



# ハードウェア（ **SG6000** ）の設定 StorageGRID

NetApp  
September 04, 2024

# 目次

ハードウェア（SG6000）の設定.....	1
StorageGRID 接続（SG6000）の設定 .....	1
SANtricity System Manager（SG6000）へのアクセスと設定 .....	23
BMC インターフェイス（SG6000）の設定 .....	30
オプション：ノード暗号化を有効にします .....	37
オプション：RAID モードを変更（SG6000 のみ） .....	40
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 .....	41

# ハードウェア（SG6000）の設定

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する必要があります。SANtricity System Manager を設定する必要があります。これは、コントローラシェルフのストレージコントローラとその他のハードウェアを監視するためのソフトウェアです。また、SG6000-CN コントローラの BMC インターフェイスにアクセスできることを確認する必要があります。

## StorageGRID 接続（SG6000）の設定

StorageGRID アプライアンスをストレージノードとして StorageGRID システムに導入するには、アプライアンスと使用するネットワークの間の接続を設定する必要があります。ネットワークを設定するには、SG6000-CN コントローラ（コンピューティングコントローラ）に事前にインストールされている StorageGRID アプライアンスインストーラにアクセスします。

### 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。

#### 必要なもの

- 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。
- SG6000-CN コントローラは、使用するすべての StorageGRID ネットワークに接続されています。
- これらのネットワーク上の SG6000-CN 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には、DHCP によって SG6000-CN 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 アドレスを使用するか（コントローラが管理ネットワークに接続されている場合）、サービスラップトップを SG6000-CN コントローラに直接接続します。

#### 手順

1. 可能であれば、SG6000-CN コントローラの管理ネットワークポートの DHCP アドレスを使用して StorageGRID アプライアンスインストーラにアクセスします。



- a. SG6000-CN コントローラの前面にある 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 アドレスを特定するには、ラベルに記載された 16 進数に \* 2 \* を追加する必要があります。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 + **https://Appliance\_Controller\_IP:8443** を入力します

「SG6000 -CN\_Controller\_IP」の場合は、DHCP 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。

# NetApp® StorageGRID® Appliance Installer

[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](#)

2. 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。
  - a. イーサネットケーブルを使用して、サービ斯拉ップトップを 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。



- b. サービ斯拉ップトップで Web ブラウザを開きます。

c. StorageGRID アプライアンス・インストーラの URL +**https://169.254.0.1:8443** を入力します

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。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、アプライアンスの現在の接続状況によって異なります。



リンクローカル接続を介して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 169.254.0.2 と設定し、再試行してください。

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。

関連情報

[Web ブラウザの要件](#)

**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する必要があります。

必要なもの

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は、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・ファイルのサポート・ファイルは '.zip' アーカイブであり '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・バージョンが' 各コントローラ・タイプのサブディレクトリに格納されています

StorageGRID アプライアンス・ファイルのサポート・ファイルをダウンロードした後 '.zip' アーカイブを展開し 'README' ファイルを参照して 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を入手してください

5. の Upgrade Firmware ページの手順に従ってください [StorageGRID アプライアンスインストーラ](#) 次の手順を実行します。
  - a. コントローラタイプとチェックサムファイルに適し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。
  - 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. 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。

## ネットワークリンクの設定（SG6000シリーズ）

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。

### 必要なもの

アプライアンスノードをクローニングする場合は、ソースアプライアンスノードで使用されるすべてのリンクについて、ターゲットアプライアンスのネットワークリンクを設定します。

25GbE のリンク速度を使用する場合は、次の要件があります。

- SFP28 TwinAx ケーブルを使用するか、使用するネットワークポートに SFP28 トランシーバを取り付けておきます。
- この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。

