Rubrik Identity Recovery

Le Foundation, Business ed Enterprise Edition di Rubrik Security Cloud (RSC) offrono funzionalità native per la protezione di Active Directory ed Entra ID. Rubrik Identity Recovery, ora disponibile anche come offerta standalone, aggiunge funzionalità avanzate di protezione e recovery per i servizi di gestione dell'identità.

Questo documento mostra le differenze principali tra questi due set di prodotti distinti.

ACTIVE DIRECTORY

La protezione nativa di Active Directory in Rubrik Security Cloud si basa su Rubrik Backup Service (RBS), che utilizza lo strumento Microsoft Windows Server Backup Admin per generare i backup di Active Directory, i quali vengono scritti sulla piattaforma Rubrik nativamente immutabile e isolata logicamente dal resto della rete. Una volta completato il backup, la condivisione di rete viene chiusa per evitare che i dati salvati siano esposti e potenzialmente accessibili da aggressori.

Questi backup possono essere utilizzati per ripristinare singoli Domain Controller o anche singoli oggetti. RBS rileva automaticamente tutti i Domain Controller presenti in un dominio, inclusi i ruoli FSMO (Flexible Single Master Operations) e altri ruoli associati ad AD, come i server DNS, quando installato su un singolo Domain Controller.

Inoltre, Identity Recovery rileva automaticamente tutti i Domain Controller in tutti i domini della Forest. I domini SLA possono essere assegnati a livello di Forest, di dominio o di singolo Domain Controller. Anche se Rubrik Security Cloud offre un piano di gestione globale per la protezione dei dati, i cluster Rubrik Secure Vault possono essere distribuiti vicino agli host, consentendo l'esecuzione dei backup in locale. Se Active Directory è distribuito globalmente, Rubrik Security Cloud coordina il recovery su tutti i cluster Secure Vault coinvolti.

Il ripristino dei domini Active Directory può essere complesso, soprattutto in ambienti in cui più domini sono collegati come tree o domini figli all'interno di grandi Forest. Rubrik Identity Recovery semplifica questo processo con un wizard intuitivo in 5 step che orchestra il recovery completo di tutti i domini all'interno di una Forest, sia sul posto (in-place) sia su host alternativi, come in un Isolated Recovery Environment (IRE). Questo secondo approccio consente di testare il recovery di Active Directory in ambienti isolati, senza interferire con i sistemi di produzione.

Oltre al recovery orchestrato di un'intera Forest AD, Identity Recovery offre un'interfaccia semplice per confrontare gli attributi di un oggetto selezionato da un backup, con lo stato attuale dello stesso oggetto in Active Directory. Grazie a questa interfaccia, è possibile ripristinare solo attributi specifici di un oggetto in un determinato punto nel tempo, senza alterare gli altri aspetti dell'oggetto stesso.

È importante notare che, sebbene sia sufficiente installare RBS su un solo host nella Forest per consentire l'autodiscovery di tutti i domini e Domain Controller, per eseguire il backup è necessario installare RBS direttamente sul Domain Controller di Active Directory.

ENTRA ID

Entra ID è un Identity Provider cloud-native che costituisce la piattaforma identitaria per Microsoft Azure e Microsoft 365. Noto in precedenza come Azure Active Directory (Azure AD), è un servizio distinto rispetto ad Active Directory tradizionale, sviluppato da zero per supportare la gestione delle identità e degli accessi in ambienti cloud moderni. Nonostante il nome precedente, Entra ID non è una versione cloud-hosted di Active Directory, ma un servizio separato e progettato specificamente per il cloud.

In Entra esistono diversi tipi di oggetti da proteggere: da utenti, gruppi e computer - simili a quelli presenti in AD - fino a entità più recenti come le Enterprise Apps e le App Registrations. Oltre a questi oggetti (che fanno riferimento a service principal), vi sono altre tipologie da considerare. Ad esempio, le Conditional Access Policies permettono agli amministratori di definire condizioni specifiche per consentire o bloccare l'accesso a determinate risorse. Un utente in ufficio ad Austin, Texas, potrebbe avere accesso ad alcune applicazioni, ma se tenta di accedervi da un aeroporto, potrebbe essere necessario bloccare l'accesso o consentirlo solo tramite VPN e con autenticazione a più fattori (MFA).

