



Configuration de l'interface BMC

StorageGRID 11.5

NetApp
April 11, 2024

Sommaire

- Configuration de l'interface BMC 1
 - Modification du mot de passe racine de l'interface BMC 1
 - Définition de l'adresse IP du port de gestion BMC..... 2
 - Accès à l'interface BMC 4
- Configuration des paramètres SNMP pour l'appliance de services 6
- Configuration des notifications par e-mail pour les alertes 6

Configuration de l'interface BMC

L'interface utilisateur du contrôleur de gestion de la carte mère (BMC) de l'appliance de services fournit des informations d'état sur le matériel et vous permet de configurer les paramètres SNMP et d'autres options pour l'appliance de services.

Étapes

- "Modification du mot de passe racine de l'interface BMC"
- "Définition de l'adresse IP du port de gestion BMC"
- "Accès à l'interface BMC"
- "Configuration des paramètres SNMP pour l'appliance de services"
- "Configuration des notifications par e-mail pour les alertes"

Modification du mot de passe racine de l'interface BMC

Pour des raisons de sécurité, vous devez modifier le mot de passe de l'utilisateur root du BMC.

Ce dont vous avez besoin

Le client de gestion utilise un navigateur Web pris en charge.

Description de la tâche

Lorsque vous installez l'appliance pour la première fois, le contrôleur BMC utilise un mot de passe par défaut pour l'utilisateur root (root/calvin). Vous devez modifier le mot de passe de l'utilisateur root pour sécuriser votre système.

Étapes

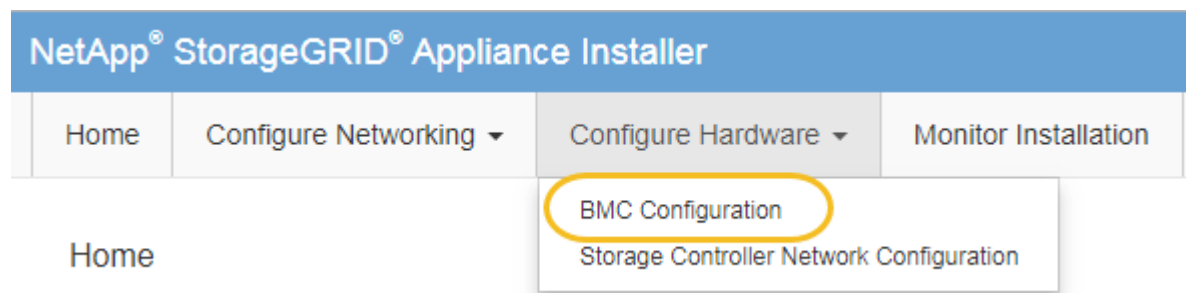
1. Dans le client, entrez l'URL du programme d'installation de l'appliance StorageGRID :

`https://services_appliance_IP:8443`

Pour `services_appliance_IP`, Utilisez l'adresse IP du serveur sur tout réseau StorageGRID.

La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

2. Sélectionnez **configurer le matériel > BMC Configuration**.



La page Configuration du contrôleur de gestion de la carte mère s'affiche.

3. Saisissez un nouveau mot de passe pour le compte racine dans les deux champs prévus à cet effet.

Baseboard Management Controller Configuration

User Settings

Root Password

.....

Confirm Root Password

.....

4. Cliquez sur **Enregistrer**.

Définition de l'adresse IP du port de gestion BMC

Avant de pouvoir accéder à l'interface BMC, vous devez configurer l'adresse IP du port de gestion BMC sur l'appliance de services.

Ce dont vous avez besoin

- Le client de gestion utilise un navigateur Web pris en charge.
- Vous utilisez n'importe quel client de gestion pouvant se connecter à un réseau StorageGRID.
- Le port de gestion BMC est connecté au réseau de gestion que vous souhaitez utiliser.

Port de gestion BMC SG100



Port de gestion BMC SG1000



Description de la tâche



Pour des raisons de prise en charge, le port de gestion BMC permet un accès matériel de faible niveau. Vous ne devez connecter ce port qu'à un réseau de gestion interne sécurisé, fiable et. Si aucun réseau de ce type n'est disponible, laissez le port BMC déconnecté ou bloqué, à moins qu'une connexion BMC ne soit demandée par le support technique.

