



E

SANtricity commands

NetApp
June 16, 2025

Sommario

E	1
Abilita il trasferimento dei dati del controller - SANtricity CLI	1
Array supportati	1
Ruoli	1
Sintassi	1
Parametro	1
Livello minimo del firmware	1
Abilita la sicurezza del pool di dischi - SANtricity CLI	1
Array supportati	1
Ruoli	2
Contesto	2
Sintassi	2
Parametro	2
Note	2
Livello minimo del firmware	2
Abilitare o disabilitare AutoSupport (tutti i singoli array) - SANtricity CLI	2
Array supportati	2
Ruoli	3
Contesto	3
Sintassi	3
Parametri	3
Verifica	3
Livello minimo del firmware	3
Abilitare la gestione delle chiavi di sicurezza esterne - SANtricity CLI	4
Array supportati	4
Ruoli	4
Contesto	4
Sintassi	4
Parametri	4
Note	5
Livello minimo del firmware	5
Abilita la funzionalità di array di archiviazione - SANtricity CLI	5
Array supportati	5
Ruoli	5
Contesto	6
Per attivare una chiave funzione	6
Per abilitare un Feature Pack	6
Per abilitare una funzione per un periodo di prova	7
Livello minimo del firmware	7
Abilita la sicurezza del gruppo di volumi - SANtricity CLI	7
Array supportati	7
Ruoli	7
Sintassi	7

Parametro	7
Note	7
Livello minimo del firmware	8
Stabilire una coppia speculare asincrona - SANtricity CLI	8
Array supportati	8
Ruoli	8
Contesto	8
Sintassi	8
Parametri	8
Note	9
Livello minimo del firmware	9
Esportazione della chiave di sicurezza dell'array di archiviazione - CLI SANtricity	9
Array supportati	9
Ruoli	10
Contesto	10
Sintassi	10
Parametri	10
Note	10
Livello minimo del firmware	11

E

Abilita il trasferimento dei dati del controller - SANtricity CLI

Il `enable controller dataTransfer` command consente di ripristinare un controller che è stato messo in stato di quiescenza durante l'esecuzione della diagnostica.

Array supportati

Questo comando si applica a qualsiasi singolo storage array, inclusi gli array E4000, E2700, E5600, E2800, E5700, EF600 e EF300, purché siano installati tutti i pacchetti SMcli.

Ruoli

Per eseguire questo comando su uno storage array E4000, E2800, E5700, EF600 o EF300, è necessario avere il ruolo di amministratore dello storage.

Sintassi

```
enable controller [(a|b)] dataTransfer
```

Parametro

Parametro	Descrizione
controller	Il controller che si desidera ripristinare. Gli identificatori del controller validi sono a oppure b, dove a È il controller nello slot A, e. b Il controller si trova nello slot B. Racchiudere l'identificatore del controller tra parentesi quadre ([]). Se non si specifica un controller, il software di gestione dello storage restituisce un errore di sintassi.

Livello minimo del firmware

6.10

Abilita la sicurezza del pool di dischi - SANtricity CLI

Il `enable diskPool security` il comando converte un pool di dischi non sicuro in un pool di dischi sicuro.

Array supportati

Questo comando si applica a qualsiasi singolo storage array, inclusi gli array E4000, E2700, E5600, E2800, E5700, EF600 e EF300, purché siano installati tutti i pacchetti SMcli.

Ruoli

Per eseguire questo comando su uno storage array E4000, E2800, E5700, EF600 o EF300, è necessario avere il ruolo di amministratore dello storage.

Contesto



Tutte le unità che compongono il pool di dischi devono essere sicure.

Sintassi

```
enable diskPool [<em>diskPoolName</em>] security
```

Parametro

Parametro	Descrizione
diskPool	Il nome del pool di dischi che si desidera inserire nello stato Security Enabled (protezione abilitata). Racchiudere l'identificatore del pool di dischi tra parentesi quadre ([]).

Note

Ciascun nome del pool di dischi deve essere univoco. È possibile utilizzare qualsiasi combinazione di caratteri alfanumerici, caratteri di sottolineatura (_), trattini (-) e cancelletto (n.) per l'etichetta utente. Le etichette dell'utente possono contenere un massimo di 30 caratteri.

Livello minimo del firmware

7.83

Abilitare o disabilitare AutoSupport (tutti i singoli array) - SANtricity CLI

Questo comando attiva o disattiva la funzione ASUP (AutoSupport) per lo storage array e consente di trasmettere messaggi al sito del supporto tecnico. Dopo aver attivato la funzione ASUP, lo storage array compatibile con ASUP viene automaticamente preparato per raccogliere e inviare i dati relativi al supporto al supporto tecnico. I dati possono quindi essere utilizzati per la risoluzione dei problemi e l'analisi dei problemi in remoto.

