



Configurare l'interfaccia BMC (SG100 e SG1000)

StorageGRID

NetApp
April 10, 2024

This PDF was generated from <https://docs.netapp.com/it-it/storagegrid-116/sg100-1000/changing-root-password-for-bmc-interface-sg1000.html> on April 10, 2024. Always check docs.netapp.com for the latest.

Sommario

- Configurare l'interfaccia BMC (SG100 e SG1000)..... 1
 - Modificare la password root per l'interfaccia BMC..... 1
 - Impostare l'indirizzo IP per la porta di gestione BMC 2
 - Accedere all'interfaccia BMC 4
 - Configurare le impostazioni SNMP per l'appliance di servizi..... 6
 - Imposta le notifiche via email per gli avvisi 7

Configurare l'interfaccia BMC (SG100 e SG1000)

L'interfaccia utente del BMC (Baseboard Management Controller) sull'appliance di servizi fornisce informazioni sullo stato dell'hardware e consente di configurare le impostazioni SNMP e altre opzioni per l'appliance di servizi.

Modificare la password root per l'interfaccia BMC

Per motivi di sicurezza, è necessario modificare la password dell'utente root del BMC.

Di cosa hai bisogno

Il client di gestione utilizza un [browser web supportato](#).

A proposito di questa attività

Quando si installa l'appliance per la prima volta, BMC utilizza una password predefinita per l'utente root (root/calvin). Per proteggere il sistema, è necessario modificare la password dell'utente root.

Fasi

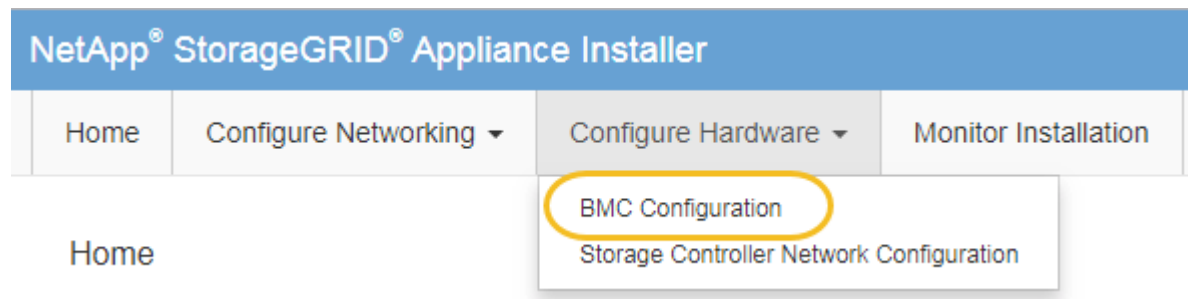
1. Dal client, immettere l'URL del programma di installazione dell'appliance StorageGRID:

`https://services_appliance_IP:8443`

Per `services_appliance_IP`, Utilizzare l'indirizzo IP dell'appliance su qualsiasi rete StorageGRID.

Viene visualizzata la pagina iniziale del programma di installazione dell'appliance StorageGRID.

2. Selezionare **Configura hardware** > **Configurazione BMC**.



Viene visualizzata la pagina Baseboard Management Controller Configuration.

3. Immettere una nuova password per l'account root nei due campi forniti.

Baseboard Management Controller Configuration

User Settings

Root Password
Confirm Root Password

4. Fare clic su **Save** (Salva).

Impostare l'indirizzo IP per la porta di gestione BMC

Prima di poter accedere all'interfaccia BMC, è necessario configurare l'indirizzo IP per la porta di gestione BMC sull'appliance di servizi.

Di cosa hai bisogno

- Il client di gestione utilizza un [browser web supportato](#).
- Si sta utilizzando qualsiasi client di gestione in grado di connettersi a una rete StorageGRID.
- La porta di gestione BMC è connessa alla rete di gestione che si intende utilizzare.

Porta di gestione BMC SG100



Porta di gestione BMC SG1000



A proposito di questa attività



A scopo di supporto, la porta di gestione BMC consente un accesso hardware di basso livello. Collegare questa porta solo a una rete di gestione interna sicura e affidabile. Se tale rete non è disponibile, lasciare la porta BMC disconnessa o bloccata, a meno che non venga richiesta una connessione BMC dal supporto tecnico.

