Gestisci utenti e accessi

NetApp Console local deployment

NetApp
August 10, 2026

Sommario

Gestisci utenti e accessi

Gestisci l’accesso dei membri nella distribuzione locale di NetApp Console

Nella distribuzione locale di NetApp Console, puoi rivedere o modificare i ruoli di un utente su più cartelle o fleet, ad esempio controllando tutto ciò a cui può accedere un storage engineer, aggiungendo un nuovo ruolo in un’altra regione o rimuovendo l’accesso di quell’utente quando cambiano le responsabilità.

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".

Puoi visualizzare e gestire l’accesso in due modi, a seconda delle tue esigenze. Se vuoi vedere i ruoli che un determinato utente ha su tutta la flotta della tua organizzazione, usa la pagina **Members**.

Se vuoi confermare chi può accedere a una flotta specifica, controlla invece i membri assegnati a quella flotta. "Gestisci le assegnazioni di accesso alla flotta".

Per aggiungere un nuovo membro, account di servizio o utente della directory e assegnargli il primo ruolo, usa invece l’attività di onboarding. "Aggiungi membri e assegna ruoli".

Scopri come viene concesso l’accesso in NetApp Console

La NetApp Console utilizza il controllo degli accessi in base al ruolo (RBAC) per gestire le autorizzazioni dei membri. Puoi assegnare ruoli predefiniti a livello di organizzazione, cartella o flotta, a seconda dell’ambito di accesso di cui un membro ha bisogno.

Utilizzo dell’ereditarietà dei ruoli

Un ruolo che assegni a livello di organizzazione o di cartella viene ereditato dagli ambiti figli sottostanti, quindi modifica un’assegnazione ereditata al livello superiore in cui l’hai originariamente concessa.

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

Visualizza i ruoli assegnati a un membro

Conferma esattamente quali ruoli ricopre un membro e a quale livello prima di apportare modifiche. Ad esempio, verifica se un collega ha già il ruolo di Storage admin sulla `Production-EU-West` fleet.

Se hai il ruolo di amministratore di cartelle o flotte, la pagina mostra tutti i membri dell’organizzazione. Tuttavia, puoi visualizzare e gestire i permessi solo per le cartelle e le flotte che amministri. "Scopri le azioni di amministratore di cartelle o flotte nella NetApp Console distribuzione locale".

1. Dalla pagina **Membri**, individua un membro nella tabella, seleziona ••• e poi seleziona **Visualizza dettagli**.
2. Nella tabella, espandi la riga corrispondente all’organizzazione, alla cartella o al fleet in cui vuoi vedere il ruolo assegnato al membro e seleziona **Visualizza** nella colonna **Ruolo**.

Assegna o modifica l’accesso dei membri

Puoi modificare l’accesso di un membro ogni volta che cambiano le sue responsabilità. Ad esempio, quando un collega si occupa del backup per una seconda regione, aggiungi il ruolo di Backup and Recovery admin alla fleet di quella regione senza toccare i suoi ruoli di storage esistenti.

Se devi aggiungere un nuovo membro e assegnargli il suo primo ruolo, consulta "Aggiungi membri e assegna ruoli".

Aggiungi un ruolo di accesso a un membro esistente

Assegna a un membro un ruolo aggiuntivo a livello di organizzazione, cartella o flotta quando le sue responsabilità si espandono. Ad esempio, assegna a uno Storage admin il ruolo di Backup and recovery admin a livello di organizzazione, così può gestire le attività di backup e recovery su tutte le flotte senza perdere le autorizzazioni di storage esistenti.

Puoi assegnare a un membro un ruolo di accesso per la tua organizzazione, cartella o flotta.

I membri possono avere più ruoli all’interno della stessa flotta e in flotte diverse. Ad esempio, le organizzazioni più piccole possono assegnare tutti i ruoli di accesso disponibili allo stesso utente, mentre le organizzazioni più grandi possono far svolgere agli utenti attività più specializzate. In alternativa, puoi anche assegnare a un utente il ruolo di admin della resilienza al ransomware a livello di organizzazione. In questo esempio, l’utente potrà eseguire attività di resilienza al ransomware su tutte le flotte all’interno della tua organizzazione.

La tua strategia di gestione dei ruoli di accesso dovrebbe essere in linea con il modo in cui hai organizzato le tue risorse NetApp.

Passaggi

1. Seleziona **Amministrazione > Identità e accesso**.
2. Seleziona **Members**.
3. Seleziona una delle schede relative ai membri: **Utenti**, **Utenti della directory** o **Account di servizio**.
4. Seleziona il menu delle azioni ••• accanto al membro a cui vuoi assegnare un ruolo e seleziona **Aggiungi un ruolo**.
5. Per aggiungere un ruolo, segui i passaggi indicati nella finestra di dialogo:
   - **Seleziona un’organizzazione, una cartella o una fleet**: scegli il livello della gerarchia delle risorse per cui il membro deve disporre delle autorizzazioni.

     Se selezioni l’organizzazione o una cartella, il membro avrà i permessi su tutto ciò che si trova all’interno dell’organizzazione o della cartella.

