

Datenblatt



ActiveProtect Appliance

DP320

Synology

ActiveProtect Appliance

DP320



Leistungsstarke Datenschutzlösung für Edge- und Zweigstellen

Das Synology ActiveProtect DP320 ist ein speziell entwickeltes Backup-Gerät für Zweigstellen, Remote-Niederlassungen, Einzelhandelsstandorte oder Managed Service Provider (MSPs). Das DP320 kann als Edge-Server eingesetzt und dabei von ActiveProtect-Geräten wie dem DP7400, DP7200 oder DP5200 verwaltet werden. Als kompaktes Desktop-Gerät können Unternehmen lokale Datensicherungen oder Sicherungskopien speichern und Daten auch mit begrenzten Ressourcen schnell wiederherstellen. Das DP320 wird mit vorkonfigurierter Hardware und Software, dem sogenannten ActiveProtect Manager, geliefert. Synology ActiveProtect ist eine leistungsstarke Datenschutzlösung, die Datensicherungen und Wiederherstellungen vereinfacht und vor Ransomware schützt, unabhängig davon, wo sich Ihre Daten befinden.

- **Schnelle Bereitstellung**
Richten Sie Ihre Backup-Geräte ein und beginnen Sie innerhalb weniger Minuten mit dem Schutz Ihrer Daten
- **Alle Workloads schützen**
Schützen Sie SaaS, IaaS, VMs, physische Geräte und Datenbanken über eine einzige Konsole
- **Umfassende Transparenz**
Stellen Sie Tower in Zweigstellen bereit, um Sicherungskopien und Offsite-Kopien zu speichern, die von 1U- oder 2U-Geräten verwaltet werden
- **Effizienz von Datensicherung und Speicher maximieren**
Optimieren Sie die Effizienz der Datensicherung mit der CBT-Technologie und deduplizieren Sie Daten durch quellseitige und serverseitige Deduplizierung
- **Schutz vor Ransomware**
Implementieren Sie die 3-2-1-1-0-Richtlinie für unveränderlichen Datenschutz, automatische Überprüfung von Datensicherungen, Offsite-Datensicherungen und DR-Tests in einer Sandbox
- **Daten plattformübergreifend wiederherstellen**
Stellen Sie Daten plattformübergreifend in Cloud- oder On-Premises-Umgebungen mit P2V-, P2C-, V2V-, V2C- und C2V-

Datenwiederherstellung wieder
her

- **Jederzeit skalieren**

Lagern Sie Daten in Cloud-
oder On-Premises-Lösungen
aus, um Speicherplatz
freizugeben

Beschleunigen Sie Ihre Implementierung

Beginnen Sie innerhalb weniger Minuten mit der Sicherung Ihrer Workloads. Wichtige Konfigurationen wie die Festplattenpartitionierung und die RAID-Einrichtung werden während der Ersteinrichtung von Synology ActiveProtect automatisch abgeschlossen. Der DP320 wird als vorkonfiguriertes Sicherungsgerät geliefert und umfasst alle erforderlichen Hardwarekomponenten.

Workload-Schutz in verschiedenen Umgebungen

Konsolidieren Sie Ihre lokalen, Cloud- und virtuellen Workloads auf einer Plattform. Schützen Sie Windows-PCs, Macs, Linux, VMware vSphere, Microsoft Hyper-V, Nutanix AHV, Proxmox VE, NetApp ONTAP, Nutanix Files, Synology NAS, Microsoft 365-Dienste, Google Workspace-Dienste, Oracle Database, Microsoft SQL Server, Azure VM und Amazon EC2.

Vollständige Datentransparenz gewährleisten

Verwalten und überwachen Sie alle Ihre Sicherungen, Sicherungskopien und Daten-Tiering-Daten über eine einheitliche Konsole. Implementieren Sie Workload-Schutzrichtlinien, um neue oder vorhandene Workloads automatisch zu schützen. Der DP320 wurde für Edge- und ROBO-Implementierungen entwickelt und bietet lokalen Sicherungsschutz oder schützt zusätzliche Sicherungskopien an verteilten Standorten.

