StorageGRID をクラウド階層として接続するために必要な情報

StorageGRID 11.5

NetApp
April 11, 2024

目次

StorageGRID をクラウド階層として接続するために必要な情報

StorageGRID をFabricPool のクラウド階層として接続する前に、StorageGRID でいくつかの設定手順を実行して特定の値を取得する必要があります。

このタスクについて

次の表に、 FabricPool のクラウド階層として StorageGRID を接続する場合に ONTAP に入力する必要がある情報を示します。このセクションのトピックでは、 StorageGRID のグリッドマネージャとテナントマネージャを使用して必要な情報を取得する方法について説明します。

表示されるフィールド名と ONTAP で必要な値の入力プロセスは、 ONTAP CLI （ storage aggregate object-store config create ）と ONTAP System Manager （ * Storage * > * Aggregates & Disks * > * Cloud Tier * ）のどちらを使用しているかによって異なります。

詳細については、以下を参照してください。

- "TR-4598：『FabricPool Best Practices for ONTAP 9.8』"
- "ONTAP 9 ドキュメンテーション・センター"

ONTAP フィールド	説明
オブジェクトストア名	一意でわかりやすい名前。例： `StorageGRID_Cloud_Tier`。
プロバイダタイプ	StorageGRID （System Manager）または `SGWS` （CLI）。
ポート	FabricPool が StorageGRID に接続するときに使用するポート。StorageGRID ロードバランサエンドポイントを定義する際に使用するポート番号を指定します。 "FabricPool のロードバランサエンドポイントの作成"
サーバ名	StorageGRID ロードバランサエンドポイントの完全修飾ドメイン名（ FQDN ）。例： `s3.storagegrid.company.com`。 次の点に注意してください。 • ここで指定するドメイン名は、 StorageGRID ロードバランサエンドポイント用にアップロードする CA 証明書のドメイン名と一致する必要があります。 • このドメイン名の DNS レコードは、 StorageGRID への接続に使用する各 IP アドレスにマッピングする必要があります。 "StorageGRID IPアドレス用のDNSサーバを設定する"

ONTAP フィールド	説明
コンテナ名	この ONTAP クラスタで使用する StorageGRID バケットの名前。例： `fabricpool-bucket`。このバケットはTenant Managerで作成します。 次の点に注意してください。 • 設定の作成後にバケット名を変更することはできません。 • バケットでバージョン管理を有効にすることはできません。 • データを StorageGRID に階層化する ONTAP クラスタごとに異なるバケットを使用する必要があります。 "S3バケットを作成してアクセスキーを取得する"
アクセスキーとシークレットのパスワード	StorageGRID テナントアカウントのアクセスキーとシークレットアクセスキー。 これらの値は Tenant Manager で生成します。 "S3バケットを作成してアクセスキーを取得する"
SSL	有効にする必要があります。
オブジェクトストアの証明書	StorageGRID ロードバランサエンドポイントの作成時にアップロードした CA 証明書。 • 注：中間 CA が StorageGRID 証明書を発行した場合は、中間 CA 証明書を指定する必要があります。StorageGRID 証明書がルート CA によって直接発行された場合は、ルート CA 証明書を指定する必要があります。 "FabricPool のロードバランサエンドポイントの作成"

完了後

必要な StorageGRID 情報を取得したら、 ONTAP にアクセスしてクラウド階層として StorageGRID を追加し、クラウド階層をアグリゲートとして追加し、ボリューム階層化ポリシーを設定できます。

ロードバランシングのベストプラクティスを参照してください

StorageGRID をFabricPool クラウド階層として接続する前に、StorageGRID グリッドマネージャを使用して少なくとも1つのロードバランサエンドポイントを設定します。

ロードバランシングとは

データを FabricPool から StorageGRID システムに階層化すると、 StorageGRID はロードバランサを使用して取り込みと読み出しのワークロードを管理します。ロードバランシングは、 FabricPool ワークロードを複数のストレージノードに分散することで、速度と接続容量を最大化します。

StorageGRID ロードバランササービスはすべての管理ノードとすべてのゲートウェイノードにインストールされ、レイヤ 7 のロードバランシングを提供します。クライアント要求の Transport Layer Security （ TLS ）終了を実行し、要求を検査し、ストレージノードへの新しいセキュアな接続を確立します。

