



# Informazioni su StorageGRID 11.5

## StorageGRID 11.5

NetApp  
April 11, 2024

# Sommario

- Informazioni su StorageGRID 11.5 ..... 1
  - Novità di StorageGRID 11.5 ..... 1
  - Funzionalità rimosse o obsolete ..... 9
  - Modifiche all'API Grid Management ..... 12
  - Modifiche all'API di gestione del tenant ..... 14

# Informazioni su StorageGRID 11.5

Prima di iniziare un aggiornamento, consulta questa sezione per scoprire le nuove funzionalità e i miglioramenti di StorageGRID 11.5, determinare se le funzionalità sono state obsolete o rimosse e scoprire le modifiche apportate alle API StorageGRID.

- ["Novità di StorageGRID 11.5"](#)
- ["Funzionalità rimosse o obsolete"](#)
- ["Modifiche all'API Grid Management"](#)
- ["Modifiche all'API di gestione del tenant"](#)

## Novità di StorageGRID 11.5

StorageGRID 11.5 introduce il blocco oggetti S3, il supporto per la crittografia KMIP dei dati, i miglioramenti dell'usabilità di ILM, un'interfaccia utente di Tenant Manager riprogettata, il supporto per la disattivazione di un sito StorageGRID e una procedura di clone del nodo dell'appliance.

### Blocco oggetti S3 per dati conformi

La funzionalità blocco oggetti S3 di StorageGRID 11.5 è una soluzione di protezione degli oggetti equivalente a blocco oggetti S3 in Amazon Simple Storage Service (Amazon S3). È possibile attivare l'impostazione di blocco oggetti S3 globale per un sistema StorageGRID per consentire agli account tenant S3 di creare bucket con blocco oggetti S3 attivato. Il tenant può quindi utilizzare un'applicazione client S3 per specificare facoltativamente le impostazioni di conservazione e conservazione legale per gli oggetti in tali bucket.

S3 Object Lock consente agli utenti tenant di rispettare le normative che richiedono la conservazione di determinati oggetti per un periodo di tempo fisso o indefinito.

#### Scopri di più

- ["Gestire gli oggetti con ILM"](#)
- ["Utilizzare S3"](#)
- ["Utilizzare un account tenant"](#)

### Gestione delle chiavi di crittografia KMS

È ora possibile configurare uno o più server di gestione delle chiavi (KMS) esterni in Grid Manager per fornire chiavi di crittografia ai servizi StorageGRID e alle appliance di storage. Ogni cluster KMS o KMS utilizza il protocollo KMIP (Key Management Interoperability Protocol) per fornire una chiave di crittografia ai nodi appliance nel sito StorageGRID associato. Una volta crittografati i volumi dell'appliance, non è possibile accedere ai dati dell'appliance a meno che il nodo non sia in grado di comunicare con il KMS.



Se si desidera utilizzare la gestione delle chiavi di crittografia, è necessario utilizzare il programma di installazione dell'appliance StorageGRID per attivare l'impostazione **crittografia del nodo** dell'appliance prima di aggiungere l'appliance alla griglia.

#### Scopri di più

- ["Amministrare StorageGRID"](#)

## Miglioramenti dell'usabilità per la gestione del ciclo di vita delle informazioni (ILM)

- È ora possibile visualizzare la capacità totale di un pool di storage, inclusa la quantità di spazio utilizzato e libero. È inoltre possibile vedere quali nodi sono inclusi in un pool di storage e quali regole ILM e profili di codifica Erasure utilizzano il pool di storage.
- È ora possibile progettare regole ILM applicabili a più account tenant.
- Quando si crea una regola ILM per la cancellazione del codice, viene ora ricordato di impostare il filtro avanzato Object Size (MB) su un valore superiore a 0.2 per garantire che gli oggetti molto piccoli non vengano sottoposti a erasure coding.
- L'interfaccia dei criteri ILM garantisce che la regola ILM predefinita venga sempre utilizzata per qualsiasi oggetto non associato a un'altra regola. A partire da StorageGRID 11.5, la regola predefinita non può utilizzare alcun filtro di base o avanzato e viene automaticamente inserita come ultima regola nel criterio.



Se la policy ILM corrente non è conforme ai nuovi requisiti, è possibile continuare a utilizzarla dopo l'aggiornamento a StorageGRID 11.5. Tuttavia, se si tenta di clonare un criterio non conforme dopo l'aggiornamento, viene richiesto di selezionare una regola predefinita che non include i filtri e di inserire la regola predefinita alla fine del criterio.

- Il pool di storage di tutti i nodi storage non viene più selezionato per impostazione predefinita quando si crea una nuova regola ILM o un nuovo profilo di codifica Erasure. Inoltre, è ora possibile rimuovere il pool di storage All Storage Node, purché non sia utilizzato in nessuna regola.