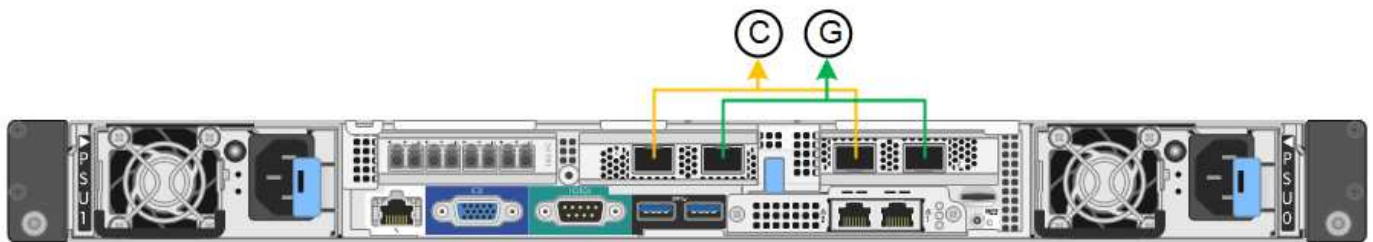
- この速度を使用するようにスイッチを設定する方法を理解しておきます。

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。

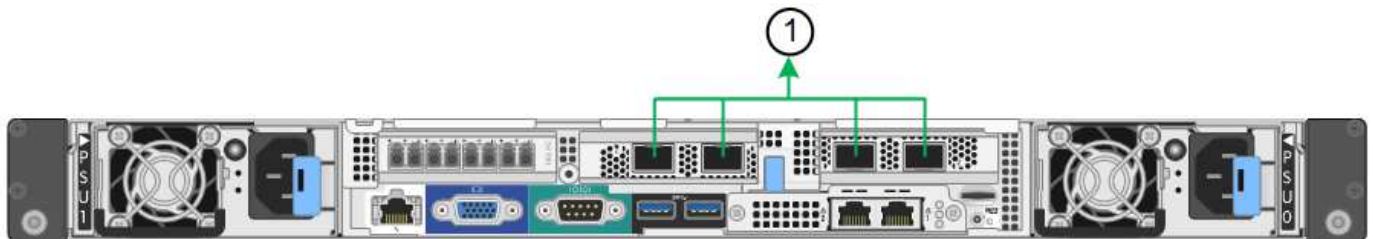
このタスクについて

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。デフォルトの設定は太字



で示しています。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。

・ \* 固定（デフォルト）ポートボンディングモード \*

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"> <li>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。</li> <li>ポート 1 と 3 は使用されません。</li> <li>VLAN タグはオプションです。</li> </ul>	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>両方のネットワークに VLAN タグを指定できます。</li> </ul>
LACP（ 802.3ad）	<ul style="list-style-type: none"> <li>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。</li> <li>ポート 1 と 3 は使用されません。</li> <li>VLAN タグはオプションです。</li> </ul>	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>両方のネットワークに VLAN タグを指定できます。</li> </ul>

・ \* アグリゲートポートボンディングモード \*

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"> <li>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。</li> <li>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。</li> </ul>	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>

を参照してください [SG6000-CN コントローラのポートボンディングモード](#) 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詳細については、[を参照してください](#)。

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。

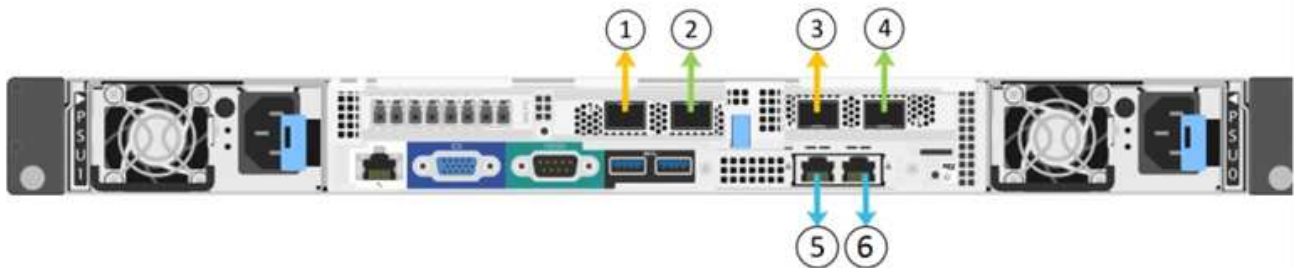


## 手順

1. StorageGRID アプライアンスインストーラから、 **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。

### Network Link Configuration



⚠ You might lose your connection if you make changes to the network or link you are connected through. If you are not reconnected within 1 minute, re-enter the URL using one of the other IP addresses assigned to the appliance.

Link Status テーブルには、番号が付けられたポートのリンクステート（アップ / ダウン）と速度（1/10/25 / 40/100Gbps）が表示されます。

### Link Status

Link	State	Speed (Gbps)
1	Up	100
2	Up	100
3	Down	N/A
4	Down	N/A
5	Up	1
6	Up	1

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。

### Link Settings

Link speed

Auto

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)

Enable VLAN (802.1q)  
tagging



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 port 5. Leave port 6 unconnected. If necessary, you can make a temporary direct Ethernet connection to port 6 and use 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



Enabling the Client Network causes the default gateway for this node to move to the Client Network. Before enabling the Client Network, ensure that you've added all necessary subnets to the Grid Network Subnet List. Otherwise, the connection to the node might be lost.

