Ruoli di accesso NetApp Console

NetApp Console setup and administration

NetApp
January 13, 2026

Sommario

Ruoli di accesso NetApp Console . . . 1
Scopri di più sui ruoli di accesso NetApp Console . . . 1
Ruoli della piattaforma . . . 1
Ruoli applicativi . . . 2
Ruoli del servizio dati . . . 2
Link correlati . . . 3
Ruoli di accesso alla piattaforma NetApp Console . . . 4
Ruoli di amministrazione dell'organizzazione . . . 4
Ruoli della Federazione . . . 5
Ruoli di partnership . . . 5
Ruoli di super amministratore e visualizzatore . . . 5
Ruoli applicativi . . . 7
Ruoli Google Cloud NetApp Volumes nella NetApp Console . . . 7
Ruoli di accesso Keystone nella NetApp Console . . . 7
Ruolo di accesso dell'analista del supporto operativo per NetApp Console . . . 8
Ruoli di accesso all'archiviazione per NetApp Console . . . 9
Ruoli dei servizi dati . . . 11
Ruoli NetApp Backup and Recovery nella NetApp Console . . . 11
Ruoli NetApp Disaster Recovery nella NetApp Console . . . 15
Ruoli di accesso alla resilienza ransomware per NetApp Console . . . 17

Ruoli di accesso NetApp Console

Scopri di più sui ruoli di accesso NetApp Console

La gestione delle identità e degli accessi (IAM) nella NetApp Console fornisce ruoli predefiniti che puoi assegnare ai membri della tua organizzazione nei diversi livelli della gerarchia delle risorse. Prima di assegnare questi ruoli, è necessario comprendere le autorizzazioni incluse in ciascun ruolo. I ruoli rientrano nelle seguenti categorie: piattaforma, applicazione e servizio dati.

Ruoli della piattaforma

I ruoli della piattaforma concedono autorizzazioni di amministrazione NetApp Console , tra cui l'assegnazione dei ruoli e la gestione degli utenti. La console ha diversi ruoli di piattaforma.

Ruolo della piattaforma	Responsabilità
"Amministratore dell'organizzazione"	Consente all'utente l'accesso illimitato a tutti i progetti e le cartelle all'interno di un'organizzazione, di aggiungere membri a qualsiasi progetto o cartella, nonché di eseguire qualsiasi attività e utilizzare qualsiasi servizio dati a cui non sia associato un ruolo esplicito. Gli utenti con questo ruolo gestiscono la tua organizzazione creando cartelle e progetti, assegnando ruoli, aggiungendo utenti e gestendo i sistemi, se dispongono delle credenziali appropriate. Questo è l'unico ruolo di accesso che può creare agenti Console.
"Amministratore di cartelle o progetti"	Consente all'utente l'accesso illimitato ai progetti e alle cartelle assegnati. Possono aggiungere membri alle cartelle o ai progetti che gestiscono, nonché eseguire qualsiasi attività e utilizzare qualsiasi servizio dati o applicazione sulle risorse all'interno della cartella o del progetto a loro assegnato. Gli amministratori di cartelle o progetti non possono creare agenti della console.
"Amministratore della Federazione"	Consente a un utente di creare e gestire federazioni con la Console, che abilita l'accesso singolo (SSO).
"Visualizzatore della federazione"	Consente a un utente di visualizzare le federazioni esistenti con la Console. Non è possibile creare o gestire federazioni.
"Amministratore della partnership"	Consente all'utente di creare e gestire partnership.
"Visualizzatore di partnership"	Consente all'utente di visualizzare le partnership esistenti. Non è possibile creare o gestire partnership.
"Super amministratore"	Fornisce all'utente un sottoinsieme di ruoli amministrativi. Questo ruolo è pensato per le organizzazioni più piccole che potrebbero non aver bisogno di distribuire le responsabilità della console tra più utenti.
"Super spettatore"	Assegna all'utente un sottoinsieme di ruoli di visualizzazione. Questo ruolo è pensato per le organizzazioni più piccole che potrebbero non aver bisogno di distribuire le responsabilità della console tra più utenti.

Ruoli applicativi

Di seguito è riportato un elenco dei ruoli nella categoria applicazione. Ogni ruolo concede autorizzazioni specifiche nell'ambito designato. Gli utenti che non possiedono il ruolo di piattaforma o applicazione richiesto non possono accedere alla rispettiva applicazione.