L'utilizzo del pool di storage All Storage Node non è consigliato perché questo pool di storage contiene tutti i siti. Se si utilizza questo pool di storage con un sistema StorageGRID che include più siti, è possibile posizionare più copie di un oggetto sullo stesso sito.

- È ora possibile rimuovere la regola Make 2 Copies (che utilizza il pool di storage All Storage Node) purché non sia utilizzata in una policy attiva o proposta.
- Gli oggetti memorizzati in un Cloud Storage Pool possono ora essere cancellati immediatamente (eliminazione sincrona).

### Scopri di più

- ["Gestire gli oggetti con ILM"](#)

## Miglioramenti a Grid Manager

- La nuova pagina account tenant semplifica la visualizzazione dell'utilizzo dell'account tenant. La tabella di riepilogo dei tenant ora include le colonne spazio utilizzato, utilizzo della quota, quota e Conteggio oggetti. Un nuovo pulsante **View Details** consente di accedere a una panoramica di ciascun tenant e ai dettagli sui bucket S3 o sui container Swift dell'account. Inoltre, ora è possibile esportarne due `.csv` file per l'utilizzo del tenant: uno contenente i valori di utilizzo per tutti i tenant e uno contenente i dettagli sui bucket o sui container di un tenant.

In relazione a questo cambiamento, sono state aggiunte tre nuove metriche Prometheus per tenere traccia dell'utilizzo dell'account tenant:

- `storagegrid_tenant_usage_data_bytes`
- `storagegrid_tenant_usage_object_count`
- `storagegrid_tenant_usage_quota_bytes`

- Il nuovo campo **Access Mode** nella pagina Admin Groups (**Configuration > Access Control**) consente di specificare se le autorizzazioni di gestione per il gruppo sono di lettura/scrittura (impostazione predefinita) o di sola lettura. Gli utenti che appartengono a un gruppo con modalità di accesso in lettura/scrittura possono modificare le impostazioni ed eseguire operazioni in Grid Manager e nell'API Grid Management. Gli utenti che appartengono a un gruppo con modalità di accesso di sola lettura possono visualizzare solo le impostazioni e le funzioni selezionate per il gruppo.



Quando si esegue l'aggiornamento a StorageGRID 11.5, l'opzione della modalità di accesso in lettura/scrittura viene selezionata per tutti i gruppi di amministratori esistenti.

- L'interfaccia utente di AutoSupport è stata riprogettata. È ora possibile configurare i messaggi AutoSupport attivati dagli eventi, attivati dall'utente e settimanali da una singola pagina in Gestione griglia. È inoltre possibile configurare una destinazione aggiuntiva per i messaggi AutoSupport.



Se AutoSupport non è stato attivato, viene visualizzato un messaggio di promemoria sul dashboard di gestione della griglia.

- Quando si visualizza il grafico **Storage used - Object Data** nella pagina Nodes (nodi), è possibile visualizzare le stime relative alla quantità di dati degli oggetti replicati e alla quantità di dati con codifica di cancellazione nella griglia, nel sito o nel nodo di storage (**Node > Grid/Site/Storage Node > Storage**).
- Le opzioni del menu di Grid Manager sono state riorganizzate per semplificare la ricerca delle opzioni. Ad esempio, è stato aggiunto un nuovo sottomenu **Impostazioni di rete** al menu **Configurazione** e le opzioni dei menu **manutenzione** e **supporto** sono ora elencate in ordine alfabetico.

#### Scopri di più

- ["Amministrare StorageGRID"](#)

## Miglioramenti di Tenant Manager

- L'aspetto e l'organizzazione dell'interfaccia utente di Tenant Manager sono stati completamente riprogettati per migliorare l'esperienza utente.
- La nuova dashboard di Tenant Manager fornisce un riepilogo di alto livello di ciascun account: Fornisce dettagli sui bucket e mostra il numero di bucket o container, gruppi, utenti e endpoint dei servizi della piattaforma (se configurati).

#### Scopri di più

- ["Utilizzare un account tenant"](#)

## Certificati client per l'esportazione delle metriche Prometheus

È ora possibile caricare o generare certificati client (**Configurazione > controllo accessi > certificati client**), che possono essere utilizzati per fornire un accesso sicuro e autenticato al database StorageGRID Prometheus. Ad esempio, è possibile utilizzare i certificati client se è necessario monitorare StorageGRID esternamente utilizzando Grafana.

#### Scopri di più

- ["Amministrare StorageGRID"](#)

## Miglioramenti del bilanciamento del carico

- Durante la gestione delle richieste di routing in un sito, il servizio Load Balancer esegue ora il routing in

base al carico: Considera la disponibilità della CPU dei nodi di storage nello stesso sito. In alcuni casi, le informazioni sulla disponibilità della CPU sono limitate al sito in cui si trova il servizio Load Balancer.