Steigern Sie die Leistung und Speichereffizienz Ihrer Sicherungen

Optimieren Sie mit der SURE-Technologie (Synology Unified Reduction Engine) von Synology ActiveProtect die Sicherungseffizienz und maximieren Sie die Speicherkapazität. Mit Changed Block Tracking (CBT) werden nur geänderte Datenblöcke gesichert. Dadurch werden die Datenübertragung minimiert und die Sicherungseffizienz optimiert. Die quellseitige Deduplizierung entfernt Daten vor der Übertragung, während die serverseitige Deduplizierung redundante Daten über mehrere Sicherungsgeräte hinweg entfernt.

Erweiterter Schutz für Ihre Daten

Der Sicherheitsmechanismus des DP320 basiert auf dem Prinzip der Authentifizierung mit geringstmöglichen Berechtigungen und dem Netzwerkschutz. Dadurch wird sichergestellt, dass Daten in jeder Phase geschützt sind – vom Datenzugriff über Sicherung und Speicherung bis zur Wiederherstellung.

- **Netzwerkarchitektur:** Konfigurieren Sie die Firewall-Einstellungen so, dass nur der Zugriff von Geräten innerhalb bestimmter IP-Bereiche und Subnetze zugelassen wird, und stellen Sie sicher, dass nur autorisierte Sicherungsgeräte Datenübertragungen durchführen können. Der integrierte Verwaltungsport ist eine isolierte, ausschließlich für Verwaltungszwecke vorgesehene Schnittstelle, die vom Datenfluss getrennt ist, um Sicherheitsrisiken zu verringern.
- **Identitäts- und Zugriffssteuerung:** Setzen Sie den Zugriff mit geringstmöglichen Berechtigungen über admin-Rollen durch, sodass jeder Benutzer nur die benötigten Berechtigungen besitzt. Integrieren Sie Active Directory, LDAP oder SAML 2.0, um Ihr vorhandenes SSO mit MFA zu verwenden, und blockieren Sie verdächtige IPs automatisch, um unbefugte Anmeldeversuche zu verhindern.
- **Verschlüsselung:** Verhindern Sie, dass vertrauliche Daten offengelegt werden, selbst wenn das Gerät gestohlen wird, indem Sie sie auf volume-Ebene verschlüsseln. So gewährleisten Sie die Vertraulichkeit der Daten und erfüllen Compliance-Anforderungen.
- **Protokollierung und Monitoring:** Bewahren Sie Protokolle für regelmäßige Audits auf, zeigen Sie sie an und exportieren Sie sie. Außerdem können Sie regelmäßig eine Zusammenfassung der Sicherungs- und Wiederherstellungsaktivitäten per E-Mail erhalten. Richten Sie für Echtzeittransparenz SNMP-Traps, SMTP-Benachrichtigungen oder syslog-Weiterleitung ein, um vorhandene Monitoring-Plattformen zu integrieren und Warnmeldungen sofort zu erhalten – so kann die IT Benutzeraktivitäten nachverfolgen und den Überblick behalten.
- **Updates und Wartung:** ActiveProtect Manager aktualisiert sich automatisch auf die neueste Version, hält Ihr System sicher und verringert das Risiko von Datenschutzverletzungen. Wenn Sicherheitslücken gefunden werden, ist Synology bereit, die Sicherheitsprobleme zu überprüfen und entsprechende Patches oder Fehlerbehebungen zu veröffentlichen.
- **Ransomware-Schutz:** Setzen Sie die Sicherungsstrategie 3-2-1-1-0 um, um die Datenresilienz zu gewährleisten. Überprüfen Sie Daten während der Sicherungen automatisch, damit fehlerfreie Kopien Ihrer Daten gespeichert werden können. Erkennen und reparieren Sie Datenfehler mithilfe der Selbstreparatur. Führen Sie DR-Übungen über die integrierte Sandbox von ActiveProtect durch. Schützen Sie Sicherungen mit der WORM-Technologie (Write Once Read Many), sodass Ihre Daten nicht geändert oder gelöscht werden können. Schützen Sie fehlerfreie Kopien Ihrer Sicherungen extern in einer Air-Gap-Umgebung durch logische oder physische Isolierung.



