Le migliori pratiche StorageGRID per FabricPool

StorageGRID software

NetApp
December 03, 2025

Sommario

Le migliori pratiche StorageGRID per FabricPool

Procedure consigliate per i gruppi ad alta disponibilità (HA)

Prima di collegare StorageGRID come livello cloud FabricPool , informati sui gruppi ad alta disponibilità (HA) StorageGRID e rivedi le best practice per l'utilizzo dei gruppi HA con FabricPool.

Che cos'è un gruppo HA?

Un gruppo ad alta disponibilità (HA) è una raccolta di interfacce provenienti da più nodi gateway StorageGRID , nodi amministrativi o entrambi. Un gruppo HA aiuta a mantenere disponibili le connessioni dati dei client. Se l'interfaccia attiva nel gruppo HA fallisce, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni FabricPool .

Ogni gruppo HA fornisce un accesso altamente disponibile ai servizi condivisi sui nodi associati. Ad esempio, un gruppo HA costituito da interfacce solo sui nodi gateway o sia sui nodi amministrativi che sui nodi gateway fornisce un accesso altamente disponibile al servizio Load Balancer condiviso.

Per saperne di più sui gruppi ad alta disponibilità, vedere"Gestire gruppi ad alta disponibilità (HA)" .

Utilizzo di gruppi HA

Le procedure consigliate per la creazione di un gruppo StorageGRID HA per FabricPool dipendono dal carico di lavoro.

- Se si prevede di utilizzare FabricPool con i dati del carico di lavoro primario, è necessario creare un gruppo HA che includa almeno due nodi di bilanciamento del carico per evitare interruzioni nel recupero dei dati.
- Se si prevede di utilizzare la politica di suddivisione in livelli del volume basata solo su snapshot FabricPool o livelli di prestazioni locali non primari (ad esempio, posizioni di disaster recovery o destinazioni NetApp SnapMirror), è possibile configurare un gruppo HA con un solo nodo.

Queste istruzioni descrivono come impostare un gruppo HA per HA Active-Backup (un nodo è attivo e l'altro è di backup). Tuttavia, potresti preferire utilizzare DNS Round Robin o Active-Active HA. Per conoscere i vantaggi di queste altre configurazioni HA, vedere"Opzioni di configurazione per i gruppi HA" .

Best practice per il bilanciamento del carico per FabricPool

Prima di collegare StorageGRID come livello cloud FabricPool , rivedere le best practice per l'utilizzo dei bilanciatori del carico con FabricPool.

Per informazioni generali sul bilanciatore del carico StorageGRID e sul certificato del bilanciatore del carico, vedere"Considerazioni sul bilanciamento del carico" .

Procedure consigliate per l'accesso del tenant all'endpoint del bilanciatore del carico utilizzato per FabricPool

È possibile controllare quali tenant possono utilizzare uno specifico endpoint del bilanciatore del carico per accedere ai propri bucket. È possibile consentire l'accesso a tutti gli inquilini, ad alcuni o bloccarne alcuni. Quando si crea un endpoint di bilanciamento del carico per l'utilizzo FabricPool , selezionare **Consenti tutti i**

tenant. ONTAP crittografa i dati inseriti nei bucket StorageGRID , pertanto questo livello di sicurezza aggiuntivo garantirebbe poca sicurezza aggiuntiva.

Buone pratiche per il certificato di sicurezza

Quando si crea un endpoint del bilanciatore del carico StorageGRID per l'utilizzo in FabricPool , si fornisce il certificato di sicurezza che consentirà a ONTAP di autenticarsi con StorageGRID.

Nella maggior parte dei casi, la connessione tra ONTAP e StorageGRID dovrebbe utilizzare la crittografia Transport Layer Security (TLS). L'utilizzo di FabricPool senza crittografia TLS è supportato ma non consigliato. Quando si seleziona il protocollo di rete per l'endpoint del bilanciatore del carico StorageGRID , selezionare **HTTPS**. Quindi fornire il certificato di sicurezza che consentirà a ONTAP di autenticarsi con StorageGRID.

Per saperne di più sul certificato del server per un endpoint di bilanciamento del carico:

- "Gestire i certificati di sicurezza"
- "Considerazioni sul bilanciamento del carico"
- "Linee guida per il rafforzamento dei certificati del server"

Aggiungi certificato a ONTAP

Quando si aggiunge StorageGRID come livello cloud FabricPool , è necessario installare lo stesso certificato sul cluster ONTAP , inclusi i certificati radice e tutti i certificati dell'autorità di certificazione (CA) subordinata.

