Installare e configurare

NetApp Console local deployment

NetApp
August 10, 2026

Sommario

Installare e configurare . . . 1
- Guida rapida per configurare la distribuzione locale di NetApp Console . . . 1
- Installa NetApp Console . . . 2
  - Installa la distribuzione locale di NetApp Console usando un OVA in vCenter . . . 2
- Pianifica l’organizzazione della tua NetApp Console . . . 4
  - Inizia a utilizzare identità e accesso nella distribuzione locale di NetApp Console . . . 4
  - Scopri cartelle e gruppi nella distribuzione locale di NetApp Console . . . 5
  - Scopri il controllo degli accessi in base al ruolo nella distribuzione locale di NetApp Console . . . 8
- Configura l’organizzazione della tua NetApp Console . . . 10
  - Aggiungi cartelle e gruppi alla tua organizzazione di distribuzione locale della NetApp Console . . . 10
  - Aggiungi i sistemi storage alla distribuzione locale di NetApp Console . . . 13
  - Gestisci le risorse in cartelle e gruppi nella NetApp Console distribuzione locale . . . 13
  - Aggiungi membri alla tua organizzazione di distribuzione locale di NetApp Console . . . 16
  - Ruoli di accesso . . . 19
- Configura le integrazioni e i servizi della NetApp Console . . . 29
  - Integra NetApp Console distribuzione locale con Active Directory . . . 29
  - Collega il tuo LLM e abilita l’assistente della NetApp Console nella distribuzione locale di NetApp Console . . . 31
  - Risolvi i problemi di integrazione LLM nella distribuzione locale di NetApp Console . . . 33
  - Configura i canali di consegna delle notifiche nella distribuzione locale di NetApp Console . . . 34

Installare e configurare

Guida rapida per configurare la distribuzione locale di NetApp Console

Dopo aver installato la distribuzione locale di NetApp Console, configura la tua organizzazione in modo che i team giusti possano gestire in modo sicuro le giuste risorse di storage. Usa questa checklist per pianificare la struttura, organizzare le risorse, aggiungere membri, configurare le integrazioni e abilitare i data services.

Ruoli di accesso richiesti

Super amministratore o amministratore dell'organizzazione. "Scopri i ruoli di accesso".

1 Installa la distribuzione locale di NetApp Console

- Esamina il flusso di lavoro di installazione per comprendere il processo di implementazione. "Scopri il flusso di lavoro di installazione per la distribuzione locale di NetApp Console".
- Installa la distribuzione locale della NetApp Console nel tuo vCenter. "Installa la distribuzione locale di NetApp Console".

2 Pianifica la tua organizzazione

- Scopri come cartelle e gruppi organizzano le tue risorse. "Scopri cartelle e flotte".
- Scopri come il controllo degli accessi in base al ruolo (RBAC) garantisce ai membri l'accesso di cui hanno bisogno. "Scopri il controllo degli accessi in base al ruolo nella distribuzione locale di NetApp Console".
- Esamina il flusso di lavoro di gestione delle identità e degli accessi. "Inizia a utilizzare IAM per gestione delle flotte e delle risorse".

3 Crea la tua organizzazione

- Aggiungi i tuoi sistemi di archiviazione alla distribuzione locale di NetApp Console. "Aggiungi sistemi di archiviazione".
- Crea la gerarchia di cartelle e fleet che corrisponde alla struttura della tua azienda. "Crea cartelle e flotte".
- Associa le risorse alle cartelle e ai gruppi corretti. "Associa le risorse a cartelle e fleet".
- Aggiungi i membri e assegna loro i ruoli iniziali. "Aggiungi membri e assegna ruoli".

4 Configura integrazioni e servizi

- Integra con Active Directory così gli utenti della directory possono accedere alla distribuzione locale della Console. "Integra con Active Directory".
- Collega il tuo modello linguistico esteso (LLM) per abilitare l'assistente della Console e la gestione assistita dall'IA. "Collega il tuo LLM".
- Configura come la distribuzione locale della Console invia le notifiche. "Configura la consegna delle notifiche".

5 **Configura NetApp Backup and Recovery**

- "Ottieni una licenza per NetApp Backup and Recovery". Puoi saltare questo passaggio se non desideri accedere ai servizi avanzati di Backup and Recovery.
- Aggiungi la licenza NetApp Backup and Recovery alla distribuzione locale di NetApp Console. "Aggiungi la licenza alla distribuzione locale di NetApp Console".
- "Concedi agli utenti l'accesso a NetApp Backup and Recovery".

Installa NetApp Console

Installa la distribuzione locale di NetApp Console usando un OVA in vCenter

Usi un file OVA per installare una distribuzione locale della NetApp Console nel tuo VCenter. Il download dell'OVA o l'URL sono disponibili tramite il sito di supporto NetApp.

Preparati a installare la distribuzione locale di NetApp Console

Prima dell'installazione, assicurati che l'host della macchina virtuale soddisfi i requisiti e che la distribuzione locale della NetApp Console possa accedere a internet e alle reti di destinazione. Per utilizzare i servizi dati NetApp come NetApp Backup and Recovery, crea le credenziali del cloud provider per la distribuzione locale della NetApp Console, così da poter eseguire azioni per tuo conto.

Esamina i requisiti host per la distribuzione locale della NetApp Console

Assicurati che la macchina host soddisfi i requisiti di installazione prima di installare la distribuzione locale della NetApp Console.

- CPU: 16 core o 16 vCPU
- RAM: 64 GB
- Spazio su disco: 596 GB (è consigliato il thick provisioning)
- vSphere 7.0u3 o superiore, con versione hardware virtuale 19 o superiore

Installa la distribuzione locale di NetApp Console in un ambiente vCenter invece che direttamente su un host ESXi.

Configura l'accesso di rete per la distribuzione locale della NetApp Console

NetApp Console local deployment utilizza uno spazio di indirizzi fisso per la comunicazione tra i servizi. Gli intervalli IP 10.42.0.0/16 e 10.43.0.0/16 sono utilizzati per la rete interna. Prima di distribuire Console local deployment, assicurati che questi intervalli IP non siano assegnati ad altre istanze di macchine virtuali, ambiti DHCP, record DNS o pool VIP del bilanciatore di carico sulle VLAN rese disponibili per Console local deployment.

Vedi l'articolo della Knowledge Base "Agent IP conflict with existing network" per le istruzioni su come cambiare l'indirizzo IP delle interfacce dell'agente.

Installa la distribuzione locale di NetApp Console nel tuo ambiente vCenter

NetApp supporta l'installazione della distribuzione locale della NetApp Console nel tuo ambiente VCenter. Il file

OVA include un'immagine di VM preconfigurata che puoi distribuire nel tuo ambiente VMware.

Scarica il file OVA o copia l'URL

Scarica l'OVA.

1. Scarica il software di distribuzione locale della Console dal sito di supporto NetApp.

Distribuisci la NetApp Console in locale nel tuo vCenter

Accedi al tuo ambiente VCenter per distribuire Console local deployment.

Passaggi

1. Se richiesto dal tuo ambiente, carica il certificato autofirmato nell'elenco dei certificati attendibili. Puoi sostituire questo certificato dopo l'installazione.
2. Distribuisci il file OVA dall'archivio di contenuti o dal sistema locale.

Dal sistema locale	Dall'archivio di contenuti
a. Fai clic con il pulsante destro del mouse e seleziona **Deploy OVF template…**. b. Scegli il file OVA dall'URL o individua la sua posizione, quindi seleziona **Next**.	a. Vai al tuo archivio di contenuti e seleziona la Console OVA. b. Seleziona **Azioni** > **Nuova VM da questo modello**

3. Completa la procedura guidata di distribuzione del modello OVF per distribuire la Console.
4. Seleziona un nome e una cartella per la macchina virtuale, quindi seleziona **Avanti**.
5. Seleziona una risorsa di calcolo, quindi seleziona **Avanti**.
6. Esamina i dettagli del modello, quindi seleziona **Avanti**.
7. Accetta il contratto di licenza, quindi seleziona **Avanti**.
8. Scegli il tipo di configurazione proxy che vuoi usare: proxy esplicito, proxy trasparente o nessun proxy.
9. Seleziona il datastore in cui desideri distribuire la VM, quindi seleziona **Avanti**. Assicurati che soddisfi i requisiti dell'host.
10. Seleziona la rete a cui vuoi connettere la VM, poi seleziona **Avanti**. Assicurati che la rete sia IPv4 e che abbia accesso outbound a Internet verso gli endpoint richiesti.
11. Nella finestra **Personalizza modello**, compila i seguenti campi:
    - **Informazioni sul proxy**
      - Se hai selezionato proxy esplicito, inserisci il nome host o l'indirizzo IP del proxy server e il numero di porta, oltre a nome utente e password.
      - Se hai selezionato proxy trasparente, carica il relativo certificato.
    - **Configurazione della macchina virtuale**
      - **Salta il controllo della configurazione**: questa check box è deselezionata per impostazione predefinita, il che significa che la NetApp Console distribuzione locale esegue un controllo della configurazione per convalidare l'accesso alla rete.
        - NetApp consiglia di lasciare questa check box deselezionata in modo che l'installazione includa un controllo di configurazione della NetApp Console distribuzione locale. Il controllo di configurazione verifica che la NetApp Console distribuzione locale abbia accesso di rete agli endpoint richiesti. Se la distribuzione non riesce a causa di problemi di connettività, puoi accedere al report di convalida e ai log dall'host della NetApp Console distribuzione locale. In

alcuni casi, se sei sicuro che la NetApp Console distribuzione locale abbia accesso di rete, puoi scegliere di saltare il controllo.

- **Password di manutenzione**: Imposta la password per l' `maint`utente che consente l'accesso alla console di manutenzione della distribuzione locale della NetApp Console.
- **Server NTP**: Specifica uno o più server NTP per la sincronizzazione dell'ora.
- **Nome host**: Imposta il nome host per questa VM. Non deve includere il domain name di ricerca. Ad esempio, un FQDN come console10.searchdomain.company.com deve essere inserito come console10.
- **Primary DNS**: Specifica il DNS server primario da utilizzare per la risoluzione dei nomi.
- **Secondary DNS**: Specifica il DNS server secondario da utilizzare per la risoluzione dei nomi.
- Domini di ricerca: specifica il domain name da usare quando risolvi il nome host. Ad esempio, se il FQDN è console10.searchdomain.company.com, inserisci searchdomain.company.com.
- **Indirizzo IPv4**: L'indirizzo IP mappato al nome host.
- **Maschera di sottorete IPv4**: La maschera di sottorete per l'indirizzo IPv4.
- **Indirizzo gateway IPv4**: L'indirizzo gateway per l'indirizzo IPv4.

12. Seleziona **Avanti**.
13. Rivedi i dettagli nella finestra **Pronto per completare**, seleziona **Fine**.

    La barra delle applicazioni di vSphere mostra l'avanzamento mentre viene distribuita la distribuzione locale della NetApp Console.

14. Accendi la macchina virtuale.

Pianifica l'organizzazione della tua NetApp Console

Inizia a utilizzare identità e accesso nella distribuzione locale di NetApp Console

Nella distribuzione locale di NetApp Console, configura la gerarchia di cartelle e flotte, aggiungi membri e autorizzazioni iniziali, e aggiungi e posiziona le risorse nelle flotte corrette in modo che i team giusti possano accedervi e gestirle.

Ruoli di accesso richiesti

Super amministratore, amministratore dell'organizzazione o amministratore di cartella o di flotta. "Scopri i ruoli di accesso".