各ノード上のロードバランササービスは、クライアントトラフィックをストレージノードに転送する際に独立して動作します。重み付きのプロセスを使用すると、ロードバランササービスは、より多くの要求をより多くの CPU を使用可能なストレージノードにルーティングします。

推奨されるロードバランシングメカニズムは StorageGRID ロードバランササービスですが、代わりにサードパーティのロードバランサを統合することもできます。詳細については、ネットアップのアカウント担当者にお問い合わせいただくか、次のテクニカルレポートを参照してください。

"StorageGRID ロードバランサオプション"

ゲートウェイノード上の別の Connection Load Balancer （ CLB ）サービスは廃止され、FabricPool での使用は推奨されなくなりました。

StorageGRID ロードバランシングのベストプラクティスを参照してください

一般的なベストプラクティスとして、 StorageGRID システムの各サイトにロードバランササービスを使用するノードが 2 つ以上必要です。たとえば、サイトには管理ノードとゲートウェイノードの両方、または管理ノードが2つ含まれている場合があります。SG100 または SG100 サービスアプライアンス、ベアメタルノード、仮想マシン（ VM ）ベースのノードのいずれを使用しているかに関係なく、各ロードバランシングノードに適切なネットワーク、ハードウェア、または仮想化インフラがあることを確認します。

StorageGRID ロードバランサエンドポイントを設定して、ゲートウェイノードと管理ノードが FabricPool の受信要求と送信要求に使用するポートを定義する必要があります。

ロードバランサエンドポイント証明書のベストプラクティス

FabricPool で使用するロードバランサエンドポイントを作成する際には、プロトコルとしてHTTPSを使用する必要があります。その後、公開された信頼された証明書またはプライベート認証局（CA）によって署名された証明書をアップロードするか、自己署名証明書を生成できます。この証明書は、 ONTAP が StorageGRID で認証することを許可します。

ベストプラクティスとして、 CA サーバ証明書を使用して接続を保護することを推奨します。CA によって署名された証明書は、無停止でローテーションできます。

ロードバランサエンドポイントで使用する CA 証明書を要求する場合は、証明書のドメイン名が、そのロードバランサエンドポイント用に ONTAP に入力するサーバ名と一致していることを確認してください。可能であれば、ワイルドカード（ * ）を使用して仮想ホスト形式の URL を許可します。例：

```
*.s3.storagegrid.company.com
```

StorageGRID を FabricPool クラウド階層として追加する場合は、 ONTAP クラスタにも同じ証明書をインストールする必要があります。また、ルート証明書と下位の認証局（ CA ）証明書もインストールする必要があります。

StorageGRID では、さまざまな目的でサーバ証明書が使用されます。ロードバランササービスに接続する場合は、Object Storage APIサービスエンドポイントのサーバ証明書をアップロードする必要はありません。

ロードバランシングエンドポイントのサーバ証明書の詳細を確認するには、次の手順を実行します。

- "負荷分散の管理"
- "サーバ証明書のセキュリティ強化ガイドライン"

ハイアベイラビリティグループのベストプラクティス

StorageGRID をFabricPool クラウド階層として接続する前に、StorageGRID グリッドマネージャを使用してハイアベイラビリティ（HA）グループを設定します。

ハイアベイラビリティ（**HA**）グループとは

FabricPool データの管理に常にロードバランササービスを使用できるようにするには、複数の管理ノードとゲートウェイノードのネットワークインターフェイスを 1 つのエンティティ（ハイアベイラビリティ（ HA ）グループと呼ばれます）にグループ化します。HA グループのアクティブノードで障害が発生した場合、グループ内の別のノードがワークロードの管理を続行できます。

各 HA グループは、関連付けられたノード上の共有サービスへの可用性の高いアクセスを提供します。たとえば、すべての管理ノードで構成されるHAグループは、一部の管理ノード管理サービスとロードバランササービスへの高可用性アクセスを提供します。ゲートウェイノードのみ、または管理ノードとゲートウェイノードの両方で構成されるHAグループは、共有ロードバランササービスへの可用性の高いアクセスを提供します。

HAグループを作成するときは、グリッドネットワーク（eth0）またはクライアントネットワーク（eth2）に属するネットワークインターフェイスを選択します。HAグループ内のすべてのインターフェイスは、同じネットワークサブネット内に存在する必要があります。

