Product Review

DCIG

Faster, More Secure Recoveries for All Virtual Machines: Highlights of the Arcserve UDP 10 Release

By DCIG Principal Analyst, Jerome Wendt

arcserve®

Contents

DCIG

PRODUCT REVIEW

Faster, More Secure Recoveries for All Virtual Machines: Highlights of the Arcserve UDP 10 Release

Implementing hybrid clouds and stopping ransomware represents operational priorities in every organization. Arcserve UDP 10 delivers on these priorities by leaning into anti-malware detection, offering fast, affordable RPOs and RTOs for all standard VMs, and delivering efficient multi-site recovery for virtual machines. In so doing, Arcserve UDP 10 positions organizations to fully, and affordably, capitalize on hybrid cloud functionality while better mitigating the threats that ransomware presents.

arcserve®

SOLUTION

Arcserve UDP 10

COMPANY

Arcserve
6600 City W. Parkway
Suite 215
Eden Prairie, MN 55344
(844) 765-7043

arcserve.com

Embracing Hybrid Clouds and Stopping Ransomware Threats: Today's Operational Priorities

Any new or upgraded solution that an organization introduces into its IT infrastructure must often satisfy two operational priorities.

Operational Priority #1: Embrace Hybrid Clouds

Organizations continue to press ahead with hybrid cloud initiatives. They recognize that deploying and supporting applications, data, and workloads both on-premises and in the cloud has merit. While many organizations still run IT operations on-premises, they also embrace the cloud to various degrees.

For some, the hybrid cloud strategy may simply entail storing their backups in the cloud. Others may perform restores or recoveries in the cloud or use the cloud for business continuity or disaster recovery. Some may even run production applications and workloads both on-premises and in the cloud.

Operational Priority #2: Stopping Ransomware Threats

A backup solution must also protect against, and ideally enable to recover from, ransomware events. Every organization, irrespective of its size, must take the ransomware threat seriously due to its pervasiveness and increasing sophistication.

These factors led the United States (US) Cybersecurity and Infrastructure Security Agency (CISA) to issue an urgent advisory in August 2024. In this advisory CISA warned of the emergence of new ransomware groups.

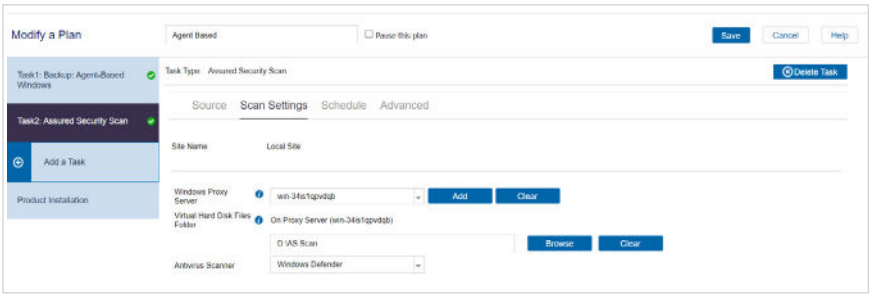
These groups seek to attract criminal talent from established ransomware groups to create even more sophisticated ransomware.[1] This sophistication often comes from their use of artificial intelligence (AI) and developing ransomware algorithms based upon large language models.

Arcserve made a point to address both corporate operational priorities in its latest Unified Data Protection (UDP) 10 release.

1. https://www.cisa.gov/news-events/alerts/2024/08/29/cisa-and-partners-release-advisory-ransomhub-ransomware. Reference 9/21/2024.

UDP 10 Leans Into Anti-malware Detection

Discovering and defending against the custom ransomware produced by hackers that specialize in this activity requires specialized cybersecurity software. To perform ransomware detection in UPD 10, Arcserve took a novel approach. It capitalizes on the freely available Microsoft Defender included with Microsoft Windows Server.

