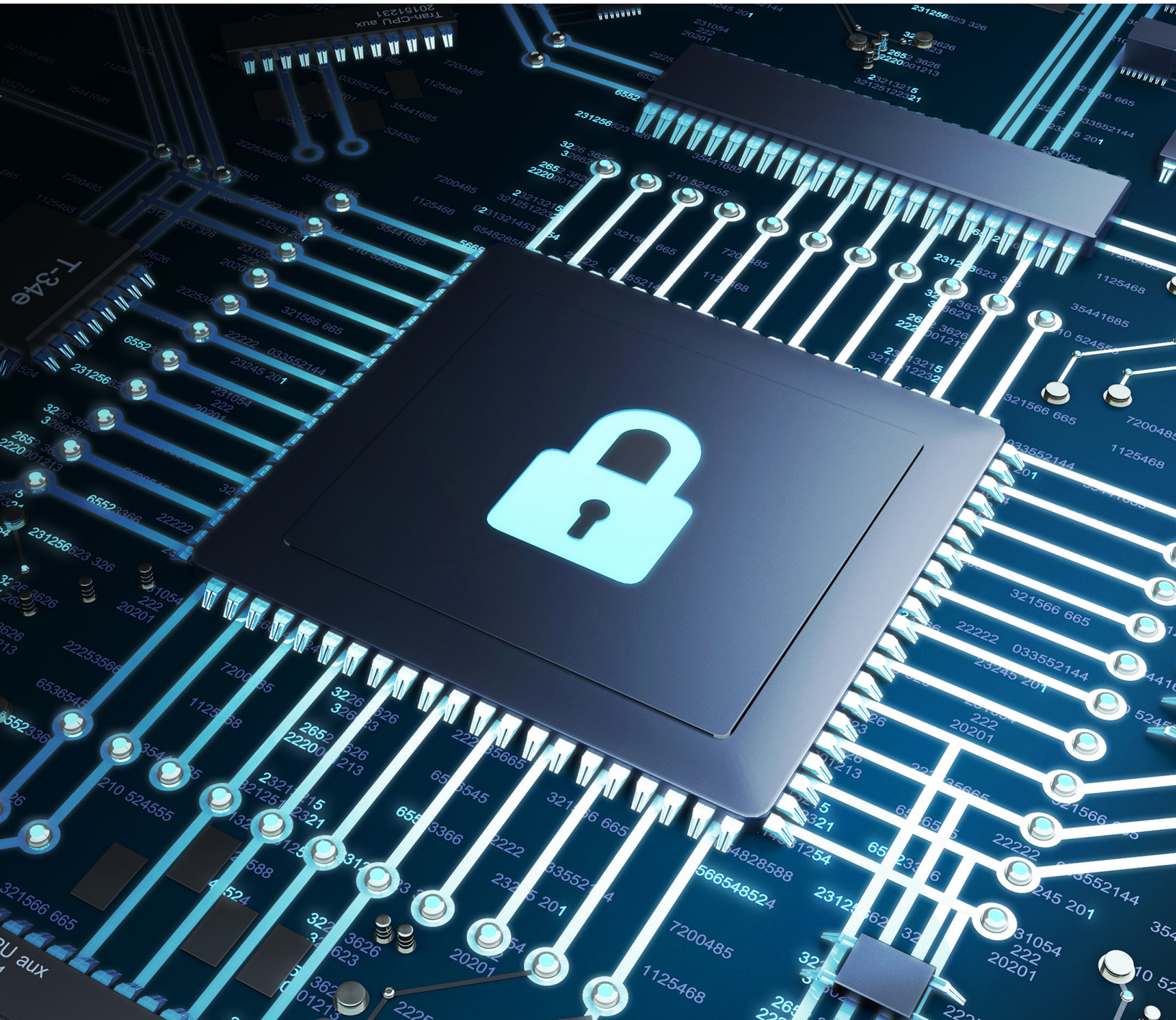
DELL Technologies

Microsoft

Opracowanie

Wzmocnienie kompleksowych zabezpieczeń danych dzięki Microsoft SQL Server, serwerom Dell™ PowerEdge™ i systemowi Windows Server 2022



W związku z masowym przejściem na pracę zdalną w wielu sektorach firmy dostosowują się do nowej normalności oraz bezpieczeństwo staje się priorytetem bardziej niż kiedykolwiek wcześniej. W 2021 roku większość liderów biznesu stwierdziła, że w dającej się przewidzieć przyszłości praca zdalna będzie kontynuowana[1]. Ze względu na większą niż kiedykolwiek liczbę pracowników rozproszonych geograficznie na większym niż kiedykolwiek obszarze oraz dużą liczbę podatnych na ataki punktów końcowych, menedżerowie IT przedsiębiorstw muszą przyjąć bardziej holistyczne podejście do bezpieczeństwa.

