Neuheiten

Arcserve Unified Data Protection 9.0

Schutz vor Ransomware. Verfügbarkeit. Orchestrierte Wiederherstellung.

Arcserve Unified Data Protection (UDP) ist eine wichtige Komponente der einheitlichen Plattform für Datenausfallsicherheit von Arcserve. Arcserve UDP bietet:

- ✔ Vollständigen Schutz vor Ransomware für gesicherte Daten
- ✔ Mehrschichtige Sicherung für Ihre unbezahlbaren digitalen Werte
- ✔ Verfügbarkeitsorientierten Schutz zur Unterstützung von immer betriebsbereiten Unternehmen
- ✔ Zugesicherte und zuverlässige Wiederherstellung mit unterbrechungsfreien DR-Tests
- ✔ Orchestrierte Wiederherstellung: Ermöglicht Ihnen die Wiederherstellung jeglicher Workloads an jedem Ort und zu jeder Zeit

Arcserve UDP ist durch Sophos Intercept X Advanced Cybersecurity geschützt und kombiniert auf einzigartige Weise Deep Learning-Serverschutz, unveränderlichen Speicher und skalierbare Onsite- und Offsite-Geschäftskontinuität. So unterstützt es Ihre Strategie zur Ausfallsicherheit von Daten.

Cloud-basierte Verwaltungskonsole

Benutzer können Arcserve UDP nun über eine cloudbasierte Verwaltungskonsole verwalten. Mit dieser Ergänzung haben Kunden die Möglichkeit, je nach Bedarf die private Verwaltungskonsole vor Ort oder die cloudbasierte Verwaltungskonsole zu nutzen. Die private Verwaltungskonsole vor Ort gibt es schon seit vielen Jahren und ist eine gute Wahl für Umgebungen, die eine private Umgebung erfordern. Die cloudbasierte Verwaltungskonsole eignet sich perfekt für Unternehmen, die Kontrollen wie z. B. die Mandantenfähigkeit benötigen, die eine bessere Flexibilität ermöglichen würden.

Mandantenfähige Verwaltungskonsole

- ✔ Einfache Konfiguration von Unterorganisationen und deren Verwaltung wie beispielsweise verschiedene Mandanten.
- ✔ Unternehmen können nun Workloads zur einfacheren Verwaltung problemlos in verschiedene Domänen aufteilen.
- ✔ Granulare Sicherheit mit flexiblen Verwaltungsfunktionen über Sicherheit auf Mandantenebene und Speicherkontrollen.

Sichere Identitätsverwaltung

- ✔ Cloud Console schützt Kundendaten mit einem robusten Benutzerauthentifizierungssystem, das Okta für Benutzerauthentifizierungsdienste nutzt.
- ✔ Die zentrale Verwaltung von Benutzerkonten vereinfacht die Authentifizierung und Zugriffskontrolle mit Arcserve Identity Services erheblich.
- ✔ Strenge Maßnahmen gegen die Übernahme von Konten bei Ransomware-Angriffen mit der Zero Trust-Implementierung von Okta unter Verwendung der Multifaktor-Authentifizierung (MFA).

Verbesserte Verfügbarkeit, Langlebigkeit und Skalierbarkeit mit Cloud Object Storage

- ✔ Speicherung deduplizierter Backups direkt in der Cloud-Objektspeicherung – AWS S3, Wasabi oder Google Cloud Storage.
- ✔ Niedrigere Gesamtbetriebskosten und bessere die DR-Unterstützung durch sichere cloudbasierte Offsite-Speicher.
- ✔ Eine Vielzahl von Funktionen wie das Kopieren von Daten in einen anderen Datenspeicher, virtueller Standby und andere, sind für die Nutzung des in AWS S3 oder anderen Objektspeichersystemen konfigurierten Datenspeichers verfügbar.

Bedienerfreundliche Schnittstelle

- ✔ Keine Installationen, keine manuelle Bereitstellung und kein erweiterter Konfigurationsbedarf.
- ✔ Intuitive Schnittstelle mit einem informativen Dashboard auf Superadministrator- oder Mandantenebene.
- ✔ Die mehrsprachige Unterstützung für die Cloud-Konsole bietet ein lokalisiertes Erlebnis.

