



ハードウェアをセットアップする

StorageGRID 11.7

NetApp
April 12, 2024

目次

ハードウェアをセットアップする	1
ハードウェアのセットアップ：概要	1
StorageGRID 接続を設定します	2
BMCインターフェイスの設定（SGF6112、SG6000、SG100、SG1000）	39
オプション：ノード暗号化を有効にします	47
オプション：RAIDモードを変更します	50
オプション：アプライアンスのネットワークポートの再マッピング	52

ハードウェアをセットアップする

ハードウェアのセットアップ：概要

アプライアンスの電源を入れたら、StorageGRID で使用するネットワーク接続を設定します。

必要なネットワーク接続を設定します

すべてのアプライアンスで、次のようないくつかのタスクを実行して、必要なネットワーク接続を設定します。

- アプライアンスインストーラにアクセスします
- ネットワークリンクを設定する
- ポートレベルのネットワーク接続を確認

追加の設定が必要になる場合があります

設定するアプライアンスのタイプによっては、ハードウェアの追加設定が必要になる場合があります。

SANtricity システムマネージャ

SG6000およびSG5700の場合は、SANtricity System Managerを設定します。SANtricity ソフトウェアを使用して、これらのアプライアンスのハードウェアを監視します。

BMC インターフェイス

次のアプライアンスには、BMCインターフェイスを設定する必要があります。

- SGF6112を参照してください
- SG6000を使用します
- SG1000 からのアクセス
- SG100

オプションの設定

- ストレージアプライアンス
 - ハードウェアの監視に使用するSANtricity System Manager（SG6000およびSG5700）を設定します
 - RAIDモードを変更します
- サービスアプライアンス
 - SG100、SG1000、およびSG6000-CNコントローラのBMCインターフェイスにアクセスします

StorageGRID 接続を設定します

StorageGRID アプライアンスインストーラにアクセスします

インストーラのバージョンを確認し、アプライアンスと 3 つの StorageGRID ネットワーク（グリッドネットワーク、管理ネットワーク（オプション）、クライアントネットワーク（オプション））の間の接続を設定するには、StorageGRID アプライアンスインストーラにアクセスする必要があります。

作業を開始する前に

- StorageGRID 管理ネットワークに接続できる管理クライアントを使用しているか、サービスラップトップを使用している必要があります。
- クライアントまたはサービスラップトップに搭載されている "サポートされている Web ブラウザ"。
- 使用するすべての StorageGRID ネットワークにサービスアプライアンスまたはストレージアプライアンスコントローラを接続しておきます。
- これらのネットワークでのサービスアプライアンスまたはストレージアプライアンスコントローラの IP アドレス、ゲートウェイ、およびサブネットを確認しておきます。
- 使用するネットワークスイッチを設定しておきます。

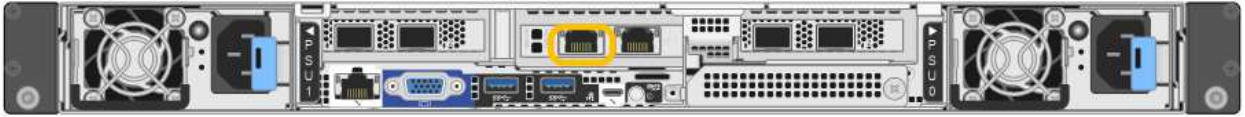
このタスクについて

StorageGRID アプライアンスインストーラに最初にアクセスするときは、DHCPによってサービスアプライアンスまたはストレージアプライアンスコントローラの管理ネットワークポートに割り当てられた IP アドレスを使用できます（管理ネットワークに接続されている場合）。または、サービスラップトップをサービスアプライアンスまたはストレージアプライアンスコントローラに直接接続することもできます。

手順

1. 可能であれば、サービスアプライアンスまたはストレージアプライアンスコントローラの管理ネットワークポートの DHCP アドレスを使用します。次の図では、管理ネットワークポートが強調表示されています。（管理ネットワークが接続されていない場合は、グリッドネットワークの IP アドレスを使用します）。

SGF6112を参照してください



SG6000-CN の情報



E5700SG

E5700SGでは、次のいずれかを実行できます。

- E5700SG コントローラのデジタル表示ディスプレイを参照してください。E5700SG コントローラの管理ポート 1 および 10 / 25GbE ポート 2 と 4 を DHCP サーバがあるネットワークに接続している場合は、エンクロージャの電源投入時に動的に割り当てられた IP アドレスの取得が試行されます。コントローラの電源投入プロセスが完了すると、デジタル表示ディスプレイに * HO * と表示され、続いて 2 つの数字が順番に表示されます。

```
HO -- IP address for Admin Network -- IP address for Grid Network  
HO
```

次の順序で実行します。

- 最初に表示される数字は、管理ネットワークに接続されているアプライアンスストレージノードの DHCP アドレスです。この IP アドレスは、E5700SG コントローラの管理ポート 1 に割り当てられています。
- 2 番目に表示される数字は、グリッドネットワーク上のアプライアンスストレージノードの DHCP アドレスです。この IP アドレスは、アプライアンスに最初に電源を投入するときに、10 / 25GbE ポート 2 と 4 に割り当てられます。



DHCP を使用して IP アドレスを割り当てるができなかった場合は、0.0.0.0 と表示されます。

SG100



SG1000 からのアクセス



- a. サービスアプライアンスまたはストレージアプライアンスの前面にあるMACアドレスラベルを確認

し、管理ネットワークポートのMACアドレスを特定します。

MAC アドレスラベルには、BMC 管理ポートの MAC アドレスが記載されています。

管理ネットワークポートのMACアドレスを確認するには、ラベルの16進数に*2を追加します。たとえば、ラベルに記載されている **MAC** アドレスの末尾が *09* の場合、管理ポートの **MAC** アドレスの末尾は *0B* となります。ラベルに記載された **MAC** アドレスの末尾が * (y) FF の場合、管理ポートの MAC アドレスの末尾は * (y+1) 01 * となります。この計算を簡単に行うには、Windows で Calculator を開き、Programmer モードに設定して Hex を選択し、MAC アドレスを入力してから、+2= と入力します。

b. MAC アドレスをネットワーク管理者に伝え、管理者が管理ネットワークでのアプライアンスの DHCP アドレスを確認できるようにします。

c. クライアントから、StorageGRID アプライアンスインストーラのURLとして「+」を入力します

https://Appliance_IP:8443

の場合 `Appliance_IP` で、DHCPアドレスを使用します（管理ネットワークがある場合は、そのIPアドレスを使用します）。

d. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書を表示およびインストールします。

次回この URL にアクセスしたときに、アラートは表示されません。

StorageGRID アプライアンスインストーラのホームページが表示されます。このページに最初にアクセスしたときに表示される情報とメッセージは、アプライアンスと StorageGRID ネットワークの現在の接続状況によって異なります。エラーメッセージが表示された場合は、以降の手順で解決されます。

[Home](#)
[Configure Networking ▾](#)
[Configure Hardware ▾](#)
[Monitor Installation](#)
[Advanced ▾](#)

Home

i The installation is ready to be started. Review the settings below, and then click Start Installation.

This Node

Node type

Storage

Node name

MM-2-108-SGA-lab25

Cancel

Save

Primary Admin Node connection

Enable Admin Node discovery

Primary Admin Node IP

172.16.1.178

Connection state

Connection to 172.16.1.178 ready

Cancel

Save

Installation

Current state

Ready to start installation of MM-2-108-SGA-lab25 into grid with Admin Node 172.16.1.178 running StorageGRID 11.2.0, using StorageGRID software downloaded from the Admin Node.

Start Installation

- DHCPを使用してIPアドレスを取得できない場合は、リンクローカル接続を使用できます。

SGF6112を参照してください

イーサネットケーブルを使用して、サービスラップトップをアプライアンスの右端のRJ-45ポートに直接接続します。



SG6000-CN の情報

イーサネットケーブルを使用して、サービスラップトップを SG6000-CN コントローラの右端の RJ-45 ポートに直接接続します。



E5700SG

イーサネットケーブルを使用して、E5700SG コントローラの管理ポート 2 にサービスラップトップを接続してください。



SG100

イーサネットケーブルを使用して、サービスラップトップをサービスアプライアンスの右端の RJ-45 ポートに直接接続します。



SG1000 からのアクセス

イーサネットケーブルを使用して、サービスラップトップをサービスアプライアンスの右端の RJ-45 ポートに直接接続します。



- サービスラップトップで Web ブラウザを開きます。
- StorageGRID アプライアンスインストーラの URL に + を入力します **https://169.254.0.1:8443**

StorageGRID アプライアンスインストーラのホームページが表示されます。このページに最初にアクセスしたときに表示される情報とメッセージは、アプライアンスと StorageGRID ネットワークの現在の接続状況によって異なります。エラーメッセージが表示された場合は、以降の手順で解決されま

す。



リンクローカル接続でホームページにアクセスできない場合は、サービスラップトップのIPアドレスをに設定します `169.254.0.2` をクリックして、もう一度やり直してください。

完了後

StorageGRID アプライアンスインストーラにアクセスしたあとに、次の手順を実行

- アプライアンスの StorageGRID アプライアンスインストーラのバージョンが StorageGRID システムにインストールされているソフトウェアのバージョンと一致していることを確認します。必要に応じて、StorageGRID アプライアンスインストーラをアップグレードします。

"StorageGRID アプライアンスインストーラのバージョンを確認してアップグレードします"

- StorageGRID アプライアンスインストーラのホームページに表示されるメッセージを確認し、必要に応じてリンク設定と IP 設定を行います。

NetApp® StorageGRID® Appliance Installer

Home | Configure Networking | Configure Hardware | Monitor Installation | Advanced

Home

This Node

Node type: Gateway

Node name: xlr8r-10

Cancel Save

Primary Admin Node connection

Enable Admin Node discovery:

Primary Admin Node IP: 192.168.7.44

Connection state: Connection to 192.168.7.44 ready

Cancel Save

Installation

Current state: Ready to start installation of xlr8r-10 into grid with Admin Node 192.168.7.44 running StorageGRID 11.6.0, using StorageGRID software downloaded from the Admin Node.

Start installation

StorageGRID アプライアンスインストーラのバージョンを確認してアップグレードします

StorageGRID のすべての機能がサポートされるようにするには、アプライアンスの StorageGRID アプライアンスインストーラのバージョンと StorageGRID システムにインストールされているソフトウェアのバージョンが一致している必要があります。

作業を開始する前に

StorageGRID アプライアンスインストーラにアクセスしておきます。

このタスクについて

StorageGRID アプライアンスは、StorageGRID アプライアンスインストーラがプリインストールされた状態で出荷されます。最近アップグレードした StorageGRID システムにアプライアンスを追加する場合は、そのアプライアンスを新しいノードとしてインストールする前に、StorageGRID アプライアンスインストーラの手動アップグレードが必要になることがあります。

新しい StorageGRID バージョンにアップグレードすると、StorageGRID アプライアンスインストーラが自動的にアップグレードされます。インストールされているアプライアンスノードで StorageGRID アプライアンスインストーラをアップグレードする必要はありません。この手順が必要になるのは、以前のバージョンの StorageGRID アプライアンスインストーラを搭載したアプライアンスをインストールする場合のみです。

手順

1. StorageGRID アプライアンス・インストーラから、* アドバンスト * > * アップグレード・ファームウェア * を選択します。
2. 現在のファームウェアバージョンと StorageGRID システムにインストールされているソフトウェアバージョンを比較します。（Grid Manager の上部からヘルプアイコンを選択し、* バージョン情報 * を選択します）。

2つのバージョンの2桁目の数字が一致している必要があります。たとえば、StorageGRID システムでバージョン 11.* 6 *。x.y_y__ を実行している場合、StorageGRID アプライアンスインストーラのバージョンは 3.* 6 * .z である必要があります。

3. アプライアンスの StorageGRID アプライアンスインストーラの下位バージョンがある場合は、に進みます ["ネットアップのダウンロード：StorageGRID アプライアンス"](#)。

ネットアップアカウントのユーザ名とパスワードを使用してサインインします。

4. StorageGRID アプライアンス * 対応するバージョンのサポート・ファイルと対応するチェックサム・ファイルをダウンロードします。

StorageGRID アプライアンスのサポート・ファイルは、.zip すべての StorageGRID アプライアンス・モデルの最新および以前のファームウェア・バージョンを含むアーカイブ。

StorageGRID アプライアンスのサポートファイルをダウンロードしたら、を展開します。 .zip StorageGRID アプライアンスインストーラのインストールに関する重要な情報については、README ファイルをアーカイブして参照してください。

5. StorageGRID アプライアンスインストーラの [Upgrade Firmware] ページに表示される手順に従って、次の手順を実行します。
 - a. コントローラのタイプに応じたサポートファイル（ファームウェアイメージ）をアップロードします。一部のファームウェアバージョンでは、チェックサムファイルのアップロードも必要です。チェ

ックサム・ファイルの入力を求められた場合は、StorageGRID アプライアンスのサポート・ファイルにも記載されています。

- b. 非アクティブなパーティションをアップグレードします。
- c. パーティションを再起動してスワップします。
- d. コントローラタイプに応じた適切なサポートファイル（ファームウェアイメージ）を再度アップロードします。一部のファームウェアバージョンでは、チェックサムファイルのアップロードも必要です。チェックサム・ファイルの入力を求められた場合は、StorageGRID アプライアンスのサポート・ファイルにも記載されています。
- e. 2つ目の（非アクティブな）パーティションをアップグレードします。

関連情報

["StorageGRID アプライアンスインストーラへのアクセス"](#)