La consapevolezza della CPU non verrà attivata fino a quando almeno due terzi dei nodi di storage di un sito non saranno stati aggiornati a StorageGRID 11.5 e non saranno state riportate le statistiche della CPU.

- Per una maggiore sicurezza, è ora possibile specificare una modalità di binding per ogni endpoint del bilanciamento del carico. Il pinning degli endpoint consente di limitare l'accessibilità di ciascun endpoint a specifici gruppi ad alta disponibilità o interfacce di nodi.

### Scopri di più

- ["Amministrare StorageGRID"](#)

## Modifiche ai metadati degli oggetti

- **Nuova metrica dello spazio riservato effettivo:** Per aiutarti a comprendere e monitorare l'utilizzo dello spazio dei metadati degli oggetti su ciascun nodo di storage, viene visualizzata una nuova metrica Prometheus nel grafico Storage Used - Object Metadata per un nodo di storage (**Node > Storage Node > Storage**).

```
storagegrid_storage_utilization_metadata_reserved
```

La metrica **spazio riservato effettivo** indica lo spazio riservato da StorageGRID per i metadati dell'oggetto su un nodo di storage specifico.

- **Spazio di metadati aumentato per le installazioni con nodi di storage più grandi:** L'impostazione spazio riservato dei metadati a livello di sistema è stata aumentata per i sistemi StorageGRID contenenti nodi di storage con almeno 128 GB di RAM, come segue:
  - **8 TB per le nuove installazioni:** Se si installa un nuovo sistema StorageGRID 11.5 e ciascun nodo di storage nella griglia dispone di almeno 128 GB di RAM, l'impostazione spazio riservato metadati a livello di sistema è ora impostata su 8 TB invece di 3 TB.
  - **4 TB per gli aggiornamenti:** Se si esegue l'aggiornamento a StorageGRID 11.5 e ogni nodo di storage di un sito dispone di almeno 128 GB di RAM, l'impostazione spazio riservato metadati a livello di sistema è ora impostata su 4 TB invece di 3 TB.

I nuovi valori per l'impostazione spazio riservato metadati aumentano lo spazio consentito per i metadati per questi nodi di storage più grandi, fino a 2.64 TB, e garantiscono che lo spazio riservato ai metadati sia adeguato per le versioni future dell'hardware e del software.



Se i nodi di storage dispongono di RAM sufficiente e spazio sufficiente sul volume 0, è possibile aumentare manualmente l'impostazione di Metadata Reserved Space fino a 8 TB dopo l'aggiornamento. Riservando ulteriore spazio di metadati dopo l'aggiornamento a StorageGRID 11.5 sarà possibile semplificare gli aggiornamenti futuri di hardware e software.

["Aumento dell'impostazione Metadata Reserved Space \(spazio riservato metadati\)"](#)

+



Se il sistema StorageGRID memorizza (o si prevede di memorizzare) più di 2.64 TB di metadati su qualsiasi nodo di storage, in alcuni casi lo spazio consentito per i metadati può essere aumentato. Se ciascuno dei nodi di storage dispone di spazio libero sul volume di storage 0 e oltre 128 GB di RAM, contattare il rappresentante NetApp. NetApp esaminerà i tuoi requisiti e, se possibile, aumenterà lo spazio di metadati consentito per ciascun nodo di storage.

- **Pulizia automatica dei metadati cancellati:** Quando il 20% o più dei metadati memorizzati su un nodo di storage è pronto per essere rimosso (perché gli oggetti corrispondenti sono stati cancellati), StorageGRID può ora eseguire una compattazione automatica su quel nodo di storage. Questo processo in background viene eseguito solo se il carico sul sistema è basso, ovvero quando sono disponibili CPU, spazio su disco e memoria. Il nuovo processo di compaction rimuove i metadati per gli oggetti cancellati prima delle release precedenti e aiuta a liberare spazio per i nuovi oggetti da memorizzare.

### Scopri di più

- ["Amministrare StorageGRID"](#)

