



# **Configurare l'hardware (SG6000)**

## **StorageGRID**

NetApp  
April 10, 2024

This PDF was generated from <https://docs.netapp.com/it-it/storagegrid-116/sg6000/accessing-storagegrid-appliance-installer-sg6000.html> on April 10, 2024. Always check docs.netapp.com for the latest.

# Sommario

- Configurare l'hardware (SG6000) ..... 1
  - Configurazione delle connessioni StorageGRID (SG6000)..... 1
  - Accesso e configurazione di Gestione di sistema SANtricity (SG6000) ..... 22
  - Configurare l'interfaccia BMC (SG6000) ..... 29
  - Facoltativo: Attivare la crittografia del nodo ..... 36
  - Opzionale: Modifica della modalità RAID (solo SG6000). .... 38
  - Opzionale: Consente di rimappare le porte di rete per l'appliance ..... 40

# Configurare l'hardware (SG6000)

Dopo aver alimentato l'appliance, è necessario configurare le connessioni di rete che verranno utilizzate da StorageGRID. È necessario configurare Gestore di sistema di SANtricity, che è il software che verrà utilizzato per monitorare i controller di storage e altro hardware nello shelf del controller. È inoltre necessario assicurarsi di poter accedere all'interfaccia BMC del controller SG6000-CN.

## Configurazione delle connessioni StorageGRID (SG6000)

Prima di poter implementare un'appliance StorageGRID come nodo di storage in un sistema StorageGRID, è necessario configurare le connessioni tra l'appliance e le reti che si intende utilizzare. È possibile configurare la rete consultando il programma di installazione dell'appliance StorageGRID, preinstallato sul controller SG6000-CN (il controller di calcolo).

### Accedere al programma di installazione dell'appliance StorageGRID

È necessario accedere al programma di installazione dell'appliance StorageGRID per verificare la versione del programma di installazione e configurare le connessioni tra l'appliance e le tre reti StorageGRID: Rete griglia, rete amministrativa (opzionale) e rete client (opzionale).

#### Di cosa hai bisogno

- Si sta utilizzando qualsiasi client di gestione in grado di connettersi alla rete amministrativa di StorageGRID o si dispone di un laptop di assistenza.
- Il laptop client o di servizio dispone di un browser Web supportato.
- Il controller SG6000-CN è collegato a tutte le reti StorageGRID che si intende utilizzare.
- Si conoscono l'indirizzo IP, il gateway e la subnet del controller SG6000-CN su queste reti.
- Sono stati configurati gli switch di rete che si intende utilizzare.

#### A proposito di questa attività

Per accedere inizialmente al programma di installazione dell'appliance StorageGRID, è possibile utilizzare l'indirizzo IP assegnato da DHCP per la porta della rete amministrativa sul controller SG6000-CN (supponendo che il controller sia collegato alla rete amministrativa) oppure collegare un laptop di assistenza direttamente al controller SG6000-CN.

#### Fasi

1. Se possibile, utilizzare l'indirizzo DHCP della porta di rete amministrativa del controller SG6000-CN per accedere al programma di installazione dell'appliance StorageGRID.



- a. Individuare l'etichetta dell'indirizzo MAC sulla parte anteriore del controller SG6000-CN e determinare l'indirizzo MAC della porta Admin Network.

L'etichetta dell'indirizzo MAC elenca l'indirizzo MAC per la porta di gestione BMC.

Per determinare l'indirizzo MAC della porta Admin Network, è necessario aggiungere **2** al numero esadecimale sull'etichetta. Ad esempio, se l'indirizzo MAC sull'etichetta termina con **09**, l'indirizzo MAC della porta di amministrazione terminerà con **0B**. Se l'indirizzo MAC sull'etichetta termina in **(y)FF**, l'indirizzo MAC per la porta di amministrazione terminerà in **(y+1)01**. È possibile eseguire facilmente questo calcolo aprendo Calculator in Windows, impostandolo sulla modalità Programmer, selezionando Hex, digitando l'indirizzo MAC e digitando **+ 2 =**.

- b. Fornire l'indirizzo MAC all'amministratore di rete, in modo che possa cercare l'indirizzo DHCP dell'appliance nella rete di amministrazione.
- c. Dal client, inserire questo URL per il programma di installazione dell'appliance StorageGRID:  
**`https://Appliance_Controller_IP:8443`**

Per *SG6000-CN\_Controller\_IP*, Utilizzare l'indirizzo DHCP.

- d. Se viene richiesto un avviso di protezione, visualizzare e installare il certificato utilizzando l'installazione guidata del browser.

L'avviso non verrà visualizzato al successivo accesso a questo URL.

Viene visualizzata la pagina iniziale del programma di installazione dell'appliance StorageGRID. Le informazioni e i messaggi visualizzati al primo accesso a questa pagina dipendono dalla modalità di connessione dell'appliance alle reti StorageGRID. Potrebbero essere visualizzati messaggi di errore che verranno risolti nelle fasi successive.

# 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. Se non è possibile ottenere un indirizzo IP utilizzando DHCP, è possibile utilizzare una connessione link-local.
  - a. Collegare un laptop di assistenza direttamente alla porta RJ-45 più a destra del controller SG6000-CN utilizzando un cavo Ethernet.



- b. Aprire un browser Web sul laptop di assistenza.
- c. Inserire questo URL per il programma di installazione dell'appliance StorageGRID:  
**https://169.254.0.1:8443**

Viene visualizzata la pagina iniziale del programma di installazione dell'appliance StorageGRID. Le informazioni e i messaggi visualizzati al primo accesso a questa pagina dipendono dalla modalità di connessione dell'appliance.



Se non è possibile accedere alla home page tramite una connessione link-local, configurare l'indirizzo IP del laptop di servizio come `169.254.0.2` e riprovare.

### Al termine

Dopo aver effettuato l'accesso al programma di installazione dell'appliance StorageGRID:

- Verificare che la versione del programma di installazione dell'appliance StorageGRID corrisponda alla versione software installata sul sistema StorageGRID. Se necessario, aggiornare il programma di installazione dell'appliance StorageGRID.

[Verificare e aggiornare la versione del programma di installazione dell'appliance StorageGRID](#)

- Esaminare tutti i messaggi visualizzati nella home page del programma di installazione dell'appliance StorageGRID e configurare la configurazione del collegamento e dell'IP, secondo necessità.

### Informazioni correlate

[Requisiti del browser Web](#)

## Verificare e aggiornare la versione del programma di installazione dell'appliance StorageGRID

La versione del programma di installazione dell'appliance StorageGRID deve corrispondere alla versione software installata sul sistema StorageGRID per garantire che tutte le funzioni StorageGRID siano supportate.

### Di cosa hai bisogno

È stato effettuato l'accesso al programma di installazione dell'appliance StorageGRID.

### A proposito di questa attività

Le appliance StorageGRID vengono fornite dalla fabbrica preinstallata con il programma di installazione dell'appliance StorageGRID. Se si aggiunge un'appliance a un sistema StorageGRID aggiornato di recente, potrebbe essere necessario aggiornare manualmente il programma di installazione dell'appliance StorageGRID prima di installare l'appliance come nuovo nodo.

Il programma di installazione dell'appliance StorageGRID viene aggiornato automaticamente quando si esegue l'aggiornamento a una nuova versione di StorageGRID. Non è necessario aggiornare il programma di installazione dell'appliance StorageGRID sui nodi dell'appliance installati. Questa procedura è necessaria solo quando si installa un'appliance che contiene una versione precedente del programma di installazione dell'appliance StorageGRID.

### Fasi

1. Dal programma di installazione dell'appliance StorageGRID, selezionare **Avanzate > Aggiorna firmware**.

2. Confrontare la versione corrente del firmware con la versione software installata sul sistema StorageGRID. (Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **About**).

La seconda cifra nelle due versioni deve corrispondere. Ad esempio, se il sistema StorageGRID utilizza la versione 11.6.x.y, la versione del programma di installazione dell'appliance StorageGRID deve essere 3.6.z.

3. Se l'appliance dispone di una versione precedente del programma di installazione dell'appliance StorageGRID, visitare il sito Web all'indirizzo "[Download NetApp: Appliance StorageGRID](#)".

Accedi con il nome utente e la password del tuo account NetApp.

4. Scaricare la versione appropriata del **file di supporto per le appliance StorageGRID** e il file checksum corrispondente.

Il file di supporto per il file delle appliance StorageGRID è un .zip Archivio che contiene le versioni firmware correnti e precedenti per tutti i modelli di appliance StorageGRID, in sottodirectory per ciascun tipo di controller.

Dopo aver scaricato il file di supporto per le appliance StorageGRID, estrarre .zip Archiviare e consultare il file Leggimi per informazioni importanti sull'installazione del programma di installazione dell'appliance StorageGRID.

5. Seguire le istruzioni riportate nella pagina Upgrade firmware di [Programma di installazione dell'appliance StorageGRID](#) per eseguire questa procedura:
  - a. Caricare il file di supporto appropriato (immagine del firmware) per il tipo di controller e il file checksum.
  - b. Aggiornare la partizione inattiva.
  - c. Riavviare e scambiare le partizioni.
  - d. Aggiornare la seconda partizione (inattiva).

## Configurazione dei collegamenti di rete (serie SG6000)

È possibile configurare i collegamenti di rete per le porte utilizzate per collegare l'appliance a Grid Network, Client Network e Admin Network. È possibile impostare la velocità di collegamento e le modalità di connessione di rete e porta.

### Di cosa hai bisogno

Se si esegue la clonazione di un nodo appliance, configurare i collegamenti di rete per l'appliance di destinazione per tutti i collegamenti utilizzati dal nodo dell'appliance di origine.

