セキュリティ形式がデータアクセスに与える影響

ONTAP 9

NetApp
April 24, 2024

目次

セキュリティ形式がデータアクセスに与える影響

セキュリティ形式とその影響とは

セキュリティ形式には、 UNIX 、 NTFS 、 mixed 、および unified の 4 種類があり、セキュリティ形式ごとにデータに対する権限の処理方法が異なります。目的に応じて適切なセキュリティ形式を選択できるように、それぞれの影響について理解しておく必要があります。

セキュリティ形式はデータにアクセスできるクライアントの種類には影響しないことに注意してください。セキュリティ形式で決まるのは、データアクセスの制御に ONTAP で使用される権限の種類と、それらの権限を変更できるクライアントの種類だけです。

たとえば、ボリュームで UNIX セキュリティ形式を使用している場合でも、 ONTAP はマルチプロトコルに対応しているため、 SMB クライアントから引き続きデータにアクセスできます（認証と許可が適切な場合）。ただし、 ONTAP では、 UNIX クライアントのみが標準のツールを使用して変更できる UNIX 権限が使用されます。

セキュリティ形式	権限を変更できるクライアント	クライアントが使用できる権限	有効になるセキュリティ形式	ファイルにアクセスできるクライアント
「 UNIX 」	NFS	NFSv3 モードビット	「 UNIX 」	NFS と SMB
		NFSv4.x ACL		
NTFS	SMB	NTFS ACL	NTFS	
混在	NFS または SMB	NFSv3 モードビット	「 UNIX 」	
		NFSv4.x ACL		
		NTFS ACL	NTFS	
統合： （ONTAP 9.4 以前のリリースでは、Infinite Volume のみ）。	NFS または SMB	NFSv3 モードビット	「 UNIX 」	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

FlexVol ボリュームでは、 UNIX 、 NTFS 、および mixed のセキュリティ形式がサポートされます。セキュリティ形式が mixed または unified の場合は、ユーザがセキュリティ形式を各自設定するため、権限を最後に変更したクライアントの種類によって有効になる権限が異なります。権限を最後に変更したクライアントが NFSv3 クライアントの場合、権限は UNIX NFSv3 モードビットになります。最後のクライアントが NFSv4 クライアントの場合、権限は NFSv4 ACL になります。最後のクライアントが SMB クライアントの場合、権限は Windows NTFS ACL になります。

unified セキュリティ形式は、 Infinite Volume でのみ使用できます。 Infinite Volume は、 ONTAP 9.5 以降のリリースではサポートされなくなりました。詳細については、を参照してください FlexGroup ボリュームの管理の概要。

ONTAP 9.2以降では、 `show-effective-permissions` パラメータをに設定します `vserver security file-directory` コマンドを使用すると、指定したファイルまたはフォルダパスに対してWindowsユーザまたはUNIXユーザに付与されている有効な権限を表示できます。また、オプションのパラメータも指定します `-share-name` 有効な共有権限を表示できます。

ONTAP で、最初にデフォルトのファイル権限がいくつか設定されます。デフォルトでは、UNIX 、 mixed 、および unified のセキュリティ形式のボリュームにあるデータについては、セキュリティ形式は UNIX 、権限の種類は UNIX モードビット（特に指定しないかぎり 0755 ）が有効になります。これは、デフォルトのセキュリティ形式で許可されたクライアントで設定するまで変わりません。NTFS セキュリティ形式のボリュームにあるデータについては、デフォルトで NTFS セキュリティ形式が有効になり、すべてのユーザにフルコントロール権限を許可する ACL が割り当てられます。

セキュリティ形式を設定する場所とタイミング

セキュリティ形式は、 FlexVol （ルートボリュームとデータボリュームの両方）および qtree で設定できます。セキュリティ形式は、作成時に手動で設定することも、自動的に継承することも、あとで変更することもできます。

SVM で使用するセキュリティ形式を決定します

ボリュームで使用するセキュリティ形式を決定するには、 2 つの要素を考慮する必要があります。第 1 の要素は、ファイルシステムを管理する管理者のタイプです。第 2 の要素は、ボリューム上のデータにアクセスするユーザまたはサービスのタイプです。

ボリュームのセキュリティ形式を設定するときは、最適なセキュリティ形式を選択して権限の管理に関する問題を回避するために、環境のニーズを考慮する必要があります。決定時には次の点を考慮すると役立ちます。