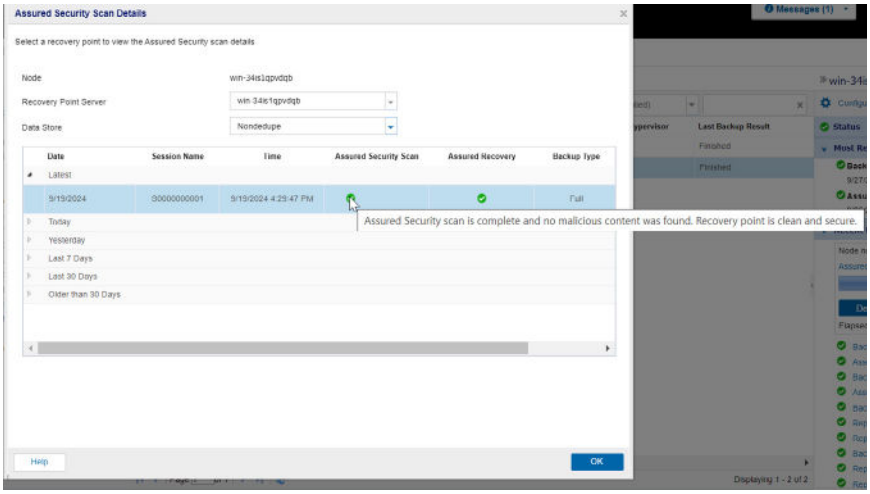


Arcserve's decision to use Microsoft Defender in this role to scan backups for ransomware makes sense for at least two reasons:

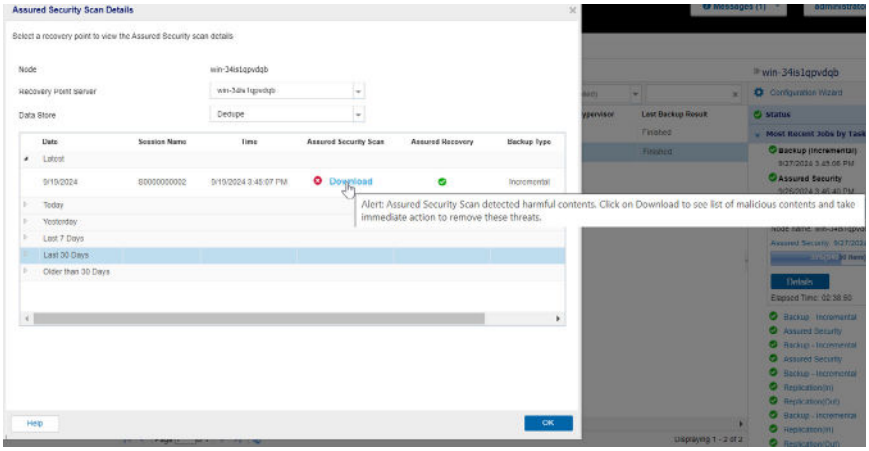
- ***Arcserve already hosts UDP 10 on Microsoft Windows Server.*** This gives Arcserve UDP ready access to Microsoft Defender's APIs to use for scanning backups.
- ***This approach eliminates the requirement for organizations to acquire specific anti-malware software to scan their UDP backups.*** Using Microsoft Defender, organizations obtain the cybersecurity functionality they need to scan their backups for malware. They simultaneously avoid needing to deploy specific anti-malware software and the extra costs and complexity that introduces.

At a high level, UDP scans backups for malware by using the following process. First, UDP 10 backs up data to disk. Once it completes the backup, UDP 10 mounts the backup recovery point and presents it to Microsoft Defender to scan.

Using Microsoft Defender's APIs, UDP 10 instructs Microsoft Defender to perform a full antivirus (AV) scan of the backup copy. Once Defender completes the scan, UDP 10 unmounts the recovery point, reports on the results of the backup scan, and generates alerts if any malware was detected.



Many organizations will find it appropriate to perform Assured Security scans immediately prior to performing a restore or recovery.



Since organizations initiate these AV scans of their backup copies, they may perform these scans at any time. UDP 10 also permits organizations to add Assured Security scans to UDP backup policies that Arcserve refers to as protection plans.

Many organizations will find it appropriate to perform Assured Security scans immediately prior to performing a restore or recovery. Using this approach the scan detects any latent forms of ransomware based on Defender's most up-to-date signatures.