Hai bisogno del ruolo di **Organization admin** o **Super admin** per completare la configurazione iniziale. Dopo la configurazione, gestisci risorse, accesso dei membri e accesso alla fleet man mano che la tua organizzazione cambia.

1 Aggiungi o scopri risorse

Aggiungi i sistemi alla distribuzione locale di NetApp Console. Durante la configurazione iniziale, in genere aggiungi i sistemi mentre è selezionata la flotta predefinita.

Scopri come creare o individuare risorse:

- "Cluster ONTAP on-premises"

2 Crea la tua gerarchia di cartelle e flotte

Crea ulteriori fleet e cartelle che corrispondano alla gerarchia della tua azienda.

"Scopri come organizzare le tue risorse con cartelle e fleet".

3 Associa le risorse alle flotte corrette

L'aggiunta o la scoperta di un sistema nella distribuzione locale di NetApp Console associa automaticamente la risorsa alla fleet attualmente selezionata. Per rendere un sistema disponibile ai team giusti, associane uno alle fleet appropriate nella tua gerarchia.

- "Scopri come gestire le risorse in cartelle e fleet".

4 Aggiungi membri e assegna le autorizzazioni iniziali

Aggiungi membri e assegna loro ruoli a livello di organizzazione, cartella o flotta in base a ciò che gestiscono.

"Scopri come gestire i membri e le loro autorizzazioni".

Dopo la configurazione iniziale

Una volta completata la configurazione iniziale, gestisci l'accesso e l'assegnazione delle risorse man mano che la tua organizzazione cambia:

- "Gestisci le risorse in cartelle e fleet"
- "Gestisci l'accesso dei membri tra flotte e cartelle (approccio incentrato sul membro)"
- "Gestisci chi può accedere a una flotta o a una cartella specifica (approccio incentrato sulla flotta)"
- "Elimina cartelle e gruppi di cartelle quando non sono più necessari"

Informazioni correlate

- "Scopri la gestione di identità e accessi in NetApp Console"
- "Scopri le API per l'identità e l'accesso"

Scopri cartelle e gruppi nella distribuzione locale di NetApp Console

Nella distribuzione locale di NetApp Console, usa cartelle e storage fleet per organizzare le tue risorse NetApp e controllare l'accesso in base alla struttura aziendale, ad esempio per sede, reparto o tipo di workload.

Usa questa pagina per la strategia gerarchica e i modelli di progettazione della flotta. Per un modello IAM completo di membri, ruoli e ambito delle risorse, "Scopri la gestione di identità e accessi nella distribuzione locale di NetApp Console".

Organizzi le risorse in una gerarchia: l'organizzazione è al vertice, poi ci sono le cartelle (che possono contenere altre cartelle o fleet), e poi le fleet, che contengono i sistemi storage. Assegna i ruoli di accesso a livello di organizzazione, cartella o fleet così gli utenti hanno il giusto accesso alle risorse.

Devi avere il ruolo di amministratore dell'organizzazione, di cartella o di fleet admin per gestire cartelle e flotte nella distribuzione locale della NetApp Console.

Componenti organizzative

Le componenti organizzative—organizzazione, cartelle e fleet—formano una gerarchia che determina come vengono raggruppate le risorse e come viene delegato l'accesso.

Organizzazione

Un'organizzazione è il livello più alto della gerarchia di distribuzione locale della NetApp Console e in genere rappresenta la tua azienda. La tua organizzazione è composta da cartelle, fleet, membri, ruoli e risorse. Le risorse sono associate alle fleet e ai membri vengono assegnati ruoli a livello di organizzazione, cartella o fleet.

Cartelle

Le cartelle raggruppano flotte correlate per organizzarle in base a posizione, sito o unità aziendale. Non puoi associare direttamente i sistemi storage alle cartelle, ma assegnando un ruolo a un membro a livello di cartella, questo avrà accesso a tutte le flotte in quella cartella.

Gli amministratori dell'organizzazione possono aggiungere una risorsa a una cartella per delegare a un amministratore di cartella o di flotta il compito di associare la risorsa alle flotte "Associa le risorse a cartelle e fleet".

Flotte

I fleet raggruppano i sistemi storage. Assegna risorse ai fleet e concedi ai membri l'accesso a livello di fleet. Le risorse possono appartenere a più fleet. I membri con accesso al fleet possono gestire le risorse in quel fleet.

Ad esempio, puoi associare un sistema ONTAP locale a una singola flotta o a tutte le flotte della tua organizzazione, a seconda delle tue esigenze.

"Scopri come creare cartelle e storage fleet".

Risorse

Una risorsa è un sistema storage di cui la distribuzione locale della Console è a conoscenza e che può essere assegnato a una fleet. Associa una risorsa a una fleet in modo che gli utenti con accesso alla fleet possano gestire la risorsa.

Ad esempio, puoi associare un ONTAP cluster a una flotta o a tutte le flotte della tua organizzazione. Come associ una risorsa dipende dalle esigenze della tua organizzazione.

"Scopri come associare le risorse alle flotte".

Membri e ruoli

I membri sono gli utenti e gli account di servizio della tua organizzazione. I ruoli definiscono quali azioni possono eseguire e a quale livello della gerarchia—organizzazione, cartella o flotta.

Membri

I membri della tua organizzazione sono account utente o account di servizio. Un account di servizio viene in genere utilizzato da un'applicazione per completare attività specifiche senza intervento umano.

Gli utenti con il ruolo di amministratore dell'organizzazione possono aggiungere nuovi membri alla tua organizzazione. Tutti gli utenti (inclusi gli account di servizio e gli utenti di Active Directory) devono essere aggiunti esplicitamente e a ciascuno deve essere assegnato almeno un ruolo per poter accedere alla distribuzione locale della Console.

"Scopri come aggiungere membri alla tua organizzazione".

Ruoli di accesso

La distribuzione locale della Console fornisce ruoli di accesso che puoi assegnare ai membri della tua organizzazione.

Quando associ un membro a un ruolo, puoi assegnare quel ruolo all'intera organizzazione, a una cartella specifica o a una specifica fleet. Il ruolo che selezioni dà al membro il permesso di accedere alle risorse nella parte selezionata della gerarchia.

L'implementazione locale della NetApp Console offre ruoli granulari che aderiscono al principio del minimo privilegio, il che significa che i ruoli di accesso sono progettati per dare ai membri accesso solo a ciò di cui hanno bisogno.

Gli utenti possono ricoprire più ruoli man mano che le loro mansioni si espandono.

Ereditarietà dei ruoli

Quando assegni un ruolo a livello di organizzazione o di cartella, le sottocartelle, le flotte e le risorse sottostanti ereditano quel ruolo, quindi la struttura delle cartelle e delle flotte determina quanto ampiamente si applica ciascuna assegnazione.

"Scopri l'ereditarietà dei ruoli nella distribuzione locale di NetApp Console".

Esempi di progettazione organizzativa

La struttura organizzativa più adatta dipende dalle dimensioni della tua organizzazione e da come sono organizzati i tuoi team. Gli esempi seguenti mostrano come diverse organizzazioni possono utilizzare la gerarchia di cartelle e fleet per gestire l'accesso in modo efficace.

Strategia per piccole organizzazioni

Per le organizzazioni con meno di 50 utenti e gestione centralizzata dello storage, considera un approccio semplificato usando i ruoli di Super admin e Super viewer.

Esempio: ABC Corporation (team di 5 persone)

- **Struttura**: Organizzazione unica con 3 fleet (Produzione, Sviluppo, Backup)
- **Ruoli**:
  - 2 membri senior: ruolo di super admin per accesso amministrativo completo
  - 3 membri del team: ruolo di super viewer per il monitoraggio senza diritti di modifica
- **Vantaggi**: Amministrazione semplificata, complessità dei ruoli ridotta, adatto a team che necessitano di un ampio accesso

Strategia aziendale multiregionale

Per le grandi organizzazioni con sedi regionali e team specializzati, implementa un approccio gerarchico con cartelle che rappresentano i confini geografici o delle unità aziendali.

Esempio: XYZ Corporation (società multinazionale)

- **Struttura**: Organizzazione > Cartelle regionali (North America, Europe, Asia-Pacific) > Flotte per regione
- **Ruoli della piattaforma**:
  - 1 Amministratore dell'organizzazione: supervisione globale e gestione delle policy
  - 3 Amministratori di cartelle o flotte: Controllo regionale (uno per regione)
  - 1 Amministratore della federazione: integrazione del servizio di directory aziendale
- **Ruoli di storage per regione**:
  - Amministratore dello storage: individua e gestisci i sistemi di storage nelle regioni assegnate
  - Visualizzatore di archiviazione: monitora risorse di storage in diverse regioni
  - Specialista della salute del sistema: Gestisci la salute dello storage senza modificare il sistema
- **Vantaggi**: Maggiore sicurezza grazie alla separazione dei ruoli, all'autonomia regionale e alla conformità alle normative locali

Strategia di specializzazione dipartimentale

Per le organizzazioni con team specializzati che necessitano di accessi specifici, usa assegnazioni di ruoli mirate in base alle responsabilità funzionali.

Esempio: TechCorp (azienda tecnologica di medie dimensioni)

- **Struttura**: Organizzazione > Cartelle di reparto (IT, Sicurezza, Sviluppo) > Risorse specifiche della flotta
- **Ruoli specializzati**:
  - Team di sicurezza: ruoli di amministratore della resilienza al ransomware e di visualizzatore della classificazione
  - Team di backup: Super amministratore per il backup e il ripristino per operazioni di backup complete
  - Team di sviluppo: amministratore dello storage per la gestione dell'ambiente di test
  - Team di conformità: analista di supporto operativo per il monitoraggio e la gestione dei casi di supporto
- **Vantaggi**: Controllo degli accessi personalizzato, maggiore efficienza operativa e chiara attribuzione di responsabilità per compiti specializzati

Prossimi passi

- "Crea cartelle e flotte di storage"
- "Associa le risorse a cartelle e fleet"
- "Gestisci le assegnazioni di accesso alla flotta"
- "Monitora o controlla le azioni di distribuzione locale della Console"

Scopri il controllo degli accessi in base al ruolo nella distribuzione locale di NetApp Console

Gestisci l'accesso degli utenti alla distribuzione locale della NetApp Console con il controllo degli accessi in base al ruolo (RBAC), assegnando ruoli predefiniti a livello di organizzazione, cartella o flotta. Ogni ruolo concede autorizzazioni specifiche che definiscono quali azioni gli utenti possono eseguire nell'ambito assegnato.

NetApp progetta i ruoli di distribuzione locale della Console con il principio del minimo privilegio, così ogni ruolo include solo le autorizzazioni necessarie per le sue attività. Questo approccio migliora la sicurezza limitando l'accesso a ciò di cui ogni membro ha bisogno.

Dopo aver organizzato le risorse in cartelle e fleet, assegna ai membri dell'organizzazione uno o più ruoli per cartelle o fleet specifici, che permettono loro di svolgere solo le proprie responsabilità.

Ad esempio, puoi assegnare a un membro il ruolo di Backup and Recovery admin per uno specifico livello di flotta, permettendogli di eseguire operazioni di Backup and Recovery per le risorse all'interno di quella flotta, senza concedergli un accesso più ampio all'intera organizzazione. A questo stesso utente puoi assegnare il ruolo per diverse flotte all'interno della tua organizzazione.