Smart Dashboard und Berichte

- ✔ One-View-Dashboard für Arcserve UDP und Arcserve Cloud Direct.
- ✔ Berichterstattung pro Mandant und detaillierte Informationen über den Sicherungsstatus.
- ✔ Aufschlussreiche Berichterstattung über den Sicherungsstatus.

Moderne Architektur, bessere Benutzererlebnisse und Workflows

- ✔ Schneller Zugriff mit nahtloser Navigation durch eine REST-API-gestützte Architektur.
- ✔ Einfacher Wechsel von der privaten Konsole vor Ort zur Cloud-Konsole zur Unterstützung einer problemlosen Migration.
- ✔ Zehnfache Verbesserung der Benutzerfreundlichkeit mit vereinfachten Arbeitsabläufen.

Verstärkte Unterstützung von Unternehmensanwendungen

Arcserve UDP bietet einen starken anwendungsspezifischen Schutz für Unternehmensanwendungen wie Oracle-Datenbanken und Microsoft SQL Server. Petabytes an Daten, die für den Geschäftsbetrieb entscheidend sind, werden in diesen Anwendungen gespeichert und stellen die Lebensader des Unternehmens dar. Je nach Anwendung setzt Arcserve UDP agentenlose Backup-Methoden ein, die die Produktionssysteme nicht belasten und einen uneingeschränkten Zugriff auf die Quellsysteme ermöglichen.

Oracle Pluggable Database (PDB)-Wiederherstellung

Oracle-PDBs präsentieren sich den Client-Anwendungen als voll funktionsfähige Oracle-DB. Mehrere PDBs können zu einer einzigen CDB zusammengefasst werden, um Größenvorteile zu erzielen.

- ✔ Schnelle Wiederherstellung von Terabytes an Oracle PDBs, die mit Oracle RMAN gesichert wurden, mit der Möglichkeit, die gesamte Oracle PDB (einschließlich aller Tablespaces und Steuerdateien) an ihrem ursprünglichen Speicherort wiederherzustellen.
- ✔ Granulare Wiederherstellung von Oracle PDB Tablespaces an ihrem ursprünglichen Speicherort.

Hinweis: Backups von Oracle CDB, die eine oder mehrere PDBs enthalten, können an Original- oder alternativen Speicherorten wiederhergestellt werden.

Plattform-Ergänzungen, -Erweiterungen und -Verbesserungen: Oracle DB-Schutz durch RMAN

- ✔ Oracle DBs (CDB und nicht-CDB) auf Solaris x64-Plattformen können mit Oracle RMAN vollständig geschützt werden. Alle vorhandenen Funktionen einschließlich unterbrechungsfreier Tests mit Assured Recovery, vollständige Wiederherstellungen auf DB-Ebene, granulare Wiederherstellung und viele andere für diese Konfiguration verfügbare Funktionen.
- ✔ Die Anforderung, dass Oracle DB auf Windows, die UDP-Konsole und RPS sich in derselben Domäne befinden müssen, ist nun aufgehoben.
- ✔ Die Authentifizierung für Oracle-Linux-Quellen mit dem SSH-Schlüssel-Dienstprogramm ist jetzt vollständig automatisiert.
- ✔ Ein einfacher Modus zur Migration von Authentifizierungsmethoden von Arcserve UDP 8.x zu Arcserve UDP 9.0.