Ruolo applicativo	Responsabilità
"Amministratore di Google Cloud NetApp Volumes"	Gli utenti con il ruolo Google Cloud NetApp Volumes possono scoprire e gestire Google Cloud NetApp Volumes.
"Visualizzatore Google Cloud NetApp Volumes"	Gli utenti con il ruolo utente Google Cloud NetApp Volumes possono visualizzare Google Cloud NetApp Volumes.
"Amministratore Keystone"	Gli utenti con il ruolo di amministratore Keystone possono creare richieste di servizio. Consente agli utenti di monitorare e visualizzare l'utilizzo, le risorse e i dettagli amministrativi all'interno del tenant Keystone a cui accedono.
"Visualizzatore Keystone"	Gli utenti con il ruolo di visualizzatore Keystone NON POSSONO creare richieste di servizio. Consente agli utenti di monitorare e visualizzare i consumi, le risorse e le informazioni amministrative all'interno del tenant Keystone a cui accedono.
Ruolo di configurazione del mediatore ONTAP	Gli account di servizio con il ruolo di configurazione ONTAP Mediator possono creare richieste di servizio. Questo ruolo è richiesto in un account di servizio per configurare un'istanza di"Mediatore cloud ONTAP" .
"Analista di supporto operativo"	Fornisce accesso ad avvisi e strumenti di monitoraggio e la possibilità di inserire e gestire casi di supporto.
"Amministratore di archiviazione"	Gestire le funzioni di governance e integrità dello storage, individuare le risorse di storage e modificare ed eliminare i sistemi esistenti.
"Visualizzatore di archiviazione"	Visualizza le funzioni di governance e di integrità dello storage, nonché le risorse di storage precedentemente scoperte. Impossibile scoprire, modificare o eliminare i sistemi di archiviazione esistenti.
"Specialista in salute del sistema"	Gestire le funzioni di archiviazione, integrità e governance; tutte le autorizzazioni dell'amministratore di archiviazione, tranne quella di non poter modificare o eliminare i sistemi esistenti.

Ruoli del servizio dati

Di seguito è riportato un elenco dei ruoli nella categoria dei servizi dati. Ogni ruolo concede autorizzazioni specifiche nell'ambito designato. Gli utenti che non dispongono del ruolo di servizio dati richiesto o di un ruolo di piattaforma non potranno accedere al servizio dati.

Ruolo del servizio dati	Responsabilità
"Super amministratore di backup e ripristino"	Eseguire qualsiasi azione in NetApp Backup and Recovery.
"Amministratore di backup e ripristino"	Eseguire backup su snapshot locali, replicare su storage secondario ed eseguire backup su storage di oggetti.

Ruolo del servizio dati	Responsabilità
"Backup e ripristino ripristino amministratore"	Ripristinare i carichi di lavoro nel backup e nel ripristino.
"Amministratore clone di backup e ripristino"	Clona applicazioni e dati nel Backup e Ripristino.
"Visualizzatore di backup e ripristino"	Visualizza le informazioni di backup e ripristino.
"Amministratore del ripristino di emergenza"	Eseguire qualsiasi azione nel servizio NetApp Disaster Recovery .
"Amministratore del failover del ripristino di emergenza"	Eseguire failover e migrazioni.
"Amministratore dell'applicazione Disaster Recovery"	Crea piani di replicazione, modifica i piani di replicazione e avvia i failover di prova.
"Visualizzatore di Disaster Recovery"	Visualizza solo le informazioni.
Visualizzatore di classificazione	Consente agli utenti di visualizzare i risultati della scansione NetApp Data Classification . Gli utenti con questo ruolo possono visualizzare le informazioni sulla conformità e generare report per le risorse per le quali hanno l'autorizzazione ad accedere. Questi utenti non possono abilitare o disabilitare la scansione di volumi, bucket o schemi di database. La classificazione non ha un ruolo amministrativo.
"Amministratore di Ransomware Resilience"	Gestisci le azioni nelle schede Proteggi, Avvisi, Ripristina, Impostazioni e Report di NetApp Ransomware Resilience.
"Visualizzatore di resilienza ransomware"	Visualizza i dati del carico di lavoro, visualizza i dati degli avvisi, scarica i dati di ripristino e scarica i report in Ransomware Resilience.
"Comportamento utente di Ransomware Resilience amministratore"	Configura, gestisci e visualizza il rilevamento, gli avvisi e il monitoraggio dei comportamenti sospetti degli utenti in Ransomware Resilience.
"Visualizzatore del comportamento dell'utente di Ransomware Resilience"	Visualizza avvisi e approfondimenti sui comportamenti sospetti degli utenti in Ransomware Resilience.
Amministratore SnapCenter	Offre la possibilità di eseguire il backup di snapshot da 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 e ripristino > Applicazioni * Gestire tutti i sistemi nei progetti e nelle cartelle per i quali dispone delle autorizzazioni * Utilizzare tutti i servizi NetApp Console SnapCenter non ha un ruolo di visualizzatore.

Link correlati

- "Scopri di più sulla gestione dell'identità e degli accessi NetApp Console"
- "Inizia con NetApp Console IAM"
- "Gestisci i membri NetApp Console e le relative autorizzazioni"

- "Scopri di più sull'API per NetApp Console IAM"

Ruoli di accesso alla piattaforma NetApp Console

Assegna ruoli di piattaforma agli utenti per concedere autorizzazioni per gestire la NetApp Console, assegnare ruoli, aggiungere utenti, creare agenti della console e gestire federazioni.

Esempio di ruoli organizzativi per una grande organizzazione multinazionale

XYZ Corporation organizza l'accesso all'archiviazione dei dati per regione (Nord America, Europa e Asia-Pacifico), garantendo un controllo regionale con supervisione centralizzata.