Puoi assegnare ai membri più ruoli per lo stesso ambito o per ambiti diversi, a seconda delle loro responsabilità. Ad esempio, un'organizzazione di piccole dimensioni potrebbe assegnare allo stesso membro sia il ruolo di Storage admin che quello di Backup and Recovery admin a livello di organizzazione, mentre un'organizzazione più grande potrebbe assegnare a membri diversi ciascun ruolo a livello di fleet.

Tipi di membri dell'organizzazione Console

NetApp Console la distribuzione locale supporta i seguenti tipi di membri:

- *Utenti*: I singoli utenti possono essere utenti locali che aggiungi alla distribuzione locale della NetApp Console e che usano credenziali locali, oppure utenti di directory che si autenticano tramite il tuo servizio Active Directory o LDAP integrato. A entrambi i tipi di utenti possono essere assegnati ruoli nella distribuzione locale della NetApp Console per accedere alle risorse.
- *Account di servizio*: account non umani che applicazioni o servizi utilizzano per interagire con NetApp Console distribuzione locale tramite API. Puoi aggiungere account di servizio direttamente all'organizzazione della distribuzione locale della Console.

"Scopri come aggiungere membri alla tua organizzazione."

Ruoli predefiniti nella distribuzione locale di NetApp Console

NetApp Console deployment locale include ruoli predefiniti che puoi assegnare ai membri dell'organizzazione. Ogni ruolo include autorizzazioni che specificano quali azioni un membro può eseguire nell'ambito assegnato (organizzazione, cartella o fleet).

NetApp Console

- Ruoli della piattaforma: Fornisci le autorizzazioni di amministrazione della distribuzione locale della Console
- Ruoli dei servizi dati: Fornisci le autorizzazioni per gestire servizi dati specifici, come Ransomware Resilience e Backup and Recovery
- Ruoli dell'applicazione: Fornisci autorizzazioni per gestire lo storage e per controllare nella Console gli eventi e gli avvisi di distribuzione locale

Puoi assegnare più ruoli a un membro in base alle sue responsabilità. Ad esempio, potresti assegnare a un membro sia il ruolo di Storage admin che quello di Backup and Recovery admin per una specifica fleet.

Per scegliere i permessi di accesso per un membro, associa la categoria di ruolo alle responsabilità del membro, quindi assegna il ruolo all'ambito (organizzazione, cartella o fleet) che corrisponde a quanto ampio dovrebbe essere l'accesso per quel membro. "Scopri come diverse organizzazioni strutturano ruoli e ambiti nella distribuzione locale della NetApp Console".

"Scopri i ruoli predefiniti che puoi assegnare ai membri in NetApp Console distribuzione locale".

Come funziona l'ereditarietà dei ruoli

Quando assegni un ruolo a livello di organizzazione o di cartella, quel ruolo viene ereditato dagli ambiti secondari all'interno di quella parte della gerarchia. Questo significa che i ruoli a livello di organizzazione si applicano all'organizzazione, i ruoli a livello di cartella si applicano a tutte le cartelle secondarie e alle flotte in quella cartella, e i ruoli a livello di flotta si applicano solo alle risorse in quella flotta.

Usa l'ambito che corrisponde all'accesso che vuoi che il membro mantenga. Ad esempio, assegna un ruolo a livello di cartella quando il membro ha bisogno dello stesso accesso su più flotte in una regione. Assegna il ruolo a livello di flotta quando il membro deve accedere solo a una flotta.

Non puoi sovrascrivere l'accesso ereditato a un livello inferiore. Se un membro eredita un ruolo dall'organizzazione o da una cartella, modifica quell'assegnazione al livello superiore in cui l'hai concessa originariamente.

"Scopri cartelle e gruppi nella distribuzione locale di NetApp Console". "Gestisci l'accesso dei membri". "Gestisci le assegnazioni di accesso alla flotta".

Configura l'organizzazione della tua NetApp Console

Aggiungi cartelle e gruppi alla tua organizzazione di distribuzione locale della NetApp Console

Crea cartelle e gruppi di risorse che rispecchiano la struttura della tua azienda, controlla l'accesso e organizza le risorse nella distribuzione locale di NetApp Console.

Ruoli di accesso richiesti

Super amministratore, amministratore dell'organizzazione o amministratore di cartella o di flotta. "Scopri i ruoli di accesso".

NetApp Console la distribuzione locale crea una fleet predefinita quando crei un'organizzazione. Puoi aggiungere altre fleet e raggrupparle in cartelle. "Scopri la gerarchia delle risorse in NetApp Console".

Usa cartelle e fleet per organizzare le risorse

Cartelle e flotte sono i due elementi costitutivi che usi per dare alla tua organizzazione una forma che rispecchi il modo in cui i tuoi team lavorano davvero. Ad esempio, una cartella per ogni regione, con una flotta di produzione e una di sviluppo all'interno di ciascuna.

- Le cartelle raggruppano flotte correlate e supportano l'amministrazione delegata e l'ereditarietà dei ruoli.
- Le flotte sono il luogo in cui associ le risorse per la gestione e concedi agli utenti l'accesso operativo.

Puoi creare prima cartelle e fleet e aggiungere risorse e accesso ai membri in un secondo momento. Questo ti permette di pianificare la gerarchia delle risorse prima di aggiungere utenti e risorse nella distribuzione locale di NetApp Console. Se la tua struttura è già definita, puoi aggiungere risorse e assegnare l'accesso quando crei la fleet. Puoi aggiornare le fleet in qualsiasi momento.

Ad esempio, metti i cluster di produzione in una flotta Production e i cluster di test in una flotta Test, e concedi a ciascun team l'accesso solo alla flotta che possiede.

Cartelle

Le cartelle organizzano le flotte in base alla struttura aziendale, come unità aziendale, regione o team. Puoi annidare le cartelle per rispecchiare la tua organizzazione.

I ruoli assegnati a livello di cartella vengono ereditati dalle sottocartelle e dalle flotte. Puoi anche usare una cartella per delegare le attività di assegnazione delle flotte a un amministratore di cartella o di flotta per quella parte della gerarchia.

> I membri lavorano in fleet, non in cartelle. Una risorsa associata solo a una cartella non è gestibile dai membri finché non viene associata a una fleet.

Ad esempio, un'azienda regionale potrebbe utilizzare le cartelle per organizzare lo storage ONTAP in base all'unità aziendale e al carico di lavoro. Potrebbe creare una cartella di primo livello per North America, sottocartelle per Production e Development, e fleet per i cluster ONTAP che ospitano volumi SAP, VMware e di backup. Gli amministratori dello storage assegnati alla cartella North America ereditano l'accesso a tutte le fleet figlie, mentre i team applicativi ottengono l'accesso solo alle fleet che gestiscono.

Flotte

Associa le risorse alle flotte in modo che i membri possano gestirle. Una flotta può esistere direttamente sotto l'organizzazione o all'interno di una cartella.

Ad esempio, un'azienda del settore sanitario utilizza lo storage ONTAP in flotte di produzione e di sviluppo separate. La flotta di produzione esegue applicazioni cliniche e database di cartelle cliniche dei pazienti, mentre la flotta di sviluppo supporta test e convalida. Questa separazione protegge i dati live, impone un accesso più rigoroso alla produzione, supporta la tracciabilità e i controlli basati sul principio del minimo privilegio e permette ai team di sviluppo di lavorare senza impattare sui carichi di lavoro rivolti ai pazienti.

Gli utenti navigano tra le flotte assegnate nella pagina **Sistemi** per gestire le risorse associate a ciascuna flotta.

Aggiungi una cartella o una fleet

Aggiungi una flotta ogni volta che hai bisogno di un nuovo confine per le risorse e l'accesso dei membri, e aggiungi una cartella quando vuoi raggruppare flotte correlate e delegarne l'amministrazione. Ad esempio, aggiungi una `Production` cartella contenente una `Production-US-East` flotta e una `Production-EU-West` flotta, poi assegna a un responsabile regionale il ruolo di amministratore della cartella o della flotta solo sulla propria flotta.

Puoi creare fino a sette livelli gerarchici.

Puoi aggiungere risorse e assegnare l'accesso ai membri quando crei una flotta o una cartella, oppure farlo in seguito.

Passaggi

1. Seleziona **Amministrazione > Identità e accesso**.
2. Seleziona **Organization**.
3. Dalla pagina **Organizzazione**, seleziona **Aggiungi cartella o flotta**.
4. Seleziona **Folder** o **Fleet**.
5. In **Nome e posizione**: Inserisci un nome e scegli una posizione per la cartella o la flotta.

1. Facoltativo: espandi la sezione **Risorse** per associare le risorse alla flotta o alla cartella.
   a. Seleziona la check box accanto alla risorsa che desideri associare e poi seleziona **Associa alla flotta**. Se non hai ancora aggiunto sistemi alla distribuzione locale della NetApp Console, puoi fare questo passaggio più tardi.

> I membri non possono accedere alle risorse in una cartella finché tali risorse non vengono assegnate a una flotta.

2. Opzionale: espandi la sezione **Accesso** per assegnare l'accesso ai membri. Seleziona **Aggiungi un membro** per assegnare l'accesso e un ruolo. Per impostazione predefinita, l'utente che crea la flotta ha accesso a essa.

   "Scopri i ruoli di accesso".

3. Seleziona **Aggiungi**.

Rinomina una cartella o un gruppo

Rinomina una cartella o un fleet secondo necessità. La ridenominazione non influisce sulle risorse associate o sull'accesso dei membri.

Passaggi

1. Dalla pagina **Organizzazione**, vai su una flotta o una cartella nella tabella, seleziona ••• e poi seleziona **Modifica cartella** o **Modifica flotta**.
2. Nella pagina **Modifica**, inserisci un nuovo nome e seleziona **Applica**.

Elimina una cartella o una fleet

Elimina le cartelle e le flotte che non ti servono più, ad esempio dopo una ristrutturazione del team o il completamento di una flotta.

Prima di eliminare una cartella o un gruppo di cartelle, completa i seguenti controlli:

- Verifica che la cartella o il gruppo non contengano risorse. "Scopri come rimuovere le associazioni di risorse".
- Esamina i membri che hanno ancora accesso alla cartella o al gruppo. "Visualizza le assegnazioni di accesso dei membri".
- Rimuovi o aggiorna l'accesso dei membri secondo necessità. "Modifica le assegnazioni di accesso dei membri".
- Se stai eliminando una flotta, sposta prima le risorse sulla flotta di destinazione. "Scopri come spostare le risorse tra le flotte".

Passaggi

1. Dalla pagina **Organizzazione**, vai su una flotta o una cartella nella tabella, seleziona ••• e poi seleziona **Elimina**.
2. Conferma che vuoi eliminare la cartella o il fleet.

Gestisci flotte e cartelle nella distribuzione locale di NetApp Console

Dopo la configurazione iniziale, puoi fare quanto segue:

- **Gestisci le associazioni di risorse per cartelle e fleet**: "Scopri come associare le risorse a fleet e cartelle".
- **Visualizza o aggiorna l'accesso per una cartella o un fleet**: "Scopri come concedere agli utenti l'accesso alle flotte".
- **Gestisci un membro su più cartelle e flotte**: "Scopri come gestire l'accesso dei membri".
- **Aggiungi altri membri e assegna le autorizzazioni iniziali**: "Scopri come gestire membri e autorizzazioni".

Informazioni correlate

- "Scopri identità e accesso in NetApp Console"
- "Inizia a usare identità e accesso in NetApp Console"
- "Gestisci le assegnazioni di accesso alla flotta"
- "Scopri le API di identità e accesso"

Aggiungi i sistemi storage alla distribuzione locale di NetApp Console

Aggiungi i sistemi storage alla distribuzione locale di NetApp Console per abilitare il monitoraggio, la gestione dell'inventario e l'amministrazione della tua infrastruttura di storage. Dopo che un sistema storage è stato aggiunto, la distribuzione locale della Console rileva il sistema e inizia a raccogliere informazioni che possono essere utilizzate per le attività di monitoraggio e gestione.

