Sicurezza e conformità

NetApp Console setup and administration

NetApp
January 23, 2026

Sommario

Sicurezza e conformità

Federazione delle identità

Abilita l’accesso singolo utilizzando la federazione delle identità con NetApp Console

L’accesso Single Sign-On (federazione) semplifica il processo di accesso e migliora la sicurezza consentendo agli utenti di accedere alla NetApp Console utilizzando le proprie credenziali aziendali. Puoi abilitare l’accesso Single Sign-On (SSO) con il tuo provider di identità (IdP) o con il sito di supporto NetApp .

Ruolo richiesto

Amministratore dell’organizzazione, amministratore della federazione, visualizzatore della federazione."Scopri di più sui ruoli di accesso."

Federazione delle identità con il sito di supporto NetApp

La federazione con il sito di supporto NetApp consente agli utenti di accedere alla console, Active IQ Digital Advisor e ad altre app associate utilizzando le stesse credenziali.

> Se esegui la federazione con il sito di supporto NetApp , non puoi eseguirla anche con il tuo provider di gestione dell’identità aziendale. Scegli quello più adatto alla tua organizzazione.

Passi

1. Scarica e completa il "Modulo di richiesta di federazione NetApp" .
2. Inviare il modulo all’indirizzo email specificato nel modulo.

   Il team di supporto NetApp esamina ed elabora la tua richiesta.

Imposta una connessione federata con il tuo provider di identità

È possibile impostare una connessione federata con il proprio provider di identità per abilitare l’accesso Single Sign-On (SSO) per la Console. Il processo prevede la configurazione del provider di identità in modo che consideri NetApp affidabile come fornitore di servizi e la successiva creazione della connessione nella Console.

> Se in precedenza hai configurato la federazione utilizzando NetApp Cloud Central (un’applicazione esterna alla Console), devi importare la federazione utilizzando la pagina Federazione per gestirla all’interno della Console."Scopri come importare la tua federazione."

Provider di identità supportati

NetApp supporta i seguenti protocolli e provider di identità per la federazione:

Protocolli

- Provider di identità Security Assertion Markup Language (SAML)
- Servizi federativi di Active Directory (AD FS)

Fornitori di identità

- ID di accesso Microsoft
- PingFederate

Federazione con flusso di lavoro NetApp Console

NetApp supporta solo SSO avviato dal provider di servizi (SP). Per prima cosa è necessario configurare il provider di identità in modo che consideri attendibile NetApp come fornitore di servizi. Quindi, è possibile creare una connessione nella Console che utilizzi la configurazione del provider di identità.

Puoi effettuare la federazione con il tuo dominio di posta elettronica o con un dominio diverso di tua proprietà. Per federarti con un dominio diverso dal tuo dominio di posta elettronica, verifica innanzitutto di essere il proprietario del dominio.

Verifica il tuo dominio (se non stai utilizzando il tuo dominio di posta elettronica)

Per federarti con un dominio diverso dal tuo dominio di posta elettronica, verifica di esserne il proprietario. Puoi federare il tuo dominio di posta elettronica senza ulteriori passaggi.

Configura il tuo IdP in modo che consideri NetApp come fornitore di servizi attendibile

Configura il tuo provider di identità in modo che si fidi NetApp creando una nuova applicazione e fornendo dettagli come l'URL ACS, l'ID entità o altre informazioni sulle credenziali. Le informazioni sul fornitore di servizi variano a seconda del fornitore di identità, pertanto per maggiori dettagli fare riferimento alla documentazione del proprio fornitore di identità specifico. Per completare questo passaggio dovrai collaborare con l'amministratore dell'IdP.

Crea la connessione federata nella Console

Fornisci l'URL o il file dei metadati SAML dal tuo provider di identità per creare la connessione. Queste informazioni vengono utilizzate per stabilire la relazione di trust tra la Console e il tuo provider di identità. Le informazioni fornite dipendono dall'IdP utilizzato. Ad esempio, se si utilizza l'ID Microsoft Entra, è necessario fornire l'ID client, il segreto e il dominio.

Prova la tua federazione nella Console

Testa la tua connessione federata prima di abilitarla. Utilizzare l'opzione di test nella pagina Federazione nella Console per verificare che l'utente di prova possa autenticarsi correttamente. Se il test ha esito positivo, è possibile abilitare la connessione.

Abilita la tua connessione nella Console

Dopo aver abilitato la connessione, gli utenti potranno accedere alla Console utilizzando le proprie credenziali aziendali.