HAグループは、グループ内のアクティブインターフェイスに追加された仮想IPアドレスを1つ以上維持します。アクティブインターフェイスが使用できなくなった場合、仮想IPアドレスは別のインターフェイスに移動します。このフェイルオーバープロセスにかかる時間は通常数秒です。クライアントアプリケーションへの影響はほとんどなく、通常の再試行で処理を続行できます。

ロードバランシングノードのHAグループを設定すると、FabricPool はそのHAグループの仮想IPアドレスに接続します。

ハイアベイラビリティ（ **HA** ）グループのベストプラクティス

FabricPool 用の StorageGRID HA グループを作成する際のベストプラクティスは、次のワークロードによって異なります。

- プライマリワークロードのデータで FabricPool を使用する場合は、データの取得の中断を回避するために、ロードバランシングノードを少なくとも 2 つ含む HA グループを作成する必要があります。
- FabricPool の snapshot-only のボリューム階層化ポリシーまたは非プライマリのローカルのパフォーマンス階層（ディザスタリカバリ先や NetApp SnapMirror ® デスティネーションなど）を使用する予定の場合は、 1 つのノードだけで HA グループを設定できます。

ここでは、アクティブ / バックアップ HA の HA グループの設定（一方のノードがアクティブでもう一方のノ

ードがバックアップ）について説明します。ただし、 DNS ラウンドロビンまたはアクティブ / アクティブ HA を使用することもできます。これらの他の HA 構成のメリットについては、を参照してください "HA グループの設定オプション"。

StorageGRID IPアドレス用のDNSサーバを設定する

ハイアベイラビリティグループとロードバランサエンドポイントを設定したら、 ONTAP システムのドメインネームシステム（ DNS ）に、 FabricPool が接続に使用する IP アドレスに StorageGRID サーバ名（完全修飾ドメイン名）を関連付けるレコードが含まれていることを確認する必要があります。

DNS レコードに入力する IP アドレスは、負荷分散ノードの HA グループを使用しているかどうかによって異なります。

- HA グループを設定している場合、 FabricPool はその HA グループの仮想 IP アドレスに接続します。
- HA グループを使用していない場合、 FabricPool は、任意のゲートウェイノードまたは管理ノードの IP アドレスを使用して StorageGRID ロードバランササービスに接続できます。

また、 DNS レコードが、ワイルドカード名を含む、必要なすべてのエンドポイントドメイン名を参照していることを確認する必要があります。

FabricPool のハイアベイラビリティ（HA）グループの作成

FabricPool で使用するように StorageGRID を設定する場合は、必要に応じて 1 つ以上のハイアベイラビリティ（ HA ）グループを作成できます。HA グループは、管理ノード、ゲートウェイノード、またはその両方の 1 つ以上のネットワークインターフェイスで構成されます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