   - **Seleziona una categoria**: Scegli una categoria di ruolo. "Scopri i ruoli di accesso".
   - Seleziona un **ruolo**: scegli un ruolo che fornisca al membro le autorizzazioni per le risorse associate all’organizzazione, alla cartella o al fleet che hai selezionato.
   - **Aggiungi ruolo**: Se vuoi concedere l’accesso a cartelle o fleet aggiuntivi all’interno della tua organizzazione, seleziona **Aggiungi ruolo**, specifica un’altra cartella o fleet o categoria di ruolo, quindi seleziona una categoria di ruolo e il ruolo corrispondente.
6. Seleziona **Aggiungi nuovi ruoli**.

Modifica il ruolo assegnato a un membro

Sostituisci il ruolo esistente di un membro con un altro quando le sue responsabilità cambiano. Ad esempio, quando un visualizzatore di Storage sulla `Production-US-East` fleet ha invece bisogno del ruolo di Storage admin.

Ogni utente deve avere almeno un ruolo. Non puoi rimuovere tutti i ruoli da un utente. Se devi rimuovere tutti i ruoli, elimina l'utente dalla tua organizzazione.

Passaggi

1. Seleziona **Amministrazione > Identità e accesso**.
2. Seleziona **Members**.
3. Seleziona una delle schede relative ai membri: **Utenti**, **Utenti della directory** o **Account di servizio**.
4. Dalla pagina **Membri**, individua un membro nella tabella, seleziona ••• e poi seleziona **Visualizza dettagli**.
5. Nella tabella, espandi la riga corrispondente all'organizzazione, alla cartella o al fleet in cui vuoi cambiare il ruolo assegnato al membro e seleziona **Visualizza** nella colonna **Ruolo** per vedere i ruoli assegnati a questo membro.
6. Puoi modificare un ruolo esistente per un membro o rimuovere un ruolo.
   a. Per modificare il ruolo di un membro, seleziona **Modifica** accanto al ruolo che vuoi modificare. Puoi cambiare un ruolo solo con un ruolo della stessa categoria di ruoli. Ad esempio, puoi passare da un ruolo di servizio dati a un altro. Conferma la modifica.
   b. Per rimuovere il ruolo da un membro, seleziona 🗑 accanto al ruolo per rimuovere al membro il rispettivo ruolo. Ti verrà chiesto di confermare la rimozione.

Rimuovi un membro dalla tua organizzazione

Rimuovi un membro quando lascia l'organizzazione o cambia ruolo in modo tale da non aver più bisogno di accedere alla Console. Ad esempio, quando termina il contratto di un collaboratore esterno o un dipendente viene trasferito a un team esterno all'organizzazione della Console.

Utenti della directory

La rimozione di un utente dalla directory impedisce a tale utente di autenticarsi. Dovresti anche rimuovere l'utente dalla tua organizzazione Console per mantenere accurato l'elenco dei membri e per rimuovere eventuali ruoli assegnati nella distribuzione locale di Console.

Passaggi

1. Seleziona **Amministrazione > Identità e accesso**.
2. Seleziona **Members**.
3. Seleziona una delle schede relative ai membri: **Utenti**, **Utenti della directory** o **Account di servizio**.
4. Dalla pagina **Membri**, individua un membro nella tabella, seleziona ••• e poi seleziona **Elimina utente**.
5. Conferma che vuoi rimuovere il membro dalla tua organizzazione.

Visualizza o modifica le assegnazioni di accesso alla flotta nella distribuzione locale di NetApp Console

Verifica o modifica le assegnazioni di accesso dei membri per cartelle e storage fleet

nella distribuzione locale di NetApp Console. Gli admin di cartelle e storage fleet di solito lavorano da questa vista perché mostra solo gli ambiti che amministrano.

Ruoli di accesso richiesti

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

In alternativa, puoi gestire tutti i ruoli di un determinato membro in più cartelle o fleet. "Gestisci l'accesso dei membri".

Come funziona l'accesso alle cartelle e alle fleet

La distribuzione locale tramite console utilizza il controllo degli accessi in base al ruolo (RBAC). Un ruolo che assegni a livello di cartella si applica a tutte le fleet e alle sottocartelle all'interno di quella cartella; un ruolo che assegni a livello di fleet si applica solo alle risorse di quella fleet. "Scopri l'ereditarietà dei ruoli nella distribuzione locale di NetApp Console".

Non puoi modificare un ruolo a livello di flotta se un membro lo eredita da una cartella o dall'organizzazione. Per modificare l'accesso ereditato, cambia il ruolo a un livello superiore.

Visualizza i membri assegnati a una cartella o a una fleet

Verifica esattamente chi può gestire una cartella o un fleet specifico. Ad esempio, prima di associare un nuovo cluster ONTAP alla `Production-US-East` fleet, apri la scheda Accesso della fleet per confermare chi ha accesso.

Passaggi

1. Seleziona **Amministrazione** > **Identità e accesso**.
2. Seleziona **Organization**.
3. Dalla pagina Organizzazione, vai a una cartella o a una fleet nella tabella, seleziona ••• e poi seleziona **Modifica cartella** o **Modifica fleet**.
4. Seleziona **Access** per visualizzare i membri che hanno accesso alla cartella o al fleet.

