Utilisation des utilisateurs et des groupes locaux par ONTAP

ONTAP 9

NetApp
March 24, 2023

Table des matières

Utilisation des utilisateurs et des groupes locaux par ONTAP

Concepts d’utilisateurs et de groupes locaux

Vous devez connaître les utilisateurs et les groupes locaux, ainsi que quelques informations de base à leur sujet, avant de déterminer si vous devez configurer et utiliser des utilisateurs et des groupes locaux dans votre environnement.

- **Utilisateur local**

  Un compte utilisateur avec un identifiant de sécurité unique (SID) qui n’a de visibilité que sur la machine virtuelle de stockage (SVM) sur laquelle elle est créée. Les comptes d’utilisateur locaux ont un ensemble d’attributs, y compris le nom d’utilisateur et le SID. Un compte utilisateur local s’authentifie localement sur le serveur CIFS à l’aide de l’authentification NTLM.

  Les comptes d’utilisateur ont plusieurs utilisations :

  - Permet d’accorder des privilèges *User Rights Management* à un utilisateur.
  - Permet de contrôler l’accès au niveau du partage et du fichier aux ressources de fichiers et de dossiers détenues par la SVM.
- **Groupe local**

  Un groupe avec un SID unique n’a de visibilité que sur le SVM sur lequel il est créé. Les groupes contiennent un ensemble de membres. Les membres peuvent être des utilisateurs locaux, des utilisateurs de domaine, des groupes de domaines et des comptes de machine de domaine. Les groupes peuvent être créés, modifiés ou supprimés.

  Les groupes ont plusieurs utilisations :

  - Utilisé pour accorder des privilèges *User Rights Management* à ses membres.
  - Permet de contrôler l’accès au niveau du partage et du fichier aux ressources de fichiers et de dossiers détenues par la SVM.
- **Domaine local**

  Domaine qui dispose de son étendue locale, limitée par le SVM. Le nom du domaine local est le nom du serveur CIFS. Les utilisateurs et groupes locaux sont contenus dans le domaine local.

- **Identificateur de sécurité (SID)**

  Un SID est une valeur numérique de longueur variable qui identifie les entités de sécurité de type Windows. Par exemple, un SID type prend le format suivant : s-1-5-21-3139654847-1303905135-2517279418-123456.

- **Authentification NTLM**

  Méthode de sécurité Microsoft Windows utilisée pour authentifier les utilisateurs sur un serveur CIFS.

- **Cluster Replicated database (RDB)**

  Base de données répliquée avec une instance sur chaque nœud d’un cluster. Les objets utilisateur et

groupe locaux sont stockés dans le RDB.

Raisons de la création d'utilisateurs et de groupes locaux

Il existe plusieurs raisons de créer des utilisateurs et des groupes locaux sur votre SVM (Storage Virtual machine). Par exemple, vous pouvez accéder à un serveur SMB à l'aide d'un compte d'utilisateur local si les contrôleurs de domaine (DCS) ne sont pas disponibles, vous pouvez utiliser des groupes locaux pour attribuer des privilèges ou si votre serveur SMB se trouve dans un groupe de travail.

Vous pouvez créer un ou plusieurs comptes utilisateur locaux pour les raisons suivantes :

- Votre serveur SMB se trouve dans un groupe de travail et les utilisateurs de domaine ne sont pas disponibles.

  Les utilisateurs locaux sont requis dans les configurations de groupe de travail.

- Vous souhaitez pouvoir vous authentifier et vous connecter au serveur SMB si les contrôleurs de domaine ne sont pas disponibles.

  Les utilisateurs locaux peuvent s'authentifier auprès du serveur SMB en utilisant l'authentification NTLM lorsque le contrôleur de domaine est en panne, ou en cas de problèmes réseau empêchant votre serveur SMB de contacter le contrôleur de domaine.

- Vous souhaitez attribuer des privilèges *User Rights Management* à un utilisateur local.

  User Rights Management permet à un administrateur de serveurs SMB de contrôler les droits des utilisateurs et des groupes sur le SVM. Vous pouvez attribuer des privilèges à un utilisateur en lui attribuant des privilèges ou en faisant de l'utilisateur un membre d'un groupe local disposant de ces privilèges.

Vous pouvez créer un ou plusieurs groupes locaux pour les raisons suivantes :

- Votre serveur SMB se trouve dans un groupe de travail et les groupes de domaines ne sont pas disponibles.

  Les groupes locaux ne sont pas requis dans les configurations de groupes de travail, mais ils peuvent être utiles pour gérer les privilèges d'accès pour les utilisateurs de groupes de travail locaux.