このタスクについて

各 HA グループは、仮想 IP アドレス（ VIP ）を使用して、関連付けられたノード上の共有サービスへの可用性の高いアクセスを提供します。

詳細については、を参照してください。を参照してください "ハイアベイラビリティグループの管理"。

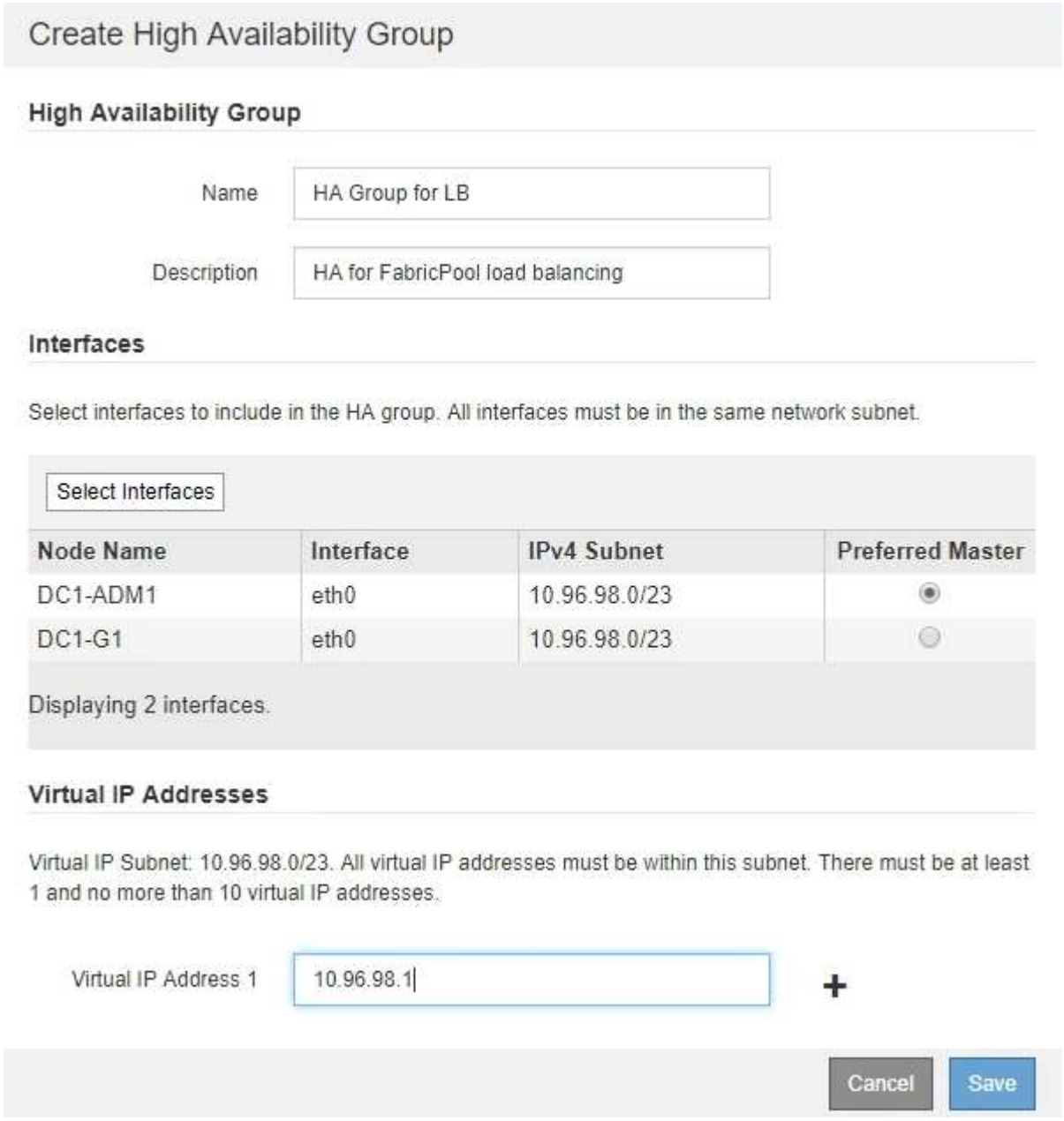
手順

1. * Configuration > Network Settings > High Availability Groups *を選択します。
2. ネットワークインターフェイスを1つ以上選択してください。ネットワークインターフェイスは、グリッドネットワーク（eth0）またはクライアントネットワーク（eth2）上の同じサブネットに属している必要があります。
3. 1つのノードを優先マスターに割り当てます。

   優先マスターは、障害が発生してVIPアドレスがバックアップインターフェイスに再割り当てされない限り、アクティブインターフェイスです。

4. HAグループのIPv4アドレスを10個まで入力します。

   すべてのメンバーインターフェイスで共有するIPv4サブネット内のアドレスを指定する必要があります。



FabricPool のロードバランサエンドポイントの作成

FabricPool で使用するStorageGRID を設定する場合は、ロードバランサエンドポイントを設定し、ロードバランサエンドポイント証明書をアップロードします。この証明書は、ONTAP とStorageGRID 間の接続を保護するために使用されます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