Se si intende utilizzare la velocità di collegamento a 25 GbE:

- Si utilizzano cavi twinax SFP28 o sono stati installati ricetrasmittitori SFP28 nelle porte di rete che si intende utilizzare.
- Le porte di rete sono state collegate a switch in grado di supportare queste funzioni.
- Si comprende come configurare gli switch per utilizzare questa velocità superiore.

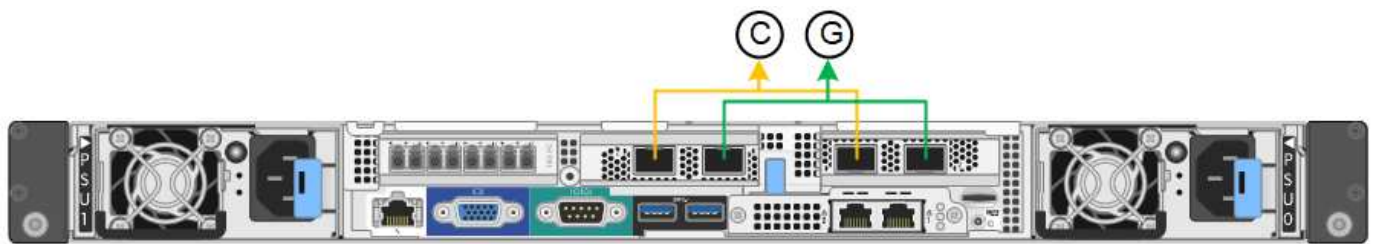
Se si intende utilizzare la modalità aggregate port bond, LACP network bond mode o tagging VLAN:

- Le porte di rete dell'appliance sono state collegate a switch in grado di supportare VLAN e LACP.

- Se nel bond LACP partecipano più switch, questi supportano i gruppi MLAG (Multi-chassis link Aggregation groups) o equivalenti.
- Si comprende come configurare gli switch per l'utilizzo di VLAN, LACP e MLAG o equivalente.
- Si conosce il tag VLAN univoco da utilizzare per ciascuna rete. Questo tag VLAN verrà aggiunto a ciascun pacchetto di rete per garantire che il traffico di rete venga instradato alla rete corretta.

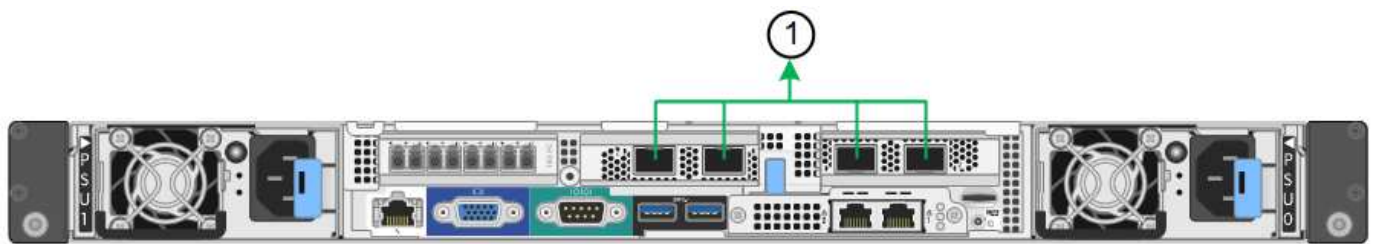
**A proposito di questa attività**

Questa figura mostra come le quattro porte di rete sono collegate in modalità Fixed Port Bond (configurazione predefinita).



Didascalia	Quali porte sono collegate
C.	Le porte 1 e 3 sono collegate tra loro per la rete client, se viene utilizzata questa rete.
G	Le porte 2 e 4 sono collegate tra loro per la rete Grid.

Questa figura mostra come le quattro porte di rete sono collegate in modalità aggregate port bond.



Didascalia	Quali porte sono collegate
1	Tutte e quattro le porte sono raggruppate in un unico collegamento LACP, consentendo l'utilizzo di tutte le porte per il traffico Grid Network e Client Network.

Le tabelle riepilogano le opzioni per la configurazione delle quattro porte di rete. Le impostazioni predefinite sono visualizzate in grassetto. Se si desidera utilizzare un'impostazione non predefinita, è necessario configurare le impostazioni nella pagina di configurazione del collegamento.

- **Modalità port bond fissa (predefinita)**



Network bond mode (modalità bond di)	Client Network disabled (rete client disattivata) (impostazione predefinita)	Rete client abilitata
Active-Backup (impostazione predefinita)	<ul style="list-style-type: none"> <li>Le porte 2 e 4 utilizzano un bond di backup attivo per Grid Network.</li> <li>Le porte 1 e 3 non vengono utilizzate.</li> <li>Un tag VLAN è opzionale.</li> </ul>	<ul style="list-style-type: none"> <li>Le porte 2 e 4 utilizzano un bond di backup attivo per Grid Network.</li> <li>Le porte 1 e 3 utilizzano un bond di backup attivo per la rete client.</li> <li>I tag VLAN possono essere specificati per entrambe le reti.</li> </ul>
LACP (802.3ad)	<ul style="list-style-type: none"> <li>Le porte 2 e 4 utilizzano un collegamento LACP per la rete Grid.</li> <li>Le porte 1 e 3 non vengono utilizzate.</li> <li>Un tag VLAN è opzionale.</li> </ul>	<ul style="list-style-type: none"> <li>Le porte 2 e 4 utilizzano un collegamento LACP per la rete Grid.</li> <li>Le porte 1 e 3 utilizzano un collegamento LACP per la rete client.</li> <li>I tag VLAN possono essere specificati per entrambe le reti.</li> </ul>

#### • Aggregate port bond mode

Network bond mode (modalità bond di)	Client Network disabled (rete client disattivata) (impostazione predefinita)	Rete client abilitata
Solo LACP (802.3ad)	<ul style="list-style-type: none"> <li>Le porte 1-4 utilizzano un unico collegamento LACP per la rete Grid.</li> <li>Un singolo tag VLAN identifica i pacchetti Grid Network.</li> </ul>	<ul style="list-style-type: none"> <li>Le porte 1-4 utilizzano un unico collegamento LACP per Grid Network e Client Network.</li> <li>Due tag VLAN consentono di separare i pacchetti Grid Network dai pacchetti Client Network.</li> </ul>

Vedere [Modalità Port Bond per controller SG6000-CN](#) per ulteriori informazioni sulle modalità port bond e network bond.

Questa figura mostra come le due porte di gestione 1-GbE sul controller SG6000-CN sono collegate in modalità bond di rete Active-Backup per la rete di amministrazione.

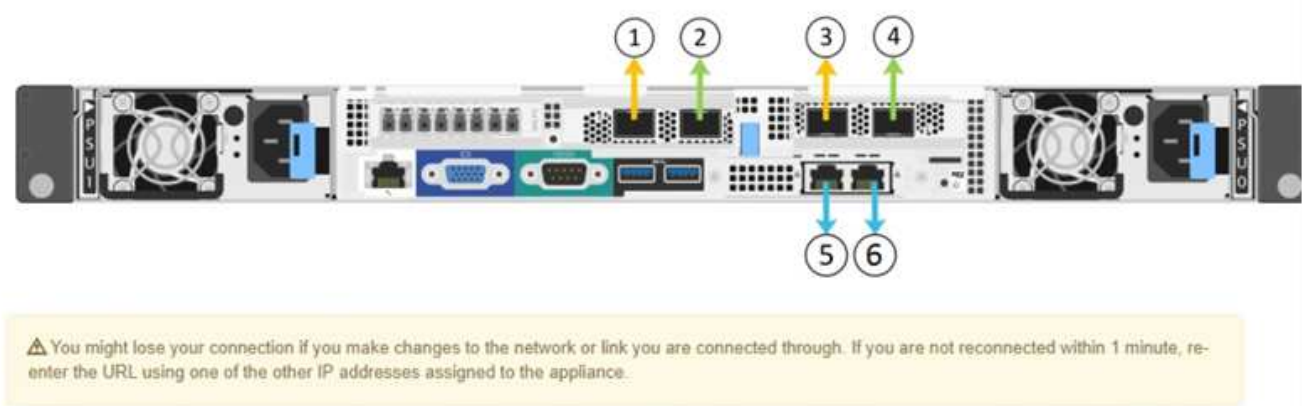


#### Fasi

1. Dal programma di installazione dell'appliance StorageGRID, fare clic su **Configura rete Configurazione del collegamento**.

La pagina Network link Configuration (Configurazione collegamento di rete) visualizza un diagramma dell'appliance con le porte di rete e di gestione numerate.

Network Link Configuration



La tabella link Status (Stato collegamento) elenca lo stato del collegamento (su/giù) e la velocità (1/10/25/40/100 Gbps) delle porte numerate.

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

La prima volta che si accede a questa pagina:

- **Velocità di collegamento** impostata su **Auto**.
- **Port bond mode** è impostato su **Fixed**.
- **Network bond mode** è impostato su **Active-Backup** per Grid Network.
- L'opzione **Admin Network** (rete amministrativa) è attivata e la modalità Network bond (bond di rete) è impostata su **Independent** (indipendente).
- La **rete client** è disattivata.

## 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. Se si intende utilizzare la velocità di collegamento 25-GbE per le porte di rete, selezionare **Auto** dall'elenco a discesa velocità di collegamento.

Anche gli switch di rete utilizzati per la rete di rete e la rete client devono supportare ed essere configurati per questa velocità. È necessario utilizzare cavi twinax SFP28 o cavi ottici e ricetrasmittitori SFP28.

3. Attivare o disattivare le reti StorageGRID che si intende utilizzare.

La rete grid è obbligatoria. Non è possibile disattivare questa rete.

