Produktbewertung

DCIG

Arcserve UDP 9.0 überwindet Backup-Komplexität und aktuelle Ransomware-Herausforderungen

Von DCIG-Präsident & Gründer, Jerome Wendt

arcserve®
Protect what's priceless.

DCIG

PRODUKTBEWERTUNG

Arcserve UDP 9.0 überwindet Backup-Komplexität und aktuelle Ransomware-Herausforderungen

Arcserve UDP 9.0 hilft Organisationen dabei, diese Herausforderungen durch Stärkung ihrer Reaktion auf diese zu bewältigen. Sie bietet für Organisationen neue Optionen zur Zentralisierung, Vereinfachung und Sicherung ihrer Backup- und Recovery-Infrastruktur in der aktuellen IT-Umgebung.

arcserve®
Protect what's priceless.

LÖSUNG

Arcserve UDP 9.0

FIRMA

Arcserve
380 Data Drive
Suite 510
Draper, Utah 84020
+1 844 639 6792

arcserve.com

Die Dynamik der Verwaltung der aktuellen unternehmensbezogenen IT-Infrastrukturen hat sich geändert – vielleicht sogar für immer. IT-Umgebungen müssen immer noch mit der Einführung neuer Funktionen, Technologien, Prozesse und Produkte kämpfen. Sie müssen sich jedoch auch gegen die neuen Bedrohungen von Ransomware wehren und verteidigen. Außerdem sind die meisten IT-Infrastrukturen hybrid geworden, was zu ihrer Managementkomplexität beiträgt.

Vielleicht wird die Komplexität der IT-Infrastruktur nirgendwo deutlicher als bei der Verwaltung von Backups und Wiederherstellungen über mehrere Standorte hinweg. Backup-Lösungen müssen Sicherungsaufträge verwalten, Sicherungen auf mehreren Speicherebenen ablegen, Wiederherstellungen erleichtern und komplexe Anwendungen schützen. Außerdem müssen sie diese Aufgaben in Umgebungen ausführen, die ständig durch Ransomware bedroht sind.

Die Bewältigung dieser Herausforderungen ist die Aufgabe von externen Anbietern von Backup-Lösungen wie Arcserve. Seine neueste Version, Unified Data Protection (UDP) 9.0, stärkt die Fähigkeit von Unternehmen, diese Probleme frontal anzugehen. Mit Arcserve können Unternehmen die Sicherung und Wiederherstellung in ihrer Hybrid-Cloud-Umgebung besser zentralisieren, vereinfachen und sichern.

Herausforderungen und Bedrohungen, denen Organisationen gegenüberstehen

Bei der Verwaltung von Backup und Recovery in der aktuellen IT-Infrastruktur stehen Organisationen häufig folgenden Herausforderungen und Gefahren gegenüber:

1. ***Keine zentralisierte Backup-Konsole.*** IT-Personal kann remote und/oder am Standort einer Organisation arbeiten. Es muss jedoch Backup- und Recovery-Aufgaben im virtuellen, physischen und Cloud-Einsatz verwalten. Dies erfordert eine einzelne Verwaltungskonsole, welche Backup und Recovery über diese verschiedenen Standorte hinweg zentral verwaltet.
2. ***Bedarf für mehrfache Backup-Administrator-Rollen.*** Die Abstellung einer Person oder sogar eines dedizierten Teams an Fachkräften zur Verwaltung von Backups und Recoveries ist nicht immer sinnvoll. Bestimmte Anwendungen bzw. Workloads in Organisationen können Personen mit Fachwissen erfordern, um diese Backups optimal zu verwalten. Eine Backup-Lösung, die unterschiedliche Administrator-Rollen unterstützt, bietet verbesserte Sicherheit und Verwaltung von Backup- und Recovery-Aufgaben.
3. ***Anfällige Identitäten von IT-Personal.*** Bad Actors entwickeln Ransomware-Varianten, die IT-Umgebungen auf Schwachstellen prüfen und diese angreifen. Manche Varianten konzentrieren sich auf die Kompromittierung von Logins zu Backup-Lösungen, indem sie jene Personen mit schwachen Passwörtern ausfindig machen. Nach der erfolgten Kompromittierung können diese Bad Actors auf die Lösung zugreifen, um bestehende Backups und Backup-Jobs zu kompromittieren oder zu löschen und/oder neue zu deaktivieren. Backup-Lösungen müssen die Identitäten von Personen bei Zugriff auf die Lösung sowie der Durchführung von Aufgaben nach der Anmeldung überprüfen.
4. ***Mangel an anspruchsvollen Backup- und Recovery-Funktionen.*** Organisationen haben ihre Wahl an mehrfachen Backup-Lösungen, die für ihre IT-Umgebungen gebaut wurden. Aktuelle Anwendungen haben jedoch häufig konkrete und anspruchsvolle Backup- und Recovery-Anforderungen. Leider fehlt manchen Backup-Lösungen die umfassende Palette an Funktionen, welche Organisationen zum umfassenden Schutz dieser Anwendungen und ihrer Daten benötigen.

Solides Fundament von Arcserve UDP

Arcserves Unified Data Protection (UDP) bietet einen entscheidenden Vorteil gegenüber zahlreichen Konkurrenten. UDP liefert erstklassige Backup- und Recovery-Funktionen der nächsten Generation, welche Organisationen regelmäßig benutzen. UDP offeriert und unterstützt seit vielen Jahren:

- Backup-Appliances, welche komplette Anlagen in externen Dienststellen und Datenzentren ermöglichen.
- Breite Unterstützung zum Schutz von Anwendungen und Betriebssystemen.
- Cloud-basierte SaaS Backup-Lösung für Microsoft 365 und andere.
- Schutz von Microsoft 365 unter Verwendung von Arcserve UDP vor Ort.
- Globale quellseitige Deduplizierung, welche Backup-Zeiten und Backup-Speicheranforderungen reduziert.
- Unterstützung für mehrfache Backup-Zielarten (Cloudspeicher, Festplatte und Band.)
- Eine formelle Beziehung mit Sophos, welche Ransomware-Erkennung und Behebung ermöglicht.
- Zahlreiche Methoden zur Durchführung von sofortiger Wiederherstellung für unterschiedliche Anwendungsanforderungen.
- Cluster-ähnliche HA für Anwendungen und Daten unter Verwendung der UDP Virtual Standby Funktion.
- Weltweiter technischer Support, der UDP-Einsätze auf der ganzen Welt unterstützt.

Die weltweite Nutzung von UDP in IT-Umgebungen bietet Arcserve einen kontinuierlichen Vorteil gegenüber den Angeboten von Konkurrenten. Arcserve muss nicht raten, welche neuen Backup- und Recovery-Funktionen Organisationen als nächstes benötigen. Sein fortgesetzter Einsatz und kontinuierliche Interaktionen mit Kunden helfen Arcserve bei der Priorisierung dessen, welche Funktionen in UDP 9.0 aufzunehmen sind.

Zentrale Cloud-Konsole für Lockdown und Lockout

Bei einer schwachen Implementierung werden Backup- und Recovery Management in IT-Umgebungen schnell zu einer mühsamen, umständlichen und fehlerbehafteten Aufgabe. Die Verwaltung von Backups über mehrfache Standorte hinweg kann zu unvorhergesehenen Ergebnissen führen, selbst wenn alle Standorte die gleiche Managementkonsole benutzen. Beispielsweise können aufgrund von schlechter Beaufsichtigung und Koordination Backup-Richtlinien uneinheitlich oder gar nicht angewendet werden. Diese Praktiken schwächen die Fähigkeit einer Organisation, die Komplexität zu reduzieren und Ransomware-Bedrohungen zu entschärfen.

