



BMC インターフェイスを設定しています

StorageGRID 11.5

NetApp
April 11, 2024

目次

BMCインターフェイスを設定しています	1
BMCインターフェイスのrootパスワードを変更しています	1
BMC管理ポートのIPアドレスを設定します	2
BMCインターフェイスへのアクセス	4
サービスアプライアンスのSNMPを設定します	6
アラート用のEメール通知の設定	6

BMC インターフェイスを設定しています

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、サービスアプライアンスで SNMP 設定やその他のオプションを設定できます。

手順

- "BMCインターフェイスのrootパスワードを変更しています"
- "BMC管理ポートのIPアドレスを設定します"
- "BMCインターフェイスへのアクセス"
- "サービスアプライアンスのSNMPを設定します"
- "アラート用のEメール通知の設定"

BMC インターフェイスのrootパスワードを変更しています

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サポートされているWebブラウザを使用している必要があります。

このタスクについて

初めてアプライアンスをインストールするとき、BMCではrootユーザのデフォルトパスワードが使用されます (root/calvin)。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。

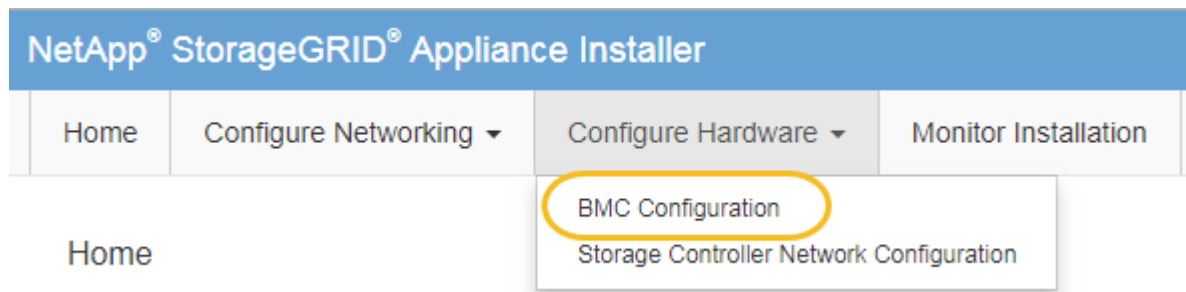
手順

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を入力します：+
https://services_appliance_IP:8443

の場合 `services_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. 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
Confirm Root Password

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、サービスアプライアンス上の 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サポートされているWebブラウザを使用している必要があります。
- 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。
- SG100 BMC 管理ポート *



- SG1000 BMC 管理ポート *



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。

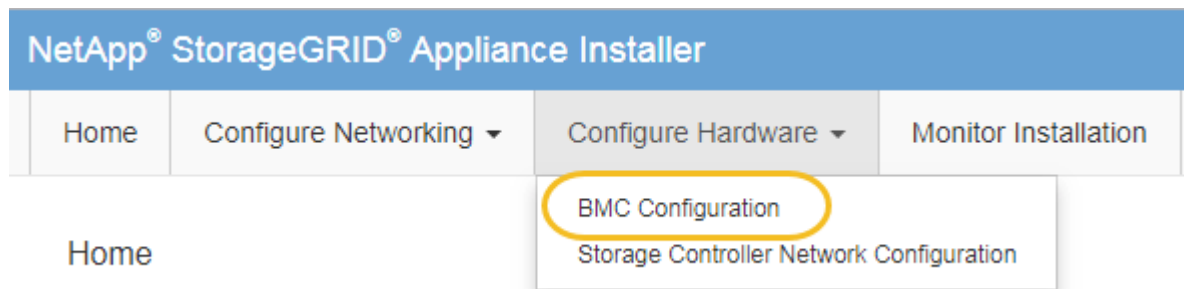
手順

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://services_appliance_IP:8443`

の場合 `services_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	d8:c4:97:28:50:62
IPv4 Address (CIDR)	10.224.3.225/21
Default gateway	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インターフェイスへのアクセス

BMC 管理ポートの DHCP または静的 IP アドレスを使用して、サービスアプライアンスの BMC インターフェイスにアクセスできます。

必要なもの

- 管理クライアントがサポートされているWebブラウザを使用している必要があります。
- サービスアプライアンスの 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必要があります。
- SG100 BMC 管理ポート *



