



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	1
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	1
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	1
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	2

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

特に設定がない限り、 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。

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
```

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。