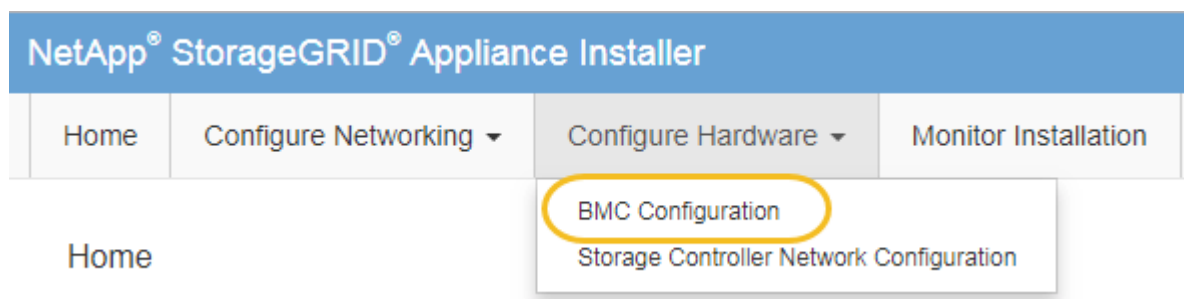
Étapes

1. Dans le client, entrez l'URL du programme d'installation de l'appliance StorageGRID :
`https://services_appliance_IP:8443`

Pour *services_appliance_IP*, Utilisez l'adresse IP du serveur sur tout réseau StorageGRID.

La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

2. Sélectionnez **configurer le matériel** > **BMC Configuration**.



La page Configuration du contrôleur de gestion de la carte mère s'affiche.

3. Notez l'adresse IPv4 qui s'affiche automatiquement.

DHCP est la méthode par défaut pour attribuer une adresse IP à ce port.



L'affichage des valeurs DHCP peut prendre quelques minutes.

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. Vous pouvez également définir une adresse IP statique pour le port de gestion BMC.



Vous devez attribuer une adresse IP statique au port de gestion BMC ou attribuer un bail permanent à l'adresse sur le serveur DHCP.

- Sélectionnez **statique**.
- Saisissez l'adresse IPv4 à l'aide de la notation CIDR.
- Saisissez la passerelle par défaut.

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. Cliquez sur **Enregistrer**.

L'application de vos modifications peut prendre quelques minutes.

Accès à l'interface BMC

Vous pouvez accéder à l'interface BMC sur le dispositif de services à l'aide du protocole DHCP ou de l'adresse IP statique du port de gestion BMC.

Ce dont vous avez besoin

- Le client de gestion utilise un navigateur Web pris en charge.
- Le port de gestion BMC de l'appliance de services est connecté au réseau de gestion que vous souhaitez utiliser.

Port de gestion BMC SG100



Port de gestion BMC SG1000



Étapes

1. Entrez l'URL de l'interface BMC :

`https://BMC_Port_IP`

Pour *BMC_Port_IP*, Utilisez l'adresse DHCP ou l'adresse IP statique pour le port de gestion BMC.

La page de connexion BMC s'affiche.

2. Entrez le nom d'utilisateur et le mot de passe racine en utilisant le mot de passe que vous avez défini

lorsque vous avez modifié le mot de passe root par défaut :