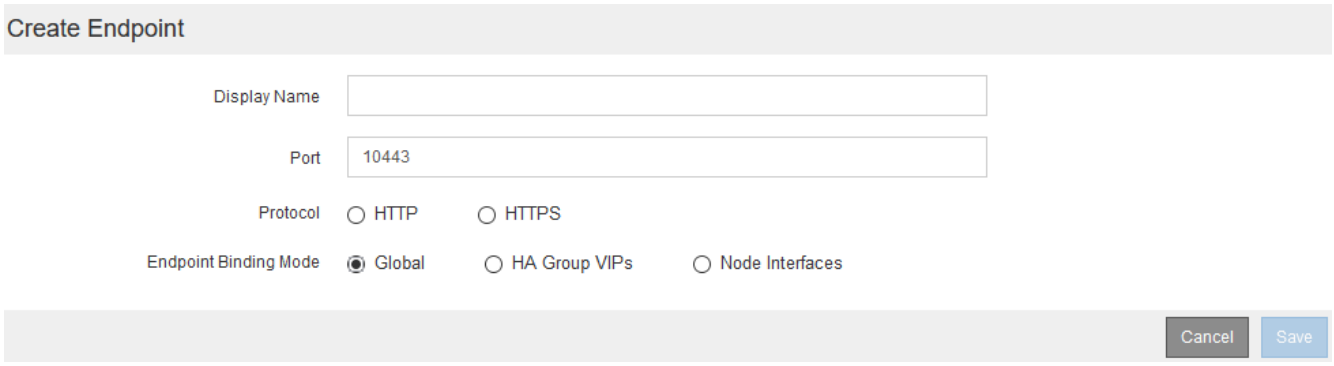
- 次のファイルが必要です。
  - Server Certificate ：カスタムサーバ証明書ファイル。
  - Server Certificate Private Key ：カスタムサーバ証明書の秘密鍵ファイル。
  - CA Bundle：各中間発行認証局（CA）の証明書を含む単一のファイル。このファイルには、 PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結して含まれている必要があります。

このタスクについて

このタスクの詳細については、を参照してください "ロードバランサエンドポイントの設定"。

手順

1. [* Configuration > Network Settings > Load Balancer Endpoints *]を選択します。



2. [エンドポイントの追加]を選択します。
3. 次の情報を入力します。

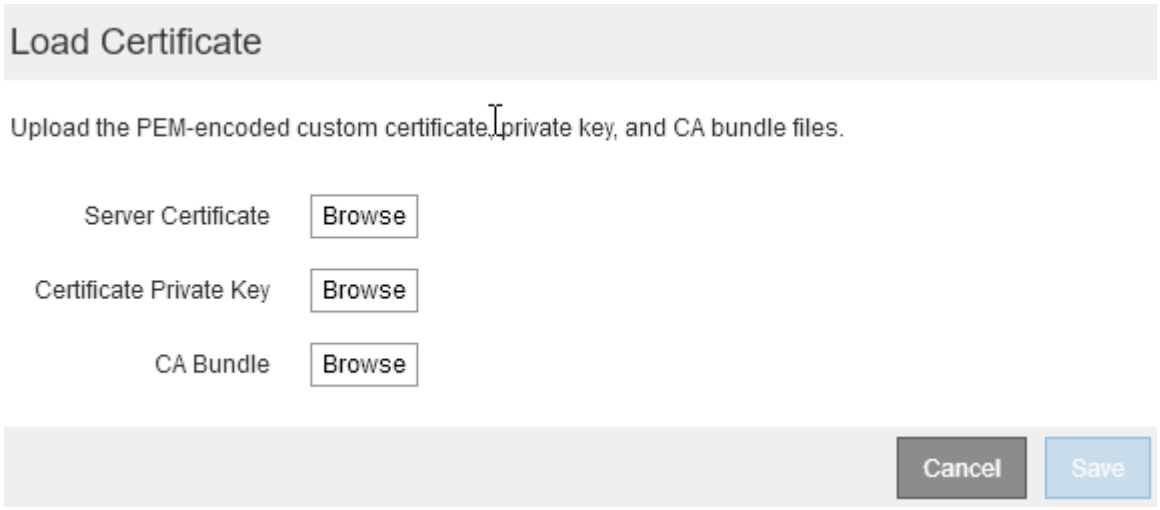
フィールド	説明
表示名	エンドポイントのわかりやすい名前
ポート	ロードバランシングに使用する StorageGRID ポート。このフィールドのデフォルト値は 10433 ですが、未使用の外部ポートを入力することもできます。80 または 443 と入力すると、エンドポイントは管理ノードで予約されているため、ゲートウェイノードにのみ設定されます。 • 注： * 他のグリッドサービスで使用されているポートは使用できません。内部および外部の通信に使用されるポートのリストを参照してください。 "ネットワークポートのリファレンス" StorageGRID を FabricPool クラウド階層として接続する場合は、 ONTAP に同じポート番号を指定する必要があります。

