



Supporto di boot

Install and maintain

NetApp

February 13, 2026

This PDF was generated from <https://docs.netapp.com/it-it/ontap-systems/asa-r2-a1k/bootmedia-replace-workflow-bmr.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Sommario

- Supporto di boot 1
 - Flusso di lavoro per la sostituzione dei supporti di avvio - ASAA1K 1
 - Requisiti per sostituire i supporti di avvio - ASAA1K 1
 - Spegnere il controller per sostituire il supporto di avvio - ASAA1K 2
 - Sostituire il supporto di avvio - ASAA1K 3
 - Ripristinare l'immagine ONTAP sul supporto di avvio - ASAA1K 5
 - Restituire il componente guasto a NetApp - ASAA1K 11

Supporto di boot

Flusso di lavoro per la sostituzione dei supporti di avvio - ASA A1K

Come iniziare a sostituire i supporti di avvio nel sistema di storage ASA A1K, rivedere i requisiti di sostituzione, spegnere il controller, sostituire i supporti di avvio, ripristinare l'immagine sui supporti di avvio e verificare la funzionalità del sistema.

1

"Esaminare i requisiti dei supporti di avvio"

Esaminare i requisiti per la sostituzione dei supporti di avvio.

2

"Spegnere il controller"

Arrestare il controller nel sistema di storage quando è necessario sostituire i supporti di avvio.

3

"Sostituire il supporto di avvio"

Rimuovere il supporto di avvio guasto dal modulo di gestione del sistema e installare il supporto di avvio sostitutivo.

4

"Ripristinare l'immagine sul supporto di avvio"

Ripristinare l'immagine ONTAP dal controller partner.

5

"Restituire la parte guasta a NetApp"

Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Requisiti per sostituire i supporti di avvio - ASA A1K

Prima di sostituire il supporto di avvio nel sistema ASA A1K, assicurarsi di soddisfare i requisiti necessari per una sostituzione corretta. Ciò include la verifica di disporre del supporto di avvio sostitutivo corretto, la conferma del corretto funzionamento delle porte del cluster sul controller danneggiato e la verifica dell'abilitazione di Onboard Key Manager (OKM) o External Key Manager (EKM).

Esaminare i seguenti requisiti.

- È necessario sostituire il supporto di avvio guasto con un supporto di avvio sostitutivo ricevuto da NetApp.
- Le porte del cluster vengono utilizzate per comunicare tra i due controller durante il processo di ripristino automatico dell'avvio. Assicurarsi che le porte del cluster sul controller danneggiato funzionino correttamente.

- Per OKM, è necessaria la passphrase dell'intero cluster e anche i dati di backup.
- Per EKM, è necessario copiare i seguenti file dal nodo partner:
 - /cfcard/kmip/servers.cfg
 - /cfcard/kmip/certs/client.crt
 - /cfcard/kmip/certs/client.key
 - /cfcard/kmip/certs/CA.pem
- Comprendere la terminologia del controller utilizzata in questa procedura:
 - Il *controller non funzionante* è il controller su cui si sta eseguendo la manutenzione.
 - Il *controllore sano* è il partner HA del controllore compromesso.

Cosa succederà

Dopo aver esaminato i requisiti dei supporti di avvio, si ["spegnere il controller"](#).

Spegnere il controller per sostituire il supporto di avvio - ASA A1K

Spegnere il controller danneggiato nel sistema di storage ASA A1K per evitare la perdita di dati e garantire la stabilità del sistema durante la sostituzione del supporto di avvio.

Per spegnere il controller compromesso, è necessario determinare lo stato del controller e, se necessario, assumere il controllo del controller in modo che il controller integro continui a servire i dati provenienti dallo storage del controller compromesso.

A proposito di questa attività

- Se si dispone di un sistema SAN, è necessario aver controllato i messaggi di evento `cluster kernel-service show` per il blade SCSI del controller danneggiato. Il `cluster kernel-service show` comando (dalla modalità avanzata precedente) visualizza il nome del nodo, ["stato quorum"](#) di quel nodo, lo stato di disponibilità di quel nodo e lo stato operativo di quel nodo.