セキュリティ形式	以下の場合に選択
「 UNIX 」	• ファイルシステムが UNIX 管理者によって管理される。 • ユーザの大半が NFS クライアントである。 • データにアクセスするアプリケーションで、サービスアカウントとして UNIX ユーザが使用される。
NTFS	• ファイルシステムは Windows 管理者によって管理されます。 • ユーザの大部分がSMBクライアントです。 • データにアクセスするアプリケーションで、サービスアカウントとして Windows ユーザが使用される。
混在	• ファイルシステムが UNIX 管理者と Windows 管理者の両方によって管理され、ユーザが NFS クライアントと SMB クライアントの両方で構成される。

セキュリティ形式の継承の仕組み

新しい FlexVol または qtree の作成時にセキュリティ形式を指定しない場合、セキュリティ形式はさまざまな方法で継承されます。

セキュリティ形式は、次のように継承されます。

- FlexVol ボリュームは、そのボリュームを含む SVM のルートボリュームのセキュリティ形式を継承します。
- qtree は、その qtree を含む FlexVol ボリュームのセキュリティ形式を継承します。
- ファイルまたはディレクトリは、そのファイルまたはディレクトリを含む FlexVol ボリュームまたは qtree のセキュリティ形式を継承します。

ONTAP による UNIX アクセス権の維持方法

UNIX アクセス権を現在持っている FlexVol ボリューム内のファイルが Windows アプリケーションによって編集および保存されても、 ONTAP は UNIX アクセス権を維持できます。

Windows クライアントのアプリケーションは、ファイルを編集して保存するときに、ファイルのセキュリティプロパティを読み取り、新しい一時ファイルを作成し、それらのプロパティを一時ファイルに適用してから、一時ファイルに元のファイル名を付けます。

セキュリティプロパティのクエリを実行すると、 Windows クライアントは、 UNIX アクセス権を正確に表す構築済み ACL を受け取ります。この構築済み ACL は、 Windows アプリケーションによってファイルが更新されるときにファイルの UNIX アクセス権を維持し、生成されたファイルが同じ UNIX アクセス権を持つようにするためだけに使用されます。ONTAP は、構築済み ACL を使用して NTFS ACL を設定しません。

Windows のセキュリティタブを使用して UNIX アクセス権を管理します

SVM 上の mixed セキュリティ形式のボリュームまたは qtree に含まれるファイルまたはフォルダの UNIX アクセス権を操作する場合は、 Windows クライアントのセキュリティタブを使用できます。また、 Windows ACL を照会および設定できるアプリケーションを使用することもできます。

- UNIX アクセス権の変更

  Windows のセキュリティタブを使用して、 mixed セキュリティ形式のボリュームまたは qtree の UNIX アクセス権を表示および変更できます。メインの [Windows Security] タブを使用して UNIX アクセス権を変更する場合は、編集する既存の ACE を削除してから（モードビットを 0 に設定）、変更を行う必要があります。または、高度なエディタを使用して権限を変更することもできます。

  モードのアクセス権を使用している場合は、リストされた UID 、 GID 、およびその他（コンピュータにアカウントを持つその他すべてのユーザ）のモードアクセス権を直接変更できます。たとえば、表示された UID に r-x のアクセス権が設定されている場合、この UID のアクセス権を rwx に変更できます。

- UNIX アクセス権を NTFS アクセス権に変更しています

  Windows のセキュリティタブを使用して、ファイルおよびフォルダのセキュリティ形式が UNIX 対応である mixed 型セキュリティ形式のボリュームまたは qtree 上で、 UNIX セキュリティオブジェクトを Windows セキュリティオブジェクトに置き換えることができます。

  適切な Windows のユーザおよびグループのオブジェクトに置き換える前に、リストされている UNIX アクセス権のエントリをすべて削除しておく必要があります。次に、 Windows のユーザおよびグループのオブジェクトに NTFS ベースの ACL を設定します。すべての UNIX セキュリティオブジェクトを削除

し、 Windows のユーザおよびグループのみを mixed セキュリティ形式のボリュームまたは qtree 上のファイルまたはフォルダに追加すると、ファイルまたはフォルダのセキュリティ形式が UNIX から NTFS へ変換されます。

フォルダの権限を変更する場合、 Windows のデフォルトの動作では、すべてのサブフォルダとファイルにこれらの変更が反映されます。したがって、セキュリティ形式の変更をすべての子フォルダ、サブフォルダ、およびファイルに反映したくない場合は、反映する範囲を希望の範囲に変更する必要があります。