

Alibaba Cloud Apsara File Storage NAS

ユーザーガイド

Document Version20190702

目次

1 ファイルシステム.....	1
2 マウントポイント.....	3
3 権限グループの使用.....	5
4 RAM を使用して RAM ユーザーに NAS の権限を与える.....	7

1 ファイルシステム

ファイルシステムリストの使用、ファイルシステムインスタンスに関する詳細情報の確認、ファイルシステムの削除など、NAS コンソール上のファイルシステムに対してあらゆる種類の操作を実行できます。

前提条件

ファイルシステムを使用する前に、次のことを行う必要があります。

1. [NAS コンソール](#)にログインします。
2. [ファイルシステムを作成する](#)、または1つ以上のファイルシステムが作成されていることを確認します。

ファイルシステムリストを使用する

左側のパネルで、[ファイルシステムリスト]をクリックし、ファイルシステムリストページを表示します。

一覧では、[ファイルシステム名]の変更、ファイルシステムへの[マウントポイントの追加]、ファイルシステムの[管理]や[削除]を行うことができます。

ファイルシステムインスタンスの詳細を確認する

インスタンスの[ファイルシステム ID]をクリックするか、インスタンスの右側にある[管理]をクリックし、[ファイルシステムの詳細]ページを開きます。

詳細ページには、以下の情報が含まれています。

- ・ ファイルシステム ID、リージョン、ゾーン、ファイルシステムの使用状況など、ファイルシステムに関する基本情報
- ・ ファイルシステムのマウントポイントリスト。ファイルシステムのマウントポイントを管理できます。

ファイルシステムを削除する

削除するファイルシステムインスタンスの右側にある、[削除]をクリックします。



注：

- ・ ファイルシステムを削除する前に、ファイルシステムのすべてのマウントポイントを削除する必要があります。
- ・ ファイルシステムが削除されると、データを復元することはできません。この操作を実行するときは注意してください。

2 マウントポイント

マウントポイントリストの確認、マウントポイントの削除、マウントポイントの権限グループの変更、マウントポイントの有効化または無効化など、NAS コンソール上のファイルシステムインスタンスのマウントポイントに対してさまざまな操作を実行できます。

前提条件

マウントポイントで操作を実行する前に、次の作業を行う必要があります。

1. [NAS コンソール](#)にログインします。
2. [ファイルシステムの作成](#)または、1つ以上のファイルシステムが作成されていることを確認します。
3. [マウントポイントの追加](#)または、ファイルシステムインスタンスに1つ以上のマウントポイントが追加されていることを確認します。

マウントポイントリストの確認

[[ファイルシステムリスト](#)] ページで、ターゲットファイルシステムインスタンスをクリックし、[[ファイルシステムの詳細](#)] ページへ移動します。ファイルシステムのマウントポイントリストが表示されます。[[マウントポイントの追加](#)]、[[権限グループの変更](#)]、マウントポイントの [[有効化](#)] または [[無効化](#)]、マウントポイントを [[削除](#)] することができます。

マウントポイントを追加する

ファイルシステムにさらにマウントポイントを追加できます。詳細は、「[マウントポイントの追加](#)」を参照してください。

マウントポイントを有効または無効にする

[[無効化](#)] をクリックして、他のクライアントがマウントポイントへアクセスできないようにすることができます。または[[有効化](#)] をクリックしてアクセスを許可することができます。

マウントポイントを削除する

[[削除](#)] をクリックしてマウントポイントを削除します。マウントポイントは、削除した後で復元することはできません。



注：

VPC を削除する前に、VPC 内のすべてのマウントポイントを削除する必要があります。

マウントポイントの権限グループを変更する

各マウントポイントに権限グループをバインドする必要があります。送信元 IP ホワイトリストを指定することで、権限グループは ECS インスタンスがマウントポイントにアクセスすることを制限できます。[権限グループの変更] をクリックして、マウントポイントの権限グループを変更します。



注：

変更された権限グループは、最長で 1 分後に有効になります。

3 権限グループの使用

NAS では、権限グループを使用してユーザーアクセスを制御できます。

はじめに

NAS では、権限グループはホワイトリストとして機能し、ファイルシステムへのアクセスを制限できます。指定した IP アドレスまたは CIDR ブロックにファイルシステムへのアクセスを許可し、権限グループにルールを追加することで、異なる IP アドレスまたは CIDR ブロックに異なるレベルのアクセス許可を割り当てることができます。