Schutz von SQL Server

Arcserve UDP schützt kritische Daten, die in SQL Server-Datenbanken gespeichert sind, und bietet verschiedene erweiterte Schutzoptionen.
Die neueste Version verbessert das Erlebnis durch Ergänzungen in wichtigen Bereichen

- ✔ Point-In-Time-Wiederherstellung für SQL-Server ist jetzt innerhalb des Wiederherstellungsablaufs verfügbar.
- ✔ Wiederherstellung der DB zu einem beliebigen Transaktionspunkt zwischen zwei Wiederherstellungspunkten mit Point-In-Time-Wiederherstellung.
- ✔ Administratoren können jetzt einzelne DB-Größen im Wiederherstellungsfenster sehen.
- ✔ Erweiterte Option zur Prüfung der Wiederherstellung der Integrität in den Job-Einstellungen.
- ✔ Flexibilität bei der Wiederherstellung von SQL-DBs auf alternativen Servern, Instanzen und Pfaden im Gegensatz zum Umbenennen von SQL-Datenbanken und ihren Dateien.
- ✔ Die Möglichkeit, proaktiv zu prüfen, ob der Dateistrom vor der Wiederherstellung aktiviert ist.
- ✔ Wiederherstellung der DB entweder im Wiederherstellungsmodus oder ohne Wiederherstellungsmodus.

Wichtige Verbesserungen zur Unterstützung der Datenstabilität

Verbessertes Benutzererlebnis. Verbesserungen der Bedienungsfreundlichkeit. Produkt-Updates

- ✔ Die Datenverfügbarkeit erhält einen Schub durch die Unterstützung von VMs der Generation 2 auf Microsoft Azure, die eine hohe Leistung und eine viel bessere Sicherheit bieten sollen. Die Unterstützung von virtuellem Standby für diese VMs ermöglicht ein schnelles Hochfahren dieser VMs und bietet sofortigen Zugriff auf Daten und Anwendungen.
- ✔ Unterstützung für das Einhalten der Vorschriften betreffend der Aufbewahrung: Ein manueller Job kann jetzt als „täglich“, „wöchentlich“ oder „monatlich“ gekennzeichnet werden, falls der geplante Job keinen Aufbewahrungspunkt erstellen konnte.
- ✔ Bericht über die Backup-Erfolgsrate bietet wichtige Einblicke: Der Erfolg der Sicherung wird auf Quellcode-Ebene, Richtlinienebene und mehr für tägliche, wöchentliche und monatliche Backups dargestellt.
- ✔ Backup-Speicherplatz kann durch das Entfernen unnötiger Wiederherstellungspunkte, die für Tests oder andere Fälle erstellt wurden, die manuelle nicht mehr relevante Jobs verwenden, eingespart werden.
- ✔ Zuverlässige Verarbeitung von Backup-Jobs, wobei Jobs als unvollständig markiert werden, wenn bei der Ausführung auffällige Warnungen auftreten, die beachtet werden müssen, aber nicht kritisch genug sind, um den Auftrag fehlschlagen zu lassen.
- ✔ Verbesserte Sicherheit durch OAuth 2.0. Google und Microsoft haben die Unterstützung für die Basisauthentifizierung eingestellt und aus ihren Angeboten entfernt. Die E-Mail-Benachrichtigungen von Arcserve UDP können jetzt Oauth als Authentifizierungstyp für Microsoft 365 und Google Cloud auswählen, um die Kommunikation zu sichern und den empfohlenen Authentifizierungstyp zu verwenden.
- ✔ Verbesserte Sicherheit durch Upgrades kritischer Komponenten von Drittanbietern auf neuere Versionen.

Neue unterstützte Plattformen

- ✔ Microsoft Windows Server 2022
- ✔ Microsoft Windows 11
- ✔ VMware vSphere 8.0
- ✔ Red Hat Enterprise Linux 8.x & 9.x
- ✔ Eigenständige und mandantenfähige Oracle 19c- und 21c-Datenbanken auf Oracle Solaris 11.x (x64)
- ✔ Oracle Database 21c
- ✔ Oracle Linux 8.4, 8.5, 8.6, 9.0
- ✔ Rocky Linux 8.4, 8.5, 8.6, 9.0
- ✔ AlmaLinux 8.4, 8.5, 8.6, 9.0
- ✔ SLES 15 SP3, SP4
- ✔ Debian 9-11
- ✔ Ubuntu 22.04 LTS
- ✔ VMware vSphere 7.0 Update 3
- ✔ UDP 9.0 Database: SQL Express 2019

Weitere Informationen

Arcserve UDP 9.0: Bookshelf | Versionshinweise | Kompatibilitätsmatrix