## Modifiche al supporto delle API REST S3

- È ora possibile utilizzare l'API REST S3 per specificare [Blocco oggetti S3](#) impostazioni:
  - Per creare un bucket con S3 Object Lock attivato, utilizzare una richiesta PUT bucket con `x-amz-bucket-object-lock-enabled` intestazione.
  - Per determinare se S3 Object Lock è attivato per un bucket, utilizzare una richiesta GET Object Lock Configuration.
  - Quando si aggiunge una versione dell'oggetto a un bucket con blocco oggetto S3 attivato, utilizzare le seguenti intestazioni di richiesta per specificare le impostazioni di conservazione e conservazione legale: `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, e. `x-amz-object-lock-legal-hold`.
- È ora possibile utilizzare L'OPZIONE DI ELIMINAZIONE di più oggetti su un bucket con versione.
- Ora puoi utilizzare LE richieste di crittografia PUT, GET ed ELIMINA bucket per gestire la crittografia per un bucket S3 esistente.
- È stata apportata una piccola modifica al nome di un campo per `Expiration` parametro. Questo parametro è incluso nella risposta a un oggetto PUT, UN oggetto HEAD o UNA richiesta DI oggetto GET se una regola di scadenza nella configurazione del ciclo di vita si applica a un oggetto specifico. Il campo che indica la regola di scadenza associata è stato precedentemente denominato `rule_id`. Questo campo è stato rinominato in `rule-id` in modo che corrisponda all'implementazione AWS.
- Per impostazione predefinita, la richiesta S3 GET Storage Usage tenta ora di recuperare lo storage utilizzato da un account tenant e dai relativi bucket utilizzando una coerenza forte-globale. Se non è possibile ottenere una coerenza globale, StorageGRID tenta di recuperare le informazioni di utilizzo utilizzando una coerenza forte del sito.
- Il `Content-MD5` l'intestazione della richiesta è ora supportata correttamente.

### Scopri di più

- ["Utilizzare S3"](#)

## Le dimensioni massime degli oggetti CloudMirror sono aumentate a 5 TB

La dimensione massima degli oggetti che possono essere replicati in un bucket di destinazione dal servizio di replica CloudMirror è stata aumentata a 5 TB, ovvero la dimensione massima degli oggetti supportata da

StorageGRID.

### Scopri di più

- ["Utilizzare S3"](#)
- ["USA Swift"](#)

## Nuovi avvisi aggiunti

Sono stati aggiunti i seguenti nuovi avvisi per StorageGRID 11.5:

- Errore di comunicazione BMC dell'appliance
- Rilevato guasto nel Fibre Channel dell'appliance
- Errore della porta HBA Fibre Channel dell'appliance
- Porta LACP dell'appliance mancante
- Errore compattatore automatico Cassandra
- Metriche del compattatore automatico Cassandra non aggiornate
- Le compaction di Cassandra sono sovraccaricate
- L'i/o del disco è molto lento
- Scadenza del certificato CA KMS
- Scadenza del certificato client KMS
- Impossibile caricare la configurazione KMS
- Errore di connettività KMS
- Nome chiave di crittografia KMS non trovato
- Rotazione della chiave di crittografia KMS non riuscita
- KMS non configurato
- La chiave KMS non è riuscita a decrittare un volume dell'appliance
- Scadenza del certificato del server KMS
- Spazio libero ridotto per il pool di storage
- Errore frame ricezione rete nodo
- Connettività dello storage dell'appliance di servizi degradata
- Connettività dello storage dell'appliance di storage degradata (in precedenza denominata connettività dello storage dell'appliance degradata)
- Utilizzo elevato della quota del tenant
- Riavvio del nodo imprevisto

### Scopri di più

- ["Monitor risoluzione dei problemi"](#)

## Supporto TCP per trap SNMP

È ora possibile selezionare il protocollo TCP (Transmission Control Protocol) come protocollo per le destinazioni trap SNMP. In precedenza, era supportato solo il protocollo UDP (User Datagram Protocol).



## Scopri di più

- ["Monitor risoluzione dei problemi"](#)

## Miglioramenti all'installazione e alla rete

- **Clonazione indirizzo MAC:** Ora è possibile utilizzare la clonazione indirizzo MAC per migliorare la sicurezza di alcuni ambienti. La clonazione dell'indirizzo MAC consente di utilizzare una NIC virtuale dedicata per Grid Network, Admin Network e Client Network. Il fatto che il container Docker utilizzi l'indirizzo MAC della NIC dedicata sull'host consente di evitare l'utilizzo di configurazioni di rete promiscue mode. Tre nuove chiavi di clonazione dell'indirizzo MAC sono state aggiunte al file di configurazione del nodo per i nodi basati su Linux (bare metal).
- **Rilevamento automatico delle route host DNS e NTP:** In precedenza, esistevano restrizioni sulla rete a cui dovevano connettersi i server NTP e DNS, come ad esempio il requisito che non era possibile avere tutti i server NTP e DNS sulla rete client. A questo punto, tali restrizioni vengono rimosse.

## Scopri di più

- ["Installare Red Hat Enterprise Linux o CentOS"](#)
- ["Installare Ubuntu o Debian"](#)

## Supporto per il ribilanciamento dei dati EC (erasure-coded) dopo l'espansione del nodo di storage

La procedura di ribilanciamento EC è un nuovo script della riga di comando che potrebbe essere richiesto dopo l'aggiunta di nuovi nodi di storage. Quando si esegue la procedura, StorageGRID ridistribuisce i frammenti con codifica erasure tra i nodi di storage esistenti e quelli appena espansi in un sito.



