非 Kerberos 環境のストレージにアクセスするには、 null セッションを使用します

ONTAP 9

NetApp
April 24, 2024

目次

非 Kerberos 環境のストレージにアクセスするには、 null セッションを使用します

非 Kerberos 環境でストレージにアクセスする場合は、 null セッションを使用します

null セッションアクセスは、ローカルシステムで稼働しているクライアントベースのサービスにストレージシステムデータなどのネットワークリソースへのアクセスを提供します。null セッションは、クライアントプロセスが「システム」アカウントを使用してネットワークリソースにアクセスするときに発生します。null セッション設定は非 Kerberos 認証に固有です。

ストレージシステムによる null セッションアクセスの実現方法

null セッション共有には認証が必要ないため、 null セッションアクセスが必要なクライアントは、その IP アドレスがストレージシステムにマッピングされている必要があります。

デフォルトでは、マッピングされていない null セッションクライアントは、共有の列挙など一部の ONTAP システムサービスにはアクセスできますが、ストレージシステムデータへのアクセスは制限されます。

> ONTAP は、でWindows RestrictAnonymousレジストリ設定値をサポートしています `-restrict-anonymous` オプションこれにより、マッピングされていない null ユーザが表示またはアクセスできるシステムリソースの範囲を制御できます。たとえば、共有の一覧や IPC$ 共有（非表示の名前付きパイプ共有）へのアクセスを無効にできます。。 `vserver cifs options modify` および `vserver cifs options show` の詳細については、のマニュアルページを参照してください `-restrict-anonymous` オプション

特に設定がないかぎり、 null セッションでストレージシステムアクセスを要求するローカルプロセスを実行しているクライアントは、「 everyone 」などの制限のないグループのみのメンバーとなります。null セッションアクセスを選択したストレージシステムリソースに制限するには、すべての null セッションクライアントが属するグループを作成します。このグループを作成すると、ストレージシステムアクセスを制限したり、null セッションクライアントのみに適用されるストレージシステムリソース権限を設定したりできます。

ONTAP には、マッピング構文が用意されています `vserver name-mapping` nullユーザセッションを使用したストレージシステムリソースへのアクセスを許可するクライアントのIPアドレスを指定するコマンドセット。null ユーザ用のグループを作成したら、 null セッションのみに適用されるストレージシステムリソースのアクセス制限およびリソース権限を指定できます。null ユーザは匿名ログオンとみなされます。null ユーザは、ホームディレクトリにアクセスできません。

マッピングされた IP アドレスからストレージシステムにアクセスするすべての null ユーザには、マッピングされたユーザ権限が付与されます。null ユーザにマッピングされたストレージシステムへの不正なアクセスを防止するため、適切な予防措置を検討してください。最大限の保護を実現するには、ストレージシステムと null ユーザによるストレージシステムアクセスが必要なすべてのクライアントを別のネットワークに配置し、IP アドレス「 SVM 」の問題を解消します。

関連情報

null ユーザにファイルシステム共有へのアクセスを許可します

null セッションクライアントによるストレージシステムリソースへのアクセスを許可するには、 null セッションクライアントに使用するグループを割り当てて null セッションクライアントの IP アドレスを記録し、ストレージシステム上の、 null セッションを使用したデータアクセスを許可するクライアントリストにその IP アドレスを追加します。

手順

1. を使用します `vserver name-mapping create` IP修飾子を使用して、nullユーザを任意の有効なWindowsユーザにマッピングするコマンド。

   次のコマンドは、有効なホスト名 google.com で user1 に null ユーザをマッピングします。

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

   次のコマンドは、有効な IP アドレス 10.238.2.54/32 で user1 に null ユーザをマッピングします。

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

2. を使用します `vserver name-mapping show` コマンドを入力してネームマッピングを確認します。

   ```
   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. を使用します `vserver cifs options modify –win-name-for-null-user` nullユーザにWindowsメンバーシップを割り当てるコマンド。

   このオプションは、 null ユーザに有効なネームマッピングが設定されている場合にのみ使用できます。

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

4. を使用します `vserver cifs options show` コマンドを使用して、nullユーザのWindowsユーザまたはグループへのマッピングを確認します。

```
vserver cifs options show

Vserver :vs1

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