L'**amministratore dell'organizzazione** nella console di XYZ Corporation crea un'organizzazione iniziale e cartelle separate per ogni regione. L'**amministratore della cartella o del progetto** di ogni regione organizza i progetti (con le risorse associate) all'interno della cartella della regione.

Gli amministratori regionali con il ruolo di **Amministratore cartella o progetto** gestiscono attivamente le proprie cartelle aggiungendo risorse e utenti. Questi amministratori regionali possono anche aggiungere, rimuovere o rinominare le cartelle e i progetti che gestiscono. L'**amministratore dell'organizzazione** eredita le autorizzazioni per tutte le nuove risorse, mantenendo la visibilità dell'utilizzo dello spazio di archiviazione nell'intera organizzazione.

All'interno della stessa organizzazione, a un utente viene assegnato il ruolo di **Amministratore federazione** 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'**amministratore dell'organizzazione** assegna a un utente il ruolo di **Visualizzatore federazione** per controllare lo stato della federazione e visualizzare le organizzazioni federate.

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

Ruoli di amministrazione dell'organizzazione

Compito	Amministratore dell'organizzazione	Amministratore di cartelle o progetti
Crea agenti	SÌ	NO
Crea, modifica o elimina sistemi dalla Console (aggiungi o scopri sistemi)	SÌ	SÌ
Crea cartelle e progetti, inclusa l'eliminazione	SÌ	NO
Rinomina cartelle e progetti esistenti	SÌ	SÌ
Assegna ruoli e aggiungi utenti	SÌ	SÌ
Associare risorse a cartelle e progetti	SÌ	SÌ
Associare agenti a cartelle e progetti	SÌ	NO
Rimuovere gli agenti dalle cartelle e dai progetti	SÌ	NO
Gestire gli agenti (modificare certificati, impostazioni e così via)	SÌ	NO

Compito	Amministratore dell'organizzazione	Amministratore di cartelle o progetti
Gestisci le credenziali da Amministrazione > Credenziali	SÌ	SÌ
Crea, gestisci e visualizza le federazioni	SÌ	NO
Registrati per ricevere supporto e invia casi tramite la Console	SÌ	SÌ
Utilizzare servizi dati non associati a un ruolo di accesso esplicito	SÌ	SÌ
Visualizza la pagina Audit e le notifiche	SÌ	SÌ

Ruoli della Federazione

Compito	Amministratore della Federazione	Visualizzatore della federazione
Creare una federazione	SÌ	NO
Verificare un dominio	SÌ	NO
Aggiungere un dominio a una federazione	SÌ	NO
Disattivare ed eliminare le federazioni	SÌ	NO
Federazioni di prova	SÌ	NO
Visualizza le federazioni e i loro dettagli	SÌ	SÌ

Ruoli di partnership

Compito	Amministratore della partnership	Visualizzatore di partnership
Può creare una partnership	SÌ	NO
Assegnare ruoli ai membri partner	SÌ	NO
Può aggiungere membri a una partnership	SÌ	NO
Può visualizzare i dettagli della partnership dell'organizzazione	SÌ	SÌ

Ruoli di super amministratore e visualizzatore

Il ruolo di **Super amministratore** fornisce accesso completo alla gestione delle funzionalità della Console, dell'archiviazione e dei servizi dati. Questo ruolo è adatto a coloro che supervisionano l'amministrazione e la governance. Al contrario, il ruolo **Super viewer** offre un accesso di sola lettura, ideale per revisori o stakeholder che necessitano di visibilità senza apportare modifiche.

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

Esempio per i ruoli super

ABC Corporation dispone di un piccolo team di cinque persone che sfrutta la NetApp Console per la gestione dei servizi dati e dello storage. Invece di distribuire più ruoli, assegnano il ruolo di **Super amministratore** a due membri senior del team che gestiscono tutte le attività amministrative, tra cui la gestione degli utenti e la configurazione delle risorse. Ai restanti tre membri del team viene assegnato il ruolo di **Super visualizzatore**, che consente loro di monitorare lo stato dell'archiviazione e del servizio dati senza la possibilità di modificare le impostazioni.

Ruolo	Ruoli ereditati
Super amministratore	• Amministratore dell'organizzazione • Amministratore di cartelle o progetti • Amministratore della Federazione • Amministratore della partnership • Amministratore di Ransomware Resilience • Amministratore del ripristino di emergenza • Super amministratore di backup • Amministratore di archiviazione • Amministratore Keystone • Amministratore di Google Cloud NetApp Volumes
Super spettatore	• Visualizzatore dell'organizzazione • Visualizzatore della federazione • Visualizzatore di partnership • Visualizzatore di resilienza ransomware • Visualizzatore di ripristino di emergenza • Visualizzatore di backup • Visualizzatore di archiviazione • Visualizzatore Keystone • Visualizzatore Google Cloud NetApp Volumes

Ruoli applicativi

Ruoli Google Cloud NetApp Volumes nella NetApp Console

È possibile assegnare il seguente ruolo agli utenti per consentire loro di accedere a Google Cloud NetApp Volumes nella NetApp Console.