- Vous souhaitez contrôler l'accès aux ressources de fichiers et de dossiers à l'aide des groupes locaux pour le contrôle du partage et de l'accès aux fichiers.
- Vous souhaitez créer des groupes locaux avec des privilèges *User Rights Management* personnalisés.

  Certains groupes d'utilisateurs intégrés ont des privilèges prédéfinis. Pour attribuer un ensemble personnalisé de privilèges, vous pouvez créer un groupe local et attribuer les privilèges nécessaires à ce groupe. Vous pouvez ensuite ajouter des utilisateurs locaux, des utilisateurs de domaine et des groupes de domaines au groupe local.

Informations associées

Fonctionnement de l'authentification des utilisateurs locaux

Liste des privilèges pris en charge

Fonctionnement de l'authentification des utilisateurs locaux

Avant qu'un utilisateur local puisse accéder aux données sur un serveur CIFS, il doit créer une session authentifiée.

SMB étant basé sur une session, l'identité de l'utilisateur peut être déterminée une seule fois, lors de la première configuration de la session. Le serveur CIFS utilise l'authentification NTLM lors de l'authentification des utilisateurs locaux. Les fournisseurs de NTLMv1 et NTLMv2 sont tous deux pris en charge.

ONTAP utilise l'authentification locale dans trois cas d'utilisation. Chaque cas d'utilisation dépend du fait que la partie du domaine du nom d'utilisateur (au format DOMAINE\utilisateur) correspond au nom de domaine local du serveur CIFS (le nom du serveur CIFS) :

- La partie domaine correspond

  Les utilisateurs qui fournissent des informations d'identification d'utilisateur local lors de la demande d'accès aux données sont authentifiés localement sur le serveur CIFS.

- La partie du domaine ne correspond pas

  ONTAP tente d'utiliser l'authentification NTLM avec un contrôleur de domaine dans le domaine auquel le serveur CIFS appartient. Si l'authentification réussit, la connexion est terminée. Si cela ne fonctionne pas, ce qui se passe ensuite dépend de la raison pour laquelle l'authentification n'a pas réussi.

  Par exemple, si l'utilisateur existe dans Active Directory mais que le mot de passe est incorrect ou expiré, ONTAP ne tente pas d'utiliser le compte d'utilisateur local correspondant sur le serveur CIFS. Au lieu de cela, l'authentification échoue. Dans d'autres cas, ONTAP utilise le compte local correspondant sur le serveur CIFS, s'il existe, pour l'authentification, même si les noms de domaine NetBIOS ne correspondent pas. Par exemple, si un compte de domaine correspondant existe mais est désactivé, ONTAP utilise le compte local correspondant sur le serveur CIFS pour l'authentification.

- La partie domaine n'est pas spécifiée

  ONTAP tente d'abord l'authentification en tant qu'utilisateur local. Si l'authentification en tant qu'utilisateur local échoue, ONTAP authentifie l'utilisateur avec un contrôleur de domaine dans le domaine auquel le serveur CIFS appartient.

Une fois l'authentification des utilisateurs locaux ou de domaine terminée, ONTAP crée un jeton d'accès complet, qui tient compte de l'appartenance et des privilèges des groupes locaux.

Pour plus d'informations sur l'authentification NTLM pour les utilisateurs locaux, consultez la documentation Microsoft Windows.

Informations associées

Activation ou désactivation de l'authentification des utilisateurs locaux

Comment les jetons d'accès utilisateur sont construits

Lorsqu'un utilisateur mappe un partage, une session SMB authentifiée est établie et un jeton d'accès utilisateur est construit qui contient des informations sur l'utilisateur, l'appartenance au groupe de l'utilisateur et les privilèges cumulatifs, ainsi que l'utilisateur UNIX mappé.

À moins que la fonctionnalité ne soit désactivée, les informations d'utilisateur et de groupe locaux sont également ajoutées au jeton d'accès utilisateur. La manière dont les jetons d'accès sont créés dépend de la manière dont la connexion est destinée à un utilisateur local ou à un utilisateur de domaine Active Directory :

- Connexion de l'utilisateur local

  Bien que les utilisateurs locaux puissent être membres de groupes locaux différents, les groupes locaux ne peuvent pas être membres d'autres groupes locaux. Le jeton d'accès utilisateur local se compose d'une Union de tous les privilèges attribués aux groupes auxquels un utilisateur local particulier est membre.

