TECHNICAL WHITE PAPER

Best Practices: Active Directory Cyber Resilience with Rubrik Identity Recovery

Jarrod Shaver & Brent VanDyke
RWP-0664

Table of Contents

INTRODUCTION

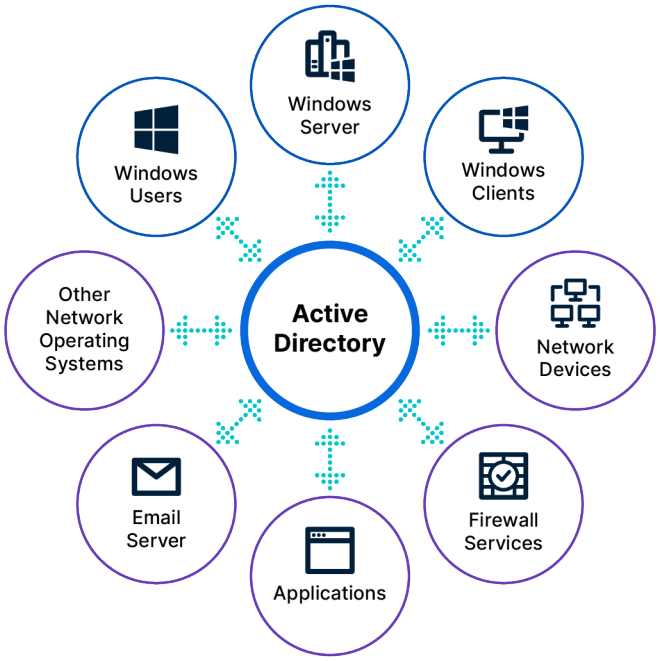
SUMMARY

Rubrik Identity Recovery, a component of Rubrik Security Cloud, addresses the critical need for resilient and efficient Active Directory (AD) protection. Leveraging Zero Trust Data Security principles, Rubrik Security Cloud delivers automated discovery and comprehensive protection for Active Directory implementations. It is designed to support enterprise-scale recovery operations, enabling organizations to restore entire forests, individual domains, domain controllers, specific objects, or even granular object attributes with precision and speed.

This document delineates best practices for safeguarding Microsoft Active Directory through Rubrik Security Cloud. It provides technical insights and guidelines to optimize AD protection, helping to streamline recovery processes.

THE NEED FOR ACTIVE DIRECTORY RESILIENCE

Microsoft Active Directory (AD) is critical in enterprise IT environments, serving as a comprehensive identity and access management service. It facilitates the authentication and authorization of users and applications. It often provides integral network services such as Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and public key infrastructure (PKI). AD's strategic significance and widespread utilization make it an attractive target for malicious actors. Recent trends in cyber threats indicate a shift from exploiting software vulnerabilities to compromising user identities, allowing unauthorized access to sensitive business systems and data.



When Active Directory or a Domain Controller is down or compromised, the path to operational recovery can be arduous and intricate. This complexity is exacerbated in expansive enterprise environments that necessitate the simultaneous restoration of multiple domains. Ensuring a swift and secure recovery process minimizes downtime and operational disruption.

CHALLENGES WITH PROTECTING ACTIVE DIRECTORY

Organizations face numerous challenges when protecting and recovering Microsoft Active Directory (AD), reflecting the complexity and critical nature of this infrastructure component. First and foremost, the highly distributed nature of AD environments can complicate monitoring and securing identity stores. Large enterprises typically operate across multiple domains and may utilize complex trust relationships, each presenting unique vulnerabilities that attackers can exploit. This fragmentation requires sophisticated management strategies and robust tools that can provide comprehensive protection across the entire AD architecture.

One of the primary challenges lies in the evolving threat landscape. Cyber adversaries are increasingly adept at circumventing traditional security measures by targeting user identities rather than software vulnerabilities. Once an identity is compromised, attackers can escalate privileges, move laterally within the network, and gain access to sensitive data and critical applications. The sophistication of these attacks requires organizations to implement advanced detection and response strategies that go beyond conventional perimeter defenses and focus on identity-centric security measures.

