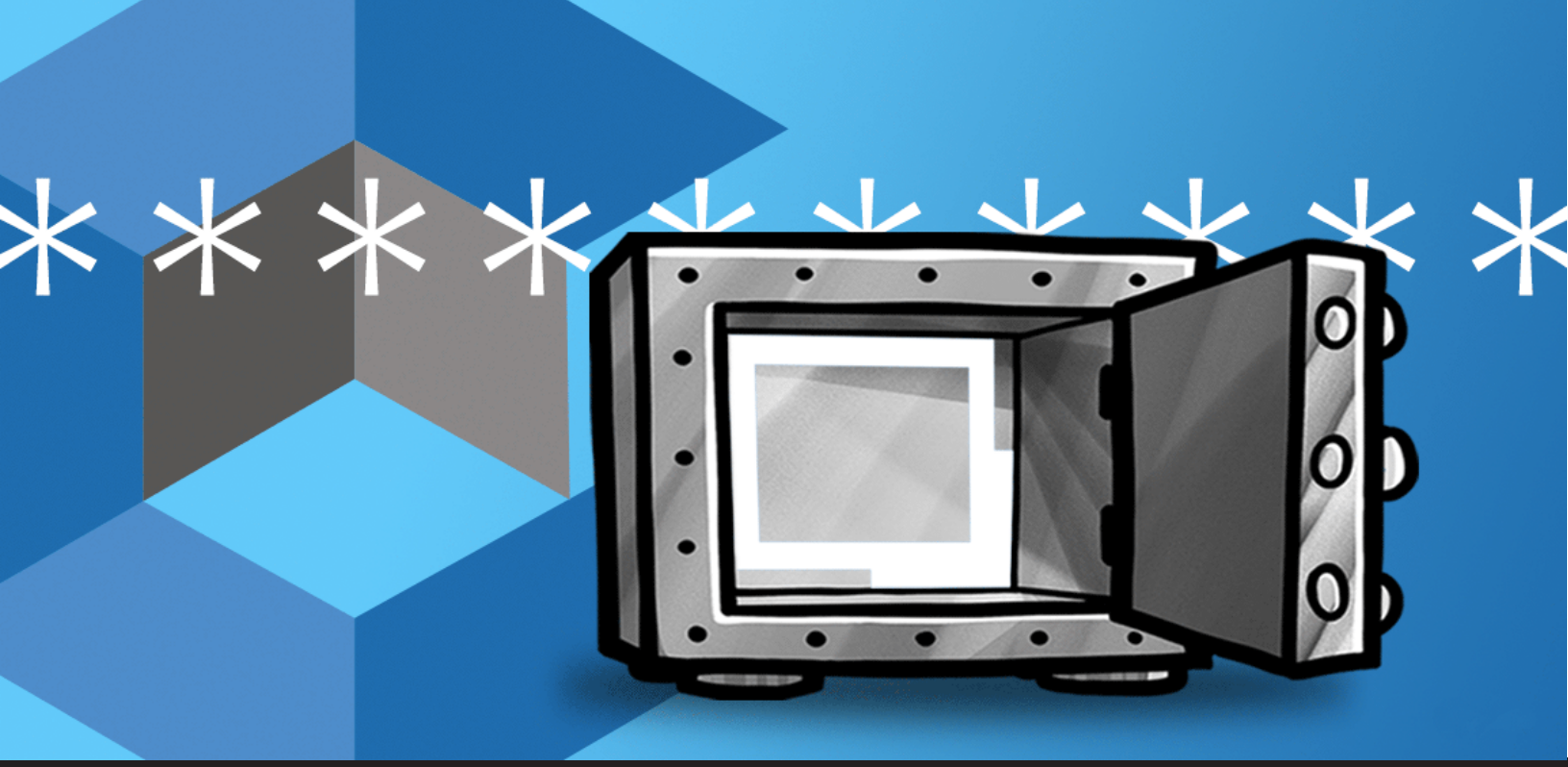


Passez en mode « sans mot de passe » avec Remote Desktop Manager et CyberArk

Devolutions

NOUS AVONS MIS À JOUR DEUX DES TROIS TYPES D'ENTRÉES CYBERARK

Au cours des derniers mois, vous avez peut-être remarqué plusieurs collaborations entre **Devolutions** et **CyberArk**. Dans RDM 2020.2, nous avons mis à jour deux des trois types d'entrées CyberArk afin de profiter de leur API améliorée.