Per iniziare, rivedi l'argomento relativo al tuo protocollo o IdP:

- "Impostare una connessione federata con AD FS"
- "Imposta una connessione federata con Microsoft Entra ID"

- "Imposta una connessione federata con PingFederate"
- "Impostare una connessione federata con un provider di identità SAML"

Verifica del dominio

Verifica il dominio email per la tua connessione federata

Se desideri federarti con un dominio diverso dal tuo dominio di posta elettronica, devi prima verificare di essere il proprietario del dominio. Per la federazione è possibile utilizzare solo domini verificati.

Ruoli richiesti

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

La verifica del tuo dominio comporta l'aggiunta di un record TXT alle impostazioni DNS del tuo dominio. Questo record viene utilizzato per dimostrare che sei il proprietario del dominio e consente alla NetApp Console di considerare attendibile il dominio per la federazione. Potrebbe essere necessario coordinarsi con l'amministratore IT o di rete per completare questo passaggio.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazione** per visualizzare la pagina **Federazioni**.
3. Selezionare **Configura nuova federazione**.
4. Seleziona **Verifica la proprietà del dominio**.
5. Inserisci il dominio che vuoi verificare e seleziona **Continua**.
6. Copiare il record TXT fornito.
7. Vai alle impostazioni DNS del tuo dominio e configura il valore TXT fornito come record TXT per il tuo dominio. Se necessario, collaborare con l'amministratore IT o di rete.
8. Dopo aver aggiunto il record TXT, tornare alla Console e selezionare **Verifica**.

Configurare le federazioni

Federare la NetApp Console con Active Directory Federation Services (AD FS)

Federa i tuoi servizi di federazione di Active Directory (AD FS) con la NetApp Console per abilitare l'accesso singolo (SSO) per la NetApp Console. Ciò consente agli utenti di accedere alla Console utilizzando le proprie credenziali aziendali.

Ruoli richiesti

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

Puoi federarti con il tuo IdP aziendale o con il sito di supporto NetApp . NetApp consiglia di scegliere l'una o l'altra opzione, ma non entrambe.

NetApp supporta solo SSO avviato dal provider di servizi (SP). Per prima cosa, configura il provider di identità in modo che consideri attendibile la NetApp Console come provider di servizi. Quindi, crea una connessione

nella Console utilizzando la configurazione del tuo provider di identità.

È possibile configurare la federazione con il server AD FS per abilitare l'accesso Single Sign-On (SSO) per NetApp Console. Il processo prevede la configurazione di AD FS in modo che consideri attendibile la Console come fornitore di servizi e quindi la creazione della connessione nella NetApp Console.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazione** per visualizzare la pagina **Federazioni**.
3. Selezionare **Configura nuova federazione**.
4. Inserisci i dettagli del tuo dominio:
   a. Scegli se vuoi utilizzare un dominio verificato o il tuo dominio di posta elettronica. Il dominio di posta elettronica è il dominio associato all'account con cui hai effettuato l'accesso.
   b. Inserisci il nome della federazione che stai configurando.
   c. Se scegli un dominio verificato, seleziona il dominio dall'elenco.
5. Selezionare **Avanti**.
6. Per il metodo di connessione, seleziona **Protocollo** e poi seleziona **Active Directory Federation Services (AD FS)**.
7. Selezionare **Avanti**.
8. Crea un trust della relying party nel tuo server AD FS. È possibile utilizzare PowerShell o configurarlo manualmente sul server AD FS. Per informazioni dettagliate su come creare un trust relying party, consultare la documentazione di AD FS.
   a. Creare il trust utilizzando PowerShell utilizzando il seguente script:

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

   b. In alternativa, è possibile creare manualmente il trust nella console di gestione di AD FS. Utilizzare i seguenti valori NetApp Console durante la creazione del trust:
      - Quando si crea il Relying Trust Identifier, utilizzare il valore **YOUR_TENANT**: `netapp-cloud-account`
      - Quando selezioni **Abilita supporto per WS-Federation**, usa il valore **YOUR_AUTH0_DOMAIN**: `netapp-cloud-account.auth0.com`
   c. Dopo aver creato il trust, copia l'URL dei metadati dal tuo server AD FS o scarica il file dei metadati della federazione. Questo URL o file ti servirà per completare la connessione nella Console.