In the unfortunate event of an AD compromise, the recovery process poses significant operational hurdles. Restoration is not merely a matter of reinstating data; it requires precise and coordinated efforts to ensure the integrity and continuity of the identity services. The challenges multiply in larger environments, where multiple domains or domain controllers need to be recovered and synchronized. Additionally, organizations often rely on a collection of disparate tools for backup and recovery, which can lead to compatibility issues, inconsistent recovery points, and fragmented recovery efforts that slow down the overall process.

Another notable challenge is the security and integrity of backups themselves. Since AD contains sensitive identity and authentication information, backup solutions must secure this data against tampering and unauthorized access. Attackers have increasingly targeted backup repositories, recognizing them as high-value targets. Compromised backups can lead to prolonged recovery times and compounded security risks, as malicious actors may use the backup data to further infiltrate or ransom the organization. Therefore, implementing robust encryption mechanisms, regularly verifying backup integrity, and ensuring compliance with data protection regulations are critical components of a secure backup strategy.

These challenges highlight the need for sophisticated and comprehensive protection and recovery solutions. Technologies like Rubrik Security Cloud offer organizations the tools to meet these challenges head-on. They provide capabilities such as automated discovery, Zero Trust Data Security, and scalable recovery options to ensure that Active Directory remains resilient against modern threats and that recovery processes can be executed with minimal disruption.

PREPARING

PLANNING & PREREQUISITES

The following section will detail the key items to document and prerequisites to follow for adequately protecting your Microsoft Active Directory environment with Rubrik Security Cloud, which significantly enhances your organization's ability to recover from Active Directory issues. While these measures will improve your chances of restoring Active Directory during a cyber-attack or system failure, this guidance should not replace your organization's comprehensive disaster recovery plan. Instead, this document will help you create additional steps and measures to further protect and recover Active Directory within your existing disaster recovery strategy. Please note that this document is not a substitute for the Rubrik user and deployment guides; it is intended to supplement those resources.

Active Directory Prerequisites

There are no mandatory prerequisites for protecting Microsoft Active Directory with Rubrik Security Cloud; however, the following recommendations will enhance your protection:

- **Enable Active Directory Recycle Bin**[1]**:** While the Active Directory Recycle Bin is not necessary for Rubrik to protect Active Directory, Microsoft recommends enabling it to use Microsoft's native tools for recovering objects from it. Once enabled, Rubrik can also recover user passwords for the defined Deleted Object Lifetime (DOL) duration.

- **Prevent Object Accidental Deletion:** Microsoft recommends enabling the "Protect object from accidental deletion" feature. This feature provides an important safeguard to help prevent the accidental deletion of critical objects within Active Directory, such as user accounts, organizational units (OUs), and other essential directory objects. Rubrik Security Cloud does not require this, but will provide an additional layer of protection from malicious or accidental deletion of Active Directory objects.

- **Utilize Centralized Logging:** While not directly related to Active Directory backup, it is highly recommended that organizations implement a robust centralized logging solution. Organizations may consolidate logs from all domain controllers into a secure, centralized repository by directing events to a Security Information and Event Management (SIEM) system and employing Windows Event Forwarding (WEF). These solutions provide valuable insights into potential attacks on Active Directory and significantly enhance the effectiveness of incident response and recovery efforts.

[1] nabling the Active Directory Recycle Bin requires a schema change, and once enabled, it remains so permanently. Enabling the Recycle Bin will immediately delete all tombstone objects from Active Directory. For more details, refer to Microsoft's documentation covering this topic.

Rubrik Prerequisites

To ensure comprehensive protection and recovery of your Active Directory environment, the following prerequisites should be implemented: installing and maintaining the Rubrik Backup Service, creating and managing necessary service accounts, and configuring archival solutions and licensing. Meeting these prerequisites will help keep your backup and recovery operations secure, stable, and effective.