ネットワークリンクを設定する

アプライアンスをグリッドネットワーク、クライアントネットワーク、および管理ネットワークに接続するために使用するポートのネットワークリンクを設定できます。リンク速度およびポートボンディングモードとネットワークボンディングモードを設定できます。



ConfigBuilderを使用してJSONファイルを生成する場合は、ネットワークリンクを自動的に設定できます。を参照してください ["アプライアンスのインストールと設定を自動化"](#)。

作業を開始する前に

- これで完了です ["追加機器を入手した"](#) ケーブルの種類とリンク速度に応じて必要です。
- 使用するリンク速度に基づいて、正しいトランシーバをポートに取り付けておきます。
- 選択した速度をサポートするスイッチにネットワークポートを接続しておきます。

アグリゲートポートボンディングモード、LACP ネットワークボンディングモード、または VLAN タギングを使用する場合

- アプライアンスのネットワークポートを、VLAN と LACP をサポートするスイッチに接続しておきます。
- 複数のスイッチを LACP ボンドに加える場合は、Multi-Chassis Link Aggregation（MLAG）グループまたは同等の機能をサポートするスイッチを使用します。
- VLAN、LACP、MLAG などを使用するようにスイッチを設定する方法について理解しておく必要があります。
- 各ネットワークに使用する一意の VLAN タグを確認しておきます。この VLAN タグが各ネットワークパケットに追加され、ネットワークトラフィックが正しいネットワークにルーティングされます。

このタスクについて

デフォルト以外の設定を使用する場合にのみ、Link Configuration ページで設定を行う必要があります。



LACP送信ハッシュポリシーはlayer2+3です。

次の図と表に、各アプライアンスのポートボンディングモードとネットワークボンディングモードのオプション

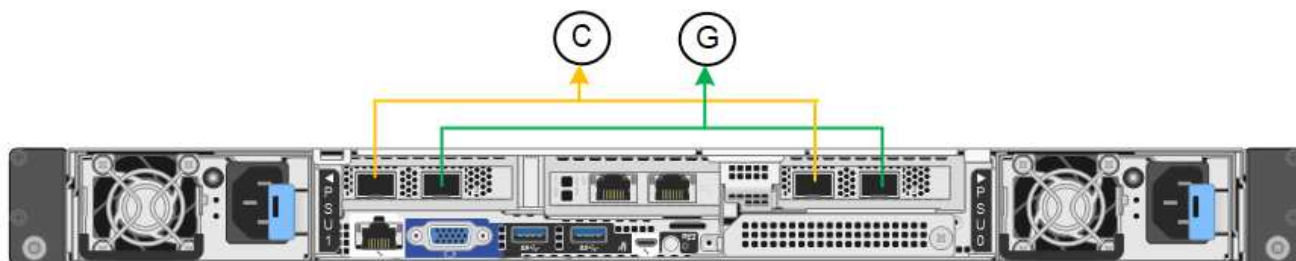
ンをまとめます。詳細については、次を参照してください。

- "ポートボンディングモード (SGF6112) "
- "ポートボンディングモード (SG6000-CN) "
- "ポートボンディングモード (E5700SG) "
- "ポートボンディングモード (SG1000およびSG100) "

SGF6112を参照してください

Fixedポートボンディングモード（デフォルト）

次の図では、4つのネットワークポートがFixedポートボンディングモードでボンディングされています（デフォルトの構成）。



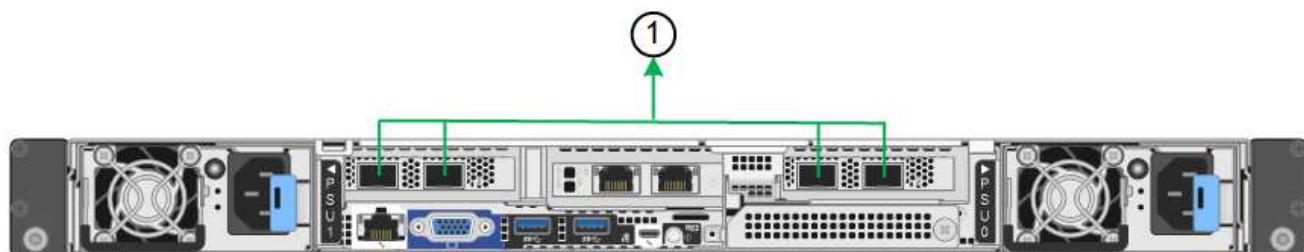
コールアウト	ボンディングされるポート
C	このネットワークを使用する場合、ポート 1 とポート 3 がクライアントネットワーク用にボンディングされます。
G	ポート 2 とポート 4 がグリッドネットワーク用にボンディングされます。

次の表は、ネットワークポートを設定するためのオプションをまとめたものです。デフォルト以外の設定を使用する場合にのみ、Link Configuration ページで設定を行う必要があります。

ネットワークボンディングモード	クライアントネットワークが無効な場合（デフォルト）	クライアントネットワークが有効になりました
Active-Backup（デフォルト）	<ul style="list-style-type: none">ポート 2 と 4 がグリッドネットワークにアクティブ / バックアップボンドを使用します。ポート 1 と 3 は使用されません。VLAN タグはオプションです。	<ul style="list-style-type: none">ポート 2 と 4 がグリッドネットワークにアクティブ / バックアップボンドを使用します。ポート 1 と 3 がクライアントネットワークに Active-Backup ボンドを使用します。ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。
LACP（802.3ad）	<ul style="list-style-type: none">ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。ポート 1 と 3 は使用されません。VLAN タグはオプションです。	<ul style="list-style-type: none">ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。ポート 1 と 3 がクライアントネットワークに LACP ボンドを使用します。ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。

Aggregate ポートボンディングモード

次の図では、4つのネットワークポートがアグリゲートポートボンディングモードでボンディングされています。



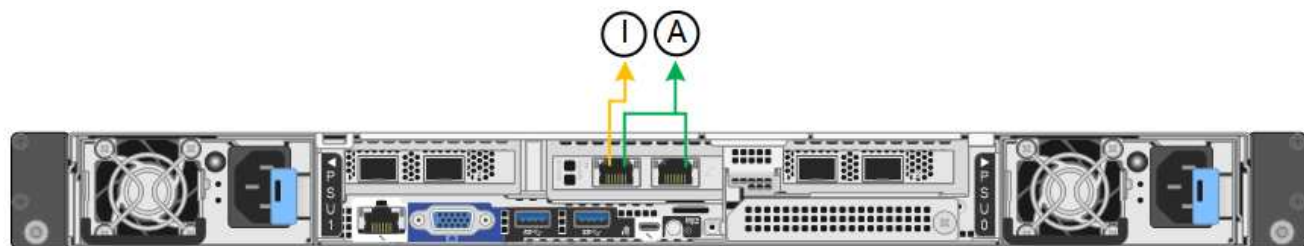
コールアウト	ボンディングされるポート
1.	4つのポートすべてを1つのLACPボンドにグループ化して、すべてのポートをグリッドネットワークとクライアントネットワークのトラフィックに使用できるようにします。

次の表は、ネットワークポートを設定するためのオプションをまとめたものです。デフォルト以外の設定を使用する場合にのみ、Link Configuration ページで設定を行う必要があります。

ネットワークボンディングモード	クライアントネットワークが無効な場合 (デフォルト)	クライアントネットワークが有効になりました
LACP (802.3ad) のみ	<ul style="list-style-type: none">ポート 1~4 がグリッドネットワークに単一の LACP ボンドを使用します。単一の VLAN タグでグリッドネットワークの packets が識別されます。	<ul style="list-style-type: none">ポート 1~4 がグリッドネットワークとクライアントネットワークに単一の LACP ボンドを使用します。2つの VLAN タグで、グリッドネットワークの packets とクライアントネットワークの packets を分離できます。

管理ポート用のActive-Backupネットワークボンディングモード

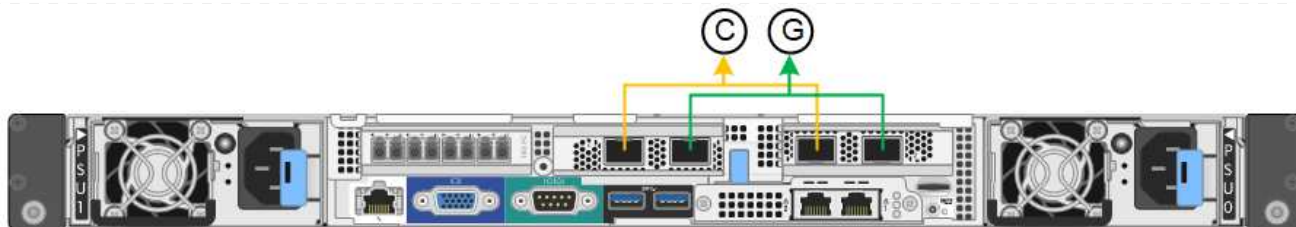
次の図では、SGF6112の2つの1GbE管理ポートが管理ネットワーク用にActive-Backupネットワークボンディングモードでボンディングされています。



SG6000を使用します

Fixedポートボンディングモード (デフォルト)

次の図では、4つのネットワークポートがFixedポートボンディングモードでボンディングされています (デフォルトの構成)。



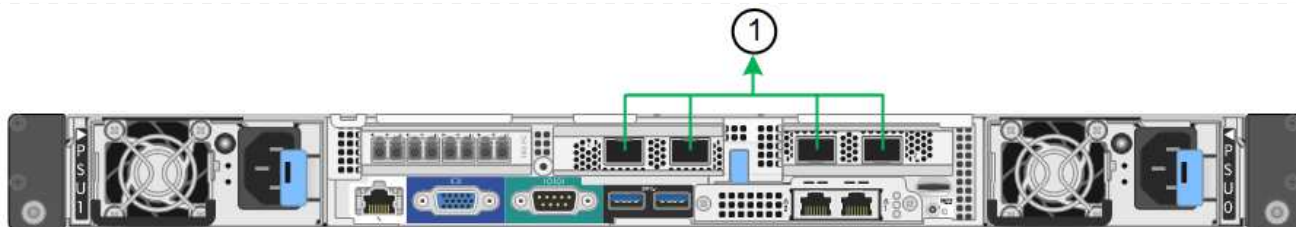
コールアウト	ボンディングされるポート
C	このネットワークを使用する場合、ポート 1 とポート 3 がクライアントネットワーク用にボンディングされます。
G	ポート 2 とポート 4 がグリッドネットワーク用にボンディングされます。

次の表は、ネットワークポートを設定するためのオプションをまとめたものです。デフォルト以外の設定を使用する場合にのみ、Link Configuration ページで設定を行う必要があります。

ネットワークボンディングモード	クライアントネットワークが無効な場合（デフォルト）	クライアントネットワークが有効になりました
Active-Backup（デフォルト）	<ul style="list-style-type: none"> ポート 2 と 4 がグリッドネットワークにアクティブ/バックアップボンドを使用します。 ポート 1 と 3 は使用されません。 VLAN タグはオプションです。 	<ul style="list-style-type: none"> ポート 2 と 4 がグリッドネットワークにアクティブ/バックアップボンドを使用します。 ポート 1 と 3 がクライアントネットワークに Active-Backup ボンドを使用します。 ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。
LACP（802.3ad）	<ul style="list-style-type: none"> ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。 ポート 1 と 3 は使用されません。 VLAN タグはオプションです。 	<ul style="list-style-type: none"> ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。 ポート 1 と 3 がクライアントネットワークに LACP ボンドを使用します。 ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。

Aggregate ポートボンディングモード

次の図では、4つのネットワークポートが Aggregate ポートボンディングモードでボンディングされています。



コールアウト	ボンディングされるポート
1.	4つのポートすべてを1つのLACPボンディングにグループ化して、すべてのポートをグリッドネットワークとクライアントネットワークのトラフィックに使用できるようにします。

次の表は、ネットワークポートを設定するためのオプションをまとめたものです。デフォルト以外の設定を使用する場合にのみ、Link Configuration ページで設定を行う必要があります。

ネットワークボンディングモード	クライアントネットワークが無効な場合（デフォルト）	クライアントネットワークが有効になりました
LACP（802.3ad）のみ	<ul style="list-style-type: none"> ポート 1~4 がグリッドネットワークに単一の LACP ボンディングを使用します。 単一の VLAN タグでグリッドネットワークの packets が識別されます。 	<ul style="list-style-type: none"> ポート 1~4 がグリッドネットワークとクライアントネットワークに単一の LACP ボンディングを使用します。 2つの VLAN タグで、グリッドネットワークの packets とクライアントネットワークの packets を分離できます。

管理ポート用の**Active-Backup**ネットワークボンディングモード

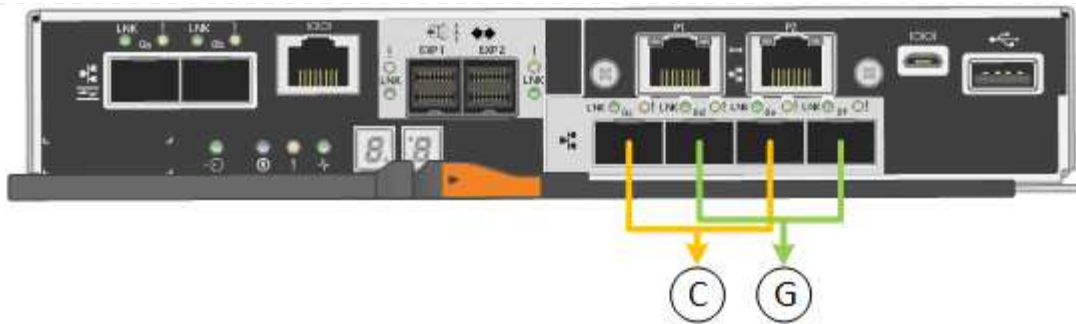
次の図では、SG6000-CN コントローラの 2つの 1GbE 管理ポートが管理ネットワーク用に Active-Backup ネットワークボンディングモードでボンディングされています。



