ASSURING DATA BACKUP SECURITY WITH ARCSERVE UNIFIED DATA PROTECTION

PROTECTING CRITICAL DATA BACKUPS FROM DATA LOSS AND UNAUTHORIZED ACCESS

Arcserve Unified Data Protection (UDP) includes a complete set of security technologies and mechanisms to ensure the safety and confidentiality of critical data backups, satisfying even the most stringent requirements. Security features include end-to-end encryption, role-based access management, backup infrastructure isolation, as well as comprehensive reporting, alerting and activity logging functionality.

ENCRYPTION AT-REST AND IN-TRANSIT

Arcserve UDP secures your confidential data before it leaves your production system, and in-transit to local, tape, remote and cloud disaster recovery storage. Your backups and files can be encrypted with advanced AES-256, AES-192 and AES-128 encryption at-rest on:

- **Local disks and shared folders**
- **Deduplicated datastores** on the Recovery Point Server (RPS)
- **Remote and cloud storage locations** for replicated backup copies, including in Amazon AWS and Microsoft Azure
- **Tape drives, autoloaders and libraries**
- **Target storage** for File Copy and File Archive tasks

In addition, your data is secure in-transit with SSL connection encryption throughout the entire backup infrastructure and beyond, including:

- All connections between Arcserve UDP Agents, the RPS, Console, and Arcserve Cloud
- Connections to proxy servers and email servers when sending email notifications
- VMware vSphere agentless backup with NBDSSL transport model
- Connections to all supported public clouds, including Amazon AWS, Microsoft Azure, Fujitsu, Appscale Eucalyptus Walrus, Nutanix Objects, Wasabi Hot Cloud Storage, Oracle Cloud, and more

AUTHENTICATION, AUTHORIZATION AND ROLE-BASED ACCESS CONTROL

To prevent unwanted access and data leaks, Arcserve UDP includes extended default and customizable configuration and features to ensure only authorized users access data backups and your data protection infrastructure. Arcserve UDP can leverage built-in local users or can be integrated with an organization's Active Directory to simplify user management

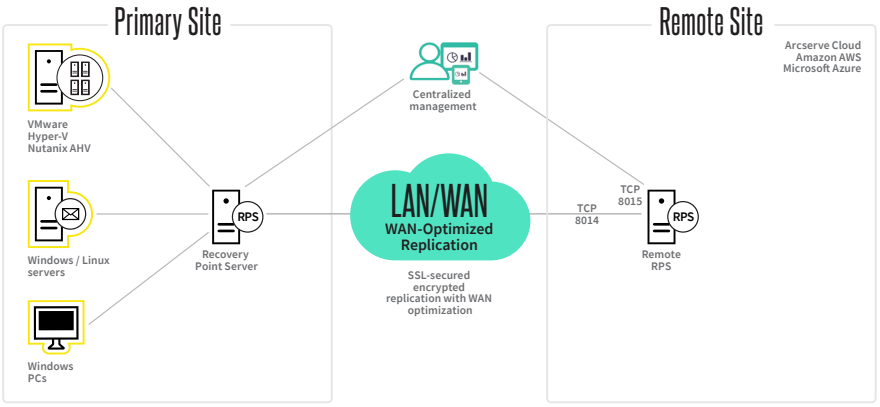
- By default, only administrators can use Arcserve UDP Agents and the RPS, and strict authentication is required for every access
- Advanced role-based access control (RBAC) functionality allows you to assign one of the pre-defined Admin, Backup, Restore, or Monitor role to users, or to define a new role with a set of permissions to more than three dozen individual features
- In Linux, Arcserve UDP components can operate under non-root user ID and use sudo command when administrative privileges are required

Arcserve UDP allows you to protect your data along Zero-Trust security strategies, satisfying the most stringent requirements of security-conscious organizations.

BACKUP INFRASTRUCTURE ISOLATION

Arcserve UDP is designed to operate in isolated environments and is largely self-sufficient.

- It requires a very small number of mainly non-standard TCP ports to be open for secure communication between its components, and the remaining operations are performed locally on the protected systems and RPS
- Its web-based interface operates over HTTPS and does not require opening potentially insecure ports, such as a remote desktop
- Periodic checks for available updates to its components are the only automated external internet query. If the environment is secure and completely isolated, the check can be disabled to prevent outbound connection attempt alerts of the firewall solutions
- Arcserve recommends keeping the Arcserve UDP backup servers unintegrated with larger Active Directories to minimize the potential attack surface of the data protection infrastructure
- When backups are replicated to remote or cloud locations, Arcserve recommends limiting direct connectivity between the networks only to the required ports – TCP/8014 to replicate data and TCP/8015 for centralized management, as shown in the diagram. This minimizes exposure of secondary backup copies in the event the primary site is attacked by hackers or ransomware



Arcserve UDP is designed for Zero-Trust security strategies and minimizes exposure of critical data backups to external threats

COMPREHENSIVE REPORTING, ALERTING AND LOGGING

Arcserve UDP includes advanced monitoring functionality to allow backup administrators rapid reaction and investigation of any aspect of backup infrastructure operations, including security.

- Multiple Arcserve UDP reports can be viewed ad-hoc or scheduled to be sent by email
- Automated email alerts can be sent for most backup operations so administrators can quickly address the issue
- Comprehensive job logs include all information necessary to investigate backup and infrastructure anomalies

Arcserve UDP allows backup administrators to be aware of anything in the backup infrastructure without having to log in to the console.

ABOUT ARCSERVE

Arcserve provides exceptional solutions to protect the priceless digital assets of organizations in need of full scale, comprehensive data protection. Established in 1983, Arcserve is the world's most experienced provider of business continuity solutions that safeguard multi-generational IT infrastructures with applications and systems in any location, on premises and in the cloud. Organizations in over 150 countries around the world rely on Arcserve's highly efficient, integrated technologies and expertise to eliminate the risk of data loss and extended downtime while reducing the cost and complexity of backing up and restoring data by up to 50 percent.

Explore more at www.arcserve.com