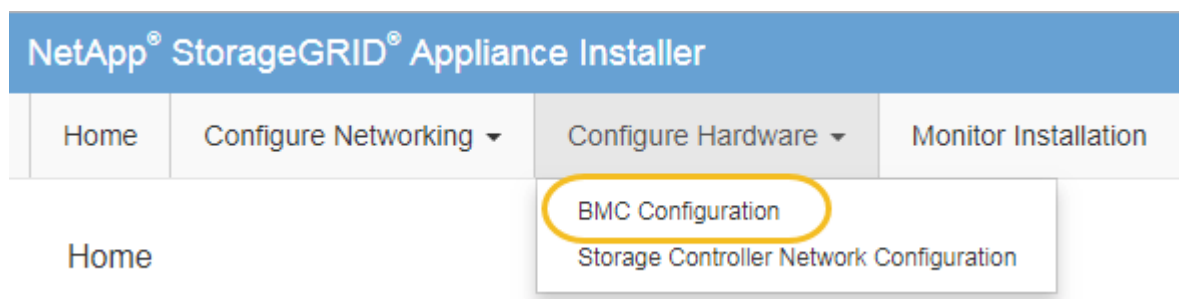
Fasi

1. Dal client, immettere l'URL del programma di installazione dell'appliance StorageGRID:
`https://services_appliance_IP:8443`

Per *services_appliance_IP*, Utilizzare l'indirizzo IP dell'appliance su qualsiasi rete StorageGRID.

Viene visualizzata la pagina iniziale del programma di installazione dell'appliance StorageGRID.

2. Selezionare **Configura hardware** > **Configurazione BMC**.



Viene visualizzata la pagina Baseboard Management Controller Configuration.

3. Annotare l'indirizzo IPv4 visualizzato automaticamente.

DHCP è il metodo predefinito per assegnare un indirizzo IP a questa porta.



La visualizzazione dei valori DHCP potrebbe richiedere alcuni minuti.

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. Facoltativamente, impostare un indirizzo IP statico per la porta di gestione BMC.



È necessario assegnare un indirizzo IP statico alla porta di gestione BMC o un lease permanente per l'indirizzo sul server DHCP.

- Selezionare **statico**.
- Inserire l'indirizzo IPv4 utilizzando la notazione CIDR.
- Inserire il gateway predefinito.

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. Fare clic su **Save** (Salva).

L'applicazione delle modifiche potrebbe richiedere alcuni minuti.

Accedere all'interfaccia BMC

È possibile accedere all'interfaccia BMC sul dispositivo di servizi utilizzando l'indirizzo IP statico o DHCP per la porta di gestione BMC.

Di cosa hai bisogno

- Il client di gestione utilizza un [browser web supportato](#).
- La porta di gestione BMC dell'appliance di servizi è connessa alla rete di gestione che si intende utilizzare.

Porta di gestione BMC SG100



Porta di gestione BMC SG1000



Fasi

1. Inserire l'URL dell'interfaccia BMC:

`https://BMC_Port_IP`

Per *BMC_Port_IP*, Utilizzare l'indirizzo IP statico o DHCP per la porta di gestione BMC.

Viene visualizzata la pagina di accesso BMC.



Se non hai ancora configurato BMC_Port_IP seguire le istruzioni riportate in [Configurare l'interfaccia BMC \(SG100/SG1000\)](#). Se non si riesce a seguire questa procedura a causa di un problema hardware e non si è ancora configurato un indirizzo IP BMC, potrebbe essere comunque possibile accedere al BMC. Per impostazione predefinita, il BMC ottiene un indirizzo IP utilizzando DHCP. Se DHCP è attivato sulla rete BMC, l'amministratore di rete può fornire l'indirizzo IP assegnato al BMC MAC, stampato sull'etichetta sulla parte anteriore del controller SG6000-CN. Se DHCP non è attivato sulla rete BMC, il BMC non risponderà dopo alcuni minuti e si assegnerà l'IP statico predefinito 192.168.0.120. Potrebbe essere necessario collegare il laptop direttamente alla porta BMC e modificare le impostazioni di rete per assegnare al laptop un indirizzo IP, ad esempio 192.168.0.200/24, per accedere a 192.168.0.120.

