Rubrik Identity Recovery

Les éditions Foundation, Business et Enterprise de Rubrik Security Cloud (RSC) incluent une protection native d'Active Directory et d'Entra ID. Rubrik Identity Recovery, désormais disponible en tant que service autonome, offre des capacités de protection et de récupération avancées pour les services d'identité.

Cette fiche recense les différences entre ces deux ensembles de produits distincts.

ACTIVE DIRECTORY

La protection Active Directory (AD) native de Rubrik Security Cloud appelle l'outil d'administration Sauvegarde Windows Server natif de Microsoft via Rubrik Backup Service (RBS) pour générer des sauvegardes d'Active Directory. Ces backups sont ensuite écrits sur la plateforme nativement immuable et protégée par air-gap logique de Rubrik, après quoi le partage réseau est fermé. Les données ne sont donc pas exposées au réseau, où un attaquant pourrait y accéder.

Ces sauvegardes peuvent alors être utilisées pour récupérer des contrôleurs de domaine individuels, voire des objets. RBS découvre automatiquement l'ensemble des contrôleurs au sein d'un domaine, y compris là où résident les rôles FSMO (Flexible Single Master Operations), ainsi que d'autres rôles associés à AD, comme le serveur DNS, lorsqu'il est installé sur un contrôleur de domaine unique.

De plus, Identity Recovery détecte automatiquement tous les contrôleurs de domaine dans l'ensemble des domaines de la forêt. Les domaines SLA peuvent être affectés au niveau de la forêt, du domaine ou du contrôleur de domaine. Là où Rubrik Security Cloud fournit un plan de gestion global pour la protection des données, les clusters Rubrik Secure Vault peuvent être déployés à proximité des hôtes et les sauvegardes effectuées localement. Si Active Directory est distribué globalement, Rubrik Security Cloud orchestre la restauration sur l'ensemble des clusters Rubrik Secure Vault nécessaires.

La récupération des domaines Active Directory est une tâche parfois complexe, d'autant que dans les forêts vastes, plusieurs domaines peuvent être raccordés sous forme d'arbres et de domaines enfants. Rubrik Identity Recovery fournit un processus en cinq étapes, simple et guidé par un assistant, qui orchestre le rétablissement complet de tous les domaines d'une forêt, que ce soit sur place ou sur des hôtes alternatifs, par exemple dans un environnement de restauration isolé (IRE). Cette dernière méthode permet de tester facilement la restauration d'Active Directory sans impacter les systèmes de production.

Outre sa capacité à orchestrer de bout en bout la récupération d'une forêt AD, Identity Recovery offre une interface intuitive, qui permet de comparer les attributs d'un objet issu d'une sauvegarde avec l'état actuel de cet objet dans Active Directory. Grâce à cette interface, vous pouvez restaurer uniquement des attributs spécifiques d'un objet à un moment donné, sans l'affecter et en toute simplicité.

À noter : il est possible d'installer RBS sur un seul hôte dans une forêt pour découvrir automatiquement tous les domaines et contrôleurs de domaine de cette forêt. En revanche, pour effectuer une sauvegarde, RBS doit être installé sur le contrôleur de domaine AD.

ENTRA ID

Entra ID, anciennement Azure Active Directory (Azure AD), est un fournisseur d'identité (IdP) cloud-native qui sert de plateforme d'identité pour Microsoft Azure et Microsoft 365. Contrairement à l'annuaire Active Directory traditionnel, Entra ID a été développé de A à Z pour sous-tendre la gestion des accès et des identités en mode cloud. Malgré ce que pourrait laisser penser son appellation initiale, Entra ID n'est pas une version d'Active Directory hébergée dans le cloud : il s'agit d'un service distinct, spécifiquement conçu pour les environnements cloud modernes.

Entra inclut de nombreux types d'objets différents à protéger, dont les objets AD classiques (utilisateurs, groupes, ordinateurs, etc.) ainsi que des concepts plus récents, comme les applications d'entreprise et les inscriptions d'applications. Ce service comprend aussi d'autres types d'objets, y compris les politiques d'accès conditionnel, qui permettent à l'administrateur de définir les conditions spécifiques dans lesquelles l'accès à certaines ressources sera autorisé ou refusé. Exemple : un collaborateur d'une agence d'Austin, au Texas, est autorisé à accéder à plusieurs applications. Lors d'un déplacement professionnel, il tente d'ouvrir ces ressources alors qu'il se trouve à l'aéroport. Dans ce cas, il sera sans doute plus judicieux soit de bloquer cet accès, soit de l'autoriser uniquement si l'utilisateur se connecte au moyen d'un VPN et d'une authentification MFA.

Tous ces différents objets doivent être protégés de sorte qu'ils puissent être restaurés en cas de changement inopportun, qu'il soit accidentel ou malveillant (modification ou suppression d'un objet, par exemple).