- a. Se l'appliance non è connessa alla rete di amministrazione, deselezionare la casella di controllo **Enable network** (attiva rete) per la rete di amministrazione.

#### **Admin Network**

---

Enable network ☐

- b. Se l'appliance è connessa alla rete client, selezionare la casella di controllo **Enable network** (attiva rete) per la rete client.

Vengono visualizzate le impostazioni di rete del client per le porte di rete.

4. Fare riferimento alla tabella e configurare la modalità Port bond e la modalità Network bond.

Questo esempio mostra:

- **Aggregate** e **LACP** selezionati per le reti Grid e Client. È necessario specificare un tag VLAN univoco per ciascuna rete. È possibile selezionare valori compresi tra 0 e 4095.
- **Active-Backup** selezionato per la rete di amministrazione.

**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. Una volta selezionate le opzioni desiderate, fare clic su **Save** (Salva).



La connessione potrebbe andare persa se sono state apportate modifiche alla rete o al collegamento tramite il quale si è connessi. Se non si riesce a riconnettersi entro 1 minuto, immettere nuovamente l'URL del programma di installazione dell'appliance StorageGRID utilizzando uno degli altri [Indirizzi IP](#) assegnato all'appliance: **https://SG6000-CN\_Controller\_IP:8443**

## Configurare gli indirizzi IP StorageGRID

Il programma di installazione dell'appliance StorageGRID consente di configurare gli indirizzi IP e le informazioni di routing utilizzati per il nodo di storage dell'appliance nella rete StorageGRID, nell'amministratore e nelle reti client.

### A proposito di questa attività

È necessario assegnare un indirizzo IP statico all'appliance su ciascuna rete connessa o un lease permanente per l'indirizzo sul server DHCP.

Se si desidera modificare la configurazione del collegamento, consultare [Istruzioni per modificare la configurazione del collegamento del controller SG6000-CN](#).

### Fasi

1. Nel programma di installazione dell'appliance StorageGRID, selezionare **Configura rete > Configurazione IP**.

Viene visualizzata la pagina IP Configuration (Configurazione IP).

2. Per configurare Grid Network, selezionare **Static** o **DHCP** nella sezione **Grid Network** della pagina.

#### 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 ☒ Static ☐ DHCP

IPv4 Address (CIDR)

172.16.3.72/21

Gateway

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)

172.18.0.0/21

✕

172.18.0.0/21

✕

192.168.0.0/21

+ ✕

MTU

1500



Cancel

Save

3. Se si seleziona **Static**, attenersi alla seguente procedura per configurare la rete di rete:

- a. Inserire l'indirizzo IPv4 statico utilizzando la notazione CIDR.
- b. Accedere al gateway.

Se la rete non dispone di un gateway, immettere nuovamente lo stesso indirizzo IPv4 statico.

- c. Se si desidera utilizzare i frame jumbo, impostare il campo MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito 1500.



Il valore MTU della rete deve corrispondere al valore configurato sulla porta dello switch a cui è connesso il nodo. In caso contrario, potrebbero verificarsi problemi di performance di rete o perdita di pacchetti.



Per ottenere le migliori performance di rete, tutti i nodi devono essere configurati con valori MTU simili sulle interfacce Grid Network. L'avviso **Grid Network MTU mismatch** (mancata corrispondenza MTU rete griglia) viene attivato se si verifica una differenza significativa nelle impostazioni MTU per Grid Network su singoli nodi. I valori MTU non devono essere uguali per tutti i tipi di rete.

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

Quando si modifica l'indirizzo IP, anche il gateway e l'elenco delle subnet potrebbero cambiare.

Se si perde la connessione al programma di installazione dell'appliance StorageGRID, immettere nuovamente l'URL utilizzando il nuovo indirizzo IP statico appena assegnato. Ad esempio, **https://services\_appliance\_IP:8443**

- e. Verificare che l'elenco delle subnet Grid Network sia corretto.

Se si dispone di subnet Grid, è necessario il gateway Grid Network. Tutte le subnet della griglia specificate devono essere raggiungibili tramite questo gateway. Queste subnet della rete di griglia devono essere definite anche nell'elenco subnet della rete di griglia sul nodo di amministrazione primario quando si avvia l'installazione di StorageGRID.



Il percorso predefinito non è elencato. Se la rete client non è attivata, il percorso predefinito utilizzerà il gateway Grid Network.

- Per aggiungere una subnet, fare clic sull'icona di inserimento **+** a destra dell'ultima voce.
- Per rimuovere una subnet inutilizzata, fare clic sull'icona di eliminazione **x**.

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

4. Se è stato selezionato **DHCP**, attenersi alla seguente procedura per configurare Grid Network:

- a. Dopo aver selezionato il pulsante di opzione **DHCP**, fare clic su **Save** (Salva).

I campi **IPv4 Address**, **Gateway** e **subnet** vengono compilati automaticamente. Se il server DHCP è impostato per assegnare un valore MTU, il campo **MTU** viene popolato con tale valore e il campo diventa di sola lettura.

Il browser Web viene reindirizzato automaticamente al nuovo indirizzo IP del programma di installazione dell'appliance StorageGRID.

b. Verificare che l'elenco delle subnet Grid Network sia corretto.

Se si dispone di subnet Grid, è necessario il gateway Grid Network. Tutte le subnet della griglia specificate devono essere raggiungibili tramite questo gateway. Queste subnet della rete di griglia devono essere definite anche nell'elenco subnet della rete di griglia sul nodo di amministrazione primario quando si avvia l'installazione di StorageGRID.



Il percorso predefinito non è elencato. Se la rete client non è attivata, il percorso predefinito utilizzerà il gateway Grid Network.

- Per aggiungere una subnet, fare clic sull'icona di inserimento **+** a destra dell'ultima voce.
- Per rimuovere una subnet inutilizzata, fare clic sull'icona di eliminazione **x**.

c. Se si desidera utilizzare i frame jumbo, impostare il campo MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito 1500.



Il valore MTU della rete deve corrispondere al valore configurato sulla porta dello switch a cui è connesso il nodo. In caso contrario, potrebbero verificarsi problemi di performance di rete o perdita di pacchetti.



Per ottenere le migliori performance di rete, tutti i nodi devono essere configurati con valori MTU simili sulle interfacce Grid Network. L'avviso **Grid Network MTU mismatch** (mancata corrispondenza MTU rete griglia) viene attivato se si verifica una differenza significativa nelle impostazioni MTU per Grid Network su singoli nodi. I valori MTU non devono essere uguali per tutti i tipi di rete.

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

5. Per configurare la rete amministrativa, selezionare **Static** o **DHCP** nella sezione **Admin Network** della pagina.



Per configurare la rete di amministrazione, è necessario attivare la rete di amministrazione nella pagina link Configuration (Configurazione collegamento).



## 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. Se si seleziona **Static**, attenersi alla seguente procedura per configurare la rete amministrativa:
  - a. Inserire l'indirizzo IPv4 statico, utilizzando la notazione CIDR, per la porta di gestione 1 sull'appliance.

La porta di gestione 1 si trova a sinistra delle due porte RJ45 da 1 GbE sul lato destro dell'appliance.
  - b. Accedere al gateway.

Se la rete non dispone di un gateway, immettere nuovamente lo stesso indirizzo IPv4 statico.
  - c. Se si desidera utilizzare i frame jumbo, impostare il campo MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito 1500.



Il valore MTU della rete deve corrispondere al valore configurato sulla porta dello switch a cui è connesso il nodo. In caso contrario, potrebbero verificarsi problemi di performance di rete o perdita di pacchetti.

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

Quando si modifica l'indirizzo IP, anche il gateway e l'elenco delle subnet potrebbero cambiare.

Se si perde la connessione al programma di installazione dell'appliance StorageGRID, immettere nuovamente l'URL utilizzando il nuovo indirizzo IP statico appena assegnato. Ad esempio, **https://services\_appliance:8443**

- e. Verificare che l'elenco delle subnet Admin Network sia corretto.

Verificare che tutte le subnet possano essere raggiunte utilizzando il gateway fornito.



Non è possibile eseguire il percorso predefinito per utilizzare il gateway Admin Network.

- Per aggiungere una subnet, fare clic sull'icona di inserimento **+** a destra dell'ultima voce.
- Per rimuovere una subnet inutilizzata, fare clic sull'icona di eliminazione **x**.

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

7. Se è stato selezionato **DHCP**, attenersi alla seguente procedura per configurare la rete amministrativa:

a. Dopo aver selezionato il pulsante di opzione **DHCP**, fare clic su **Save** (Salva).

I campi **IPv4 Address**, **Gateway** e **subnet** vengono compilati automaticamente. Se il server DHCP è impostato per assegnare un valore MTU, il campo **MTU** viene popolato con tale valore e il campo diventa di sola lettura.

Il browser Web viene reindirizzato automaticamente al nuovo indirizzo IP del programma di installazione dell'appliance StorageGRID.

b. Verificare che l'elenco delle subnet Admin Network sia corretto.

Verificare che tutte le subnet possano essere raggiunte utilizzando il gateway fornito.



Non è possibile eseguire il percorso predefinito per utilizzare il gateway Admin Network.

- Per aggiungere una subnet, fare clic sull'icona di inserimento **+** a destra dell'ultima voce.
- Per rimuovere una subnet inutilizzata, fare clic sull'icona di eliminazione **x**.

c. Se si desidera utilizzare i frame jumbo, impostare il campo MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito 1500.



Il valore MTU della rete deve corrispondere al valore configurato sulla porta dello switch a cui è connesso il nodo. In caso contrario, potrebbero verificarsi problemi di performance di rete o perdita di pacchetti.

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

8. Per configurare la rete client, selezionare **Static** o **DHCP** nella sezione **Client Network** della pagina.



Per configurare la rete client, è necessario attivare la rete client nella pagina link Configuration (Configurazione collegamento).

