Ogólne rekomendacje Dell Technologies w zakresie cyberbezpieczeństwa przetwarzania aplikacji oraz baz danych

Wstęp

Środowiska dedykowane do przetwarzania danych i aplikacji charakteryzuje kilka popularnych i kluczowych parametrów:

- Bezpieczeństwo
- Wydajność – mierzona jako IOPS i czas odpowiedzi lub przepustowość strumienia danych
- Wymagana pojemność – niezależnie czy ma to być pojemność z, czy bez redukcji danych – tzw. deduplikacja i kompresja danych
- Parametry SLA
- Możliwości rozbudowy wydajności i pojemności
- Zakres i czas trwania wsparcia technicznego

Powyższe wymagania można zaadresować na dwa poniżej wskazane sposoby przy czym, w niniejszym dokumencie Dell Technologies skupia się wyłącznie na kwestiach związanych z zapewnieniem cyberbezpieczeństwa przetwarzania danych w obszarze systemów pamięci masowych

- Dobierając odpowiednią architekturę rozwiązania
- Wybierając technologie pozwalające na zwiększenie bezpieczeństwa przetwarzania danych

Architektura

Architektura rozwiązania jest dobierana w zależności od wymaganego SLA opisanego parametrami RTO (Recovery Time Objective – czyli jak szybko chcemy wznowić przetwarzanie po awarii) i RPO (Recovery Point Objective – z jak dużą utratą danych godzimy się w efekcie awarii)

Zapewnienie oczekiwanego RTO

Uwaga – bardzo krótkie RTO można uzyskać jedynie, kiedy cały stos aplikacyjny posiada stosowne mechanizmy – np. w przypadku baz danych Oracle konieczne jest stosowanie klastra Active/Active Oracle RAC.

Poniżej przedstawiamy zalecenia odnośnie spełnienia RTO od najkrótszego do najdłuższego dla infrastruktury sprzętowej

1. RTO zero lub bliskie zero

    - zbudowanie geograficznie rozciągniętego klastra active/active na warstwie storage (tzw. Metro Cluster), sieci SAN lub IP i środowiska przetwarzania włącznie z całym stosem aplikacyjnym w co najmniej 2 ośrodkach przetwarzania

    - Jako parametr graniczny wymaganej wydajności łącza przyjmuje się RTT (Round Trip time, czyli czas propagacji pakietu w dwie strony między lokalizacjami) na poziomie <5ms, czyli praktycznie ok. 40 do 50km. Parametr ma charakter wysoce istotnego, ponieważ do każdego zapisu na macierz należy doliczyć ten czas.

    - Należy zwrócić uwagę na zapewnienie możliwości równoczesnego odczytu i zapisu danych do macierzy w obu lokalizacjach, aby pakiety nie musiały być przesyłane niepotrzebnie przez sieć, wprowadzając dodatkowe opóźnienia

    - O ile w przypadku awarii kluczowy jest czas przełączenia do drugiej lokalizacji (Fail-Over), to równie ważne jest zapewnienie, aby powrót do lokalizacji podstawowej (Fail-Back) nie wymagał przepisania wszystkich danych. Należy wybierać rozwiązania, które przechowują tzw. delty, czyli zapamiętują które dane się zmieniły lub przyrosły i w wyniku Fail-back dosynchronizowują tylko takie zmiany.

    - Ważne, aby również macierze dyskowe zbudowane były na bazie zwielokrotnionych kontrolerów pracujących w trybie Active/Active, aby awaria pojedynczego kontrolera nie wymagała czasu na przełączenie na kontroler zapasowy jak ma to miejsce w architekturze Active/Passive

2. RTO kilkadziesiąt sekund lub kilka minut – w wielu przepadkach jest to rozwiązanie podobne jak w przypadku pkt. 1, przy czym możliwe do zrealizowania bez zaawansowanych klastrów aplikacyjnych. Posiadając klaster active/active na warstwie storage, czas przestoju zależny jest głównie od czasu potrzebnego na uruchomienie bazy danych i aplikacji w ośrodku zapasowym. Często realizowany, poprzez przesyłanie do ośrodka tzw. redo logów i aplikowanie do bazy po awarii ośrodka podstawowego