SG5700を使用します

Fixedポートボンディングモード（デフォルト）

次の図では、4つの 10 / 25GbE ポートが Fixed ポートボンディングモードでボンディングされています（デフォルトの構成）。



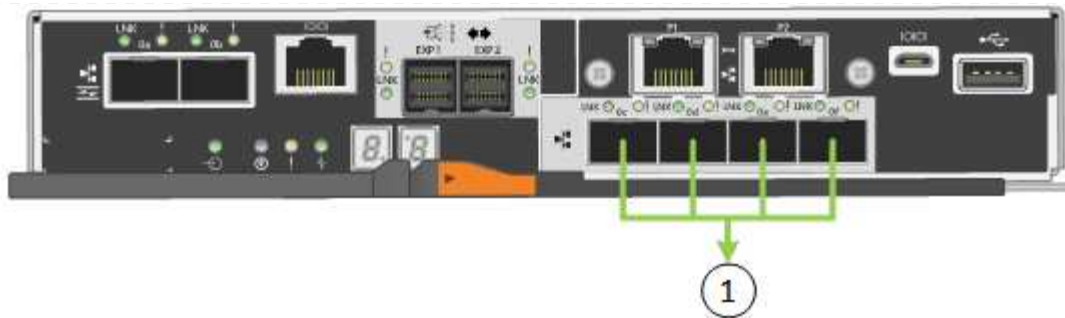
コールアウト	ボンディングされるポート
C	このネットワークを使用する場合、ポート 1 とポート 3 がクライアントネットワーク用にボンディングされます。
G	ポート 2 とポート 4 がグリッドネットワーク用にボンディングされます。

次の表に、4 つの 10 / 25GbE ポートを設定するためのオプションをまとめます。デフォルト以外の設定を使用する場合にのみ、Link Configuration ページで設定を行う必要があります。

ネットワークボンディングモード	クライアントネットワークが無効な場合 (デフォルト)	クライアントネットワークが有効になりました
Active-Backup (デフォルト)	<ul style="list-style-type: none"> ポート 2 と 4 がグリッドネットワークにアクティブ / バックアップボンドを使用します。 ポート 1 と 3 は使用されません。 VLAN タグはオプションです。 	<ul style="list-style-type: none"> ポート 2 と 4 がグリッドネットワークにアクティブ / バックアップボンドを使用します。 ポート 1 と 3 がクライアントネットワークに Active-Backup ボンドを使用します。 ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。
LACP (802.3ad)	<ul style="list-style-type: none"> ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。 ポート 1 と 3 は使用されません。 VLAN タグはオプションです。 	<ul style="list-style-type: none"> ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。 ポート 1 と 3 がクライアントネットワークに LACP ボンドを使用します。 ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。

Aggregate ポートボンディングモード

次の図では、4 つの 10 / 25GbE ポートがアグリゲートポートボンディングモードでボンディングされています。



コールアウト	ボンディングされるポート
1.	4つのポートすべてを1つのLACPボンドにグループ化して、すべてのポートをグリッドネットワークとクライアントネットワークのトラフィックに使用できるようにします。

次の表に、4つの10/25GbEポートを設定するためのオプションをまとめます。デフォルト以外の設定を使用する場合にのみ、Link Configuration ページで設定を行う必要があります。

ネットワークボンディングモード	クライアントネットワークが無効な場合 (デフォルト)	クライアントネットワークが有効になりました
LACP (802.3ad) のみ	<ul style="list-style-type: none"> ポート 1~4 がグリッドネットワークに単一のLACPボンドを使用します。 単一のVLANタグでグリッドネットワークのパケットが識別されます。 	<ul style="list-style-type: none"> ポート 1~4 がグリッドネットワークとクライアントネットワークに単一のLACPボンドを使用します。 2つのVLANタグで、グリッドネットワークのパケットとクライアントネットワークのパケットを分離できます。

管理ポート用のActive-Backupネットワークボンディングモード

この図では、E5700SGコントローラの2つの1GbE管理ポートが管理ネットワーク用にActive-Backupネットワークボンディングモードでボンディングされています。

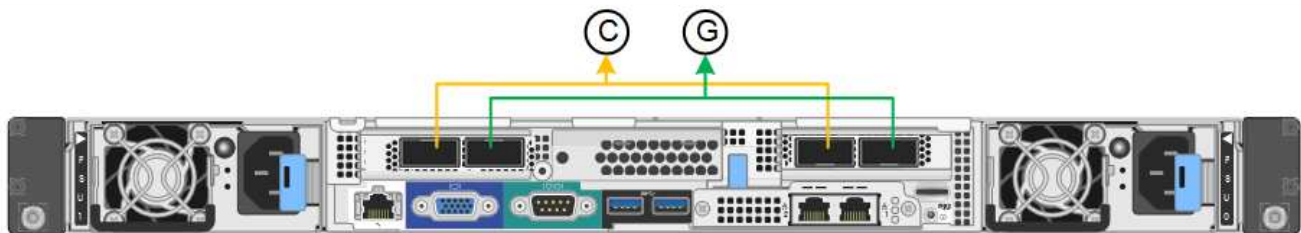


SG100およびSG1000

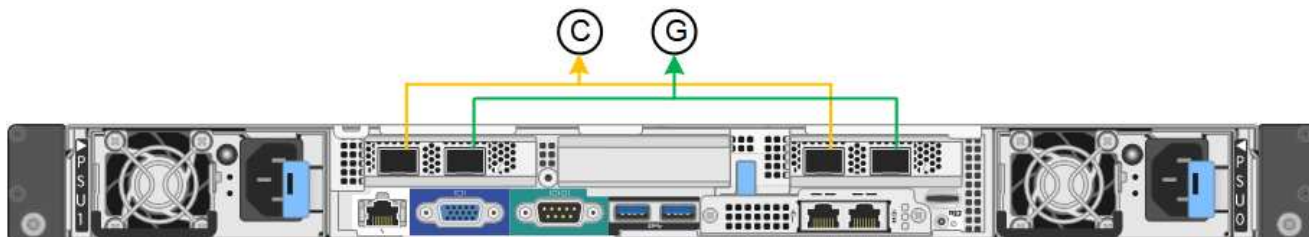
Fixedポートボンディングモード (デフォルト)

次の図では、SG1000またはSG100の4つのネットワークポートがFixedポートボンディングモードでボンディングされています (デフォルトの構成)。

SG1000 :



SG100 :



コールアウト	ボンディングされるポート
C	このネットワークを使用する場合、ポート 1 とポート 3 がクライアントネットワーク用にボンディングされます。
G	ポート 2 とポート 4 がグリッドネットワーク用にボンディングされます。

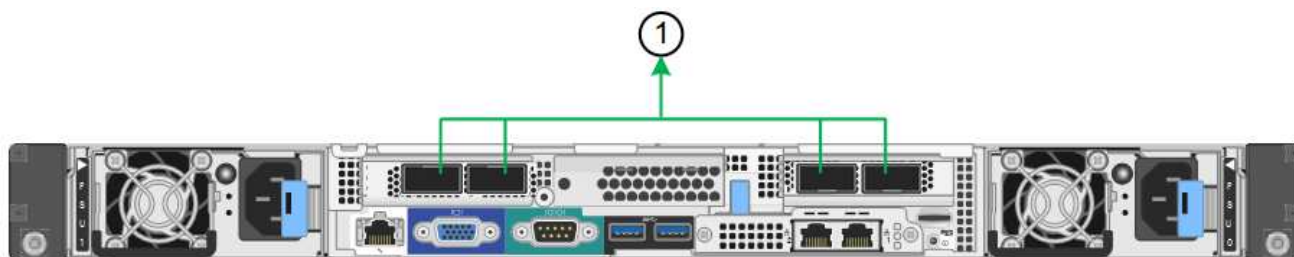
次の表に、4つのネットワークポートを設定するためのオプションをまとめます。デフォルト以外の設定を使用する場合にのみ、Link Configuration ページで設定を行う必要があります。

ネットワークボンディングモード	クライアントネットワークが無効な場合 (デフォルト)	クライアントネットワークが有効になりました
Active-Backup (デフォルト)	<ul style="list-style-type: none"> ポート 2 と 4 がグリッドネットワークにアクティブ/バックアップボンドを使用します。 ポート 1 と 3 は使用されません。 VLAN タグはオプションです。 	<ul style="list-style-type: none"> ポート 2 と 4 がグリッドネットワークにアクティブ/バックアップボンドを使用します。 ポート 1 と 3 がクライアントネットワークに Active-Backup ボンドを使用します。 ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。
LACP (802.3ad)	<ul style="list-style-type: none"> ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。 ポート 1 と 3 は使用されません。 VLAN タグはオプションです。 	<ul style="list-style-type: none"> ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。 ポート 1 と 3 がクライアントネットワークに LACP ボンドを使用します。 ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。

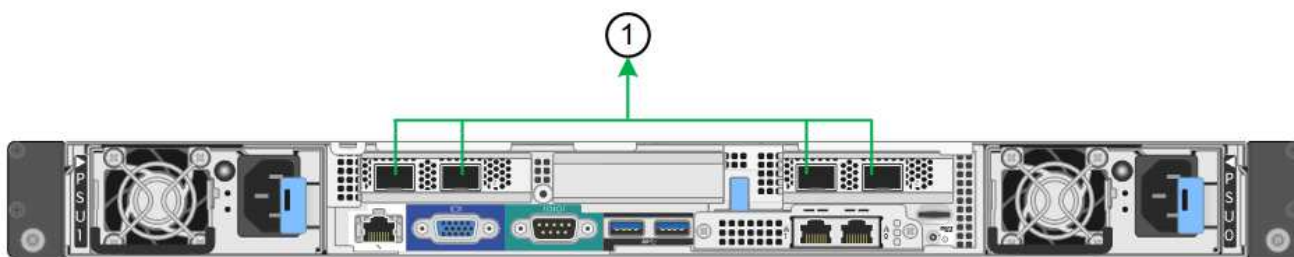
Aggregate ポートボンディングモード

次の図では、4つのネットワークポートがアグリゲートポートボンディングモードでボンディングされています。

SG1000 :



SG100 :



コールアウト	ボンディングされるポート
1.	4つのポートすべてを1つのLACPボンディングにグループ化して、すべてのポートをグリッドネットワークとクライアントネットワークのトラフィックに使用できるようにします。

次の表に、4つのネットワークポートを設定するためのオプションをまとめます。デフォルト以外の設定を使用する場合にのみ、Link Configuration ページで設定を行う必要があります。

ネットワークボンディングモード	クライアントネットワークが無効な場合 (デフォルト)	クライアントネットワークが有効になりました
LACP (802.3ad) のみ	<ul style="list-style-type: none"> ポート 1~4 がグリッドネットワークに単一のLACP ボンドを使用します。 単一のVLAN タグでグリッドネットワークのパケットが識別されます。 	<ul style="list-style-type: none"> ポート 1~4 がグリッドネットワークとクライアントネットワークに単一のLACP ボンドを使用します。 2つのVLAN タグで、グリッドネットワークのパケットとクライアントネットワークのパケットを分離できます。

管理ポート用のActive-Backupネットワークボンディングモード

次の図では、アプライアンスの2つの1GbE管理ポートが管理ネットワーク用にActive-Backupネットワークボンディングモードでボンディングされています。

SG1000 :



SG100 :



手順

1. StorageGRID アプライアンスインストーラのメニューバーから、*Configure Networking*>*Link Configuration* をクリックします。

Network Link Configuration ページには、アプライアンスの図と、ネットワークポートおよび管理ポートの番号が表示されます。

Link Statusテーブルには、番号付きポートのリンク状態、リンク速度、およびその他の統計情報が表示されます。

このページに初めてアクセスしたときの動作は次のとおりです。

- *リンク速度* は *自動* に設定されています。
 - *ポートボンディングモード* は「*Fixed」に設定されます。
 - *グリッドネットワークの場合、ネットワークボンディングモード* が「アクティブ/バックアップ」に設定されます。
 - *管理ネットワーク* が有効になっており、ネットワークボンディングモードが *Independent* に設定されています。
 - *クライアントネットワーク* が無効になっています。
2. [*Link speed* (リンク速度*)] ドロップダウンリストから、ネットワークポートのリンク速度を選択します。

グリッドネットワークとクライアントネットワークに使用するネットワークスイッチも、この速度をサポートし、この速度に対応するように設定する必要があります。設定されたリンク速度に適したアダプタまたはトランシーバを使用する必要があります。このオプションはリンク速度と前方誤り訂正 (FEC) モードの両方をリンクパートナーとネゴシエートするため、可能な場合は自動リンク速度を使用します。

SG6000またはSG5700ネットワークポートに25GbEのリンク速度を使用する場合は、次の手順を実行します。

- SFP28トランシーバとSFP28 Twinaxケーブルまたは光ケーブルを使用します。
- SG6000の場合、[リンク速度]ドロップダウンリストから*[自動]*を選択します。

◦ SG5700の場合は、ドロップダウンリストから 25GbE *を選択します。

3. 使用する StorageGRID ネットワークを有効または無効にします。

グリッドネットワークは必須です。このネットワークを無効にすることはできません。

- a. アプライアンスが管理ネットワークに接続されていない場合は、管理ネットワークの*[ネットワークを有効にする]*チェックボックスをオフにします。
- b. アプライアンスがクライアントネットワークに接続されている場合は、クライアントネットワークの*[ネットワークを有効にする]*チェックボックスを選択します。

これで、データ NIC ポートでのクライアントネットワークの設定が表示されます。

4. 表を参照して、ポートボンディングモードとネットワークボンディングモードを設定します。

次の例では、次のよう

- * グリッドネットワークとクライアントネットワークでアグリゲート * と * LACP * を選択。各ネットワークに一意の VLAN タグを指定する必要があります。値は 0~4095 の間で選択できます。
- * 管理ネットワーク用に選択されたアクティブ / バックアップ *。

Link Settings

Link speed

Port bond mode Fixed Aggregate

Choose Fixed port bond mode if you want to use ports 2 and 4 for the Grid Network and ports 1 and 3 for the Client Network (if enabled). Choose Aggregate port bond mode if you want all connected ports to share a single LACP bond for both the Grid and Client Networks.