La procedura di ribilanciamento EC deve essere eseguita solo in casi limitati. Ad esempio, se non è possibile aggiungere il numero consigliato di nodi di storage in un'espansione, è possibile utilizzare la procedura di ribilanciamento EC per consentire la memorizzazione di oggetti con codifica di cancellazione aggiuntivi.

## Scopri di più

- ["Espandi il tuo grid"](#)

## Procedure di manutenzione nuove e riviste

- **Disattivazione sito:** È ora possibile rimuovere un sito operativo dal sistema StorageGRID. La procedura di decommissionamento del sito connesso rimuove un sito operativo e conserva i dati. La nuova procedura guidata del sito di decommissionazione guida l'utente attraverso il processo (**Maintenance > Decommission > Decommission Site**).
- **Appliance node cloning:** È ora possibile clonare un nodo appliance esistente per aggiornare il nodo a un nuovo modello di appliance. Ad esempio, è possibile clonare un nodo appliance di capacità inferiore in un'appliance di capacità superiore. È inoltre possibile clonare un nodo appliance per implementare nuove funzionalità, come la nuova impostazione **Node Encryption** richiesta per la crittografia KMS.
- **Possibilità di modificare la passphrase di provisioning:** È ora possibile modificare la passphrase di provisioning (**Configuration > Access Control > Grid passwords**). La passphrase è necessaria per le procedure di ripristino, espansione e manutenzione.
- **Comportamento avanzato della password SSH:** Per migliorare la sicurezza delle appliance StorageGRID, la password SSH non viene più modificata quando si attiva la modalità di manutenzione dell'appliance. Inoltre, i nuovi certificati host SSH e le chiavi host vengono generati quando si aggiorna un

nodo a StorageGRID 11.5.



Se si utilizza SSH per accedere a un nodo dopo l'aggiornamento a StorageGRID 11.5, viene visualizzato un avviso che indica che la chiave host è stata modificata. Questo comportamento è previsto e puoi approvare la nuova chiave in tutta sicurezza.

### Scopri di più

- ["Mantieni Ripristina"](#)

## Modifiche alle appliance StorageGRID

- **Accesso diretto a Gestione di sistema SANtricity per le appliance di storage:** È ora possibile accedere all'interfaccia utente di Gestione di sistema e-Series SANtricity dal programma di installazione dell'appliance StorageGRID e da Gestione griglia. L'utilizzo di questi nuovi metodi consente di accedere a Gestore di sistema di SANtricity senza utilizzare la porta di gestione dell'appliance. Gli utenti che devono accedere a Gestione di sistema SANtricity da Gestione griglia devono disporre dell'autorizzazione di amministratore per le nuove appliance di storage.
- **Crittografia del nodo:** Come parte della nuova funzione di crittografia KMS, è stata aggiunta una nuova impostazione **crittografia del nodo** al programma di installazione dell'appliance StorageGRID. Se si desidera utilizzare la gestione delle chiavi di crittografia per proteggere i dati dell'appliance, è necessario attivare questa impostazione durante la fase di configurazione hardware dell'installazione dell'appliance.
- **Connettività della porta UDP:** È ora possibile verificare la connettività di rete di un'appliance StorageGRID alle porte UDP, ad esempio quelle utilizzate per un server NFS o DNS esterno. Dal programma di installazione dell'appliance StorageGRID, selezionare **Configura rete > Test connettività porta (nmap)**.
- **Installazione e configurazione automatizzate:** È stata aggiunta una nuova pagina di caricamento della configurazione JSON al programma di installazione dell'appliance StorageGRID (**Avanzate > Aggiorna configurazione dell'appliance**). Questa pagina consente di utilizzare un unico file per configurare più appliance in griglie di grandi dimensioni. Inoltre, il `configure-sga.py` Lo script Python è stato aggiornato per soddisfare le funzionalità del programma di installazione dell'appliance StorageGRID.

### Scopri di più

- ["SG100 SG1000 Services appliance"](#)
- ["Appliance di storage SG6000"](#)
- ["Appliance di storage SG5700"](#)
- ["Appliance di storage SG5600"](#)

## Modifiche ai messaggi di audit

- **Pulizia automatica degli oggetti sovrascritti:** In precedenza, gli oggetti sovrascritti non venivano rimossi dal disco in casi specifici, con conseguente consumo di spazio aggiuntivo. Questi oggetti sovrascritti, inaccessibili agli utenti, vengono ora rimossi automaticamente per risparmiare spazio di storage. Per ulteriori informazioni, fare riferimento al messaggio di audit LKCU.
- **Nuovi codici di audit per S3 Object Lock:** Quattro nuovi codici di audit sono stati aggiunti al messaggio di audit SPUT da includere [Blocco oggetti S3](#) intestazioni delle richieste:
  - LKEN: Blocco oggetto attivato
  - LKLH: Blocco oggetto blocco Legal Hold
  - LKMD: Modalità di conservazione blocco oggetti