Gestisci la scadenza del certificato

> Se il certificato utilizzato per proteggere la connessione tra ONTAP e StorageGRID scade, FabricPool smetterà temporaneamente di funzionare e ONTAP perderà temporaneamente l'accesso ai dati suddivisi in livelli su StorageGRID.

Per evitare problemi di scadenza dei certificati, seguire queste best practice:

- Monitorare attentamente tutti gli avvisi che segnalano l'avvicinarsi della data di scadenza dei certificati, come gli avvisi **Scadenza del certificato dell'endpoint del bilanciatore del carico** e **Scadenza del certificato del server globale per l'API S3**.
- Mantenere sempre sincronizzate le versioni StorageGRID e ONTAP del certificato. Se si sostituisce o si rinnova il certificato utilizzato per un endpoint del bilanciatore del carico, è necessario sostituire o rinnovare il certificato equivalente utilizzato da ONTAP per il livello cloud.
- Utilizzare un certificato CA firmato pubblicamente. Se si utilizza un certificato firmato da una CA, è possibile utilizzare l'API Grid Management per automatizzare la rotazione dei certificati. Ciò consente di sostituire i certificati prossimi alla scadenza senza interruzioni.
- Se hai generato un certificato StorageGRID autofirmato e tale certificato sta per scadere, devi sostituirlo manualmente sia in StorageGRID che in ONTAP prima che scada il certificato esistente. Se un certificato autofirmato è già scaduto, disattivare la convalida del certificato in ONTAP per evitare la perdita di accesso.

  Vedere "Knowledge Base NetApp : come configurare un nuovo certificato server autofirmato StorageGRID su una distribuzione ONTAP FabricPool esistente" per istruzioni.

Procedure consigliate per l'utilizzo di ILM con i dati FabricPool

Se si utilizza FabricPool per suddividere i dati in livelli per StorageGRID, è necessario comprendere i requisiti per l'utilizzo della gestione del ciclo di vita delle informazioni (ILM) StorageGRID con i dati FabricPool .

> FabricPool non ha alcuna conoscenza delle regole o delle policy ILM StorageGRID . Se la policy StorageGRID ILM non è configurata correttamente, si può verificare una perdita di dati. Per informazioni dettagliate, vedere"Utilizzare le regole ILM per gestire gli oggetti" E"Creare policy ILM" .

Linee guida per l'utilizzo di ILM con FabricPool

Quando si utilizza la procedura guidata di configurazione FabricPool , questa crea automaticamente una nuova regola ILM per ogni bucket S3 creato e aggiunge tale regola a un criterio inattivo. Ti verrà chiesto di attivare la policy. La regola creata automaticamente segue le best practice consigliate: utilizza la codifica di cancellazione 2+1 in un singolo sito.

Se si configura StorageGRID manualmente anziché utilizzare la procedura guidata di configurazione FabricPool , consultare queste linee guida per assicurarsi che le regole e i criteri ILM siano adatti ai dati FabricPool e ai requisiti aziendali. Potrebbe essere necessario creare nuove regole e aggiornare le policy ILM attive per soddisfare queste linee guida.

- È possibile utilizzare qualsiasi combinazione di regole di replicazione e di codifica di cancellazione per proteggere i dati del livello cloud.

  La migliore pratica consigliata è quella di utilizzare la codifica di cancellazione 2+1 all'interno di un sito per una protezione dei dati conveniente. La codifica di cancellazione utilizza più CPU, ma offre una capacità di archiviazione notevolmente inferiore rispetto alla replicazione. Gli schemi 4+1 e 6+1 utilizzano meno capacità rispetto allo schema 2+1. Tuttavia, gli schemi 4+1 e 6+1 sono meno flessibili se è necessario aggiungere nodi di archiviazione durante l'espansione della griglia. Per maggiori dettagli, vedere "Aggiungere capacità di archiviazione per oggetti con codice di cancellazione" .

- Ogni regola applicata ai dati FabricPool deve utilizzare la codifica di cancellazione oppure deve creare almeno due copie replicate.

  > Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo espone i dati al rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, tale oggetto viene perso se un nodo di archiviazione si guasta o presenta un errore significativo. Inoltre, durante le procedure di manutenzione, come gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

- Se hai bisogno di"rimuovere i dati FabricPool da StorageGRID" , utilizzare ONTAP per recuperare tutti i dati per il volume FabricPool e promuoverlo al livello di prestazioni.