2. 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、リンク速度のドロップダウンリストから \* Auto \* 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。また、SFP28 TwinAx ケーブル、または光ケーブルと SFP28 トランシーバを使用する必要があります。

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。このネットワークは無効にできません。

- 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 \* チェックボックスの選択を解除します。

#### Admin Network

---

Enable network ☐

- 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オンにします。

これで、ネットワーク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 \* が選択されました。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

### 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.

### 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

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、他のいずれかの URL 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 [IP アドレス](#) アプライアンスに割り当てられています： `https://SG6000-CN_Controller_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。

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場合は、を参照してください [SG6000-CN コントローラのリンク設定を変更する手順](#)。

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。

### Grid Network

The Grid Network is used for all internal StorageGRID traffic. The Grid Network provides connectivity between all nodes in the grid, across all sites and subnets. All hosts on the Grid Network must be able to talk to all other hosts. The Grid Network can consist of multiple subnets. Networks containing critical grid services, such as NTP, can also be added as Grid subnets.

IP Assignment	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IPv4 Address (CIDR)	<input type="text" value="172.16.3.72/21"/>
Gateway	<input type="text" value="172.16.0.1"/>

 All required Grid Network subnets must also be defined in the Grid Network Subnet List on the Primary Admin Node before starting installation.

Subnets (CIDR)	<input type="text" value="172.18.0.0/21"/>	✗
	<input type="text" value="172.18.0.0/21"/>	✗
	<input type="text" value="192.168.0.0/21"/>	+ ✗
MTU	<input type="text" value="1500"/>	
<div><div>Cancel</div><div>Save</div></div>		



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、**+https://services\_appliance\_IP:8443** と入力します

- 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 **✕**。

- 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する必要があります。



## 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、**+https://services\_appliance:8443** と入力します

- 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は作成できません。

- 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は作成できません。

- 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 Client Network を有効にする必要があります。

## 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す。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し、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。

- 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。

- [ 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。

- [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し、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

Network: Grid

Destination IPv4 Address or FQDN:

Test MTU: ☐

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 \* チェックボックスをオンにして、ネットワーク経由でデスティネーションへのパス全体の 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	<input type="text" value="Grid"/>
Destination IPv4 Address or FQDN	<input type="text" value="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（SG6000）の設定](#)

[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。これらのポートの一覧については、StorageGRID ネットワークのガイドラインにあるポートリファレンスを参照してください。



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 11.6.1 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
<button>Test Connectivity</button>	

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、「Port connectivity test failed」というメッセージが赤い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。

