SCALITY

Fast IT solutions

ARKUSZ ROZWIĄZANIA

Izolowane kopie zapasowe w Scality ARTESCA

Niektóre firmy wymagają, aby nośniki ich kopii zapasowych były fizycznie odizolowane od reszty sieci, co ma zapewnić poziom bezpieczeństwa podobny jak w przypadku fizycznego usunięcia taśmy z biblioteki. I choć taśmy z natury pozwalają łatwo uzyskać taki poziom izolacji danych, wprowadza to również komplikacje operacyjne związane z zarządzaniem nośnikami i ich fizyczną obsługą.

Kopie zapasowe przechowywane na taśmach są zapisywane sekwencyjnie, ale ich przywracanie następuje z różnych fragmentów danych zapisanych w wielu kopiach zapasowych. Takie rozwiązanie prowadzi do częstego zatrzymywania czytników i przewijania taśm, a co za tym idzie — spowalnia proces przywracania. Dane zapisane na taśmie są często replikowane na dwóch dyskach, ponieważ nie ma gwarancji, że będą one zawsze czytelne i dostępne na nośnikach taśmowych.

Firmy preferują korzystanie z rozwiązań opartych o dyski — takich jak ARTESCA — które pozwalają na natychmiastowe i szybkie tworzenie i przywracanie kopii. Rozwiązania oparte na dyskach są bardziej wydajne w procesie ochrony danych, zawsze przeprowadzają kontrole CRC w tle i przechowują dane wraz z kodowaniem wymazywania, co zapewnia najwyższą trwałość danych.

Jak Scality ARTESCA chroni dane poprzez izolację?

ARTESCA to rozwiązanie zbudowane w oparciu o najsilniejsze reguły bezpieczeństwa danych i zasadę zerowego zaufania, które powstało, by sprostać stale zmieniającym się potrzebom w dziedzinie ochrony danych. ARTESCA oferuje znacznie większe korzyści niż tylko niezmienność danych osiąganą za pomocą S3 Object Lock, dzięki czemu zapewnia kompleksową odporność cybernetyczną zgodną z podejściem CORE5.

Niezmienność danych i funkcja S3 Object Lock pozwalają osiągnąć taki sam logiczny poziom ochrony, jak w przypadku fizycznego odłączenia nośnika danych od reszty systemu. Zabezpieczenie obiektów kopii zapasowych przed zmianami chroni je przed usunięciem lub modyfikacją do momentu, gdy aplikacja nie będzie ich już potrzebować. Mimo to w niektórych organizacjach panują rygorystyczne zasady, które wymagają fizycznego izolowania kopii zapasowych — tak jak ma to miejsce w przypadku taśm.

W ramach podejścia CORE5 do kompleksowej odporności cybernetycznej ARTESCA obsługuje izolowanie danych na poziomie samej architektury. Aby to zademonstrować, musimy najpierw zrozumieć samą architekturę sieciową ARTESCA.

ARTESCA — łączność

Najpierw przyjrzyjmy się architekturze dostępu do sieci ARTESCA.

System został zaprojektowany z uwzględnieniem trzech różnych punktów dostępu do sieci, co pozwala na rzeczywistą segregację sieci na potrzeby różnych rodzajów ruchu. Takie podejście zapewnia najwyższy poziom bezpieczeństwa sieciowego.

Dostęp frontend

Jest to rodzaj dostępu, jaki ARTESCA zapewnia do aplikacji, która działa w sieci produkcyjnej. Jedynymi usługami dostępnymi w sieci frontend są punkty końcowe S3 — w ten sposób aplikacje łączą się z ARTESCA, aby korzystać z pamięci masowej rozwiązania. Punkt końcowy jest domyślnie chroniony protokołem HTTPS na porcie 443, a w tej sieci nie istnieją żadne procesy nasłuchujące.

Po nawiązaniu połączenia za pośrednictwem HTTPS dostęp do danych odbywa się ze standardowymi ograniczeniami bezpieczeństwa AWS: AWS Authentication v4 oraz koncepcjami kont, użytkowników i grup IAM. Dostęp do dowolnego zasobu pamięci masowej w ARTESCA jest kontrolowany przez parę klucz dostępu/klucz tajny kontrolowaną przez administratora systemu. Ponadto dostęp do punktów końcowych ARTESCA może być ograniczony na poziomie IAM do określonego źródłowego adresu IP lub zakresu adresów — takich jak serwer kopii zapasowych.