2. Inserire il nome utente root e la password, utilizzando la password impostata quando si modifica la password root predefinita:

root

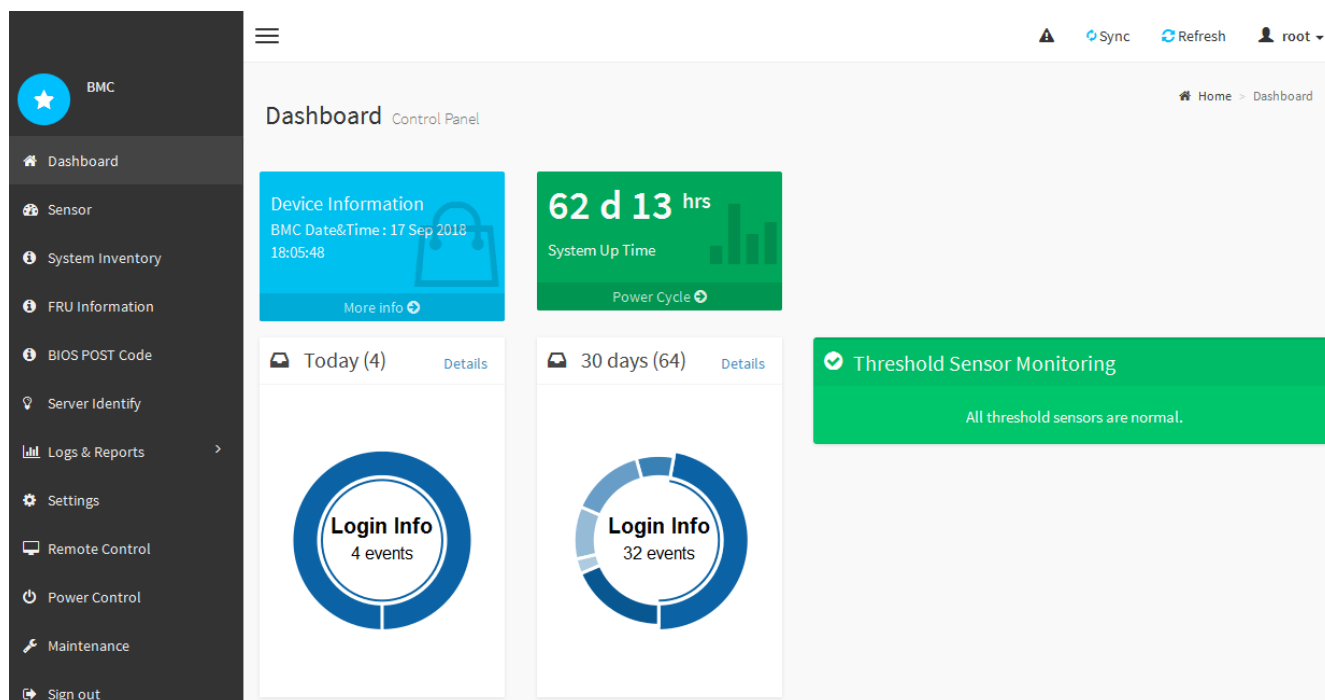
password



The image shows a login form for the NetApp BMC interface. It consists of a light gray rectangular box containing two input fields. The first field is labeled 'root' and contains the text 'root'. The second field is for the password, represented by a series of dots and a cursor. Below the password field is a checkbox labeled 'Remember Username'. At the bottom of the form is a blue button with the text 'Sign me in'. Below the button is a link that says 'I forgot my password'.

3. Fare clic su **Accedi**

Viene visualizzata la dashboard BMC.



4. Facoltativamente, creare utenti aggiuntivi selezionando **Impostazioni > Gestione utente** e facendo clic su qualsiasi utente “dabilitato”.