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
```

## 関連情報

### ネットワークのガイドライン



# SANtricity System Manager（SG6000）へのアクセスと設定

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。

必要なもの

- 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の管理者権限またはルート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（11.70）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 内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 System Manager 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. 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



StorageGRID アプライアンスインストーラが使用できない場合やログインページが表示されない場合は、を使用する必要があります [ストレージコントローラの IP アドレス](#)。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。

[More \(10 total\) >](#)**1** Welcome**2** Verify Hardware**3** Verify Hosts**4** Select Applications**5** Define Workloads**6** Act

Welcome to the SANtricity® System Manager! With System Manager, you can...

- Configure your storage array and set up alerts.
- Monitor and troubleshoot any problems when they occur.
- Keep track of how your system is performing in real time.

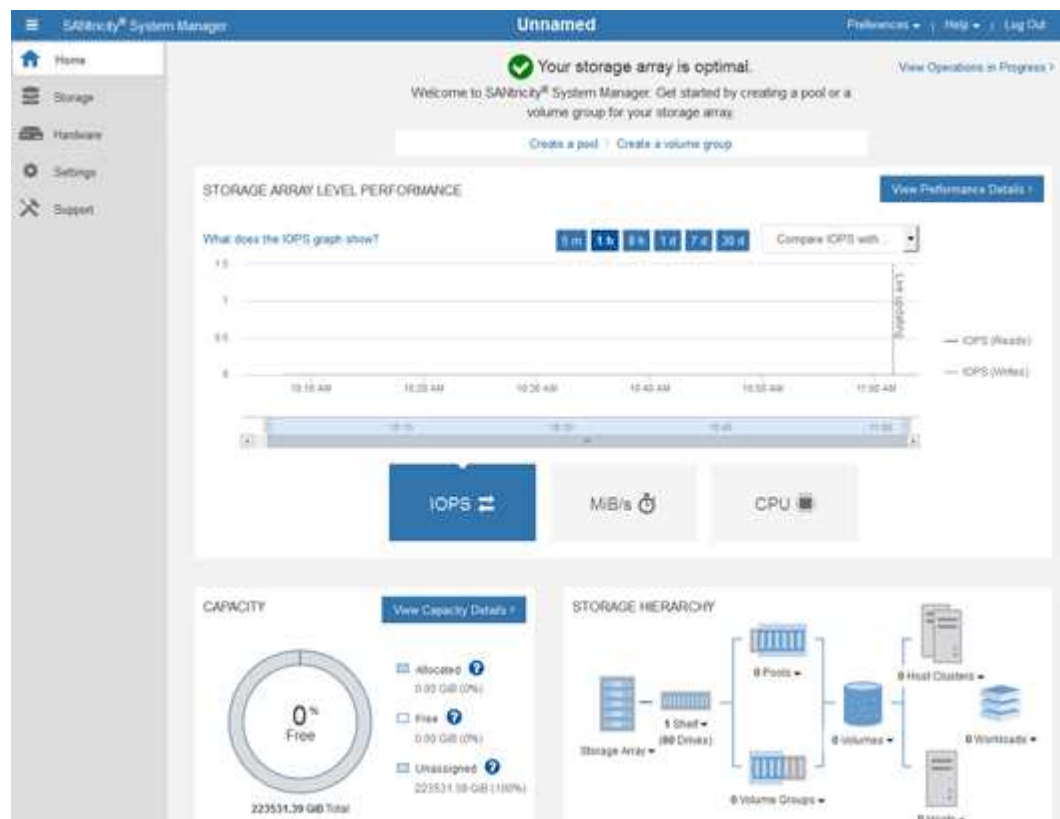
Cancel

Next &gt;

3. 「\* キャンセル \*」を選択してウィザードを閉じます。



StorageGRID アプライアンスにはセットアップ・ウィザードを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。

必要なもの

- 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を介して SANtricity システムマネージャ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ルート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（11.70）以降が必要です。

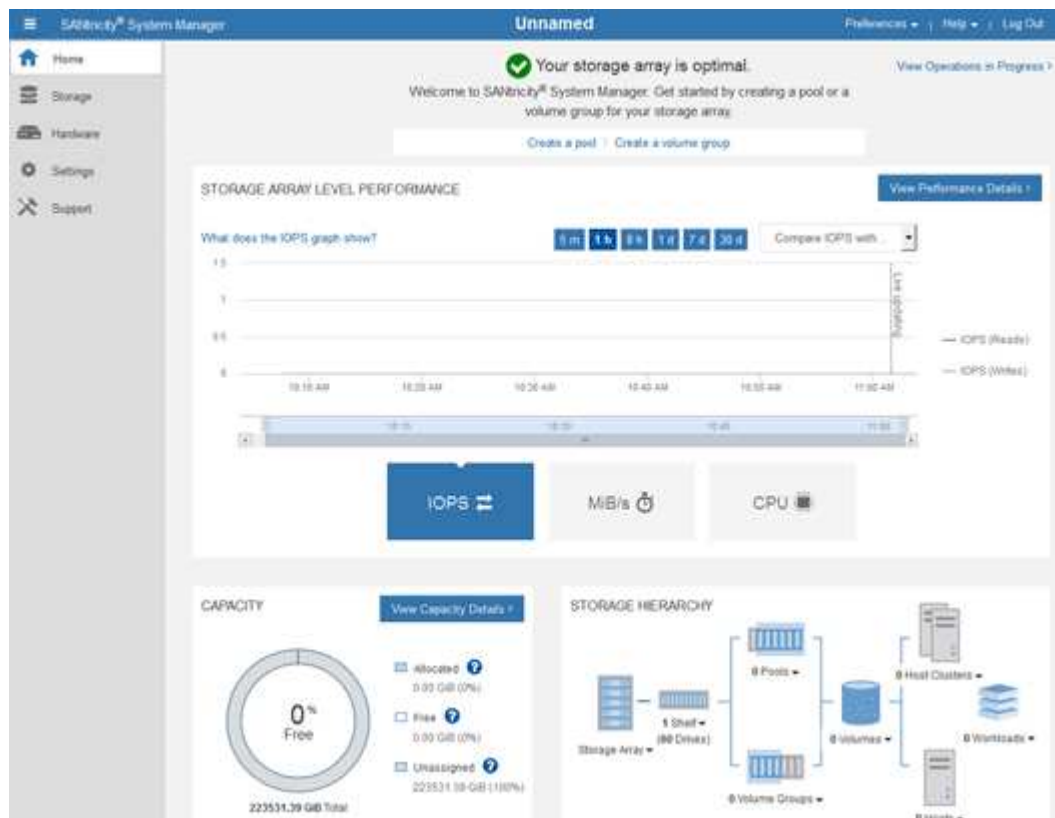


グリッドマネージャまたはアプライアンスインストーラから SANtricity システムマネージャにアクセスする方法は、通常、ハードウェアを監視して E シリーズ AutoSupport を設定することだけを目的としています。ファームウェアのアップグレードなど、SANtricity System Manager 内の多くの機能や操作は、StorageGRID アプライアンスの監視には適用されません。問題を回避するには、アプライアンスのハードウェアの設置とメンテナンスの手順に必ず従ってください。

## 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。

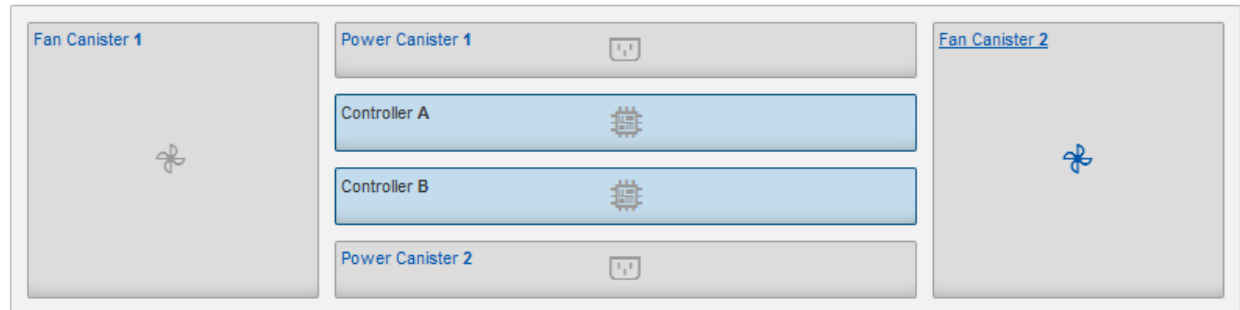
## HARDWARE

[Learn More >](#)

Legend ▾

☐ Show status icon details ?

Controller Shelf 99 ▾

