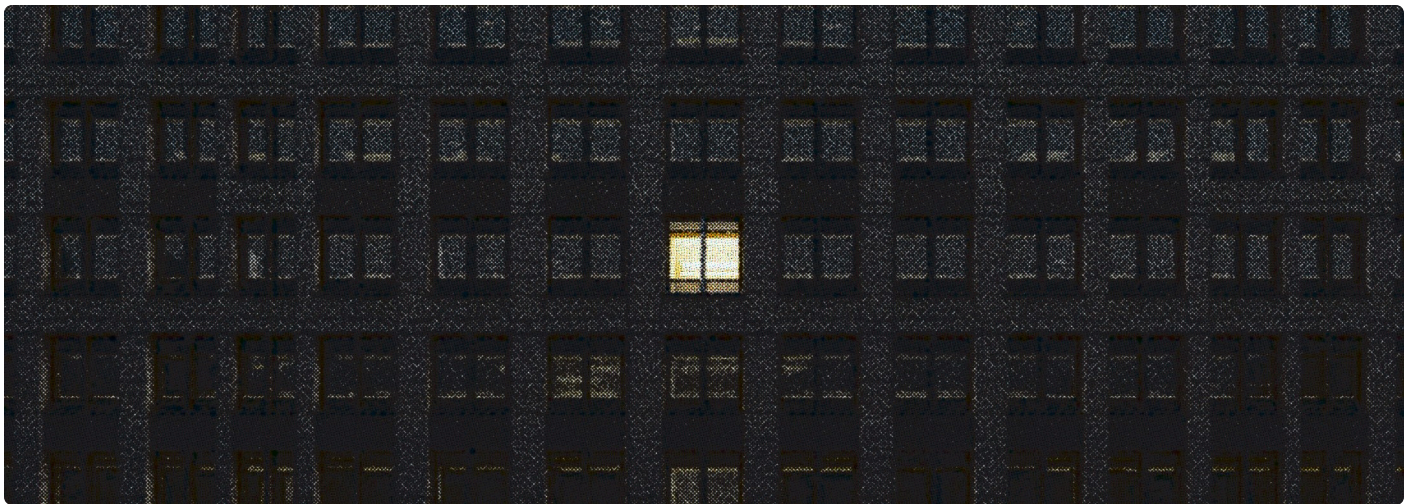


GUIDE · IDENTITY RECOVERY

After an attack, recovery starts with identity.

Almost everything else depends on it. Until Active Directory and Entra ID are trustworthy again, people can't sign in, and restored applications and data can't be used safely. This guide covers what to protect, the two kinds of identity recovery, and the order a forest rebuild follows.



9 in 10

cyberattacks involve Active Directory

50–100+

tasks in a manual AD forest recovery

Days–weeks

typical manual AD recovery time

Source: Commvault Active Directory protection, citing a Dark Reading 2021 estimate for attacks involving AD.

WHAT TO PROTECT

The directory, and everything that hangs off it.

Active Directory

Users, groups, group policy objects and the relationships between them, recoverable down to a single object or attribute.

Entra ID

Users, groups, roles, conditional access policies and app registrations, so deleted or modified objects can be restored and access comes back.

TWO KINDS OF RECOVERY

One bad change, or the whole forest.

Object restore

Rolls back the individual users, groups, policies or attributes that were deleted or changed, so only what broke is touched.

Forest recovery

Rebuilds Active Directory itself, domain controller by domain controller, when the whole directory is compromised.

RUNBOOK OUTLINE

A forest recovery, in order.

An outline to build your own runbook from. Done by hand, these steps run to dozens of tasks; automated, runbook-driven recovery handles most of them and shows progress as it goes.

01	Declare and contain	Stop the spread: isolate affected systems and agree who leads the recovery and how the team communicates.
02	Find a known-clean point	Compare the directory between two points in time to see exactly what changed, and choose the last backup taken before the attack.
03	Pick the restore order	Use the topology to decide which domain controllers come back first, usually one per domain.
04	Restore the first domain controllers	Bring the first DC in each domain back from the clean backup, isolated from the compromised network.
05	Run the consistency tasks	Seize FSMO roles and adjust the RID pool, as Microsoft's forest recovery guidance describes.
06	Rebuild the rest	Restore or promote the remaining domain controllers to rebuild the pre-incident infrastructure.
07	Reset privileged credentials	Reset administrator and service account passwords, and the KRBTGT account, before anyone signs in again.
08	Restore Entra ID and validate	Restore deleted or changed Entra ID users, groups, roles and conditional access policies, then confirm people can sign in before applications come back.

TEST IT FIRST

Prove it before an attacker forces you to.

Run forest recovery in a non-production lab, so the process is proven before you need it. KELYN plans and runs those tests with you.

- 01 Do you back up Active Directory and Entra ID frequently, including roles, policies and relationships?
- 02 Could you restore a single deleted user, group or attribute without a full rollback?
- 03 Is there a written, tested forest recovery runbook, and who owns it?
- 04 Have you run forest recovery in a non-production lab in the last year?

HOW KELYN HELPS

 Commvault protects the directory; KELYN runs the recovery, from a single deleted group to a full forest rebuild. Talk to a recovery engineer: sales@kelyntech.com · 1-888-937-1230.