Daten flexibel migrieren und wiederherstellen

Verschieben Sie Daten nahtlos zwischen Cloud- und lokalen Plattformen. Stellen Sie Daten flexibel in Cloud-, virtuellen und physischen Umgebungen wie Azure VM, Amazon EC2, VMware vSphere, Microsoft Hyper-V und weiteren Umgebungen wieder her. Erfüllen Sie die Recovery Time Objectives (RTO) für die Notfallwiederherstellung und gewährleisten Sie schnellen Datenzugriff zur Aufrechterhaltung des Geschäftsbetriebs. Führen Sie Bare-Metal-Wiederherstellungen und Wiederherstellungen auf Dateiebene durch und laden Sie Ihre Sicherungen herunter, um Daten bei Bedarf wiederherzustellen.

Führen Sie regelmäßig Notfallwiederherstellungsübungen in einer Sandbox-Umgebung durch, ohne Ihre Produktionsumgebung zu beeinträchtigen. Überprüfen Sie Ihre Sicherungen und erstellen Sie für Audit-Zwecke automatisch Wiederherstellungsvideos.

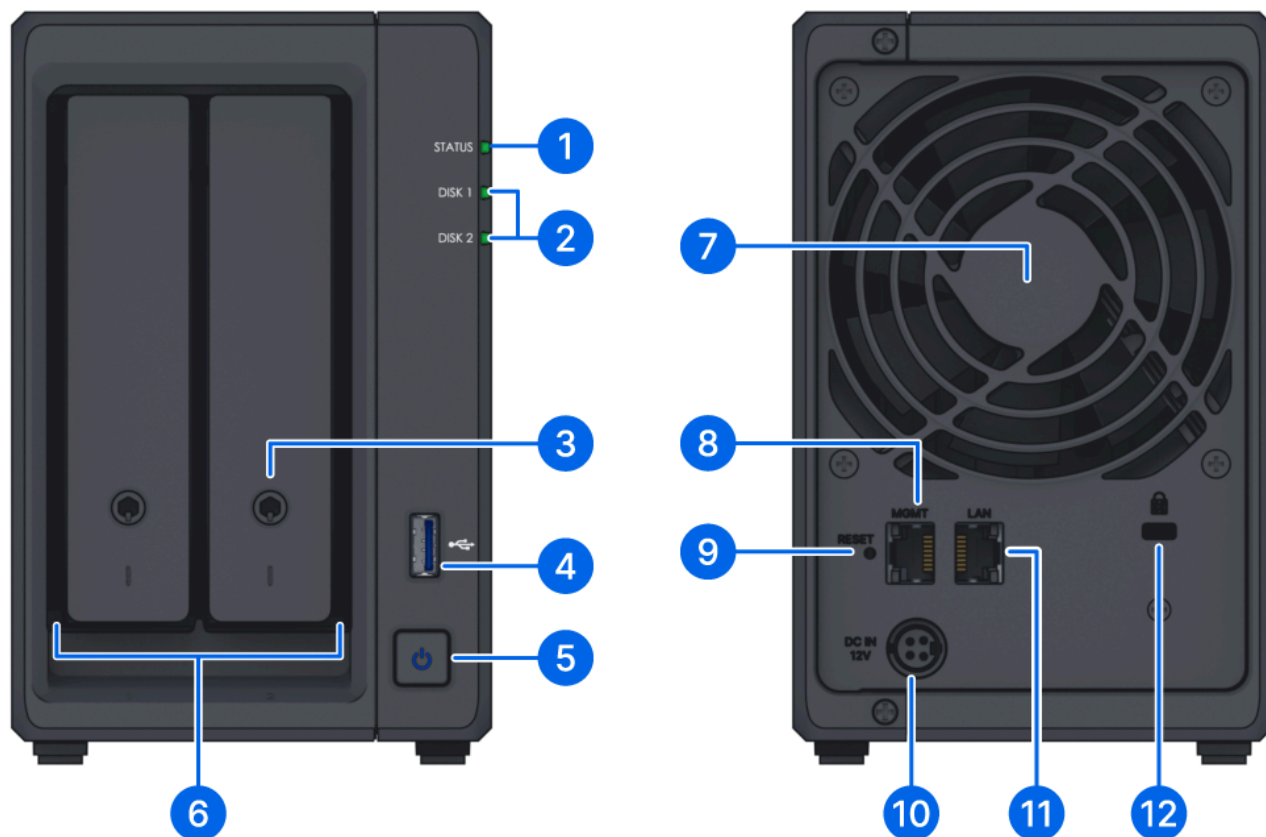


Skalierbarkeit nach Bedarf

Verwenden Sie Versions-Tiering, um Daten auf Remote-Speicher wie Synology NAS, C2 Object Storage, Wasabi Cloud Storage, Azure Blob Storage oder AWS S3 zu verschieben und so die Speicherkapazität einfach zu erweitern und Daten langfristig aufzubewahren.

