S3セットアップウィザードを使用する

StorageGRID 11.8

NetApp
May 17, 2024

目次

S3セットアップウィザードを使用する

S3セットアップウィザードの「考慮事項と要件」を使用します

S3セットアップウィザードを使用して、StorageGRID をS3アプリケーションのオブジェクトストレージシステムとして設定できます。

S3セットアップウィザードを使用するタイミング

S3セットアップウィザードの手順に従って、S3アプリケーションで使用するStorageGRID を設定します。ウィザードを完了すると、ファイルをダウンロードしてS3アプリケーションに値を入力します。ウィザードを使用すると、システムをより迅速に設定し、設定がStorageGRID のベストプラクティスに準拠していることを確認できます。

を使用している場合 "rootアクセス権限"S3セットアップウィザードは、StorageGRIDグリッドマネージャの使用を開始したときに完了することも、あとからアクセスして完了することもできます。要件に応じて、必要な項目の一部またはすべてを手動で設定し、ウィザードを使用してS3アプリケーションで必要な値をアセンブルすることもできます。

ウィザードを使用する前に

ウィザードを使用する前に、これらの前提条件を満たしていることを確認してください。

IPアドレスを取得し、**VLAN**インターフェイスを設定します

ハイアベイラビリティ（HA）グループを設定する場合は、S3アプリケーションが接続するノードと使用するStorageGRID ネットワークを確認しておきます。また、サブネットCIDR、ゲートウェイIPアドレス、および仮想IP（VIP）アドレスに入力する値も確認しておきます。

仮想LANを使用してS3アプリケーションからトラフィックを分離する場合は、VLANインターフェイスがすでに設定されています。を参照してください "VLAN インターフェイスを設定します"。

アイデンティティフェデレーションと**SSO**を設定する

StorageGRID システムでアイデンティティフェデレーションまたはシングルサインオン（SSO）を使用する場合は、これらの機能を有効にしておきます。また、S3アプリケーションが使用するテナントアカウントへのルートアクセスが必要なフェデレーテッドグループも確認しておきます。を参照してください "アイデンティティフェデレーションを使用する" および "シングルサインオンを設定します"。

ドメイン名を取得して設定します

StorageGRID に使用するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を確認しておきます。ドメインネームサーバ（DNS）のエントリによって、このFQDNが、ウィザードを使用して作成するHAグループの仮想IP（VIP）アドレスにマッピングされます。

S3仮想ホスト形式の要求を使用する場合は、をインストールしておく必要があります "S3エンドポイントのドメイン名が設定されました"。仮想ホスト形式の要求を使用することを推奨します。

ロードバランサとセキュリティ証明書の要件を確認します

StorageGRID ロードバランサを使用する場合は、ロードバランシングに関する一般的な考慮事項を確認しておきます。アップロードする証明書、または証明書の生成に必要な値を用意しておきます。

外部（サードパーティ）のロードバランサエンドポイントを使用する場合は、そのロードバランサの完全修飾ドメイン名（FQDN）、ポート、および証明書が必要です。

グリッドフェデレーション接続を設定します

S3テナントがグリッドフェデレーション接続を使用してアカウントデータをクローニングし、バケットオブジェクトを別のグリッドにレプリケートできるようにする場合は、ウィザードを開始する前に次の点を確認してください。

- これで完了です "グリッドフェデレーション接続を設定しました"。
- 接続のステータスは*接続済み*です。
- Root Access 権限が割り当てられている。

S3セットアップウィザードにアクセスして実行します

S3セットアップウィザードを使用して、S3アプリケーションで使用するStorageGRIDを設定できます。セットアップウィザードには、StorageGRID バケットへのアクセスとオブジェクトの保存に必要な値が表示されます。