Current Instant Recovery Challenges

An Instant Recovery of a VM typically implies a recovery in seconds, minutes, or perhaps up to an hour. Offering this functionality as a recovery option for all virtual machines appeals to many organizations.

Yet as they explore this option, they will uncover multiple costs associated with providing Instant Recovery to VMs at scale. They must reserve needed computing and disk capacity to recover a virtual machine. This may require more network bandwidth to facilitate the additional traffic. They may even find they must obtain additional software licenses and IT staff to successfully implement it. These challenges lead organizations to limit Instant Recovery's availability to business and mission critical VMs.

Indeed, many virtual machines that organizations run may not require recovery times of minutes or less. Instead, organizations want affordable, simple recoveries for all their VMs that they may reliably complete in a few minutes or hours.

Fast and Affordable RPOs and RTOs for All Standard VMs

Despite the improvements in cybersecurity software and the improving security posture of many organizations, ransomware events still occur. During these times, organizations may need to quickly deliver disaster recovery (DR) for all their virtual machines. This can present a dilemma, especially for all the virtual machines that organizations need to recover from backups.

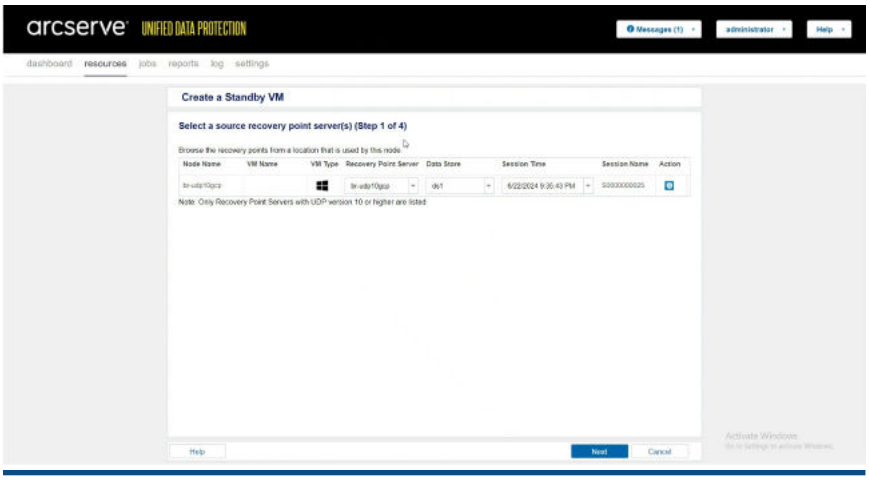
Standard, as opposed to business-critical or mission-critical, virtual machines often represent the majority of VMs found in organizations. These virtual machines that host standard

business applications and data may have longer recovery time objectives (RTOs) of a few hours. However, their downtime becomes more impactful if recovering them takes many hours or days.

Arcserve UDP 10's new On-demand Virtual Standby feature addresses this underserved need for standard virtual machines to recover more quickly.

Arcserve UDP 10's new On-demand Virtual Standby feature addresses this underserved need for standard virtual machines to recover more quickly. Using UDP 10's On-demand Virtual Standby feature, organizations may meet the RTOs associated with these virtual machines. Further, they may accomplish this objective with minimal cost and administrative overhead.

To use On-demand Virtual Standby, a UDP 10 administrator selects the VM or VMs to recover, the target location, and initiates the recovery. Arcserve UDP 10 then creates a new virtual machine for each selected VM at its target location. UDP 10 completes the process by creating each virtual machine, copying its data, and booting the virtual machine.



While the On-demand Virtual Standby process resembles Instant Recovery, it distinguishes itself in at least three ways.

On-demand Virtual Standby does not reserve any computing or storage capacity at the target location ahead of time.