Array supportati

Questo comando si applica a qualsiasi singolo storage array, inclusi gli array E4000, E2700, E5600, E2800, E5700, EF600 e EF300, purché siano installati tutti i pacchetti SMcli.

Ruoli

Per eseguire questo comando su uno storage array E4000, E2800, E5700, EF600 o EF300, è necessario avere il ruolo di amministratore dello storage.

Contesto

Dopo aver attivato questa funzione, è possibile attivare la funzione AutoSupport on Demand (se si desidera), quindi attivare la funzione di diagnostica remota AutoSupport (se si desidera).

È necessario attivare le tre funzioni in questo ordine:

1. **Attiva AutoSupport**
2. **Attiva AutoSupport OnDemand**
3. **Attiva diagnostica remota AutoSupport**

Sintassi

```
set storageArray autoSupport (enable | disable)
```

Parametri

Parametro	Descrizione
`enable`	disable`

Esempi

```
SMcli -n Array1 -c "set storageArray autoSupport enable;"  
  
SMcli completed successfully.
```

Verifica

Utilizzare `show storageArray autoSupport` per verificare se la funzione è stata attivata. La riga iniziale dell'output visualizzato mostra lo stato di abilitazione:

```
The AutoSupport feature is enabled on this storage array.
```

Livello minimo del firmware

7.86 - comando aggiunto per tutti gli array di storage fino al modello E2700 ed E5600

8.40 - supporto aggiunto per E2800 ed E5700

Abilitare la gestione delle chiavi di sicurezza esterne - SANtricity CLI

Il `enable storageArray externalKeyManagement file` Command consente la gestione esterna delle chiavi di sicurezza per un array di storage dotato di dischi con crittografia completa del disco e crea la chiave di sicurezza iniziale del disco.

Array supportati

Questo comando si applica a un singolo array di storage E4000, E2800, E5700, EF600 o EF300. Non funziona sugli storage array E2700 o E5600.

Ruoli

Per eseguire questo comando su uno storage array E4000, E2800, E5700, EF600 o EF300, è necessario disporre del ruolo di amministratore della sicurezza.

Contesto



Questo comando si applica solo alla gestione esterna delle chiavi.

Sintassi

```
enable storageArray externalKeyManagement
file="<em>fileName</em>"
passPhrase="<em>passPhraseString</em>"
saveFile=<em>(TRUE | FALSE)</em>
```

Parametri

Parametro	Descrizione
file	<p>Il percorso del file e il nome del file in cui verrà memorizzata la nuova chiave di sicurezza. Racchiudere il percorso del file e il nome del file tra virgolette doppie (" "). Ad esempio:</p> <div><pre>file="C:\Program Files\CLI\sup\drivesecurity.slk"</pre></div> <div> Il nome del file deve avere un'estensione di .slk.</div>

Parametro	Descrizione
passPhrase	Stringa di caratteri che crittografa la chiave di protezione in modo da potervi memorizzare in un file esterno. Racchiudere la stringa di caratteri della password tra virgolette doppie (" ").
saveFile	Verifica e salva la chiave di sicurezza in un file. Impostare su FALSE per non salvare e verificare la chiave di sicurezza in un file. Il valore predefinito è TRUE.

Note

La password deve soddisfare i seguenti criteri:

- La lunghezza deve essere compresa tra 8 e 32 caratteri.
- Deve contenere almeno una lettera maiuscola.
- Deve contenere almeno una lettera minuscola.
- Deve contenere almeno un numero.
- Deve contenere almeno un carattere non alfanumerico, ad esempio < > @ +.



Se la password non soddisfa questi criteri, viene visualizzato un messaggio di errore.

Livello minimo del firmware

8.40

8.70 aggiunge *saveFile* parametro.

Abilita la funzionalità di array di archiviazione - SANtricity CLI

Il `enable storageArray feature file` il comando consente di attivare una funzionalità per un aggiornamento permanente dello storage array o per un periodo di prova.

Array supportati

Questo comando si applica a qualsiasi singolo storage array, inclusi gli array E4000, E2700, E5600, E2800, E5700, EF600 e EF300, purché siano installati tutti i pacchetti SMcli.

Ruoli

Per eseguire questo comando su uno storage array E4000, E2800, E5700, EF600 o EF300, è necessario disporre del ruolo di amministratore dello storage o di amministratore del supporto.