Rubrik Security Cloud assure la protection et la restauration des utilisateurs, groupes et rôles dans les éditions Foundation, Business et Enterprise. Contrairement à Active Directory, cette protection

ne requiert pas le déploiement de clusters Rubrik Secure Vault : dans un modèle cloud-native, il n'est pas logique d'exiger le déploiement de matériel dans vos data centers.

Que vous disposiez de l'édition Foundation / Business / Enterprise ou d'Identity Recovery, la protection des données Entra est fournie en tant que service managé, et Rubrik se charge de gérer le stockage des sauvegardes. Celles-ci sont stockées dans le cloud Azure pour une récupération simple et rapide, dans un tenant géré par Rubrik qui assure une protection par air-gap logique entre vos sauvegardes et votre tenant Entra. Si l'un de vos administrateurs Entra est victime d'une compromission, le compte correspondant n'a pas accès aux sauvegardes : la récupération est donc garantie.

Rubrik Security Cloud (éditions Foundation, Business et Enterprise) protège et récupère les utilisateurs, les groupes et les rôles. Rubrik Identity Recovery s'appuie sur ces capacités pour étendre la protection aux applications d'entreprise, inscriptions d'applications et politiques d'accès conditionnel.

RÉCUPÉRATION HYBRIDE

Des milliers d'entreprises dans le monde utilisent encore exclusivement Active Directory. De nombreuses autres utilisent uniquement Entra une fois leur migration vers le cloud terminée. Cependant, la grande majorité des entreprises s'appuient sur un modèle hybride : elles déploient Entra Connect sur des serveurs au sein d'Active Directory pour synchroniser une partie ou l'ensemble des comptes utilisateurs avec Entra. Dans ce scénario, un ou plusieurs domaines Active Directory peuvent être synchronisés avec un seul tenant Entra.

Or, les objets synchronisés depuis AD vers Entra posent certains défis en matière de protection : bien qu'ils possèdent souvent des attributs spécifiques à Entra qui leur sont associés, il n'est pas possible de les restaurer directement dans Entra en cas de problème. Il vous faudra d'abord les récupérer dans Active Directory, avec lequel Entra Connect se synchronisera pour les rétablir dans Entra. Une fois la synchronisation avec Entra terminée, les attributs spécifiques à ce service peuvent être récupérés.

Cette démarche fastidieuse représente une charge considérable pour vos équipes, surtout si vous utilisez plusieurs outils ou si la récupération s'opère à grande échelle. Rubrik Identity Recovery propose un workflow amélioré qui gère l'ensemble du processus de restauration de bout en bout.

	Édition Foundation / Business / Enterprise	Identity Recovery
Protection au niveau du domaine	✓	✓
Protection au niveau de la forêt		✓
Récupération des objets	✓	✓
Récupération des attributs d'objets		✓
Comparaison des attributs d'objets		✓
Récupération de contrôleurs de domaine individuels	✓	✓
Récupération de domaines	✓	✓
Récupération de forêt AD entièrement orchestrée		✓
Protection et récupération des utilisateurs, groupes et rôles Entra ID	✓	✓
Applications d'entreprise, inscriptions d'applications et politiques d'accès conditionnel Entra ID		✓
Récupération hybride		✓

CONCLUSION

Rubrik Identity Recovery orchestre la restauration complète des forêts Active Directory, d'Entra ID et des environnements hybrides, le tout avec un seul et même abonnement. Avec Identity Recovery, vous bénéficiez d'une récupération robuste et garantie pour les services d'identité sur site et dans le cloud, sans avoir à gérer de multiples outils.

rubrik

Siège mondial
3495 Deer Creek Road
Palo Alto, CA 94304
États-Unis

+31 208 113 222
france@rubrik.com
www.rubrik.com/fr

Rubrik (NYSE: RBRK) s'est donné pour mission de sécuriser les données du monde entier. Au travers de la solution Zero Trust Data Security™, nous aidons les entreprises à assurer leur résilience face aux cyberattaques, aux menaces internes et aux perturbations opérationnelles. Optimisé par le machine learning, Rubrik Security Cloud protège les données sur l'ensemble des applications métiers, cloud et SaaS. Intégrité, disponibilité à toute épreuve, surveillance des risques et des menaces, récupération en cas d'attaque... Nous agissons sur tous les fronts de la protection et de la préservation de vos données.

Pour en savoir plus, rendez-vous sur notre site www.rubrik.com/fr et suivez notre compte @rubrikInc sur X (anciennement Twitter) et Rubrik sur LinkedIn.

Rubrik est une marque déposée de Rubrik, Inc. Tous les noms de sociétés, noms de produits et autres noms similaires figurant dans le présent document sont des marques déposées ou des marques commerciales de la société concernée.

ds-rubrik-identity-recovery-Rubrik_IDML-fr-FR#DTP_CUXHQR# / 20250715