Grid Network

Enable network

Network bond mode Active-Backup LACP (802.3ad)

If the port bond mode is Aggregate, all bonds must be in LACP (802.3ad) mode.

Enable VLAN (802.1q) tagging

VLAN (802.1q) tag

MAC Addresses 50:6b:4b:42:d7:00 50:6b:4b:42:d7:01 50:6b:4b:42:d7:24 50:6b:4b:42:d7:25

If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

Admin Network

Enable network

Network bond mode Independent Active-Backup

Connect the Admin Network to ports 5 and 6. If necessary, you can make a temporary direct Ethernet connection by disconnecting ports 5 and 6, then connecting to port 6 and using link-local IP address 169.254.0.1 for access.

MAC Addresses d8:c4:97:2a:e4:95

If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

Client Network

Enable network

Network bond mode Active-Backup LACP (802.3ad)

If the port bond mode is Aggregate, all bonds must be in LACP (802.3ad) mode.

Enable VLAN (802.1q) tagging

VLAN (802.1q) tag

MAC Addresses 50:6b:4b:42:d7:00 50:6b:4b:42:d7:01 50:6b:4b:42:d7:24 50:6b:4b:42:d7:25

If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

5. 選択に問題がなければ、* 保存 * をクリックします。



接続しているネットワークまたはリンクを変更すると、接続が失われる可能性があります。1分以内に再接続されない場合は、アプライアンスに割り当てられている他のIPアドレスのいずれかを使用してStorageGRID アプライアンスインストーラのURLを再入力します
: + https://appliance_IP:8443

StorageGRID IP アドレスを設定する

StorageGRID アプライアンスインストーラを使用して、StorageGRID のグリッドネットワーク、管理ネットワーク、クライアントネットワークでサービスアプライアンスまたはアプライアンスストレージノードに使用されるIPアドレスとルーティング情報を設定します。

ConfigBuilderを使用してJSONファイルを生成する場合は、IPアドレスを自動的に設定できます。を参照してください ["アプライアンスのインストールと設定を自動化"](#)。

このタスクについて

接続された各ネットワークでアプライアンスの静的 IP を割り当てるか、DHCP サーバでアドレスの永久リースを割り当てる必要があります。

リンク設定を変更するには、次の手順を参照してください。

- ["SGF6112アプライアンスのリンク設定を変更します"](#)
- ["SG6000-CNコントローラのリンク設定を変更します"](#)
- ["E5700SG コントローラのリンク設定の変更"](#)
- ["SG100またはSG1000サービスアプライアンスのリンク設定を変更します"](#)

手順

1. StorageGRID アプライアンスインストーラで、* ネットワークの設定 * > * IP 構成 * を選択します。

[IP Configuration] ページが表示されます。

2. グリッドネットワークを設定するには、ページの * グリッドネットワーク * セクションで * 静的 * または * DHCP * のいずれかを選択します。
3. 「* Static *」を選択した場合は、次の手順に従ってグリッドネットワークを設定します。
 - a. CIDR 表記を使用して静的 IPv4 アドレスを入力します。
 - b. ゲートウェイを入力します。

ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスを再入力します。

- c. ジャンボフレームを使用する場合は、MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。



ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。



ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、* Grid Network MTU mismatch * アラートがトリガーされます。MTU値はすべてのネットワークタイプで同じである必要はありません。

d. [保存 (Save)]をクリックします。

IP アドレスを変更すると、ゲートウェイとサブネットのリストも変更される可能性があります。

StorageGRID アプライアンスインストーラへの接続が失われた場合は、割り当てた新しい静的 IP アドレスを使用して URL を再入力します。たとえば、「+」と入力します **https://
appliance_IP:8443**

e. グリッドネットワークのサブネットのリストが正しいことを確認します。

グリッドサブネットがある場合は、グリッドネットワークゲートウェイが必要です。指定するすべてのグリッドサブネットが、このゲートウェイ経由でアクセス可能であることが必要です。StorageGRID のインストールを開始するときに、プライマリ管理ノードのグリッドネットワークサブネットリストでこれらのサブネットも定義する必要があります。



デフォルトルートはリストされません。クライアントネットワークが有効になっていない場合は、デフォルトルートがグリッドネットワークゲートウェイを使用します。

- サブネットを追加するには、挿入アイコンをクリックします **+** アイコン"] をクリックします。
- 使用されていないサブネットを削除するには、削除アイコンをクリックします **x**。

f. [保存 (Save)]をクリックします。

4. 「* DHCP *」を選択した場合は、次の手順に従ってグリッドネットワークを設定します。

a. [DHCP] ラジオボタンを選択した後、[Save] をクリックします。

[* IPv4 アドレス*]、[* ゲートウェイ*]、および[* サブネット*] フィールドには、自動的に値が入力されます。DHCP サーバが MTU 値を割り当てるように設定されている場合は、**MTU** フィールドにその値が入力され、フィールドは読み取り専用になります。

Web ブラウザは、StorageGRID アプライアンスインストーラの新しい IP アドレスに自動的にリダイレクトされます。

b. グリッドネットワークのサブネットのリストが正しいことを確認します。

グリッドサブネットがある場合は、グリッドネットワークゲートウェイが必要です。指定するすべてのグリッドサブネットが、このゲートウェイ経由でアクセス可能であることが必要です。StorageGRID のインストールを開始するときに、プライマリ管理ノードのグリッドネットワークサブネットリストでこれらのサブネットも定義する必要があります。



デフォルトルートはリストされません。クライアントネットワークが有効になっていない場合は、デフォルトルートがグリッドネットワークゲートウェイを使用します。

- サブネットを追加するには、挿入アイコンをクリックします **+** アイコン"] をクリックします。
- 使用されていないサブネットを削除するには、削除アイコンをクリックします **x**。

c. ジャンボフレームを使用する場合は、MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。



ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。



ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、* Grid Network MTU mismatch * アラートがトリガーされます。MTU値はすべてのネットワークタイプで同じである必要はありません。

a. [保存 (Save)] をクリックします。

5. 管理ネットワークを設定するには、ページの * 管理ネットワーク * セクションで * 静的 * または * DHCP * のいずれかを選択します。



管理ネットワークを設定するには、[Link Configuration] ページで管理ネットワークを有効にします。

Admin Network

The Admin Network is a closed network used for system administration and maintenance. The Admin Network is typically a private network and does not need to be routable between sites.

IP Assignment Static DHCP

IPv4 Address (CIDR)

Gateway

Subnets (CIDR) +

MTU

6. 「 * Static * 」 を選択した場合は、次の手順に従って管理ネットワークを設定します。

a. アプライアンスの管理ポート 1 に対して、CIDR 表記を使用して静的 IPv4 アドレスを入力します。

管理ポート 1 は、アプライアンス右端にある 2 つの 1GbE RJ45 ポートのうち、左側のポートです。

b. ゲートウェイを入力します。

ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスを再入力します。

- c. ジャンボフレームを使用する場合は、MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。



ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

- d. [保存 (Save)] をクリックします。

IP アドレスを変更すると、ゲートウェイとサブネットのリストも変更される可能性があります。

StorageGRID アプライアンスインストーラへの接続が失われた場合は、割り当てた新しい静的 IP アドレスを使用して URL を再入力します。たとえば、「+」と入力します **https://appliance:8443**

- e. 管理ネットワークのサブネットのリストが正しいことを確認します。

指定したゲートウェイを使用してすべてのサブネットにアクセスできることを確認する必要があります。



管理ネットワークゲートウェイを使用するデフォルトルートを作成することはできません。

- サブネットを追加するには、挿入アイコンをクリックします **+** アイコン"] をクリックします。
- 使用されていないサブネットを削除するには、削除アイコンをクリックします **x**。

- f. [保存 (Save)] をクリックします。

7. [DHCP] を選択した場合は、次の手順に従って管理ネットワークを設定します。

- a. [DHCP] ラジオボタンを選択した後、[Save] をクリックします。

[* IPv4 アドレス*]、[* ゲートウェイ*]、および[* サブネット*] フィールドには、自動的に値が入力されます。DHCP サーバが MTU 値を割り当てるように設定されている場合は、**MTU** フィールドにその値が入力され、フィールドは読み取り専用になります。

Web ブラウザは、StorageGRID アプライアンスインストーラの新しい IP アドレスに自動的にリダイレクトされます。

- b. 管理ネットワークのサブネットのリストが正しいことを確認します。

指定したゲートウェイを使用してすべてのサブネットにアクセスできることを確認する必要があります。



管理ネットワークゲートウェイを使用するデフォルトルートを作成することはできません。

- サブネットを追加するには、挿入アイコンをクリックします **+** アイコン"] をクリックします。
- 使用されていないサブネットを削除するには、削除アイコンをクリックします **x**。

- c. ジャンボフレームを使用する場合は、MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。



ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

d. [保存 (Save)] をクリックします。

8. クライアントネットワークを設定するには、ページの * クライアントネットワーク * セクションで * 静的 * または * DHCP * のいずれかを選択します。



クライアントネットワークを設定するには、[Link Configuration] ページでクライアントネットワークを有効にします。

Client Network

The Client Network is an open network used to provide access to client applications, including S3 and Swift. The Client Network enables grid nodes to communicate with any subnet reachable through the Client Network gateway. The Client Network does not become operational until you complete the StorageGRID configuration steps.

IP Assignment Static DHCP

IPv4 Address (CIDR)

Gateway

MTU

9. * Static * を選択した場合は、次の手順に従ってクライアントネットワークを設定します。
- CIDR 表記を使用して静的 IPv4 アドレスを入力します。
 - [保存 (Save)] をクリックします。
 - クライアントネットワークゲートウェイの IP アドレスが正しいことを確認します。



クライアントネットワークが有効になっている場合は、デフォルトルートが表示されません。デフォルトルートはクライアントネットワークゲートウェイを使用するため、クライアントネットワークが有効になっている間は別のインターフェイスに移動できません。

- d. ジャンボフレームを使用する場合は、MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。



ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

e. [保存 (Save)] をクリックします。

10. [DHCP] を選択した場合は、次の手順に従ってクライアントネットワークを設定します。

a. [DHCP] ラジオボタンを選択した後、[Save] をクリックします。

[IPv4 Address] フィールドと [Gateway] フィールドが自動的に入力されます。DHCP サーバが MTU 値を割り当てるように設定されている場合は、MTU フィールドにその値が入力され、フィールドは読み取り専用になります。

Web ブラウザは、StorageGRID アプライアンスインストーラの新しい IP アドレスに自動的にリダイレクトされます。

a. ゲートウェイが正しいことを確認します。



クライアントネットワークが有効になっている場合は、デフォルトルートが表示されません。デフォルトルートはクライアントネットワークゲートウェイを使用するため、クライアントネットワークが有効になっている間は別のインターフェイスに移動できません。

b. ジャンボフレームを使用する場合は、MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。



ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

ネットワーク接続を確認します

使用する StorageGRID ネットワークに、アプライアンスからアクセスできることを確認する必要があります。ネットワークゲートウェイ経由のルーティングを検証するには、StorageGRID アプライアンスインストーラと異なるサブネット上の IP アドレスとの接続をテストする必要があります。MTU 設定を確認することもできます。

手順

1. StorageGRID アプライアンスインストーラのメニューバーから、*Configure Networking *>*Ping and MTU Test* をクリックします。

[Ping and MTU Test] ページが表示されます。

Ping and MTU Test

Use a ping request to check the appliance's connectivity to a remote host. Select the network you want to check connectivity through, and enter the IP address of the host you want to reach. To verify the MTU setting for the entire path through the network to the destination, select Test MTU.

Ping and MTU Test

The screenshot shows a web form titled "Ping and MTU Test". It contains three main input fields: "Network" with a dropdown menu showing "Grid", "Destination IPv4 Address or FQDN" with an empty text box, and "Test MTU" with an unchecked checkbox. Below these fields is a blue button labeled "Test Connectivity".

2. [* ネットワーク *] ドロップダウンボックスから、テストするネットワークを選択します。グリッド、管理、またはクライアント。
3. そのネットワーク上のホストの IPv4 アドレスまたは完全修飾ドメイン名（FQDN）を入力します。
たとえば、ネットワーク上のゲートウェイやプライマリ管理ノードに ping を送信できます。
4. 必要に応じて、*[Test MTU（MTUのテスト）]*チェックボックスを選択して、ネットワーク経由でデステイネーションまでのパス全体のMTU設定を確認します。
たとえば、アプライアンスノードと別のサイトのノードの間のパスをテストできます。
5. [接続のテスト *] をクリックします。

ネットワーク接続が有効な場合は、「Ping test passed」メッセージと ping コマンドの出力が表示されます。

Ping and MTU Test

Use a ping request to check the appliance's connectivity to a remote host. Select the network you want to check connectivity through, and enter the IP address of the host you want to reach. To verify the MTU setting for the entire path through the network to the destination, select Test MTU.