Prima di iniziare, assicurati di disporre delle autorizzazioni necessarie per aggiungere sistemi storage e che il sistema storage sia raggiungibile dalla distribuzione locale di NetApp Console.

Passaggi

1. Seleziona **Storage > Management**.
2. Dall'elenco a discesa Scope, seleziona la fleet a cui vuoi aggiungere un sistema storage.
3. Seleziona **Aggiungi sistema**.
4. Inserisci i dettagli richiesti del sistema storage, incluse le informazioni di connessione e le credenziali.
5. Rivedi le informazioni inserite e seleziona **Aggiungi**.

   Il sistema storage viene aggiunto alla fleet selezionata. Il deployment locale della Console inizia a rilevare e monitorare il sistema. A seconda dell'ambiente e della connettività di rete, potrebbero volerci alcuni minuti prima che il sistema risulti completamente gestito.

Puoi anche aggiungere un sistema storage dalla pagina **Amministrazione > Identità e accesso** selezionando **Aggiungi sistema** e fornendo le informazioni di sistema richieste.

Gestisci le risorse in cartelle e gruppi nella NetApp Console distribuzione locale

Gestisci l'accesso alle risorse nella distribuzione locale di NetApp Console associando le risorse alla cartella o alla fleet corretta, che controlla quali team possono accedervi e gestirle.

Ruoli di accesso richiesti

Super amministratore, amministratore dell'organizzazione o amministratore di cartella o di flotta. "Scopri i ruoli di accesso".

Colloca le risorse dove i team giusti possano gestirle, spostale quando cambia la proprietà e rimuovi le associazioni quando non sono più necessarie.

Una *risorsa* è un'entità che la distribuzione locale di Console riconosce, come una risorsa di storage o un workload di Backup and Recovery.

Tipi di risorse della console

La distribuzione locale tramite console supporta sia le risorse di storage che i carichi di lavoro di Backup and Recovery. Associa uno dei due tipi di risorsa a una fleet per controllare accesso e gestione.

Risorse di storage

Le risorse di storage sono il tipo di risorsa più comune nella tua organizzazione. Quando aggiungi un sistema storage alla distribuzione locale di Console, associalo a una fleet così che i team appropriati possano accedervi e gestirlo. Ad esempio, dopo aver aggiunto un ONTAP cluster, associalo alla `Production-US-East` fleet.

Carichi di lavoro di backup e ripristino

Anche i carichi di lavoro di Backup and Recovery sono considerati risorse. Puoi assegnare ai membri le autorizzazioni per accedere ai carichi di lavoro di Backup and Recovery associando i carichi di lavoro alle flotte. Ad esempio, assegna a un membro l'accesso a un carico di lavoro di Backup and Recovery associandolo a una flotta a cui il membro può accedere e concedendo il ruolo di Backup and Recovery appropriato.

Visualizza le risorse della tua organizzazione

Visualizza le risorse della tua organizzazione per trovare una risorsa specifica e vedere a quali fleet o cartelle è associata. Se non hai creato cartelle o fleet, tutte le risorse sono associate alla fleet predefinita direttamente sotto l'organizzazione.

Passaggi

1. Seleziona **Amministrazione > Identità e accesso**.
2. Seleziona **Risorse**.
3. Seleziona **Ricerca e filtri avanzati**.
4. Utilizza le opzioni disponibili per trovare una risorsa:
   - **Cerca per nome della risorsa**: inserisci una stringa di testo e seleziona **Aggiungi**.
   - **Piattaforma**: Seleziona una o più piattaforme, ad esempio Amazon Web Services.
   - **Risorse**: Seleziona una o più risorse, ad esempio Cloud Volumes ONTAP.
   - **Organizzazione, cartella o flotta**: Seleziona l'intera organizzazione, una cartella specifica o una flotta specifica.
5. Seleziona **Cerca**.

Associa una risorsa a una cartella o a una fleet

Associa una risorsa a un gruppo o a una cartella in modo che i team appropriati possano gestirla. Ad esempio, dopo aver aggiunto un ONTAP cluster, associalo al `Production-US-East` fleet in modo che gli

amministratori regionali delle risorse di storage per quel fleet possano gestirlo.

Gli utenti con il ruolo di amministratore dell'organizzazione possono aggiungere risorse a una cartella per delegare le attività di associazione della flotta all'amministratore della cartella o della flotta per quella cartella. "Associa una risorsa a una cartella".

Passaggi

1. Dalla pagina **Risorse**, individua una risorsa nella tabella, seleziona ••• e poi seleziona **Associa a una cartella o a un gruppo**.
2. Seleziona una cartella o una fleet e poi seleziona **Accetta**.
3. Per associare un'ulteriore cartella o flotta, seleziona **Aggiungi cartella o flotta** e poi seleziona la cartella o la flotta.

   Tieni presente che puoi selezionare solo le cartelle e i fleet per cui hai i permessi di amministratore.

4. Seleziona **Associa risorse**.
   - Se hai associato la risorsa alle flotte, i membri che dispongono delle autorizzazioni per tali flotte ora possono accedere alla risorsa dalla Console.
   - Se hai associato la risorsa a una cartella, un amministratore di cartella o di flotta può ora accedere alla risorsa e associarla a una flotta all'interno della cartella. "Associa una risorsa a una cartella".

Visualizza le cartelle e le flotte associate a una risorsa

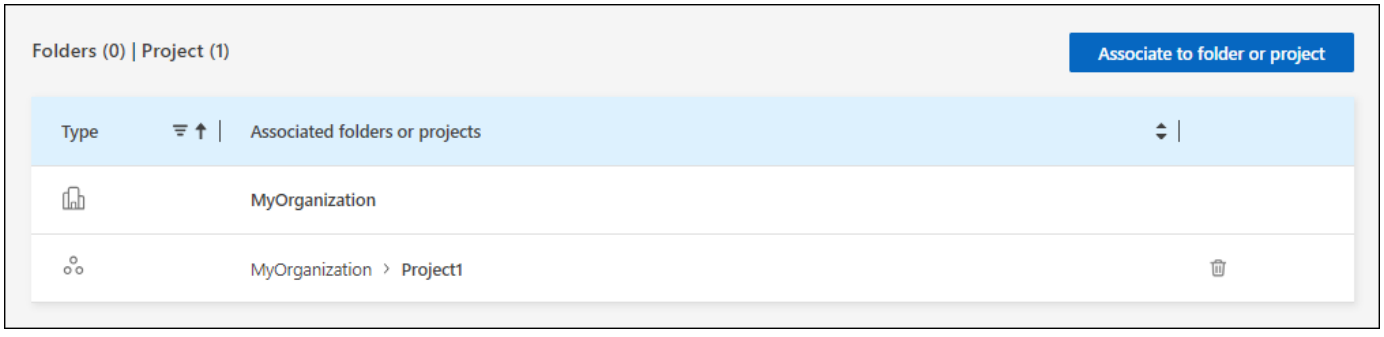
Verifica a quali fleet o cartelle è associata una risorsa.

Per vedere quali membri hanno accesso alla risorsa, controlla i membri assegnati alla cartella o al fleet associato. "Gestisci le assegnazioni di accesso alla flotta".

Passaggi

1. Dalla pagina **Risorse**, individua una risorsa nella tabella, seleziona ••• e poi seleziona **Visualizza dettagli**.

L'esempio seguente mostra una risorsa associata a una flotta.



Per vedere quali membri hanno accesso alla risorsa, controlla la cartella o il fleet associati.

"Gestisci le assegnazioni di accesso alla flotta". "Gestisci l'accesso dei membri".

Rimuovi una risorsa da una cartella o da una fleet

Rimuovi l'associazione di una risorsa con una cartella o un fleet per impedire ai membri di gestirla lì.

Per rimuovere un sistema storage dall'intera organizzazione, vai alla pagina **Sistemi** e rimuovi il sistema.

Passaggi

1. Dalla pagina **Risorse**, individua una risorsa nella tabella, seleziona ••• e poi seleziona **Visualizza dettagli**.
2. Per rimuovere una risorsa da una cartella o da un fleet, seleziona accanto alla cartella o al fleet.
3. Seleziona **Elimina** per rimuovere l'associazione.

Sposta una risorsa tra flotte

Sposta una risorsa da una flotta a un'altra rimuovendo la sua associazione con la flotta attuale e poi associandola alla flotta di destinazione.

L'accesso alla risorsa cambia non appena cambia l'associazione. Se possibile, completa entrambi i passaggi in un'unica finestra di manutenzione.

Passaggi

1. Dalla pagina **Risorse**, individua una risorsa nella tabella, seleziona ••• e poi seleziona **Visualizza dettagli**.
2. Seleziona accanto alla flotta corrente e seleziona **Elimina**.
3. Seleziona **Aggiungi cartella o flotta**.
4. Seleziona la flotta di destinazione e seleziona **Accetta**.
5. Seleziona **Associa risorse**.

Informazioni correlate

- "Scopri identità e accesso in NetApp Console"
- "Inizia a usare identità e accesso in NetApp Console"
- "Gestisci le assegnazioni di accesso alla flotta dopo lo spostamento delle risorse"
- "Scopri le API per l'identità e l'accesso"

Aggiungi membri alla tua organizzazione di distribuzione locale di NetApp Console

Aggiungi membri alla tua organizzazione di distribuzione locale della NetApp Console e assegna ruoli per concedere l'accesso a livello di organizzazione, cartella o flotta per utenti, account di servizio e utenti di directory.

Ruoli di accesso richiesti

Super admin, admin dell'organizzazione o admin di cartelle o fleet (per le cartelle e le fleet che stai amministrando). "Scopri i ruoli di accesso".

Prima di iniziare

- Crea la gerarchia di cartelle e di flotta che corrisponde alla tua organizzazione. "Scopri come organizzare le tue risorse con cartelle e fleet".
- Associa le risorse alle flotte corrette prima di assegnare l'accesso ai membri. "Scopri come gestire le risorse in cartelle e fleet".

- Se stai aggiungendo un utente alla directory, integra prima il tuo servizio di directory. "Scopri come integrarti con il tuo servizio di directory".

Scopri come viene concesso l'accesso nella distribuzione locale di NetApp Console

NetApp Console utilizza il controllo degli accessi in base al ruolo (RBAC) per gestire le autorizzazioni. Assegna ruoli ai membri per fornire l'accesso necessario. Ogni ruolo definisce le azioni consentite per risorse specifiche.

Nota quanto segue sulla concessione dell'accesso nella distribuzione locale di NetApp Console:

- Devi aggiungere esplicitamente ogni utente alla tua organizzazione e assegnargli almeno un ruolo prima che possa accedere alle risorse.
- Il ruolo che assegni a livello di organizzazione o di cartella viene ereditato dagli ambiti secondari, quindi scegli attentamente l'ambito di assegnazione per dare al membro accesso solo dove necessario. "Scopri l'ereditarietà dei ruoli nella distribuzione locale di NetApp Console".

Aggiungi membri alla tua organizzazione

NetApp Console supporta tre tipi di membri: account utente, utenti della directory e account di servizio.

> Devi prima configurare un server di posta elettronica da usare con la distribuzione locale della Console prima di poter aggiungere utenti. "Scopri come configurare un server di posta elettronica."

