Gestire l'accesso e la sicurezza degli utenti

NetApp Console setup and administration

NetApp
February 11, 2026

Sommario

Gestire l’accesso e la sicurezza degli utenti

Scopri di più sul controllo degli accessi basato sui ruoli (RBAC) NetApp Console

Gestisci l’accesso degli utenti alla NetApp Console con il controllo degli accessi basato sui ruoli (RBAC), assegnando ruoli predefiniti a livello di organizzazione, cartella o progetto. Ogni ruolo concede autorizzazioni specifiche che definiscono quali azioni gli utenti possono eseguire nell’ambito loro assegnato.

NetApp progetta i ruoli della console con privilegi minimi, in modo che ogni ruolo includa solo le autorizzazioni necessarie per le sue attività. Questo approccio aumenta la sicurezza limitando l’accesso a ciò di cui ogni membro ha bisogno.

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

Ad esempio, è possibile assegnare a un membro il ruolo di amministratore di Ransomware Resilience per un livello di progetto specifico, consentendogli di eseguire operazioni di Ransomware Resilience per le risorse all’interno di quel progetto, senza concedergli un accesso più ampio all’intera organizzazione. Allo stesso utente può essere concesso il ruolo per diversi progetti all’interno della tua organizzazione.

È possibile assegnare agli utenti più ruoli per lo stesso ambito o per ambiti diversi, a seconda delle loro responsabilità. Ad esempio, un’organizzazione più piccola potrebbe avere lo stesso utente che gestisce sia le attività di Ransomware Resilience sia quelle di Backup e ripristino a livello di organizzazione, mentre un’organizzazione più grande potrebbe avere utenti diversi assegnati a ciascun ruolo a livello di progetto.

Tipi di membri dell’organizzazione della console

Esistono tre tipi di membri in un’organizzazione NetApp Console : * *Account utente*: singoli utenti che accedono a NetApp Console per gestire le risorse. Gli utenti devono registrarsi alla NetApp Console prima di poter essere aggiunti a un’organizzazione. * *Account di servizio*: account non umani utilizzati dalle applicazioni o dai servizi per interagire con la NetApp Console tramite API. Puoi aggiungere account di servizio direttamente all’organizzazione della tua Console. * *Gruppi federati*: gruppi sincronizzati dal tuo provider di identità (IdP) che ti consentono di gestire l’accesso di più utenti collettivamente. Ogni utente all’interno di un gruppo federato deve essersi registrato alla NetApp Console ed essere stato aggiunto all’organizzazione con un ruolo di accesso prima di poter accedere alle risorse concesse al gruppo.

"Scopri come aggiungere membri alla tua organizzazione."

Ruoli predefiniti nella NetApp Console

NetApp Console include ruoli predefiniti che è possibile assegnare ai membri dell’organizzazione. Ogni ruolo include autorizzazioni che specificano quali azioni un membro può eseguire nell’ambito assegnatogli (organizzazione, cartella o progetto).

I ruoli NetApp Console utilizzano principi di privilegi minimi che garantiscono che i membri abbiano solo le autorizzazioni necessarie per le loro attività e categorizzano i ruoli in base al tipo di accesso che forniscono:

- Ruoli della piattaforma: fornire autorizzazioni di amministrazione della console
- Ruoli dei servizi dati: fornire autorizzazioni per la gestione di servizi dati specifici, come Ransomware

Resilience e Backup e ripristino

- Ruoli dell'applicazione: fornire autorizzazioni per la gestione dell'archiviazione e per il controllo degli eventi e degli avvisi della console

È possibile assegnare più ruoli a un membro in base alle sue responsabilità. Ad esempio, potresti assegnare a un membro sia il ruolo di amministratore Ransomware Resilience sia il ruolo di amministratore Backup e ripristino per un progetto specifico.

"Scopri i ruoli predefiniti disponibili nella NetApp Console".

Gestisci l'accesso dei membri nella NetApp Console

Gestisci l'accesso dei membri nella tua organizzazione Console. Assegnare ruoli per impostare le autorizzazioni. Rimuovi i membri quando se ne vanno.

Ruoli di accesso richiesti

Super amministratore, amministratore dell'organizzazione o amministratore di cartelle o progetti (per le cartelle e i progetti che amministrano). Link:reference-iam-predefined-roles.html[Scopri di più sui ruoli di accesso].