[Show front of shelf](#)

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。

- 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。
- 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。
- [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、各ストレージコントローラの静的 IP アドレスを設定して、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への管理接続が失われないようにする必要があります。

### 必要なもの

- 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バラップトップに、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（\* アドバンスド \* > \* SANtricity システムマネージャ \*）またはグリッドマネージャ（\* ノード \* > \* 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 + **https://Appliance\_Controller\_IP:8443** と入力します

「Appliance\_Controller\_IP」の場合は、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	<input type="radio"/> Static <input checked="" type="radio"/> 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 : `https://Storage_Controller_IP*` として使用します

## BMC インターフェイス ( SG6000 ) の設定

SG6000-CN コントローラ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は、ハードウェアに関するステータス情報を提供し、SG6000-CN コントローラの SNMP 設定やその他のオプションを設定できます。

### BMC インターフェイスの root パスワードを変更します

セキュリティを確保するために、BMC の root ユーザのパスワードを変更する必要があります。

必要なもの

- 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

最初にアプライアンスをインストールすると、BMC は root ユーザ ( 「 root/calvin 」 ) のデフォルトパスワードを使用します。システムを保護するために、root ユーザのパスワードを変更する必要があります。

手順

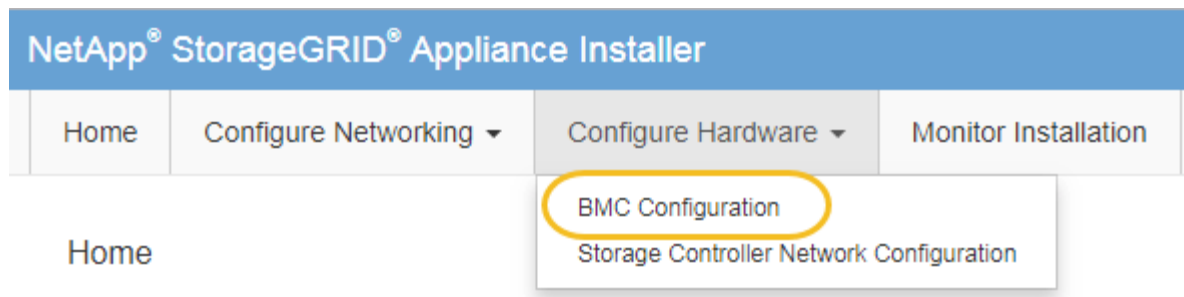
1. クライアントから、StorageGRID アプライアンス・インストーラの URL を + `https://Appliance_Controller_IP:8443` と入力します

「 `Appliance_Controller_IP` 」の場合は、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. 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。

## Baseboard Management Controller Configuration

### User Settings

Root Password	<input type="password" value="....."/>
Confirm Root Password	<input type="password" value="....."/>

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には、SG6000-CN コントローラの BMC 管理ポートの IP アドレスを設定する必要があります。

必要なもの

- 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](#)。