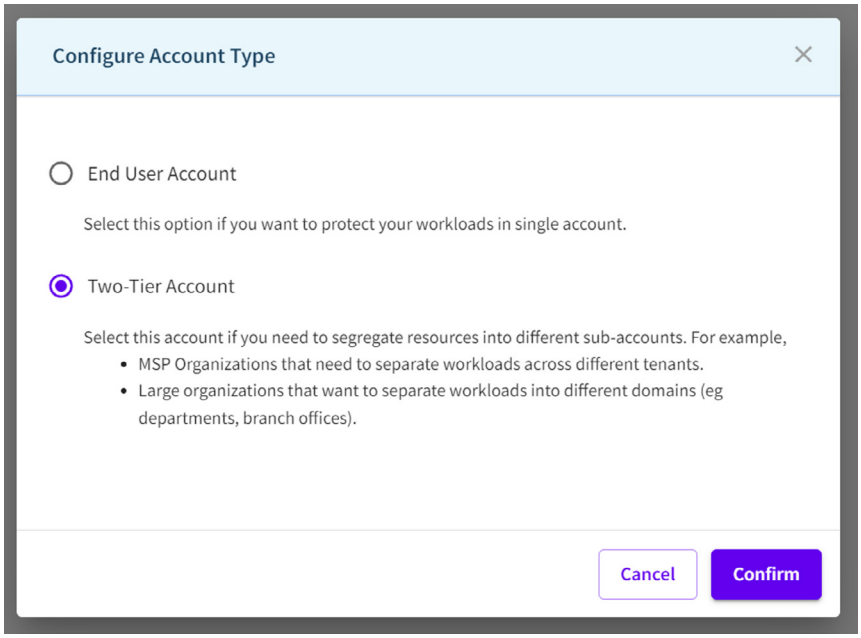
Die Einführung einer Cloud-Konsole durch UDP 9.0 stärkt die Reaktion einer Organisation auf Ransomware auf mehrfache Weise. Arcserve hostet und verwaltet diese Konsole in einem Cloud-Rechenzentrum. Auf diese Weise muss das IT-Personal die Konsole nicht manuell bereitstellen oder installieren oder viel Zeit mit ihrer Konfiguration verbringen. Stattdessen können sie sich schnell anmelden und über die intuitive Benutzeroberfläche mit der Durchführung von Aufgaben beginnen, die zur Sicherung ihrer Backups beitragen. Zu diesen Aufgaben gehören:

- Erstellen und Definieren von Backup-Richtlinien.
- Konfiguration der Infrastruktur, Quellgruppen und Benutzerzugriffskontrollen.
- Verwaltung von Kontoressourcen, einschließlich der Benutzerverwaltung.
- Überwachung und Analyse von Backup- und Recovery-Jobs in der gesamten Organisation.

Die UDP Cloud Console authentifiziert jede Anmeldung durch ihre MFA-Integration mit Okta. Diese MFA-Authentifizierung verifiziert die Identität jedes Benutzers und wehrt mögliche Angriffe von böswilligen Akteuren ab.

Zur Vereinfachung der laufenden Benutzerverwaltung bietet die UDP-Cloud-Konsole nach der Anmeldung zentrale Benutzerverwaltung. Sie bietet beispielsweise rollenbasierte Zugriffskontrolle (RBAC), welche mittels Arcserve Identity Services Benutzeraktivitäten verwaltet und kontrolliert. Mit diesen Kontrollen werden IT-Personal entweder „Super“ Admin oder Tenant-Level-Rollen mit den jeweils zugewiesenen Verantwortlichkeiten zugeordnet.

Zur Vereinfachung der laufenden Benutzerverwaltung bietet die UDP-Cloud-Konsole nach der Anmeldung zentrale Benutzerverwaltung.

