rubrik

Rubrik Identity Recovery for Active Directory & Entra ID

Rubrik Security Cloud (RSC) Foundation, Business, and Enterprise Editions provide the base capability to natively protect Active Directory (AD) and Entra ID. Rubrik Identity Recovery, now available as a standalone offering, provides enhanced protection and recovery capabilities for identity services.

This sheet details the differences between these 2 distinct product sets.

ACTIVE DIRECTORY

Rubrik Security Cloud's native Active Directory protection leverages the Rubrik Backup Service (RBS) to call Microsoft's native Windows Server Backup Admin tool to generate backups of Active Directory that are then written to Rubrik's natively immutable, logically airgapped platform. Once the backup is written, the network share is closed, so that the backup data is not exposed to the network, where an attacker might be able to access it.

These backups can then be called on to recover individual domain controllers or even objects. RBS automatically discovers all domain controllers within a domain, including where the Flexible Single Master Operations (FSMO) roles reside, and other AD-associated roles, such as DNS server, when it is installed on a single domain controller.

In addition to this, Identity Recovery automatically discovers all domain controllers in all domains in the forest. SLA domains can be assigned at the forest, the domain, or the domain controller level. While Rubrik Security Cloud provides a global management plane for data protection, Rubrik Secure Vault clusters can be deployed close to the hosts, and backups taken locally. In the event that Active Directory is globally distributed, Rubrik Security Cloud orchestrates recovery across all required Rubrik Secure Vault clusters.

The recovery of Active Directory domains can be complex, especially when you consider how multiple domains are stitched together as tree and child domains in large forests. Rubrik Identity Recovery provides a simple-to-use, 5-step wizard-driven process that orchestrates the entire recovery of all domains within a forest, whether this is in-place or to alternate hosts, such as into an Isolated Recovery Environment (IRE). This latter method makes it easy to test the recovery of Active Directory without impacting production systems.

Outside of the ability to fully orchestrate the recovery of an entire AD forest, Identity Recovery provides a simple interface through which to compare the attributes of a selected object from any backup against that object's current state in Active Directory. Through this interface, it is simple to roll back only specific attributes for an object to a selected point in time, without otherwise affecting the object.

*Note that while installing RBS to a single host in a forest enables full autodiscovery of all domains and DCs in the forest, in order to take a backup, RBS **must** be installed on the AD Domain Controller.*

ENTRA ID

Entra ID is a cloud-native Identity Provider (IdP) that serves as the identity platform for Microsoft Azure and Microsoft 365. Formerly known as Azure Active Directory (Azure AD), it is distinct from traditional Active Directory and was developed from the ground up to support cloud-based identity and access management. Despite its previous name, Entra ID is not a cloud-hosted version of Active Directory but a separate service designed specifically for modern cloud environments.

Within Entra, there are many different types of objects to protect, from users, groups, and computers, as you may be familiar with from AD, to newer constructs such as Enterprise Apps and App Registrations. Beyond service principal objects like these, there are other object types to consider, too. For instance, Conditional Access Policies allow an administrator to define specific conditions under which to allow or disallow access to specific resources. For example, a user in a corporate office in Austin, Texas, might have access to specific applications, but if that same user were to be travelling, and attempt to access those same resources from an airport, it might be desirable that this access either be blocked, or only allowed when on VPN, and even then, enforce MFA for login.

All of these different constructs need to be protected so that they can be recovered in the event of a bad change,

whether accidental or malicious in nature, such as an object being edited or deleted.

Rubrik Security Cloud provides the ability to protect and recover users, groups, and roles in Foundation, Business, and Enterprise Editions. Unlike with Active Directory, this protection does not require the deployment of Rubrik Secure Vault clusters - in a cloud native model, it does not make sense to require the deployment of hardware into your data centers.

Whether you have Foundation/ Business/ Enterprise Edition or Identity Recovery, data protection for Entra is provided as a managed service, where Rubrik manages the backup storage. These backups are stored in the Azure cloud for quick and easy recovery, but in a tenant managed by Rubrik, providing a logical airgap between your Entra tenant and the backups. In the event that one of your Entra administrators were compromised, the compromised account has no access to the backups, so you can rest assured that you can recover.

Rubrik Security Cloud Foundation, Business, and Enterprise edition can protect and recover Users, Groups, and Roles. Rubrik Identity Recovery builds on this baseline, also protecting Enterprise Apps, App Registrations, Conditional Access Policies, Administrative Units, Devices, BitLocker Recovery Keys & Local Admin Passwords for Entra joined computers.

HYBRID RECOVERY

Thousands of organisations worldwide are still Active Directory only. Many have completed their journey to the cloud, so they are Entra only. However, the vast majority of businesses are operating a hybrid model where they deploy Entra Connect to servers within Active Directory to synchronize some or all user accounts into Entra. In this scenario, one or more Active Directory domains can be synchronized into a single Entra tenant.

Objects synchronized into Entra from AD represent something of a challenge from a protection perspective. While these objects in many cases may have Entra-specific attributes associated with them, it is not possible to recover them directly to Entra in the event of an issue. Instead, the recovery workflow would be to recover the objects first into Active Directory, from which Entra Connect would sync them into Entra. Once synced into Entra, the Entra-specific attributes can be recovered.

This extra administrative overhead can be a significant burden, especially when using multiple tools, or when recovering at scale. Rubrik Identity Recovery includes an improved workflow that handles this whole recovery process end-to-end.

	Foundation/ Business/ Enterprise Edition	Identity Recovery
Protection at Domain level	✓	✓
Protection at Forest level		✓
Recover Objects	✓	✓
Recover Object Attributes		✓
Object Attribute Comparison		✓
Recover Individual Domain Controllers	✓	✓
Recover Domains	✓	✓
Fully orchestrated AD forest recovery		✓
Entra ID Users, Groups & Roles protection and recovery	✓	✓
Entra ID Enterprise Apps, App Registrations, Conditional Access Policies & Administrative Units		✓
Devices, BitLocker Recovery Keys, Local Admin Password for Entra joined computers		✓
Hybrid Recovery		✓

SUMMARY

Rubrik Identity Recovery delivers completely orchestrated recovery of Active Directory forests, Entra ID, and hybrid environments with a single subscription license. With Identity Recovery, you get robust, assured recoverability for on-premises and cloud identity services, without the need to manage multiple tools.

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.

ds-rubrik-identity-recovery / 20260113