È possibile assegnare ruoli di accesso in base al progetto o alla cartella. Ad esempio, assegnare un ruolo a un utente per due progetti specifici o assegnare il ruolo a livello di cartella per assegnare a un utente il ruolo di amministratore di Ransomware Resilience per tutti i progetti in una cartella

Aggiungi le tue cartelle e i tuoi progetti prima di assegnare l'accesso agli utenti. "Scopri come aggiungere cartelle e progetti."

Scopri come viene concesso l'accesso nella NetApp Console

NetApp Console utilizza un modello di controllo degli accessi basato sui ruoli (RBAC) per gestire le autorizzazioni degli utenti. È possibile assegnare ruoli predefiniti ai membri individualmente o tramite gruppi federati. È possibile aggiungere e assegnare ruoli agli account di servizio, nonché ai gruppi federati. Ogni ruolo definisce quali azioni un membro può eseguire sulle risorse associate.

Tenere presente quanto segue in merito alla concessione dell'accesso nella NetApp Console:

- Tutti gli utenti devono prima registrarsi alla NetApp Console prima di poter ottenere l'accesso alle risorse.
- È necessario assegnare esplicitamente un ruolo a ciascun utente nella Console prima che possa accedere alle risorse, anche se è membro di un gruppo federato a cui è stato assegnato un ruolo.
- È possibile aggiungere account di servizio direttamente dalla Console e assegnare loro ruoli.

Utilizzo dell'ereditarietà dei ruoli

Quando si assegna un ruolo a livello di organizzazione, cartella o progetto in NetApp Console, tale ruolo viene automaticamente ereditato da tutte le risorse nell'ambito selezionato. Ad esempio, i ruoli a livello di cartella si applicano a tutti i progetti contenuti, mentre i ruoli a livello di progetto si applicano a tutte le risorse all'interno di quel progetto.

Visualizza i membri dell'organizzazione

Per capire quali risorse e autorizzazioni sono disponibili per un membro, puoi visualizzare i ruoli assegnati al membro ai diversi livelli della gerarchia delle risorse della tua organizzazione."Scopri come utilizzare i ruoli per

controllare l'accesso alle risorse della Console."

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Membri**.

   Nella tabella **Membri** sono elencati i membri della tua organizzazione.

3. Dalla pagina **Membri**, vai a un membro nella tabella, seleziona ••• e poi seleziona **Visualizza dettagli**.

Visualizza i ruoli assegnati a un membro

Puoi verificare quali ruoli sono attualmente assegnati loro.

Se si dispone del ruolo di *Amministratore cartella o progetto*, la pagina visualizza tutti i membri dell'organizzazione. Tuttavia, puoi visualizzare e gestire le autorizzazioni dei membri solo per le cartelle e i progetti per i quali disponi delle autorizzazioni. "Scopri di più sulle azioni che un *amministratore di cartella o di progetto* può completare" .

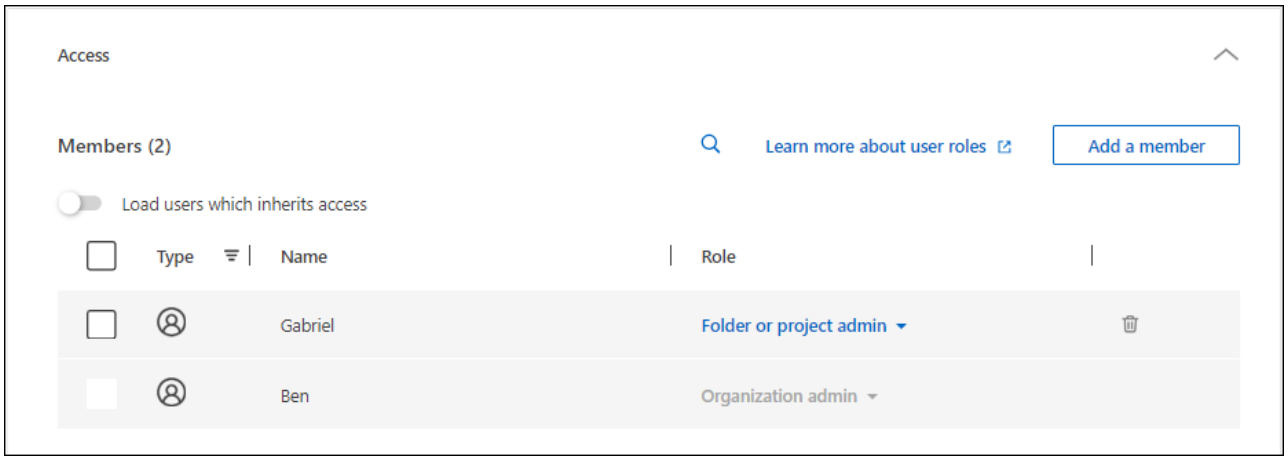
1. Dalla pagina **Membri**, vai a un membro nella tabella, seleziona ••• e poi seleziona **Visualizza dettagli**.
2. Nella tabella, espandi la riga corrispondente all'organizzazione, alla cartella o al progetto in cui desideri visualizzare il ruolo assegnato al membro e seleziona **Visualizza** nella colonna **Ruolo**.