Gli utenti della directory si autenticano tramite il servizio di directory integrato, ma devi comunque aggiungere ciascun utente singolarmente e assegnare i ruoli nella distribuzione locale della Console. Crea gli account di servizio direttamente nella Console.

Tutti i membri devono avere almeno un ruolo assegnato esplicitamente per poter accedere alla distribuzione locale di Console.

Quando aggiungi un membro, scegli l'organizzazione, la cartella o il fleet a cui il membro deve accedere e assegna il ruolo o i ruoli iniziali di cui ha bisogno.

Aggiungi un account utente

Devi avere il ruolo di Organization admin, Folder admin o fleet admin per aggiungere un utente a un'organizzazione, una cartella o un fleet, così potrà accedere alle risorse.

Passaggi

1. Seleziona **Amministrazione > Identità e accesso**.
2. Seleziona **Members**.
3. Seleziona **Aggiungi un membro**.
4. Per **Tipo di membro**, lascia selezionato **Utente**.
5. Per **Email dell'utente**, inserisci l'indirizzo email dell'utente associato all'accesso che ha creato.
6. Utilizza la sezione **Seleziona un'organizzazione, una cartella o un gruppo** per scegliere dove il membro deve avere accesso.

   Nota quanto segue:

   - Puoi selezionare solo le cartelle e i fleet per cui hai i permessi.

- Quando selezioni un'organizzazione o una cartella, concedi al membro le autorizzazioni per tutti i suoi contenuti.
- Puoi assegnare il ruolo di **Organization admin** solo a livello di organizzazione.

7. **Seleziona una categoria** e poi seleziona un **Ruolo** che dia al membro le autorizzazioni iniziali di cui ha bisogno per l'organizzazione, la cartella o il fleet che hai selezionato.

   "Scopri i ruoli di accesso".

8. Per concedere l'accesso a più cartelle, fleet o ruoli, seleziona **Aggiungi ruolo**, scegli la cartella, la fleet o la categoria di ruolo e seleziona un ruolo.
9. Seleziona **Aggiungi**.

   La Console invia le istruzioni all'utente tramite e-mail.

Aggiungi un account di servizio

Aggiungi un account di servizio quando devi automatizzare le attività o connetterti in modo sicuro alle API della Console. Dopo aver creato l'account, copia il suo client ID e il client secret per l'integrazione che lo utilizzerà.

Passaggi

1. Seleziona **Amministrazione > Identità e accesso**.
2. Seleziona **Members**.
3. Seleziona **Aggiungi un membro**.
4. Per **Tipo di membro**, seleziona **Account di servizio**.
5. Inserisci un nome per l'account di servizio.
6. Utilizza la sezione **Seleziona un'organizzazione, una cartella o un fleet** per scegliere dove l'account di servizio deve accedere.

   Nota quanto segue:

   - Puoi selezionare solo le cartelle e i gruppi per cui hai le autorizzazioni.
   - Selezionando un'organizzazione o una cartella, concedi al membro i permessi su tutti i suoi contenuti.
   - Puoi assegnare il ruolo di **Organization admin** solo a livello di organizzazione.

7. Seleziona una **Categoria** e poi un **Ruolo** che assegna all'account di servizio le autorizzazioni iniziali necessarie per l'organizzazione, la cartella o il fleet che hai selezionato.

   "Scopri i ruoli di accesso".

8. Per concedere l'accesso a più cartelle, fleet o ruoli, seleziona **Aggiungi ruolo**, scegli la cartella, la fleet o la categoria di ruolo e seleziona un ruolo.
9. Scarica o copia l'ID client e il client secret.

   La Console mostra il client secret una sola volta. Copialo in modo sicuro; puoi ricrearlo più tardi se lo perdi.

10. Seleziona **Chiudi**.

Aggiungi un utente della directory alla tua organizzazione

Aggiungi un utente dal tuo servizio di directory integrato e assegnagli i primi ruoli. Ad esempio, aggiungi un nuovo storage engineer da Active Directory e assegna il ruolo Storage admin sulla `Production-US-East` fleet così potrà lavorare in quella fleet.

Devi prima configurare il servizio di directory prima di poter aggiungere utenti della directory. "Scopri come integrarti con il tuo servizio di directory".

Passaggi

1. Seleziona **Amministrazione > Identità e accesso**.
2. Seleziona **Members**.
3. Seleziona **Aggiungi un membro**.
4. Per **Tipo di membro**, seleziona **Utente della directory**.
5. Per **Email dell'utente**, inserisci l'indirizzo email dell'utente della directory che vuoi aggiungere. Questo indirizzo email deve corrispondere all'indirizzo email associato all'accesso dell'utente nella tua directory.
6. Utilizza la sezione **Seleziona un'organizzazione, una cartella o un fleet** per scegliere dove l'utente della directory deve accedere.

   Nota quanto segue:

   - Puoi selezionare solo le cartelle e i gruppi per cui hai le autorizzazioni.
   - Selezionando un'organizzazione o una cartella, concedi al membro i permessi su tutti i suoi contenuti.
   - Puoi assegnare il ruolo di **Organization admin** solo a livello di organizzazione.
7. Seleziona una **Categoria** e poi seleziona un **Ruolo** che dia all'utente della directory le autorizzazioni iniziali di cui ha bisogno per l'organizzazione, la cartella o il fleet che hai selezionato.

   "Scopri i ruoli di accesso".
8. Per concedere all'utente un accesso aggiuntivo ad altre cartelle, fleet o ruoli, seleziona **Aggiungi ruolo**, scegli la cartella o il fleet, la categoria di ruolo e seleziona un ruolo.

Ruoli di accesso

NetApp Console ruoli di accesso alla distribuzione locale

La gestione delle identità e degli accessi (IAM) nella distribuzione locale della NetApp Console offre ruoli predefiniti che puoi assegnare ai membri della tua organizzazione a diversi livelli della gerarchia delle risorse. Prima di assegnare questi ruoli, dovresti capire quali autorizzazioni include ciascun ruolo. I ruoli rientrano nelle seguenti categorie: piattaforma, applicazione e servizio dati.

Ruoli della piattaforma

I ruoli della piattaforma concedono le autorizzazioni di amministrazione della distribuzione locale della NetApp Console, inclusa l'assegnazione dei ruoli e la gestione degli utenti. La distribuzione locale della Console prevede diversi ruoli della piattaforma.

Ruolo della piattaforma	Responsabilità
"Amministratore dell'organizzazione"	Consente a un utente accesso illimitato a tutti i gruppi e le cartelle all'interno di un'organizzazione, aggiungere membri a qualsiasi gruppo o cartella, oltre a eseguire qualsiasi attività e usare qualsiasi servizio dati che non abbia un ruolo esplicito associato. Gli utenti con questo ruolo gestiscono la tua organizzazione creando cartelle e gruppi, assegnando ruoli, aggiungendo utenti e gestendo i sistemi se hanno le credenziali appropriate.
"Amministratore di cartelle o flotte"	Consente a un utente l'accesso illimitato a flotte e cartelle assegnate. Puoi aggiungere membri alle cartelle o flotte che gestisci, oltre a svolgere qualsiasi attività e utilizzare qualsiasi servizio dati o applicazione sulle risorse all'interno della cartella o della flotta a cui sei assegnato.
"Amministratore della federazione"	Consente a un utente di creare e gestire federazioni di servizi di directory con la Console, così gli utenti possono autenticarsi con le loro credenziali di directory esistenti.
"Visualizzatore della Federation"	Consente a un utente di visualizzare le federazioni di servizi di directory esistenti tramite la Console. Non puoi creare o gestire federazioni.
"Super amministratore"	Conferisce all'utente tutti i ruoli di amministratore. Questo ruolo è pensato per le organizzazioni di piccole dimensioni che potrebbero non aver bisogno di distribuire le responsabilità della Console tra più utenti.
"Super visualizzatore"	Conferisce all'utente tutti i ruoli di visualizzazione. Questo ruolo è pensato per le organizzazioni di piccole dimensioni che potrebbero non aver bisogno di distribuire le responsabilità della Console tra più utenti.

Ruoli applicativi

Di seguito trovi un elenco dei ruoli nella categoria applicazione. Ogni ruolo concede autorizzazioni specifiche all'interno del proprio ambito. Gli utenti senza il ruolo applicazione o piattaforma richiesto non possono accedere alla rispettiva applicazione.

Ruolo applicazione	Responsabilità
"Analista di supporto operativo"	Consente l'accesso ad avvisi e strumenti di monitoraggio come la pagina Audit.
"Amministratore dello storage"	Gestisci le funzioni di integrità e governance dello storage, scopri le risorse di storage, oltre a modificare ed eliminare i sistemi esistenti.
"Visualizzatore di storage"	Visualizza le funzioni di integrità e governance dello storage, oltre alle risorse di storage precedentemente rilevate. Non puoi rilevare, modificare o eliminare i sistemi di storage esistenti.
"Specialista salute sistema"	Gestisci le funzioni di storage, integrità e governance, con tutti i permessi dell'amministratore dello storage, tranne che non puoi modificare o eliminare i sistemi esistenti.

Ruoli del servizio dati

Di seguito trovi un elenco dei ruoli nella categoria servizio dati. Ogni ruolo concede autorizzazioni specifiche all'interno del proprio ambito. Gli utenti che non hanno il ruolo servizio dati richiesto o un ruolo di piattaforma non potranno accedere al servizio dati.

Ruolo del servizio dati	Responsabilità
"Super admin di backup e recovery"	Esegui qualsiasi operazione in NetApp Backup and Recovery.
"Amministratore di backup e ripristino"	Esegui backup su snapshot locali, replica su storage secondario e fai il backup su storage a oggetti.
"Backup and recovery ripristino admin"	Ripristina i carichi di lavoro in Backup and Recovery.
"Admin del clone di backup e ripristino"	Clona applicazioni e dati in Backup and Recovery.
"Visualizzatore di backup e ripristino"	Visualizza le informazioni di backup e ripristino.
Visualizzatore di classificazione	Consente agli utenti di visualizzare i risultati della scansione di NetApp Data Classification. Gli utenti con questo ruolo possono visualizzare le informazioni di conformità e generare report per le risorse a cui hanno il permesso di accesso. Questi utenti non possono abilitare o disabilitare la scansione di volumi, bucket o database schema. Data Classification non ha un ruolo admin.
amministratore SnapCenter	Fornisce la possibilità di eseguire il backup degli snapshot dai cluster ONTAP locali utilizzando NetApp Backup and Recovery per le applicazioni. Un membro che ha questo ruolo può completare le seguenti azioni: * Completare qualsiasi azione da Backup and Recovery > Applications * Gestire tutti i sistemi nelle flotte e nelle cartelle per cui ha le autorizzazioni * Utilizzare tutti i servizi NetApp Console SnapCenter non ha un ruolo di visualizzatore.

Link correlati

- "Scopri la gestione dell'identità e dell'accesso della NetApp Console"
- "Inizia a usare identità e accesso in NetApp Console"
- "Aggiungi membri e assegna ruoli in un'organizzazione NetApp Console"
- "Scopri l'API per NetApp Console IAM"

NetApp Console ruoli di accesso alla piattaforma di distribuzione locale

Assegna ruoli di piattaforma agli utenti per concedere le autorizzazioni per gestire la distribuzione locale della NetApp Console, assegnare ruoli, aggiungere utenti, creare fleet e gestire l'autenticazione degli utenti.

Esempio di ruoli organizzativi per una grande organizzazione multinazionale

XYZ Corporation organizza l'accesso allo storage per regione—Nord America, Europa e Asia-Pacifico—fornendo un controllo regionale con supervisione centralizzata.