- **Verify Compatibility:** Consult the Rubrik Compatibility Matrix on the support portal to ensure your version of Rubrik CDM supports your Windows Server and Active Directory versions.
- **Install the Rubrik Backup Service (RBS):** The RBS must be installed on all Domain Controllers that Rubrik will protect.
- **Create a Group Managed Service Account (gMSA):** The RBS supports using gMSAs and recommends implementing them as part of your Rubrik deployment. gMSAs enhance security by providing automatic password management, reducing the risk of manual password handling and potential vulnerabilities. Additionally, they simplify the administration of service accounts by allowing multiple servers to share a single account, streamlining management and ensuring consistent access across services.
- **Configure SMB Security:** Since Rubrik utilizes the SMB protocol (SMBv3) for Active Directory backups, secure SMB must be configured within the CDM cluster responsible for protecting Active Directory Domain Controllers. This ensures backups occur over a securely encrypted communication protocol.
- **License Rubrik's Identity Recovery:** Rubrik's Foundation Edition provides backup and recovery for Active Directory Users, Groups, Containers, OUs, Computers, and Domain Controllers. A Rubrik Identity Recovery license is required to leverage Rubrik's ability to perform Forest Recovery, object attribute comparison, and attribute recovery.

WHAT TO DOCUMENT

DOCUMENTING YOUR ACTIVE DIRECTORY ENVIRONMENT

A thoroughly documented Active Directory (AD) environment is essential for robust data protection and disaster recovery. Accurate and comprehensive documentation clearly explains your AD architecture, configurations, and dependencies, enabling swift and precise action during incidents. Maintaining detailed records of your domain structure, policies, roles, and operational processes can enhance recovery speed, minimize downtime, and reduce the risk of misconfiguration.

Thus, it is crucial to collect and document the following information as part of your disaster recovery plan:

- **Document your Active Directory Environment:** Maintain an up-to-date Active Directory design document that includes forest structure, domain names, sites, trust relationships, and replication topology.
- **Document your Domain Controllers:** Include an inventory of all Domain Controllers, including their roles within the Active Directory Domain and Forest (e.g., Root Domain Controller(s), Flexible Single Master Operations (FSMO) owners, and Global Catalog Servers) as well as their Windows version.

- **Maintain a list of Custom Extensions:** Custom extensions to your Active Directory schema should be thoroughly documented, and changes should be updated as part of your change management procedures.

- **Document all Active Directory Dependencies:** Document and understand your Microsoft Active Directory dependencies within your environment. These may include external IP Management Solutions, Domain Name System (DNS), Network Time Protocol (NTP), and Dynamic Host Configuration Protocol (DHCP) hosted outside your Microsoft Active Directory deployment.

- **Deploy an Enterprise-Grade Password Management System:** Implementing an enterprise-level password management solution is highly recommended. At a minimum, securely document privileged Active Directory account information in your recovery plan, including Forest and Domain Administrator accounts, Directory Services Recovery Mode passwords, and any necessary BitLocker Recovery Keys for post-recovery system booting. If your environment uses rotating passwords, ensure that you can retrieve the administrative account passwords as they were at the time of the backup.

- **Document Non-Human Identities (NHI) / Service Accounts:** Ensure thorough and detailed documentation of all NHI within your Active Directory environment, such as Service Accounts and Group-Managed Service Accounts (gMSAs). This documentation should include specific permissions assigned to each account, as well as a comprehensive list of systems, applications, and services that use these accounts for authentication and authorization.

- **Document Privileged Groups & Users:** Documenting privileged groups and users is essential for maintaining a secure Active Directory environment. This includes providing detailed records of administrator groups, their memberships, and any user accounts with specific elevated privileges. Regularly update and review this documentation to ensure accuracy and adherence to security policies. Keeping thorough records helps manage access control and supports an effective incident response.

- **Document Critical Systems that Depend on Active Directory:** Critical systems and applications that rely on Active Directory for authentication should be detailed in your disaster recovery plan to prevent unnecessary recovery attempts for these systems, streamlining the recovery process.

Note: While the Directory Services Recovery Mode (DSRM) password is not required to use Rubrik's orchestrated recovery capabilities, saving and securing this password is advisable. Retaining the DSRM password ensures you can recover Domain Controllers using methods outside of Rubrik's orchestrated recovery capabilities if needed, and it also allows you to employ other troubleshooting methods that may require DSRM access.