   NetApp consiglia di utilizzare l'URL dei metadati per consentire alla NetApp Console di recuperare automaticamente la configurazione AD FS più recente. Se scarichi il file dei metadati della federazione, dovrai aggiornarlo manualmente nella NetApp Console ogni volta che vengono apportate modifiche alla configurazione di AD FS.
9. Torna alla Console e seleziona **Avanti** per creare la connessione.

10. Creare la connessione con AD FS.
    a. Inserisci l'URL di AD FS copiato dal server AD FS nel passaggio precedente oppure carica il file dei metadati di federazione scaricato dal server AD FS.
11. Seleziona **Crea connessione**. La creazione della connessione potrebbe richiedere alcuni secondi.
12. Selezionare **Avanti**.
13. Seleziona **Test connessione** per testare la tua connessione. Verrai indirizzato a una pagina di accesso per il tuo server IdP. Accedi con le tue credenziali IdP. Dopo aver effettuato l'accesso, torna alla Console per abilitare la connessione.

    Quando si utilizza la Console in modalità limitata, copiare l'URL in una finestra del browser in incognito o in un browser separato per accedere al proprio IdP.

14. Nella Console, seleziona **Avanti** per rivedere la pagina di riepilogo.
15. Imposta le notifiche.

    Scegli tra sette giorni o 30 giorni. Il sistema invia notifiche di scadenza tramite e-mail e le mostra nella Console a tutti gli utenti con i seguenti ruoli: Super amministratore, Amministratore organizzazione, Amministratore federazione e Visualizzatore federazione.

16. Rivedi i dettagli della federazione e seleziona **Abilita federazione**.
17. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti accedono alla NetApp Console utilizzando le proprie credenziali aziendali.

Federare la NetApp Console con l'ID Microsoft Entra

Federati con il tuo provider IdP Microsoft Entra ID per abilitare l'accesso Single Sign-On (SSO) per NetApp Console. Ciò consente agli utenti di accedere utilizzando le proprie credenziali aziendali.

Ruoli richiesti

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

Puoi federarti con il tuo IdP aziendale o con il sito di supporto NetApp . NetApp consiglia di scegliere l'una o l'altra opzione, ma non entrambe.

NetApp supporta solo SSO avviato dal provider di servizi (SP). Per prima cosa è necessario configurare il provider di identità in modo che consideri attendibile NetApp come fornitore di servizi. Quindi, è possibile creare una connessione nella Console che utilizzi la configurazione del provider di identità.

È possibile impostare una connessione federata con Microsoft Entra ID per abilitare l'accesso Single Sign-On (SSO) per la Console. Il processo prevede la configurazione del tuo ID Microsoft Entra in modo che consideri attendibile la Console come fornitore di servizi e quindi la creazione della connessione nella Console.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazione** per visualizzare la pagina **Federazioni**.

3. Selezionare **Configura nuova federazione**.

Dettagli del dominio

1. Inserisci i dettagli del tuo dominio:
   a. Scegli se vuoi utilizzare un dominio verificato o il tuo dominio di posta elettronica. Il dominio di posta elettronica è il dominio associato all'account con cui hai effettuato l'accesso.
   b. Inserisci il nome della federazione che stai configurando.
   c. Se scegli un dominio verificato, seleziona il dominio dall'elenco.
2. Selezionare **Avanti**.

Metodo di connessione

1. Per il metodo di connessione, seleziona **Provider** e poi seleziona **Microsoft Entra ID**.
2. Selezionare **Avanti**.

Istruzioni di configurazione

1. Configura il tuo ID Microsoft Entra per considerare NetApp attendibile come fornitore di servizi. Devi eseguire questo passaggio sul tuo server Microsoft Entra ID.
   a. Utilizzare i seguenti valori durante la registrazione dell'app Microsoft Entra ID per considerare attendibile la console:
      - Per l'URL di reindirizzamento, utilizzare `https://services.cloud.netapp.com`
      - Per l'**URL di risposta**, usa `https://netapp-cloud-account.auth0.com/login/callback`
   b. Crea un segreto client per la tua app Microsoft Entra ID. Per completare la federazione sarà necessario fornire l'ID client, il segreto client e il nome di dominio ID Entra.
2. Torna alla Console e seleziona **Avanti** per creare la connessione.

Crea connessione

1. Crea la connessione con Microsoft Entra ID
   a. Inserisci l'ID client e il segreto client creati nel passaggio precedente.
   b. Inserisci il nome di dominio dell'ID Microsoft Entra.
2. Seleziona **Crea connessione**. Il sistema crea la connessione in pochi secondi.