Visualizza i membri associati a una cartella o a un progetto

Puoi visualizzare i membri che hanno accesso a una cartella o a un progetto specifico.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Organizzazione**.
3. Dalla pagina **Organizzazione**, vai a un progetto o a una cartella nella tabella, seleziona ••• e poi seleziona **Modifica cartella** o **Modifica progetto**.
   - Selezionare **Accesso** per visualizzare i membri che hanno accesso alla cartella o al progetto.



Assegna o modifica l'accesso dei membri

Dopo che un utente si è registrato a NetApp Console, puoi aggiungerlo alla tua organizzazione e assegnargli un ruolo per fornire l'accesso alle risorse. "Scopri come aggiungere membri alla tua organizzazione."

È possibile modificare l'accesso di un membro aggiungendo o rimuovendo ruoli in base alle esigenze.

Aggiungere un ruolo di accesso a un membro

Solitamente si assegna un ruolo quando si aggiunge un membro all'organizzazione, ma è possibile aggiornarlo in qualsiasi momento rimuovendo o aggiungendo ruoli.

Puoi assegnare a un utente un ruolo di accesso per la tua organizzazione, cartella o progetto.

I membri possono avere più ruoli all'interno dello stesso progetto e in progetti diversi. Ad esempio, le organizzazioni più piccole potrebbero assegnare tutti i ruoli di accesso disponibili allo stesso utente, mentre le organizzazioni più grandi potrebbero far svolgere agli utenti attività più specializzate. In alternativa, è possibile assegnare a un utente il ruolo di amministratore di Ransomware Resilience a livello di organizzazione. In questo esempio, l'utente sarebbe in grado di eseguire attività di Ransomware Resilience su tutti i progetti all'interno della tua organizzazione.

La strategia del ruolo di accesso deve essere in linea con il modo in cui hai organizzato le tue risorse NetApp .

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Membri**.
3. Selezionare una delle schede dei membri: **Utenti**, **Account di servizio** o **Gruppi federati**.
4. Seleziona il menu azioni ••• accanto al membro a cui vuoi assegnare un ruolo e seleziona **Aggiungi un ruolo**.
5. Per aggiungere un ruolo, completare i passaggi nella finestra di dialogo:
   - **Seleziona un'organizzazione, una cartella o un progetto**: scegli il livello della gerarchia delle risorse per il quale il membro deve avere le autorizzazioni.

     Se selezioni l'organizzazione o una cartella, il membro avrà autorizzazioni per tutto ciò che risiede all'interno dell'organizzazione o della cartella.

   - **Seleziona una categoria**: Scegli una categoria di ruolo. "Scopri di più sui 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 progetto selezionato.
   - **Aggiungi ruolo**: se desideri concedere l'accesso a cartelle o progetti aggiuntivi all'interno della tua organizzazione, seleziona **Aggiungi ruolo**, specifica un'altra cartella, un altro progetto o una categoria di ruolo, quindi seleziona una categoria di ruolo e un ruolo corrispondente.
6. Seleziona **Aggiungi nuovi ruoli**.

Modificare il ruolo assegnato a un membro

Modifica i ruoli di un membro per aggiornarne l'accesso.

Agli utenti deve essere assegnato almeno un ruolo. Non è possibile rimuovere tutti i ruoli da un utente. Se devi rimuovere tutti i ruoli, devi eliminare l'utente dalla tua organizzazione.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Membri**.
3. Selezionare una delle schede dei membri: **Utenti**, **Account di servizio** o **Gruppi federati**.
4. Dalla pagina **Membri**, vai a un membro nella tabella, seleziona ••• e poi seleziona **Visualizza dettagli**.
5. Nella tabella, espandi la riga corrispondente all'organizzazione, alla cartella o al progetto in cui desideri modificare il ruolo assegnato al membro e seleziona **Visualizza** nella colonna **Ruolo** per visualizzare i ruoli assegnati a questo membro.
6. È possibile 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 desideri modificare. È possibile modificare un ruolo solo in un ruolo all'interno della stessa categoria di ruoli. Ad esempio, è possibile passare da un ruolo di servizio dati a un altro. Conferma la modifica.
   b. Per annullare l'assegnazione del ruolo a un membro, selezionare 🗑 accanto al ruolo per rimuovere il rispettivo ruolo dal membro. Ti verrà chiesto di confermare la rimozione.