L'**Organization admin** nella distribuzione locale della Console di XYZ Corporation crea un'organizzazione iniziale e cartelle separate per ogni regione. Il **Folder o fleet admin** per ciascuna regione organizza le fleet (con le risorse associate) all'interno della cartella della regione.

Gli amministratori regionali con il ruolo di **Folder o fleet admin** gestiscono attivamente le proprie cartelle aggiungendo risorse e utenti. Questi amministratori regionali possono anche aggiungere, rimuovere o rinominare le cartelle e le flotte che gestiscono. L'**Organization admin** eredita le autorizzazioni per tutte le

nuove risorse, mantenendo la visibilità sull'utilizzo dello storage in tutta l'organizzazione.

All'interno della stessa organizzazione, a un utente viene assegnato il ruolo di **Federation admin** per gestire la federazione dell'organizzazione con il proprio IdP aziendale. Questo utente può aggiungere o rimuovere organizzazioni federate, ma non può gestire utenti o risorse all'interno dell'organizzazione. L'**Organization admin** assegna a un utente il ruolo di **Federation viewer** per verificare lo stato della federazione e visualizzare le organizzazioni federate.

Le tabelle seguenti indicano le azioni che ciascun ruolo della piattaforma di distribuzione locale della Console può eseguire.

Ruoli di amministrazione dell'organizzazione

Attività	Amministratore dell'organizzazione	Amministratore di cartelle o flotte
Crea, modifica o elimina sistemi dalla distribuzione locale della Console (aggiungi o individua sistemi)	Sì	Sì
Crea cartelle e flotte, inclusa l'eliminazione	Sì	No
Rinomina le cartelle e i gruppi esistenti	Sì	Sì
Assegna ruoli e aggiungi utenti	Sì	Sì
Associa le risorse a cartelle e fleet	Sì	Sì
Registrati per ricevere assistenza e invia le richieste tramite la Console	Sì	Sì
Usa servizi dati non associati a un ruolo di accesso esplicito	Sì	Sì
Visualizza la pagina Audit e le notifiche	Sì	Sì

ruoli della federazione

Attività	Amministratore della federazione	Visualizzatore della Federation
Crea e aggiorna le integrazioni del servizio di directory	Sì	No
Visualizza le federazioni e i relativi dettagli	Sì	Sì

Ruoli di super amministratore e spettatore

Il ruolo di **Super amministratore** offre accesso completo per gestire le funzionalità della Console, lo storage e i servizi dati. Questo ruolo è adatto a chi si occupa di amministrazione e governance. Al contrario, il ruolo di **Super visualizzatore** offre accesso in sola lettura, ideale per revisori o stakeholder che necessitano di visibilità senza poter apportare modifiche.

Le organizzazioni dovrebbero utilizzare l'accesso **Super admin** con parsimonia per ridurre al minimo i rischi per la sicurezza e allinearsi al principio del minimo privilegio. La maggior parte delle organizzazioni dovrebbe assegnare ruoli granulari con solo le autorizzazioni necessarie per ridurre i rischi e migliorare la tracciabilità.

Esempio di super ruoli

ABC Corporation ha un piccolo team di cinque persone che utilizza la NetApp Console per i servizi dati e la gestione dello storage. Invece di distribuire più ruoli, assegnano il ruolo di **Super admin** a due membri senior

del team che gestiscono tutte le attività amministrative, inclusa la gestione degli utenti e la configurazione delle risorse. I restanti tre membri del team ricevono il ruolo di **Super viewer**, che permette loro di monitorare lo stato dello storage e dei servizi dati senza poter modificare le impostazioni.

Ruolo	Ruoli ereditati
Super amministratore	• Amministratore dell'organizzazione • Amministratore di cartelle o flotte • Super admin di backup e recovery • Amministratore dello storage
Super visualizzatore	• Visualizzatore dell'organizzazione • Visualizzatore di backup • Visualizzatore di storage

Ruolo di analista del supporto operativo per l'accesso nella distribuzione locale di NetApp Console

Nella distribuzione locale di NetApp Console, puoi assegnare agli utenti il ruolo di Operational support analyst per consentire loro l'accesso agli avvisi e al monitoraggio.

Analista del supporto operativo

Attività	Puoi eseguire
Visualizza i sistemi di storage	Sì
Visualizza la pagina Audit e le notifiche	Sì
Visualizza, scarica e configura gli avvisi	Sì

Ruoli di accesso allo storage per la distribuzione locale di NetApp Console

Puoi assegnare i seguenti ruoli agli utenti per consentire loro di accedere alle funzionalità di gestione dello storage nella distribuzione locale di NetApp Console. Puoi assegnare agli utenti un ruolo amministrativo per gestire lo storage o un ruolo di visualizzatore per il monitoraggio.

Gli amministratori possono assegnare ruoli di storage agli utenti per le seguenti risorse di storage e funzionalità:

Risorse di storage:

- Cluster ONTAP on-premises

Servizi e funzionalità della console:

- funzioni di integrità dello storage

Esempio di ruoli di storage nella distribuzione locale di NetApp Console

XYZ Corporation, una multinazionale, ha un grande team di storage engineer e storage administrator. Permettono a questo team di gestire le risorse di storage per le loro regioni, limitando però l'accesso alle attività principali di distribuzione locale della Console, come la gestione degli utenti e delle licenze.

All'interno di un team di 12 persone, a due utenti viene assegnato il ruolo di **Storage viewer**, che permette loro di monitorare le risorse di storage associate alle flotte di distribuzione locale della Console a cui sono assegnati. Ai restanti nove viene assegnato il ruolo di **Storage admin**, che include la possibilità di gestire gli aggiornamenti software, accedere a ONTAP System Manager tramite la distribuzione locale della Console, oltre che individuare risorse di storage (aggiungere sistemi). A una persona del team viene assegnato il ruolo di **System health specialist** così può gestire lo stato di salute delle risorse di storage nella propria regione, ma non modificare o eliminare alcun sistema. Questa persona può anche eseguire aggiornamenti software sulle risorse di storage per le flotte a cui è assegnata.

L'organizzazione dispone di due utenti aggiuntivi con il ruolo di **Organization admin** che possono gestire tutti gli aspetti della distribuzione locale della Console, inclusa la gestione degli utenti e delle licenze, nonché di diversi utenti con il ruolo di **Folder or fleet admin** che possono eseguire attività di amministrazione della distribuzione locale della Console per le cartelle e le flotte a cui sono assegnati.

La tabella seguente mostra le azioni eseguite da ciascun ruolo di storage.

Caratteristica e azione	Amministratore dello storage	Specialista salute sistema	Visualizzatore di storage
Gestione dello storage:			
Scopri nuove risorse (aggiungi sistemi)	Sì	Sì	No
Visualizza i sistemi aggiunti	Sì	Sì	No
Elimina i sistemi dalla Console	Sì	No	No
Modifica i sistemi	Sì	No	No
Accesso a System Manager			
Puoi inserire le credenziali	Sì	Sì	No

NetApp Backup and Recovery ruoli nella distribuzione locale di NetApp Console

Nella distribuzione locale di NetApp Console, puoi assegnare i seguenti ruoli agli utenti per fornire loro l'accesso a NetApp Backup and Recovery all'interno della Console. I ruoli di Backup and Recovery ti danno la flessibilità di assegnare agli utenti un ruolo specifico per le attività che devono svolgere all'interno della tua organizzazione. Come assegni i ruoli dipende dalle tue pratiche aziendali e di gestione dello storage.

Il servizio utilizza i seguenti ruoli specifici per NetApp Backup and Recovery.

- **Super amministratore di NetApp Backup and Recovery**: Puoi eseguire qualsiasi operazione in NetApp Backup and Recovery.
- **Amministratore del backup e del ripristino**: Esegui backup su snapshot locali, replica su storage secondario ed esegui backup su storage a oggetti nelle azioni di NetApp Backup and Recovery.
- **Backup and recovery restore admin**: Ripristina i carichi di lavoro utilizzando NetApp Backup and Recovery.
- **Amministratore della clonazione di backup e recovery**: Clona applicazioni e dati utilizzando NetApp Backup and Recovery.
- **Visualizzatore di backup e recovery**: Visualizza le informazioni in NetApp Backup and Recovery, ma non puoi eseguire alcuna azione.

Per dettagli su tutti i ruoli di accesso alla NetApp Console, vedi "la documentazione relativa alla configurazione e all'amministrazione della Console".

Ruoli utilizzati per azioni comuni

La tabella seguente indica le azioni che ciascun ruolo di NetApp Backup and Recovery può eseguire per tutti i carichi di lavoro.

Caratteristica e azione	Super admin di backup e recovery	Amministratore di backup e ripristino	Backup and recovery ripristino admin	Admin del clone di backup e ripristino	Visualizzatore di backup e ripristino
Aggiungi, modifica o elimina host	Sì	No	No	No	No
Installa i plugin	Sì	No	No	No	No
Aggiungi le credenziali (host, istanza, vCenter)	Sì	No	No	No	No
Visualizza la dashboard e tutte le schede	Sì	Sì	Sì	Sì	Sì
Inizia la prova gratuita	Sì	No	No	No	No
Avvia la scoperta dei carichi di lavoro	No	Sì	Sì	Sì	No
Visualizza le informazioni sulla licenza	Sì	Sì	Sì	Sì	Sì
Attiva licenza	Sì	No	No	No	No
Visualizza gli host	Sì	Sì	Sì	Sì	Sì
Pianificazioni:					

Caratteristica e azione	Super admin di backup e recovery	Amministratore di backup e ripristino	Backup and recovery ripristino admin	Admin del clone di backup e ripristino	Visualizzatore di backup e ripristino
Attiva gli orari	Sì	Sì	Sì	Sì	No
Sospendi le pianificazioni	Sì	Sì	Sì	Sì	No
Politiche e protezione:					
Visualizza i piani di protezione	Sì	Sì	Sì	Sì	Sì
Crea, modifica o elimina i piani di protezione	Sì	Sì	No	No	No
Ripristina i carichi di lavoro	Sì	No	Sì	No	No
Crea, dividi o elimina cloni	Sì	No	No	Sì	No
Crea, modifica o elimina una policy	Sì	Sì	No	No	No
Report:					
Visualizza i report	Sì	Sì	Sì	Sì	Sì
Crea report	Sì	Sì	Sì	Sì	No
Elimina report	Sì	No	No	No	No
Importa da SnapCenter e gestisci l'host:					
Visualizza i dati importati di SnapCenter	Sì	Sì	Sì	Sì	Sì
Importa dati da SnapCenter	Sì	Sì	No	No	No
Gestisci (migra) host	Sì	Sì	No	No	No
Configura le impostazioni:					
Configura la directory dei log	Sì	Sì	Sì	No	No
Associa o rimuovi le credenziali dell'istanza	Sì	Sì	Sì	No	No
Bucket:					

Caratteristica e azione	Super admin di backup e recovery	Amministratore di backup e ripristino	Backup and recovery ripristino admin	Admin del clone di backup e ripristino	Visualizzatore di backup e ripristino
Visualizza i bucket	Sì	Sì	Sì	Sì	Sì
Crea, modifica o elimina bucket	Sì	Sì	No	No	No

Ruoli utilizzati per azioni specifiche del workload

La tabella seguente indica le azioni che ciascun ruolo di NetApp Backup and Recovery può eseguire per specifici carichi di lavoro.

Carichi di lavoro Kubernetes

Questa tabella indica le azioni che ciascun ruolo di NetApp Backup and Recovery può eseguire per le azioni specifiche dei carichi di lavoro Kubernetes.