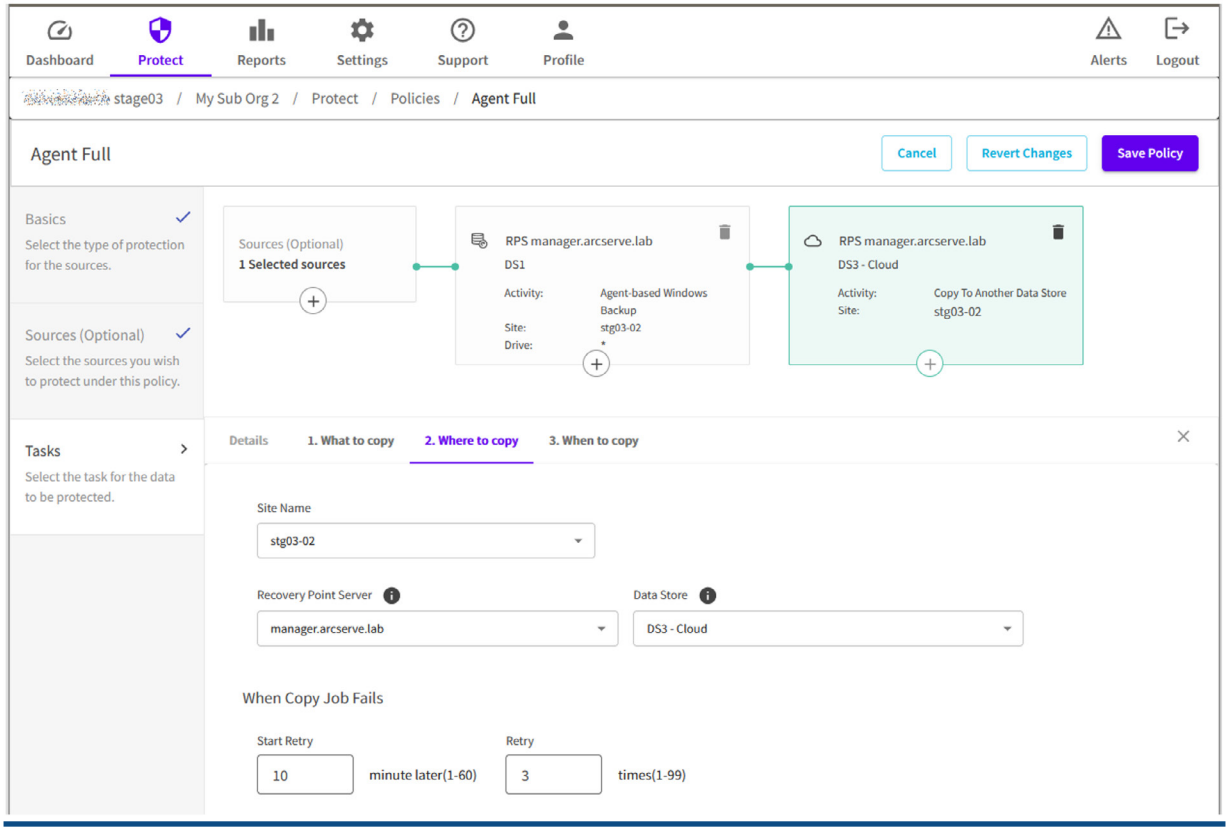


Abhängig von seinen zugewiesenen Berechtigungen kann das IT-Personal mittels Cloud-Konsole UDP-Backup und Recoveries an jedem beliebigen Standort innerhalb einer Organisation verwalten. Der Protect Tab an der Konsole ermöglicht dem Personal:

- die Auswahl der zu schützenden Workloads.
- die Auswahl der Standorte, an welchen es die Backups aufbewahren möchte. Dieser Standort kann auch die Wahl eines zentralen Arcserve Recovery Point Server (RPS) als Speicherziel beinhalten.
- die Durchführungen von Datenwiederherstellungen (Restores und Recoveries).