Google Cloud NetApp Volumes utilizza il seguente ruolo:

- * Amministratore Google Cloud NetApp Volumes *: scopri e gestisci Google Cloud NetApp Volumes nella Console.
- * Visualizzatore Google Cloud NetApp Volumes *: visualizza Google Cloud NetApp Volumes nella Console.

Ruoli di accesso Keystone nella NetApp Console

I ruoli Keystone forniscono l'accesso alle dashboard Keystone e consentono agli utenti di visualizzare e gestire il proprio abbonamento Keystone . Esistono due ruoli Keystone : amministratore Keystone e visualizzatore Keystone . La differenza principale tra i due ruoli riguarda le azioni che possono intraprendere in Keystone. Il ruolo di amministratore Keystone è l'unico a cui è consentito creare richieste di servizio o modificare abbonamenti.

Esempio di ruoli Keystone nella NetApp Console

XYZ Corporation dispone di quattro tecnici di archiviazione provenienti da reparti diversi che visualizzano le informazioni sugli abbonamenti Keystone . Sebbene tutti questi utenti debbano monitorare l'abbonamento Keystone , solo il responsabile del team è autorizzato a effettuare richieste di assistenza. A tre membri del team viene assegnato il ruolo di * Keystone viewer*, mentre al responsabile del team viene assegnato il ruolo di * Keystone admin*, in modo che vi sia un punto di controllo sulle richieste di servizio per l'azienda.

La tabella seguente indica le azioni che ciascun ruolo Keystone può eseguire.

Caratteristica e azione	Amministratore Keystone	Visualizzatore Keystone
Visualizza le seguenti schede: Abbonamento, Risorse, Monitoraggio e Amministrazione	SÌ	SÌ
* Pagina di abbonamento Keystone *:		
Visualizza gli abbonamenti	SÌ	SÌ
Modificare o rinnovare gli abbonamenti	SÌ	NO
* Pagina delle risorse Keystone *:		
Visualizza risorse	SÌ	SÌ
Gestire le risorse	SÌ	NO
* Pagina degli avvisi Keystone *:		

Caratteristica e azione	Amministratore Keystone	Visualizzatore Keystone
Visualizza avvisi	SÌ	SÌ
Gestisci gli avvisi	SÌ	NO
Crea avvisi per te stesso	SÌ	SÌ
* Licenses and subscriptions*:		
Può visualizzare licenze e abbonamenti	SÌ	SÌ
* Pagina dei report Keystone *:		
Scarica i report	SÌ	SÌ
Gestisci i report	SÌ	SÌ
Crea report per te stesso	SÌ	SÌ
Richieste di servizio:		
Crea richieste di servizio	SÌ	NO
Visualizza le richieste di servizio create da qualsiasi utente all'interno dell'organizzazione	SÌ	SÌ

Ruolo di accesso dell'analista del supporto operativo per NetApp Console

È possibile assegnare agli utenti il ruolo di analista del supporto operativo per consentire loro di accedere ad avvisi e monitoraggio. Gli utenti con questo ruolo possono anche aprire casi di supporto.

Analista di supporto operativo

Compito	Può eseguire
Gestisci le tue credenziali utente da Impostazioni > Credenziali	SÌ
Visualizza le risorse scoperte	SÌ
Registrati per ricevere supporto e invia casi tramite la Console	SÌ
Visualizza la pagina Audit e le notifiche	SÌ
Visualizza, scarica e configura gli avvisi	SÌ

Ruoli di accesso all’archiviazione per NetApp Console

È possibile assegnare i seguenti ruoli agli utenti per consentire loro di accedere alle funzionalità di gestione dello storage nella NetApp Console. È possibile assegnare agli utenti un ruolo amministrativo per gestire l’archiviazione o un ruolo di visualizzatore per il monitoraggio.

Questi ruoli non sono disponibili dall’API di partnership NetApp Console .

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

Risorse di archiviazione:

- Cluster ONTAP on-premise
- StorageGRID
- Serie E

Servizi e funzionalità della console:

- Consulente digitale
- Aggiornamenti software
- Pianificazione del ciclo di vita
- Sostenibilità

Esempio di ruoli di archiviazione nella NetApp Console

XYZ Corporation, una multinazionale, dispone di un ampio team di ingegneri e amministratori di storage. Consentono a questo team di gestire le risorse di archiviazione per le proprie regioni, limitando al contempo l’accesso alle attività principali della Console, come la gestione degli utenti, la creazione degli agenti e la gestione delle licenze.