Ogni processo SCSI-blade deve essere in quorum con gli altri nodi del cluster. Eventuali problemi devono essere risolti prima di procedere con la sostituzione.

- Se si dispone di un cluster con più di due nodi, questo deve trovarsi in quorum. Se il cluster non è in quorum o un controller integro mostra false per idoneità e salute, è necessario correggere il problema prima di spegnere il controller compromesso; vedere ["Sincronizzare un nodo con il cluster"](#).

Fasi

1. Se AutoSupport è attivato, eliminare la creazione automatica del caso richiamando un messaggio AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=<# of hours>h
```

Il seguente messaggio AutoSupport elimina la creazione automatica del caso per due ore:

```
cluster1:> system node autosupport invoke -node * -type all -message MAINT=2h
```

2. Disattiva la restituzione automatica:

- a. Immettere il seguente comando dalla console del controller funzionante:

```
storage failover modify -node impaired_node_name -auto-giveback false
```

b. Entra *y* quando vedi il messaggio *Vuoi disattivare la restituzione automatica?*

3. Portare la centralina danneggiata al prompt DEL CARICATORE:

Se il controller non utilizzato visualizza...	Quindi...
Il prompt DEL CARICATORE	Passare alla fase successiva.
In attesa di un giveback...	Premere Ctrl-C, quindi rispondere <i>y</i> quando richiesto.
Prompt di sistema o prompt della password	<p>Assumere il controllo o arrestare il controller compromesso dal controller integro:</p> <pre>storage failover takeover -ofnode <i>impaired_node_name</i> -halt true</pre> <p>Il parametro <i>-halt true</i> consente di visualizzare il prompt di Loader.</p>

Cosa succederà

Dopo aver spento il controller danneggiato, si "[sostituire il supporto di avvio](#)".

Sostituire il supporto di avvio - ASA A1K

Il supporto di avvio del sistema ASA A1K memorizza i dati di configurazione e il firmware essenziali. Il processo di sostituzione prevede la rimozione del modulo di gestione del sistema, la rimozione dei supporti di avvio danneggiati, l'installazione dei supporti di avvio sostitutivi nel modulo di gestione del sistema, quindi la reinstallazione del modulo di gestione del sistema.

Il supporto di avvio si trova all'interno del modulo di gestione del sistema ed è accessibile rimuovendo il modulo dal sistema.

Fasi

1. Se non si è già collegati a terra, mettere a terra l'utente.
2. Scollegare i cavi di alimentazione dagli alimentatori.



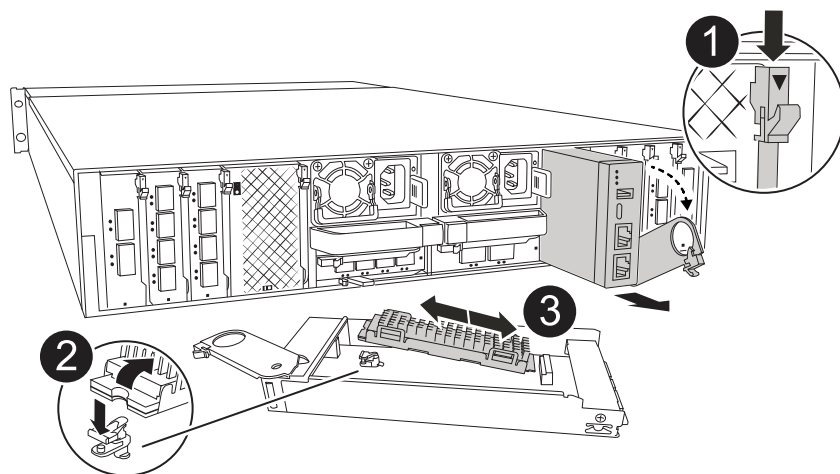
Se il sistema di storage è dotato di alimentatori CC, scollegare il blocco cavi di alimentazione dagli alimentatori.

3. Rimuovere il modulo di gestione del sistema:

- a. Rimuovere tutti i cavi collegati al modulo di gestione del sistema. Assicurarsi di etichettare il punto in cui sono stati collegati i cavi, in modo da poterli collegare alle porte corrette quando si reinstalla il modulo.
- b. Ruotare il vassoio di gestione dei cavi verso il basso tirando i pulsanti su entrambi i lati all'interno del vassoio di gestione dei cavi, quindi ruotare il vassoio verso il basso.