88% ankietowanych liderów IT spodziewa się, że jakaś forma pracy zdalnej będzie kontynuowana, a korzystanie z wielu repozytoriów treści prawdopodobnie pozostanie problemem w perspektywie krótkoterminowej[1].

Zespoły IT mogą poprawić bezpieczeństwo danych w całym przedsiębiorstwie, stosując podejście „całego stosu" w centrum danych: od sprzętu przez aplikację bazy danych po system operacyjny. Modernizacja infrastruktury i konsolidacja danych w najnowszej wersji platformy Microsoft SQL Server na serwerach Dell™ PowerEdge™ i Windows Server 2022 zapewnia przedsiębiorstwom solidną podstawę kompleksowej ochrony danych w zmieniającym się środowisku pracy.

Dzisiejsze wyzwania dla przedsiębiorstw związane z bezpieczeństwem

Gwałtowny rozwój pracy zdalnej sprawił, że przedsiębiorstwa są jeszcze bardziej narażone na wcześniejsze cyberataki:

- **Gwałtowny wzrost ilości treści.** Gwałtowny wzrost ilości treści jest naturalną konsekwencją wieloletniego dostępu wielu pracowników do danych i aplikacji przedsiębiorstwa oraz korzystania z nich. Dane są przechowywane w różnych lokalizacjach i w wielu repozytoriach. A ich ilość wciąż rośnie. IDC szacuje, że w ciągu najbliższych pięciu lat ilość danych będzie nadal rosła w tempie 24 procent skumulowanej rocznej stopy wzrostu (CAGR)[2]. Ponad połowa ankietowanych liderów IT (52%) twierdzi, że ich firmy mają co najmniej 10 repozytoriów plików[1]. Podobnie jak posiadanie wielu przedmiotów w domu może prowadzić do bałaganu i ryzyka utraty, treści zapisane lub zduplikowane na wielu serwerach i w wielu bazach danych mogą stanowić zagrożenie dla danych.

41% liderów IT twierdzi, że ich głównym zmartwieniem związanym z rozrastaniem się ilości treści jest większe ryzyko naruszenia i wycieku danych[1].

- **Osobiste urządzenia pracowników (BYOD) i zjawisko shadow IT.** Większe zagrożenie bezpieczeństwa wynikające z rozrastania się treści jest potęgowane przez zasady związane z osobistymi urządzeniami pracowników (BYOD), zgodnie z którymi organizacje zezwalają na korzystanie z osobistych smartfonów i tabletów do pracy. Urządzenia te mogą nie być regularnie aktualizowane za pomocą najnowszych poprawek zabezpieczeń oraz mogą być używane w niezabezpieczonych sieciach Wi-Fi. „Zjawisko shadow IT", czyli poleganie na samozwańczych funkcjach bezpieczeństwa aplikacji opartych na chmurze, to kolejny potencjalny wektor ataku dla hakerów ze względu na nieodłączny brak wewnętrznej kontroli i widoczności.
- **Różne harmonogramy poprawek zabezpieczeń.** Wiele organizacji używa oprogramowania SQL Server jako platformy danych, ale z czasem kończą z różnymi wersjami oprogramowania baz danych, co komplikuje zarządzanie danymi i łatanie zabezpieczeń. A ponieważ poprawki mogą spowolnić działanie systemów i wymagać przestoju serwera, zespoły IT muszą określić idealny czas na wprowadzenie poprawek dla każdej wersji, co może opóźniać aktualizacje.
- **Różne poziomy dostępu pracowników.** Administratorzy IT muszą starać się zachować ustawienia uprawnień, gdy pracownicy są zatrudniani lub odchodzą z organizacji. Jeśli nie zostaną odpowiednio skonfigurowane lub zaktualizowane w odpowiednim czasie, ktoś w organizacji może przypadkowo lub celowo narazić dane firmy i klienta na ataki typu ransomware i hakerów.

Modernizacja zarządzania danymi na bezpiecznym fundamencie

Obsługa programu SQL Server na serwerach Dell PowerEdge i w systemie Windows Server 2022 pomaga administratorom IT przezwyciężyć te problemy i zabezpieczyć obciążenia robocze o znaczeniu krytycznym dla działalności w ramach nowoczesnej infrastruktury na poziomie sprzętu, systemu operacyjnego (OS) i oprogramowania.