Caratteristica e azione	Super admin di backup e recovery	Amministratore di backup e ripristino	Backup and recovery ripristino admin	Visualizzatore di backup e ripristino
Visualizza cluster, namespace, classi di archiviazione e risorse API	Sì	Sì	Sì	Sì
Aggiungi nuovi cluster Kubernetes	Sì	Sì	No	No
Aggiorna le configurazioni del cluster	Sì	No	No	No
Rimuovi i cluster dalla gestione	Sì	No	No	No
Visualizza le applicazioni	Sì	Sì	Sì	Sì
Crea e definisci nuove applicazioni	Sì	Sì	No	No
Aggiorna le configurazioni dell’applicazione	Sì	Sì	No	No
Rimuovi le applicazioni dalla gestione	Sì	Sì	No	No
Visualizza le risorse protette e lo stato del backup	Sì	Sì	Sì	Sì
Crea backup e proteggi le applicazioni con le policy	Sì	Sì	No	No

Caratteristica e azione	Super admin di backup e recovery	Amministratore di backup e ripristino	Backup and recovery ripristino admin	Visualizzatore di backup e ripristino
Rimuovi la protezione dalle app e cancella i backup	Sì	Sì	No	No
Visualizza i punti di ripristino e i risultati del visualizzatore di risorse	Sì	Sì	Sì	Sì
Ripristina le applicazioni dai punti di ripristino	Sì	No	Sì	No
Visualizza le policy di backup di Kubernetes	Sì	Sì	Sì	Sì
Crea policy di backup per Kubernetes	Sì	Sì	Sì	No
Aggiorna le politiche di backup	Sì	Sì	Sì	No
Elimina le policy di backup	Sì	Sì	Sì	No
Visualizza gli hook di esecuzione e le sorgenti degli hook	Sì	Sì	Sì	Sì
Crea hook di esecuzione e sorgenti di hook	Sì	Sì	Sì	No
Aggiorna gli hook di esecuzione e le relative sorgenti	Sì	Sì	Sì	No
Elimina gli hook di esecuzione e le relative sorgenti	Sì	Sì	Sì	No
Visualizza i modelli di hook di esecuzione	Sì	Sì	Sì	Sì
Crea modelli di hook di esecuzione	Sì	Sì	Sì	No
Aggiorna i modelli degli hook di esecuzione	Sì	Sì	Sì	No
Elimina i modelli di hook di esecuzione	Sì	Sì	Sì	No
Visualizza il riepilogo del carico di lavoro e le dashboard di analisi	Sì	Sì	Sì	Sì

Caratteristica e azione	Super admin di backup e recovery	Amministratore di backup e ripristino	Backup and recovery ripristino admin	Visualizzatore di backup e ripristino
Visualizza i bucket e le destinazioni di archiviazione StorageGRID	Sì	Sì	Sì	Sì

Configura le integrazioni e i servizi della NetApp Console

Integra NetApp Console distribuzione locale con Active Directory

Integra la distribuzione locale di NetApp Console con Active Directory per l'accesso e la ricerca degli utenti basati su directory. Usa il tuo servizio di directory per autenticare gli utenti, poi assegna l'accesso a quegli utenti nella distribuzione locale di NetApp Console.

Ruoli di accesso richiesti

Super amministratore o amministratore dell'organizzazione. "Scopri i ruoli di accesso".

Quando integri Active Directory, la distribuzione locale di Console autentica gli utenti tramite la tua directory esistente. Dopo che hai aggiunto un utente alla directory, assegna i ruoli di accesso di Console per controllare a cosa può accedere quell'utente.

L'integrazione con Active Directory ti aiuta anche a soddisfare i requisiti di conformità applicando i controlli, le tracce di controllo e le policy esistenti all'accesso alla distribuzione locale della Console.

- L'integrazione con Active Directory non crea gruppi federati, non sincronizza le assegnazioni tra directory e gruppi e non concede automaticamente l'accesso. Gli amministratori continuano ad aggiungere utenti di directory all'organizzazione e ad assegnare ruoli nella distribuzione locale della Console.
- È supportata una sola integrazione con Active Directory alla volta. Una volta configurata un'integrazione, il pulsante **Aggiungi integrazione** viene disabilitato. Per passare a una directory diversa, disabilita o elimina prima l'integrazione esistente.
- Gli utenti della directory non configurano né utilizzano l'autenticazione a più fattori (MFA). La distribuzione locale della console supporta l'MFA solo per gli utenti locali. "Scopri come gestire le impostazioni di sicurezza dei membri".

Prima di iniziare

Prima di integrare Active Directory, verifica di avere:

- Un dominio Active Directory e le credenziali che possono interrogare la directory
- L'indirizzo del LDAP server e il nome distinto di base (DN) per l'albero della directory
- Accesso di rete dal deployment locale della Console al LDAP server sulla porta 389 (LDAP) o 636 (LDAPS)
- Certificati SSL/TLS, se prevedi di utilizzare LDAPS

Passaggi

1. Seleziona **Amministrazione > Identità e accesso**.
2. Seleziona **Directory services** per aprire la pagina Federations.
3. Seleziona **Aggiungi integrazione**.
4. Inserisci i dettagli di connessione per il tuo server Active Directory:
   - Un nome descrittivo per l'integrazione.
   - L'host LDAP: nome host o indirizzo IP del LDAP server. Per più server, inserisci quello principale.
   - La porta: 389 per LDAP o 636 per LDAPS.
   - Il **timeout di connessione** in millisecondi. Il valore predefinito è 1000 ms.
5. Seleziona **Usa SSL/TLS** per utilizzare LDAPS. Verifica che il tuo LDAP server supporti LDAPS e che la Console possa accedere ai certificati necessari.
6. Verifica la connessione. Se non riesce, controlla l'host LDAP, la porta, la connettività di rete e i certificati SSL/TLS.
7. Dopo che il test ha esito positivo, inserisci la directory e i dettagli dell'utente:
   - **Associazione DN di base**: Inserisci il Bind DN per l'account LDAP/AD che questa app userà per connettersi alla directory e inserisci la Bind credential (password) per quell'account. NetApp Console usa questi dettagli per associarsi a LDAP e convalidare la connessione.
   - **DN utente**: un account utente con l'autorizzazione a interrogare la directory. Ad esempio, `CN=ldap-reader,OU=Service Accounts,DC=example,DC=com`.
8. Seleziona **Aggiungi** per salvare l'integrazione.

Dopo aver finito

Dopo aver salvato l'integrazione, aggiungi gli utenti della directory alla tua organizzazione e assegna loro i ruoli. Devi configurare e abilitare almeno un'integrazione con Active Directory prima di poter aggiungere utenti della directory. "Scopri come aggiungere utenti alla directory e assegnare ruoli".

Disabilita o abilita l'integrazione con Active Directory

Disabilita un'integrazione per sospendere temporaneamente l'autenticazione basata su directory senza eliminare la configurazione. Quando disabiliti un servizio di directory, gli utenti della directory non possono accedere tramite la directory.

Passaggi

1. Seleziona **Amministrazione > Identità e accesso**.
2. Seleziona **Directory services** per aprire la pagina Federations.
3. Nell'elenco delle integrazioni, individua l'integrazione e seleziona il menu delle azioni per quella riga.
4. Seleziona **Disabilita** per sospendere l'integrazione oppure **Abilita** per ripristinarla.

Elimina un'integrazione di Active Directory

Elimina un'integrazione per rimuovere definitivamente la configurazione del servizio di directory. Prima di eliminarla, controlla eventuali avvisi sugli utenti della directory collegati all'integrazione, perché il loro accesso sarà influenzato.

Passaggi

1. Seleziona **Amministrazione > Identità e accesso**.

2. Seleziona **Directory services** per aprire la pagina Federations.
3. Nell'elenco delle integrazioni, individua l'integrazione e seleziona il menu delle azioni per quella riga.
4. Seleziona **Elimina** e conferma l'eliminazione.

Collega il tuo LLM e abilita l'assistente della NetApp Console nella distribuzione locale di NetApp Console

Collega il tuo modello linguistico esteso (LLM) alla distribuzione locale di NetApp Console per abilitare l'assistente di Console e la gestione dello storage assistita dall'IA.

> Questa documentazione relativa alla connessione di un LLM all'assistente della Console per abilitare le funzionalità di intelligenza artificiale è fornita come anteprima tecnologica. Con questa offerta in anteprima, NetApp si riserva il diritto di modificare i dettagli dell'offerta, i contenuti e la tempistica prima della disponibilità generale.

Ruoli di accesso richiesti

Super amministratore o amministratore dell'organizzazione. "Scopri i ruoli di accesso".

Dopo la configurazione, gli utenti aprono l'assistente della Console dalla dashboard e scelgono una modalità di accesso:

- In modalità **sola lettura**, l'assistente risponde alle domande e fornisce indicazioni senza apportare modifiche.
- In modalità **lettura/scrittura**, l'assistente può intervenire sull'infrastruttura di archiviazione. Mostra i dettagli per la revisione e la conferma prima di ogni modifica. Per le operazioni asincrone, come la creazione di volumi, crea un processo che puoi controllare tramite l'assistente.

Per connettere il tuo LLM, seleziona un percorso del provider, inserisci i dettagli dell'endpoint e la chiave API, quindi seleziona un modello in **Administration > AI Tools**. Le azioni dell'Assistant rimangono all'interno delle tue policy di archiviazione e in base al ruolo dei controlli di accesso.

Raccogli tutto il necessario prima di connetterti a un LLM

Prima di collegare il tuo LLM, raccogli quanto segue:

- La tua scelta sul tipo di fornitore: OpenAI o compatibile con OpenAI. "Scopri le opzioni dei provider."
- Una chiave API valida per il percorso del provider che selezioni.
- L'URL dell'endpoint per il percorso del tuo provider.
- L'URL del tuo proxy o gateway, se la tua organizzazione ne richiede uno.
- Il tuo nome utente o single sign-on (SSO) ID per l'account del provider LLM, se richiesto.
- Accesso alla rete dalla distribuzione locale della Console all'endpoint selezionato.
- Classi di archiviazione e controlli di accesso in base al ruolo per le azioni dell'assistente che vuoi consentire.

Per i dettagli sui modelli supportati, vedi "Scopri i provider e i modelli LLM supportati nella distribuzione locale di NetApp Console".

Connetti un LLM alla distribuzione locale della NetApp Console

Inserisci le impostazioni del provider, la chiave API e il modello per connettere il tuo LLM alla distribuzione locale di Console.

Passaggi

1. Accedi alla distribuzione locale della NetApp Console.
2. Seleziona **Amministrazione > Strumenti di IA**.
3. Seleziona il menu, quindi seleziona **Modifica**.
4. In **Tipo di fornitore**, seleziona un tipo di fornitore.

   "Scopri l'integrazione di LLM nella distribuzione locale di NetApp Console".

5. Se ti viene richiesto un endpoint del provider, inserisci l'URL dell'endpoint per il percorso del provider che hai selezionato.
6. Inserisci l'URL del proxy o del gateway e le relative credenziali.
7. Nel campo **Nome utente**, inserisci il tuo nome utente o l'SSO ID se il percorso del tuo provider lo richiede.
8. Nel campo **Chiave API**, incolla la chiave API dal percorso del provider selezionato.
9. Seleziona un modello dall'elenco.
10. Rivedi la configurazione, quindi seleziona **Salva**.