## 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. Se si seleziona **Static** (statico), attenersi alla seguente procedura per configurare la rete client:

- Inserire l'indirizzo IPv4 statico utilizzando la notazione CIDR.
- Fare clic su **Save** (Salva).
- Verificare che l'indirizzo IP del gateway di rete client sia corretto.



Se la rete client è attivata, viene visualizzato il percorso predefinito. Il percorso predefinito utilizza il gateway di rete client e non può essere spostato in un'altra interfaccia mentre la rete client è attivata.

- Se si desidera utilizzare i frame jumbo, impostare il campo MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito 1500.



Il valore MTU della rete deve corrispondere al valore configurato sulla porta dello switch a cui è connesso il nodo. In caso contrario, potrebbero verificarsi problemi di performance di rete o perdita di pacchetti.

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

10. Se si seleziona **DHCP**, seguire questa procedura per configurare la rete client:

- Dopo aver selezionato il pulsante di opzione **DHCP**, fare clic su **Save** (Salva).

I campi **IPv4 Address** e **Gateway** vengono compilati automaticamente. Se il server DHCP è impostato per assegnare un valore MTU, il campo **MTU** viene popolato con tale valore e il campo diventa di sola lettura.

Il browser Web viene reindirizzato automaticamente al nuovo indirizzo IP del programma di installazione

dell'appliance StorageGRID.

- a. Verificare che il gateway sia corretto.



Se la rete client è attivata, viene visualizzato il percorso predefinito. Il percorso predefinito utilizza il gateway di rete client e non può essere spostato in un'altra interfaccia mentre la rete client è attivata.

- b. Se si desidera utilizzare i frame jumbo, impostare il campo MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito 1500.



Il valore MTU della rete deve corrispondere al valore configurato sulla porta dello switch a cui è connesso il nodo. In caso contrario, potrebbero verificarsi problemi di performance di rete o perdita di pacchetti.

## Verificare le connessioni di rete

Verificare che sia possibile accedere alle reti StorageGRID utilizzate dall'appliance. Per convalidare il routing attraverso i gateway di rete, è necessario verificare la connettività tra il programma di installazione dell'appliance StorageGRID e gli indirizzi IP su diverse subnet. È inoltre possibile verificare l'impostazione MTU.

### Fasi

1. Dalla barra dei menu del programma di installazione dell'appliance StorageGRID, fare clic su **Configura rete > Test ping e MTU**.

Viene visualizzata la pagina Ping and MTU Test (Test Ping e MTU).

#### 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. Dalla casella a discesa **Network** (rete), selezionare la rete che si desidera testare: Grid (rete), Admin (Amministratore) o Client (Client).
3. Inserire l'indirizzo IPv4 o il nome di dominio completo (FQDN) per un host su tale rete.

Ad esempio, è possibile eseguire il ping del gateway sulla rete o sul nodo di amministrazione primario.

4. Facoltativamente, selezionare la casella di controllo **Test MTU** per verificare l'impostazione MTU per l'intero percorso attraverso la rete verso la destinazione.

Ad esempio, è possibile verificare il percorso tra il nodo dell'appliance e un nodo di un altro sito.

5. Fare clic su **Test Connectivity** (verifica connettività).

Se la connessione di rete è valida, viene visualizzato il messaggio "Test ping superato", con l'output del comando ping elencato.

### 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
```

### Informazioni correlate

[Configurazione dei collegamenti di rete \(SG6000\)](#)

[Modificare l'impostazione MTU](#)

## Verificare le connessioni di rete a livello di porta

Per garantire che l'accesso tra il programma di installazione dell'appliance StorageGRID e gli altri nodi non sia ostacolato da firewall, verificare che il programma di installazione dell'appliance StorageGRID sia in grado di connettersi a una porta TCP o a un set di porte specifico all'indirizzo IP o all'intervallo di indirizzi specificati.

## A proposito di questa attività

Utilizzando l'elenco delle porte fornito nel programma di installazione dell'appliance StorageGRID, è possibile verificare la connettività tra l'appliance e gli altri nodi della rete grid.

Inoltre, è possibile verificare la connettività sulle reti Admin e Client e sulle porte UDP, ad esempio quelle utilizzate per server NFS o DNS esterni. Per un elenco di queste porte, consultare il riferimento alle porte nelle linee guida per la rete StorageGRID.



Le porte della rete griglia elencate nella tabella di connettività delle porte sono valide solo per StorageGRID versione 11.6.0. Per verificare quali porte sono corrette per ciascun tipo di nodo, consultare sempre le linee guida di rete per la versione di StorageGRID in uso.

## Fasi

1. Dal programma di installazione dell'appliance StorageGRID, fare clic su **Configura rete > Test di connettività della porta (nmap)**.

Viene visualizzata la pagina Port Connectivity Test (Test connettività porta).

La tabella di connettività delle porte elenca i tipi di nodo che richiedono la connettività TCP sulla rete Grid. Per ciascun tipo di nodo, la tabella elenca le porte Grid Network che devono essere accessibili all'appliance.

È possibile verificare la connettività tra le porte dell'appliance elencate nella tabella e gli altri nodi della rete Grid.

2. Dal menu a discesa **Network** (rete), selezionare la rete che si desidera testare: **Grid**, **Admin** o **Client**.
3. Specificare un intervallo di indirizzi IPv4 per gli host su tale rete.

Ad esempio, è possibile verificare il gateway sulla rete o sul nodo di amministrazione primario.

Specificare un intervallo utilizzando un trattino, come illustrato nell'esempio.

4. Inserire un numero di porta TCP, un elenco di porte separate da virgole o un intervallo di porte.

**Port Connectivity Test**

Network: Grid

IPv4 Address Ranges: 10.224.6.160-161

Port Ranges: 22,2022

Protocol: ☒ TCP ☐ UDP

**Test Connectivity**

5. Fare clic su **Test Connectivity** (verifica connettività).
- Se le connessioni di rete a livello di porta selezionate sono valide, viene visualizzato il messaggio "Port Connectivity test passed" (Test di connettività porta superato) in un banner verde. L'output del comando nmap è elencato sotto il banner.

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
```

- Se viene stabilita una connessione di rete a livello di porta all'host remoto, ma l'host non è in ascolto su una o più porte selezionate, viene visualizzato il messaggio "Port Connectivity test failed" (Test di connettività porta non riuscito) in un banner giallo. L'output del comando nmap è elencato sotto il banner.

Tutte le porte remote che l'host non sta ascoltando hanno uno stato "chiuso". Ad esempio, questo banner giallo potrebbe essere visualizzato quando il nodo a cui si sta tentando di connettersi è preinstallato e il servizio NMS StorageGRID non è ancora in esecuzione su tale nodo.

 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
```

- Se non è possibile stabilire una connessione di rete a livello di porta per una o più porte selezionate, viene visualizzato il messaggio "Port Connectivity test failed" (Test di connettività porta non riuscito) in un banner rosso. L'output del comando nmap è elencato sotto il banner.

Il banner rosso indica che è stato eseguito un tentativo di connessione TCP a una porta dell'host remoto, ma non è stato restituito nulla al mittente. Quando non viene restituita alcuna risposta, la porta ha uno stato "filtrato" e probabilmente è bloccata da un firewall.



Vengono elencate anche le porte con "closed".

❗ 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
```

## Informazioni correlate

[Linee guida per il networking](#)

# Accesso e configurazione di Gestione di sistema SANtricity (SG6000)

È possibile utilizzare Gestore di sistema di SANtricity per monitorare lo stato dei controller di storage, dei dischi di storage e di altri componenti hardware nello shelf del controller di storage. È inoltre possibile configurare un proxy per e-Series AutoSupport che consente di inviare messaggi AutoSupport dall'appliance senza utilizzare la porta di gestione.

## Configurare e accedere a Gestore di sistema di SANtricity

Potrebbe essere necessario accedere a Gestore di sistema di SANtricity sul controller di storage per monitorare l'hardware nello shelf del controller di storage o per configurare e-Series AutoSupport.

### Di cosa hai bisogno

- Si sta utilizzando un [browser web supportato](#).
- Per accedere a Gestore di sistema SANtricity tramite Gestione griglia, è necessario aver installato StorageGRID e disporre dell'autorizzazione di amministratore o di accesso root.
- Per accedere a Gestione di sistema di SANtricity utilizzando il programma di installazione dell'appliance di StorageGRID, è necessario disporre del nome utente e della password dell'amministratore di Gestione di sistema di SANtricity.
- Per accedere direttamente a Gestore di sistema di SANtricity utilizzando un browser Web, è necessario disporre del nome utente e della password dell'amministratore di Gestione di sistema di SANtricity.





È necessario disporre del firmware SANtricity 8.70 (11.70) o superiore per accedere a Gestione sistemi SANtricity utilizzando Gestione griglia o il programma di installazione dell'appliance StorageGRID. È possibile verificare la versione del firmware utilizzando il programma di installazione dell'appliance StorageGRID e selezionando **Guida > informazioni**.



L'accesso a Gestione di sistema SANtricity da Gestione griglia o dal programma di installazione dell'appliance è generalmente destinato solo al monitoraggio dell'hardware e alla configurazione di e-Series AutoSupport. Molte funzionalità e operazioni di Gestione sistema di SANtricity, come l'aggiornamento del firmware, non si applicano al monitoraggio dell'appliance StorageGRID. Per evitare problemi, seguire sempre le istruzioni di installazione e manutenzione dell'hardware dell'appliance.