Quando gli utenti accedono per la prima volta, potrebbe essere richiesto di modificare la password per una maggiore sicurezza.

Informazioni correlate

[Modificare la password root per l'interfaccia BMC](#)

Configurare le impostazioni SNMP per l'appliance di servizi

Se si ha familiarità con la configurazione di SNMP per l'hardware, è possibile utilizzare l'interfaccia BMC per configurare le impostazioni SNMP per l'appliance di servizi. È possibile fornire stringhe di comunità sicure, attivare la trap SNMP e specificare fino a cinque destinazioni SNMP.

Di cosa hai bisogno

- Sai come accedere alla dashboard BMC.
- Hai esperienza nella configurazione delle impostazioni SNMP per le apparecchiature SNMPv1-v2c.



Le impostazioni BMC eseguite con questa procedura potrebbero non essere mantenute in caso di guasto dell'appliance e devono essere sostituite. Assicurarsi di disporre di una registrazione di tutte le impostazioni applicate, in modo che possano essere riapplicate facilmente dopo la sostituzione dell'hardware, se necessario.

Fasi

1. Dalla dashboard BMC, selezionare **Impostazioni > Impostazioni SNMP**.
2. Nella pagina SNMP Settings (Impostazioni SNMP), selezionare **Enable SNMP V1/V2** (attiva SNMP V1/V2*), quindi fornire una stringa di comunità di sola lettura e una stringa di comunità di lettura/scrittura.

La stringa di comunità di sola lettura è simile a un ID utente o a una password. Modificare questo valore per impedire agli intrusi di ottenere informazioni sulla configurazione di rete. La stringa di comunità Read-Write protegge il dispositivo da modifiche non autorizzate.

3. Facoltativamente, selezionare **Enable Trap** (attiva trap) e inserire le informazioni richieste.



Inserire l'IP di destinazione per ogni trap SNMP utilizzando un indirizzo IP. I nomi di dominio pienamente qualificati non sono supportati.

Attivare i trap se si desidera che l'appliance di servizi invii notifiche immediate a una console SNMP quando si trova in uno stato anomalo. Le trap potrebbero indicare condizioni di collegamento up/down, temperature superiori a determinate soglie o traffico elevato.

4. Facoltativamente, fare clic su **Send Test Trap** (Invia trap di test) per verificare le impostazioni.
5. Se le impostazioni sono corrette, fare clic su **Salva**.

Imposta le notifiche via email per gli avvisi

Se si desidera che le notifiche e-mail vengano inviate quando si verificano avvisi, è necessario utilizzare l'interfaccia BMC per configurare le impostazioni SMTP, gli utenti, le destinazioni LAN, i criteri di avviso e i filtri degli eventi.



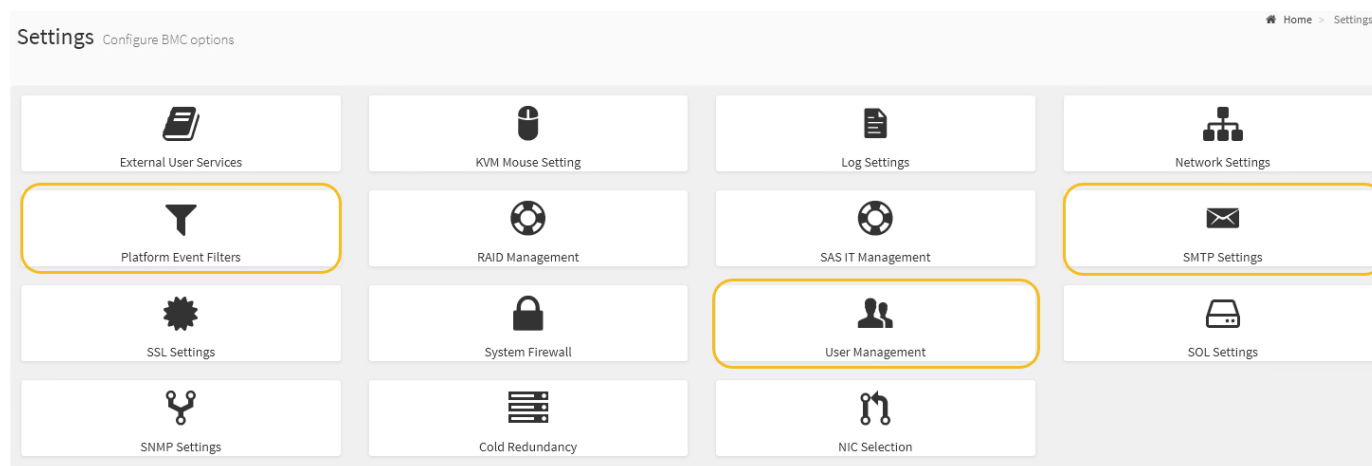
Le impostazioni BMC eseguite con questa procedura potrebbero non essere mantenute in caso di guasto dell'appliance e devono essere sostituite. Assicurarsi di disporre di una registrazione di tutte le impostazioni applicate, in modo che possano essere riapplicate facilmente dopo la sostituzione dell'hardware, se necessario.