All’interno di un team di 12 persone, a due utenti viene assegnato il ruolo di **Visualizzatore di archiviazione**, che consente loro di monitorare le risorse di archiviazione associate ai progetti della Console a cui sono assegnati. Ai restanti nove viene assegnato il ruolo di **Amministratore di storage**, che include la possibilità di gestire gli aggiornamenti software, accedere a ONTAP System Manager tramite la Console e scoprire le risorse di storage (aggiungere sistemi). A una persona del team viene assegnato il ruolo di **Specialista dell’integrità del sistema**, in modo che possa gestire l’integrità delle risorse di storage nella propria regione, ma non modificare o eliminare alcun sistema. Questa persona può anche eseguire aggiornamenti software sulle risorse di archiviazione per i progetti a lei assegnati.

L’organizzazione dispone di altri due utenti con il ruolo di **Amministratore organizzazione** che possono gestire tutti gli aspetti della Console, tra cui la gestione degli utenti, la creazione degli agenti e la gestione delle licenze, nonché di diversi utenti con il ruolo di **Amministratore cartella o progetto** che possono eseguire attività di amministrazione della Console per le cartelle e i progetti a cui sono assegnati.

Nella tabella seguente vengono illustrate le azioni eseguite da ciascun ruolo di archiviazione.

Caratteristica e azione	Amministratore di archiviazione	Specialista in salute del sistema	Visualizzatore di archiviazione
Gestione dell'archiviazione:			
Scoprire nuove risorse (creare sistemi)	SÌ	SÌ	NO
Visualizza i sistemi scoperti	SÌ	SÌ	NO
Elimina i sistemi dalla Console	SÌ	NO	NO
Modificare i sistemi	SÌ	NO	NO
Crea agenti	NO	NO	NO
Consulente digitale			
Visualizza tutte le pagine e le funzioni	SÌ	SÌ	SÌ
* Licenses and subscriptions*			
Visualizza tutte le pagine e le funzioni	NO	NO	NO
Aggiornamenti software			
Visualizza la landing page e i consigli	SÌ	SÌ	SÌ
Esaminare le potenziali raccomandazioni sulla versione e i principali vantaggi	SÌ	SÌ	SÌ
Visualizza i dettagli di aggiornamento per un cluster	SÌ	SÌ	SÌ
Esegui controlli pre-aggiornamento e scarica il piano di aggiornamento	SÌ	SÌ	SÌ
Installa gli aggiornamenti software	SÌ	SÌ	NO
Pianificazione del ciclo di vita			
Esaminare lo stato di pianificazione della capacità	SÌ	SÌ	SÌ
Scegli l'azione successiva (migliore pratica, livello)	SÌ	NO	NO
Trasferisci i dati inattivi nell'archiviazione cloud e libera spazio di archiviazione	SÌ	SÌ	NO
Imposta promemoria	SÌ	SÌ	SÌ
Sostenibilità			
Visualizza dashboard e consigli	SÌ	SÌ	SÌ

Caratteristica e azione	Amministratore di archiviazione	Specialista in salute del sistema	Visualizzatore di archiviazione
Scarica i dati del report	SÌ	SÌ	SÌ
Modifica la percentuale di mitigazione del carbonio	SÌ	SÌ	NO
Correggi le raccomandazioni	SÌ	SÌ	NO
Rinviare le raccomandazioni	SÌ	SÌ	NO
Accesso al gestore del sistema			
Può inserire le credenziali	SÌ	SÌ	NO
Credenziali			
Credenziali utente	SÌ	SÌ	NO

Ruoli dei servizi dati

Ruoli NetApp Backup and Recovery nella NetApp Console

È possibile assegnare i seguenti ruoli agli utenti per consentire loro di accedere a NetApp Backup and Recovery all'interno della Console. I ruoli di backup e ripristino offrono la flessibilità di assegnare agli utenti un ruolo specifico per le attività che devono svolgere all'interno della tua organizzazione. Il modo in cui si assegnano i ruoli dipende dalle proprie pratiche aziendali e di gestione dell'archiviazione.

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

- **Super amministratore di Backup e Recovery**: esegue qualsiasi azione in NetApp Backup and Recovery.
- **Amministratore di backup e ripristino**: esegue backup su snapshot locali, replica su storage secondario ed esegue il backup su azioni di storage di oggetti in NetApp Backup and Recovery.
- **Amministratore di Backup e ripristino**: ripristina i carichi di lavoro utilizzando NetApp Backup and Recovery.
- **Amministratore di backup e ripristino Clone**: clona applicazioni e dati utilizzando NetApp Backup and Recovery.
- **Visualizzatore di backup e ripristino**: visualizza le informazioni in NetApp Backup and Recovery, ma non esegue alcuna azione.

Per i dettagli su tutti i ruoli di accesso NetApp Console , vedere "la documentazione di configurazione e amministrazione della console" .