Tutte queste entità devono essere protette, in modo da poter essere recuperate in caso di modifiche indesiderate - accidentali o malevole - come un oggetto modificato o eliminato.

Rubrik Security Cloud consente di proteggere e ripristinare utenti, gruppi e ruoli in ogni Edition: Foundation, Business ed Enterprise. A differenza di Active Directory, per questa protezione non è necessario distribuire cluster Rubrik Secure Vault: in un modello

cloud-native, non ha senso aggiungere hardware nei data center.

La protezione dei dati Entra viene erogata come servizio gestito: sia con la Foundation/Business/Enterprise Edition che con Identity Recovery, Rubrik si occupa della gestione dello storage dei backup. I backup vengono archiviati nel cloud Azure, pronti per il recovery rapido, ma all'interno di un tenant gestito da Rubrik, che crea un isolamento logico tra il tuo tenant Entra e i backup stessi. Nel caso in cui un amministratore Entra venga compromesso, l'account compromesso non ha accesso ai backup, garantendo la possibilità di eseguire il recovery in totale sicurezza.

Rubrik Security Cloud (Foundation, Business ed Enterprise Edition) consente di proteggere e ripristinare utenti, gruppi e ruoli. Rubrik Identity Recovery espande questa protezione includendo anche Enterprise Apps, App Registrations e Conditional Access Policies.

RECOVERY IBRIDO

Migliaia di organizzazioni nel mondo continuano a utilizzare solo Active Directory. Altre hanno completato la migrazione al cloud e lavorano in modalità Entra-only. La maggior parte adotta però un modello ibrido, utilizzando Entra Connect per sincronizzare parte o tutti gli account utente da Active Directory a Entra. In questo scenario, uno o più domini Active Directory possono essere sincronizzati in un unico tenant Entra.

Gli oggetti sincronizzati da AD a Entra presentano alcune criticità dal punto di vista della protezione. Anche se questi oggetti possono includere attributi specifici di Entra, non è possibile ripristinarli direttamente in Entra in caso di problemi. Il flusso di recovery corretto prevede prima il ripristino degli oggetti in Active Directory, da cui verranno sincronizzati verso Entra tramite Entra Connect. Una volta sincronizzati, sarà possibile ripristinare anche gli attributi specifici di Entra.

Questo ulteriore passaggio comporta un carico amministrativo importante, soprattutto quando si utilizzano più strumenti o si deve intervenire su larga scala. Rubrik Identity Recovery include un flusso di lavoro ottimizzato che gestisce l'intero processo end-to-end, semplificando il recovery negli ambienti ibridi.

	Foundation/ Business/ Enterprise Edition	Identity Recovery
Protezione a livello di dominio	✓	✓
Protezione a livello di Forest		✓
Ripristino di oggetti	✓	✓
Ripristino di attributi di oggetto		✓
Confronto attributi oggetto		✓
Ripristino di singoli Domain Controller	✓	✓
Ripristino di interi domini	✓	✓
Recovery orchestrato dell'intera Forest AD		✓
Protezione e recovery di utenti, gruppi e ruoli Entra ID	✓	✓
Protezione e recovery di Enterprise Apps, App Registrations e Conditional Access Policies		✓
Recovery ibrido		✓

RIEPILOGO

Rubrik Identity Recovery offre un recovery completamente orchestrato di Active Directory, Entra ID e ambienti ibridi, con un'unica licenza di abbonamento. Con Identity Recovery, ottieni una protezione solida e affidabile per i servizi di identità on-premise e cloud, senza dover gestire strumenti separati.

rubrik

Sede internazionale
3495 Deer Creek Road
Palo Alto, CA 94304
Stati Uniti

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

ds-rubrik-identity-recovery-Rubrik_IDML-it-IT#DTP_CUXHQP# / 20250723