DOCUMENTING YOUR RUBRIK ENVIRONMENT

Documenting your Rubrik environment is crucial for enhancing operational efficiency, ensuring consistency and standardization, and supporting effective disaster recovery. Additionally, such documentation aids in training and onboarding new team members, demonstrating compliance with regulatory requirements, and facilitating change management. Finally, comprehensive documentation streamlines troubleshooting and support and informs future planning and upgrades. The following items must be documented and added to your disaster recovery plan.

- **Document your Rubrik CDM Backup Environment:** Document and maintain comprehensive records of your Rubrik CDM cluster(s) physical locations, administrative users' account details, and multi-factor authentication (MFA) devices and configurations. Additionally, recognizing that DNS may not be available during incident response, IP configuration (including associated interfaces and VLANs) should be included.

- **Document Archival Target Details:** Ensure thorough documentation of Rubrik archival target information, including encryption keys, cloud account credentials, access keys, and any other pertinent details necessary for connecting to your archive target(s) (such as firewall rules, static routes or otherwise), along with any vendor-specific configuration requirements (e.g., Azure ExpressRoute details, source IP range limitations, et al.).

- **Keep Rubrik Software Current:** Integrate the updating of Rubrik clusters with the latest General Availability CDM release into your maintenance and patch management protocols. This practice helps mitigate the risk of exploitation through known vulnerabilities and ensures optimal performance.

- **Document Rubrik SLAs:** Document your Rubrik Service Level Agreements, specifying their applications, archival targets, and replication destinations

- **Map Business RPO/RTOs to Rubrik SLAs:** Outline your business Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), detailing how these objectives align with your configured Rubrik Service Level Agreements (SLAs).

BE PROACTIVE

PROACTIVE MEASURES

Taking proactive measures is essential for ensuring the security, stability, and efficiency of your Rubrik environment and Active Directory infrastructure. The following best practices focus on implementing robust access controls, comprehensive logging and notifications, regular disaster recovery drills, structured change management, secure administrative operations, and having a designated recovery team to effectively handle incidents. These steps collectively enhance your organization's resilience and readiness to respond to and recover from potential disruptions quickly.

- **Ensure Notification Configuration for Critical Events:** Proper notification configuration ensures the ability to respond promptly to events that may negatively impact your ability to recover if an incident response is needed. After ascertaining which key users and/or groups should act upon such events, ensure your organization's preferred notification mechanism is configured to alert the specified accounts.

Rubrik Security Cloud allows significant flexibility in notification management by integrating with other organizations' existing monitoring and alerting systems via webhooks, syslog, SNMP, or any combination thereof. Additionally, email alerts may be configured to notify users directly without needing separate systems or integrations.

- **Perform Regular Disaster Recovery Drills:** To validate the effectiveness of your recovery processes, routinely execute comprehensive forest and domain recovery simulations within a controlled lab environment. Integrating insights and lessons from these exercises can help you revise and enhance the recovery plan.

- **Deploy Change Management:** Implementing rigorous change management procedures in your Rubrik infrastructure enhances overall system stability, security, compliance, and operational efficiency, while also facilitating better communication, risk management, and resource allocation.

- **Consider Implementing Privileged Access Workstations (PAWs):** It is highly recommended that administrative operations within Active Directory, as well as within Rubrik and any other highly sensitive or critical infrastructure, be conducted exclusively from secure, hardened workstations. This approach enhances security by limiting access to sensitive infrastructure to a specific number of systems.

- **Designate a Recovery Team:** A designated recovery team for Active Directory disaster recovery incidents ensures a rapid and coordinated response, minimizing downtime and disruption to critical services. With in-depth knowledge of the AD environment and recovery procedures, this specialized team can swiftly execute the recovery plan, address any unforeseen issues, and efficiently restore directory services. Furthermore, a dedicated team enhances accountability and communication, helping to streamline decision-making and improving the overall effectiveness of the recovery efforts.

- **Generate a Protection Task Detail Report:** Create a custom Rubrik Security Cloud report filtered by Object Type "Active Directory Domain Controller" with a time frame that matches your retention period, as Rubrik may not always retain logging details that align with your business requirements. Schedule this report to be emailed regularly to ensure timely identification and resolution of failing jobs. This proactive approach supports compliance with business or regulatory requirements and offers insights into trends within the environment over time.