Mittels UDP-Cloud-Konsole kann das IT-Personal auch Arcserve Cloud Direct Backup Jobs ansehen und verwalten. Arcserve Cloud Direct arbeitet separat als ein Backup-as-a-Service (BaaS), welcher Arcserve auch in seiner Cloud hostet. Cloud Direct führt Backups vor Ort ohne die Notwendigkeit von Hardware- oder Software-Installationen durch und sendet Backups direkt an die Arcserve-Cloud.

Diese UDP 9.0-Funktionen sollten dazu führen, dass immer mehr Organisationen zur Verbesserung Ihrer Sicherheitsposition ihre Backup-Verwaltung zentralisieren. Zur Erfüllung dieses prognostizierten Bedarfs bietet und unterstützt Arcserve weiterhin eine private Verwaltungskonsole vor Ort, die zehn unterschiedliche Sprachen unterstützt. Organisationen können weiterhin diese Konsole verwenden und dann jederzeit auf die UDP-Cloud-Konsole umschalten.



Ein leistungsfähiges Cloud-Backup-Erlebnis

IT-Personal hat wenig Geduld oder Toleranz für langsame, passive Management-Webschnittstellen, insbesondere, wenn diese in der Cloud arbeiten. Wenn sie in der Cloud arbeiten, müssen sie schneller und besser funktionieren. Zur Erfüllung dieser Erwartungen benutzt Arcserve jetzt REST APIs. Durch Nutzung dieser APIs bietet die Cloud-Konsole Reaktionszeiten, die Benutzer von lokalen UDP erwarten.

Durch Nutzung dieser APIs bietet die Cloud-Konsole Reaktionszeiten, die Benutzer von lokalen UDP erwarten.

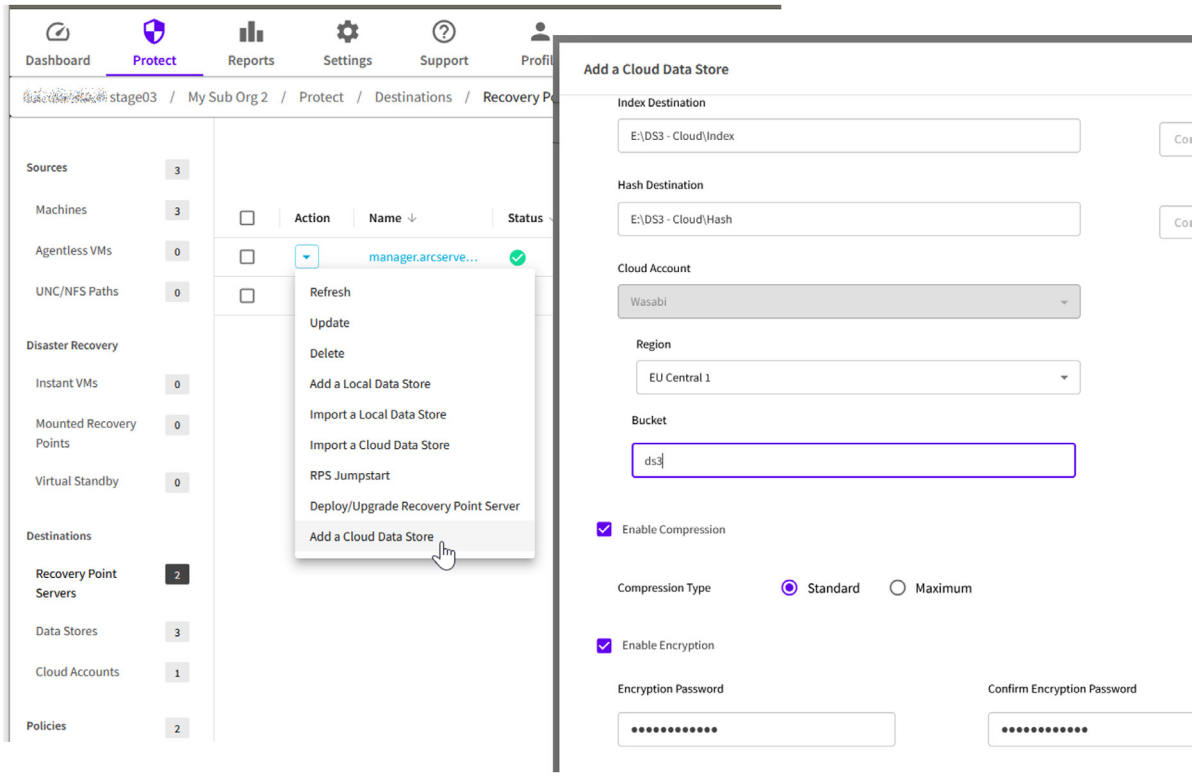
Diese zentralisierte Management-Konsole befähigt Benutzer auch anderweitig, indem sie diesen schnelleren Zugriff auf neue Funktionen ermöglicht. Dies ist bereits in Arcserves Support einer erhöhten Anzahl von Cloud Speicherzielen zu sehen. Arcserve UDP 9.0 kann Backups direkt auf folgende Cloud-Objektspeicherangebote durchführen:

- Amazon Web Services (AWS) Simple Storage Services (S3))
- Google Cloud Storage
- Wasabi Cloud Storage

Die Sicherung auf diesen Speicherzielen ermöglicht es Organisationen, die Vorteile zu nutzen, die Cloud-Objektspeicher anbietet. Zu diesen Vorteilen gehören:

- Zugriff auf erschwingliche Speicherkapazität, die schnell und einfach hinzugefügt werden kann.
- Hohe Verfügbarkeit, Zuverlässigkeit und Resilienz.

Die Unterstützung von Arcserve UDP für weitere Cloud-Objektspeicherziele ergänzt die Unterstützung für lokale Backups. Diese bleiben eine Notwendigkeit für Produktions-Workloads, die schnelle Backups, Wiederherstellungen und Wiederherstellungen erfordern. Mit lokalen Backups vermeiden Unternehmen die potenziell langen Wartezeiten, die mit dem Abrufen von Daten aus der Cloud verbunden sind.



Leistungsfähigere Sicherungs- und Wiederherstellungsoptionen

Die Nutzung führender Datenbanken, Cloud-Plattformen, Hypervisors und Betriebssysteme (OS) durch Organisationen hat nicht nachgelassen. Im Gegenteil, Unternehmen benutzen diese immer mehr und benötigen daher zu deren Schutz leistungsfähigere Backup- und Recovery-Funktionen. Arcserve UDP 9.0 spricht diese Bedenken folgendermaßen an.

UDP 9.0 kann eine granulare Wiederherstellung einer Oracle PDB bis auf einen konkreten Tablespace innerhalb von Oracle durchführen.

Oracle- und SQL-Server-Datenschutz

Bezüglich von Datenbanken verbessert UDP 9.0 die bestehenden Datenschutzfunktionen für Oracle- und SQL-Server-Datenbanken. Arcserve UDP 9.0 bietet vollständige oder granulare Wiederherstellung/Recovery für Oracle Pluggable Databases (PDBs).

Durch seine Integration mit Oracle RMAN seit dem UDP 8.x Release bietet Arcserve UDP agentenloses Backup von Oracle Database. UDP 9.0 baut auf dieser Integration auf, um zahlreiche Terabytes einer Oracle PDB schnell zu sichern und wiederherzustellen.

UDP 9.0 kann eine granulare Wiederherstellung einer Oracle PDB bis auf einen konkreten Tablespace innerhalb von Oracle durchführen. Dieser Support erstreckt sich sogar auf Oracle DBs, die auf Solaris x64 Plattformen betrieben werden. Es stehen alle bestehenden Funktionen zur Verfügung, inklusive zerstörungsfreier Prüfung via Assured Recovery, vollständiger Wiederherstellungen auf Datenbankebene, granularer Wiederherstellung und anderer Funktionen.