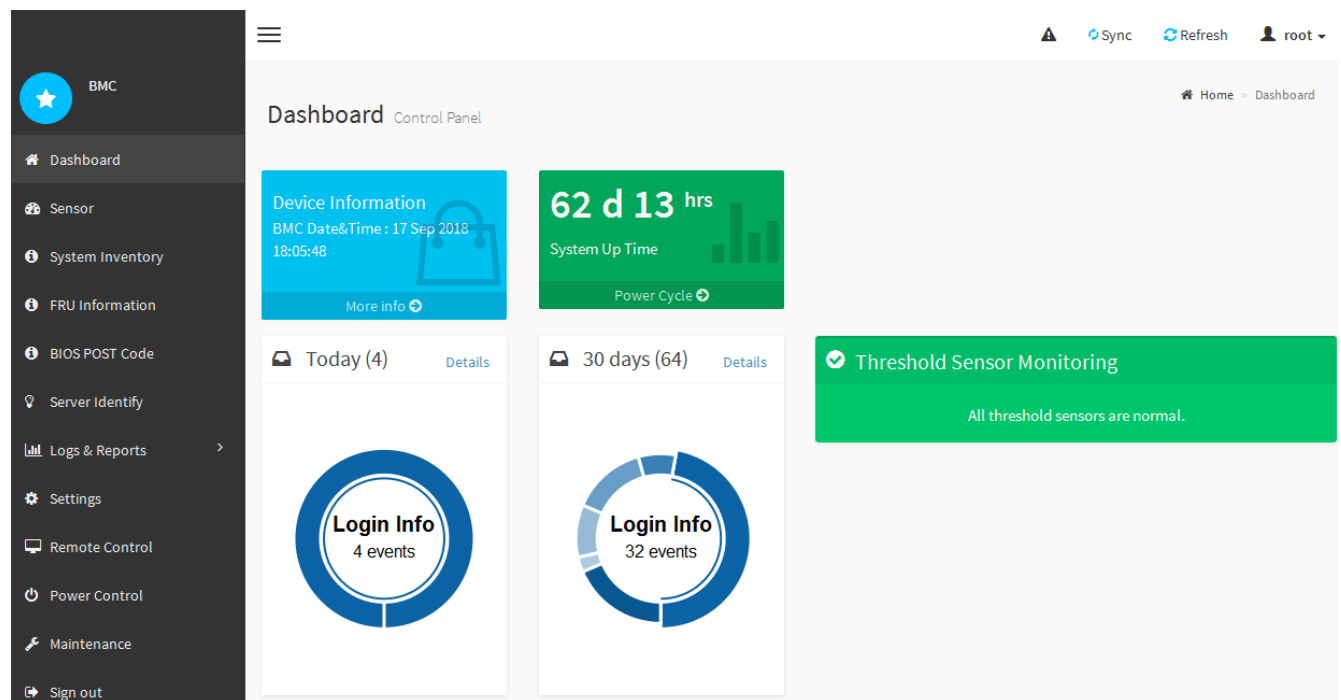
root

password

A login form for the NetApp BMC interface. It consists of a light gray box containing a username field with 'root' entered, a password field with masked characters '.....', and a checkbox labeled 'Remember Username'. Below the form is a blue 'Sign me in' button and a link 'I forgot my password'.

3. Cliquez sur **connexion**

Le tableau de bord BMC s'affiche.



4. Vous pouvez également créer d'autres utilisateurs en sélectionnant **Paramètres > gestion des utilisateurs** et en cliquant sur tout utilisateur « désactivé ».



Lorsque les utilisateurs se connectent pour la première fois, ils peuvent être invités à modifier leur mot de passe pour une sécurité accrue.

Informations associées

"Modification du mot de passe racine de l'interface BMC"

Configuration des paramètres SNMP pour l'appliance de services

Si vous êtes familier avec la configuration de SNMP pour le matériel, vous pouvez utiliser l'interface BMC pour configurer les paramètres SNMP pour l'appliance services. Vous pouvez fournir des chaînes de communauté sécurisées, activer le Trap SNMP et spécifier jusqu'à cinq destinations SNMP.

Ce dont vous avez besoin

- Vous savez comment accéder au tableau de bord BMC.
- Vous avez de l'expérience dans la configuration des paramètres SNMP pour les équipements SNMPv1-v2c.

Étapes

1. Dans le tableau de bord BMC, sélectionnez **Paramètres > Paramètres SNMP**.
2. Sur la page Paramètres SNMP, sélectionnez **Activer SNMP V1/V2**, puis fournissez une chaîne de communauté en lecture seule et une chaîne de communauté en lecture-écriture.

La chaîne de communauté en lecture seule est comme un ID utilisateur ou un mot de passe. Vous devez modifier cette valeur pour empêcher les intrus d'obtenir des informations sur la configuration de votre réseau. La chaîne de communauté lecture-écriture protège le périphérique contre les modifications non autorisées.

3. Vous pouvez également sélectionner **Activer le recouvrement** et saisir les informations requises.



Entrez l'adresse IP de destination pour chaque interruption SNMP utilisant une adresse IP. Les noms de domaine complets ne sont pas pris en charge.

Activez les traps si vous souhaitez que le dispositif de Services envoie des notifications immédiates à une console SNMP lorsqu'il est dans un état inhabituel. Les pièges peuvent indiquer des conditions de liaison vers le haut/bas, des températures dépassant certains seuils ou un trafic élevé.

4. Vous pouvez également cliquer sur **Envoyer piège de test** pour tester vos paramètres.
5. Si les paramètres sont corrects, cliquez sur **Enregistrer**.