65% dyrektorów działów IT i innych liderów IT podejrzewa, że pliki i dokumenty zawierające poufne informacje są zapisywane lokalnie na urządzeniach osobistych pracowników[1].

Serwery Dell PowerEdge

Serwery Dell PowerEdge pomagają przedsiębiorstwom bronić się przed zagrożeniami związanymi z dzisiejszym środowiskiem dzięki bezpiecznej infrastrukturze obsługującej pełen zakres nowoczesnych obciążeń roboczych i celów. Serwery PowerEdge zostały zaprojektowane z myślą o szybszym wdrażaniu i zwiększeniu wydajności aplikacji bazodanowych, systemów obliczeniowych o wysokiej wydajności (HPC), środowisk wirtualizacji i obliczeń brzegowych. Narzędzia Dell™ OpenManage™ umożliwiają administratorom IT łatwe i skuteczne zarządzanie dużymi klastrami.

Serwery PowerEdge są zbudowane na niezmiennym, opartym na technologii krzemowej źródle zaufania i umożliwiają korzystanie z funkcji zabezpieczeń, takich jak kompleksowa weryfikacja rozruchu, w tym dostosowywanie bezpiecznego rozruchu interfejsu UEFI (Unified Extensible Firmware Interface), zaufany system BIOS, łańcuch zaufania oprogramowania wewnętrznego i zweryfikowany program ładujący systemu operacyjnego. Oprogramowanie wewnętrzne jest chronione zgodnie z wytycznymi National Institute of Standards and Technology (NIST), łącznie z podpisanymi aktualizacjami oprogramowania wewnętrznego, a zarządzanie certyfikatami jest uproszczone dzięki automatycznemu odnawianiu.

Serwery PowerEdge zapewniają również ochronę danych w stanie spoczynku przy użyciu rozwiązania SEKM (Secure Enterprise Key Manager) oraz ochronę danych w użyciu za pomocą technologii procesora do poufnego przetwarzania. Aby ograniczyć zagrożenia, takie jak podrobione komponenty, złośliwe oprogramowanie i ingerencje w oprogramowanie wewnętrzne, firma Dell Technologies stosuje kompleksowe podejście do bezpieczeństwa łańcucha dostaw, wdrażając narzędzia do unikania fałszerstw, kontroli pochodzenia produktu, podpisywania kodów, włamywania się do obudowy i zabezpieczania opakowań w sposób umożliwiający manipulację. Ponadto funkcja Secured Component Verification (SCV) zwiększa bezpieczeństwo łańcucha dostaw poprzez weryfikację integralności komponentów serwera.

Firma Dell Technologies, jeden z największych partnerów firmy Microsoft, ściśle współpracuje z nią od prawie czterdziestu lat, opracowując najlepsze w branży zabezpieczone rozwiązania sprzętowe i programowe. W ramach tej współpracy oprogramowanie firmy Microsoft, takie jak Windows Server i SQL Server, działa optymalnie na serwerach Dell PowerEdge.

Windows Server 2022

System Windows Server 2022 zawiera funkcję serwera z zabezpieczonymi rdzeniami opartą na systemie Windows, która wykorzystuje możliwości sprzętu, oprogramowania wewnętrznego i systemu operacyjnego w celu ochrony przed obecnymi i przyszłymi zagrożeniami. Serwery z zabezpieczonymi rdzeniami wykorzystują obsługę technologii DRTM (Dynamic Root of Trust for Measurement) w celu odizolowania oprogramowania wewnętrznego, dzięki czemu poziom prawdopodobieństwa wpływu na kod oprogramowania wewnętrznego ze strony dowolnego rodzaju naruszeń jest dużo niższy. Ponadto zabezpieczenia oparte na wirtualizacji (VBS) izolują krytyczne części systemu operacyjnego, takie jak jądro, od reszty systemu w celu ochrony aplikacji i danych, jednocześnie zapewniając koncentrację serwerów na obsłudze krytycznych obciążeń roboczych.

Te funkcje zabezpieczonego rdzenia umożliwiają aktywną obronę i zakłócenie działania wielu ścieżek, które atakujący mogą wykorzystać do ingerencji w systemy. Serwery z zabezpieczonymi rdzeniami obsługują wiele technologii zabezpieczeń firmy Microsoft. Wiele z nich stanowi również ich wyposażenie standardowe, w tym integralność kodu chroniona przez monitor maszyny wirtualnej w VBS, moduł TPM (Trusted Platform Module) 2.0, szyfrowanie dysków funkcją BitLocker i bezpieczny rozruch UEFI.