Ping and MTU Test

Network	Grid	▼
Destination IPv4 Address or FQDN	10.96.104.223	
Test MTU	<input checked="" type="checkbox"/>	
<input type="button" value="Test Connectivity"/>		

Ping test passed

Ping command output

```
PING 10.96.104.223 (10.96.104.223) 1472(1500) bytes of data.  
1480 bytes from 10.96.104.223: icmp_seq=1 ttl=64 time=0.318 ms  
  
--- 10.96.104.223 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.318/0.318/0.318/0.000 ms  
  
Found MTU 1500 for 10.96.104.223 via br0
```

関連情報

- ["ネットワークリンクを設定する"](#)
- ["MTU 設定を変更します"](#)

ポートレベルのネットワーク接続を確認

StorageGRID アプライアンスインストーラとその他のノードの間のアクセスがファイアウォールの妨げにならないように、StorageGRID アプライアンスインストーラが指定した IP アドレスまたはアドレス範囲にある特定の TCP ポートまたはポートセットに接続できることを確認します。

このタスクについて

StorageGRID アプライアンスインストーラに付属のポートのリストを使用して、アプライアンスとグリッドネットワーク内の他のノードの間の接続をテストできます。

また、外部 NFS サーバや DNS サーバで使用されるポートなど、管理ネットワークとクライアントネットワーク、および UDP ポートで接続をテストすることもできます。これらのポートのリストについては、を参照してください ["ネットワークポート参照"](#)。



ポート接続テーブルに表示されているグリッドネットワークポートは、StorageGRID バージョン11.7.0でのみ有効です。各ノードタイプに適したポートを確認するには、使用している StorageGRID のバージョンに対応したネットワークガイドラインを確認する必要があります。

手順

1. StorageGRID アプライアンスインストーラから、**Configure Networking** * > Port Connectivity Test (nmap)* をクリックします。

Port Connectivity Test ページが表示されます。

ポート接続テーブルには、グリッドネットワークでの TCP 接続を必要とするノードタイプが表示されます。各ノードタイプについて、アプライアンスにアクセスできる必要があるグリッドネットワークのポートがテーブルに表示されます。

表に記載されたアプライアンスポートとグリッドネットワーク内のその他のノードの間の接続をテストできます。

2. [* ネットワーク *] ドロップダウンから、テストするネットワークを選択します。* グリッド *、* 管理者 *、または * クライアント *。
3. そのネットワーク上のホストの IPv4 アドレスの範囲を指定します。

たとえば、ネットワーク上のゲートウェイやプライマリ管理ノードをプローブできます。

次の例に示すように、ハイフンを使用して範囲を指定します。

4. TCP ポート番号、カンマで区切ったポートのリスト、またはポートの範囲を入力します。

Port Connectivity Test

Network	Grid ▼
IPv4 Address Ranges	10.224.6.160-161
Port Ranges	22,2022
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
<input type="button" value="Test Connectivity"/>	

5. [接続のテスト *] をクリックします。

◦ 選択したポートレベルのネットワーク接続が有効な場合は、「Port connectivity test passed」というメッセージが緑色のバナーに表示されます。nmap コマンドの出力は、バナーの下に表示されます。

Port connectivity test passed

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
2022/tcp  open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
2022/tcp  open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

- ポートレベルのネットワーク接続がリモートホストに確立されても、ホストが選択したポートの1つ以上をリッスンしていない場合は、ポート接続テストに失敗しましたというメッセージが黄色のバナーに表示されます。nmap コマンドの出力は、バナーの下に表示されます。

ホストがリッスンしていないリモート・ポートの状態はすべて「closed」です。たとえば、接続しようとしているノードがインストール済みの状態で、StorageGRID NMS サービスがまだ実行されていない場合に、黄色のバナーが表示されることがあります。

🚫 Port connectivity test failed

Connection not established. Services might not be listening on target ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:07:02 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,80,443,1504,1505,1506,1508,7443,9999
Nmap scan report for 172.16.4.71
Host is up (0.00020s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
1504/tcp  closed evb-elm
1505/tcp  open  funkproxy
1506/tcp  open  utcd
1508/tcp  open  diagmond
7443/tcp  open  oracleas-https
9999/tcp  open  abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:07:03 2020 -- 1 IP address (1 host up) scanned in 0.59 seconds
```

- 選択した1つ以上のポートに対してポートレベルのネットワーク接続を確立できない場合は、赤いバナーに「Port connectivity test failed」というメッセージが表示されます。nmap コマンドの出力は、バナーの下に表示されます。

赤いバナーは、リモートホストのポートへのTCP接続試行が行われたが、送信者には何も返されなかったことを示します。応答が返されない場合、ポートの状態は「filtered」となり、ファイアウォールによってブロックされている可能性があります。



「閉」のポートも一覧表示されます。

Port connectivity test failed
Connection failed to one or more ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71
Nmap scan report for 172.16.4.71
Host is up (0.00029s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
79/tcp    filtered finger
80/tcp    open  http
443/tcp    open  https
1504/tcp   closed evb-elm
1505/tcp   open  funkproxy
1506/tcp   open  utcd
1508/tcp   open  diagmond
7443/tcp   open  oracleas-https
9999/tcp   open  abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:11:02 2020 -- 1 IP address (1 host up) scanned in 1.60 seconds
```

SANtricity システムマネージャの設定（SG6000およびSG5700）

SANtricity System Manager を使用して、ストレージコントローラシェルフのストレージコントローラ、ストレージディスク、その他のハードウェアコンポーネントのステータスを監視できます。E シリーズ AutoSupport のプロキシを設定することもできます。管理ポートを使用せずにアプライアンスから AutoSupport メッセージを送信できます。

SANtricity System Manager をセットアップしてアクセスします

ストレージコントローラシェルフのハードウェアを監視したり、E シリーズ AutoSupport を設定したりするために、ストレージコントローラの SANtricity System Manager へのアクセスが必要になる場合があります。

作業を開始する前に

- を使用している "サポートされている Web ブラウザ"。
- グリッドマネージャからSANtricity システムマネージャにアクセスするには、StorageGRID をインストールし、ストレージアプライアンス管理者またはRootアクセス権限が必要です。
- StorageGRID アプライアンスインストーラを使用してSANtricity System Managerにアクセスするには、SANtricity System Manager管理者のユーザ名とパスワードが必要です。
- Webブラウザを使用してSANtricity System Managerに直接アクセスするには、SANtricity System Manager管理者のユーザ名とパスワードが必要です。



グリッドマネージャまたは StorageGRID アプライアンスインストーラを使用して SANtricity System Manager にアクセスするには、SANtricity ファームウェア 8.70 以降が必要です。StorageGRID アプライアンス・インストーラを使用してファームウェアのバージョンを確認し、* Help * > * About * を選択します。



グリッドマネージャまたはアプライアンスインストーラから SANtricity システムマネージャにアクセスする方法は、通常、ハードウェアを監視して E シリーズ AutoSupport を設定することだけを目的としています。ファームウェアのアップグレードなど、SANtricity System Manager の多くの機能や操作は、StorageGRID アプライアンスの監視には適用されません。問題を回避するには、アプライアンスのハードウェアの設置とメンテナンスの手順に必ず従ってください。

このタスクについて

SANtricity System Manager にアクセスする方法は 3 種類あり、その方法はインストールおよび設定のどの段階にあるかによって異なります。

- アプライアンスが StorageGRID システムにノードとして導入されていない場合は、StorageGRID アプライアンスインストーラの Advanced タブを使用します。



導入されたノードは、StorageGRID アプライアンスインストーラを使用して SANtricity システムマネージャにアクセスできなくなります。

- アプライアンスを StorageGRID システムにノードとして導入している場合は、グリッドマネージャのノードページにある SANtricity システムマネージャタブを使用します。
- StorageGRID アプライアンスインストーラまたはグリッドマネージャを使用できない場合は、管理ポートに接続された Web ブラウザを使用して SANtricity システムマネージャに直接アクセスできます。

この手順には、SANtricity システムマネージャに最初にアクセスする手順が含まれています。SANtricity System Manager をすでにセットアップしている場合は、に進みます [ハードウェアアラートの設定手順](#)。



グリッドマネージャまたは StorageGRID アプライアンスインストーラを使用すると、アプライアンスの管理ポートを設定または接続しなくても SANtricity System Manager にアクセスできます。

SANtricity System Manager を使用して次の項目を監視します。

- ストレージレイレベルのパフォーマンス、I/O レイテンシ、CPU 利用率、スループットなどのパフォーマンスデータ
- ハードウェアコンポーネントのステータス
- 診断データの表示などの機能をサポートします

SANtricity System Manager を使用して、次の設定を行うことができます。

- ストレージコントローラシェルフのコンポーネントの E メールアラート、SNMP アラート、または syslog アラート
- ストレージコントローラシェルフのコンポーネントの E シリーズ AutoSupport の設定。

E シリーズ AutoSupport の詳細については、を参照してください ["NetApp E シリーズシステムのドキュメントのサイト"](#)。

- セキュリティ保護されたドライブのロックを解除するために必要なドライブセキュリティキー（ドライブセキュリティ機能が有効になっている場合はロックの解除が必要）
- SANtricity システムマネージャにアクセスするための管理者パスワード

手順

1. 次のいずれかを実行します。

- StorageGRID アプライアンス・インストーラを使用して、* アドバンスト * > * SANtricity システム・マネージャ * を選択します
- Grid Managerを使用して、* nodes >を選択します ***appliance Storage Node** > * SANtricity システム・マネージャ*



これらのオプションが使用できない場合、またはログインページが表示されない場合は、[ストレージコントローラの IP アドレス](#)を使用します。SANtricity System Manager にアクセスするには、ストレージコントローラの IP にアクセスします。

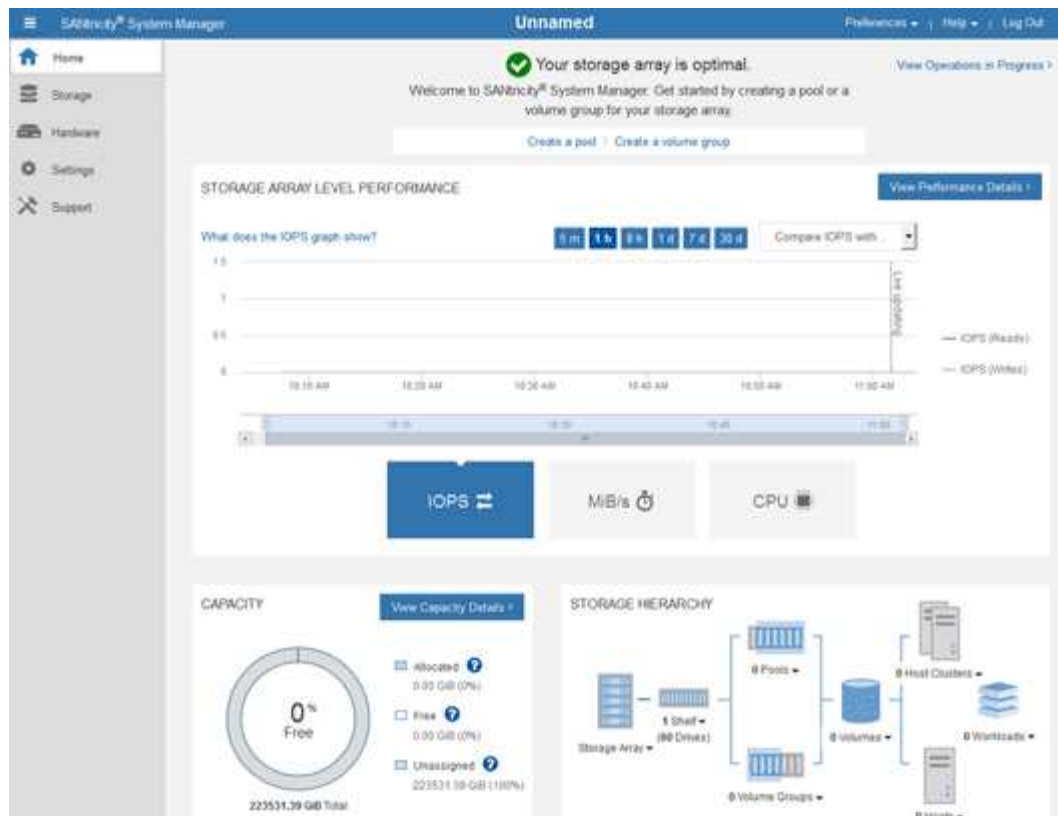
2. 管理者パスワードを設定または入力します。

SANtricity System Manager では、すべてのユーザで共有する管理者パスワードを 1 つ使用します。

3. 「* キャンセル * 」を選択してウィザードを閉じます。



StorageGRID アプライアンスのセットアップ・ウィザードは実行しないでください。



4. ハードウェアアラートを設定します。
 - a. SANtricity System Manager のオンラインヘルプにアクセスするには、 * Help * を選択します。
 - b. オンラインヘルプの「 * Settings * > * Alerts * 」 (* 設定 * > * アラート *) セクションを使用して、アラートについて学習します。
 - c. How To の指示に従って ' メール・アラート 'SNMP アラート ' または syslog アラートを設定します
5. ストレージコントローラシェルフのコンポーネントの AutoSupport を管理します。
 - a. SANtricity System Manager のオンラインヘルプにアクセスするには、 * Help * を選択します。
 - b. オンラインヘルプの「 * support * > * Support Center * 」セクションで、AutoSupport 機能について学習します。
 - c. 「 How To 」の指示に従って、AutoSupport を管理します。