Testare e abilitare la connessione

1. Selezionare **Avanti**.
2. Seleziona **Test connessione** per testare la tua connessione. Verrai indirizzato a una pagina di accesso per il tuo server IdP. Accedi con le tue credenziali IdP. Dopo aver effettuato l'accesso, torna alla Console per abilitare la connessione.

   Quando si utilizza la Console in modalità limitata, copiare l'URL in una finestra del browser in incognito o in un browser separato per accedere al proprio IdP.

3. Nella Console, seleziona **Avanti** per rivedere la pagina di riepilogo.

4. Imposta le notifiche.

   Scegli tra sette giorni o 30 giorni. Il sistema invia notifiche di scadenza tramite e-mail e le mostra nella Console a tutti gli utenti con i seguenti ruoli: Super amministratore, Amministratore organizzazione, Amministratore federazione e Visualizzatore federazione.

5. Rivedi i dettagli della federazione e seleziona **Abilita federazione**.
6. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti accedono alla NetApp Console utilizzando le proprie credenziali aziendali.

Federare la NetApp Console con PingFederate

Federati con il tuo provider IdP PingFederate per abilitare l'accesso singolo (SSO) per la NetApp Console. Ciò consente agli utenti di accedere utilizzando le proprie credenziali aziendali.

Ruoli richiesti

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

Puoi federarti con il tuo IdP aziendale o con il sito di supporto NetApp . NetApp consiglia di scegliere l'una o l'altra opzione, ma non entrambe.

NetApp supporta solo SSO avviato dal provider di servizi (SP). Per prima cosa è necessario configurare il provider di identità in modo che consideri attendibile NetApp come fornitore di servizi. Quindi, è possibile creare una connessione nella Console che utilizzi la configurazione del provider di identità.

È possibile impostare una connessione federata con PingFederate per abilitare l'accesso singolo (SSO) per la Console. Il processo prevede la configurazione del server PingFederate in modo che consideri attendibile la Console come fornitore di servizi e quindi la creazione della connessione nella Console.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazione** per visualizzare la pagina **Federazioni**.
3. Selezionare **Configura nuova federazione**.
4. Inserisci i dettagli del tuo dominio:
   a. Scegli se vuoi utilizzare un dominio verificato o il tuo dominio di posta elettronica. Il dominio di posta elettronica è il dominio associato all'account con cui hai effettuato l'accesso.
   b. Inserisci il nome della federazione che stai configurando.
   c. Se scegli un dominio verificato, seleziona il dominio dall'elenco.
5. Selezionare **Avanti**.
6. Per il metodo di connessione, seleziona **Provider** e poi seleziona **PingFederate**.
7. Selezionare **Avanti**.
8. Configura il tuo server PingFederate in modo che consideri NetApp affidabile come fornitore di servizi. Devi eseguire questo passaggio sul tuo server PingFederate.

a. Utilizzare i seguenti valori quando si configura PingFederate per considerare attendibile la NetApp Console:
   - Per l'URL di risposta o l'URL del servizio consumatori di asserzione (ACS), utilizzare `https://netapp-cloud-account.auth0.com/login/callback`
   - Per l'URL di disconnessione, utilizzare `https://netapp-cloud-account.auth0.com/logout`
   - Per **ID pubblico/entità**, utilizzare `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` dove <fed-domain-name-pingfederate> è il nome di dominio della federazione. Ad esempio, se il tuo dominio è `example.com` , l'ID Pubblico/Entità sarebbe `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .

b. Copia l'URL del server PingFederate. Questo URL sarà necessario quando si crea la connessione nella Console.

c. Scarica il certificato X.509 dal tuo server PingFederate. Deve essere in formato PEM codificato in Base64 (.pem, .crt, .cer).

9. Torna alla Console e seleziona **Avanti** per creare la connessione.
10. Crea la connessione con PingFederate
    a. Inserisci l'URL del server PingFederate che hai copiato nel passaggio precedente.
    b. Carica il certificato di firma X.509. Il certificato deve essere in formato PEM, CER o CRT.
11. Seleziona **Crea connessione**. Il sistema crea la connessione in pochi secondi.
12. Selezionare **Avanti**.
13. Seleziona **Test connessione** per testare la tua connessione. Verrai indirizzato a una pagina di accesso per il tuo server IdP. Accedi con le tue credenziali IdP. Dopo aver effettuato l'accesso, torna alla Console per abilitare la connessione.