Modifica l'accesso dei membri da una cartella o da una fleet

Modifica i ruoli dei membri che già appartengono alla tua organizzazione, con ambito limitato a una singola cartella o flotta. Ad esempio, quando un membro del team passa da una flotta di sviluppo a una flotta di produzione, promuovilo da Storage viewer a Storage admin nella flotta di produzione senza influire sul suo accesso altrove.

Per aggiungere un nuovo membro e assegnargli il suo primo ruolo, usa invece l'attività di onboarding. "Aggiungi membri e assegna ruoli".

Passaggi

1. Dalla pagina Organizzazione, vai a una cartella o a una fleet nella tabella, seleziona ••• e poi seleziona **Modifica cartella** o **Modifica fleet**.
2. Seleziona **Access** per visualizzare l'elenco dei membri che hanno accesso.
3. Modifica l'accesso dei membri:
   - **Modifica il ruolo di un membro**: Per qualsiasi membro con un ruolo diverso da Organization admin, seleziona il ruolo attuale e scegli un nuovo ruolo. La modifica si applica solo a questo livello; i ruoli

ereditati da un livello superiore non vengono visualizzati qui.

- **Rimuovi l'accesso del membro a questo ambito**: Per un membro a cui è stato assegnato un ruolo direttamente in questa cartella o flotta, rimuovi il ruolo per revocarne l'accesso a questo ambito. Questa operazione non rimuove il membro dall'organizzazione né influisce sui ruoli che ha in altri ambiti.

  "Rimuovi un membro dalla tua organizzazione".

4. Seleziona **Applica**.

Gestisci la sicurezza dei membri nella distribuzione locale di NetApp Console

Proteggi l'accesso degli utenti alla tua organizzazione di distribuzione locale della NetApp Console gestendo le impostazioni di sicurezza dei membri. Puoi indirizzare gli utenti locali a cambiare le proprie password, gestire l'autenticazione a più fattori (MFA) degli utenti locali e ricreare le credenziali degli account di servizio.

Ruoli di accesso richiesti

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

Reimposta le password utente (solo utenti locali)

Gli amministratori non possono reimpostare direttamente le password degli utenti locali.

Indirizza gli utenti locali a reimpostare la loro password dalla pagina di accesso alla distribuzione locale della Console selezionando **Password dimenticata?**.

Questa opzione non è disponibile per gli utenti della directory.

Gestisci l'autenticazione a più fattori (MFA) di un utente locale

Se un utente locale perde l'accesso al proprio dispositivo MFA, puoi rimuovere o disabilitare la sua configurazione MFA.

L'autenticazione a più fattori è disponibile solo per gli utenti locali. Gli utenti della directory non possono abilitare MFA tramite la distribuzione locale della Console.

Usa queste linee guida per scegliere l'azione giusta:

- Seleziona **Disabilita** quando l'utente perde temporaneamente l'accesso al dispositivo MFA. Disabilitare l'MFA permette un accesso senza MFA per otto ore, poi l'MFA viene riattivata automaticamente.
- Seleziona **Rimuovi** quando l'utente deve reimpostare completamente l'autenticazione a più fattori (MFA). Dopo aver rimosso MFA, l'utente accede senza MFA finché non la configura nuovamente.

Se un utente ha salvato un codice di recupero, può accedere utilizzandolo. Se un utente non ha un codice di recupero, disabilita MFA così l'utente può accedere e riottenere l'accesso.

Per gestire l'autenticazione a più fattori di un utente locale, devi avere un indirizzo email nello stesso dominio dell'utente interessato.

Passaggi

1. Seleziona **Amministrazione** > **Identità e accesso**.
2. Seleziona **Members**.
3. Dalla pagina Membri, individua un membro nella tabella, seleziona ••• e poi seleziona **Gestisci autenticazione a più fattori**.
4. Scegli se rimuovere o disabilitare la configurazione MFA dell'utente.

Dopo aver finito

Esamina il registro di controllo per confermare chi ha modificato l'accesso MFA, quando lo ha modificato e se l'azione è andata a buon fine "Scopri come controllare l'attività di distribuzione locale della NetApp Console".

Ricrea le credenziali per un account di servizio

È possibile creare nuove credenziali per un account di servizio in caso di smarrimento o necessità di aggiornamento delle stesse.

La creazione di nuove credenziali elimina quelle vecchie. Non puoi usare le vecchie credenziali.

Passaggi

1. Seleziona **Amministrazione** > **Identità e accesso**.
2. Seleziona **Members**.
3. Nella tabella Membri, vai su un account di servizio, seleziona ••• e poi seleziona **Ricrea segreti**.
4. Seleziona **Ricrea**.
5. Scarica o copia l'ID client e il client secret.

   La distribuzione locale della Console mostra il segreto del client una sola volta. Assicurati di copiarlo o scaricarlo e di conservarlo in un luogo sicuro.

Informazioni sul copyright

Informazioni sul marchio commerciale