フィールド	説明
プロトコル	は* HTTPS *にする必要があります。
エンドポイントバインドモード	[グローバル * （ Global * ）] 設定を使用するか（推奨）、このエンドポイントのアクセス性を次のいずれかに制限します。 • 特定のハイアベイラビリティ（ HA ）仮想 IP アドレス（ VIP ）。このオプションは、ワークロードの分離レベルを大幅に高める必要がある場合にのみ使用してください。 • 特定のノードの特定のネットワークインターフェイス。

4. [保存（ Save ）] を選択します。

   [Edit Endpoint]ダイアログボックスが表示されます。

5. 「* Endpoint Service Type 」で「 S3 *」を選択します。
6. [証明書のアップロード*(推奨)]を選択し、サーバ証明書、証明書の秘密鍵、およびCAバンドルを参照します。



7. [保存（ Save ）] を選択します。

FabricPool のテナントアカウントの作成

Grid Manager で FabricPool 用のテナントアカウントを作成する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

テナントアカウントを使用すると、クライアントアプリケーションで StorageGRID に対してオブジェクトの格納や読み出しを行うことができます。各テナントアカウントには、専用のアカウント ID 、許可されたグループとユーザ、バケット、オブジェクトがあります。

複数の ONTAP クラスタに同じテナントアカウントを使用できます。また、必要に応じて、 ONTAP クラスタごとに専用のテナントアカウントを作成することもできます。

> この手順は、 Grid Manager にシングルサインオン（ SSO ）が設定されていることを前提としています。SSOを使用していない場合は、の手順を使用します "StorageGRID がSSOを使用していない場合のテナントアカウントの作成"。

手順

1. 「* tenants *」を選択します
2. 「 * Create * 」を選択します。
3. FabricPool テナントアカウントの表示名を入力します。
4. S3 を選択します。
5. プラットフォームサービスの使用を有効にするには、[プラットフォームサービスを許可]チェックボックスをオンのままにします。

   プラットフォームサービスが有効になっている場合、テナントは外部サービスにアクセスする CloudMirror レプリケーションなどの機能を使用できます。
6. Storage Quota *フィールドは空白のままにします。
7. [* Root Access Group]フィールドで、テナントに対する最初のRoot Access権限を持つ既存のフェデレーテッドグループをGrid Managerから選択します。
8. [保存（ Save ）] を選択します。

S3バケットを作成してアクセスキーを取得する

FabricPool ワークロードで StorageGRID を使用する前に、 FabricPool データ用の S3 バケットを作成する必要があります。また、 FabricPool に使用するテナントアカウントのアクセスキーとシークレットアクセスキーを取得する必要があります。

必要なもの

- FabricPool で使用するテナントアカウントを作成しておく必要があります。

このタスクについて

ここでは、 StorageGRID テナントマネージャを使用してバケットを作成し、アクセスキーを取得する方法について説明します。テナント管理 API または StorageGRID S3 REST API を使用してこれらのタスクを実行することもできます。

詳細については、以下をご覧ください。

- "テナントアカウントを使用する"
- "S3 を使用する"

手順

1. Tenant Manager にサインインします。

   次のいずれかを実行できます。

   - Grid Manager の Tenant Accounts ページで、テナントの * Sign In * リンクを選択し、クレデンシャルを入力します。
   - Web ブラウザでテナントアカウントの URL を入力し、クレデンシャルを入力します。

2. FabricPool データ用の S3 バケットを作成する。

   使用する ONTAP クラスタごとに一意のバケットを作成する必要があります。

   a. ストレージ（ S3 ） * > * バケット * を選択します。
   b. [* バケットの作成 *] を選択します。
   c. FabricPool で使用する StorageGRID バケットの名前を入力します。例： `fabricpool-bucket`。

