



Rubrik Identity Resilience

Identity First Recovery for Active Directory

Restore a Clean Directory to Any Target, Up to 56% Faster.

Active Directory (AD) is the Tier-0 service at the center of nearly every enterprise identity stack. More than [90%](#) of global businesses and 95% of the Fortune 1000 run on it, and Mandiant reports that nearly [9 in 10](#) intrusions involve it. When AD goes down, everything goes down. A full Active Directory Forest Recovery (ADFR) is one of the hardest tasks in disaster recovery, a largely manual playbook that can take weeks, and while the Identity and Access Management (IAM) team works through it, the business stays offline.

Why Traditional Forest Recovery Fails

Rubrik has long supported ADFR through System State Recovery (SSR) and Bare Metal Recovery (BMR), and both remain the right tool for surgical jobs such as restoring a single failed domain controller. But both bind the AD database to the operating system (OS) it was backed up from. In a full forest compromise, that coupling creates two problems:

- **Environment Rigidity:** the target machine has to match the source: hypervisor, patch level, drivers, disk layout. Real recoveries land on new cloud instances or different hardware, and the small discrepancies fail the restore at the moment speed matters most.
- **The Malware Persistence Trap:** malware lives in OS binaries, DLLs, and registry hives. Restore the full image and you restore the attacker's persistence with it, live again the moment the domain controller powers on.

Recover the Directory, Not the Whole Machine

Rubrik Identity First Recovery (IFR) recovers the directory into a clean OS instead of restoring the OS it came from. Rubrik extracts ntds.dit, the core database of every AD object, schema, and hash, plus SYSVOL, and reintroduces them into a fresh Windows Server instance you provide, on-premises or in the cloud. The OS layer, and everything an attacker planted in it, is left behind.

IMAGE-BASED RESTORE

60 GB+

Full system image, OS included

Target must match the source

Restores OS-level persistence

IDENTITY FIRST RECOVERY

About 2 GB

Directory only: ntds.dit and SYSVOL

Any clean Windows Server target

Persistence stays behind

Decouple identity data
from the OS



Move a roughly 2 GB identity database instead of a 60 GB system image: less to transfer, and nothing infected to carry over.

Up to 56%

faster recovery in Rubrik's internal testing (500 MB AD database)

28 Steps

in Microsoft's forest recovery playbook, most of them manual

150+ Pages

of guidance to work through while the business is offline

How Identity First Recovery Works

Three capabilities make the recovery clean, automated, and portable:

STEP 01

Security Built Into Recovery

Every AD snapshot is checked continuously against Rubrik's threat intelligence feeds through Rubrik Threat Hunting and Threat Monitoring, looking for known indicators of compromise such as adversary-created Group Policy Objects and planted scripts. Verdicts appear inside the recovery wizard, so IAM teams pick a clean point in time without raising a ticket to security and waiting days.

STEP 02

Automated Target Host Preparation

You provide a plain Windows Server instance. Rubrik verifies the local system account, renames the host to assume the source domain controller's identity, installs the AD DS role, promotes the new domain controller, restores the directory data, recovers the original boot key from the mounted snapshot, and re-encrypts the password encryption key against the new host.

STEP 03

Recovery to Any Clean Target

No more matching the source machine's patch level, drivers, or hypervisor. IFR is any-to-any: physical to virtual, across a hypervisor upgrade, or onto cloud instances, as long as the target runs the same major Windows Server version as the source.

Cluster	Cluster Type	Snapshot
cdm-cluster-r85afc-nmc0mty	Source	26/08/2026 10:24

Identity First Recovery is the recommended method in the Active Directory Forest Recovery wizard. SSR and BMR remain available.

Business Value

- **A Clean Point in Time, Proactively:** recover to a vetted snapshot instead of rolling back to a stale, potentially infected one, and stop waiting on security to validate snapshots in a separate tool.
- **Accelerated Forest Recovery:** less data to move and a faster path back. In Rubrik's internal testing, IFR cut recovery times by up to 56% for AD databases of around 500 MB.
- **Recovery Beyond Your Data Center:** the OS is independent of the backup, so the forest can come back on virtual machines, across a hypervisor upgrade, or on cloud instances.

Available Now: Identity First Recovery is part of Rubrik Identity Resilience for Active Directory and requires Rubrik Cloud Data Management (CDM) version 9.5.3p2 or later.

Schedule a Demo >

SAFE HARBOR

Any unreleased services or features referenced on this page are not currently available and may not be made generally available on time or at all, as may be determined in our sole discretion. Any such referenced services or features do not represent promises to deliver, commitments, or obligations of Rubrik, Inc. and may not be incorporated into any contract. Customers should make their purchase decisions based upon services and features that are currently generally available.

NOTE

Please speak to Rubrik representatives to confirm the availability and functionality of Rubrik's products and services before making any purchase or renewal decisions.



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

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

Rubrik (RBRK), the Security and AI company, operates at the intersection of data protection, cyber resilience and enterprise AI acceleration. The Rubrik Security Cloud platform is designed to deliver robust cyber resilience and recovery including identity resilience to ensure continuous business operations, all on top of secure metadata and data lake. Rubrik's offerings also include Predibase to help further secure and deploy GenAI while delivering exceptional accuracy and efficiency for agentic applications.

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.