Utilisez des sessions null pour accéder au stockage dans des environnements non Kerberos

ONTAP 9

NetApp
April 24, 2024

Sommaire

Utilisez des sessions null pour accéder au stockage dans des environnements non Kerberos

Utilisez les sessions null pour accéder au stockage dans les environnements non Kerberos

L'accès aux sessions null fournit des autorisations pour les ressources réseau, telles que les données du système de stockage, ainsi que pour les services basés sur les clients s'exécutant sous le système local. Une session null se produit lorsqu'un processus client utilise le compte "système" pour accéder à une ressource réseau. La configuration de session null est spécifique à l'authentification non Kerberos.

Comment le système de stockage fournit un accès de session nul

Comme les partages de session NULL ne nécessitent pas d'authentification, les clients qui ont besoin d'un accès de session nul doivent avoir leurs adresses IP mappées sur le système de stockage.

Par défaut, les clients de session null non mappés peuvent accéder à certains services système ONTAP, tels que l'énumération de partage, mais l'accès aux données du système de stockage est limité.

> ONTAP prend en charge les valeurs des paramètres de registre Windows RestrictAnonymous avec l' `-restrict-anonymous` option. Cela vous permet de contrôler la mesure dans laquelle les utilisateurs nuls non mappés peuvent afficher ou accéder aux ressources système. Par exemple, vous pouvez désactiver l'énumération de partage et l'accès au partage IPC$ (le partage de tuyauterie nommé masqué). Le `vserver cifs options modify` et `vserver cifs options show` les pages man fournissent plus d'informations sur le `-restrict-anonymous` option.

Sauf configuration contraire, un client exécutant un processus local qui demande l'accès au système de stockage via une session nulle est membre uniquement de groupes non restrictifs, tels que « tout le monde ». Pour limiter l'accès à une session nulle aux ressources du système de stockage sélectionnées, vous pouvez créer un groupe auquel appartiennent tous les clients de session nulle. La création de ce groupe vous permet de limiter l'accès au système de stockage et de définir des autorisations de ressources du système de stockage qui s'appliquent spécifiquement aux clients de session nul.

ONTAP fournit une syntaxe de mappage dans le `vserver name-mapping` Ensemble de commandes permettant de spécifier l'adresse IP des clients autorisés à accéder aux ressources du système de stockage à l'aide d'une session utilisateur null. Une fois que vous avez créé un groupe pour les utilisateurs nuls, vous pouvez spécifier des restrictions d'accès pour les ressources du système de stockage et les autorisations de ressources qui s'appliquent uniquement aux sessions nulles. L'utilisateur null est identifié comme une connexion anonyme. Les utilisateurs null n'ont accès à aucun répertoire personnel.

Les autorisations d'utilisateur mappées sont accordées à tout utilisateur null accédant au système de stockage à partir d'une adresse IP mappée. Prenez les précautions appropriées pour empêcher tout accès non autorisé

aux systèmes de stockage mappés avec des utilisateurs nuls. Pour une protection maximale, placez le système de stockage et tous les clients nécessitant un accès nul au système de stockage utilisateur sur un réseau distinct, afin d'éliminer la possibilité d'une adresse IP « couverture ».

Informations associées

Configuration des restrictions d'accès pour les utilisateurs anonymes

Accorder aux utilisateurs nuls l'accès aux partages de système de fichiers

Vous pouvez autoriser l'accès aux ressources de votre système de stockage par les clients de session null en attribuant un groupe à utiliser par les clients de session null et en enregistrant les adresses IP des clients de session null à ajouter à la liste des clients autorisés à accéder aux données à l'aide de sessions null du système de stockage.

Étapes

1. Utilisez le `vserver name-mapping create` Commande permettant de mapper l'utilisateur null à un utilisateur Windows valide, avec un qualificateur IP.

   La commande suivante mappe l'utilisateur null à user1 avec un nom d'hôte valide google.com :

   ```
   vserver name-mapping create –direction win-unix  -position 1 –pattern
   "ANONYMOUS LOGON" –replacement user1 – hostname google.com
   ```

   La commande suivante mappe l'utilisateur null à utilisateur1 avec une adresse IP valide 10.238.2.54/32 :

   ```
   vserver name-mapping create –direction win-unix  -position 2 –pattern
   "ANONYMOUS LOGON" –replacement user1 –address 10.238.2.54/32
   ```

2. Utilisez le `vserver name-mapping show` commande pour confirmer le mappage de nom.

   ```
   vserver name-mapping show

   Vserver:   vs1
   Direction: win-unix
   Position Hostname         IP Address/Mask
   -------- --------         ----------------
   1       -                 10.72.40.83/32      Pattern: anonymous logon
                                            Replacement: user1
   ```

3. Utilisez le `vserver cifs options modify –win-name-for-null-user` Commande permettant d'attribuer l'appartenance à Windows à l'utilisateur nul.

   Cette option est applicable uniquement lorsqu'il existe un mappage de nom valide pour l'utilisateur nul.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. Utilisez le `vserver cifs options show` Commande pour confirmer le mappage de l'utilisateur null à l'utilisateur ou au groupe Windows.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```