- **Permissions Control:** Recovery operations should be restricted to authorized personnel with elevated permissions to prevent unauthorized access and ensure the secure handling of backup data.

- **Maintain the Principle of Least Privilege:** Ensure that each user and group's access is restricted solely to the necessary systems and privilege levels. Rubrik Security Cloud user and group accounts should also be regularly audited.

- **Templates & Golden Images:** Create and maintain physical and virtual "golden image" templates corresponding to your Domain Controller's Windows version and hard disk drive layout. These prepared templates enable rapid host deployment and swift recovery of Active Directory Domain Controllers, making them essential during recovery operations.

BACKUP BEST PRACTICES

RUBRIK SLA DOMAIN BEST PRACTICES

Several best practices should be employed to safeguard your Active Directory environment and align with business and regulatory requirements. These include aligning Rubrik Service Level Agreements (SLAs) with business recovery objectives, retaining backups for sufficient durations, leveraging archive solutions with object-level immutability, and enabling features such as instant archive and backup replication. Rubrik's SLA inheritance feature can minimize human error and ensure consistent protection across your Active Directory infrastructure.

- **Align Business Recovery Objectives with SLA Domains:** To ensure regulatory compliance, implement Rubrik SLAs that align with your defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). These SLAs should be tailored to meet the stringent requirements set forth by your organization and any applicable governing bodies, industry standards, or compliance needs (e.g., GDPR, HIPAA, FIPS, or SOX) to maintain adherence to legal and operational mandates.

- **Leverage an Archive with Immutability:** To ensure the highest level of data protection for Active Directory, configure AD and its dependencies to back up and archive to an immutable storage location such as Rubrik Cloud Vault (RCV). This configuration prevents data modification and deletion, safeguarding your backups from ransomware attacks and inadvertent alterations. Additionally, redundancy options should be considered to meet business objectives related to data locality, redundancy, and access class. For the most current list of platforms Rubrik supports for immutable archival locations, please consult the Rubrik Compatibility Matrix.

- **Enable Instant Archive:** For SLAs assigned to Active Directory Domain Controllers and their dependencies, configure "instant archive" to store the latest backups in your designated archive target immediately. This ensures that you can quickly restore Active Directory to the most recent off-site recovery point in the event of a localized disaster.

- **Replicate Backups between Active Directory Sites:** In addition to utilizing an off-site target for archiving, take advantage of Rubrik's ability to replicate backups between sites using Rubrik clusters. This enhances protection against regional disasters. Configure your SLAs to replicate data from remote sites to your primary data center and from the primary data center to a secondary or tertiary location, potentially mirroring your Active Directory topology.

- **Prevent Alteration with Retention Lock:** Rubrik's Retention Lock enhances data protection by preventing the alteration or deletion of backup data for a specified period. This safeguards against accidental or malicious change and ensures compliance with regulatory requirements. This feature also defends against ransomware attacks and legal hold needs, maintaining the integrity and availability of critical backup data.

- **Leverage Rubrik's SLA Inheritance:** Utilize Rubrik's Autoprotect feature by assigning SLAs at the Forest Root or Domain level. This ensures that all Domain Controllers within the domain and forest automatically inherit these SLAs, including new domains and Domain Controllers, which will receive the appropriate SLA assignments automatically. This automated policy inheritance minimizes human error, ensuring consistent protection across your Active Directory environment and preventing gaps in backup coverage.

ACTIVE DIRECTORY BACKUP BEST PRACTICES

Rubrik's Active Directory backups capture crucial components such as the Domain Controllers' System State, SYSVOL, Registry, and NTDS.DIT database. By utilizing the VSS writer, Rubrik ensures that Active Directory backups occur in a consistent state, adhering to Microsoft's best practices for Active Directory backups. Because Rubrik securely backs up all these components, this approach enables AD to be recovered to an alternate host built with a standard template, providing flexibility in your disaster recovery strategy.

This section covers essential strategies for backing up Active Directory with Rubrik. Key practices include protecting Forest-Root Domain Controllers, FSMO role holders, and DNS servers, establishing a rigorous backup schedule, using local Rubrik clusters, and thoroughly documenting backup procedures. Additionally, avoiding relying solely on hypervisor snapshots is essential to ensure database consistency and quick recovery.