Sieć administracyjna

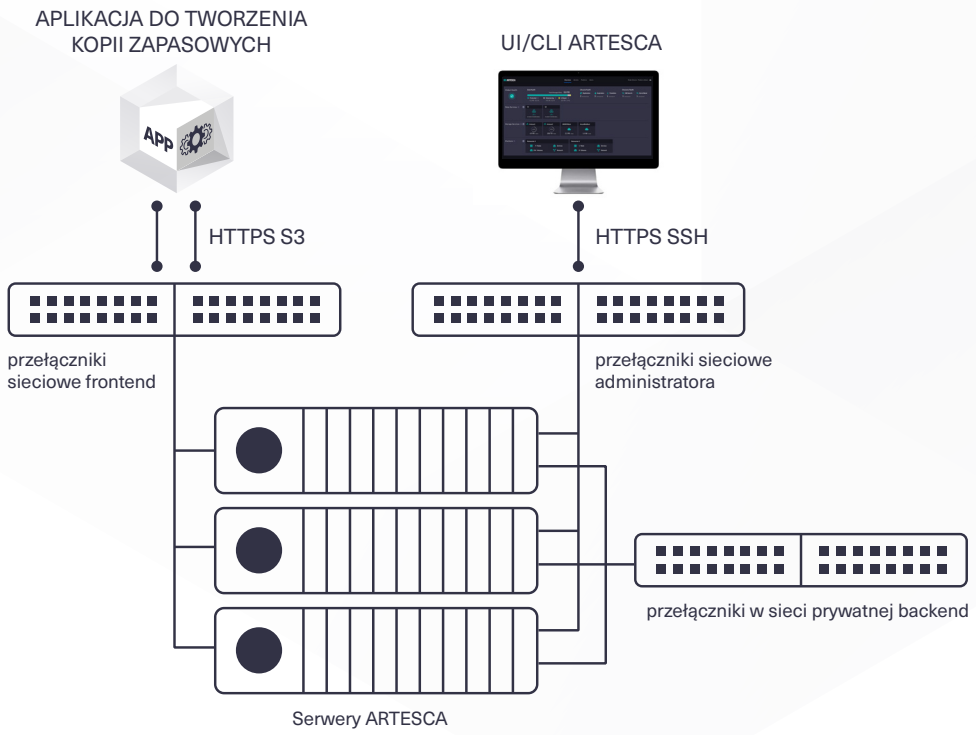
Sieć administracyjna jest potrzebna administratorowi systemu ARTESCA do konfigurowania zasobów, zabezpieczania systemu i monitorowania jego stanu. Dostęp administratora odbywa się przez dedykowany port sieciowy i umożliwia dostęp HTTPS tylko do interfejsu GUI systemu oraz dostęp SSH do zarządzania CLI.

Dostęp do interfejsu użytkownika dla administratorów, którzy muszą monitorować system lub nim zarządzać, jest chroniony za pomocą uwierzytelniania wieloskładnikowego (MFA). Takie rozwiązanie chroni konto przed typowymi zdarzeniami związanymi z bezpieczeństwem, takimi jak naruszenia hasła, ataki brute force, keylogging, ataki man-in-the-middle i inżynieria społeczna. Za dostęp użytkowników do funkcji systemu odpowiada kontrola dostępu oparta na rolach (RBAC), która przyznaje uprawnienia administratora wyłącznie osobom, które tego potrzebują.

Komunikacja backend

W wieloserwerowym rozwiązaniu ARTESCA komunikacja między serwerami odbywa się za pośrednictwem dedykowanej, izolowanej sieci wewnętrznej, która przenosi tylko wewnętrzny ruch ARTESCA — taki jak kodowania wymazywania sieci, zarządzanie klastrami Kubernetes i informacje sprawozdawcze.

Żadne inne urządzenie sieciowe nie może uzyskać dostępu do tej sieci prywatnej — izolacja jest osiągana za pomocą dedykowanych przełączników fizycznych lub, jeśli nie są one dostępne, poprzez tagowanie VLAN. Najlepsza praktyka nakazuje stosowanie dwóch przełączników w celu osiągnięcia redundancji, która zapewni ciągłość usługi w przypadku awarii jednego przełącznika. Domyślnie procesy Kubernetes są chronione za pomocą zautomatyzowanych wbudowanych zapór sieciowych, co dodatkowo zabezpiecza system. W przypadku używania jednoserwerowej konfiguracji ARTESCA nie ma potrzeby korzystania z sieci wewnętrznej.



Tworzenie kopii zapasowych z użyciem ARTESCA

Teraz, gdy już znamy możliwości sieciowe rozwiązania ARTESCA, możemy sprawdzić, jak tworzyć odizolowane kopie zapasowe. Do sterowania procesem potrzebny jest skrypt utworzony przez integratora systemu. Skrypt ten będzie opierał się na możliwościach zarządzania dostawcy przełącznika. Będzie on uruchamiany przez aplikację do tworzenia kopii zapasowych i będzie obejmował następujące etapy:

- Otwarcie portów przełącznika kontrolujących dostęp do punktów końcowych frontend S3 rozwiązania ARTESCA
- Rozpoczęcie tworzenia kopii zapasowej
- Odczekanie, aż zadanie dobiegnie końca
- Zamknięcie portów przełącznika frontend ARTESCA

Takie podejście gwarantuje, że klaster ARTESCA pracuje w trybie online tylko podczas tworzenia kopii zapasowych. Przez pozostały czas jest on hermetycznie odizolowany od reszty sieci.

ARTESCA — administracja

Domyślnie w rozwiązaniu odizolowanym dostęp administratora do systemu uniemożliwia zamknięty port sieciowy. Gdy administrator systemu potrzebuje uzyskać dostęp do ARTESCA w celu zarządzania zadaniami — takimi jak konfigurowanie nowych zasobów lub sprawdzanie stanu systemu — można otworzyć porty na przełączniku sieciowym używanym do zarządzania.

Podsumowanie

Zastosowana architektura daje całkowitą kontrolę nad tym, kto może połączyć się z odizolowanym klastrem ARTESCA w celu zarządzania nim, a w razie potrzeby pozwala zastosować niezwykle szczegółowe zasady bezpieczeństwa. Takie rozwiązanie zapewnia również organizacji korzyści płynące z dyskowego systemu pamięci masowej opartego na obiektach, który pozwala osiągnąć czołowe w branży czasy przywracania danych oraz najwyższy poziom odporności cybernetycznej.

SCALITY

Odwiedź stronę **www.scality.com** E-mail **ARTESCA@scality.com** San Francisco • Paryż • Waszyngton • Tokio • Londyn