



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	1
Utilisez les sessions null pour accéder au stockage dans les environnements non Kerberos	1
Comment le système de stockage fournit un accès de session nul	1
Accorder aux utilisateurs nuls l'accès aux partages de système de fichiers	2

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'option `-restrict-anonymous`. 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
```

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.