Ruoli utilizzati per azioni comuni

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

Caratteristica e azione	Super amministratore di backup e ripristino	Backup e ripristino amministratore del backup	Backup e ripristino ripristino amministratore	Amministratore 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 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
Avviare la scoperta dei carichi di lavoro	NO	SÌ	SÌ	SÌ	NO
Visualizza le informazioni sulla licenza	SÌ	SÌ	SÌ	SÌ	SÌ
Attiva la licenza	SÌ	NO	NO	NO	NO
Visualizza gli host	SÌ	SÌ	SÌ	SÌ	SÌ
Orari:					
Attivare gli orari	SÌ	SÌ	SÌ	SÌ	NO
Sospendere gli orari	SÌ	SÌ	SÌ	SÌ	NO
Politiche e protezione:					
Visualizza i piani di protezione	SÌ	SÌ	SÌ	SÌ	SÌ
Creare, modificare o eliminare piani di protezione	SÌ	SÌ	NO	NO	NO
Ripristinare 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
Segnalazioni:					

Caratteristica e azione	Super amministratore di backup e ripristino	Backup e ripristino amministratore del backup	Backup e ripristino ripristino amministratore	Amministratore clone di backup e ripristino	Visualizzatore di backup e ripristino
Visualizza i report	SÌ	SÌ	SÌ	SÌ	SÌ
Crea report	SÌ	SÌ	SÌ	SÌ	NO
Elimina i report	SÌ	NO	NO	NO	NO
Importa da SnapCenter e gestisci l'host:					
Visualizza i dati SnapCenter importati	SÌ	SÌ	SÌ	SÌ	SÌ
Importa dati da SnapCenter	SÌ	SÌ	NO	NO	NO
Gestisci (migra) l'host	SÌ	SÌ	NO	NO	NO
Configura impostazioni:					
Configurare la directory dei registri	SÌ	SÌ	SÌ	NO	NO
Associare o rimuovere le credenziali dell'istanza	SÌ	SÌ	SÌ	NO	NO
Secchi:					
Visualizza i bucket	SÌ	SÌ	SÌ	SÌ	SÌ
Crea, modifica o elimina bucket	SÌ	SÌ	NO	NO	NO

Ruoli utilizzati per azioni specifiche del carico di lavoro

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

Carichi di lavoro Kubernetes

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

Caratteristica e azione	Super amministratore di backup e ripristino	Backup e ripristino amministratore del backup	Backup e ripristino ripristino amministratore	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
Rimuovere i cluster dalla gestione	SÌ	NO	NO	NO
Visualizza le applicazioni	SÌ	SÌ	SÌ	SÌ
Creare e definire nuove applicazioni	SÌ	SÌ	NO	NO
Aggiorna le configurazioni dell'applicazione	SÌ	SÌ	NO	NO
Rimuovere 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 policy	SÌ	SÌ	NO	NO
Rimuovi la protezione dalle app ed elimina i backup	SÌ	SÌ	NO	NO
Visualizza i punti di ripristino e i risultati del visualizzatore delle 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
Creare policy di backup di Kubernetes	SÌ	SÌ	SÌ	NO
Aggiorna i criteri di backup	SÌ	SÌ	SÌ	NO

Caratteristica e azione	Super amministratore di backup e ripristino	Backup e ripristino amministratore del backup	Backup e ripristino ripristino amministratore	Visualizzatore di backup e ripristino
Elimina i criteri di backup	SÌ	SÌ	SÌ	NO
Visualizza gli hook di esecuzione e le sorgenti degli hook	SÌ	SÌ	SÌ	SÌ
Creare hook di esecuzione e sorgenti di hook	SÌ	SÌ	SÌ	NO
Aggiorna gli hook di esecuzione e le sorgenti degli hook	SÌ	SÌ	SÌ	NO
Eliminare gli hook di esecuzione e le sorgenti degli hook	SÌ	SÌ	SÌ	NO
Visualizza i modelli di hook di esecuzione	SÌ	SÌ	SÌ	SÌ
Creare modelli di hook di esecuzione	SÌ	SÌ	SÌ	NO
Aggiorna i modelli di hook di esecuzione	SÌ	SÌ	SÌ	NO
Elimina i modelli di hook di esecuzione	SÌ	SÌ	SÌ	NO
Visualizza i dashboard di riepilogo e analisi del carico di lavoro	SÌ	SÌ	SÌ	SÌ
Visualizza i bucket StorageGRID e le destinazioni di archiviazione	SÌ	SÌ	SÌ	SÌ

Ruoli NetApp Disaster Recovery nella NetApp Console

È possibile assegnare i seguenti ruoli agli utenti per consentire loro di accedere a NetApp Disaster Recovery all'interno della Console. I ruoli di Disaster Recovery offrono la flessibilità di assegnare agli utenti un ruolo specifico per le attività che devono svolgere all'interno della tua organizzazione. Il modo in cui si assegnano i ruoli dipende dalle proprie pratiche aziendali e di gestione dell'archiviazione.

Il ripristino di emergenza utilizza i seguenti ruoli:

- **Amministratore del ripristino di emergenza**: Esegui qualsiasi azione.
- **Amministratore failover di disaster recovery**: esegue failover e migrazioni.

- **Amministratore dell'applicazione di ripristino di emergenza**: crea piani di replica. Modificare i piani di replicazione. Avviare i failover di prova.
- **Visualizzatore di ripristino di emergenza**: visualizza solo le informazioni.

La tabella seguente indica le azioni che ciascun ruolo può eseguire.