Di cosa hai bisogno

Sai come accedere alla dashboard BMC.

A proposito di questa attività

Nell'interfaccia BMC, utilizzare le opzioni **Impostazioni SMTP**, **Gestione utente** e **Platform Event Filters** nella pagina Impostazioni per configurare le notifiche e-mail.



Fasi

1. Configurare le impostazioni SMTP.

- a. Selezionare **Impostazioni > Impostazioni SMTP**.
- b. Per l'ID e-mail mittente, immettere un indirizzo e-mail valido.

Questo indirizzo e-mail viene fornito come indirizzo di origine quando il BMC invia il messaggio e-mail.

2. Impostare gli utenti per la ricezione degli avvisi.

- a. Dalla dashboard BMC, selezionare **Impostazioni > Gestione utenti**.
- b. Aggiungere almeno un utente per ricevere le notifiche di avviso.

L'indirizzo e-mail configurato per un utente è l'indirizzo a cui il BMC invia le notifiche di avviso. Ad esempio, è possibile aggiungere un utente generico, ad esempio "notification-user," e utilizzare l'indirizzo e-mail di una lista di distribuzione e-mail del team di supporto tecnico.

3. Configurare la destinazione LAN per gli avvisi.

- a. Selezionare **Impostazioni > Platform Event Filters > Destinazioni LAN**.
- b. Configurare almeno una destinazione LAN.
 - Selezionare **Email** come tipo di destinazione.
 - Per BMC Username (Nome utente BMC), selezionare un nome utente aggiunto in precedenza.
 - Se sono stati aggiunti più utenti e si desidera che tutti ricevano e-mail di notifica, è necessario aggiungere una destinazione LAN per ciascun utente.
- c. Invia un avviso di test.

4. Configurare le policy di avviso in modo da definire quando e dove inviare gli avvisi da BMC.

- a. Selezionare **Impostazioni > Platform Event Filters > Alert Policies**.
- b. Configurare almeno un criterio di avviso per ciascuna destinazione LAN.
 - Per numero gruppo di criteri, selezionare **1**.
 - Per azione policy, selezionare **Invia sempre avviso a questa destinazione**.
 - Per il canale LAN, selezionare **1**.
 - In Destination Selector (selettore di destinazione), selezionare la destinazione LAN per il criterio.

5. Configurare i filtri degli eventi per indirizzare gli avvisi per diversi tipi di eventi agli utenti appropriati.

- a. Selezionare **Impostazioni > Platform Event Filters > Event Filters**.
- b. Per il numero gruppo di criteri di avviso, immettere **1**.
- c. Creare filtri per ogni evento di cui si desidera che venga inviata una notifica al gruppo di criteri di avviso.
 - È possibile creare filtri per eventi per azioni di alimentazione, eventi specifici dei sensori o tutti gli eventi.
 - In caso di dubbi sugli eventi da monitorare, selezionare **tutti i sensori** per tipo di sensore e **tutti gli eventi** per Opzioni evento. Se si ricevono notifiche indesiderate, è possibile modificare le selezioni in un secondo momento.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.