- 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。



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。

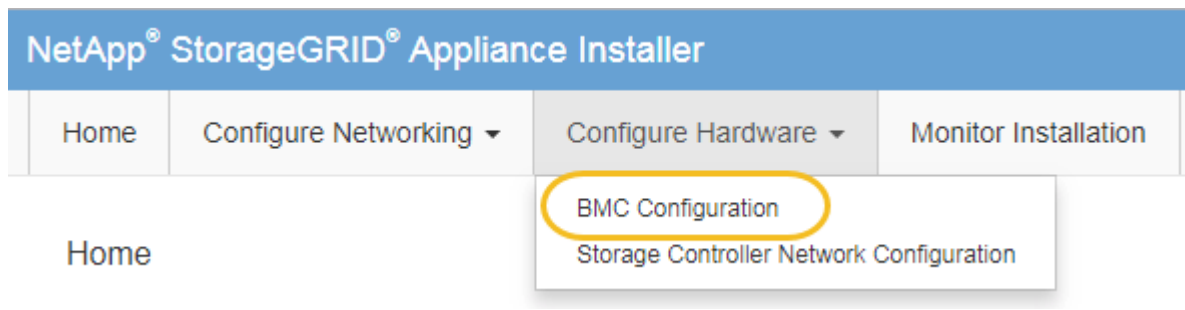
## 手順

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 **+https://SG6000-CN\_Controller\_IP:8443** と入力します

「SG6000-CN」の場合は、任意の StorageGRID ネットワークでアプライアンスの 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	d8:c4:97:28:50:62
IPv4 Address (CIDR)	10.224.3.225/21
Default gateway	10.224.0.1

Cancel	Save
--------	------

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

Cancel Save

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

BMC 管理ポートの DHCP または静的 IP アドレスを使用して、SG6000-CN コントローラの BMC インターフェイスにアクセスできます。

必要なもの

- SG6000-CN コントローラの 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。



- 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](#)。

手順

1. BMC インターフェイスの URL を入力します： **+https://BMC\_Port\_IP**

「 *BMC\_Port\_IP* 」の場合は、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。



「BMC\_Port\_IP」をまだ設定していない場合は、の手順に従います [BMC インターフェイス（SG6000）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が、SG6000-CN コントローラの前面のラベルに記載された BMC MAC に割り当てられた IP アドレスを指定できます。BMC ネットワークで DHCP が有効になっていない場合、BMC は数分後に応答せず、デフォルトの静的 IP アドレス 192.168.0.120 を割り当てます。「192.168.0.120」を参照するには、ラップトップを BMC ポートに直接接続し、ラップトップに「192.168.0.200/24」などの IP アドレスを割り当てるようにネットワーク設定を変更する必要がある場合があります。

2. root のユーザ名とパスワードを入力します。このときに設定したパスワードを使用します [デフォルトの root パスワードが変更されました](#)：

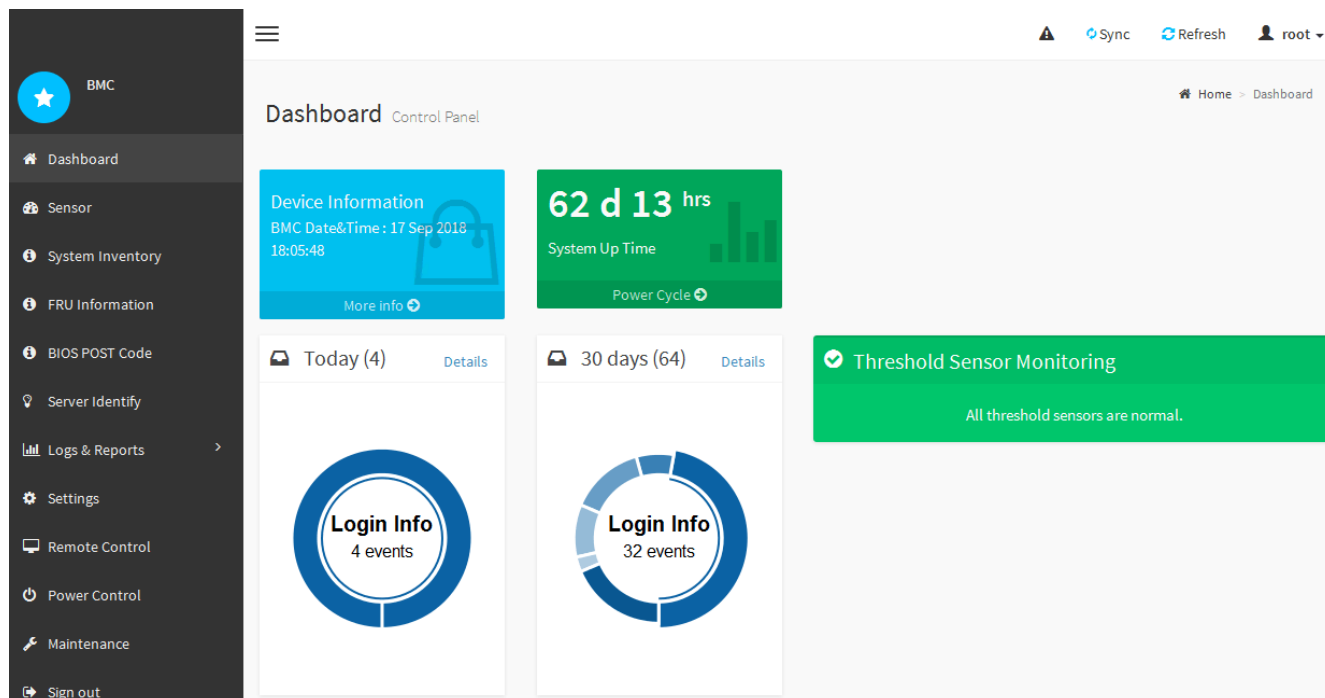


☐ Remember Username

Sign me in

[I forgot my password](#)

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。

## SG6000-CN コントローラの SNMP を設定します

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 SG6000-CN コントローラの 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。

### 必要なもの

- 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、SG6000-CN に障害が発生して交換する必要がある場合は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。