### A proposito di questa attività

Esistono tre modi per accedere a Gestore di sistema di SANtricity, a seconda della fase del processo di installazione e configurazione in cui ci si trova:

- Se l'appliance non è ancora stata implementata come nodo nel sistema StorageGRID, utilizzare la scheda Avanzate del programma di installazione dell'appliance StorageGRID.



Una volta implementato il nodo, non è più possibile utilizzare il programma di installazione dell'appliance StorageGRID per accedere a Gestione di sistema di SANtricity.

- Se l'appliance è stata implementata come nodo nel sistema StorageGRID, utilizzare la scheda Gestore di sistema di SANtricity nella pagina nodi di Gestione griglia.
- Se non è possibile utilizzare il programma di installazione dell'appliance StorageGRID o Gestione griglia, è possibile accedere direttamente a Gestione sistema SANtricity utilizzando un browser Web collegato alla porta di gestione.

Questa procedura include i passaggi per l'accesso iniziale a Gestore di sistema di SANtricity. Se è già stato configurato Gestore di sistema di SANtricity, accedere alla [fase di configurazione degli avvisi hardware](#).



L'utilizzo di Gestione griglia o del programma di installazione dell'appliance StorageGRID consente di accedere a Gestione di sistema SANtricity senza dover configurare o collegare la porta di gestione dell'appliance.

Si utilizza Gestore di sistema di SANtricity per monitorare quanto segue:

- Dati sulle performance come performance a livello di array storage, latenza i/o, utilizzo della CPU e throughput
- Stato dei componenti hardware
- Funzioni di supporto, inclusa la visualizzazione dei dati diagnostici

È possibile utilizzare Gestore di sistema di SANtricity per configurare le seguenti impostazioni:

- Avvisi e-mail, SNMP o syslog per i componenti nello shelf dello storage controller
- Impostazioni AutoSupport e-Series per i componenti nello shelf dello storage controller.

Per ulteriori informazioni su e-Series AutoSupport, consultare ["Sito di documentazione dei sistemi NetApp e-Series"](#).

- Drive Security keys, necessari per sbloccare dischi protetti (questa operazione è necessaria se la funzione Drive Security è attivata)
- Password dell'amministratore per accedere a Gestione di sistema di SANtricity

## Fasi

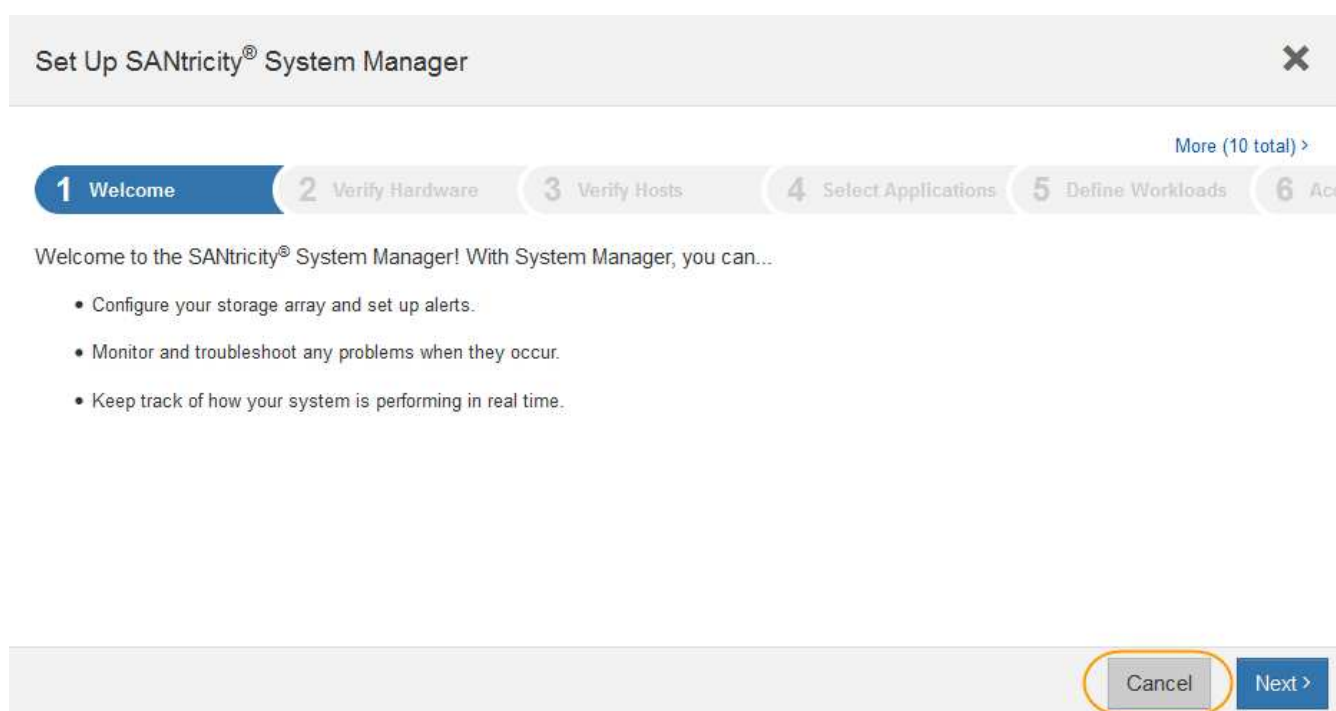
1. Utilizzare il programma di installazione dell'appliance StorageGRID e selezionare **Avanzate > Gestore di sistema SANtricity**



Se il programma di installazione dell'appliance StorageGRID non è disponibile o la pagina di accesso non viene visualizzata, è necessario utilizzare [Indirizzi IP per i controller di storage](#). Accedere a Gestore di sistema SANtricity accedendo all'IP del controller di storage.

2. Impostare o inserire la password dell'amministratore.

Gestore di sistema di SANtricity utilizza una singola password di amministratore condivisa tra tutti gli utenti.



3. Selezionare **Annulla** per chiudere la procedura guidata.



Non completare la configurazione guidata di un'appliance StorageGRID.



4. Configura avvisi hardware.
  - a. Selezionare **Guida** per accedere alla guida in linea di Gestione di sistema di SANtricity.
  - b. Per ulteriori informazioni sugli avvisi, consultare la sezione **Impostazioni > Avvisi** della guida in linea.
  - c. Seguire le istruzioni “How To” per impostare avvisi e-mail, SNMP o syslog.
5. Gestire AutoSupport per i componenti nello shelf dello storage controller.
  - a. Selezionare **Guida** per accedere alla guida in linea di Gestione di sistema di SANtricity.
  - b. Consulta la sezione **SUPPORT > Support Center** della guida in linea per scoprire la funzionalità di AutoSupport.
  - c. Seguire le istruzioni “How To” per gestire AutoSupport.

Per istruzioni specifiche sulla configurazione di un proxy StorageGRID per l'invio di messaggi AutoSupport e-Series senza utilizzare la porta di gestione, consultare [istruzioni per la configurazione delle impostazioni dello storage proxy](#).
6. Se la funzione Drive Security è attivata per l'appliance, creare e gestire la chiave di sicurezza.
  - a. Selezionare **Guida** per accedere alla guida in linea di Gestione di sistema di SANtricity.
  - b. Per ulteriori informazioni su Drive Security, consultare la sezione **Impostazioni > sistema > Gestione delle chiavi di sicurezza** della guida in linea.
  - c. Seguire le istruzioni “How To” per creare e gestire la chiave di sicurezza.
7. Se si desidera, modificare la password dell'amministratore.
  - a. Selezionare **Guida** per accedere alla guida in linea di Gestione di sistema di SANtricity.
  - b. Consultare la sezione **Home > Amministrazione array di storage** della guida in linea per informazioni sulla password dell'amministratore.

- c. Seguire le istruzioni “How To” per modificare la password.

## Esaminare lo stato dell'hardware in Gestore di sistema di SANtricity

È possibile utilizzare Gestione di sistema di SANtricity per monitorare e gestire i singoli componenti hardware nello shelf dello storage controller e per esaminare informazioni ambientali e diagnostiche dell'hardware, come la temperatura dei componenti, nonché i problemi relativi ai dischi.

### Di cosa hai bisogno

- Si sta utilizzando un [browser web supportato](#).
- Per accedere a Gestione di sistema SANtricity tramite Gestione griglia, è necessario disporre dell'autorizzazione Amministratore appliance di storage o dell'autorizzazione di accesso root.
- Per accedere a Gestione di sistema di SANtricity utilizzando il programma di installazione dell'appliance di StorageGRID, è necessario disporre del nome utente e della password dell'amministratore di Gestione di sistema di SANtricity.
- Per accedere direttamente a Gestore di sistema di SANtricity utilizzando un browser Web, è necessario disporre del nome utente e della password dell'amministratore di Gestione di sistema di SANtricity.



È necessario disporre del firmware SANtricity 8.70 (11.70) o superiore per accedere a Gestione sistemi SANtricity utilizzando Gestione griglia o il programma di installazione dell'appliance StorageGRID.