管理ポートを使用せずにEシリーズAutoSupport メッセージを送信するためのStorageGRID プロキシを設定する具体的な手順については、を参照してください"[ストレージプロキシの設定手順](#)".
6. アプライアンスでドライブセキュリティ機能が有効になっている場合は、セキュリティキーを作成して管理します。
 - a. SANtricity System Manager のオンラインヘルプにアクセスするには、 * Help * を選択します。
 - b. オンラインヘルプの「 * Settings * > * System * > * Security key management * 」セクションでドライブセキュリティについて学習します。
 - c. 「 How To 」の指示に従って、セキュリティキーを作成および管理します。
7. 必要に応じて、管理者パスワードを変更します。
 - a. SANtricity System Manager のオンラインヘルプにアクセスするには、 * Help * を選択します。

- b. オンラインヘルプの * Home * > * Storage array administration * セクションで、管理者パスワードを確認してください。
- c. 「How To」の指示に従ってパスワードを変更します。

SANtricity システムマネージャでハードウェアステータスを確認します

SANtricity System Manager を使用して、ストレージコントローラシェルフの個々のハードウェアコンポーネントを監視および管理したり、コンポーネントの温度やドライブに関連する問題など、ハードウェア診断および環境に関する情報を確認したりできます。

作業を開始する前に

- を使用している "サポートされている Web ブラウザ"。
- Grid ManagerからSANtricity System Managerにアクセスするには、ストレージアプライアンス管理者の権限またはRoot Access権限が必要です。
- StorageGRID アプライアンスインストーラを使用してSANtricity System Managerにアクセスするには、SANtricity System Manager管理者のユーザ名とパスワードが必要です。
- Webブラウザを使用してSANtricity System Managerに直接アクセスするには、SANtricity System Manager管理者のユーザ名とパスワードが必要です。



グリッドマネージャまたは StorageGRID アプライアンスインストーラを使用して SANtricity System Manager にアクセスするには、SANtricity ファームウェア 8.70 以降が必要です。

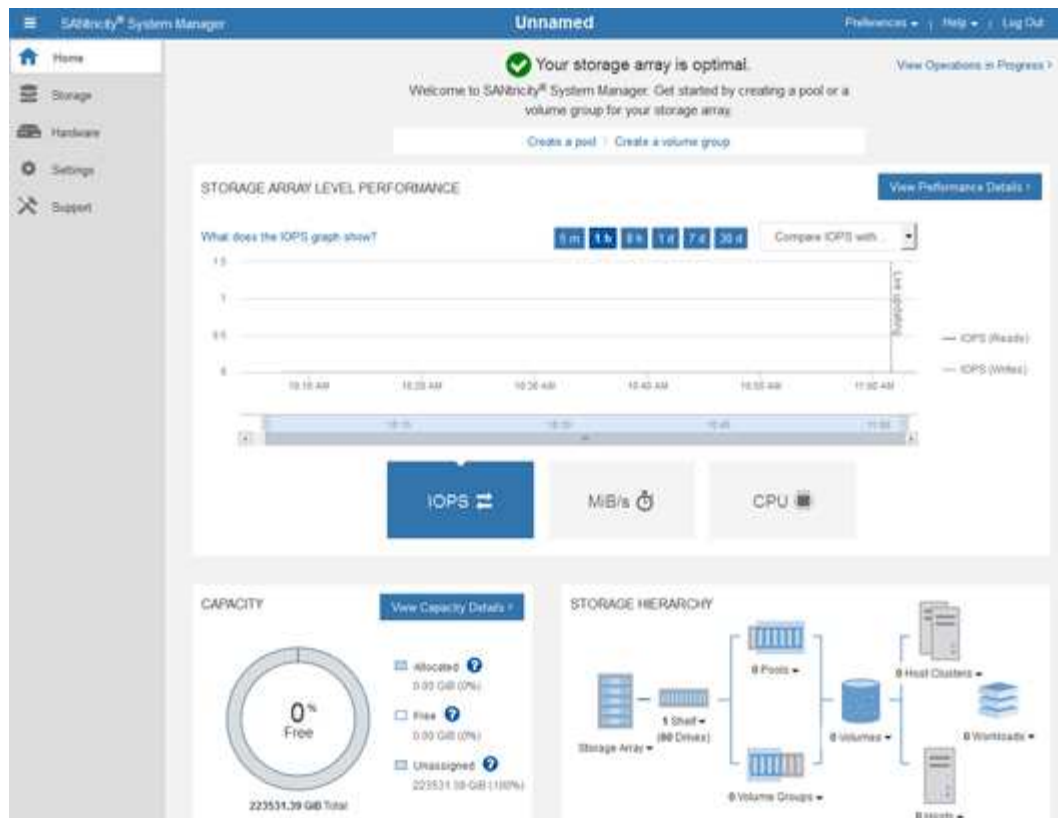


グリッドマネージャまたはアプライアンスインストーラから SANtricity システムマネージャにアクセスする方法は、通常、ハードウェアを監視して E シリーズ AutoSupport を設定することだけを目的としています。ファームウェアのアップグレードなど、SANtricity System Manager の多くの機能や操作は、StorageGRID アプライアンスの監視には適用されません。問題を回避するには、アプライアンスのハードウェアの設置とメンテナンスの手順に必ず従ってください。

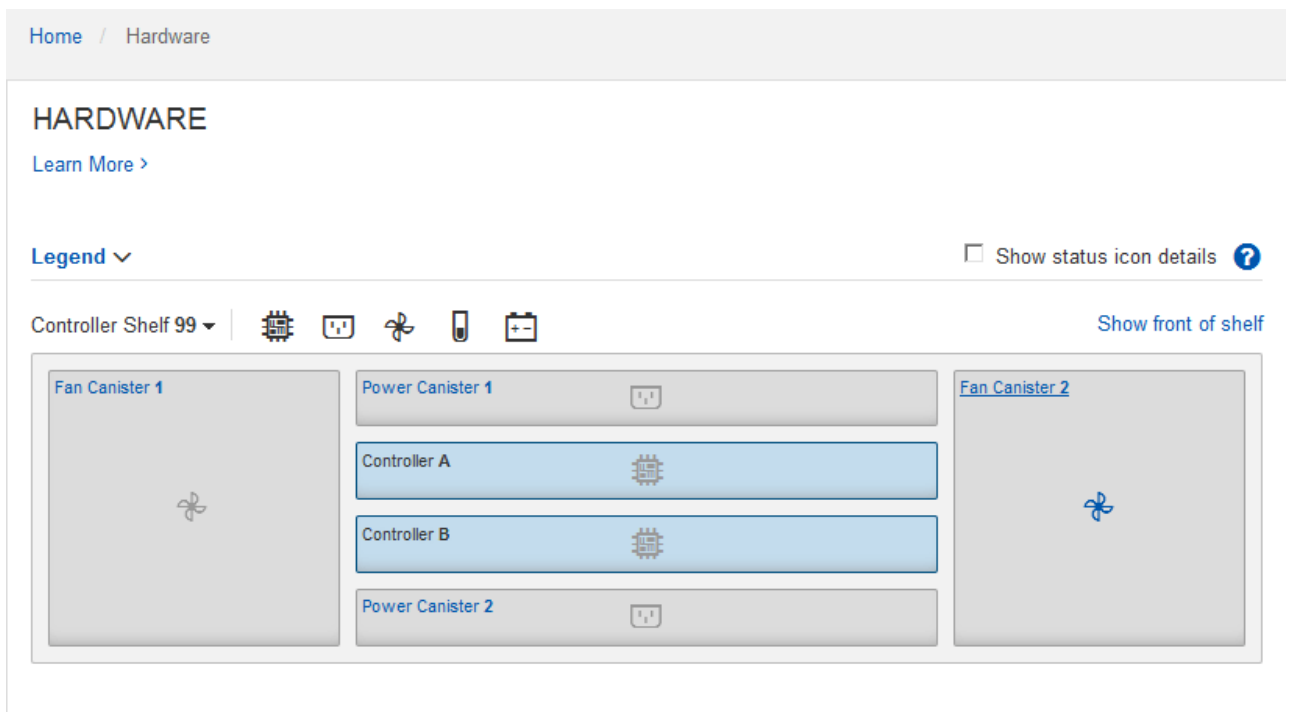
手順

1. SANtricity システムマネージャにアクセスします。
2. 必要に応じて、管理者のユーザ名とパスワードを入力します。
3. セットアップウィザードを閉じて SANtricity システムマネージャのホームページを表示するには、* Cancel * をクリックします。

SANtricity の System Manager ホームページが表示されます。SANtricity System Manager では、コントローラシェルフがストレージアレイと表示されます。



4. アプライアンスハードウェアについて表示された情報を確認し、すべてのハードウェアコンポーネントのステータスが「Optimal」であることを確認します。
 - a. [* ハードウェア *] タブをクリックします。
 - b. Show back of shelf* (シェルフの背面を表示) をクリックします。



シェルフの背面から、両方のストレージコントローラ、各ストレージコントローラのバッテリー、電源キャ

ニスター 2 台、ファンキャニスター 2 台、および拡張シェルフ（ある場合）を確認できます。構成部品の温度を表示することもできます。

- a. 各ストレージコントローラの設定を表示するには、コントローラを選択し、コンテキストメニューから * 設定の表示 * を選択します。
- b. シェルフの背面にある他のコンポーネントの設定を確認するには、対象となるコンポーネントを選択します。
- c. [Show front of shelf*（シェルフの前面を表示）] をクリックし、表示するコンポーネントを選択します。

シェルフの前面からは、ストレージコントローラシェルフまたは拡張シェルフ（ある場合）のドライブとドライブドローを確認できます。

ステータスが「Needs Attention」になっているコンポーネントがある場合は、Recovery Guru に示される手順に従って問題を解決するか、テクニカルサポートに連絡してください。

StorageGRID アプライアンスインストーラを使用してストレージコントローラの IP アドレスを設定します

各ストレージコントローラの管理ポート 1 を使用して、アプライアンスを SANtricity System Manager の管理ネットワークに接続します。StorageGRID アプライアンスインストーラから SANtricity System Manager にアクセスできない場合は、コントローラシェルフのハードウェアおよびコントローラファームウェアとの管理接続が失われないように、各ストレージコントローラに静的 IP アドレスを設定します。

作業を開始する前に

- StorageGRID 管理ネットワークに接続できる管理クライアントを使用しているか、サービスラップトップを使用している必要があります。
- クライアントまたはサービスラップトップに、サポートされている Web ブラウザをインストールしておきます。

このタスクについて

DHCP によって割り当てられたアドレスは、いつ変更されるかわかりません。一貫したアクセスを確保するために、コントローラには静的 IP アドレスを割り当ててください。



この手順は、StorageGRID アプライアンスインストーラ（アドバンスト>* SANtricity システムマネージャ*）またはグリッドマネージャ（* nodes > SANtricity システムマネージャ*）から SANtricity システムマネージャにアクセスできない場合にのみ使用してください。

手順

1. クライアントから、StorageGRID アプライアンスインストーラの URL を入力します：+
https://Appliance_Controller_IP:8443

の場合 `Appliance_Controller_IP` には、任意の StorageGRID ネットワーク上のアプライアンスの IP アドレスを使用します。

StorageGRID アプライアンスインストーラのホームページが表示されます。

2. Configure Hardware * > * Storage Controller Network Configuration * を選択します。

Storage Controller Network Configuration ページが表示されます。

3. ネットワーク構成に応じて、IPv4、IPv6、またはその両方で * Enabled * を選択します。
4. 自動的に表示される IPv4 アドレスを書き留めます。

ストレージコントローラの管理ポートに IP アドレスを割り当てるためのデフォルトの方法は、DHCP です。



DHCP 値が表示されるまでに数分かかる場合があります。

IPv4 Address Assignment Static DHCP

IPv4 Address (CIDR) 10.224.5.166/21

Default Gateway 10.224.0.1

5. 必要に応じて、ストレージコントローラの管理ポートに静的 IP アドレスを設定します。



管理ポートに静的 IP を割り当てるか、DHCP サーバでアドレスの永久リースを割り当てる必要があります。

- a. 「* Static *」を選択します。
- b. CIDR 表記を使用して IPv4 アドレスを入力します。
- c. デフォルトゲートウェイを入力します。

IPv4 Address Assignment Static DHCP

IPv4 Address (CIDR) 10.224.2.200/21

Default Gateway 10.224.0.1

- d. [保存 (Save)] をクリックします。

変更が適用されるまで数分かかる場合があります。

SANtricity System Managerに接続するときは、新しい静的IPアドレスをURL：+として使用します
`https://Storage_Controller_IP`

BMCインターフェイスの設定 (SGF6112、SG6000、SG100、SG1000)

BMCインターフェイス：概要 (SGF6112、SG6000、SG100、およびSG1000)

SGF6112、SG6000、またはサービスアプライアンスのベースボード管理コントローラ

(BMC) のユーザインターフェイスには、ハードウェアに関するステータス情報が表示され、アプライアンスのSNMP設定やその他のオプションを設定できます。

このセクションの次の手順に従って、アプライアンスの設置時にBMCを設定します。

- ["BMCインターフェイスの管理者パスワードまたはrootパスワードの変更"](#)
- ["BMC 管理ポートの IP アドレスを設定します"](#)
- ["BMC インターフェイスにアクセスします"](#)
- ["SNMPを設定します"](#)
- ["BMCアラートのEメール通知を設定する"](#)

アプライアンスがグリッドにすでに設置されていて、StorageGRIDソフトウェアを実行している場合は、次の手順を実行します。



- ["アプライアンスをメンテナンスモードにします"](#) をクリックして、StorageGRIDアプライアンスインストーラにアクセスします。
- を参照してください ["BMC 管理ポートの IP アドレスを設定します"](#) StorageGRIDアプライアンスインストーラを使用してBMCインターフェイスにアクセスする方法については、を参照してください。