- ***First, it only creates virtual machines at the target location after the UDP 10 administrator initiates the recovery.*** On-demand Virtual Standby does not reserve any computing or storage capacity at the target location ahead of time. A virtual machine only starts consuming resources at the target location after an administrator initiates its recovery.
- ***Second, organizations may recover the virtual machine to any supported on-premises hypervisor or cloud provider.*** Administrators may choose from any hypervisor or cloud provider supported by UDP 10 to perform an On-demand Virtual Standby recovery. Supported hypervisors include Microsoft Hyper-V and VMware vSphere with cloud support available for AWS EC2, Azure VMs, and Google Compute Engine.
- ***Third, recoveries using On-demand Virtual Standby meet the RPOs and RTOs of standard VMs.*** It may take anywhere from a few minutes to a few hours to recover a virtual machine using On-demand Virtual Standby. Its recovery time varies according to the amount of data restored, number of VMs restored, and available network bandwidth. Using this approach, On-demand Virtual Standby satisfies the less demanding RPOs, and RTOs associated with standard VMs.

Using On-demand Virtual Standby, organizations can immediately benefit as it offers them a higher return on their investment. On-demand Virtual Standby specifically equips organizations to quickly and easily recover any and every virtual machine in their IT infrastructure. Further, this solution offers the flexibility and scalability to meet the RPO/RTO requirements of most workloads in their business.

On-demand Virtual Standby offers the flexibility and scalability to meet the RPO/RTO requirements of most workloads.

UDP Instant Recovery Options for Business and Mission Critical VMs

UDP 10's new On-demand Virtual Standby feature complements UDP's two current instant recovery features designed for business and mission critical VMs.

- ***Instant VM.*** UDP's Instant VM creates a VM with a reference disk at a target recovery location. This reference disk contains the core data that a VM and its application need to boot. The remaining VM and applications data only gets read from the backup server when booting the VM. Using Instant VM, IT staff may quickly recover a VM directly from a backup without first needing to recover or rehydrate the backup. However, the Instant VM application's performance may be substandard until it restores all data from the backup.
- ***Virtual Standby (VSB).*** VSB offers a highly available configuration for data and applications for faster recoveries than Instant VM. VSB creates and maintains a standby VM with a recovery point at a target location that is ready to boot. Once configured, VSB constantly monitors the heartbeat of the source (production) node. Should VSB detect that the source node fails or goes off-line, the standby VM immediately takes over as the primary node.

Efficient Multisite Virtual Machine Backup Recovery

UDP 10's On-demand Virtual Standby gives organizations new flexibility to recover all their VMs almost anywhere. However, to quickly perform VM recoveries offsite or in the cloud, organizations must first move their data to these locations.

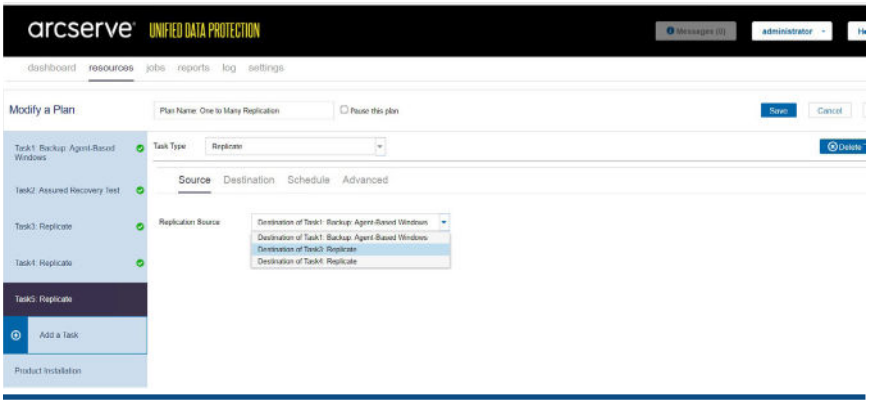
The threat of ransomware gives organizations further impetus to copy their backups to immutable data storage that also often resides in these locations. This threat means organizations should copy backups to different locations in a timely, reliable, and efficient manner.

To meet these various new organization needs, Arcserve UDP 10 introduces One-to-Many Replication Support.

The concept of one-to-many (1:M) replication (replicating a copy of data to multiple destinations) itself is not new. This technology has existed for some time. However, Arcserve UDP 10 manages 1:M replication in such a way that makes it practical for organizations to implement more widely.

Replicating a recently completed backup represents a common use case for UDP 10's One-to-Many Replication Support feature. Once UDP completes making a backup, UDP must replicate the backup to multiple replication target locations. These target locations may include an on-premises target, a target at a secondary location, or cloud object storage.