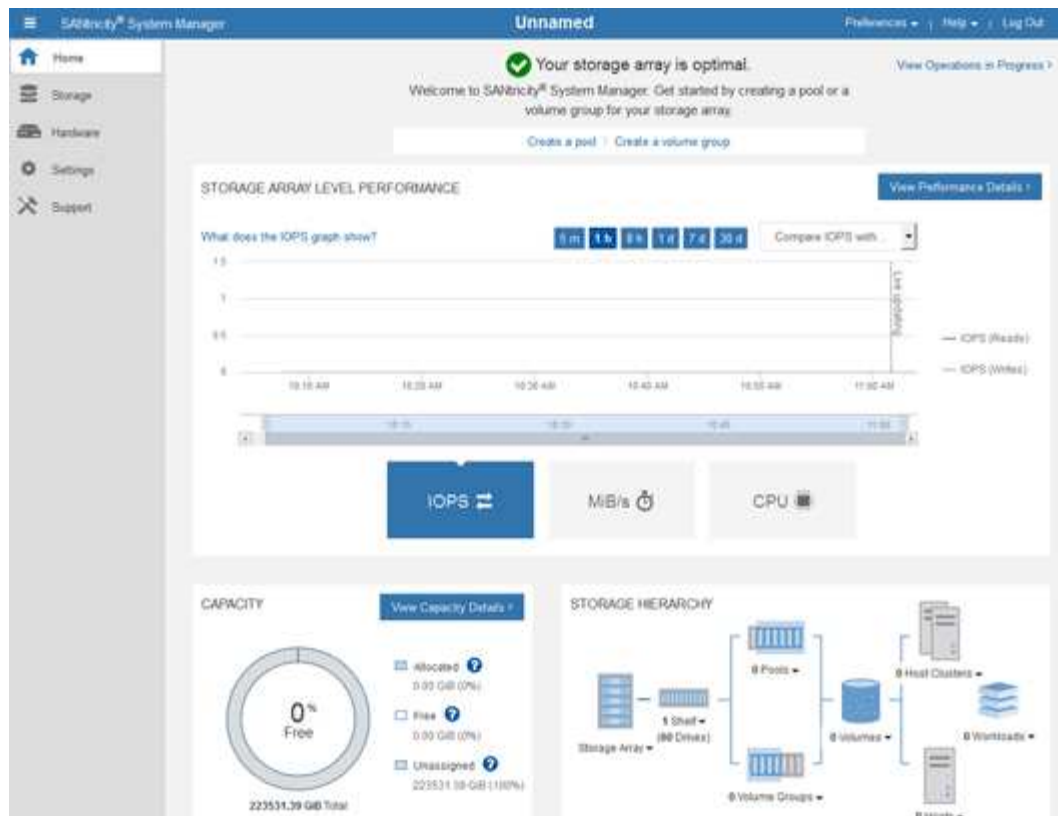


L'accesso a Gestione di sistema SANtricity da Gestione griglia o dal programma di installazione dell'appliance è generalmente destinato solo al monitoraggio dell'hardware e alla configurazione di e-Series AutoSupport. Molte funzionalità e operazioni di Gestione sistema di SANtricity, come l'aggiornamento del firmware, non si applicano al monitoraggio dell'appliance StorageGRID. Per evitare problemi, seguire sempre le istruzioni di installazione e manutenzione dell'hardware dell'appliance.

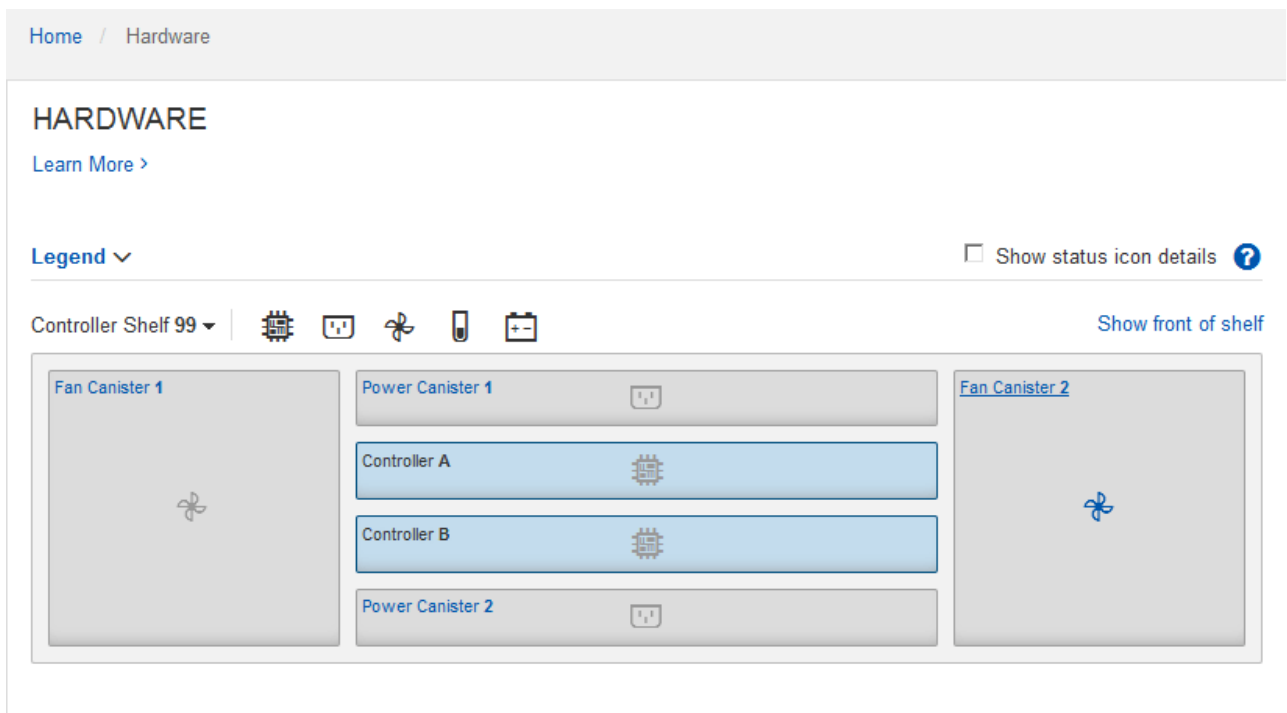
### Fasi

1. [Accedere a Gestore di sistema di SANtricity](#).
2. Se necessario, immettere il nome utente e la password dell'amministratore.
3. Fare clic su **Annulla** per chiudere la procedura guidata di configurazione e visualizzare la home page di Gestore di sistema di SANtricity.

Viene visualizzata la home page di Gestore di sistema di SANtricity. In Gestore di sistema di SANtricity, lo shelf del controller viene definito storage array.



4. Esaminare le informazioni visualizzate per l'hardware dell'appliance e verificare che tutti i componenti hardware abbiano uno stato ottimale.
  - a. Fare clic sulla scheda **hardware**.
  - b. Fare clic su **Mostra retro dello shelf**.



Dal retro dello shelf, è possibile visualizzare entrambi i controller di storage, la batteria di ciascun controller di storage, i due contenitori di alimentazione, i due contenitori per ventole e gli eventuali shelf di

espansione. È inoltre possibile visualizzare le temperature dei componenti.

- a. Per visualizzare le impostazioni di ciascun controller di storage, selezionare il controller e selezionare **View settings** (Visualizza impostazioni) dal menu di scelta rapida.
- b. Per visualizzare le impostazioni degli altri componenti sul retro dello shelf, selezionare il componente che si desidera visualizzare.
- c. Fare clic su **Mostra parte anteriore dello shelf** e selezionare il componente che si desidera visualizzare.

Dalla parte anteriore dello shelf, è possibile visualizzare le unità e i cassetti delle unità per lo shelf del controller di storage o gli shelf di espansione (se presenti).

Se lo stato di un componente richiede attenzione, seguire la procedura descritta nel Recovery Guru per risolvere il problema o contattare il supporto tecnico.

## Impostare gli indirizzi IP per i controller di storage utilizzando il programma di installazione dell'appliance StorageGRID

La porta di gestione 1 di ciascun controller di storage collega l'appliance alla rete di gestione per Gestione di sistema di SANtricity. Se non è possibile accedere a Gestione di sistema SANtricity dal programma di installazione dell'appliance StorageGRID, è necessario impostare un indirizzo IP statico per ciascun controller di storage per garantire che non si perda la connessione di gestione all'hardware e al firmware del controller nello shelf del controller.

### Di cosa hai bisogno

- Si sta utilizzando qualsiasi client di gestione in grado di connettersi alla rete amministrativa di StorageGRID o si dispone di un laptop di assistenza.
- Il laptop client o di servizio dispone di un browser Web supportato.

### A proposito di questa attività

Gli indirizzi assegnati da DHCP possono cambiare in qualsiasi momento. Assegnare indirizzi IP statici ai controller per garantire un'accessibilità coerente.



Seguire questa procedura solo se non si dispone dell'accesso a Gestore di sistema SANtricity dal programma di installazione dell'appliance StorageGRID (**Avanzate > Gestore di sistema SANtricity**) o da Gestore di griglia (**NODI > Gestore di sistema SANtricity**).

### Fasi

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

Per *Appliance\_Controller\_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 **Configure hardware > Storage Controller Network Configuration**.

Viene visualizzata la pagina Storage Controller Network Configuration (Configurazione di rete dello Storage Controller).

3. A seconda della configurazione di rete, selezionare **Enabled** per IPv4, IPv6 o entrambi.
4. Annotare l'indirizzo IPv4 visualizzato automaticamente.

DHCP è il metodo predefinito per assegnare un indirizzo IP alla porta di gestione del controller di storage.



La visualizzazione dei valori DHCP potrebbe richiedere alcuni minuti.

IPv4 Address Assignment    ☐ Static    ☒ DHCP

IPv4 Address (CIDR)    10.224.5.166/21

Default Gateway    10.224.0.1

5. Facoltativamente, impostare un indirizzo IP statico per la porta di gestione del controller di storage.



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

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

IPv4 Address Assignment    ☒ Static    ☐ DHCP

IPv4 Address (CIDR)    10.224.2.200/21

Default Gateway    10.224.0.1

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

L'applicazione delle modifiche potrebbe richiedere alcuni minuti.

Quando ci si connette a Gestore di sistema di SANtricity, si utilizzerà il nuovo indirizzo IP statico come URL:

**`https://Storage_Controller_IP`**

## Configurare l'interfaccia BMC (SG6000)

L'interfaccia utente del BMC (Baseboard Management Controller) sul controller SG6000-CN fornisce informazioni sullo stato dell'hardware e consente di configurare le impostazioni SNMP e altre opzioni per il controller SG6000-CN.