Contesto

Questo comando esegue una delle seguenti azioni:

- Attiva una chiave funzione per un aggiornamento permanente di una funzione
- Attiva una chiave funzione per un aggiornamento permanente di un Feature Pack
- Attiva una funzione per un periodo di prova

Un Feature Pack è un set predefinito di diverse funzionalità, come partizione dello storage e mirroring sincrono. Queste funzioni sono combinate per la comodità degli utenti. Quando gli utenti installano un Feature Pack, tutte le funzionalità del Feature Pack vengono installate contemporaneamente.

Ogni funzionalità è gestita da una chiave di licenza generata per una funzionalità o un Feature Pack specifico e per uno storage array specifico. La chiave di licenza viene fornita come file eseguito per applicare la licenza per la funzione.

Per determinare le funzionalità caricate nell'array di storage, eseguire `show storageArray features` comando. Il `show storageArray features` command elenca tutte le funzionalità installate sullo storage array, le quali possono essere valutate per un periodo di prova, le funzionalità attivate e le funzionalità disattivate.

Per attivare una chiave funzione

```
enable storageArray feature file="<em>filename</em>"
```

Il `file` il parametro identifica il percorso del file e il nome di un file feature key valido. Racchiudere il percorso del file e il nome del file tra virgolette doppie (" "). Ad esempio:

```
file="C:\Program Files\CLI\dnld\ftrkey.key"
```

I nomi di file validi per i file delle chiavi di funzione terminano con `.key` interno.

Per ciascuna funzione che si desidera attivare, è necessario un file delle chiavi di funzione.

Per abilitare un Feature Pack

```
enable storageArray featurePack file="<em>filename</em>"
```

Il `file` il parametro identifica il percorso del file e il nome del file di un file feature pack valido. Racchiudere il percorso del file e il nome del file tra virgolette doppie (" "). Ad esempio:

```
file="C:\Program Files\CLI\dnld\ftrpk.key"
```

I nomi di file validi per i file delle chiavi di funzione terminano con `.key` interno.

Per abilitare una funzione per un periodo di prova

```
enable storageArray feature=<em>featureAttributeList</em>
```

Per valutare una funzione per un periodo di prova, è possibile immettere uno o più dei seguenti valori di attributo per `featureAttributeList`. Se si inseriscono più valori di attributo, separare i valori con uno spazio.

- `driveSecurity`

Livello minimo del firmware

8.25 rimuove tutti gli attributi che non sono più validi.

Abilita la sicurezza del gruppo di volumi - SANtricity CLI

Il `enable volumeGroup security` il comando converte un gruppo di volumi non sicuro in un gruppo di volumi sicuro.

Array supportati

Questo comando si applica a qualsiasi singolo storage array, inclusi gli array E4000, E2700, E5600, E2800, E5700, EF600 e EF300, purché siano installati tutti i pacchetti SMcli.

Ruoli

Per eseguire questo comando su uno storage array E4000, E2800, E5700, EF600 o EF300, è necessario avere il ruolo di amministratore dello storage.

Sintassi

```
enable volumeGroup [<em>volumeGroupName</em>] security
```

Parametro

Parametro	Descrizione
<code>volumeGroup</code>	Il nome del gruppo di volumi che si desidera inserire nello stato Security Enabled (protezione abilitata). Racchiudere il nome del gruppo di volumi tra parentesi quadre ([]).

Note

Queste condizioni devono essere soddisfatte per eseguire correttamente questo comando.

- Tutti i dischi del gruppo di volumi devono essere dischi con crittografia completa.

- La funzione Drive Security deve essere attivata.
- È necessario impostare la chiave di sicurezza dello storage array.
- Il gruppo di volumi è ottimale e non dispone di volumi di repository.

Il firmware del controller crea un blocco che limita l'accesso ai dischi FDE. I dischi FDE hanno uno stato chiamato Security Capable. Quando si crea una chiave di sicurezza, lo stato viene impostato su Security Enabled (protezione abilitata), che limita l'accesso a tutti i dischi FDE presenti nell'array di storage.

Livello minimo del firmware

7.40

Stabilire una coppia speculare asincrona - SANtricity CLI

Il `establish asyncMirror volume` il comando completa una coppia di mirroring asincrono sull'array di storage remoto aggiungendo un volume secondario a un gruppo di mirror asincrono esistente.

Array supportati

Questo comando si applica a qualsiasi singolo storage array, inclusi gli array E4000, E2700, E5600, E2800, E5700, EF600 e EF300, purché siano installati tutti i pacchetti SMcli.

Ruoli

Per eseguire questo comando su uno storage array E4000, E2800, E5700, EF600 o EF300, è necessario avere il ruolo di amministratore dello storage.

Contesto

Prima di eseguire questo comando, il gruppo di mirror asincrono deve esistere e il volume primario deve esistere nel gruppo di mirror asincrono. Una volta completato correttamente questo comando, viene avviato il mirroring asincrono tra il volume primario e il volume secondario.