Więcej informacji na temat funkcji zaawansowanej ochrony systemu Windows Server 2022 na serwerach Dell PowerEdge można znaleźć w opracowaniu „Uzyskaj zaawansowaną ochronę bezpieczeństwa dzięki połączeniu możliwości systemu Windows Server 2022 i serwerów Dell EMC PowerEdge nowej generacji”.

Ochrona danych na poziomie aplikacji bazodanowych

Program SQL Server został stworzony z myślą o bezpieczeństwie. Jednak, jak wspomniano wcześniej, wiele przedsiębiorstw korzysta z kilku wersji oprogramowania SQL Server, a działy IT poszukują prostszej, skonsolidowanej strategii dotyczącej baz danych.

Ponadto rozszerzona pomoc techniczna dla oprogramowania SQL Server 2012 kończy się w lipcu 2022 r., co sprawia, że pilniejszym problemem jest konsolidacja baz danych w najnowszej wersji SQL Server. Mimo tego, że starsze wersje baz danych SQL Server będą nadal działać, to jednak w przypadku problemów nie będzie dostępna poprawka obsługiwana przez producenta. Poprawki lub aktualizacje zabezpieczeń również nie będą dostarczane, co może narazić systemy na złośliwe ataki.

Najprostszą i najbardziej praktyczną ścieżką do konsolidacji dla wielu przedsiębiorstw jest uaktualnienie programu SQL Server do najnowszej wersji i uruchomienie starszych wersji w trybie zgodności. Administratorzy baz danych mogą po prostu utworzyć kopię zapasową starszej bazy danych SQL Server, a następnie załadować ją i uruchomić w SQL Server 2019/2022 w trybie zgodności. Takie podejście może być szybkim i prostym sposobem uaktualnienia, jeśli pełne testowanie regresji nie jest konieczne. SQL Server 2019 (z poziomem zgodności 150) może obsługiwać wersje do SQL Server 2008 R2 (poziom zgodności 100).

Najlepsze praktyki w zakresie bezpieczeństwa

Aby dodatkowo chronić dane, zespoły IT mogą chcieć upewnić się, że postępują zgodnie z najlepszymi rozwiązaniami w zakresie zabezpieczeń programu SQL Server (aby uzyskać więcej informacji na temat tych najlepszych rozwiązań i sposobów ich wdrażania, przeczytaj wpis w blogu firmy Microsoft „Securing SQL Server"). Te najlepsze praktyki w zakresie bezpieczeństwa dotyczą wszystkich poziomów infrastruktury centrum danych, w tym sprzętu i systemu operacyjnego, oraz obejmują:

- **Zwiększenie bezpieczeństwa fizycznego.** Zabezpieczenia fizyczne ściśle ograniczają dostęp do fizycznego serwera i komponentów sprzętowych. Oznacza to korzystanie z zamkniętych pomieszczeń z ograniczonym dostępem do serwerów i urządzeń sieciowych. Dostęp do nośników kopii zapasowych jest ograniczony przez przechowywanie ich w bezpiecznej lokalizacji zewnętrznej. Zalecane jest podejście warstwowe: uniemożliwianie dostępu lub wymaganie karty/zgody na obwodzie obiektu, na obwodzie budynku, wewnątrz budynku i pomieszczeniach centrum danych.
- **Utrzymywanie aktualności systemu operacyjnego.** Dodatki Service Pack i uaktualnienia systemu operacyjnego zawierają ważne udoskonalenia zabezpieczeń. Aktualizacje i uaktualnienia systemu operacyjnego mogą być stosowane po przetestowaniu ich z aplikacjami bazodanowymi.
- **Korzystanie z zapór sieciowych.** Zapory sieciowe zwiększają bezpieczeństwo na poziomie systemu operacyjnego, zapewniając punkt kontrolny, w którym można skoncentrować środki bezpieczeństwa.
- **Zmniejszenie powierzchni.** Należy ograniczać obszary, które są narażone na naruszenia, wyłączając fizycznie lub programowo funkcje i komponenty, które nie są używane. Powierzchnię programu SQL Server można zmniejszyć, uruchamiając wymagane usługi, o „najniższych uprawnieniach" i które przyznają usługi i prawa użytkowników na odpowiednim poziomie.
- **Wdrożenie kontroli dostępu opartej na rolach (RBAC) do „zabezpieczanych elementów"**[3]. Zabezpieczane elementy obejmują takie komponenty, jak serwer, baza danych i obiekty, które baza danych zawiera. Zabezpieczone elementy to zasoby, do których dostęp jest regulowany przez system autoryzacji aparatu bazy danych programu SQL Server.
- **Szyfrowanie danych na wszystkich poziomach.** Obejmuje to szyfrowanie danych aplikacji i pamięci masowej.
- **Tworzenie i używanie certyfikatów.** Certyfikaty to klucze programowe, które umożliwiają dwóm serwerom bezpieczną komunikację. W programie SQL Server certyfikaty zwiększają bezpieczeństwo obiektów i łączności.
- **Ograniczenie dostępu do plików systemu operacyjnego używanych przez program SQL Server.**
- **Używanie silnych haseł w całej organizacji.** Jest to prosta, ale często niedoceniana praktyka bezpieczeństwa.
- **Przeprowadzanie audytów.** Upewnij się, że odzyskiwanie danych po utworzeniu kopii zapasowej działa zgodnie z oczekiwaniami i że dostęp jest odpowiednio kontrolowany.
- **Korzystanie z programu Microsoft Defender dla baz danych SQL Server.** Microsoft Defender dla baz danych SQL Server skanuje bazy danych w poszukiwaniu luk w zabezpieczeniach. Wykrywają anomalie, które wskazują na nietypowe i potencjalnie szkodliwe próby uzyskania dostępu do baz danych lub ich wykorzystania. Anomalie te obejmują podejrzane działania bazy danych, potencjalne luki w zabezpieczeniach, ataki polegające na wstrzyknięciu kodu SQL oraz nietypowe wzorce dostępu do bazy danych i zapytań.

Wreszcie każda nowa wersja SQL Server zawiera nowe funkcje zabezpieczeń, które zwiększają ochronę danych. Nowa funkcja rejestru, zapowiedziana dla SQL Server 2022, pomaga chronić integralność danych, tworząc niezmienny rejestr modyfikacji danych w czasie. Może to pomóc w ochronie danych przed manipulacją przez złośliwe podmioty i jest korzystne w scenariuszach, takich jak audyty wewnętrzne i zewnętrzne.

Rejestr SQL Server

- Używa niezmiennego rejestru w celu ochrony danych przed manipulacją przez złośliwe podmioty
- Ustanawia cyfrowe zaufanie w scentralizowanym systemie wykorzystującym technologię blockchain
- Poświadcza brak naruszeń integralności danych względem innych podmiotów

Konsolidacja i ochrona — od sprzętu po bazę danych

Rola IT będzie rosła wraz ze wzrostem ilości danych w cyfrowym przedsiębiorstwie. A ponieważ temu bogactwu danych towarzyszą coraz sprytniejsze i częstsze cyberataki, zespoły IT powinny przyjąć strategię bezpieczeństwa danych, która pomoże chronić infrastrukturę na wszystkich poziomach. Uaktualnienie systemów SQL Server i Windows Server na serwerach Dell PowerEdge do najnowszej wersji może pomóc firmom w ochronie wrażliwych danych firmy i klientów.

Postaw bezpieczeństwo swojej infrastruktury na pierwszym miejscu. Dowiedz się więcej w jaki sposób rozwiązania firm Dell i Microsoft mogą pomóc: www.dell.com/en-us/dt/solutions/microsoft-data-platform/index.htm.

Przeczytaj „Uzyskaj zaawansowaną ochronę bezpieczeństwa dzięki połączeniu możliwości systemu Windows Server 2022 i serwerów Dell EMC PowerEdge nowej generacji”.

[1] Egnyte. „2021 Data Governance Trends: Predictions, pitfalls and technologies for the future of digital work”. 2021. www.egnyte.com/sites/default/files/2021-09/2021DataGovernanceTrendsReport.pdf.
[2] IDC. „Data Creation and Replication Will Grow at a Faster Rate than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts”. Marzec 2021 r.
[3] Aby uzyskać więcej informacji o elementach zabezpieczanych, przeczytaj https://docs.microsoft.com/en-us/sql/relational-databases/security/securables.

DELL Technologies

Microsoft

Przeprowadź modernizację z użyciem systemu Windows Server 2022. Gotowy do pracy w chmurze system operacyjny, który zwiększa wartość inwestycji lokalnych dzięki możliwościom hybrydowym.