Rubrik Identity Recovery

Rubrik Security Cloud (RSC) のFoundation、Business、Enterpriseの各Editionは、Active DirectoryとEntra IDをネイティブに保護するための基盤となる機能を提供しています。Rubrik Identity Recoveryは現在、スタンドアロン製品としてご利用いただけます。アイデンティティサービスの保護と復旧を目的とした高度な機能を備えます。

本資料ではActive DirectoryとEntra IDという異なる2つの製品セットの違いについて詳しく説明します。

ACTIVE DIRECTORY

Active DirectoryにネイティブなRubrik Security Cloudの保護機能では、Rubrik Backup Service (RBS) を利用してMicrosoft標準搭載のWindows Server Backup管理ツールを呼び出し、Active Directoryのバックアップを生成します。次に、生成したバックアップをRubrikの完全隔離かつネイティブに書き換え不可のプラットフォームに書き込みます。バックアップが書き込まれるとネットワーク共有は閉じられるため、そのバックアップは攻撃者がアクセスできる可能性があるネットワークには開示されなくなります。

このバックアップを呼び出すことで、個々のドメインコントローラやオブジェクトなどを復元することができます。RBSは任意のドメイン内のすべてのドメインコントローラを自動検知します。Flexible Single Master Operations (FSMO) の各役割、DNSサーバーなどその他のAD関連の役割などが配置されている場所も検知します (単一のドメインコントローラにインストールされている場合) 。

さらに、Identity Recoveryではフォレスト内のすべてのドメインのすべてのドメインコントローラを自動検知します。SLAドメインは、フォレスト、ドメイン、またはドメインコントローラレベルで割り当てることができます。Rubrik Security Cloudはデータ保護を目的としたグローバルな管理プレーンになります。一方、Rubrik Secure Vaultクラスタはホストの近くに導入することでローカルにバックアップを行うことができるようになります。Active Directoryがグローバルに分散している場合、Rubrik Security Cloudは必要なすべてのRubrik Secure Vaultクラスタに対して体系的に復元を行います。

Active Directoryドメインの復元は、特に複数のドメインで形成されるツリーや子ドメインの大きなフォレストにおける構造を考えると簡単ではありません。Rubrik Identity Recoveryは使いやすい5ステップのウィザード形式で進めることができます。同じ場所への復元か代替ホスト (分離された復元環境 - IRE : Isorated Recovery Environment) への復元かに変わらず、フォレスト内の全ドメインの包括的な復元を体系的に行います。代替ホストへの復元を利用すると、本番システムに影響を与えることなく、Active Directoryの復旧テストを容易に行うことができます。

ADフォレスト全体の体系的な復元を完全に行える他、Identity Recoveryのシンプルなインターフェイスを利用すると、バックアップから選択したオブジェクトの属性とActive Directory内の同じオブジェクトの現在の状態とを比較することができます。このインターフェイスを使用すると、オブジェクトの特定の属性のみを選択した時点に簡単にロールバックできます。オブジェクト自体には影響を与えません。

フォレスト内の単一のホストにRBSをインストールすると、フォレスト内のすべてのドメインとDCの完全な自動検知ができるようになりますが、バックアップを取得するには、RBSをADドメインコントローラにインストールする必要がありますので注意してください。

ENTRA ID

Entra IDは、Microsoft AzureとMicrosoft 365のアイデンティティプラットフォームとして機能するクラウドネイティブなIDプロバイダ (IdP) です。以前はAzure Active Directory (Azure AD) と呼ばれていましたが、従来のActive Directoryとは異なり、クラウドベースのアイデンティティおよびアクセス管理に対応できるようゼロから開発されました。以前の名称とは異なり、Entra IDはActive Directoryのクラウドホスト型バージョンではなく、最新のクラウド環境に合わせて特別に設計された独立したサービスになります。

Entraには、ADで扱い慣れているユーザー、グループ、コンピュータから、エンタープライズアプリやアプリ登録などの新しい構成要素まで、保護すべきさまざまなタイプのオブジェクトがあります。こうしたサービスに重要となるオブジェクト以外にも、考慮すべきオブジェクトタイプがあります。たとえば、条件付きアクセスポリシーを使用すると、管理者は特定のリソースへのアクセスを許可または拒否するための特定の条件を定義できます。例を挙げると、あるユーザーがテキサス州オースティンにある会社のオフィスに勤務していて、特定のアプリケーションにアクセスできるとします。このユーザーが旅行中に空港から同じリソースにアクセスしようとした場合、対応としては、このアクセスをブロックするか、VPNを使用している場合にのみ許可して、加えてログインにはMFAを適用するのが望ましいでしょう。