- **Protect the Active Directory Forest-Root Domain Controller(s):** Protect your Active Directory Forest-Root Domain Controllers. These Domain Controllers reside within the Forest Root Domain and host the Schema Master and Domain Naming Master roles.

- **Protect Domain Controllers in Each Domain:** Ensure that you are protecting at least one Domain Controller in each of the Domains within your Active Directory Forest.

- **Protect Domain Controllers with FSMO Roles:** Ensure the protection of your Active Directory Domain Controllers that hold FSMO roles for every domain within the Active Directory forest. When Domain Controllers are integrated into Rubrik Security Cloud, FSMO role owners are automatically discovered and documented within the user console, aiding in identifying and managing these critical roles.

- **Protect Active Directory DNS Servers:** If Active Directory DNS is hosted on servers that are not Domain Controllers or FSMO role holders, and is not yet protected by Rubrik, ensure it is protected using the same SLA assigned to your protected domain controllers.

- **Establish a Rigorous Backup Schedule:** Execute regular backups of your Active Directory environment, ideally every 4 to 12 hours, to capture frequent changes to AD objects. This consistent backup routine is crucial for ensuring that recent modifications are preserved and can be quickly restored in case of data loss or system failure.

- **Protect Domain Controllers with Local Rubrik Clusters:** If your Active Directory forest spans geographical sites, deploy either virtual or physical Rubrik clusters to protect the Domain Controllers at those locations. A localized backup copy increases recovery speed, as inter-site links or wide-area network connections may be unavailable during an incident or disaster response.

- **Document Backup Procedures:** Documenting your backup procedures is essential for maintaining consistency, ensuring operational continuity, supporting training and compliance, facilitating troubleshooting, enhancing disaster recovery planning, mitigating risks, managing changes, and improving overall communication within the organization.

- **Avoid Sole Reliance on Hypervisor Snapshots:** Relying exclusively on hypervisor snapshots for AD backups can lead to database consistency issues, as these snapshots may not capture the AD database in a consistent and application-aware state. This can result in recovery failures or significantly extended recovery times. To mitigate these risks, it is crucial to use Rubrik's native AD protection, ensuring

consistent and reliable backups for physical and virtual Domain Controllers. Moreover, if malware is present on a domain controller when a snapshot is taken, that malware will be restored along with the domain controller. Therefore, it is recommended that hypervisor snapshots be used in conjunction with Rubrik's AD protection. Hypervisor-based snapshots can be valuable in incident response within controlled environments.

- **Domain Controller Templates:** Incorporate your Domain Controller "Golden Image" templates into your backup plan. Ensure they follow the exact replication and archive policies as your Domain Controller-assigned SLAs. Additionally, these templates should adhere to the same update and patching schedules as their corresponding Domain Controllers.

CONCLUSION

Ensuring the resilience of your Microsoft Active Directory environment is paramount to maintaining your enterprise's critical identity and access management infrastructure. Rubrik Security Cloud's comprehensive protection and recovery capabilities, strategic planning, and diligent documentation provide a robust framework to safeguard your AD environment. By implementing the best practices outlined in this document, organizations can enhance their security posture, maintain compliance with regulatory requirements, and ensure swift and effective recovery during an incident. These proactive measures will significantly bolster your ability to manage and protect Active Directory, ensuring operational continuity and minimizing risks in today's ever-evolving threat landscape.

VERSION HISTORY

Version	Date	Summary of Changes	Author
1.0	March 2025	Initial Release	Jarrod Shaver & Brent VanDyke
1.1	April 2025	Minor corrections and updates	Jarrod Shaver & Brent VanDyke

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik (NYSE: RBRK) is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information please visit www.rubrik.com and follow @rubrikInc on X (formerly Twitter) and Rubrik on LinkedIn.

Rubrik is a registered trademark of Rubrik, Inc. All company names, product names, and other such names in this document are registered trademarks or trademarks of the relevant company.

rwp-active-directory-cyber-resilience-with-rubrik-identity-recovery / 20250821