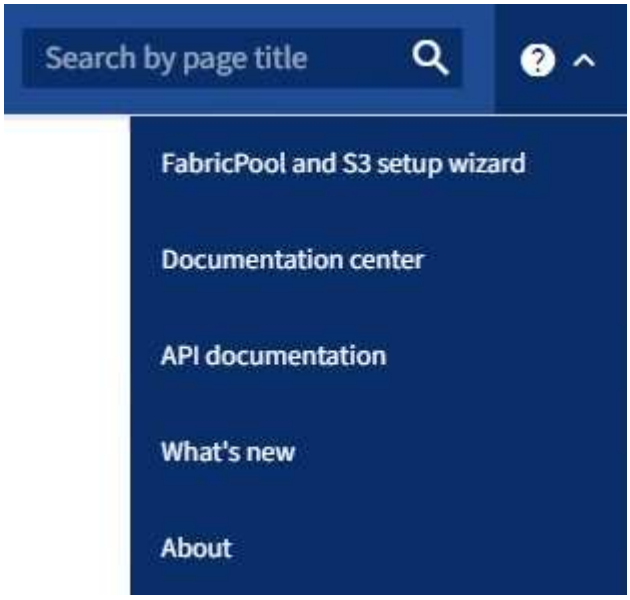
作業を開始する前に

- を使用することができます "rootアクセス権限"。
- を確認しておきます "考慮事項と要件" ウィザードを使用します。

ウィザードにアクセスします

手順

1. を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
2. ダッシュボードに「FabricPool and S3 setup wizard」バナーが表示された場合は、バナー内のリンクを選択します。バナーが表示されなくなった場合は、グリッドマネージャのヘッダーバーでヘルプアイコンを選択し、 FabricPool and S3 setup wizard *を選択します。



3. FabricPool とS3のセットアップウィザードのページのS3アプリケーションセクションで、*今すぐ設定*を選択します。

手順1/6：HAグループを設定する

HAグループは、それぞれにStorageGRID ロードバランササービスが含まれるノードの集まりです。HAグループには、ゲートウェイノード、管理ノード、またはその両方を含めることができます。

HAグループを使用すると、S3データ接続の可用性を維持できます。HAグループのアクティブインターフェイスで障害が発生しても、バックアップインターフェイスでワークロードを管理できるため、S3処理への影響はほとんどありません。

このタスクの詳細については、を参照してください "ハイアベイラビリティグループを管理します"。

手順

1. 外部のロードバランサを使用する場合は、HAグループを作成する必要はありません。[Skip this step]*を選択し、に進みます [手順2/6：ロードバランサエンドポイントの設定]。
2. StorageGRID ロードバランサを使用するには、新しいHAグループを作成するか、既存のHAグループを使用します。

HA グループを作成します

a. 新しいHAグループを作成するには、*[HAグループの作成]*を選択します。

b. [詳細を入力]*ステップで、次のフィールドに値を入力します。

フィールド	説明
HAグループ名	このHAグループの一意の表示名。
概要 （オプション）	このHAグループの概要 。

c. [インターフェイスの追加]*手順で、このHAグループで使用するノードインターフェイスを選択します。

列ヘッダーを使用して行をソートするか、検索キーワードを入力してインターフェイスをより迅速に検索します。

ノードは1つ以上選択できますが、ノードごとに選択できるインターフェイスは1つだけです。

d. [* prioritize interfaces]ステップでは、このHAグループのプライマリインターフェイスとバックアップインターフェイスを決定します。

行をドラッグして、*優先順位*列の値を変更します。

リストの最初のインターフェイスはプライマリインターフェイスです。プライマリインターフェイスは、障害が発生しないかぎり、アクティブインターフェイスです。

HAグループに複数のインターフェイスが含まれていて、アクティブインターフェイスで障害が発生した場合、仮想IP（VIP）アドレスは優先順位に従って最初のバックアップインターフェイスに移動します。そのインターフェイスに障害が発生すると、 VIP アドレスは次のバックアップインターフェイスに移動します。障害が解決されると、VIPアドレスは使用可能な最もプライオリティの高いインターフェイスに戻ります。

e. [IPアドレスの入力]*ステップで、次のフィールドに値を入力します。

フィールド	説明
サブネットCIDR	VIPサブネットのアドレス（CIDR表記）。IPv4アドレス、スラッシュ、およびサブネットの長さ（0〜32）。 ネットワークアドレスにホストビットを設定しないでください。例： `192.16.0.0/22`。
ゲートウェイIPアドレス（オプション）	StorageGRID へのアクセスに使用するS3 IPアドレスがStorageGRID VIPアドレスと同じサブネットにない場合は、StorageGRID VIPローカルゲートウェイのIPアドレスを入力します。ローカルゲートウェイの IP アドレスは VIP サブネット内にある必要があります。

フィールド	説明
仮想IPアドレス	HAグループ内のアクティブインターフェイスのVIPアドレスを1つ以上10個以下で入力します。すべてのVIPアドレスがVIPサブネット内にある必要があります。 IPv4アドレスを少なくとも1つ指定する必要があります。必要に応じて、追加の IPv4 アドレスと IPv6 アドレスを指定できます。

f. を選択し、[終了]*を選択してS3セットアップウィザードに戻ります。

g. [続行]*を選択して、ロードバランサの手順に進みます。

既存の**HA**グループを使用する

a. 既存のHAグループを使用するには、*[HAグループの選択]*からHAグループ名を選択します。

b. [続行]*を選択して、ロードバランサの手順に進みます。

手順**2/6**：ロードバランサエンドポイントの設定

StorageGRID は、ロードバランサを使用してクライアントアプリケーションからワークロードを管理します。ロードバランシングは、複数のストレージノードにわたって速度と接続容量を最大化します。