BMCインターフェイスの管理者パスワードまたはrootパスワードの変更

セキュリティを確保するため、BMCの管理者ユーザまたはrootユーザのパスワードを変更する必要があります。

作業を開始する前に

管理クライアントがを使用している必要があります ["サポートされている Web ブラウザ"](#)。

このタスクについて

アプライアンスの初回インストール時には、BMCではadminユーザまたはrootユーザのデフォルトのパスワードが使用されます。システムを保護するために、adminユーザまたはrootユーザのパスワードを変更する必要があります。

デフォルトのユーザは、StorageGRIDアプライアンスのインストール時期によって異なります。デフォルトのユーザは、新規インストールの場合は* admin、古いインストールの場合は root *です。

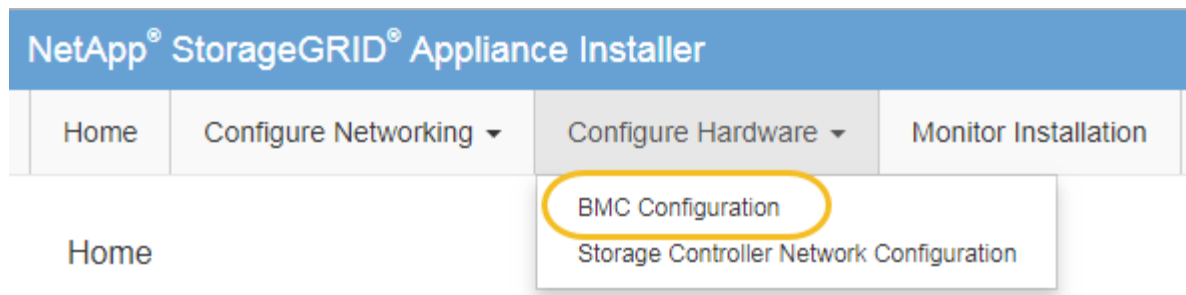
手順

1. クライアントから、StorageGRID アプライアンスインストーラのURLを入力します：+
https://Appliance_IP:8443

の場合 `Appliance_IP` には、任意のStorageGRID ネットワーク上のアプライアンスのIPアドレスを使用します。

StorageGRID アプライアンスインストーラのホームページが表示されます。

2. [ハードウェアの設定 > BMC 構成] を選択します。



[Baseboard Management Controller Configuration] ページが表示されます。

3. 管理者アカウントまたはrootアカウントの新しいパスワードを2つのフィールドに入力します。
4. [保存 (Save)] をクリックします。

BMC 管理ポートの IP アドレスを設定します

BMC インターフェイスにアクセスする前に、SGF6112、SG6000-CN コントローラ、またはサービスアプライアンスの BMC 管理ポートの IP アドレスを設定します。

ConfigBuilder を使用して JSON ファイルを生成する場合は、IP アドレスを自動的に設定できます。を参照してください ["アプライアンスのインストールと設定を自動化"](#)。

作業を開始する前に

- 管理クライアントが使用している必要があります ["サポートされている Web ブラウザ"](#)。
- StorageGRID ネットワークに接続できる管理クライアントを使用している必要があります。
- BMC 管理ポートが、使用する管理ネットワークに接続されている必要があります。

SG6112



SG6000 を使用します



SG1000 からのアクセス



SG100



このタスクについて

BMC 管理ポートでは、サポート目的で下位レベルのハードウェアアクセスが許可されます。



このポートは、信頼されているセキュアな内部管理ネットワークにのみ接続してください。該当するネットワークがない場合は、テクニカルサポートから BMC 接続の要請があった場合を除き、BMC ポートを接続しないか、またはブロックしたままにしてください。

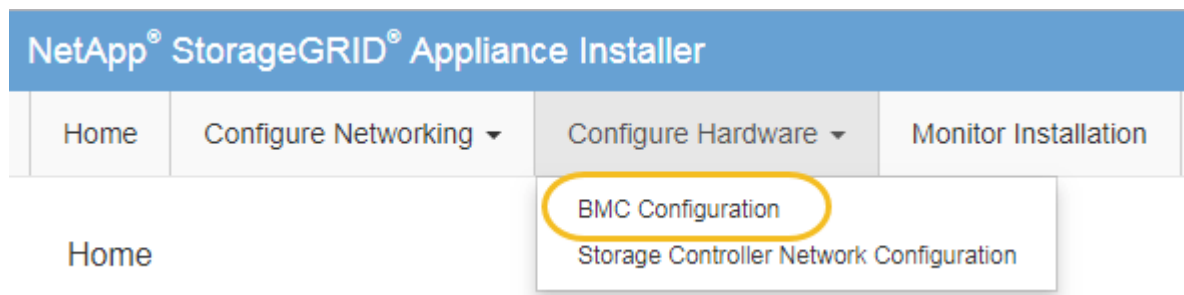
手順

1. クライアントから、StorageGRID アプライアンスインストーラの URL を入力します：+
https://Appliance_IP:8443

の場合 `Appliance_IP` には、任意の StorageGRID ネットワーク上のアプライアンスの IP アドレスを使用します。

StorageGRID アプライアンスインストーラのホームページが表示されます。

2. [ハードウェアの設定 >> BMC 構成] を選択します。



[Baseboard Management Controller Configuration] ページが表示されます。

3. 自動的に表示される IPv4 アドレスを書き留めます。

このポートに IP アドレスを割り当てるためのデフォルトの方法は、DHCP です。



DHCP 値が表示されるまでに数分かかる場合があります。

Baseboard Management Controller Configuration

LAN IP Settings

IP Assignment	<input type="radio"/> Static <input checked="" type="radio"/> DHCP
MAC Address	<input type="text" value="d8:c4:97:28:50:62"/>
IPv4 Address (CIDR)	<input type="text" value="10.224.3.225/21"/>
Default gateway	<input type="text" value="10.224.0.1"/>

4. 必要に応じて、BMC 管理ポートに静的 IP アドレスを設定します。



BMC 管理ポートに静的 IP を割り当てるか、DHCP サーバでアドレスの永久リースを割り当てる必要があります。

- a. 「* Static *」を選択します。
- b. CIDR 表記を使用して IPv4 アドレスを入力します。
- c. デフォルトゲートウェイを入力します。

Baseboard Management Controller Configuration

LAN IP Settings

IP Assignment	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
MAC Address	d8:c4:97:28:50:62
IPv4 Address (CIDR)	10.224.3.225/21
Default gateway	10.224.0.1

- d. [保存 (Save)] をクリックします。

変更が適用されるまで数分かかる場合があります。

BMC インターフェイスにアクセスします

次のアプライアンスモデルでは、BMC管理ポートのDHCPまたは静的IPアドレスを使用してBMCインターフェイスにアクセスできます。

- SGF6112を参照してください
- SG6000を使用します
- SG1000 からのアクセス
- SG100

作業を開始する前に

- 管理クライアントがを使用している必要があります "[サポートされている Web ブラウザ](#)"。
- アプライアンスのBMC管理ポートを、使用する管理ネットワークに接続しておきます。

SGF6112を参照してください



SG6000を使用します



SG1000 からのアクセス



SG100



手順

1. BMCインターフェイスのURLとして「+」を入力します `https://BMC_Port_IP`

の場合 `BMC_Port_IP` BMC管理ポートのDHCPまたは静的IPアドレスを使用します。

BMC のサインインページが表示されます。



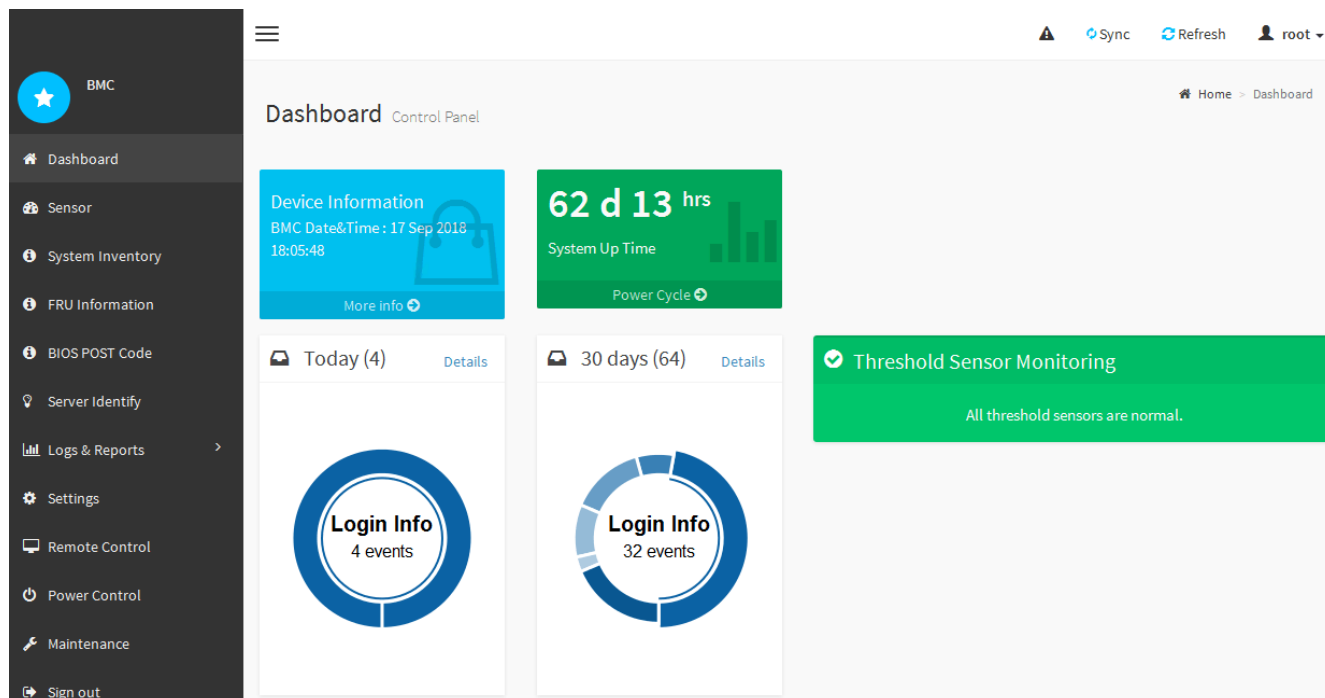
をまだ構成していない場合 `BMC_Port_IP`` の手順に従ってください **"BMCインターフェイスの設定"**。ハードウェアの問題が原因で手順 `を使用できず、BMC の IP アドレスを設定していない場合でも、BMC にアクセスできる可能性があります。デフォルトでは、BMC は DHCP を使用して IP アドレスを取得します。BMCネットワークでDHCPが有効になっている場合は、ネットワーク管理者からBMC MACに割り当てられたIPアドレスを指定できます。このIPアドレスは、アプライアンス前面のラベルに印刷されています。BMCネットワークでDHCPが有効になっていない場合、数分後にBMCが応答なくなり、BMCにはデフォルトの静的IPが割り当てられます `192.168.0.120。ラップトップをBMCポートに直接接続し、ネットワーク設定を変更してラップトップなどのIPを割り当てなければならない場合があります `192.168.0.200/24` をクリックしてを参照します `192.168.0.120。

2. 管理者またはrootのユーザ名とパスワードを、 **"デフォルトの root パスワードが変更されました"** :



デフォルトのユーザは、StorageGRIDアプライアンスのインストール時期によって異なります。デフォルトのユーザは、新規インストールの場合は* admin、古いインストールの場合は root *です。

3. 「* サインイン *」を選択します。



4. 必要に応じて、**Settings**>*User Management* を選択し、「disabled」ユーザをクリックして、追加のユーザを作成します。



ユーザが初めてサインインすると、セキュリティを強化するためにパスワードの変更を求められる場合があります。

BMCのSNMP設定を行います

ハードウェアのSNMPの設定に精通している場合は、BMCインターフェイスを使用してSGF6112、SG6000、およびサービスアプライアンスのSNMP設定を行うことができます。セキュリティで保護されたコミュニティストリングを指定し、SNMPトラップを有効にし、SNMPの送信先を最大5つ指定できます。

作業を開始する前に

- BMC ダッシュボードへのアクセス方法を確認しておく必要があります。
- SNMPv1-v2c 機器の SNMP 設定経験が必要です。



この手順で作成された BMC 設定は、アプライアンスに障害が発生して交換が必要な場合に、保持されることがあります。適用したすべての設定を記録し、必要に応じてハードウェアの交換後に簡単に再適用できるようにします。

手順

1. BMC ダッシュボードで、* Settings * > * SNMP Settings * を選択します。
2. SNMP 設定ページで、* SNMP V1/V2* を有効にするを選択し、読み取り専用コミュニティストリングと読み取り / 書き込みコミュニティストリングを指定します。

読み取り専用コミュニティストリングは、ユーザ ID やパスワードのようなものです。侵入者がネットワーク設定に関する情報を取得できないようにするには、この値を変更する必要があります。読み取り / 書

き込みコミュニティストリングは、不正な変更からデバイスを保護します。

- 必要に応じて、* トラップを有効にする * を選択し、必要な情報を入力します。



IP アドレスを使用して、各 SNMP トラップの送信先 IP を入力します。完全修飾ドメイン名はサポートされていません。

アプライアンスが異常な状態になったときにSNMPコンソールに通知がすぐに送信されるようにするには、トラップを有効にします。デバイスによっては、トラップは、さまざまなコンポーネントのハードウェア障害、リンクのアップ/ダウン状態、温度しきい値を超えている、またはトラフィックが多いことを示している場合があります。