- c. Premere il pulsante della camma di gestione del sistema.
- d. Ruotare il dispositivo di chiusura della camma verso il basso fino in fondo.
- e. Rimuovere il modulo di gestione del sistema dal contenitore agganciando il dito all'apertura della leva della camma ed estraendo il modulo dal contenitore.
- f. Posizionare il modulo di gestione del sistema su un tappetino antistatico, in modo che il supporto di avvio sia accessibile.

4. Rimuovere il supporto di avvio dal modulo di gestione:



1	Dispositivo di chiusura della camma del modulo di gestione del sistema
2	Pulsante di blocco dei supporti di avvio
3	Supporto di boot

- a. Premere il pulsante di bloccaggio blu.
 - b. Ruotare il supporto di avvio verso l'alto, farlo scorrere fuori dallo zoccolo e metterlo da parte.
5. Installare il supporto di avvio sostitutivo nel modulo di gestione del sistema:
- a. Allineare i bordi del supporto di avvio con l'alloggiamento dello zoccolo, quindi spingerlo delicatamente a squadra nello zoccolo.
 - b. Ruotare il supporto di avvio verso il basso verso il pulsante di bloccaggio.
 - c. Premere il pulsante di bloccaggio, ruotare completamente il supporto di avvio e rilasciare il pulsante di bloccaggio.
6. Reinstallare il modulo di gestione del sistema:
- a. Allineare il modulo con i bordi dell'apertura dello slot del contenitore.
 - b. Far scorrere delicatamente il modulo nello slot fino in fondo al contenitore, quindi ruotare il dispositivo di chiusura della camma completamente verso l'alto per bloccare il modulo in posizione.
7. Ruotare il vassoio di gestione dei cavi verso l'alto fino alla posizione di chiusura.
- a. Eseguire il richiamo del modulo Gestione del sistema.
8. Collegare i cavi di alimentazione agli alimentatori e reinstallare il fermo del cavo di alimentazione.

Il controller inizia ad avviarsi non appena l'alimentazione viene ricollegata al sistema.

Cosa succederà

Dopo aver sostituito fisicamente i supporti di avvio danneggiati, ["Ripristinare l'immagine ONTAP dal nodo partner"](#).

Ripristinare l'immagine ONTAP sul supporto di avvio - ASA A1K

Dopo aver installato il nuovo dispositivo multimediale di avvio nel sistema ASA A1K, è possibile avviare il processo di ripristino automatico del supporto di avvio per ripristinare la configurazione dal nodo partner.

Durante il processo di ripristino, il sistema controlla se la crittografia è attivata e determina il tipo di crittografia della chiave in uso. Se la crittografia della chiave è attivata, il sistema guida l'utente attraverso le procedure appropriate per ripristinarla.

Prima di iniziare

- Determina il tipo di gestore delle chiavi:
 - Onboard Key Manager (OKM): richiede passphrase e dati di backup per l'intero cluster
 - External Key Manager (EKM): richiede i seguenti file dal nodo partner:
 - /cfcard/kmip/servers.cfg
 - /cfcard/kmip/certs/client.crt
 - /cfcard/kmip/certs/client.key
 - /cfcard/kmip/certs/CA.pem

Fasi

1. Dal prompt LOADER, avviare il processo di ripristino del supporto di avvio:

```
boot_recovery -partner
```

Sullo schermo viene visualizzato il seguente messaggio:

```
Starting boot media recovery (BMR) process. Press Ctrl-C to abort...
```

2. Monitorare il processo di ripristino dell'installazione dei supporti di avvio.

Il processo viene completato e viene visualizzato il `Installation complete` messaggio.

3. Il sistema verifica la crittografia e visualizza uno dei seguenti messaggi:

Se viene visualizzato questo messaggio...	Eeguire questa operazione...
key manager is not configured. Exiting.	<p>La crittografia non è installata sul sistema.</p> <ol style="list-style-type: none"> Attendi che venga visualizzato il prompt di accesso. Accedi al nodo e restituisci lo storage: <pre>storage failover giveback -ofnode impaired_node_name</pre> Vai a riattivazione della restituzione automatica se fosse disabilitato.
key manager is configured.	La crittografia è installata. Vai a aripristino del gestore delle chiavi .



Se il sistema non riesce a identificare la configurazione del gestore delle chiavi, visualizza un messaggio di errore e chiede di confermare se il gestore delle chiavi è configurato e di che tipo (integrato o esterno). Rispondi alle richieste per procedere.

- Ripristina il key manager utilizzando la procedura appropriata per la tua configurazione:

Onboard Key Manager (OKM)

Il sistema visualizza il seguente messaggio e inizia a eseguire l'opzione BootMenu 10:

```
key manager is configured.  
Entering Bootmenu Option 10...
```

```
This option must be used only in disaster recovery procedures. Are  
you sure? (y or n):
```

- Entra `y` alla richiesta di conferma di voler avviare il processo di ripristino OKM.
- Quando richiesto, immettere la passphrase per la gestione delle chiavi integrate.
- Quando richiesto, immettere nuovamente la passphrase per confermare.
- Quando richiesto, immettere i dati di backup per il gestore delle chiavi integrato.

Mostra un esempio di richiesta di passphrase e dati di backup

```
Enter the passphrase for onboard key management:  
-----BEGIN PASSPHRASE-----  
<passphrase_value>  
-----END PASSPHRASE-----  
Enter the passphrase again to confirm:  
-----BEGIN PASSPHRASE-----  
<passphrase_value>  
-----END PASSPHRASE-----  
Enter the backup data:  
-----BEGIN BACKUP-----  
<passphrase_value>  
-----END BACKUP-----
```

- Monitorare il processo di ripristino mentre ripristina i file appropriati dal nodo partner.

Una volta completato il processo di ripristino, il nodo si riavvia. I seguenti messaggi indicano un ripristino riuscito:

```
Trying to recover keymanager secrets....  
Setting recovery material for the onboard key manager  
Recovery secrets set successfully  
Trying to delete any existing km_onboard.keydb file.  
  
Successfully recovered keymanager secrets.
```

- Dopo il riavvio del nodo, verificare che il sistema sia di nuovo online e operativo.

g. Riportare la centralina guasta al normale funzionamento restituendo la memoria:

```
storage failover giveback -ofnode impaired_node_name
```

h. Dopo che il nodo partner è completamente attivo e fornisce dati, sincronizzare le chiavi OKM nel cluster:

```
security key-manager onboard sync
```

Vai a [riattivazione della restituzione automatica](#) se fosse disabilitato.

Gestore chiavi esterno (EKM)

Il sistema visualizza il seguente messaggio e inizia a eseguire l'opzione BootMenu 11:

```
key manager is configured.  
Entering Bootmenu Option 11...
```

a. Quando richiesto, immettere le impostazioni di configurazione EKM:

i. Immettere il contenuto del certificato client da `/cfcard/kmip/certs/client.crt` file:

Mostra un esempio di contenuto del certificato client

```
-----BEGIN CERTIFICATE-----  
<certificate_value>  
-----END CERTIFICATE-----
```

ii. Immettere il contenuto del file chiave client da `/cfcard/kmip/certs/client.key` file:

Mostra un esempio di contenuto del file della chiave client

```
-----BEGIN RSA PRIVATE KEY-----  
<key_value>  
-----END RSA PRIVATE KEY-----
```

iii. Immettere il contenuto del file CA del server KMIP da `/cfcard/kmip/certs/CA.pem` file:

Mostra un esempio del contenuto del file del server KMIP

```
-----BEGIN CERTIFICATE-----  
<KMIP_certificate_CA_value>  
-----END CERTIFICATE-----
```

- iv. Immettere il contenuto del file di configurazione del server da /cfcard/kmip/servers.cfg file:

Mostra un esempio del contenuto del file di configurazione del server