- Connexion utilisateur du domaine

  Lorsqu'un utilisateur de domaine se connecte, ONTAP obtient un jeton d'accès utilisateur contenant le SID de l'utilisateur et les SID pour tous les groupes de domaine auxquels l'utilisateur est membre. ONTAP utilise l'Union du jeton d'accès d'utilisateur du domaine avec le jeton d'accès fourni par les membres locaux des groupes de domaine de l'utilisateur (le cas échéant), ainsi que tout privilège direct attribué à l'utilisateur du domaine ou à l'un de ses membres de groupe de domaine.

Pour les connexions utilisateur locales et de domaine, le GROUPE principal RID est également défini pour le jeton d'accès utilisateur. Le RID par défaut est `Domain Users` (RID 513). Vous ne pouvez pas modifier la valeur par défaut.

Le processus de mappage de noms Windows-to-UNIX et UNIX-to-Windows suit les mêmes règles pour les comptes locaux et de domaine.

> Il n'y a pas de mappage automatique implicite d'un utilisateur UNIX vers un compte local. Si cela est nécessaire, une règle de mappage explicite doit être spécifiée à l'aide des commandes de mappage de noms existantes.

Consignes relatives à l'utilisation de SnapMirror sur des SVM contenant des groupes locaux

Notez les instructions lorsque vous configurez SnapMirror sur des volumes appartenant aux SVM contenant des groupes locaux.

Vous ne pouvez pas utiliser des groupes locaux dans des ACE appliqués à des fichiers, des répertoires ou des partages qui sont répliqués par SnapMirror vers une autre SVM. Si vous utilisez la fonctionnalité SnapMirror pour créer un miroir de reprise sur incident sur un volume situé sur un autre SVM et que le volume dispose d'une version ACE pour un groupe local, l'ACE n'est pas valide pour le miroir. Si les données sont répliquées sur un autre SVM, celles-ci se croisent efficacement et un autre domaine local. Les autorisations accordées aux utilisateurs et groupes locaux ne sont valides qu'au sein du périmètre de la SVM sur lequel ils ont été créés.

Ce qui arrive aux utilisateurs et aux groupes locaux lors de la suppression des serveurs CIFS

L'ensemble par défaut des utilisateurs et groupes locaux est créé lors de la création d'un serveur CIFS et ils sont associés au serveur virtuel de stockage (SVM) qui héberge le serveur CIFS. Les administrateurs SVM peuvent créer à tout moment des utilisateurs et groupes locaux. Lorsque vous supprimez le serveur CIFS, vous devez connaître ce qui

arrive aux utilisateurs et aux groupes locaux.

Les utilisateurs et groupes locaux sont associés à des SVM ; ils ne sont donc pas supprimés lorsque des serveurs CIFS sont supprimés pour des raisons de sécurité. Bien que les utilisateurs et groupes locaux ne soient pas supprimés lors de la suppression du serveur CIFS, ils sont masqués. Vous ne pouvez ni afficher ni gérer des utilisateurs et groupes locaux tant que vous n'avez pas recréés un serveur CIFS sur la SVM.

L'état d'administration du serveur CIFS n'affecte pas la visibilité des utilisateurs ou des groupes locaux.

Utilisation de la console de gestion Microsoft avec des utilisateurs et des groupes locaux

Vous pouvez afficher des informations sur les utilisateurs et groupes locaux à partir de la console de gestion Microsoft. Avec cette version de ONTAP, vous ne pouvez pas effectuer d'autres tâches de gestion pour les utilisateurs et groupes locaux à partir de la console de gestion Microsoft.

Instructions pour le rétablissement

Si vous prévoyez de restaurer le cluster à une version de ONTAP qui ne prend pas en charge les utilisateurs et groupes locaux, ainsi que les utilisateurs et groupes locaux utilisés pour gérer l'accès aux fichiers ou les droits des utilisateurs, vous devez tenir compte de certaines considérations.

- Pour des raisons de sécurité, les informations concernant les utilisateurs, groupes et privilèges locaux configurés ne sont pas supprimées lorsque ONTAP est rétabli sur une version qui ne prend pas en charge les fonctionnalités des utilisateurs et des groupes locaux.
- Lors de la restauration d'une version majeure antérieure de ONTAP, ONTAP n'utilise pas d'utilisateurs et de groupes locaux pendant l'authentification et la création des informations d'identification.
- Les utilisateurs et groupes locaux ne sont pas supprimés des listes de contrôle d'accès aux fichiers et aux dossiers.
- Les demandes d'accès aux fichiers qui dépendent de l'accès sont refusées en raison des autorisations accordées aux utilisateurs ou groupes locaux.

  Pour autoriser l'accès, vous devez reconfigurer les autorisations d'accès aux fichiers afin d'autoriser l'accès en fonction des objets de domaine au lieu d'objets d'utilisateur et de groupe locaux.

Informations sur le copyright

Informations sur les marques commerciales