Caratteristica e azione	Amministratore del ripristino di emergenza	Amministratore del failover del ripristino di emergenza	Amministratore dell'applicazione di ripristino di emergenza	Visualizzatore di ripristino di emergenza
Visualizza la dashboard e tutte le schede	SÌ	SÌ	SÌ	SÌ
Inizia la prova gratuita	SÌ	NO	NO	NO
Avviare la scoperta dei carichi di lavoro	SÌ	NO	NO	NO
Visualizza le informazioni sulla licenza	SÌ	SÌ	SÌ	SÌ
Attiva la licenza	SÌ	NO	SÌ	NO
Nella scheda Siti:				
Visualizza i siti	SÌ	SÌ	SÌ	SÌ
Aggiungere, modificare o eliminare siti	SÌ	NO	NO	NO
Nella scheda Piani di replicazione:				
Visualizza i piani di replicazione	SÌ	SÌ	SÌ	SÌ
Visualizza i dettagli del piano di replicazione	SÌ	SÌ	SÌ	SÌ
Creare o modificare piani di replicazione	SÌ	SÌ	SÌ	NO
Crea report	SÌ	NO	NO	NO
Visualizza istantanee	SÌ	SÌ	SÌ	SÌ
Eseguire test di failover	SÌ	SÌ	SÌ	NO
Eseguire failover	SÌ	SÌ	NO	NO
Eseguire failback	SÌ	SÌ	NO	NO
Eseguire migrazioni	SÌ	SÌ	NO	NO

Caratteristica e azione	Amministratore del ripristino di emergenza	Amministratore del failover del ripristino di emergenza	Amministratore dell'applicazione di ripristino di emergenza	Visualizzatore di ripristino di emergenza
Nella scheda Gruppi di risorse:				
Visualizza gruppi di risorse	SÌ	SÌ	SÌ	SÌ
Crea, modifica o elimina gruppi di risorse	SÌ	NO	SÌ	NO
Nella scheda Monitoraggio lavori:				
Visualizza i lavori	SÌ	NO	SÌ	SÌ
Annulla lavori	SÌ	SÌ	SÌ	NO

Ruoli di accesso alla resilienza ransomware per NetApp Console

I ruoli di Ransomware Resilience forniscono agli utenti l'accesso a NetApp Ransomware Resilience. Ransomware Resilience supporta i seguenti ruoli:

Ruoli di base

- Amministratore di Ransomware Resilience: configura le impostazioni di Ransomware Resilience; esamina e rispondi agli avvisi di crittografia
- Visualizzatore di resilienza ransomware: visualizza incidenti di crittografia, report e impostazioni di rilevamento

Ruoli di attività comportamentali dell'utente"Rilevamento di attività sospette degli utenti" Gli avvisi forniscono visibilità sui dati, ad esempio sugli eventi di attività dei file; questi avvisi includono i nomi dei file e le azioni sui file (ad esempio Lettura, Scrittura, Eliminazione, Rinomina) eseguite dall'utente. Per limitare la visibilità di questi dati, solo gli utenti con questi ruoli possono gestire o visualizzare questi avvisi.

- Comportamento utente Ransomware Resilience - Attiva il rilevamento delle attività sospette degli utenti, indaga e rispondi agli avvisi di attività sospette degli utenti
- Visualizzatore del comportamento utente di Ransomware Resilience: visualizza gli avvisi sulle attività sospette degli utenti

> I ruoli di comportamento dell'utente non sono ruoli autonomi; sono progettati per essere aggiunti ai ruoli di amministratore o visualizzatore di Ransomware Resilience. Per maggiori informazioni, vedere Ruoli comportamentali dell'utente.

Per descrizioni dettagliate di ciascun ruolo, consultare le tabelle seguenti.

Ruoli di base

Nella tabella seguente vengono descritte le azioni disponibili per i ruoli di amministratore e visualizzatore di Ransomware Resilience.

Caratteristica e azione	Amministratore di Ransomware Resilience	Visualizzatore di resilienza ransomware
Visualizza la dashboard e tutte le schede	SÌ	SÌ
Nella dashboard, aggiorna lo stato della raccomandazione	SÌ	NO
Inizia la prova gratuita	SÌ	NO
Avviare la scoperta dei carichi di lavoro	SÌ	NO
Avviare la riscoperta dei carichi di lavoro	SÌ	NO
Nella scheda Proteggi:		
Aggiungere, modificare o eliminare piani di protezione per le policy di *crittografia*	SÌ	NO
Proteggere i carichi di lavoro	SÌ	NO
Identificare l'esposizione ai dati sensibili con la classificazione dei dati	SÌ	NO
Elencare i piani di protezione e i dettagli	SÌ	SÌ
Elenca i gruppi di protezione	SÌ	SÌ
Visualizza i dettagli del gruppo di protezione	SÌ	SÌ
Crea, modifica o elimina gruppi di protezione	SÌ	NO
Scarica i dati	SÌ	SÌ
Nella scheda Avvisi:		
Visualizza gli avvisi di crittografia e i dettagli degli avvisi	SÌ	SÌ
Modifica lo stato dell'incidente di crittografia	SÌ	NO
Segnala l'avviso di crittografia per il ripristino	SÌ	NO
Visualizza i dettagli dell'incidente di crittografia	SÌ	SÌ
Ignorare o risolvere gli incidenti di crittografia	SÌ	NO
Ottieni l'elenco completo dei file interessati dall'evento di crittografia	SÌ	NO
Scarica i dati degli avvisi degli eventi di crittografia	SÌ	SÌ