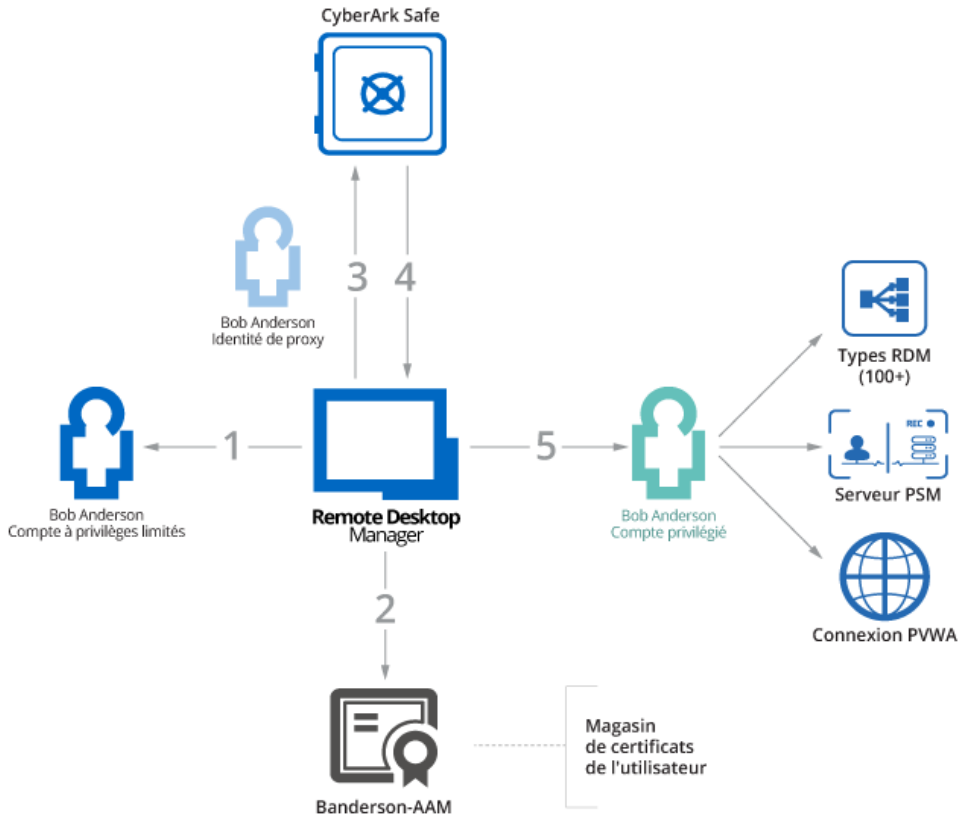
Aujourd'hui, je suis heureux de vous annoncer que le troisième type d'entrée a été mis à jour dans RDM 2020.3. Ça complète la série d'améliorations en cours et permet essentiellement aux organisations de **se passer de mots de passe** pour leurs flux de travail quotidiens.

Installation de l'AAM

La seule exigence pour créer un système sans mots de passe est d'installer l'**Application Access Manager** (AAM) de CyberArk lorsque vous déployez leurs solutions au sein de votre entreprise. Ce module permet l'**authentification par clé privée**, ce qui signifie que toute la phase d'identification/authentification est gérée par votre département informatique. Ça rend les mots de passe complètement inutiles.

Présentation du système

Une fois que vous avez installé l'AAM de CyberArk, vous devrez vous authentifier auprès de RDM, quelle que soit la source de données que vous utilisez. Le schéma suivant illustre ce système :



1. L'utilisateur est authentifié auprès de RDM avec un **compte limité (de moindre privilège)**. Ça donne à l'utilisateur une vue du contenu RDM selon les autorisations définies dans le contrôle d'accès basé sur les rôles.
2. Lorsqu'un **compte privilégié** est requis pour lancer une technologie prise en charge, RDM obtient la clé privée appropriée du poste de travail (la clé doit être conservée dans le magasin de certificats de l'utilisateur).
3. La clé privée est utilisée pour s'authentifier auprès du CyberArk Vault. Elle est configurée en tant qu'objet « application ». C'est essentiellement un **proxy utilisateur** utilisé pour interroger le coffre.
4. RDM obtient les détails d'un compte privilégié. Cela signifie que l'utilisateur ne connaît même pas le mot de passe de son propre compte privilégié!
5. RDM utilise le compte privilégié pour lancer une connexion PSM, se connecter au PVWA ou lancer une session prise en charge par RDM. Pendant que tout ça se produit, le mot de passe reste caché pour l'utilisateur.