```
xxx.xxx.xxx.xxx:5696.host=xxx.xxx.xxx.xxx
xxx.xxx.xxx.xxx:5696.port=5696
xxx.xxx.xxx.xxx:5696.trusted_file=/cfcard/kmip/certs/CA.pem
xxx.xxx.xxx.xxx:5696.protocol=KMIP1_4
1xxx.xxx.xxx.xxx:5696.timeout=25
xxx.xxx.xxx.xxx:5696.nbio=1
xxx.xxx.xxx.xxx:5696.cert_file=/cfcard/kmip/certs/client.crt
xxx.xxx.xxx.xxx:5696.key_file=/cfcard/kmip/certs/client.key
xxx.xxx.xxx.xxx:5696.ciphers="TLSv1.2:kRSA:!CAMELLIA:!IDEA:
!RC2:!RC4:!SEED:!eNULL:!aNULL"
xxx.xxx.xxx.xxx:5696.verify=true
xxx.xxx.xxx.xxx:5696.netapp_keystore_uuid=<id_value>
```

- v. Se richiesto, immettere l'UUID del cluster ONTAP dal nodo partner. È possibile controllare l'UUID del cluster dal nodo partner utilizzando `cluster identify show` comando.

Mostra un esempio di prompt UUID del cluster ONTAP

```
Notice: bootarg.mgwd.cluster_uuid is not set or is empty.
Do you know the ONTAP Cluster UUID? {y/n} y
Enter the ONTAP Cluster UUID: <cluster_uuid_value>

System is ready to utilize external key manager(s).
```

- vi. Se richiesto, immettere l'interfaccia di rete temporanea e le impostazioni per il nodo:
- L'indirizzo IP per la porta
 - La netmask per la porta
 - L'indirizzo IP del gateway predefinito

Mostra un esempio di richieste di impostazione di rete temporanee

```
In order to recover key information, a temporary network
interface needs to be
configured.
```

```
Select the network port you want to use (for example,
'e0a')
e0M
```

```
Enter the IP address for port : xxx.xxx.xxx.xxx
Enter the netmask for port : xxx.xxx.xxx.xxx
Enter IP address of default gateway: xxx.xxx.xxx.xxx
Trying to recover keys from key servers....
[discover_versions]
[status=SUCCESS reason= message=]
```

b. Verificare lo stato di ripristino della chiave:

- Se vedi `kmip2_client: Successfully imported the keys from external key server: xxx.xxx.xxx.xxx:5696` nell'output, la configurazione EKM è stata ripristinata correttamente. Il processo ripristina i file appropriati dal nodo partner e riavvia il nodo. Procedere al passaggio successivo.
- Se il ripristino della chiave non riesce, il sistema si blocca e visualizza messaggi di errore e di avviso. Eseguire nuovamente il processo di ripristino dal prompt `LOADER: boot_recovery -partner`

Mostrare un esempio di messaggi di errore e di avvertenza relativi al ripristino della chiave

```
ERROR: kmip_init: halting this system with encrypted
mroot...
WARNING: kmip_init: authentication keys might not be
available.
*****
*                      A T T E N T I O N                      *
*                                                                *
*          System cannot connect to key managers.              *
*                                                                *
*****
ERROR: kmip_init: halting this system with encrypted
mroot...
.
Terminated

Uptime: 11m32s
System halting...

LOADER-B>
```

- c. Dopo il riavvio del nodo, verificare che il sistema sia di nuovo online e operativo.
- d. Riportare il controller al funzionamento normale restituendo lo storage:

```
storage failover giveback -ofnode impaired_node_name
```

Vai a [riattivazione della restituzione automatica](#) se fosse disabilitato.

- 5. Se il giveback automatico è stato disabilitato, riabilitalo:

```
storage failover modify -node local -auto-giveback true
```

- 6. Se AutoSupport è attivato, ripristinare la creazione automatica dei casi:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Cosa succederà

Dopo aver ripristinato l'immagine ONTAP e dopo aver attivato e distribuito i dati, si ["Restituire la parte guasta a NetApp"](#).

Restituire il componente guasto a NetApp - ASA A1K

Se un componente del sistema ASA A1K non funziona, restituire il componente guasto a NetApp. Vedere la ["Restituzione e sostituzione delle parti"](#) pagina per ulteriori

informazioni.

Informazioni sul copyright

Copyright © 2026 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.