NAS を有効化すると、デフォルトの VPC 許可グループが自動的に生成されます。これにより、VPC 内のすべての IP アドレスが完全な権限でマウントポイントにアクセスできるようになります。完全な権限には、root ユーザーに対する制限のない読み取り/書き込み権限が含まれています。



注：

- ・ 従来のネットワークマウントポイントでは、デフォルトの権限グループは提供されていません。さらに、権限グループルールで許可されている IP アドレスは、CIDR ブロックではなく単一の IP アドレスである必要があります。
- ・ アクセス許可グループのルールを慎重に追加し、必要な IP アドレスのみを許可することを推奨します。

権限グループの作成

権限グループを作成するには、次の手順に従います。

1. [NAS コンソール](#) にログインします。
2. 左側のナビゲーションウィンドウで、[権限グループ]をクリックし、[権限グループの作成]をクリックします。
3. [権限グループの作成] ページで、名前を入力して [OK] をクリックします。



注：

Alibaba Cloud アカウントには最大 10 の権限グループが許可されます。

権限グループのルール管理

以下のとおり、権限グループルールを追加、編集、または削除できます。

1. [NAS コンソール](#) にログインします。

2. 左側のナビゲーションウィンドウで、[アクセス許可グループ]をクリックし、[管理]をクリックします。
3. [権限グループのルール] ページでは、[ルールの追加]、ルールの [変更]、ルールの [削除] を行うことができます。

権限グループルールは、次の属性で構成されています。

属性	値	説明
許可されたアドレス	単一の IP アドレスまたは CDIR ブロック (従来のネットワークは単一の IP アドレスのみをサポートします)	ルールの許可されたオブジェクト
読み取りおよび書き込み権限	読み取り専用または読み取り/書き込み	許可されたオブジェクトにファイルシステムへの読み取り専用または読み取り/書き込みアクセスを許可します。
ユーザー権限	root ユーザーを制限しない (no_squash)、root ユーザーを制限する (root_squash)、すべてのユーザーを制限する (all_squash)	(list) ファイルシステム内の許可されたオブジェクトの Linux システムユーザーの権限を制限するかどうかを決定します。ファイルまたはディレクトリのアクセス権を決定するとき root ユーザーを制限すると、root ユーザーは誰もいないものとして扱われます。すべてのユーザーを制限すると、root ユーザーを含むすべてのユーザーは誰もいないものとして扱われます。
優先度	1~100、1 が最高の優先順位	同じ許可オブジェクトが複数のルールに一致すると、優先順位が最も高いルールが残り、優先順位が最も低いルールを上書きします。

4 RAM を使用して RAM ユーザーに NAS の権限を与える

リソースアクセス管理 (RAM) は、ユーザー ID を管理し、リソースアクセスを管理するように設計された Alibaba Cloud サービスです。RAM を使用すると、サブアカウント (RAM ユーザー) に NAS に対する操作を許可することができます。セキュリティのベストプラクティスに従い、NAS へのアクセスに RAM ユーザーアカウントを使用することを推奨します。この文書では、RAM に利用できる NAS の動作とリソースについて説明します。

RAM に対して利用可能な NAS アクション

RAM では、RAM ユーザーに次の NAS 操作を実行する権限を与えることができます。

API	説明
DescribeFileSystems	ファイルシステムを一覧表示します。
DescribeMountTargets	ファイルシステムのマウントポイントを一覧表示します。
DescribeAccessGroup	権限グループを一覧表示します。
DescribeAccessRule	権限グループルールを一覧表示します。
CreateMountTarget	ファイルシステムのマウントポイントを追加します。
CreateAccessGroup	権限グループを作成します。
CreateAccessRule	権限グループルールを追加します。
DeleteFileSystem	ファイルシステムを作成します。
DeleteMountTarget	マウントポイントを削除します。
DeleteAccessGroup	権限グループを削除します。
DeleteAccessRule	権限グループルールを削除します。
ModifyMountTargetStatus	マウントポイントを無効または有効にします。
ModifyMountTargetAccessGroup	マウントポイントの権限グループを変更します。
ModifyAccessGroup	権限グループを編集します。
ModifyAccessRule	権限ルールを編集します。

RAM に利用可能な NAS リソース

RAM 承認ポリシーでは、NAS は次のリソース抽象化のみをサポートします。

リソース	説明
*	すべての NAS リソースを示します。

権限付与ポリシーの例

次のポリシーは、すべての NAS リソースに対して読み取り専用の動作を許可します。

```
{
  "Version ": " 1 ",
  "Statement ": [
    {
      "Action ": " slb : Describe *",
      "Resource ": "*",
      "Effect ": " Allow "
    }
  ]
}
```