Configuration de CyberArk Application Access Manager (AAM)

La première étape pour configurer l'AAM est d'émettre une clé privée pour chacun de vos utilisateurs, puis de les déployer sur leur poste de travail. Évidemment, la meilleure source pour bien comprendre la procédure est la documentation de CyberArk. Cependant, nous avons inclus des instructions de base dans notre guide d'intégration. En ce qui concerne le côté de RDM, nous prenons à nouveau en charge différentes méthodes de gestion de clé privée :

1. **Les informations de clés privées sont stockées sous forme d'entrées qui existent dans le coffre privé de l'utilisateur.** C'est sûrement la méthode la plus simple, parce que vous avez une relation one-to-one entre les utilisateurs/clés/comptes. Cependant, ça doit être fait par les utilisateurs eux-mêmes.
2. **Les informations de clés privées sont stockées dans « paramètres de mon compte »**. Cette méthode permet aux administrateurs de créer des entrées AAM dans RDM, tandis que chaque utilisateur définit ses propres détails de clé privée dans ses paramètres personnels. Étant donné que la recherche de compte utilise des mots-clés spécifiés dans l'entrée AAM, cela signifie que vous avez deux options :

- **Géré dans CyberArk** : pour chaque utilisateur, il doit y avoir un seul compte privilégié accessible à partir des mêmes mots-clés. Il revient à l'administrateur de les isoler dans divers coffres et de s'assurer que le compte de chacun a les mêmes mots-clés.

- **Géré dans RDM** : pour trouver leur compte privilégié, les administrateurs doivent créer une entrée AAM unique par utilisateur avec les mots-clés. Le contrôle d'accès basé sur les rôles de RDM doit être utilisé pour garantir que les utilisateurs peuvent afficher et utiliser uniquement les entrées appropriées.

Comme toujours avec RDM, vous pouvez mélanger les approches en fonction de vos propres besoins.

Configuration de CyberArk Privileged Session Manager (PSM)

Une explication complète sur le PSM serait sûrement trop longue pour ce billet de blogue, je vais donc à nouveau vous référer à la documentation de CyberArk. Comme pour RDM, dans votre entrée PSM-Server, vous pouvez utiliser un de nos mécanismes pour que la connexion passe par l'entrée AAM configurée à l'étape précédente.

Si vous avez choisi l'option AAM #1 ci-dessus, vous devez utiliser les paramètres spécifiques à l'utilisateur dans RDM pour créer le lien entre l'entrée PSM-Server et l'entrée AAM qui est stockée dans le coffre de l'utilisateur.

Si, au contraire, vous avez choisi les options #2a ou # 2b, je pense que la meilleure option est de configurer l'entrée PSM-Server pour utiliser le dépôt d'identifiants et l'option « Demander à la connexion ». Ça améliore l'expérience pour les nouveaux utilisateurs et les utilisateurs expérimentés sauront comment passer aux paramètres spécifiques à l'utilisateur pour rendre leur choix permanent.

Configuration du SDK des services Web de CyberArk

Ceci permet à votre organisation de récupérer certains mots de passe chaque fois que le PSM (ou le courtage de compte du RDM) n'est pas une option, tout en garantissant que l'accès n'est disponible qu'à partir d'un compte privilégié que l'utilisateur ne contrôle pas.

Lorsque vous restez dans les limites de votre écosystème CyberArk, vous n'avez généralement pas besoin d'utiliser cette option. Cependant, dans RDM 2020.3, nous l'avons rendu disponible au cas où votre organisation souhaiterait l'installer.

Conclusion

Pour plus d'informations, voici la documentation officielle de chacune de nos intégrations, ainsi que quelques liens vers notre propre documentation sur les fonctionnalités mentionnées dans cet article:

1. **Guides d'intégration** (en anglais seulement)

- Guide d'intégration AAM
- Guide d'intégration PSM
- Guide d'intégration du SDK des services Web

2. **Aide de Remote Desktop Manager**

- Paramètres de mon compte
- Paramètres spécifiques de l'utilisateur

Comme toujours, veuillez contacter notre équipe d'assistance à ticket@devolutions.net si vous souhaitez une démonstration en direct ou si vous avez besoin d'informations. Je vous invite également à commenter ci-dessous avec des questions ou des impressions.