While simple in concept, replicating backups to multiple targets in different locations becomes problematic due to varying target response times. Backups replicated to an on-premises target may complete the write quickly, perhaps in a few milliseconds (ms). Backups replicated to a secondary site, or the cloud, may take longer to complete, perhaps a second or longer.



In this configuration, 1:M replication normally must wait until each replicated write completes at each target location. Only after each block of backup data gets written to all replication target locations does the next block of data get replicated. As a result, the replication target location with the highest latency determines the time for the entire replication process to complete.

UDP 10's implementation of 1:M replication ends this write co-dependency across all replication targets. UDP 10's One-to-Many Replication Support replicates each block of backup data to each replication target independently of the other targets. This technique ensures UDP One-to-Many Replication Support quickly creates a backup copy at the replication target location with the lowest latency.

UDP 10's One-to-Many Replication technology copies blocks of backup data to each replication target in parallel, independently of the other targets. This technology quickly creates a backup copy at the replication target location with the lowest latency.

It also permits organizations to create one replication job that replicates backups to multiple target locations regardless of each target location's latency. Latencies associated with each offsite and cloud target location can and do vary from one replication job to the next.

UDP 10's One-to-Many Replication Support feature overcomes this ever-present concern by successfully replicating backups to all the targets. It ensures replication to the target location with the lowest latency completes first. This refined approach to replication offers organizations greater resilience and assurance that they have successfully copied a backup to another location.

Going Deeper Yet with Microsoft SQL Server Restores

Arcserve has long prioritized providing in-depth data protection support for multiple databases. Further, in every UDP release, Arcserve ups its level of protection for one or more of these databases. Arcserve continues that trend in its UDP 10 release.

In UDP 10, Arcserve specifically more deeply integrates with Microsoft SQL Server by introducing new restore options. Now when restoring from a Microsoft SQL Server backup, organizations may extract a specific point-in-time copy of the database.

They may then mount this recovery point on the backup server and extract SQL content from it at a granular level. This granularity may be at an individual SQL Server database, table, or file level. Once extracted, UDP can then restore any of these individual components to a production Microsoft SQL Server database.

Faster, More Secure Recoveries for All Virtual Machines Highlights UDP 10 Release

Organizations recognize they must continue to take steps to ward off ransomware attacks. However, they cannot let concerns about ransomware stop their forward progress. They recognize they must continue to adopt hybrid cloud technologies even as they watch their bottom lines. To meet these competing objectives, organizations must identify solutions that address them.

Arcserve UDP 10 provides a reliable last-line-of-defense in the face of ransomware challenges that budget-conscious organizations face in their complex hybrid and multi-cloud environments.

Arcserve UDP 10 represents one such solution to which organizations can turn. UDP 10 already offers the core backup and recovery features that most organizations need. These include protecting multiple operating systems, databases, and endpoints, storing backups on multiple different targets, offering multiple Instant Recovery options, and using deduplication to minimize storage costs.

UDP 10 builds on these core competencies by capitalizing on the availability of Microsoft Defender within Microsoft Windows. Utilizing Defender, UDP 10 can affordably and reliably scan backups for malware to help organizations secure both their backups and restores.

Then using UDP 10's On-demand Virtual Standby feature organizations may quickly and securely recover any virtual machine anywhere from their backups. This includes performing fast VM recoveries on-premises, at secondary sites, and in multiple clouds to include AWS, Azure, and GCP.

This ability to quickly recover anywhere happens in large part thanks to UDP 10's new One-to-Many Replication Support feature. Organizations may use this feature to easily, confidently, and more quickly replicate backups to any location using one replication job.

Arcserve UDP 10 does more than help keep organizations ahead of the hybrid cloud and ransomware challenges they face. It positions them to fully, and affordably, capitalize on hybrid cloud functionality while better mitigating the threats that ransomware presents. In so doing, Arcserve UDP 10 provides a reliable last-line-of-defense in the face of ransomware challenges that budget-conscious organizations face in their complex hybrid and multi-cloud environments. ■