### 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ません。

SG6000-CN コントローラが異常な状態になったときに SNMP コンソールにすぐに通知を送信するには、トラップを有効にします。トラップは、さまざまなコンポーネントや温度のしきい値のハードウェア障害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。

## アラート用の E メール通知を設定します

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 宛先、アラートポリシー、およびイベントフィルタを設定する必要があります。



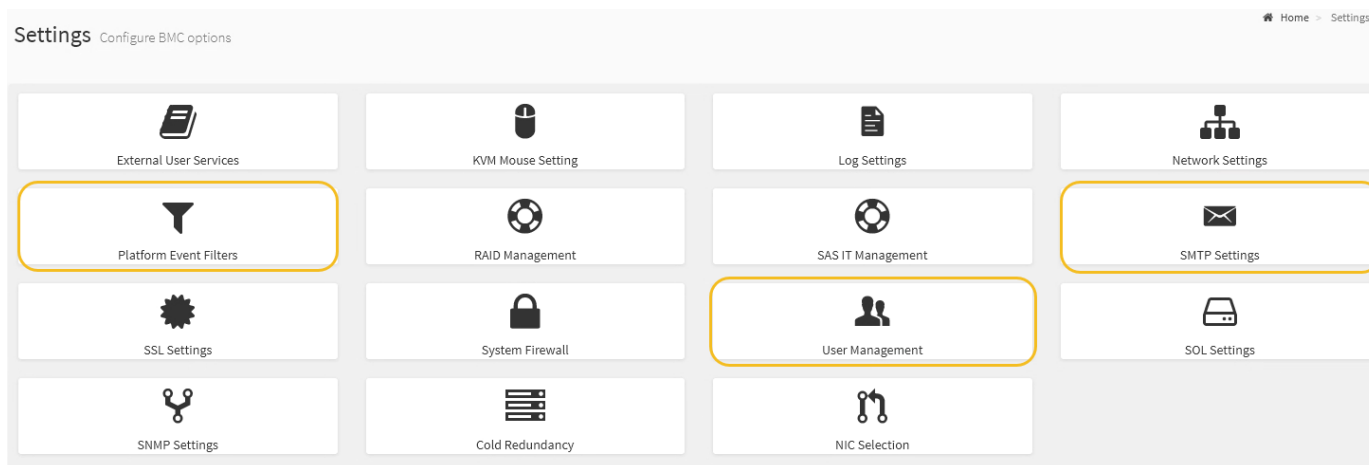
この手順で作成された BMC 設定は、SG6000-CN に障害が発生して交換する必要がある場合は保持されないことがあります。適用したすべての設定を記録し、必要に応じてハードウェアの交換後に簡単に再適用できるようにします。

### 必要なもの

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。



### 手順

- SMTP を設定します。
  - [ \* 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には、ユーザごとに LAN 宛先を追加する必要があります。
- 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。また、KMS 暗号化プロセスが開始されると、ノード暗号化の選択を解除できません。

#### 必要なもの

StorageGRID の管理手順の KMS に関する情報を確認します。

#### 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）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。



ノード暗号化が有効になっているアプライアンスで KMS に接続する前に存在するデータは、セキュアでない一時キーで暗号化されます。キーが KMS から提供される値に設定されるまで、アプライアンスの取り外しや盗難は防止されません。

ディスクの復号化に KMS キーが必要な場合を除いて、アプライアンス上のデータを取得することはできず、データが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。このキーにアクセスできなくなるのは、KMS の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を削除することで。

#### 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\* 」と入力します

「Controller\_IP」は、3 つの StorageGRID ネットワークのいずれか上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。



アプライアンスを KMS キーで暗号化すると、アプライアンスディスクを復号化する際に同じ KMS キーを使用する必要がなくなります。

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、データ損失のリスクなしにノード暗号化を有効にする \* を選択解除できます。インストールが開始されると、アプライアンスノードは StorageGRID システム内の KMS 暗号化キーにアクセスして、ディスク暗号化を開始します。アプライアンスのインストール後、ノード暗号化を無効にすることはできません。



KMS を含む 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すると、そのノードで KMS 暗号化を使用するの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。

関連情報

[StorageGRID の管理](#)

[メンテナンスモード \( SG6000 \) でのノード暗号化の監視](#)

## オプション：RAID モードを変更（SG6000 のみ）

アプライアンスでは、ストレージとリカバリの要件に応じて別の 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。