    Quando si utilizza la Console in modalità limitata, copiare l'URL in una finestra del browser in incognito o in un browser separato per accedere al proprio IdP.

14. Nella Console, seleziona **Avanti** per rivedere la pagina di riepilogo.
15. Imposta le notifiche.

    Scegli tra sette giorni o 30 giorni. Il sistema invia notifiche di scadenza tramite e-mail e le mostra nella Console a tutti gli utenti con i seguenti ruoli: Super amministratore, Amministratore organizzazione, Amministratore federazione e Visualizzatore federazione.

16. Rivedi i dettagli della federazione e seleziona **Abilita federazione**.
17. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti accedono alla NetApp Console utilizzando le proprie credenziali aziendali.

Federare con un provider di identità SAML

Federati con il tuo provider IdP SAML 2.0 per abilitare l'accesso Single Sign-On (SSO) per la console NEtApp. Ciò consente agli utenti di accedere utilizzando le proprie credenziali aziendali.

Ruolo richiesto

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

Puoi federarti con il tuo IdP aziendale o con il sito di supporto NetApp . Non è possibile federarsi con entrambi.

NetApp supporta solo SSO avviato dal provider di servizi (SP). Per prima cosa è necessario configurare il provider di identità in modo che consideri attendibile NetApp come fornitore di servizi. Quindi, è possibile creare una connessione nella Console che utilizzi la configurazione del provider di identità.

È possibile impostare una connessione federata con il provider SAML 2.0 per abilitare l'accesso Single Sign-On (SSO) per la Console. Il processo prevede la configurazione del provider in modo che consideri attendibile NetApp come fornitore di servizi e la successiva creazione della connessione nella Console.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazione** per visualizzare la pagina **Federazioni**.
3. Selezionare **Configura nuova federazione**.
4. Inserisci i dettagli del tuo dominio:
   a. Scegli se vuoi utilizzare un dominio verificato o il tuo dominio di posta elettronica. Il dominio di posta elettronica è il dominio associato all'account con cui hai effettuato l'accesso.
   b. Inserisci il nome della federazione che stai configurando.
   c. Se scegli un dominio verificato, seleziona il dominio dall'elenco.
5. Selezionare **Avanti**.
6. Per il metodo di connessione, seleziona **Protocollo** e poi seleziona **Provider di identità SAML**.
7. Selezionare **Avanti**.
8. Configura il tuo provider di identità SAML in modo che consideri attendibile NetApp come fornitore di servizi. È necessario eseguire questo passaggio sul server del provider SAML.
   a. Assicurati che il tuo IdP abbia l'attributo `email` impostato sull'indirizzo email dell'utente. Ciò è necessario affinché la Console identifichi correttamente gli utenti:

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

1. Utilizzare i seguenti valori quando si registra l'applicazione SAML con la Console:

- Per l'URL di risposta o l'URL del servizio consumatori di asserzione (ACS), utilizzare `https://netapp-cloud-account.auth0.com/login/callback`
- Per l'URL di disconnessione, utilizzare `https://netapp-cloud-account.auth0.com/logout`
- Per **ID pubblico/entità**, utilizzare `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` dove <fed-domain-name-saml> è il nome di dominio che si desidera utilizzare per la federazione. Ad esempio, se il tuo dominio è `example.com` , l'ID Pubblico/Entità sarebbe `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .

2. Dopo aver creato il trust, copia i seguenti valori dal server del tuo provider SAML:
   - URL di accesso
   - URL di disconnessione (facoltativo)
3. Scarica il certificato X.509 dal server del tuo provider SAML. Deve essere in formato PEM, CER o CRT.
   a. Torna alla Console e seleziona **Avanti** per creare la connessione.
   b. Creare la connessione con SAML.
4. Inserisci l'**URL di accesso** del tuo server SAML.
5. Carica il certificato X.509 che hai scaricato dal server del tuo provider SAML.
6. Facoltativamente, inserisci l'**URL di disconnessione** del tuo server SAML.
   a. Seleziona **Crea connessione**. Il sistema crea la connessione in pochi secondi.
   b. Selezionare **Avanti**.
   c. Seleziona **Test connessione** per testare la tua connessione. Verrai indirizzato a una pagina di accesso per il tuo server IdP. Accedi con le tue credenziali IdP. Dopo aver effettuato l'accesso, torna alla Console per abilitare la connessione.

      Quando si utilizza la Console in modalità limitata, copiare l'URL in una finestra del browser in incognito o in un browser separato per accedere al proprio IdP.

   d. Nella Console, seleziona **Avanti** per rivedere la pagina di riepilogo.
   e. Imposta le notifiche.