## 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

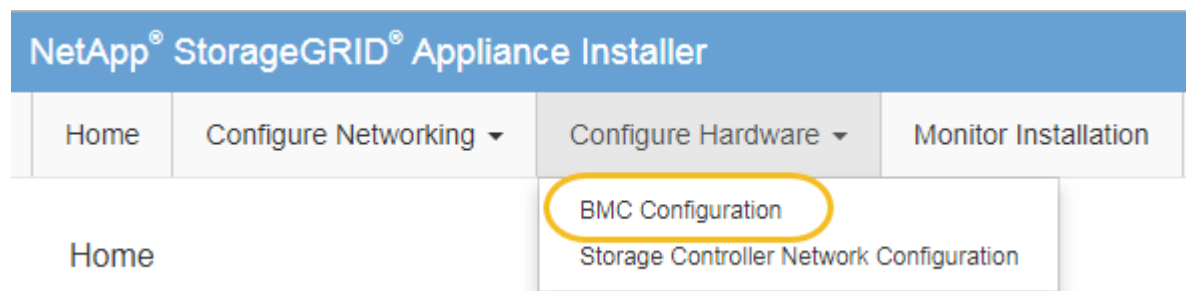
1. Dal client, immettere l'URL del programma di installazione dell'appliance StorageGRID:

**`https://Appliance_Controller_IP:8443`**

Per *Appliance\_Controller\_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	<input type="password" value="....."/>
Confirm Root Password	<input type="password" value="....."/>

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 sul controller SG6000-CN.



## 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.



## 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

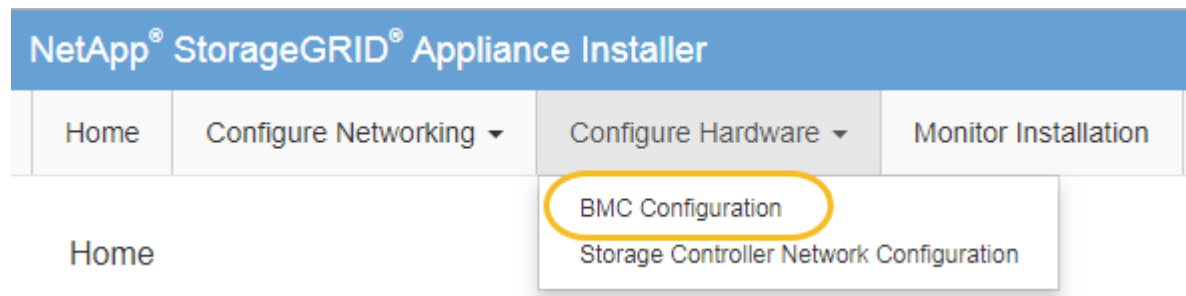
1. Dal client, immettere l'URL del programma di installazione dell'appliance StorageGRID:

**`https://SG6000-CN_Controller_IP:8443`**

Per SG6000-CN\_Controller\_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.

## 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

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

L'applicazione delle modifiche potrebbe richiedere alcuni minuti.

## Accedere all'interfaccia BMC

È possibile accedere all'interfaccia BMC sul controller SG6000-CN utilizzando l'indirizzo IP statico o DHCP per la porta di gestione BMC.

### Di cosa hai bisogno

- La porta di gestione BMC del controller SG6000-CN è collegata alla rete di gestione che si intende utilizzare.



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

## 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 in [Configurare l'interfaccia BMC \(SG6000\)](#). 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. Immettere il nome utente root e la password, utilizzando la password impostata al momento dell'installazione [modificata la password root predefinita](#):

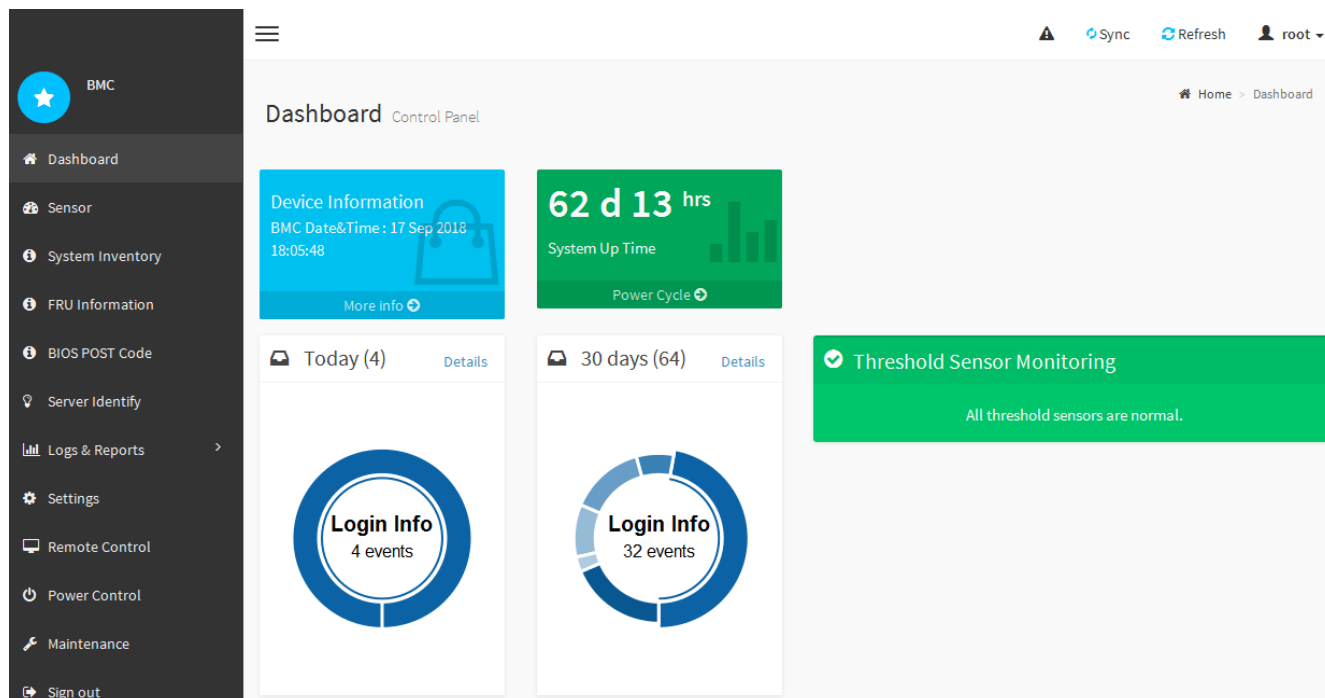


☐ Remember Username

[Sign me in](#)

[I forgot my password](#)

3. Selezionare **Accedi**.



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.

## Configurare le impostazioni SNMP per il controller SG6000-CN

Se si ha familiarità con la configurazione di SNMP per l'hardware, è possibile utilizzare l'interfaccia BMC per configurare le impostazioni SNMP per il controller SG6000-CN. 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 se il sistema SG6000-CN non funziona correttamente e deve essere sostituito. 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 il controller SG6000-CN invii notifiche immediate a una console SNMP quando si trova in uno stato anormale. I trap potrebbero indicare guasti hardware di vari componenti o il superamento delle soglie di temperatura.

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.



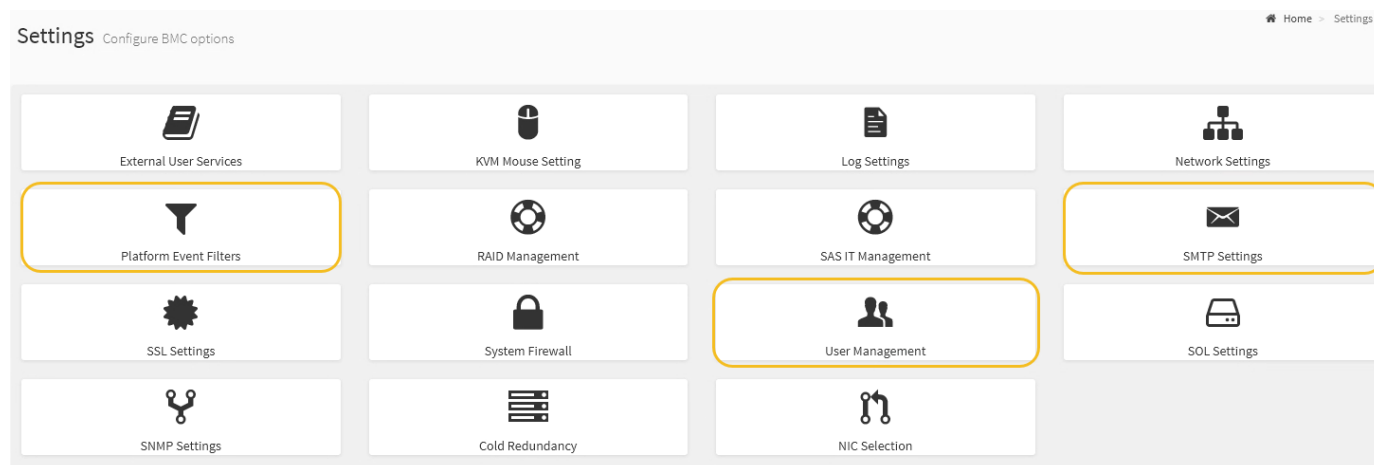
Le impostazioni BMC eseguite con questa procedura potrebbero non essere mantenute se il sistema SG6000-CN non funziona correttamente e deve essere sostituito. Assicurarsi di disporre di una registrazione di tutte le impostazioni applicate, in modo che possano essere riapplicate facilmente dopo la sostituzione 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.

