rubrik

Identity Recovery for Microsoft Entra ID

Modern enterprises depend on Microsoft Entra ID (formerly Azure Active Directory) as the backbone of identity and access management. It governs authentication, enforces security, and connects users to critical SaaS and cloud applications. While Entra ID provides native protections, it is not designed for comprehensive recovery in the face of ransomware, insider threats, or accidental deletions.

Rubrik Identity Recovery solves this by providing orchestrated, immutable, and hybrid-aware backup and recovery across both Active Directory (AD) and Entra ID. This paper focuses on Entra ID, the keys to the kingdom when it comes to access to cloud, SaaS, and hybrid workloads and data stores..

THE CHALLENGES OF PROTECTING ENTRA ID

Many organizations still believe that by running a service in the cloud, the cloud provider is responsible for the protection of the data, including backups. However this is not the case as there is a shared responsibility model at play. In the case of Entra, Microsoft is responsible for the *availability* of Entra ID, but not the administration or back up of it.

Microsoft provides the Entra ID Recycle Bin, which comes with some benefits, such as objects being recovered with the same ObjectID, and relationships intact, there are a number of challenges to be aware of:

⚠ **Limited Retention:** Objects are only recoverable for up to 30 days. Beyond this period, they are permanently deleted.

✕ **No Air Gap:** Deleted objects held in the Recycle Bin are stored within the same tenant as your production data, making them susceptible to a logical or malicious attack that compromises the entire Entra ID tenant. If an adversary is able to compromise an administrative identity, they will very likely purge the Recycle Bin.

Considerations for Third-Party Protection

Those who are aware of the limitations of the Recycle Bin may invest in third party tooling to take data backups of Entra ID. When researching the capabilities of these tools, it is key to pay special attention to any of the following functionality gaps, which may be painful to remediate when it comes to performing a recovery.

✕ **No Air Gap:** While some tools will claim that storing your Entra backups in your own Azure tenant provides greater security, consider the use cases that you are protecting against. As with the Recycle Bin, if there is an administrative compromise, it is unlikely that your backups will survive. In this scenario, recovery may be impossible.

✕ **Lack of Granularity:** In many cases, there is no capability to perform on-demand backups, or restore specific relationships between objects, which is critical for a full and functional recovery.

✕ **No Orchestrated Recovery:** Without orchestration, there is no unified way to protect and recover hybrid environments, where users and groups are provisioned from on-premises Active Directory (AD) into Entra ID. Hybrid objects cannot be recovered directly into Entra, and must first be restored to AD, then reprovisioned into Entra, and finally, the hybrid object's attributes must be restored to the newly provisioned Entra object. Without this, application assignments, conditional access policies, and more will require manual reconfiguration. Add the scale of the cloud in, and this could be a very time consuming, and error-prone process.

RUBRIK'S APPROACH TO IDENTITY RECOVERY

Rubrik Security Cloud enhances and extends Entra ID's native capabilities by providing a logically air-gapped, immutable, and orchestrated recovery solution. More than a feature, identity recovery is a core component of your security strategy.

Enhanced Protection

Rubrik's Identity Recovery solution builds on the native Entra ID Recycle Bin with key enhancements:

Increased Retention & Frequency: Take on-demand and policy-driven backups of Entra ID, and retain snapshots for as long as required, providing a robust historical record.

Unified Management: Manage backups for Entra ID, Microsoft 365, on-premises workloads, and other cloud-native assets from a single interface.

Immutable Backups: Snapshots are stored in a Rubrik-managed Azure tenant, providing a **logically air-gapped** copy of your identity data that's safe from accidental deletion or tampering. This is crucial for ransomware recovery, or administrative compromise.

Orchestrated Recovery: Restore not just individual users, but also their group memberships, administrative unit assignments, and critical relationships. This ensures a faster, more complete return to normal operations.

Hybrid and Multi-IdP Orchestration

Most enterprises operate in a hybrid identity model, where users flow between AD and Entra ID. This makes recovery especially complex.

Rubrik orchestrates the process:

1. **Recover the user object in Active Directory.**
2. **Once recovered into Active Directory, Entra Connect/Cloud Sync provisions the user into the Entra ID tenant as a new object.**
3. **Entra-specific attributes and policies are restored to the newly provisioned Entra ID object from Rubrik's immutable backup.**

This ensures identities are rebuilt end-to-end, which is something native tools simply cannot do.

ENTRA TECHNICAL OVERVIEW

Rubrik's protection process is simple and secure.

- **Authorization** uses a secure OAuth workflow to create a service principal in your Entra ID directory. This grants Rubrik the minimum required permissions to interact with the Microsoft Graph APIs, ensuring a least-privilege approach to security.
- **Backups** are initiated based on a customizable Service Level Agreement (SLA) policy. Rubrik's Exocompute framework, deployed in a Rubrik-managed Azure tenant, pulls a delta of changes from your Entra ID environment. This metadata is then stored immutably in a separate, logically air-gapped storage account.
- **Recovery** is streamlined withRubrik restoring from its immutable backup. It reconstructs the object along with its relationships, ensuring a full and complete recovery, even if the original object ID is lost.

Key Differentiators

Feature	Microsoft Entra ID Recycle Bin	Rubrik Identity Recovery
Recovery Window	Up to 30 days	Customizable (years)
Backup Location	Same platform as production data	Logically air-gapped and immutable
Management	Separate interfaces per IdP	Single pane of glass for all data
Administrative Compromise/ Ransomware	Vulnerable to logical attack	Immutable and air-gapped
Hybrid Recovery	Not supported	Orchestrated recovery from AD to Entra

Identity is the new perimeter, and attackers know it. Compromise of Entra ID or AD can lock users out of applications, disrupt authentication and authorization across the enterprise, and grind operations to a halt. Rubrik Identity Recovery ensures:

- Faster, complete recovery from deletions or attacks.
- Immutable, air-gapped protection for your most critical system.
- Confidence across hybrid environments by orchestrating AD + Entra recovery.

With Rubrik, identity recovery becomes more than a feature, it becomes your last line of defense for business continuity, strengthening your identity and cyber resilience, ensuring you can withstand and recover from even the most sophisticated attacks.

rubrik

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

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

brf-identity-recovery-for-microsoft-entra-id / 20250912