- LKRU: Conservazione blocco oggetto fino alla data
- **Nuovi campi per l'ora dell'ultima modifica e la dimensione dell'oggetto precedente:** È ora possibile tenere traccia del momento in cui un oggetto è stato sovrascritto e della dimensione dell'oggetto originale.
  - Il campo MTME (ultima modifica) è stato aggiunto ai seguenti messaggi di audit:
    - SDEL (ELIMINAZIONE S3)
    - SPUT (S3 PUT)
    - WDEL (ELIMINAZIONE Swift)
    - WPUT (Swift PUT)
  - Il campo CSIZ (Previous Object Size) è stato aggiunto al messaggio di audit OVWR (Object Overwrite).

#### Scopri di più

- ["Esaminare i registri di audit"](#)

## Nuovo file nms.requestlog

Un nuovo file di log, `/var/local/log/nms.requestlog`, Viene gestito su tutti i nodi Admin. Questo file contiene informazioni sulle connessioni in uscita dall'API di gestione ai servizi StorageGRID interni.

#### Scopri di più

- ["Monitor risoluzione dei problemi"](#)

## Modifiche alla documentazione di StorageGRID

- Per facilitare la ricerca e la chiarimento delle informazioni e dei requisiti di rete applicabili anche ai nodi appliance StorageGRID, la documentazione di rete è stata spostata dalle guide di installazione basate su software (RedHat Enterprise Linux/CentOS, Ubuntu/Debian e VMware) a una nuova guida di rete.

["Linee guida per la rete"](#)

- Per semplificare la ricerca di istruzioni ed esempi relativi a ILM, la documentazione per la gestione degli oggetti con gestione del ciclo di vita delle informazioni è stata spostata dalla *Guida dell'amministratore* a una nuova guida ILM.

["Gestire gli oggetti con ILM"](#)

- Una nuova guida FabricPool fornisce una panoramica sulla configurazione di StorageGRID come livello cloud NetApp FabricPool e descrive le Best practice per la configurazione di ILM e altre opzioni StorageGRID per un carico di lavoro FabricPool.

["Configurare StorageGRID per FabricPool"](#)

- Ora puoi accedere a diversi video di istruzioni da Grid Manager. I video attuali forniscono istruzioni per la gestione di avvisi, avvisi personalizzati, regole ILM e policy ILM.

## Funzionalità rimosse o obsolete

Alcune funzionalità sono state rimosse o obsolete in StorageGRID 11.5. È necessario esaminare questi elementi per capire se è necessario aggiornare le applicazioni client o modificare la configurazione prima di eseguire l'aggiornamento.

## Rimozione di un controllo di coerenza debole

Il controllo di coerenza debole è stato rimosso per StorageGRID 11.5. Dopo l'aggiornamento, si applicano i seguenti comportamenti:

- Le richieste di impostazione della coerenza debole per un bucket S3 o un container Swift avranno esito positivo, ma il livello di coerenza verrà effettivamente impostato su disponibile.
- I bucket e i container esistenti che utilizzano una scarsa coerenza verranno aggiornati in modo invisibile per utilizzare la coerenza disponibile.
- Le richieste con un'intestazione di controllo della coerenza debole utilizzeranno effettivamente la coerenza disponibile, se applicabile.

Il controllo di coerenza disponibile si comporta come il livello di coerenza "read-after-new-write", ma fornisce solo una coerenza finale per le operazioni HEAD. Il controllo di coerenza disponibile offre una maggiore disponibilità per le operazioni HEAD rispetto a "read-after-new-write" se i nodi storage non sono disponibili.


## Allarme per stato di salute della rete deprecato

Il `/grid/health/topology` L'API, che verifica la presenza di *allarmi* attivi sui nodi, è obsoleta. Al suo posto, un nuovo `/grid/node-health` è stato aggiunto l'endpoint. Questa API restituisce lo stato corrente di ciascun nodo controllando i *alert* attivi sui nodi.

## Funzionalità di compliance obsoleta

La funzionalità blocco oggetti S3 di StorageGRID 11.5 sostituisce la funzionalità di conformità disponibile nelle versioni precedenti di StorageGRID. Poiché la nuova funzione blocco oggetti S3 è conforme ai requisiti di Amazon S3, non è più compatibile con la funzionalità proprietaria di conformità StorageGRID, ora denominata "conformità legacy".

Se in precedenza è stata attivata l'impostazione di conformità globale, la nuova impostazione di blocco oggetti S3 globale viene attivata automaticamente quando si esegue l'aggiornamento a StorageGRID 11.5. Gli utenti del tenant non saranno più in grado di creare nuovi bucket con la conformità abilitata in StorageGRID; tuttavia, come richiesto, gli utenti del tenant possono continuare a utilizzare e gestire qualsiasi bucket compatibile esistente.