## Facoltativo: Attivare la crittografia del nodo

Se si attiva la crittografia dei nodi, i dischi dell'appliance possono essere protetti mediante crittografia KMS (Secure Key Management Server) contro la perdita fisica o la rimozione dal sito. È necessario selezionare e attivare la crittografia del nodo durante l'installazione dell'appliance e non è possibile deselectare la crittografia del nodo una volta avviato il processo di crittografia KMS.

## Di cosa hai bisogno

Consultare le informazioni relative a KMS nelle istruzioni per l'amministrazione di StorageGRID.

## A proposito di questa attività

Un'appliance con crittografia dei nodi abilitata si connette al server di gestione delle chiavi (KMS) esterno configurato per il sito StorageGRID. Ogni KMS (o cluster KMS) gestisce le chiavi di crittografia per tutti i nodi appliance del sito. Queste chiavi crittografano e decrittano i dati su ciascun disco di un'appliance che ha attivato la crittografia dei nodi.

È possibile configurare un KMS in Grid Manager prima o dopo l'installazione dell'appliance in StorageGRID. Per ulteriori informazioni, consultare le informazioni relative a KMS e alla configurazione dell'appliance nelle istruzioni per l'amministrazione di StorageGRID.

- Se viene configurato un KMS prima di installare l'appliance, la crittografia controllata da KMS inizia quando si attiva la crittografia dei nodi sull'appliance e la si aggiunge a un sito StorageGRID in cui è configurato KMS.
- Se un KMS non viene configurato prima dell'installazione dell'appliance, la crittografia controllata da KMS viene eseguita su ogni appliance che ha attivato la crittografia del nodo non appena un KMS viene configurato e disponibile per il sito che contiene il nodo dell'appliance.



I dati che esistono prima della connessione al KMS su un'appliance con crittografia del nodo attivata vengono crittografati con una chiave temporanea non sicura. L'apparecchio non è protetto da rimozione o furto fino a quando la chiave non viene impostata su un valore fornito dal KMS.

Senza la chiave KMS necessaria per decrittare il disco, i dati sull'appliance non possono essere recuperati e vengono effettivamente persi. Questo accade quando non è possibile recuperare la chiave di decrittografia dal KMS. La chiave diventa inaccessibile se si cancella la configurazione del KMS, si scade una chiave KMS, si perde la connessione al KMS o se l'appliance viene rimossa dal sistema StorageGRID in cui sono installate le chiavi KMS.

## Fasi

1. Aprire un browser e inserire uno degli indirizzi IP del controller di elaborazione dell'appliance.

**`https://Controller_IP:8443`**

*Controller\_IP* È l'indirizzo IP del controller di calcolo (non dello storage controller) su una qualsiasi delle tre reti StorageGRID.

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



Dopo aver crittografato l'appliance con una chiave KMS, i dischi dell'appliance non possono essere decifrati senza utilizzare la stessa chiave KMS.

2. Selezionare **Configura hardware > crittografia nodo**.

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. Selezionare **Enable node Encryption** (attiva crittografia nodo).

Prima dell'installazione dell'appliance, è possibile deselezionare l'opzione **Enable node Encryption** (attiva crittografia del nodo) senza rischi di perdita di dati. All'avvio dell'installazione, il nodo appliance accede alle chiavi di crittografia KMS nel sistema StorageGRID e avvia la crittografia del disco. Non è possibile disattivare la crittografia dei nodi dopo l'installazione dell'appliance.



Dopo aver aggiunto un'appliance con crittografia dei nodi abilitata a un sito StorageGRID con KMS, non è possibile interrompere l'utilizzo della crittografia KMS per il nodo.

### 4. Selezionare **Salva**.

### 5. Implementa l'appliance come nodo nel tuo sistema StorageGRID.

La crittografia controllata DA KMS inizia quando l'appliance accede alle chiavi KMS configurate per il sito StorageGRID. Il programma di installazione visualizza messaggi di avanzamento durante il processo di crittografia KMS, che potrebbero richiedere alcuni minuti a seconda del numero di volumi di dischi nell'appliance.



Le appliance vengono inizialmente configurate con una chiave di crittografia casuale non KMS assegnata a ciascun volume di disco. I dischi vengono crittografati utilizzando questa chiave di crittografia temporanea, che non è sicura, fino a quando l'appliance che ha attivato la crittografia dei nodi non accede alle chiavi KMS configurate per il sito StorageGRID.

### Al termine

È possibile visualizzare lo stato della crittografia del nodo, i dettagli KMS e i certificati in uso quando il nodo dell'appliance è in modalità di manutenzione.

### Informazioni correlate

[Amministrare StorageGRID](#)

[Monitorare la crittografia dei nodi in modalità di manutenzione \(SG6000\)](#)

## Opzionale: Modifica della modalità RAID (solo SG6000)

È possibile passare a una modalità RAID diversa sull'appliance per soddisfare i requisiti



di storage e ripristino. È possibile modificare la modalità solo prima di implementare il nodo di storage dell'appliance.

#### Di cosa hai bisogno

- Si sta utilizzando qualsiasi client in grado di connettersi a StorageGRID.
- Il client dispone di un [browser web supportato](#).

#### A proposito di questa attività

Prima di implementare l'appliance come nodo di storage, è possibile scegliere una delle seguenti opzioni di configurazione del volume:

- **DDP:** Questa modalità utilizza due unità di parità ogni otto unità dati. Questa è la modalità predefinita e consigliata per tutti gli appliance. Rispetto a RAID6, DDP offre migliori prestazioni di sistema, tempi di ricostruzione ridotti dopo guasti al disco e facilità di gestione.



DDP non fornisce la protezione contro la perdita di cassetto nelle appliance SG6060 a causa dei due SSD. La protezione dalle perdite dei cassette è efficace in tutti gli shelf di espansione aggiunti a un SG6060.

- **DDP16:** Questa modalità utilizza due unità di parità ogni 16 unità dati, il che comporta una maggiore efficienza dello storage rispetto al DDP. Rispetto a RAID6, il sistema DDP16 offre migliori performance di sistema, tempi di ricostruzione ridotti dopo guasti del disco, facilità di gestione ed efficienza dello storage paragonabile. Per utilizzare la modalità DDP16, la configurazione deve contenere almeno 20 dischi. Il DDP16 non fornisce la protezione contro le perdite di cassetto.
- **RAID6:** Questa modalità utilizza due unità di parità per ogni 16 o più unità dati. Per utilizzare la modalità RAID 6, la configurazione deve contenere almeno 20 dischi. Sebbene RAID6 possa aumentare l'efficienza dello storage dell'appliance rispetto a DDP, non è consigliato per la maggior parte degli ambienti StorageGRID.



Se alcuni volumi sono già stati configurati o se StorageGRID è stato installato in precedenza, la modifica della modalità RAID comporta la rimozione e la sostituzione dei volumi. Tutti i dati presenti su tali volumi andranno persi.

#### Fasi

1. Aprire un browser e inserire uno degli indirizzi IP del controller di elaborazione dell'appliance.

**`https://Controller_IP:8443`**

*Controller\_IP* È l'indirizzo IP del controller di calcolo (non dello storage controller) su una qualsiasi delle tre reti StorageGRID.

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

2. Selezionare **Advanced** (Avanzate) > **RAID Mode** (modalità RAID).
3. Nella pagina **Configure RAID Mode** (Configura modalità RAID), selezionare la modalità RAID desiderata dall'elenco a discesa Mode (modalità).
4. Fare clic su **Save** (Salva).

#### Informazioni correlate

["Sito di documentazione dei sistemi NetApp e-Series"](#)

## Opzionale: Consente di rimappare le porte di rete per l'appliance

Potrebbe essere necessario rimappare le porte interne del nodo di storage dell'appliance a diverse porte esterne. Ad esempio, potrebbe essere necessario rimappare le porte a causa di un problema di firewall.

### Di cosa hai bisogno

- In precedenza è stato effettuato l'accesso al programma di installazione dell'appliance StorageGRID.
- Non sono stati configurati e non si prevede di configurare gli endpoint del bilanciamento del carico.



Se si rimappano le porte, non è possibile utilizzare le stesse porte per configurare gli endpoint del bilanciamento del carico. Se si desidera configurare gli endpoint del bilanciamento del carico e le porte sono già state rimappate, seguire la procedura descritta in [Rimuovere i rimap delle porte](#).

### Fasi

1. Dal programma di installazione dell'appliance StorageGRID, fare clic su **Configura rete Porte rimappate**.

Viene visualizzata la pagina Remap Port (porta Remap).

2. Dalla casella a discesa **Network** (rete), selezionare la rete per la porta che si desidera rimappare: Grid, Admin o Client.
3. Dalla casella di riepilogo **Protocol** (protocollo), selezionare il protocollo IP: TCP o UDP.
4. Dalla casella a discesa **Remap Direction** (direzione rimappamento), selezionare la direzione del traffico che si desidera rimappare per questa porta: Inbound (in entrata), Outbound (in uscita) o Bi-directional (bidirezionale).
5. Per **Original Port** (porta originale), immettere il numero della porta che si desidera rimappare.
6. Per **Mapped-to Port**, inserire il numero della porta che si desidera utilizzare.
7. Fare clic su **Add Rule** (Aggiungi regola).

La nuova mappatura delle porte viene aggiunta alla tabella e il remapping ha effetto immediato.

### 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.

Network	Protocol	Remap Direction	Original Port	Mapped-To Port
Grid	TCP	Bi-directional	1800	1801

8. Per rimuovere una mappatura delle porte, selezionare il pulsante di opzione della regola che si desidera rimuovere e fare clic su **Remove Selected Rule** (Rimuovi regola selezionata).

## 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.