naukowymi zawartymi w tym raporcie.