In Tenant Manager, un'icona di shield  Indica un bucket compatibile legacy. I bucket conformi alle versioni precedenti potrebbero anche avere un badge Hold  per indicare che il bucket è sottoposto a un blocco legale.

["KB: Come gestire i bucket legacy conformi in StorageGRID 11.5"](#)

["Gestire gli oggetti con ILM"](#)

## Rimozione dell'avviso "s 3 multiparte troppo piccola"

L'avviso **S3 multipart too Small** è stato rimosso. In precedenza, questo avviso veniva attivato se un client S3 tentava di completare un caricamento multiparte con parti che non soddisfacevano i limiti di dimensione di Amazon S3. Dopo l'aggiornamento a StorageGRID 11.5, tutte le richieste di caricamento multiparte che non soddisfano i seguenti limiti di dimensione non avranno esito positivo:

- Ciascuna parte di un caricamento multiparte deve essere compresa tra 5 MiB (5,242,880 byte) e 5 GiB (5,368,709,120 byte).

- L'ultima parte può essere inferiore a 5 MiB (5,242,880 byte).
- In generale, le dimensioni delle parti devono essere il più grandi possibile. Ad esempio, utilizzare le dimensioni delle parti di 5 GiB per un oggetto 100 GiB. Poiché ogni parte è considerata un oggetto unico, l'utilizzo di parti di grandi dimensioni riduce l'overhead dei metadati StorageGRID.
- Per gli oggetti di dimensioni inferiori a 5 GiB, prendere in considerazione l'utilizzo di un caricamento non multiparte.

## Rimozione degli avvisi "collegamento dell'appliance alla rete Grid"

I seguenti avvisi sono stati rimossi. Se Grid Network non è attivo, le metriche che attiverrebbero questi avvisi non sono accessibili:

- Collegamento dell'appliance di servizi su Grid Network
- Collegamento dell'appliance di storage su Grid Network

## Supporto per nome di dominio completo rimosso dalla configurazione SNMP

Quando si configura un server SNMP nel BMC (Baseboard Management Controller) per SG6000, SG100 o SG1000, è necessario specificare un indirizzo IP invece di un nome di dominio completo. Se in precedenza era stato configurato un nome di dominio completo, cambiarlo in un indirizzo IP prima di eseguire l'aggiornamento a StorageGRID 11.5.

## Rimozione degli attributi legacy

I seguenti attributi legacy sono stati rimossi. A seconda dei casi, le informazioni equivalenti vengono fornite dalle metriche Prometheus:

Attributo legacy	Metrica Prometheus equivalente
BEC	storagegrid_service_network_received_bytes
BTRA	storagegrid_service_network_transmitted_bytes
CQST	storagegrid_metadata_queries_average_latency_millisecondi
HAIS	storagegrid_http_sessions_incoming_tented
HCC	storagegrid_http_sessions_incoming_currently_established
HEL5	storagegrid_http_sessions_incoming_failed
ISC	storagegrid_http_sessions_incoming_successful
LHAC	<i>nessuno</i>
NREC	<i>nessuno</i>
NTSO (Time Source Offset scelto)	storagegrid_ntp_chouged_time_source_offset_millisecondi

Attributo legacy	Metrica Prometheus equivalente
NTRA	<i>nessuno</i>
SLOD	storagegrid_service_load
SMEM	storagegrid_service_memory_usage_bytes
SUTM	storagegrid_service_cpu_seconds
SVUT	storagegrid_service_uptime_seconds
TRB (bit totali al secondo ricevuti)	<i>nessuno</i>
TRXB	storagegrid_network_received_bytes
TTBS (bit totali al secondo trasmessi)	<i>nessuno</i>
TTXB	storagegrid_network_transmitted_bytes

Sono state apportate anche le seguenti modifiche correlate:

- Il `network_received_bytes` e `network_transmitted_bytes` Le metriche Prometheus sono state modificate da indicatori a contatori perché i valori di queste metriche aumentano solo. Se si utilizzano attualmente queste metriche nelle query Prometheus, è necessario iniziare a utilizzare `increase()` nella query.
- La tabella risorse di rete è stata rimossa dalla scheda risorse per i servizi StorageGRID. (Selezionare **supporto > Strumenti > topologia griglia**. quindi, selezionare **nodo > servizio > risorse**.)
- La pagina delle sessioni HTTP è stata rimossa per i nodi di storage. In precedenza, era possibile accedere a questa pagina selezionando **supporto > Strumenti > topologia griglia** e selezionando **nodo di storage > LDR > HTTP**.
- L'allarme HCC (sessioni in entrata attualmente stabilite) è stato rimosso.
- L'allarme NTSO (Time Source Offset) è stato rimosso.

