Dane aktualne na dzień: 16-05-2026 11:37

Link do produktu: https://sklep.ps.com.pl/serwer-nas-dp320-amd-r1600-1x8gb-2x8tb-8gb-ram-3y-p-350988.html

Serwer NAS DP320 AMD R1600 1x8GB 2x8TB 8GB RAM 3Y

Cena brutto	**9 564,99 zł**
Cena netto	**7 776,41 zł**
Numer katalogowy	**NBSYNNT02DP3200**
Kod producenta	**DP320**
Kod EAN	**4711174725779**
Obsługa hot-swap dysków	**Nie**
Gniazda we/wy	**2 x RJ-45 LAN**
Interfejs dysku	**SATA**
Format szerokości dysku	**3,5'' (LFF)**
Procesor	**AMD R1600 (2 rdzenie)**
Wymagania środowiskowe	**Środowisko pracy Temperatura: od 0°C do 45°C Wilgotność względna: od 8% do 80% Środowisko przechowywania Temperatura: od -20°C do 60°C Wilgotność względna: od 5% do 95%**
Waga	**2.9**
Akcesoria w zestawie	**1 jednostka główna DP320 2 dysków 3,5 SATA HDD 1 zasilacz 1 kabel zasilający 2 przewody RJ-45 LAN 1 pakiet akcesoriów 1 przewodnik szybkiej instalacj**
Wymiary	**166 × 106 × 223 mm**
Uwaga	**CE+WEEE**
Gwarancja	**36 mc.**
Interfejs sieciowy	**2 x 10/100/1000 Mbit/s**
Wbudowana pamięć RAM	**8**
Architektura sieci (switche)	**GigabitEthernet**
Certyfikaty	**FCC, CE, UKCA, BSMI, RCM, NCC, VCCI**
Rodzaj pamięci	**DDR4**
Pojemność sumaryczna wszystkich zainstalowanych dysków	**16**
Liczba zainstalowanych dysków tw.	**2**
Typ dysku	**HDD**
RAID	**Tak**

Poziomy RAID	**1**
Obudowa serw.	**Tower**
Liczba wentylatorów	**1**

Opis produktu

Odporne na cyfrowe zagrożenia rozwiązanie do ochrony danych dla punktów końcowych
Urządzenie Synology ActiveProtect DP320 to rozwiązanie do ochrony danych wstępnie skonfigurowane ze sprzętem obsługującym ActiveProtect Manager, system operacyjny zaprojektowany specjalnie do tworzenia kopii zapasowych. Dzięki możliwości wykonywania kopii zapasowych, przywracania, deduplikowania, replikacji i zarządzania przy jednoczesnym zapewnieniu bezpieczeństwa, serwer DP320 jest idealnym serwerem kopii zapasowych dla małych i średnich punktów końcowych. Bezproblemowo integruje wszystkie bieżące i przyszłe obciążenia w wielu lokalizacjach w klastry, umożliwiając scentralizowane zarządzanie za pośrednictwem jednej platformy. Dzięki niezmienności, fizycznie izolowanym kopiom zapasowym i kontroli dostępu, DP320 chroni przed atakami ransomware i chroni wszystkie dane.

Najważniejsze cechy

- Szybkie wdrożenie: Konfiguracja serwera w kilka minut
- Zabezpieczenie wszystkich obciążeń: Ochrona maszyn wirtualnych, SaaS, baz danych, serwerów fizycznych i innych
- Widoczność: Monitorowanie stanu serwerów i kopii zapasowych na scentralizowanej platformie
- Niezawodne tworzenie kopii zapasowych: Sprawdzanie kopii zapasowych i testowanie planu odzyskiwania po awarii w środowisku piaskownicy
- Elastyczne odzyskiwanie: Odzyskiwanie na poziomie plików lub natychmiastowe przywracanie P2V/V2V w celu osiągnięcia potrzebnego docelowego RTO
- Ochrona przed oprogramowaniem ransomware: Wykorzystywanie globalnej deduplikacji po stronie źródła i specjalistyczny silnik tworzenia kopii zapasowych
- Zoptymalizowana wydajność tworzenia kopii zapasowych: Odzyskiwanie na poziomie plików lub natychmiastowe przywracanie P2V/V2V w celu osiągnięcia potrzebnego docelowego RTO
- Zabezpieczenie danych: Implementowanie najniższych uprawnień dzięki kontroli dostępu, zaporze i izolacji w celu osiągnięcia solidnej architektury

Szybkie i bezproblemowe wdrażanie
Podstawowa konfiguracja, taka jak partycjonowanie dysków i konfiguracja macierzy RAID, jest przeprowadzana automatycznie, dzięki czemu wdrożenie jest szybkie i łatwe, a ochronę danych można rozpocząć natychmiast.