すべてのゲートウェイノードと管理ノードに存在するStorageGRID ロードバランササービスを使用することも、外部（サードパーティ）のロードバランサに接続することもできます。StorageGRID ロードバランサを使用することを推奨します。

このタスクの詳細については、を参照してください "ロードバランシングに関する考慮事項"。

StorageGRID ロードバランササービスを使用するには、* StorageGRID load balancer タブを選択し、使用するロードバランサエンドポイントを作成または選択します。外部ロードバランサを使用するには、[外部ロードバランサ]*タブを選択し、設定済みのシステムに関する詳細を入力します。

エンドポイントを作成します

手順

1. ロードバランサエンドポイントを作成するには、*[エンドポイントの作成]*を選択します。
2. Enter endpoint details *ステップで、次のフィールドに値を入力します。

フィールド	説明
名前	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。最初に作成するエンドポイントのデフォルトは10433ですが、未使用の外部ポートを入力できます。80または443を入力すると、ゲートウェイノードでのみエンドポイントが設定されます。これらのポートは管理ノードで予約されているためです。 *注：*他のグリッドサービスで使用されるポートは許可されません。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"。
クライアントタイプ	は* S3 *にする必要があります。
ネットワークプロトコル	[**HTTPS**] を選択します。 注：TLS暗号化なしでのStorageGRID との通信はサポートされていますが、推奨されません。

3. [結合モードの選択]ステップで、結合モードを指定します。バインドモードは、任意のIPアドレスまたは特定のIPアドレスとネットワークインターフェイスを使用してエンドポイントにアクセスする方法を制御します。

モード	説明
グローバル（デフォルト）	クライアントは、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、任意のネットワーク上の任意のHAグループの仮想IP（VIP）アドレス、または対応するFQDNを使用して、エンドポイントにアクセスできます。 このエンドポイントのアクセスを制限する必要がある場合を除き、 * グローバル * 設定（デフォルト）を使用します。
HA グループの仮想 IP	クライアントがこのエンドポイントにアクセスするには、HAグループの仮想IPアドレス（または対応するFQDN）を使用する必要があります。 このバインドモードのエンドポイントでは、エンドポイント用に選択したHAグループが重複しないかぎり、すべて同じポート番号を使用できます。

モード	説明
ノードインターフェイス	クライアントがこのエンドポイントにアクセスするには、選択したノードインターフェイスのIPアドレス（または対応するFQDN）を使用する必要があります。
ノードタイプ	選択したノードのタイプに基づいて、クライアントがこのエンドポイントにアクセスするには、いずれかの管理ノードのIPアドレス（または対応するFQDN）か、いずれかのゲートウェイノードのIPアドレス（または対応するFQDN）を使用する必要があります。

4. [Tenant access]ステップで、次のいずれかを選択します。

フィールド	説明
Allow all tenants（デフォルト）	すべてのテナントアカウントは、このエンドポイントを使用してバケットにアクセスできます。
選択したテナントを許可します	このエンドポイントを使用してバケットにアクセスできるのは、選択したテナントアカウントのみです。
選択したテナントをブロックします	選択したテナントアカウントは、このエンドポイントを使用してバケットにアクセスできません。他のすべてのテナントでこのエンドポイントを使用できます。

5. [証明書の添付]*ステップで、次のいずれかを選択します。

フィールド	説明
証明書のアップロード（推奨）	このオプションは、CA署名済みサーバ証明書、証明書秘密鍵、およびオプションのCAバンドルをアップロードする場合に使用します。
証明書の生成	このオプションは、自己署名証明書を生成する場合に使用します。を参照してください "ロードバランサエンドポイントを設定する" を参照してください。
StorageGRID S3およびSwift証明書を使用する	このオプションは、StorageGRID グローバル証明書のカスタムバージョンをすでにアップロードまたは生成している場合にのみ使用します。を参照してください "S3 および Swift API 証明書を設定する" を参照してください。

6. [Finish]*を選択してS3セットアップウィザードに戻ります。
7. [続行]*を選択してテナントとバケットの手順に進みます。

> エンドポイント証明書の変更がすべてのノードに適用されるまでに最大 15 分かかることがあります。

既存のロードバランサエンドポイントを使用する

手順

1. 既存のエンドポイントを使用する場合は、*[ロードバランサエンドポイントの選択]*からそのエンドポイントの名前を選択します。
2. [続行]*を選択してテナントとバケットの手順に進みます。