Arcserve verstärkte ebenfalls die UDP 9.0 Backup- und Recovery-Funktionen für Microsoft SQL Server. Bei der Durchführung von Konsistenzprüfungen müssen SQL Server Backups einen zusätzlichen Schritt ausführen. Bei Nichtbestehen der Konsistenzprüfung wird eine Warnung ausgegeben, und das Backup als für die Wiederherstellung unbrauchbar gekennzeichnet.

UDP 9.0 bietet Point-in-Time-Wiederherstellungen, die in der UDP UI verfügbar sind. Dies ermöglicht es dem IT-Personal, mittels der Point-in-Time Recovery Funktion eine Datenbank an einem beliebigen Transaktionspunkt zwischen zwei Wiederherstellungspunkten wiederherzustellen.

UDP 9.0 ermöglicht es dem IT-Personal, mittels der Point-in-Time Recovery Funktion eine Datenbank an einem beliebigen Transaktionspunkt zwischen zwei Wiederherstellungspunkten wiederherzustellen.

Weitere neue Optionen, die UDP 9.0 zum verbesserten Schutz und verbesserter Wiederherstellung der SQL-Server-Datenbank anbietet, beinhalten:

- Erhöhte Sicherheit durch Zugriffsbeschränkungen auf spezifische Rollen.
- Freiheit, eine SQL-Server-Datenbank auf alternative Server, Instanzen und Pfade wiederherzustellen.
- Wahl zwischen Recovery und Norecovery Modus.
- Proaktive Verifizierung, dass vor Beginn einer Wiederherstellung ein SQL-Server-Ziel FileStream Aktiviert hat.

OS-Plattform-Support

Auch Betriebssysteme (OS) entwickeln sich ständig weiter, da Organisationen regelmäßig ihre aktuellen OS-Versionen aktualisieren, um den ununterbrochenen technischen Support sicherzustellen. Zur Erfüllung dieser Anforderungen fügt Arcserve UDP 9.0 Support für die neuesten Linux, Microsoft Windows, Microsoft Windows Server und VMware vSphere OS-Versionen hinzu.

Bei Einsatz von Virtual Standby (VSB) fügt UDP 9.0 Support für Gen 2 VMs in Microsoft Azure hinzu.

Virtual Standby bietet cluster-ähnliche hohe Verfügbarkeit (HA) für Anwendungen und Daten. Es kann auch die Wiederherstellungspunkte/Recovery Points (Backups) rasch auf ein breites Spektrum an VM-Formaten umsetzen.

Organisationen können diese Wiederherstellungspunkte zur automatischen oder manuellen Anschaltung einer VM benutzen. Virtual Standby unterstützt VMs, die auf mehrfachen privaten und öffentlichen Cloud Plattformen gehostet werden, darunter Amazon EC2, Microsoft Azure und Hyper-V, Nutanix AHV und VMware vSphere.

Arcserve UPD 9.0 Support für Datenbank- und Betriebssystem-Plattformen

Arcserve UDP 9.0 unterstützt die neuesten Versionen folgender Datenbanken, Hypervisors und Betriebssysteme.

Plattform	Version/Release
Datenbanken	· Oracle 19c und 21c Stand-alone on Oracle Solaris 11.x (x64) · Oracle Database 21c
Hypervisors	· VMware vSphere 7.0 Update 3 · VMware vSphere 8.0
Linux	· AlmaLinux 8.4, 8.5, 8.6, 9.0 · Debian 9 – 11 · Oracle Linux 8.4, 8.5, 8.6, 9.0 · Red Hat Enterprise Linux 8.x, 9.x · Rocky Linux 8.4, 8.5, 8.6, 9.0 · SLES 15 SP3, SP4 · Ubuntu 22.04 LTS
Windows	· Microsoft Windows 11 · Microsoft Windows Server 2022

UDPs vielfache Backup- und DR-Funktionen

Arcserve UDP liefert seit einiger Zeit fortgeschrittene Datenschutzfunktionen, die regelmäßig von Organisationen genutzt werden. Arcserve bietet sowohl agentenbasierte als auch agentenlose Backup-Optionen. Diese Optionen geben Organisationen die Flexibilität zur Nutzung des besten Backup-Ansatzes, um die konkreten Datenschutzanforderungen der jeweiligen Anwendung zu erfüllen.