- 必要に応じて、[テストトラップの送信] をクリックして設定をテストします。
- 設定が正しい場合は、* 保存 * をクリックします。

BMCアラートのEメール通知を設定する

アラート発生時にEメール通知が送信されるようにするには、BMCインターフェイスを使用してSMTP設定、ユーザ、LANデスティネーション、アラートポリシー、およびイベントフィルタを設定します。



SG6000-CNコントローラまたはサービスアプライアンスに障害が発生して交換が必要になった場合、この手順で行ったBMC設定が保持されないことがあります。適用したすべての設定を記録し、必要に応じてハードウェアの交換後に簡単に再適用できるようにします。

作業を開始する前に

BMC ダッシュボードへのアクセス方法を確認しておく必要があります。

このタスクについて

BMC インターフェイスでは、[設定] ページの *SMTP 設定*、*ユーザー管理*、および *プラットフォーム・イベント・フィルタ* オプションを使用して、電子メール通知を設定します。

Settings Configure BMC options

External User Services	KVM Mouse Setting	Log Settings	Network Settings
Platform Event Filters	RAID Management	SAS IT Management	SMTP Settings
SSL Settings	System Firewall	User Management	SOL Settings
SNMP Settings	Cold Redundancy	NIC Selection	

手順

- "BMCのSNMP設定を行います"。
 - [* 設定 * > * SMTP 設定 *] を選択します。

b. [送信者電子メール ID] に、有効な電子メールアドレスを入力します。

この E メールアドレスは、BMC が E メールを送信したときの送信元アドレスとして提供されます。

2. アラートを受信するようにユーザを設定します。

a. BMC ダッシュボードで、* Settings * > * User Management * を選択します。

b. アラート通知を受信するユーザを少なくとも 1 人追加してください。

ユーザに設定する E メールアドレスは、BMC がアラート通知の送信先アドレスです。たとえば、「notification-user」などの一般的なユーザーを追加し、テクニカルサポートチームの Email宛先リストの電子メールアドレスを使用できます。

3. LAN 宛先にアラートを設定します。

a. [* 設定 * > * プラットフォーム・イベント・フィルタ * > * LAN 宛先 *] を選択します。

b. LAN 宛先を少なくとも 1 つ設定します。

- [宛先の種類] で [Email] を選択します。

- BMC Username には、前に追加したユーザ名を選択します。

- 複数のユーザを追加し、すべてのユーザが通知メールを受信できるようにする場合は、ユーザごとに LAN 宛先を追加します。

c. テストアラートを送信します。

4. アラートポリシーを設定して、BMC がアラートを送信するタイミングと場所を定義できるようにします。

a. [* 設定 * > * プラットフォーム・イベント・フィルタ * > * アラート・ポリシー *] を選択します。

b. LAN 宛先ごとに少なくとも 1 つのアラートポリシーを設定します。

- [ポリシーグループ番号 (Policy Group Number)] で、* 1 * を選択します。

- [ポリシーアクション] で、[* 常にこの宛先にアラートを送信する *] を選択します。

- LAN チャンネルの場合、* 1 * を選択します。

- [Destination Selector] で、ポリシーの LAN 宛先を選択します。

5. イベントフィルタを設定して、さまざまなイベントタイプのアラートを適切なユーザに送信します。

a. [* 設定 * > * プラットフォーム・イベント・フィルタ * > * イベント・フィルタ *] を選択します。

b. Alert Policy Group Number (アラートポリシーグループ番号) に * 1 * を入力します。

c. アラートポリシーグループに通知するイベントごとにフィルタを作成します。

- 電源アクション、特定のセンサーイベント、またはすべてのイベントのイベントフィルタを作成できます。

- 監視するイベントが不明な場合は、センサーの種類として「* すべてのセンサー *」を選択し、イベントオプションとして「すべてのイベント *」を選択します。不要な通知を受け取った場合は、選択内容をあとで変更できます。

オプション：ノード暗号化を有効にします

ノードの暗号化を有効にすると、アプライアンス内のディスクを安全なキー管理サーバ

(KMS) 暗号化によってサイト内での物理的な損失やデータの削除から保護することができます。アプライアンスのインストール時に、ノード暗号化を選択して有効にする必要があります。KMS暗号化プロセスの開始後は、ノード暗号化を無効にすることはできません。

ConfigBuilderを使用してJSONファイルを生成する場合は、ノード暗号化を自動的に有効にすることができます。を参照してください ["アプライアンスのインストールと設定を自動化"](#)。

作業を開始する前に

に関する情報を確認します ["KMSを設定しています"](#)。

このタスクについて

ノード暗号化が有効になっているアプライアンスは、StorageGRID サイト用に設定されている外部キー管理サーバ (KMS) に接続します。各 KMS (または KMS クラスター) は、サイトにあるすべてのアプライアンスノードの暗号化キーを管理します。これらのキーは、ノード暗号化が有効なアプライアンスで、各ディスク上のデータを暗号化および復号化します。

Grid Manager StorageGRID では、アプライアンスのインストール前またはインストール後に KMS を設定できます。詳細については、StorageGRID の管理手順の KMS とアプライアンスの設定に関する情報を参照してください。

- アプライアンスをインストールする前に KMS を設定すると、KMS で制御される暗号化が開始されます。この暗号化は、アプライアンスでノード暗号化を有効にし、KMS が設定されている StorageGRID サイトに追加します。
- アプライアンスをインストールする前に KMS が設定されていない場合は、KMS が設定され、アプライアンスノードを含むサイトで利用可能になった時点で、ノード暗号化が有効になっている各アプライアンスで KMS 制御された暗号化が実行されます。



ノード暗号化を有効にしてアプライアンスを設置すると、一時キーが割り当てられます。アプライアンスのデータは、アプライアンスがキー管理システム (KMS) に接続され、KMSセキュリティキーが設定されるまで保護されません。を参照してください ["KMSアプライアンスの設定の概要"](#) 追加情報 の場合。

ディスクの復号化にKMSキーが必要でないと、アプライアンス上のデータを取得できず、実質的に失われます。これは、KMSから復号化キーを取得できない場合に発生します。顧客が KMS 設定をクリアするか、KMS キーの有効期限が切れるか、KMS への接続が失われるか、KMS キーがインストールされている StorageGRID システムからアプライアンスが削除されると、キーにアクセスできなくなります。

手順

1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。

`https://Controller_IP:8443`

`Controller_IP` は、3つのStorageGRID ネットワークのいずれかでのコンピューティングコントローラ (ストレージコントローラではない) のIPアドレスです。

StorageGRID アプライアンスインストーラのホームページが表示されます。



アプライアンスがKMSキーで暗号化されたあとは、同じKMSキーを使用しないとアプライアンスのディスクを復号化できません。

2. Configure Hardware * > * Node Encryption * を選択します。

NetApp® StorageGRID® Appliance Installer Help ▾

Home | Configure Networking ▾ | **Configure Hardware ▾** | Monitor Installation | Advanced ▾

Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

Encryption Status

⚠ You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption

Save

Key Management Server Details

3. [ノード暗号化を有効にする *] を選択します。

アプライアンスをインストールする前に、*[ノード暗号化の有効化]*を選択解除してデータが失われるリスクはありません。インストールを開始すると、アプライアンスノードがStorageGRID システム内のKMS暗号化キーにアクセスし、ディスク暗号化を開始します。アプライアンスの設置後にノード暗号化を無効にすることはできません。



KMSを使用するStorageGRID サイトにノード暗号化が有効になっているアプライアンスを追加したあとで、そのノードでKMS暗号化の使用を停止することはできません。

4. [保存 (Save)] を選択します。
5. アプライアンスを StorageGRID システムのノードとして導入します。

KMS で制御される暗号化は、アプライアンスが StorageGRID サイト用に設定されている KMS キーにアクセスすると開始されます。KMS 暗号化プロセス中にインストーラによって進捗状況のメッセージが表示されます。この処理には、アプライアンス内のディスクボリュームの数によっては数分かかることがあります。



アプライアンスは、最初に各ディスクボリュームにランダムな KMS 以外の暗号化キーを割り当てて構成します。ディスクはこの一時的な暗号化キーを使用して暗号化されます。このキーは、ノード暗号化が有効になっているアプライアンスが StorageGRID サイト用に設定されている KMS キーにアクセスするまではセキュリティ保護されません。

完了後

アプライアンスノードがメンテナンスモードのときに使用されているノード暗号化ステータス、KMS の詳細、および証明書を確認できます。を参照してください "[メンテナンスモードでノード暗号化を監視します](#)" を参照してください。

オプション：RAIDモードを変更します

一部のアプライアンスモデルでは、ストレージとリカバリの要件に合わせてアプライアンス上で別のRAIDモードに変更できます。モードを変更できるのは、アプライアンスストレージノードを導入する前だけです。

ConfigBuilderを使用してJSONファイルを生成する場合は、RAIDモードを自動的に変更できます。を参照してください ["アプライアンスのインストールと設定を自動化"](#)。

このタスクについて

アプライアンスでサポートされている場合は、次のいずれかのボリューム構成オプションを選択できます。

- * Dynamic Disk Pools (DDP) * : データドライブ8本につきパリティドライブを2本使用します。すべてのアプライアンスに推奨されるデフォルトのモードです。DDPはRAID 6よりもシステムパフォーマンスに優れ、ドライブ障害が発生したあとのリビルド時間が短く、管理も容易です。DDPは、SG5760アプライアンスにドロー損失からの保護も提供します。



SG6060アプライアンスではSSDが2本あるため、DDPはドロー損失からの保護を提供しません。ドロー損失の保護は、SG6060に追加するすべての拡張シェルフで有効です。

- * DDP16 * : このモードはデータドライブ 16 本につきパリティドライブを 2 本使用するため、DDP よりもストレージ効率が高くなります。RAID 6と比較すると、システムパフォーマンスが向上し、ドライブ障害が発生したあとのリビルド時間が短縮され、管理が容易になり、ストレージ効率も同等に向上します。DDP16 モードを使用するには、構成にドライブが 20 本以上含まれている必要があります。ドロー損失からの保護は提供しません。
- * RAID6 * : このモードは 16 台以上のデータドライブごとに 2 本のパリティドライブを使用します。これは、各ディスクでパリティドライブを使用するハードウェア保護方式であり、データが失われる前にRAIDセット内の2つのディスク障害を許容します。RAID 6 モードを使用するには、構成にドライブが 20 本以上含まれている必要があります。RAID 6はDDPよりもアプライアンスのストレージ効率を高めることができますが、ほとんどのStorageGRID 環境では推奨されません。



ボリュームがすでに構成されている場合や StorageGRID が事前にインストールされている場合に RAID モードを変更すると、ボリュームが削除されて置き換えられます。対象となったボリュームのデータはすべて失われます。

SG6000を使用します

作業を開始する前に

- StorageGRID に接続できるクライアントを使用している必要があります。
- クライアントにはがあります ["サポートされている Web ブラウザ"](#)。

手順

1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。

`https://Controller_IP:8443`

Controller_IP は、3つのStorageGRID ネットワークのいずれかでのコンピューティングコントローラ（ストレージコントローラではない）のIPアドレスです。

StorageGRID アプライアンスインストーラのホームページが表示されます。

2. 「* アドバンスト *」 > 「* RAID モード *」の順に選択します。
3. [Configure RAID Mode*] ページで、[Mode] ドロップダウンリストから目的の RAID モードを選択します。
4. [保存 (Save)] をクリックします。

SG5760

作業を開始する前に

- 60本のドライブを搭載したSG5760があります。SG5712を使用している場合は、デフォルトのDDPモードを使用する必要があります。
- StorageGRID に接続できるクライアントを使用している必要があります。
- クライアントにはがあります ["サポートされている Web ブラウザ"](#)。

手順

1. サービスラップトップでWebブラウザを開き、StorageGRID アプライアンスインストーラの+にアクセスします **`https://E5700SG_Controller_IP:8443`**

ここで *E5700SG_Controller_IP* E5700SGコントローラのいずれかのIPアドレスです。

2. 「* アドバンスト *」 > 「* RAID モード *」の順に選択します。
3. [Configure RAID Mode*] ページで、[Mode] ドロップダウンリストから目的の RAID モードを選択します。
4. [保存 (Save)] をクリックします。

関連情報

["NetApp E シリーズシステムのドキュメントのサイト"](#)

オプション：アプライアンスのネットワークポートの再マッピング

必要に応じて、アプライアンスノードの内部ポートを別の外部ポートに再マッピングできます。たとえば、ファイアウォールの問題が原因でポートの再マッピングが必要になることがあります。

作業を開始する前に

- 以前に StorageGRID アプライアンスインストーラにアクセスしていた場合。

このタスクについて

再マッピングされたポートをロードバランサエンドポイントに使用することはできません。再マッピングされたポートを削除する必要がある場合は、の手順に従います "[ポートの再マッピングを削除](#)"。

手順

1. StorageGRID アプライアンスインストーラで、**[ネットワークの設定]>[ポートの再マッピング]**を選択します。

Remap Port ページが表示されます。

2. Network * ドロップダウンボックスから、再マッピングするポートのネットワーク（Grid、Admin、または Client）を選択します。
3. **[Protocol]** ドロップダウンボックスから、IP プロトコルとして [TCP] または [UDP] を選択します。
4. **[* Remap Direction]** * ドロップダウンボックスから、このポートに再マッピングするトラフィック方向（インバウンド、アウトバウンド、または双方向）を選択します。
5. 「* Original Port *」に、再マッピングするポートの番号を入力します。
6. 「* mapped-to Port *」には、代わりに使用するポートの番号を入力します。
7. **[ルールの追加]**を選択します。

新しいポートマッピングがテーブルに追加され、新しいマッピングがただちに有効になります。

8. ポートマッピングを削除するには、削除するルールのラジオボタンを選択し、**[Remove Selected Rule]**を選択します。

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。