    Se il salvataggio o il test non riescono, verifica il tipo di provider, l'URL dell'endpoint, la chiave API e il modello selezionato, quindi riprova.

"Risolvi i problemi di integrazione di LLM".

Verifica che l'integrazione con LLM funzioni

Dopo aver salvato la configurazione, verifica la disponibilità e il comportamento dell'assistente.

Passaggi

1. Conferma che il pulsante **Assistente console** appare sulla dashboard di distribuzione locale della NetApp Console.
2. Apri l'assistente in modalità **sola lettura** ed esegui una query di base.
3. Apri l'assistente in modalità **lettura/scrittura** e verifica che le azioni che modificano lo storage richiedano la conferma dell'utente prima dell'esecuzione.
4. Verifica che gli utenti che necessitano di flussi di lavoro di azione abbiano i controlli di accesso in base al ruolo richiesti.

Dopo aver completato la convalida, gli utenti possono aprire l'assistente Console dalla dashboard e descrivere le attività in linguaggio naturale. Per esempi di utilizzo e flussi di lavoro per gli utenti finali, vedi "Usa l'assistente della NetApp Console".

Proteggi le credenziali e monitora l'utilizzo di LLM

- Quando possibile, usa una chiave API dedicata per l'integrazione della distribuzione locale della Console.
- Ruota le chiavi API in base alle policy della tua organizzazione.
- Limita la possibilità di modificare le impostazioni di AI Tools solo ai ruoli amministrativi necessari.

- Monitora l’utilizzo delle API lato provider e gli avvisi per individuare attività anomale o picchi di costo.

Risolvi i problemi di integrazione LLM nella distribuzione locale di NetApp Console

Utilizza questo flusso di triage rapido per diagnosticare e risolvere i problemi comuni di integrazione LLM nella NetApp Console in una distribuzione locale.

> Questa documentazione relativa alla connessione di un LLM all’assistente della Console per abilitare le funzionalità di intelligenza artificiale è fornita come anteprima tecnologica. Con questa offerta in anteprima, NetApp si riserva il diritto di modificare i dettagli dell’offerta, i contenuti e la tempistica prima della disponibilità generale.

Se non hai completato la configurazione, consulta "Collega il tuo LLM e abilita l’assistente della NetApp Console".

Gestisci rapidamente i problemi di integrazione LLM

1. Convalida la configurazione degli strumenti di AI in **Amministrazione > Strumenti di AI**.

   Conferma il tipo di provider, l’URL dell’endpoint, la chiave API, il modello selezionato e l’accesso di rete outbound.

2. Verifica la disponibilità dell’assistente sulla dashboard.

   Conferma che il pulsante **Console assistant** appare per gli utenti e le organizzazioni previsti.

3. Convalida il comportamento in fase di esecuzione.

   Esegui una semplice richiesta di sola lettura e verifica la raggiungibilità dell’endpoint del provider, la disponibilità del modello e lo stato del servizio del provider.

Risolvi i problemi in base ai sintomi

Sintomo	Probabile causa	Cosa controllare	Prossima azione
Salvataggio o test non riusciti in AI Tools	Mancata corrispondenza di configurazione o connettività	Tipo di provider, URL dell’endpoint, formato della chiave API, modello selezionato e outbound access	Correggi il valore che non supera la convalida e salva di nuovo
Il pulsante **Assistente console** non è presente	Stato di integrazione non corretto, mancata corrispondenza dell’organizzazione o mancata corrispondenza in base al ruolo (RBAC)	Salvataggio riuscito degli strumenti di AI, stato di integrazione, organizzazione corrente e ruolo di accesso previsto	Aggiorna la sessione e verifica con un account admin noto e funzionante

Sintomo	Probabile causa	Cosa controllare	Prossima azione
L'assistente si apre ma la richiesta fallisce	Problema relativo al provider o al percorso di runtime	Raggiungibilità dell'endpoint, disponibilità del modello su quell'endpoint, limiti del provider e stato temporaneo del provider	Riprova dopo aver risolto i problemi di incompatibilità tra endpoint/modello o i problemi relativi ai limiti lato provider
La risposta dell'assistente è lenta o incoerente	Dimensioni del prompt, prestazioni dell'endpoint o instabilità della rete/proxy	Breve test di verifica, stato del servizio del provider e stabilità della rete/proxy	Utilizza un prompt più breve, prova un altro modello supportato e stabilizza il routing di rete o proxy

Rispondi alla divulgazione o all'uso improprio delle credenziali LLM

Se sospetti l'esposizione della chiave API o un utilizzo non autorizzato:

1. Revoca la chiave API esistente nel sistema del tuo provider.
2. Crea una nuova chiave API.
3. Aggiorna la chiave in **Amministrazione > Strumenti AI**.
4. Verifica l'avvenuta riconnessione con un test assistente in sola lettura.

Configura i canali di consegna delle notifiche nella distribuzione locale di NetApp Console

Nella distribuzione locale di NetApp Console, puoi configurare più canali per le notifiche di avviso, inclusi email e webhook.

Ruoli di accesso richiesti

Super amministratore o amministratore dell'organizzazione. "Scopri i ruoli di accesso".

Per impostazione predefinita, la distribuzione locale della Console visualizza le notifiche tramite il suo sistema di notifica integrato. Configurando canali di consegna aggiuntivi puoi ricevere le notifiche nel modo che si adatta meglio al tuo flusso di lavoro.

Puoi inviare tutte le notifiche tramite gli stessi canali oppure usare canali diversi per diversi tipi di notifica. Ad esempio, potresti inviare avvisi urgenti relativi allo storage tramite email, mentre instradi il traffico di altri avvisi a uno strumento di monitoraggio di terze parti tramite un webhook.

Dopo aver configurato i canali di invio delle notifiche, puoi configurare le regole di notifica e assegnarle ai diversi canali. "Scopri come configurare le regole di notifica".

Configura un server di posta elettronica

Quando configuri un server di posta elettronica, la distribuzione locale di Console invia notifiche, avvisi e inviti agli utenti tramite quel server. La distribuzione locale di Console supporta i server di posta elettronica SMTP, che possono essere il tuo server di posta elettronica aziendale esistente o un servizio di posta elettronica di terze parti.

Passaggi

1. Seleziona **Administration > Console**.
2. Seleziona **Configuration** per aprire la pagina delle configurazioni di sistema.
3. Nella sezione **Server di posta elettronica**, seleziona **Configura**.
4. Inserisci i dettagli di connessione per il tuo server di posta elettronica:
   - Aggiungi il nome del mittente e l'indirizzo email del mittente.
   - L'host SMTP: nome host o indirizzo IP del tuo server SMTP. Per più server, inserisci quello principale.
   - Seleziona il protocollo di connessione dall'elenco a discesa **Sicurezza della connessione**. La porta è configurata per te ed è di sola lettura: 25 per SMTP con STARTTLS o 465 per SMTPS.

     SMTPS (porta 465) stabilisce immediatamente una connessione crittografata ed è consigliato per ambienti sensibili alla sicurezza. STARTTLS (porta 25) aggiorna una connessione non crittografata a una crittografata e può tornare alla trasmissione non crittografata se la negoziazione della crittografia fallisce.
5. Seleziona **Test email** per inviare un'email di prova a un destinatario che specifichi tu.
6. Dopo che il test ha esito positivo, seleziona **Salva** per salvare la configurazione.

   Se il test non va a buon fine, verifica nuovamente le impostazioni inserite e assicurati che la distribuzione locale della Console abbia accesso di rete al server di posta elettronica.

Aggiorna la configurazione del server di posta elettronica

Puoi aggiornare la configurazione di un server di posta elettronica esistente se vuoi usare un server di posta elettronica diverso.

Passaggi

1. Seleziona **Administration > Console**.
2. Seleziona **Configuration** per aprire la pagina delle configurazioni di sistema.
3. Nella sezione **Server di posta elettronica**, seleziona **Configura**.
4. Seleziona **Cancella campi** per cancellare la configurazione esistente.
5. Inserisci i nuovi dati di connessione per il tuo server di posta elettronica.
6. Seleziona **Test email** per inviare un'email di prova a un destinatario che specifichi tu.
7. Dopo che il test ha esito positivo, seleziona **Salva** per salvare la nuova configurazione.

   Se il test non va a buon fine, verifica nuovamente le impostazioni inserite e assicurati che la distribuzione locale della Console abbia accesso di rete al server di posta elettronica.

Rimuovi la configurazione del server di posta elettronica

Puoi rimuovere la configurazione del server di posta elettronica se non vuoi più che la distribuzione locale della Console invii email.

Passaggi

1. Seleziona **Administration > Console**.
2. Seleziona **Configuration** per aprire la pagina di configurazione dei sistemi.
3. Nella sezione **Server di posta elettronica**, seleziona **Configura**.

4. Seleziona **Cancella campi** per cancellare la configurazione esistente.
5. Seleziona **Salva** per salvare la configurazione cancellata, che rimuove la configurazione del server di posta elettronica dalla distribuzione locale della Console.

Configura un webhook

Configura i webhook per inviare notifiche dalla distribuzione locale della Console ad altri strumenti o servizi. Puoi configurare più webhook, ognuno dei quali punta a un endpoint diverso. Ad esempio, uno per un SIEM e un altro per un servizio di paging di reperibilità.

Dopo che crei un webhook, gli utenti con il ruolo di Storage admin possono assegnarlo a specifiche regole di avviso. Ad esempio, possono inviare avvisi critici via email mentre inviano tutti gli avvisi a uno strumento di monitoraggio di terze parti tramite un webhook.

> La distribuzione locale della console non impone il controllo degli accessi agli endpoint webhook. Qualsiasi utente o sistema in grado di raggiungere l'URL dell'endpoint riceve i dati di avviso. Assicurati che l'accesso all'applicazione ricevente sia limitato agli utenti autorizzati tramite i controlli di accesso dell'applicazione stessa.

Prima di iniziare

Conferma che la distribuzione locale della Console possa raggiungere l'applicazione ricevente tramite la rete e raccogli l'URL dell'endpoint, il metodo HTTP e tutti i dettagli di autenticazione o certificato richiesti da quell'applicazione.

Passaggi

1. Seleziona **Administration > Console**.
2. Seleziona **Configuration** per aprire la pagina delle configurazioni di sistema.
3. Nella sezione **Integrazione Webhook**, seleziona **Configura**.
4. Inserisci i dettagli richiesti per il webhook:
   - Un nome descrittivo per il webhook.
   - L'URL dell'endpoint fornito dall'applicazione ricevente.
   - metodo HTTP
   - Facoltativo: un certificato autofirmato in formato PEM.
   - Eventuali intestazioni o segreti richiesti (credenziali per l'autenticazione).
   - Il formato da utilizzare per l'invio del webhook. JSON e OTEL (OpenTelemetry) sono supportati.

     Utilizza JSON per webhook generici ed endpoint REST personalizzati. Utilizza OTEL per piattaforme di osservabilità che consumano segnali OpenTelemetry in modo nativo, come Grafana o altri collector compatibili con OpenTelemetry.
5. Seleziona **Test webhook** per testare la connessione webhook e assicurarti che la distribuzione locale della Console possa inviare correttamente messaggi all'applicazione ricevente.
6. Dopo che il test ha esito positivo, seleziona **Salva** per creare il webhook.

   Dopo aver salvato il webhook, è disponibile per gli utenti selezionarlo dove i webhook sono supportati, ad esempio nelle opzioni di invio degli avvisi. "Scopri come creare regole di avviso e assegnare webhook per la consegna degli avvisi."

Informazioni sul copyright

Informazioni sul marchio commerciale