Caratteristica e azione	Amministratore di Ransomware Resilience	Visualizzatore di resilienza ransomware
Blocca utente (con configurazione agente Workload Security)	SÌ	NO
Nella scheda Recupera:		
Scarica i file interessati dall'evento di crittografia	SÌ	NO
Ripristina il carico di lavoro dall'evento di crittografia	SÌ	NO
Scarica i dati di recupero dall'evento di crittografia	SÌ	SÌ
Scarica i report dall'evento di crittografia	SÌ	SÌ
Nella scheda Impostazioni:		
Aggiungere o modificare le destinazioni di backup	SÌ	NO
Elenca le destinazioni di backup	SÌ	SÌ
Visualizza gli obiettivi SIEM connessi	SÌ	SÌ
Aggiungere o modificare gli obiettivi SIEM	SÌ	NO
Configurare l'esercitazione di preparazione	SÌ	NO
Avvia, reimposta o modifica l'esercitazione di preparazione	SÌ	NO
Esaminare lo stato di preparazione dell'esercitazione	SÌ	SÌ
Aggiorna la configurazione di rilevamento	SÌ	NO
Visualizza la configurazione di rilevamento	SÌ	SÌ
Nella scheda Report:		
Scarica i report	SÌ	SÌ

Ruoli comportamentali dell'utente

Per configurare le impostazioni relative al comportamento sospetto degli utenti e rispondere agli avvisi, un utente deve disporre del ruolo di amministratore del comportamento utente di Ransomware Resilience. Per visualizzare solo gli avvisi relativi a comportamenti sospetti degli utenti, l'utente deve disporre del ruolo di visualizzatore del comportamento utente Ransomware Resilience.

I ruoli di comportamento dell'utente dovrebbero essere conferiti agli utenti con privilegi di amministratore o visualizzatore di Ransomware Resilience esistenti che necessitano di accesso a"impostazioni e avvisi di attività utente sospette" . Ad esempio, un utente con il ruolo di amministratore Ransomware Resilience

dovrebbe ricevere il ruolo di amministratore del comportamento utente Ransomware Resilience per configurare gli agenti di attività utente e bloccare o sbloccare gli utenti. Il ruolo di amministratore del comportamento utente di Ransomware Resilience non deve essere conferito a un visualizzatore di Ransomware Resilience.

Per attivare il rilevamento delle attività sospette degli utenti, è necessario disporre del ruolo di amministratore dell'organizzazione della console.

Nella tabella seguente vengono descritte le azioni disponibili per i ruoli di amministratore e visualizzatore del comportamento utente di Ransomware Resilience.

Caratteristica e azione	Comportamento utente di Ransomware Resilience amministratore	Visualizzatore del comportamento dell'utente di Ransomware Resilience
Nella scheda Impostazioni:		
Crea, modifica o elimina l'agente di attività utente	SÌ	NO
Crea o elimina il connettore della directory utente	SÌ	NO
Metti in pausa o riprendi il raccoglitore dati	SÌ	NO
Eseguire un'esercitazione di preparazione alla violazione dei dati	SÌ	NO
Nella scheda Proteggi:		
Aggiungere, modificare o eliminare piani di protezione per le policy relative al *comportamento sospetto degli utenti*	SÌ	NO
Nella scheda Avvisi:		
Visualizza gli avvisi sulle attività degli utenti e i dettagli degli avvisi	SÌ	SÌ
Modifica lo stato dell'incidente dell'attività dell'utente	SÌ	NO
Contrassegna l'avviso di attività dell'utente per il ripristino	SÌ	NO
Visualizza i dettagli dell'incidente relativo all'attività dell'utente	SÌ	SÌ
Ignora o risolvi gli incidenti relativi alle attività degli utenti	SÌ	NO
Ottieni l'elenco completo dei file interessati dall'utente sospetto	SÌ	SÌ
Scarica i dati degli avvisi sugli eventi di attività dell'utente	SÌ	SÌ
Blocca o sblocca l'utente	SÌ	NO

Caratteristica e azione	Comportamento utente di Ransomware Resilience amministratore	Visualizzatore del comportamento dell'utente di Ransomware Resilience
Nella scheda Recupera:		
Scarica i file interessati dall'evento di attività dell'utente	SÌ	NO
Ripristina il carico di lavoro dall'evento di attività dell'utente	SÌ	NO
Scarica i dati di recupero dall'evento di attività dell'utente	SÌ	SÌ
Scarica i report dagli eventi di attività dell'utente	SÌ	SÌ

Informazioni sul copyright

Informazioni sul marchio commerciale