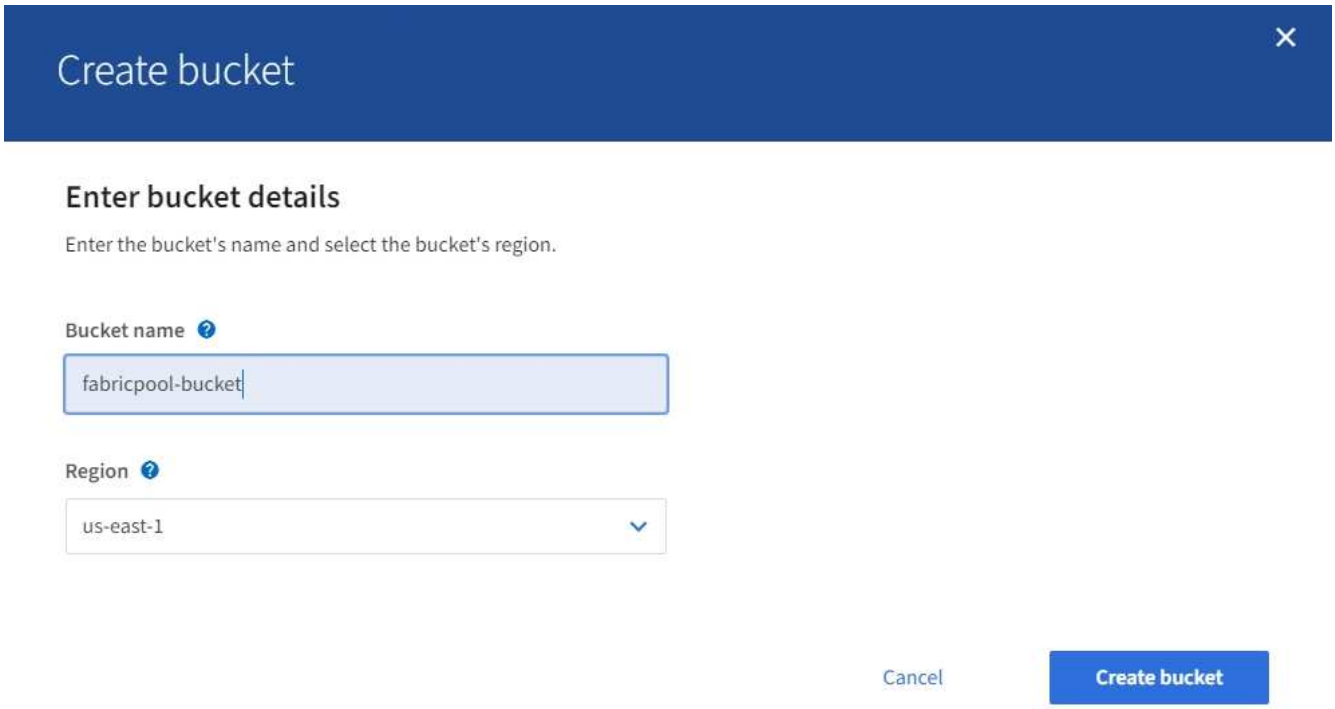
      バケットの作成後にバケット名を変更することはできません。

      バケット名は次のルールを満たす必要があります。

      - StorageGRID システム全体で（テナントアカウント内だけではなく）一意である必要があります。
      - DNS に準拠している必要があります。
      - 3 文字以上 63 文字以下にする必要があります。
      - 1 つ以上のラベルを連続して指定できます。隣接するラベルはピリオドで区切ります。各ラベルの先頭と末尾の文字は小文字のアルファベットか数字にする必要があり、使用できる文字は小文字のアルファベット、数字、ハイフンのみです。
      - テキスト形式の IP アドレスのようにはできません。
      - 仮想ホスト形式の要求でピリオドを使用しないでください。ピリオドを使用すると、サーバワイルドカード証明書の検証で原因 の問題が発生します。

   d. このバケットのリージョンを選択します。

      デフォルトでは、すべてのバケットがに作成されます `us-east-1` リージョン：



a. [* バケットの作成 *] を選択します。

3. アクセスキーとシークレットアクセスキーを作成します。

a. 「 * storage （ S3 ） * > * My access keys * 」を選択します。

b. 「 * キーの作成 * 」を選択します。

c. [アクセスキーの作成 *] を選択します。

d. アクセスキー ID とシークレットアクセスキーを安全な場所にコピーするか、「 * Download.csv * 」を選択してアクセスキー ID とシークレットアクセスキーを含むスプレッドシートファイルを保存します。

これらの値は、 ONTAP で StorageGRID を FabricPool クラウド階層として設定するときに入力します。

今後新しいアクセスキーとシークレットアクセスキー StorageGRID を作成する場合は、 ONTAP がデータの格納と読み出しを中断なく行えるように、 ONTAP で対応する値をただちに更新する必要があります。

著作権に関する情報

商標に関する情報