- SG1000 BMC 管理ポート *



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。

2. rootのユーザ名とパスワードを入力します。デフォルトのrootパスワード+を変更したときに設定したパス

ワードを使用します **root**

password

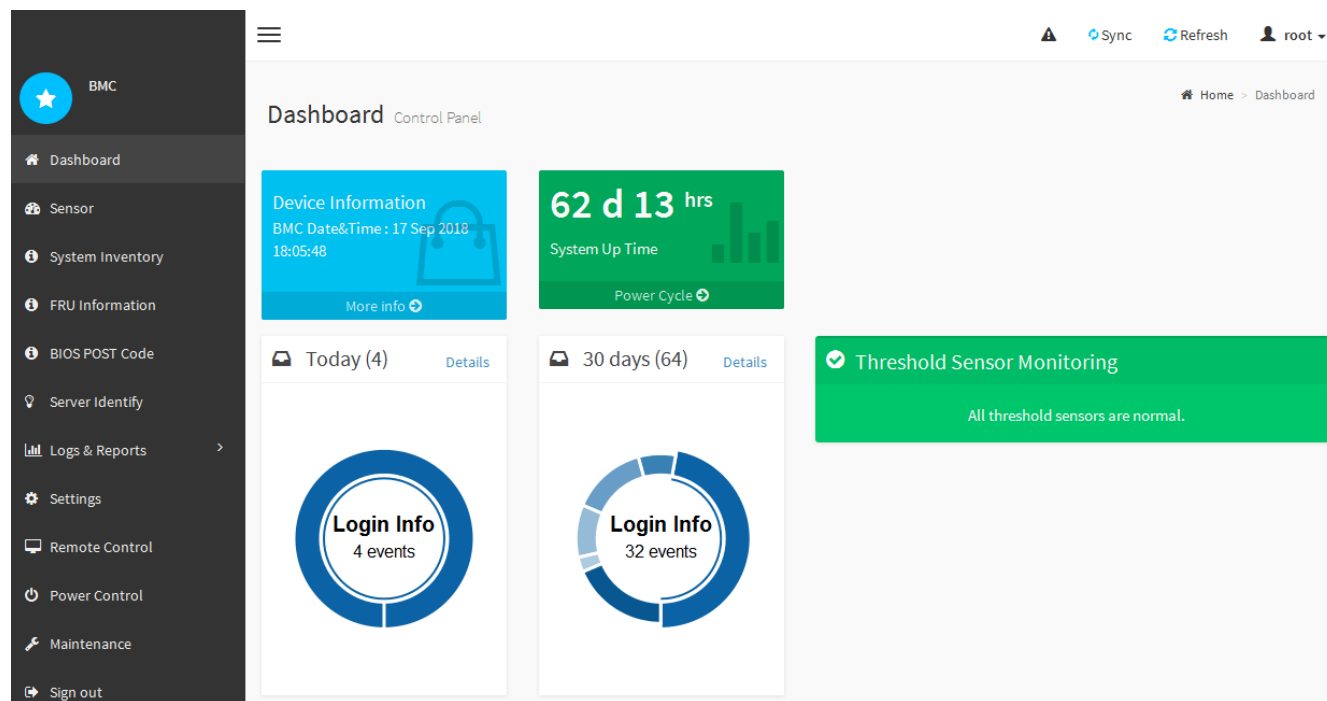


NetApp®

A login form with two input fields. The first field contains the text 'root'. The second field contains a password represented by seven dots. Below the fields is a checkbox labeled 'Remember Username' which is unchecked. A blue button labeled 'Sign me in' is positioned below the checkbox. Below the button is a link that says 'I forgot my password'.

3. [サインイン (Sign me in)]をクリックします

BMC ダッシュボードが表示されます。



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。

関連情報

["BMCインターフェイスのrootパスワードを変更しています"](#)

サービスアプライアンスの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。

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。

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。

3. 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。

サービスアプライアンスから SNMP コンソールが異常な状態になったときに通知をすぐに送信するには、トラップを有効にします。トラップは、リンクの稼働 / 停止状態、しきい値を超えた温度、トラフィックの増加を示している場合があります。

4. 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。
5. 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メール通知の設定

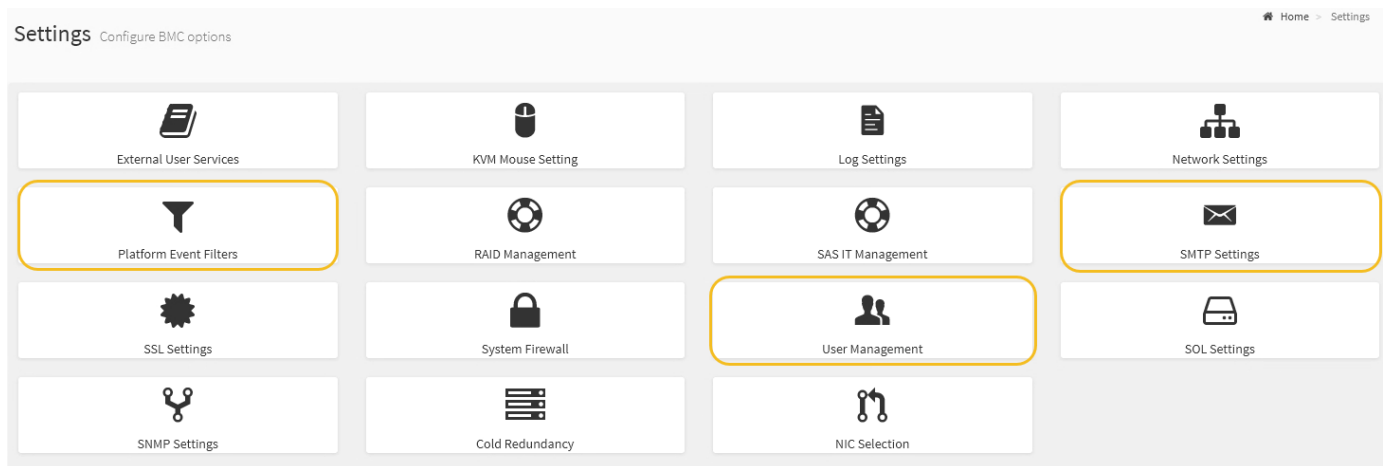
アラート発生時に E メール通知が送信されるようにするには、BMC インターフェイスを使用して SMTP 設定、ユーザ、LAN 宛先、アラートポリシー、およびイベントフィルタを設定する必要があります。

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

1. SMTP を設定します。

- [*設定* > *SMTP 設定*] を選択します。
- [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。

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

- [*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。
- 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。
- 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。

- [*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。

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。