Wenn Ihr Unternehmen wächst, können Sie neue DP320-Tower hinzufügen und sie zentral über ein 1U- oder 2U-ActiveProtect-Gerät verwalten, auf dem ActiveProtect Manager ausgeführt wird.

Hardwareübersicht



Nr.	Name	Nr.	Name
1.	Ein-/Aus-Schalter	10.	Netzteil-Lüfter
2.	Betriebsanzeige	11.	PCI-Express-Erweiterungssteckplatz
3.	Warnanzeige	12.	Netzteilanzeigen
4.	Laufwerkstatusanzeigen	13.	Befestigungsbohrungen
5.	Statusanzeige	14.	USB 3.2 Gen.-1-Ports
6.	Taste zum Stummschalten des Alarms	15.	10-GbE-RJ-45-Ports
7.	Laufwerkfachverriegelungen	16.	Reset-Taste
8.	Laufwerkfächer	17.	Erweiterungsport
9.	Stromanschlüsse	18.	Verwaltungsport

Technische Daten

Allgemein

Empfohlene Sicherungsquelle	5 TB ¹
Empfohlene integrierte wiederhergestellte VM	1 ²
Cluster-Verwaltungskapazität	Unterstützt bis zu 10 Server oder 500 Workloads ³
Notizen	1. Diese Werte sind Schätzungen auf Grundlage von Telemetriedaten und können je nach Nutzungsbedingungen im Unternehmen variieren. 2. Eine ActiveProtect-Lizenz ist erforderlich.

Hardware

Formfaktor	Desktop
CPU	AMD Ryzen R1600 (2 Kerne)
Speicher	8 GB
Speicherkonfiguration	2 × 8 TB 3,5" HDD (RAID 1)
Netzwerk-Interface	• 1 × 1GbE RJ-45 (Datenübertragung) • 1 × 1GbE RJ-45 (Verwaltung)
Produktabmessungen (HxBxT)	166 × 106 × 223 mm
Gewicht	2,9 kg
AC Eingangsspannung	100 V bis 240 V Wechselstrom
Stromfrequenz	50 / 60 Hz, einphasig
Stromverbrauch	21,07 W
Britische Wärmeeinheit	71,85 BTU/h
Betriebsumgebung	• Temperatur: 32 °F bis 104 °F (0 °C bis 45 °C) • Relative Luftfeuchtigkeit: 8 % bis 80 % RH
Lagerumgebung	• Temperatur: -5 °F bis 140 °F (-20 °C bis 60 °C) • Relative Luftfeuchtigkeit: 5 % bis 95 % RH

Umwelt und Verpackung

Zertifizierung	FCC, CE, BSMI, VCCI, RCM, UKCA, EAC, KC, UL, BIS
Umweltsicherheit	RoHS-konform
Packungsinhalt	• 1 x DP320 Hauptgerät • 1 x Zubehörpaket • 1 x Kurzanleitung zur Installation • 2 × 3,5" SATA-HDD
Garantie	3 Jahre
Notizen	Der Garantiezeitraum beginnt mit dem auf dem Beleg angegebenen Kaufdatum. Erfahren Sie mehr über die eingeschränkte Produktgarantie.

SYNOLOGY INC. © 2026, Synology Inc. Alle Rechte vorbehalten. Synology und das Synology-Logo sind Marken oder eingetragene Marken von Synology Inc. Weitere hier genannte Produkte und Firmennamen sind Marken der entsprechenden Unternehmen. Synology kann ohne vorherige Ankündigung jederzeit Änderungen an den technischen Daten und Produktbeschreibungen vornehmen.