

Rubrik Identity Recovery

Rubrik Security Cloud (RSC) ist als Foundation, Business und Enterprise Edition verfügbar und stellt die grundlegenden Funktionen bereit, die für den nativen Schutz von Active Directory und Entra ID erforderlich sind. Rubrik Identity Recovery ist nun auch als alleinstehende Lösung verfügbar und bietet zusätzliche Sicherungs- und Wiederherstellungsfunktionen für Identitäts-Services.

Dieses Datenblatt zeigt die Unterschiede zwischen diesen beiden Produktangeboten auf.

ACTIVE DIRECTORY (AD)

Die native Active Directory-Sicherung von Rubrik Security Cloud nutzt den Rubrik Backup Service (RBS), um das native Microsoft-Tool Windows Server Backup Admin aufzurufen und Backups von Active Directory zu erstellen, die anschließend auf der nativ unveränderlichen, durch logische Air Gaps geschützten Plattform von Rubrik gespeichert werden. Sobald das Backup gespeichert ist, wird die Netzwerkfreigabe geschlossen, damit die Backups nicht über das Netzwerk (und damit möglicherweise auch für Angreifer) erreichbar sind.

Diese Backups können dann genutzt werden, um einzelne Domänencontroller oder sogar einzelne Objekte wiederherzustellen. RBS erkennt und katalogisiert automatisch alle Domänencontroller in einer Domäne und auch, wo die Rollen für Flexible Single Master Operations (FSMO) gespeichert sind. DNS-Server und andere mit AD verbundene, auf einem einzigen Domänenserver installierte Rollen werden ebenfalls katalogisiert.

Darüber hinaus erkennt Identity Recovery automatisch sämtliche Domänencontroller in allen Domänen im AD Forest. SLA-Domänen können auf Forest-, Domänen- oder Domänencontroller-Ebene zugewiesen werden. Während Rubrik Security Cloud eine globale Managementebene für die Datensicherung bereitstellt, können Rubrik Secure Vault-Cluster in der Nähe der Hosts bereitgestellt werden, um Backups vor Ort zu erstellen. Für global verteilte Active Directory-Umgebungen orchestriert Rubrik Security Cloud die Wiederherstellung über alle benötigten Rubrik Secure Vault-Cluster hinweg.

Die Wiederherstellung von Active Directory-Domänen kann sich als komplex erweisen, insbesondere, wenn es sich um große Forests mit zahlreichen, zu Tree- und Tochterdomänen verbundenen Domänen handelt. Rubrik Identity Recovery stellt einen einfachen, aus fünf Schritten bestehenden, assistentengestützten Prozess bereit, der die gesamte Wiederherstellung für alle Domänen in einem Forest orchestriert – unabhängig davon, ob die Wiederherstellung am ursprünglichen Speicherort oder auf einem anderen Host, zum Beispiel in einer Isolated Recovery

Environment (IRE), stattfinden soll. Mit letzterer Methode kann die Wiederherstellung von Active Directory getestet werden, ohne die Produktionssysteme zu beeinträchtigen.

Neben der Möglichkeit, einen ganzen AD Forest wiederherzustellen, bietet Identity Recovery auch eine benutzerfreundliche Oberfläche, von der aus die Eigenschaften eines ausgewählten Objekts in einem beliebigen Backup mit dem aktuellen Zustand des Objekts in Active Directory verglichen werden können. Von derselben Oberfläche aus lassen sich einzelne Eigenschaften eines Objekts zu ihrem Zustand zu einem ausgewählten Zeitpunkt zurücksetzen, während die anderen Eigenschaften des Objekts unverändert bleiben.

Hinweis: RBS muss nur auf einem einzigen Host in einem AD Forest installiert sein, um sämtliche Domänen und Domänencontroller in diesem Forest zu erkennen. Zur Erstellung von Backups muss RBS jedoch auf dem Domänencontroller von Active Directory installiert sein.

ENTRA ID

Entra ID ist ein Cloud-nativer Identitätsanbieter, der als Identitätsplattform für Microsoft Azure und Microsoft 365 genutzt wird. Der vormalig als Azure Active Directory (Azure AD) bezeichnete Service wurde von Grund auf für das Cloud-basierte Identitäts- und Zugriffsmanagement entwickelt. Trotz seines früheren Namens handelt es sich also nicht um eine in der Cloud gehostete Version von Active Directory, sondern um einen eigenständigen, speziell für moderne Cloud-Umgebungen entwickelten Service.

Entra schützt viele verschiedene Arten von Objekten, von Benutzerkonten, Gruppen und Computern (mit denen Sie vielleicht schon von AD vertraut sind) bis hin zu neueren Konstrukten wie Unternehmensanwendungen, Anwendungsregistrierungen und darüber hinaus. Mit Richtlinien für bedingten Zugriff können Administratoren beispielsweise bestimmte Bedingungen festlegen, unter denen der Zugriff auf gewisse Ressourcen gestattet oder verwehrt werden soll. So könnte ein Benutzer beispielsweise Zugang zu bestimmten Anwendungen erhalten, wenn er sich in einem Büro seines Unternehmens in Düsseldorf befindet. Wenn derselbe Benutzer jedoch unterwegs ist und zum Beispiel von einem Flughafen aus auf dieselben Anwendungen zugreifen will, könnte es erwünscht sein, diesen Zugriff entweder ganz zu verwehren oder nur zu gestatten, wenn der Benutzer ein VPN benutzt. Selbst dann könnte zusätzlich eine Multi-Faktor-Authentifizierung erzwungen werden.

All diese verschiedenen Konstrukte müssen geschützt werden, damit sie wiederhergestellt werden können, falls

sie versehentlich oder böswillig auf unerwünschte Weise geändert oder gelöscht werden.