必要なもの

- 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](#)。

このタスクについて

アプライアンスをストレージノードとして導入する前に、次のいずれかのボリューム設定オプションを選択できます。

- **\* 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。RAID6 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も短く、管理も簡単です。



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。RAID6 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も短く、管理も簡単です。ストレージ効率は RAID6 と同等です。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。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。DDP よりもアプライアンスのストレージ効率を上げ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。

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\*」と入力します

「Controller\_IP」は、3 つの StorageGRID ネットワークのいずれか上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。

#### 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

アプライアンスストレージノードの内部ポートを別の外部ポートに再マッピングすることが必要になる場合があります。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。

#### 必要なもの

- 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。
- ロードバランサエンドポイントを設定しておらず、設定する予定もない状態である必要があります。



ポートを再マッピングする場合、同じポートを使用してロードバランサエンドポイントを設定することはできません。ポートを再マッピング済みの場合にロードバランサエンドポイントを設定するには、の手順を実行します [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から、 **Configure Networking** \* > Remap Port\* をクリックします。

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 \* ]** をクリックします。

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。

## Remap Ports

If required, you can remap the internal ports on the appliance Storage Node to different external ports. For example, you might need to remap ports because of a firewall issue.

✕ Remove Selected Rule

+ Add Rule

NetworkGridProtocolTCP

Remap DirectionInboundOriginal Port1

Mapped-To Port1

	Network	Protocol	Remap Direction	Original Port	Mapped-To Port
<input type="radio"/>	Grid	TCP	Bi-directional	1800	1801

8. ポートマッピングを削除するには、削除するルールオプションボタンを選択し、\* 選択したルールの削除 \* をクリックします。

## 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。