I due volumi che comprendono una coppia di mirroring asincrono funzionano come una singola entità. La creazione di una coppia asincrona con mirroring consente di eseguire azioni sull'intera coppia con mirroring rispetto ai due singoli volumi.

Sintassi

```
establish asyncMirror volume="<secondaryVolumeName>"
asyncMirrorGroup="<asyncMirrorGroupName>"
primaryVolume="<primaryVolumeName>"
```

Parametri

Parametro	Descrizione
volume	Il nome di un volume esistente nell'array di storage remoto che si desidera utilizzare per il volume secondario. Racchiudere il nome del volume tra virgolette doppie (" ").
asyncMirrorGroup	Il nome di un gruppo di mirror asincrono esistente che si desidera utilizzare per contenere la coppia di mirroring asincrono. Racchiudere il nome del gruppo mirror asincrono tra virgolette doppie (" ").
primaryVolume	Il nome di un volume esistente nell'array di storage locale che si desidera utilizzare per il volume primario. Racchiudere il nome del volume tra virgolette doppie (" ").

Note

Una coppia di mirroring asincrono è composta da due volumi, un volume primario e un volume secondario, che contengono copie identiche degli stessi dati. La coppia mirrorata fa parte di un gruppo di mirror asincrono, che consente alla coppia mirrorata di sincronizzarsi contemporaneamente a qualsiasi altra coppia mirrorata all'interno del gruppo di mirror asincrono.

È possibile utilizzare qualsiasi combinazione di caratteri alfanumerici, trattini e caratteri di sottolineatura per i nomi. I nomi possono avere un massimo di 30 caratteri.

Quando si scelgono il volume primario e il volume secondario, il volume secondario deve avere dimensioni uguali o superiori a quelle del volume primario. Il livello RAID del volume secondario non deve essere lo stesso del volume primario.

Livello minimo del firmware

7.84

11.80 aggiunge il supporto degli array EF600 e EF300

Esportazione della chiave di sicurezza dell'array di archiviazione - CLI SANtricity

Il `export storageArray securityKey` il comando salva una chiave di sicurezza del disco in un file.

Array supportati

Se è abilitata la gestione esterna delle chiavi, questo comando si applica solo agli array E4000, E2800, E5700, EF600 e EF300. Se è attivata la gestione delle chiavi interne, il comando si applica a qualsiasi singolo array di storage, purché siano installati tutti i pacchetti SMcli.

Ruoli

Per eseguire questo comando su uno storage array E4000, E2800, E5700, EF600 o EF300, è necessario disporre del ruolo di amministratore della sicurezza.

Contesto

Quando il file delle chiavi viene esportato da un array di storage, tale chiave può essere importata in un altro array di storage. In questo modo è possibile spostare dischi con funzionalità di sicurezza tra array di storage.



Questo comando si applica alla gestione delle chiavi sia interna che esterna.

Sintassi

```
export storageArray securityKey  
passPhrase="<em>passPhraseString</em>"  
file="<em>fileName</em>"
```

Parametri

Parametro	Descrizione
passPhrase	Stringa di caratteri che crittografa la chiave di protezione in modo da potervi memorizzare in un file esterno. Racchiudere la passphrase tra virgolette doppie (" ").
file	<div>Il percorso del file e il nome del file in cui si desidera salvare la chiave di sicurezza. Ad esempio:</div> <div><pre>file="C:\Program Files\CLI\sup\drivesecurity.slk"</pre></div> <div> Il nome del file deve avere un'estensione di .slk.</div>

Note

L'array di storage su cui verranno trasferiti i dischi deve avere dischi con una capacità uguale o superiore a quella dei dischi che si stanno importando.

Il firmware del controller crea un blocco che limita l'accesso ai dischi con crittografia completa del disco (FDE). I dischi FDE hanno uno stato chiamato Security Capable. Quando si crea una chiave di sicurezza, lo stato viene impostato su Security Enabled (protezione abilitata), che limita l'accesso a tutti i dischi FDE presenti nell'array di storage.

La password deve soddisfare i seguenti criteri:

- La lunghezza deve essere compresa tra 8 e 32 caratteri.
- Non deve contenere spazi vuoti.
- Deve contenere almeno una lettera maiuscola.
- Deve contenere almeno una lettera minuscola.
- Deve contenere almeno un numero.
- Deve contenere almeno un carattere non alfanumerico, ad esempio < > @ +.



Se la password non soddisfa questi criteri, viene visualizzato un messaggio di errore e viene richiesto di riprovare a eseguire il comando.

Livello minimo del firmware

7.40

Informazioni sul copyright

Copyright © 2025 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.