3. RTO – kilkanaście minut do kilka godzin – rozwiązanie podobne do pkt 2, przy czym na warstwie storage nie budujemy klastra Active/Active, a korzystamy z replikacji synchronicznej (nie tracimy danych) lub asynchronicznej (możemy utracić część ostatnio wykonanych transakcji, które nie zostały przesłane przez sieć).
   Rozwiązanie możliwe do uzyskania poprzez:

    - Replikację macierzową

    - Replikację software'ową

    - Replikacją w ramach systemu backupu, który replikuje dane między ośrodkami i pozwala na uruchomienie się w zdalnej lokalizacji bezpośrednio z medium z minimalną wydajnością powyżej 1000 IOps

Jednocześnie w każdym z przypadków istotne jest czy w zdalnej lokalizacji mamy jedna kopię danych czy też mamy możliwości powrotu / odtworzenia / testowania do różnych chwil czasowych. Rekomendowane jest by można było się odtworzyć do wielu chwil czasowych których odstępy są nie rzadsze niż 15 minut.

4. RTO – kilkanaście -kilkadziesiąt godzin – wariant bez replikacji między macierzami, ale z nawet minimalną infrastrukturą serwerowo-storageową w lokalizacji zapasowej - stosujemy klasyczne odtwarzanie z kopii zapasowych – aktualna kopia zapasowa musi być dostępna w lokalizacji zapasowej, najlepiej aby była replikowana z lokalizacji podstawowej z wykorzystaniem deduplikacji i kompresji aby zoptymalizować wymaganą przepustowość łącza.

5. RTO – kilka dni-tygodni – przeważnie dla przetwarzania w jednym ośrodku, z backup tylko w tym ośrodku lub na taśmach. Przetwarzania można wznowić dopiero po usunięciu awarii uszkodzonych elementów lub ich wymiany i odtworzenia danych z kopii zapasowych. Jest to wariant, który nie powinien być stosowany dla żadnej, ważnej aplikacji lub danych.

Zapewnienie oczekiwanego RPO

Oczekiwane parametry RTO, czyli ilości danych, które możemy stracić w wyniku awarii możemy zrealizować w następujące sposoby, uporządkowane od RPO=0 do dłuższych czasów

1. RPO równe 0 możemy zrealizować replikując synchronicznie dane między macierzami dyskowymi w tej samej lokalizacji lub w dwóch ośrodkach przetwarzania odległych o maksymalnie 40km. Dla większych odległości replikacja synchroniczna powoduje odczuwalne zmniejszenie wydajności. Należy pamiętać o zapewnieniu jak najlepszego parametru RTT dla pakietów, ponieważ każdy zapis do macierzy w jednym ośrodku wymaga aby zapis ten został wysłany do drugiej macierzy, zapisany na niej, a następnie potwierdzenie wysłane zostało do ośrodka głównego. Dopiero wtedy zapis jest potwierdzany do aplikacji w podstawowym ośrodku przetwarzania. Mamy dzięki temu pewność, że zapis został dokonany w obu ośrodkach (dlatego RPO=0, czyli nie ma możliwości utraty danych) ale czas komunikacji między ośrodkami powiększa czas zapisu.

2. RPO kilka do kilkudziesięciu sekund, albo minuty – w zależności od przepustowości łączy do replikacji zapewnia replikacja asynchroniczna między macierzami. Różni się tym od pkt 1, że zapis nie musi być potwierdzony przez macierz w ośrodku zapasowym, więc odpowiedź do aplikacji jest szybsza, ale możemy stracić wszystkie zapisy, które nie zostały przesłane do drugiej macierzy przed awarią.

3. RPO kilka do kilkudziesięciu sekund do godzin - w celu lepszego zabezpieczenia aplikacji przed utratą danych stosuje się kopie migawkowe, czyli snapshot'y macierzowe, które pozwalają stworzyć kopię danych na macierzy w sposób najbardziej efektywny lub klon danych, gdzie tworzymy pełną kopię danych na macierzy, co niestety oznacza konieczność zapewnienia miejsca na przechowywanie tych kopii. Zalecane jest replikowanie tak utworzonych kopii migawkowych do drugiego ośrodka w celu zapewnienia niskiego RTO i RPO