Funktionen zur Sicherung und Wiederherstellung von Benutzerkonten, Gruppen und Rollen sind in der Foundation, Business und Enterprise Edition von Rubrik Security Cloud enthalten. Im Gegensatz zu Active Directory sind für diese Sicherung keine Rubrik Secure Vault-Cluster erforderlich, da die Installation von Hardware in Ihrem Rechenzentrum nicht zu einem Cloud-nativen Modell passen würde.

Unabhängig davon, ob Sie die Foundation, Business oder Enterprise Edition oder Identity Recovery verwenden, wird die Datensicherung für Entra als Managed Service bereitgestellt, wobei Rubrik die Speicherung der Backups verwaltet. Diese Backups werden in der Azure-Cloud gespeichert, um eine schnelle und einfache Wiederherstellung zu ermöglichen. Aus Sicherheitsgründen handelt es sich dabei jedoch um eine von Rubrik verwaltete Mandantenumgebung, die durch eine logische Air Gap von Ihrem Entra-Mandanten isoliert ist. Selbst wenn Cyber-Kriminelle die Kontrolle über eines Ihrer Entra-Administratorkonten erlangen, können sie nicht auf die Backups zugreifen. Diese stehen also weiterhin für die Wiederherstellung zur Verfügung.

Die Foundation, Business und Enterprise Edition von Rubrik Security Cloud eignen sich zur Sicherung und Wiederherstellung von Benutzerkonten, Gruppen und Rollen. Rubrik Identity Recovery baut darauf auf und schützt zusätzlich Unternehmensanwendungen, Anwendungsregistrierungen und Richtlinien für bedingten Zugriff.

HYBRIDE WIEDERHERSTELLUNG

Tausende von Organisationen weltweit nutzen bislang nur Active Directory. Viele andere haben die Migration in die Cloud abgeschlossen und benutzen nur Entra. Doch die überwältigende Mehrheit der Unternehmen benutzt ein Hybrid-Modell, in dem Entra Connect auf Servern in Active Directory eingesetzt wird, um einige oder alle Benutzerkonten mit den äquivalenten Entra-Konten zu synchronisieren. In diesem Szenario können eine oder mehrere Active Directory-Domänen mit einem einzigen Entra-Mandanten synchronisiert werden.

In puncto Sicherung stellen diese von AD aus zu Entra synchronisierten Objekte allerdings eine Herausforderung dar. Obwohl sie oft Entra-spezifische Eigenschaften aufweisen, können sie nach einem Vorfall nicht direkt in Entra wiederhergestellt werden. Stattdessen müssen sie zuerst in Active Directory wiederhergestellt und dann von Entra Connect zu Entra synchronisiert werden. Nach der Synchronisierung können dann die Entra-spezifischen Eigenschaften wiederhergestellt werden.

Dieser zusätzliche administrative Aufwand kann eine erhebliche Belastung darstellen, insbesondere, wenn mehrere Tools genutzt werden müssen oder die Wiederherstellung sehr umfangreich ist. Rubrik Identity Recovery enthält einen verbesserten Workflow, der den gesamten Wiederherstellungsprozess vom Anfang bis zum Ende abdeckt.

	Foundation/ Business/ Enterprise Edition	Identity Recovery
Schutz auf Domänen-Ebene	✓	✓
Schutz auf Forest-Ebene		✓
Wiederherstellung von Objekten	✓	✓
Wiederherstellung von Objekteigenschaften		✓
Vergleich von Objekteigenschaften		✓
Wiederherstellung einzelner Domänencontroller	✓	✓
Wiederherstellung von Domänen	✓	✓
Vollständig orchestrierte Wiederherstellung eines AD Forests		✓
Sicherung und Wiederherstellung von Entra ID-Benutzern, -Gruppen und -Rollen	✓	✓
Entra ID-Unternehmensanwendungen, Anwendungsregistrierungen und Richtlinien für bedingten Zugriff		✓
Hybride Wiederherstellung		✓

ZUSAMMENFASSUNG

Rubrik Identity Recovery deckt mit einer abonnementbasierten Lizenz die vollständig orchestrierte Wiederherstellung von Active Directory Forests, Entra ID- und Hybrid-Umgebungen ab. Mit Identity Recovery erwerben Sie eine zuverlässige, gesicherte Wiederherstellbarkeit für lokale und Cloud-basierte Identitäts-Services, ohne mehrere Tools verwalten zu müssen.



Hauptsitz
3495 Deer Creek Road
Palo Alto, CA 94304
USA

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

Rubrik (NYSE: RBRK) hat es zu seiner Mission gemacht, die Daten der Welt zu sichern. Mit Zero Trust Data Security™ helfen wir Unternehmen, sich vor Cyber-Angriffen, böswilligen Insidern und Betriebsunterbrechungen zu schützen. Rubrik Security Cloud basiert auf maschinellem Lernen und sichert Daten im Unternehmen, in der Cloud und in SaaS-Anwendungen. Wir unterstützen Unternehmen bei der Wahrung der Datenintegrität, der Sicherstellung der Datenverfügbarkeit auch unter widrigen Umständen, der kontinuierlichen Überwachung von Datenrisiken und -bedrohungen sowie der Wiederherstellung von Unternehmensdaten nach einem Angriff auf die Infrastruktur.

Weitere Informationen finden Sie unter www.rubrik.com/de, unter [@rubrikinc](https://twitter.com/rubrikinc) auf X (ehemals Twitter) sowie unter [Rubrik](https://www.linkedin.com/company/rubrik) auf LinkedIn.

Rubrik ist eine eingetragene Marke von Rubrik, Inc. Alle Firmennamen, Produktnamen und weiteren Bezeichnungen in diesem Dokument sind eingetragene Marken oder Marken des jeweiligen Unternehmens.