  > Per evitare la perdita di dati, non utilizzare una regola ILM che farà scadere o eliminerà i dati del livello cloud FabricPool . Impostare il periodo di conservazione in ogni regola ILM su **per sempre** per garantire che gli oggetti FabricPool non vengano eliminati da StorageGRID ILM.

- Non creare regole che sposteranno i dati del livello cloud FabricPool dal bucket a un'altra posizione. Non è

possibile utilizzare un Cloud Storage Pool per spostare i dati FabricPool in un altro archivio oggetti.

> L'utilizzo di Cloud Storage Pool con FabricPool non è supportato a causa della latenza aggiuntiva necessaria per recuperare un oggetto dalla destinazione di Cloud Storage Pool.

- A partire da ONTAP 9.8, è possibile creare facoltativamente tag di oggetti per facilitare la classificazione e l'ordinamento dei dati a livelli, semplificandone la gestione. Ad esempio, è possibile impostare i tag solo sui volumi FabricPool collegati a StorageGRID. Quindi, quando si creano regole ILM in StorageGRID, è possibile utilizzare il filtro avanzato Object Tag per selezionare e posizionare questi dati.

Altre best practice per StorageGRID e FabricPool

Quando si configura un sistema StorageGRID per l'utilizzo con FabricPool, potrebbe essere necessario modificare altre opzioni StorageGRID . Prima di modificare un'impostazione globale, valutare l'impatto della modifica sulle altre applicazioni S3.

Destinazioni dei messaggi di controllo e dei registri

I carichi di lavoro FabricPool presentano spesso un elevato tasso di operazioni di lettura, che può generare un volume elevato di messaggi di audit.

- Se non è necessario un record delle operazioni di lettura del client per FabricPool o qualsiasi altra applicazione S3, è possibile passare facoltativamente a **CONFIGURAZIONE** > **Monitoraggio** > **Server di audit e syslog**. Modificare l'impostazione **Letture client** su **Errore** per ridurre il numero di messaggi di controllo registrati nel registro di controllo. Vedere"Configurare i messaggi di controllo e le destinazioni dei registri" per i dettagli.
- Se si dispone di una griglia di grandi dimensioni, si utilizzano più tipi di applicazioni S3 o si desidera conservare tutti i dati di audit, configurare un server syslog esterno e salvare le informazioni di audit in remoto. L'utilizzo di un server esterno riduce al minimo l'impatto sulle prestazioni della registrazione dei messaggi di controllo senza ridurre la completezza dei dati di controllo. Vedere"Considerazioni per il server syslog esterno" per i dettagli.

Crittografia degli oggetti

Durante la configurazione di StorageGRID, è possibile abilitare facoltativamente"opzione globale per la crittografia degli oggetti memorizzati" se è richiesta la crittografia dei dati per altri client StorageGRID . I dati suddivisi in livelli da FabricPool a StorageGRID sono già crittografati, pertanto non è necessario abilitare l'impostazione StorageGRID . Le chiavi di crittografia lato client sono di proprietà di ONTAP.

Compressione degli oggetti

Quando si configura StorageGRID, non abilitare"opzione globale per comprimere gli oggetti memorizzati" . I dati suddivisi in livelli da FabricPool a StorageGRID sono già compressi. L'utilizzo dell'opzione StorageGRID non ridurrà ulteriormente le dimensioni di un oggetto.

Consistenza del secchio

Per i bucket FabricPool , la coerenza consigliata è **Read-after-new-write**, che è la coerenza predefinita per un nuovo bucket. Non modificare i bucket FabricPool per utilizzare **Disponibile** o **Strong-site**.

Struttura a FabricPool

Se un nodo StorageGRID utilizza storage assegnato da un sistema NetApp ONTAP , verificare che il volume non abbia un criterio di suddivisione in livelli FabricPool abilitato. Ad esempio, se un nodo StorageGRID è in esecuzione su un host VMware, assicurarsi che il volume che supporta il datastore per il nodo StorageGRID non abbia un criterio di suddivisione in livelli FabricPool abilitato. La disattivazione della suddivisione in livelli FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di archiviazione.

Non utilizzare mai FabricPool per riportare i dati relativi a StorageGRID a StorageGRID stesso. Il riordino dei dati StorageGRID su StorageGRID aumenta la complessità operativa e la risoluzione dei problemi.