Auf der Recovery-Seite bietet Arcserve UDP mehrfache Disaster Recovery (DR) Optionen, die beinhalten:

- ***DRaaS.*** Arcserve UDP bietet umfassenden Datenschutz mit lokalem und Cloud-basiertem Einsatz. DRaaS ist als vollständig verwaltete Cloud-Services-Erweiterung namens Cloud Hybrid verfügbar. Sein DRaaS Service hält kritische Daten und Workloads außerhäusig geschützt und bereit und ermöglicht Organisationen während oder nach ungeplanten lokalen Ausfällen die Fortsetzung des Betriebes.
- ***Instant Restores.*** Durch die Verwendung der Instant Restore Funktion kann IT-Personal eine VM direkt aus einem Backup heraus rasch hochfahren. Es kann eine VM wiederherzustellen, ohne zuerst das Backup wiederherstellen bzw. rehydrieren zu müssen.
- ***Virtual Standby (VSB).*** Bietet eine hochverfügbare Konfiguration für Daten und Anwendungen für noch schnellere Recoveries als seine Instant Restore Funktion. VSB erstellt und unterhält eine VM mit einem Wiederherstellungspunkt, der jederzeit zum Booten bereitsteht. Nach der Konfiguration überwacht VSB kontinuierlich den Heartbeat des Source Nodes (Produktion). Wird ein Ausfall oder eine Ausschaltung des Source Nodes erkannt, übernimmt die VM sofort als Primary Node.

Arcserve UDP 9.0 überwindet Backup-Komplexität und aktuelle Ransomware-Herausforderungen

Keine Organisation kann auf die aktuelle Backup-Komplexität und Ransomware-Herausforderungen mit einer schwachen Backup-Lösung reagieren. Sie benötigen eine Backup-Lösung, die jenen überlegen ist. Sie muss ihre Sicherheitslage stärken und sie gleichzeitig in die Lage versetzen, komplexere IT-Umgebungen zu schützen.

Arcserve UDP 9.0 bietet diese leistungsfähige Antwort auf die Erwartungen und Bedürfnisse von modernen Organisationen durch:

- Bereitstellung einer neuen Cloud-basierten, mandantenfähigen Cloud-Konsole zur zentralen Verwaltung von UDP und Cloud Direct.
- Verbesserung des Schutzes der Unternehmensanwendungen wie Oracle und MS SQL Server
- Durchführung von Verbesserungen der Architektur und Benutzeroberfläche zur Leistungssteigerung und Vereinfachung der Verwaltung.
- Verbesserte Daten-Resilienz, Verfügbarkeit und Beständigkeit durch Support für mehrfache Cloud-Objektspeicheranbieter.

Diese Funktionen gemeinsam mit Arcserves bestehender Integration mit Sophos bietet Organisationen eine bewehrte Bastion gegenüber Ransomware-Bedrohungen. Mit Arcserve UDP 9.0 sind Unternehmen in der Lage, sich gegen die neuesten Ransomware-Bedrohungen zu verteidigen und jede Komplexität, die auf sie zukommt, zu bewältigen. ■

About DCIG

The Data Center Intelligence Group (DCIG) empowers the IT industry with actionable analysis. DCIG analysts provide informed third-party analysis of various cloud, data protection, and data storage technologies. DCIG independently develops licensed content in the form of TOP 5 Reports and Solution Profiles. More information is available at **www.dcig.com.**