外部のロードバランサを使用する

手順

1. 外部のロードバランサを使用するには、次のフィールドに値を入力します。

フィールド	説明
FQDN	外部ロードバランサの完全修飾ドメイン名（FQDN）。
ポート	S3アプリケーションが外部ロードバランサへの接続に使用するポート番号。
証明書	外部ロードバランサのサーバ証明書をコピーして、このフィールドに貼り付けます。

2. [続行]*を選択してテナントとバケットの手順に進みます。

ステップ**3 / 6**：テナントとバケットを作成

テナントは、S3アプリケーションを使用してStorageGRID でオブジェクトの格納と読み出しを行うことができるエンティティです。各テナントには、独自のユーザ、アクセスキー、バケット、オブジェクト、および特定の機能セットがあります。S3アプリケーションがオブジェクトの格納に使用するバケットを作成する前に、テナントを作成する必要があります。

バケットは、テナントのオブジェクトとオブジェクトメタデータを格納するためのコンテナです。一部のテナントには多数のバケットが含まれている場合もありますが、このウィザードを使用すると、テナントとバケットを最も簡単かつ迅速に作成できます。Tenant Managerは、あとで必要なバケットを追加するために使用できます。

このS3アプリケーションで使用する新しいテナントを作成できます。必要に応じて、新しいテナント用のバケットを作成することもできます。最後に、ウィザードでテナントのrootユーザのS3アクセスキーを作成できます。

このタスクの詳細については、を参照してください "テナントアカウントを作成する" および "S3 バケットを作成する"。

手順

1. [テナントの作成] を選択します。
2. [Enter details]ステップで、次の情報を入力します。

フィールド	説明
名前	テナントアカウントの名前。テナント名は一意である必要はありません。作成したテナントアカウントには、一意の数値アカウント ID が割り当てられます。
概要 （オプション）	テナントの特定に役立つ概要 。
クライアントタイプ	このテナントで使用するクライアントプロトコルのタイプ。S3セットアップウィザードでは、* S3 *が選択され、フィールドは無効になっています。
ストレージクォータ（オプション）	このテナントにストレージクォータを設定する場合は、クォータとユニットの数値。

3. 「 * Continue * 」を選択します。
4. 必要に応じて、このテナントに付与する権限を選択します。

これらの権限の一部には追加の要件があります。詳細については、各権限のヘルプアイコンを選択してください。

アクセス権	選択した項目
プラットフォームサービスを許可します	テナントでは、CloudMirrorなどのS3プラットフォームサービスを使用できます。を参照してください "S3 テナントアカウントのプラットフォームサービスを管理します"。
独自のアイデンティティソースを使用する	テナントでは、フェデレーテッドグループおよびフェデレーテッドユーザの独自のアイデンティティソースを設定および管理できます。がある場合、このオプションは無効になります "SSOを設定しました" をStorageGRID クリックします。
S3を許可するを選択します	テナントは、オブジェクトデータのフィルタリングと読み出しを行うためのS3 SelectObjectContent API要求を問題 できます。を参照してください "テナントアカウント用の S3 Select を管理します"。 重要：SelectObjectContent要求を実行すると、すべてのS3クライアントとすべてのテナントのロードバランサのパフォーマンスが低下する可能性があります。この機能は、必要な場合にのみ有効にし、信頼できるテナントに対してのみ有効にします。

アクセス権	選択した項目
グリッドフェデレーション接続を使用する	テナントはグリッドフェデレーション接続を使用できます。 このオプションの選択： • このテナント、およびアカウントに追加されたすべてのテナントグループとユーザが、このグリッド（*source grid*）から、選択した接続（*destination grid*）内の他のグリッドにクローニングされます。 • このテナントで、各グリッド上の対応するバケット間のグリッド間レプリケーションを設定できます。 を参照してください "グリッドフェデレーションに許可されたテナントを管理します"。

5. [Use grid federation connection]*を選択した場合は、使用可能なグリッドフェデレーション接続のいずれかを選択します。
6. StorageGRID システムでが使用されているかどうかに基づいて、テナントアカウントのルートアクセスを定義します "アイデンティティフェデレーション"、 "シングルサインオン（SSO）"またはその両方。