Configuration des notifications par e-mail pour les alertes

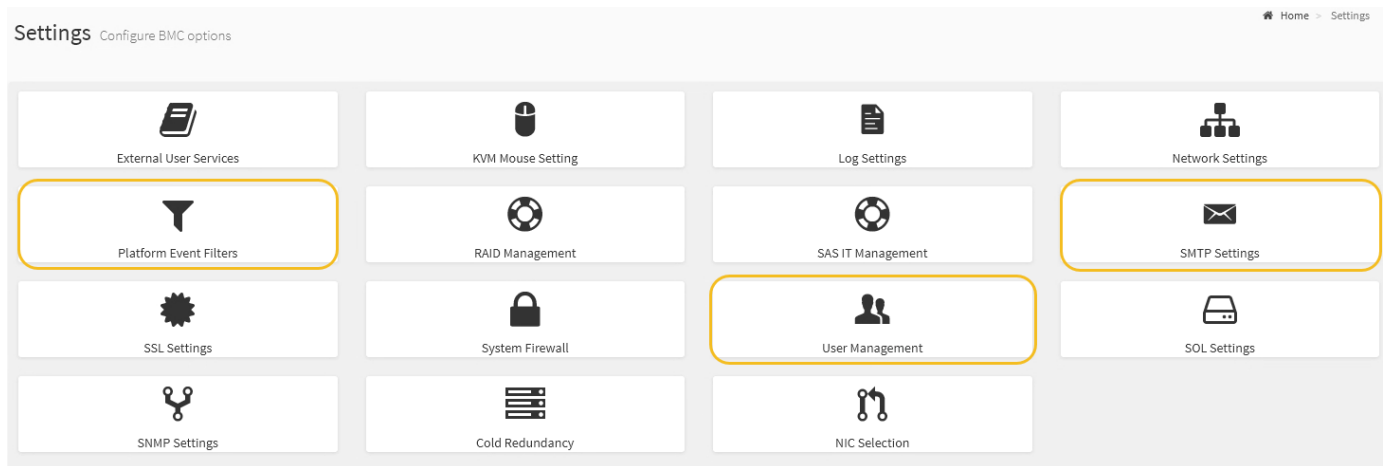
Si vous souhaitez que des notifications par e-mail soient envoyées lorsque des alertes se produisent, vous devez utiliser l'interface BMC pour configurer les paramètres SMTP, les utilisateurs, les destinations LAN, les stratégies d'alerte et les filtres d'événements.

Ce dont vous avez besoin

Vous savez comment accéder au tableau de bord BMC.

Description de la tâche

Dans l'interface BMC, vous utilisez les options **Paramètres SMTP**, **gestion des utilisateurs** et **filtres d'événements de la plate-forme** de la page Paramètres pour configurer les notifications par e-mail.



Étapes

1. Configurez les paramètres SMTP.

- Sélectionnez **Paramètres > Paramètres SMTP**.
- Pour l'ID e-mail de l'expéditeur, saisissez une adresse e-mail valide.

Cette adresse e-mail est fournie comme adresse de lorsque le contrôleur BMC envoie un e-mail.

2. Configurez les utilisateurs pour recevoir des alertes.

- Dans le tableau de bord BMC, sélectionnez **Paramètres > User Management**.
- Ajoutez au moins un utilisateur pour recevoir des notifications d'alerte.

L'adresse e-mail que vous configurez pour un utilisateur est l'adresse à laquelle le contrôleur BMC envoie des notifications d'alerte. Par exemple, vous pouvez ajouter un utilisateur générique, tel que « utilisateur de notification », et utiliser l'adresse électronique d'une liste de diffusion par courrier électronique de l'équipe d'assistance technique.

3. Configurez la destination du réseau local pour les alertes.

- Sélectionnez **Paramètres > filtres d'événements plateforme > destinations LAN**.
- Configurez au moins une destination LAN.
 - Sélectionnez **Email** comme Type de destination.
 - Pour le nom d'utilisateur BMC, sélectionnez un nom d'utilisateur que vous avez ajouté précédemment.
 - Si vous avez ajouté plusieurs utilisateurs et que vous souhaitez que tous les utilisateurs reçoivent des e-mails de notification, vous devez ajouter une destination LAN pour chaque utilisateur.
- Envoyer une alerte de test.

4. Configurez les règles d'alerte afin de définir le moment et l'emplacement d'envoi des alertes par le contrôleur BMC.

- Sélectionnez **Paramètres > filtres d'événements de plateforme > stratégies d'alerte**.

- b. Configurez au moins une règle d'alerte pour chaque destination LAN.
 - Pour Numéro de groupe de polices, sélectionnez **1**.
 - Pour l'action de police, sélectionnez **toujours envoyer l'alerte à cette destination**.
 - Pour le canal LAN, sélectionnez **1**.
 - Dans le sélecteur de destination, sélectionnez la destination LAN de la stratégie.
- 5. Configurez les filtres d'événements pour diriger les alertes pour différents types d'événements vers les utilisateurs appropriés.
 - a. Sélectionnez **Paramètres > filtres d'événements de plate-forme > filtres d'événements**.
 - b. Pour Numéro de groupe de police d'alerte, entrez **1**.
 - c. Créez des filtres pour chaque événement auquel vous souhaitez que le groupe de stratégies d'alerte soit averti.
 - Vous pouvez créer des filtres d'événements pour les actions de puissance, les événements de capteur spécifiques ou tous les événements.
 - Si vous n'êtes pas certain des événements à surveiller, sélectionnez **tous les capteurs** pour Type de capteur et **tous les événements** pour Options d'événements. Si vous recevez des notifications indésirables, vous pouvez modifier vos sélections ultérieurement.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.