4. RPO 15 minut do godziny– uzyskujemy stosując nowoczesne rozwiązania do tworzenia kopii zapasowych. Krótkie RPO możliwe przy częstym wykonywaniu kopii zapasowych i jednoczesnej replikacji, przy czym należy korzystać z rozwiązań backup, które nie będą zbytnio obciążały aplikacji częstym wykonywaniem kopii. Możliwe do realizacji przy systemach kopii zapasowych, które śledzą zmiany i wykonują jedynie kopię tych zmian, potrafiąc stworzyć z tych zmian i wcześniej zapisanych kopii, spójną kopię pełną wszystkich danych. Mniej zaawansowane systemy

oznaczają, że kopię zapasową wykonuje się przeważnie raz dziennie, w nocy, czyli w przypadku awarii tracimy wszystkie dane od ostatniej kopii, czyli nawet z całego dnia.

Uwagi dotyczące RPO

Należy zwrócić uwagę czy pozyskiwane rozwiązanie oferuje dostęp w zdalnej lokalizacji tylko do ostatniej kopii danych czy też mamy dostęp do wielu kopii danych. Rekomendujemy pozyskiwanie rozwiązań przechowujących wiele replik z możliwie krótkim interwałem czasowym.

Technologie

Oprócz rozwiązań wymienionych powyżej, rekomendujemy stosować technologie zawierające::

1. Szyfrowanie danych na dyskach – najbardziej optymalne są systemy pamięci masowych wyposażone w dyski SED, czyli Self-Encrypting Drive, gdzie funkcja szyfrowania realizowana jest bezpośrednio przez elektronikę dysku i nie obciąża kontrolerów macierzy

2. Mechanizmy klasy WORM, czyli ochroną przed skasowaniem danych przed upłynięciem określonego okresu lub po spełnieniu określonych parametrów. Jest to rozwiązanie szczególnie efektywne w przypadku zabezpieczania kopii migawkowych lub wersjonowania plików lub obiektów

3. Stosowanie mechanizmów WORM (Compliance) na mediach backupowych i zapewnienie w ten sposób ochrony kopii zapasowych przed ransmoware/hacker

4. Ciągłą kontrolę poprawności i spójności kopii zapasowych – jeśli kopia zapasowa ma nam gwarantować możliwość odtworzenia danych w przypadku awarii musimy mieć pewność, że w momencie jej tworzenia jest spójna z danymi produkcyjnymi, ale co najważniejsze, że podczas całego okresu jej przechowywania umożliwia odtworzenie. Najbardziej efektywne w tym zakresie są systemy przechowywania kopii zapasowych oparte o dyski, ponieważ system może nieprzerwanie monitorować stan nośników i wyliczać sumy kontrolne, a najmniej efektywne w tym obszarze są systemy oparte o taśmy magnetyczne, które charakteryzują się najniższym kosztem za TB, ale jednocześnie mają bardzo długi czas dostępu, a weryfikacja poprawności przechowywanych danych jest procesem długotrwałym i żmudnym ponieważ wymaga załadowania każdej taśmy, jej odczytania, a następnie odłożenia do swojego slotu.

5. Cyber/Isolated Recovery – czyli przechowywanie dodatkowej kopii zapasowej danych w dodatkowym ośrodku (cyfrowym bunkrze), w którym możemy zapewnić

    - Izolację sieciową od pozostałej infrastruktury
    - Gwarantowaną niezmienialność danych (WORM, Compliance)
    - Historię środowiska za ostatni miesiąc do pół roku
    - Weryfikację danych versus ransmoware
    - Automatyczny restore / testowanie

6. Fizycznie połączenie między centrum przetwarzania, a bunkrem zestawiane jest wyłącznie na czas replikacji kopii zapasowej. Rozwiązanie to chroni przed zaszyfrowaniem lub wymazaniem danych w wyniku np. ataku Ransomware, celowego działania administratora lub hakera. Zapewnia bezpieczną kopię danych z której można odtworzyć systemy. Do optymalnego wdrożenia wymagane, aby system przechowywania danych pozwalał na efektywną kompresję i deduplikację i aby replikowane były dane zdeduplikowane, aby replikacja do tak przygotowanego ośrodka była jak najkrótsza, dzięki czemu otwarcie połączenia do ośrodków podstawowych można było jak najszybciej zakończyć.