オプション	手順
アイデンティティフェデレーションが有効になっていない場合	ローカルrootユーザとしてテナントにサインインするときに使用するパスワードを指定します。
アイデンティティフェデレーションが有効になっている場合	a. テナントに対するRoot Access権限を割り当てる既存のフェデレーテッドグループを選択します。 b. 必要に応じて、ローカルrootユーザとしてテナントにサインインする際に使用するパスワードを指定します。
アイデンティティフェデレーションとシングルサインオン（SSO）の両方が有効になっている場合	テナントに対するRoot Access権限を割り当てる既存のフェデレーテッドグループを選択します。ローカルユーザはサインインできません。

7. ルートユーザのアクセスキーIDとシークレットアクセスキーをウィザードで作成する場合は、* Create root user S3 access key automatically *を選択します。

> テナントのユーザをrootユーザだけにする場合は、このオプションを選択します。他のユーザがこのテナントを使用する場合は、Tenant Managerを使用してキーと権限を設定します。

8. 「* Continue * 」を選択します。
9. [Create bucket]手順では、必要に応じてテナントのオブジェクト用のバケットを作成します。それ以外の場合は、*[Create tenant without bucket]*を選択してに移動します データステップをダウンロードします。

> グリッドでS3オブジェクトロックが有効になっている場合、この手順で作成したバケットではS3オブジェクトロックが有効になりません。このS3アプリケーションにS3オブジェクトロックバケットを使用する必要がある場合は、*[Create tenant without bucket]*を選択します。次に、Tenant Managerを使用してを実行します "バケットを作成します" 代わりに、

a. S3アプリケーションが使用するバケットの名前を入力します。例： `S3-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。

b. このバケットの*[Region]*を選択します。

   デフォルトのリージョンを使用 (`us-east-1`）今後ILMを使用してバケットのリージョンに基づいてオブジェクトをフィルタリングする予定がないかぎり、

c. このバケットに各オブジェクトの各バージョンを格納する場合は、*[オブジェクトのバージョン管理を有効にする]*を選択します。

d. [Create tenant and bucket]*を選択し、データのダウンロード手順に進みます。

ステップ4/6：データをダウンロードします

ダウンロードデータステップでは、1つまたは2つのファイルをダウンロードして、設定した内容の詳細を保存できます。

手順

1. [Create root user S3 access key automatically]*を選択した場合は、次のいずれかまたは両方を実行します。
   - Download access keys（アクセスキーのダウンロード）*を選択してをダウンロードします `.csv` テナントアカウント名、アクセスキーID、シークレットアクセスキーを含むファイル。
   - コピーアイコン（）をクリックして、アクセスキーIDとシークレットアクセスキーをクリップボードにコピーします。
2. [Download configuration values]*を選択してをダウンロードします `.txt` ロードバランサエンドポイント、テナント、バケット、およびrootユーザの設定を含むファイル。
3. この情報を安全な場所に保存してください。

> 両方のアクセスキーをコピーするまで、このページを閉じないでください。このページを閉じると、キーは使用できなくなります。この情報はStorageGRID システムからデータを取得するために使用できるため、必ず安全な場所に保存してください。

4. プロンプトが表示されたら、チェックボックスをオンにして、キーをダウンロードまたはコピーしたことを確認します。
5. [続行]*を選択してILMルールとポリシーの手順に進みます。

手順5 / 6：S3のILMルールとILMポリシーを確認します

情報ライフサイクル管理（ILM）ルールは、StorageGRID システム内のすべてのオブジェクトの配置、期間、取り込み動作を制御します。StorageGRID に含まれているILMポリシーは、すべてのオブジェクトのレプリケートコピーを2つ作成します。このポリシーは、新しいポリシーを少なくとも1つアクティブ化するまで有効

です。

手順

1. ページに表示された情報を確認します。
2. 新しいテナントまたはバケットに属するオブジェクトに対する具体的な手順を追加する場合は、新しいルールと新しいポリシーを作成します。を参照してください "ILM ルールを作成する" および "ILMポリシー：概要"。
3. [I have review these steps and understand what I need to do]*を選択します。
4. チェックボックスをオンにして、次に何をすべきかを理解していることを示します。
5. を選択して[概要]*に進みます。

ステップ**6 / 6**：概要を確認します

手順

1. 概要を確認します。
2. 次の手順の詳細をメモしておいてください。S3クライアントに接続する前に必要になる可能性がある追加の設定について説明しています。たとえば、*[Sign in as root]*を選択するとTenant Managerに移動し、テナントユーザの追加、バケットの作成、バケットの設定の更新を行うことができます。
3. [完了] を選択します。
4. StorageGRID からダウンロードしたファイルまたは手動で取得した値を使用して、アプリケーションを設定します。