Rimuovi un membro dalla tua organizzazione

Rimuovi un membro se abbandona la tua organizzazione.

Quando si rimuove un membro, il sistema revoca le autorizzazioni della Console, ma conserva i relativi account Console e NetApp Support Site.

Membri federati

- Gli utenti federati perdono automaticamente l'accesso alla NetApp Console quando vengono rimossi dal tuo IdP. Tuttavia, dovresti comunque rimuoverli dall'organizzazione della tua Console per mantenere aggiornato l'elenco dei membri.
- Se rimuovi un utente da un gruppo federato nel tuo IdP, l'utente perderà l'accesso alla Console associato a quel gruppo. Tuttavia, mantengono comunque qualsiasi accesso associato a un ruolo esplicito loro assegnato nella Console.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Membri**.
3. Selezionare una delle schede dei membri: **Utenti**, **Account di servizio** o **Gruppi federati**.
4. Dalla pagina **Membri**, vai a un membro nella tabella, seleziona ••• quindi seleziona **Elimina utente**.
5. Conferma che desideri rimuovere il membro dalla tua organizzazione.

Sicurezza dell'utente

Proteggi l'accesso degli utenti alla tua organizzazione NetApp Console gestendo le impostazioni di sicurezza dei membri. È possibile reimpostare le password utente, gestire l'autenticazione a più fattori (MFA) e ricreare le credenziali dell'account di servizio.

Ruoli di accesso richiesti

Super amministratore, amministratore dell'organizzazione o amministratore di cartelle o progetti (per le cartelle e i progetti che amministrano). Link:reference-iam-predefined-roles.html[Scopri di più sui ruoli di accesso].

Reimposta le password utente (solo utenti locali)

Gli amministratori dell'organizzazione non possono reimpostare le password degli utenti locali. Possono tuttavia chiedere agli utenti di reimpostare autonomamente le proprie password.

Chiedere all'utente di reimpostare la propria password dalla pagina di accesso della Console selezionando **Password dimenticata?**.

Questa opzione non è disponibile per gli utenti di un'organizzazione federata.

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

Se un utente perde l'accesso al proprio dispositivo MFA, è possibile rimuovere o disabilitare la configurazione MFA.

L'autenticazione a più fattori è disponibile solo per gli utenti locali. Gli utenti federati non possono abilitare MFA.

Gli utenti devono configurare nuovamente l'MFA quando effettuano l'accesso dopo la rimozione. Se l'utente perde temporaneamente l'accesso al proprio dispositivo MFA, può utilizzare il codice di ripristino salvato per effettuare l'accesso.

Se non hanno il codice di ripristino, disattivare temporaneamente l'MFA per consentire l'accesso. Quando si disattiva l'MFA per un utente, questa viene disattivata solo per otto ore e poi riattivata automaticamente. All'utente è consentito un solo accesso durante tale periodo senza MFA. Dopo otto ore, l'utente deve utilizzare MFA per effettuare l'accesso.

Per gestire l'autenticazione a più fattori di un utente, è necessario disporre di un indirizzo email nello stesso dominio dell'utente interessato.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Membri**.

   Nella tabella **Membri** sono elencati i membri della tua organizzazione.

3. Dalla pagina **Membri**, vai a un membro nella tabella, seleziona ••• e quindi seleziona **Gestisci autenticazione a più fattori**.
4. Scegliere se rimuovere o disabilitare la configurazione MFA dell'utente.

Ricreare le credenziali per un account di servizio

Puoi creare nuove credenziali per un servizio se le perdi o devi aggiornarle.

La creazione di nuove credenziali elimina quelle vecchie. Non è possibile utilizzare le vecchie credenziali.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Seleziona **Membri**.
3. Nella tabella **Membri**, vai a un account di servizio, seleziona ••• e poi seleziona **Ricrea segreti**.

4. Seleziona **Ricrea**.
5. Scarica o copia l'ID client e il segreto client.

   La console mostra il segreto del client solo una volta. Assicuratevi di copiarlo o scaricarlo e conservarlo in modo sicuro.