## Modifiche all'API Grid Management

StorageGRID 11.5 utilizza la versione 3 dell'API per la gestione dei grid. La versione 3 è obsoleta della versione 2; tuttavia, la versione 1 e la versione 2 sono ancora supportate.



È possibile continuare a utilizzare la versione 1 e la versione 2 dell'API di gestione con StorageGRID 11.5; tuttavia, il supporto per queste versioni dell'API verrà rimosso in una release futura di StorageGRID. Dopo l'aggiornamento a StorageGRID 11.5, le API v1 e v2 obsolete possono essere disattivate utilizzando `PUT /grid/config/management API`.

## Nuova sezione certificati-client

La nuova sezione, `/grid/client-certificates`, Consente di configurare i certificati client per fornire un accesso sicuro e autenticato al database StorageGRID Prometheus. Ad esempio, è possibile monitorare StorageGRID esternamente utilizzando Grafana.

## Gli endpoint di compliance legacy sono stati spostati nella nuova sezione s3-Object-lock

Con l'introduzione del blocco a oggetti StorageGRID S3, le API utilizzate per gestire le impostazioni di conformità legacy per la griglia sono state spostate in una nuova sezione dell'interfaccia utente di Swagger. La sezione **s3-Object-lock** include i due elementi `/grid/compliance-global` Endpoint API, che ora controllano l'impostazione globale S3 Object Lock. Gli URI degli endpoint rimangono invariati per la compatibilità con le applicazioni esistenti.

## Endpoint Swift-admin-password account rimosso

Il seguente endpoint API degli account, obsoleto in StorageGRID 10.4, è stato rimosso:

```
https://<IP-Address>/api/v1/grid/accounts/<AccountID>/swift-admin-password
```

## Nuova sezione Grid-password

La sezione **grid-password** consente di gestire le password grid. La sezione include due `/grid/change-provisioning-passphrase` Endpoint API. Gli endpoint consentono agli utenti di modificare la passphrase di provisioning StorageGRID e recuperare lo stato della modifica della passphrase.

## Autorizzazione storageAdmin aggiunta all'API gruppi

Il `/grid/groups` API ora include l'autorizzazione `storageAdmin`.

## Nuovo parametro per l'API di utilizzo dello storage

Il GET `/grid/accounts/{id}/usage` L'API ora dispone di un `strictConsistency` parametro. Per applicare una coerenza forte e globale durante il recupero delle informazioni sull'utilizzo dello storage nei nodi di storage, impostare questo parametro su `true`. Quando questo parametro è impostato su `false` (Impostazione predefinita), StorageGRID tenta di recuperare le informazioni di utilizzo utilizzando una coerenza globale forte, ma ritorna alla coerenza del sito forte se non è possibile soddisfare una coerenza globale forte.

## Nuova API Node Health

Un nuovo `/grid/node-health` è stato aggiunto l'endpoint. Questa API restituisce lo stato corrente di ciascun nodo controllando i `alert` attivi sui nodi. Il `/grid/health/topology` L'API, che verifica la presenza di `allarmi` attivi sui nodi, è obsoleta.

## Passare all'ID della regola di avviso "ApplianceStorageShelvesPowerSupplyDebraded"

L'ID della regola di avviso "ApplianceStorageShelvesPowerSupplyDebraded" è stato rinominato

"ApplianceStorageShelvesDebraded" per riflettere meglio il comportamento effettivo dell'avviso.

#### Informazioni correlate

["Amministrare StorageGRID"](#)

## Modifiche all'API di gestione del tenant

StorageGRID 11.5 utilizza la versione 3 dell'API di gestione dei tenant. La versione 3 è obsoleta della versione 2; tuttavia, la versione 1 e la versione 2 sono ancora supportate.



È possibile continuare a utilizzare la versione 1 e la versione 2 dell'API di gestione con StorageGRID 11.5; tuttavia, il supporto per queste versioni dell'API verrà rimosso in una release futura di StorageGRID. Dopo l'aggiornamento a StorageGRID 11.5, le API v1 e v2 obsolete possono essere disattivate utilizzando `PUT /grid/config/management API`.

## Nuovo parametro per l'API di utilizzo dello storage del tenant

Il `GET /org/usage` L'API ora dispone di un `strictConsistency` parametro. Per applicare una coerenza forte e globale durante il recupero delle informazioni sull'utilizzo dello storage nei nodi di storage, impostare questo parametro su `true`. Quando questo parametro è impostato su `false` (Impostazione predefinita), StorageGRID tenta di recuperare le informazioni di utilizzo utilizzando una coerenza globale forte, ma ritorna alla coerenza del sito forte se non è possibile soddisfare una coerenza globale forte.

#### Informazioni correlate

["Utilizzare S3"](#)

["Utilizzare un account tenant"](#)



## 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.