これらのさまざまな構成要素はすべて、オブジェクトが編集されたり削除されたりするなど、偶発的または悪意のある不適切な変更が発生した際に復元できるように保護する必要があります。

Rubrik Security Cloudには、Foundation、Business、Enterpriseの各Editionで、ユーザー、グループ、ロールを保護し、復元する機能があります。Active Directoryとは異なり、Rubrik Secure Vaultクラスタを導入する必要はありません。クラウドネイティブのモデルの場合、データセンターにハードウェアを導入する意味がないからです。

Foundation、Business、EnterpriseのEditionまたはIdentity Recoveryのいずれを使用する場合でも、Entraのデータ保護はマネージドサービスとして提供され、Rubrikがバックアップストレージを管理します。これらのバックアップは、迅速かつ簡単に復元できるようにAzureクラウドで保存されますが、Rubrikが管理するテナントに保存されるため、バックアップはEntraテナントとは完全に隔離されます。Entra管理者の1人が侵害を受けたとしても、侵害されたアカウントはバックアップにアクセスできません。そのため確実に復旧できるので安心です。

Rubrik Security CloudのFoundation、Business、Enterpriseの各Editionではユーザー、グループ、ロールを保護し、復元できます。Rubrik Identity Recoveryはこれを基盤として、さらにエンタープライズアプリ、アプリ登録、条件付きアクセスポリシーも保護します。

ハイブリッド復旧

世界中の何千という組織が依然としてActive Directoryのみを使用しています。クラウドへの移行を完了しており、Entraのみを使用している組織も多数存在します。しかし、大多数の企業は、Active Directory内のサーバーにEntra Connectを展開して一部またはすべてのユーザーアカウントをEntraに同期するハイブリッドモデルを採用しています。この場合、1つまたは複数のActive Directoryドメインを単一のEntraテナントに同期できます。

保護の観点からすると、ADからEntraに同期されたオブジェクトにはある種の課題が見られます。多くの場合、これらのオブジェクトにはEntra固有の属性が関連付けられていますが、問題発生時にその属性をEntraに直接復元することができません。代わりに、復元ワークフローでは、まずオブジェクトをActive Directoryに復元し、次に復元したオブジェクトをEntra ConnectがEntraに同期します。Entraへの同期が完了すると、Entra固有の属性を復元できます。

この追加的な管理オーバーヘッドは、特に複数のツールを使用する場合や大規模に復元する場合に相当の負担になる可能性があります。Rubrik Identity Recoveryには、この復元プロセス全体をエンドツーエンドで処理できる強化ワークフローが用意されています。

	Foundation/ Business/ Enterprise Edition	Identity Recovery
ドメインレベルでの保護	✓	✓
フォレストレベルでの保護		✓
オブジェクトの復元	✓	✓
オブジェクト属性の復元		✓
オブジェクト属性の比較		✓
個々のドメインコントローラの復元	✓	✓
ドメインの復元	✓	✓
体系的なADフォレストの完全復旧		✓
Entra IDユーザー、グループ、ロールの保護と復元	✓	✓
Entra IDエンタープライズアプリ、アプリ登録、条件付きアクセスポリシー		✓
ハイブリッド復旧		✓

要約

Rubrik Identity Recoveryは、単一のサブスクリプションライセンスで、Active Directoryのフォレスト、Entra ID、ハイブリッド環境の完全復旧を体系的に行います。Identity Recoveryを使用すると、オンプレミスとクラウドのアイデンティティサービスを堅牢かつ確実に復旧できます。

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）は、世界中のデータの安全を確保することを使命としています。弊社はZero Trust Data Security™を使用して、サイバー攻撃、悪意ある内部の脅威、業務の中断に対するビジネスレジリエンスを組織が実現できるよう支援します。機械学習を活用したRubrik Security Cloudは、オンプレミス、クラウド、SaaSアプリケーションに分散するデータを横断的に保護します。Rubrikは、データ整合性の維持、厳しい状況におけるデータ可用性の確保、データのリスクと脅威の常時監視、インフラが攻撃を受けた場合のデータによる業務の復旧など、さまざまな局面で組織をサポートします。

詳しくは、www.rubrik.comをご覧ください。また、X（旧Twitter）で@rubrikIncをフォローいただくか、LinkedInの場合はRubrik, Inc.をフォローしてください。

RubrikはRubrik, Inc.の登録商標です。本書に記載されているすべての会社名、製品名、およびその他の名称は各社の登録商標または商標です。

ds-rubrik-identity-recovery / 20250729