Ochrona obciążeń za pomocą określonych zasad Chroń wszystkie obciążenia, w tym VMware vSphere, Microsoft Hyper-V, Windows, macOS, Linux, NetApp ONTAP, Pliki Nutanix, usługi Microsoft 365, Oracle Database, i Microsoft SQL Server. Ustal zasady dla firm w celu spełnienia wymagań SLA i zautomatyzuj ochronę danych poprzez wykrywanie istniejących i przyszłych obciążeń, zapewniając, że zostaną zabezpieczone zgodnie z odpowiednimi zasadami. W prosty sposób przeglądaj i modyfikuj zasady oraz zarządzaj nimi.

Niezawodne tworzenie kopii zapasowych i elastyczne odzyskiwanie danych
Urządzenie DP320 obsługuje funkcję automatycznej naprawy z ciągłym wykrywaniem cichego uszkodzenia danych za pomocą sumy kontrolnej Btrfs. Zapewnia brak błędów poprzez naprawę uszkodzonych danych za pomocą technologii RAID. Aby zweryfikować możliwość odzyskania danych z kopii zapasowych, można regularnie przeprowadzać testowe odzyskiwanie po awarii w środowisku piaskownicy, bez wpływu na główne miejsce produkcji. Dostępna jest również weryfikacja kopii zapasowej, która automatycznie generuje testowe pliki wideo z odzyskiwania dla celów audytu. W przypadku awarii dane mogą być elastycznie przywracane w oparciu o cele czasu odzyskiwania (RTO) za pomocą przywracania całego urządzenia, odzyskiwania na poziomie plików, metod przywracania danych fizycznych do wirtualnych (P2V) lub wirtualnych do wirtualnych (V2V) do wyznaczonej lokalizacji.

Bezkompromisowa ochrona przed oprogramowaniem ransomware
Aby zapobiec atakom ransomware, DP320 chroni kopie zapasowe danych i kopie zapasowe z niezmiennością i pamięcią WORM (Write-Once-Read-Many), aby zapewnić, że nikt nie będzie mógł zmodyfikować danych, które zostały utworzone w określonym okresie przechowywania. Ponadto integruje funkcje szyfrowania, umożliwiając szyfrowanie danych lokalnie przed utworzeniem kopii zapasowej w zdalnych miejscach docelowych. Aby jeszcze bardziej zwiększyć bezpieczeństwo, można również fizycznie odizolować zdalne środowisko.

Zoptymalizowana wydajność tworzenia kopii zapasowych
Serwer DP320 optymalizuje alokację miejsca na dysku poprzez integrację sprzętu i oprogramowania. Dzięki optymalizacji organizacji danych i konsolidacji wielu plików w jeden obraz przyspiesza przetwarzanie danych. Zarówno kopie zapasowe i ich kopie wykorzystują globalną deduplikację po stronie źródła, ponieważ porównuje dane u źródła i przesyła tylko niezduplikowane dane, aby zaoszczędzić przepustowość i przestrzeń dyskową.

Bezpieczeństwo danych u podstaw

Mechanizm bezpieczeństwa urządzenia DP320 opiera się na zasadzie uwierzytelniania na najniższym poziomie uprawnień i architekturze ochrony sieci. Mechanizm ten umożliwia dostęp do danych tylko upoważnionemu personelowi, ogranicza dostęp do określonych urządzeń oraz dostęp do infrastruktury kopii zapasowych w wyznaczonych godzinach, aby zapewnić bezpieczeństwo danych.

- W przypadku upoważnionego personelu: Integracja z usługą Active Directory, LDAP i SAML 2.0 umożliwia przedsiębiorstwom korzystanie z istniejącego SSO z uprawnieniami MFA i granulowanymi w celu zwiększenia kontroli dostępu.
- W przypadku urządzeń: Ustawienia zapory można skonfigurować tak, aby zezwalały na dostęp tylko z urządzeń w określonych zakresach IP i podsieciach. Wbudowany port zarządzania jest izolowanym interfejsem przeznaczonym do celów zarządzania. Jest on oddzielony od przepływu danych w celu zmniejszenia zagrożeń bezpieczeństwa.
- Zwiększona izolacja: Zabezpiecz zdalną infrastrukturę kopii zapasowych za pomocą rozwiązań umożliwiających osiągnięcie izolacji sieciowej lub fizycznej. Ogranicz dostęp do sieci do określonych godzin lub ustaw włączanie i wyłączanie urządzeń.