      Scegli tra sette giorni o 30 giorni. Il sistema invia notifiche di scadenza tramite e-mail e le mostra nella Console a tutti gli utenti con i seguenti ruoli: Super amministratore, Amministratore organizzazione, Amministratore federazione e Visualizzatore federazione.

   f. Rivedi i dettagli della federazione e seleziona **Abilita federazione**.
   g. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti accedono alla NetApp Console utilizzando le proprie credenziali aziendali.

Gestire le federazioni

Gestisci le federazioni nella NetApp Console

Puoi gestire la tua federazione nella NetApp Console. Puoi disattivarlo, aggiornare le credenziali scadute e anche disattivarlo se non ti serve più.

Ruoli richiesti

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

Puoi anche aggiungere un ulteriore dominio verificato a una federazione esistente, il che ti consente di utilizzare più domini per la tua connessione federata.

- Se hai configurato la federazione utilizzando NetApp Cloud Central, importala tramite la pagina **Federazione** per gestirla nella Console."Scopri come importare la tua federazione"
- È possibile visualizzare gli eventi di gestione della federazione, come l'abilitazione, la disabilitazione e l'aggiornamento delle federazioni, nella pagina Audit. "Scopri di più sulle operazioni di monitoraggio nella NetApp Console."

Abilitare una federazione

Se hai creato una federazione ma non è abilitata, puoi abilitarla tramite la pagina **Federazione**. L'abilitazione di una federazione consente agli utenti associati alla federazione di accedere alla Console utilizzando le proprie credenziali aziendali. Creare e testare correttamente la federazione prima di abilitarla.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare la scheda **Federazione**.
3. Seleziona il menu azioni ••• accanto alla federazione che vuoi abilitare e seleziona **Abilita**.

Aggiungi un dominio verificato a una federazione esistente

È possibile aggiungere un dominio verificato a una federazione esistente nella Console per utilizzare più domini con lo stesso provider di identità (IdP).

Prima di poterlo aggiungere a una federazione, è necessario aver già verificato il dominio nella Console. Se non hai ancora verificato il dominio, puoi farlo seguendo i passaggi in"Verifica il tuo dominio nella Console" .

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare la scheda **Federazione**.
3. Seleziona il menu azioni ⋮ accanto alla federazione a cui vuoi aggiungere un dominio verificato e seleziona **Aggiorna domini**. Nella finestra di dialogo **Aggiorna domini** viene visualizzato il dominio già associato a questa federazione.
4. Seleziona un dominio verificato dall'elenco dei domini disponibili.
5. Selezionare **Aggiorna**. I nuovi utenti del dominio possono ottenere l'accesso alla Console federata entro 30 secondi.

Aggiornamento di una connessione federata in scadenza

È possibile aggiornare i dettagli di una federazione nella Console. Ad esempio, sarà necessario aggiornare la federazione se le credenziali, come un certificato o un segreto client, scadono. Se necessario, aggiorna la data di notifica per ricordarti di aggiornare la connessione prima che scada.

Aggiornare prima la Console prima di aggiornare l'IdP per evitare problemi di accesso. Rimani connesso alla Console durante il processo.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare la scheda **Federazione**.
3. Selezionare il menu azioni (tre punti verticali) accanto alla federazione che si desidera aggiornare e selezionare **Aggiorna federazione**.
4. Aggiornare i dettagli della federazione secondo necessità.
5. Selezionare **Aggiorna**.

Testare una federazione esistente

Testare la connessione di una federazione esistente per verificarne il funzionamento. Ciò può aiutarti a identificare eventuali problemi con la federazione e a risolverli.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare la scheda **Federazione**.
3. Seleziona il menu azioni accanto alla federazione a cui vuoi aggiungere un dominio verificato e seleziona **Test connessione**.
4. Selezionare **Test**. Il sistema ti chiederà di accedere con le tue credenziali aziendali. Se la connessione riesce, verrai reindirizzato alla NetApp Console. Se la connessione fallisce, viene visualizzato un messaggio di errore che indica il problema con la federazione.
5. Selezionare **Fine** per tornare alla scheda **Federazione**.

Disattivare una federazione

Se non hai più bisogno di una federazione, puoi disattivarla. Ciò impedisce agli utenti associati alla federazione di accedere alla Console utilizzando le proprie credenziali aziendali. Se necessario, potrai riattivare la federazione in un secondo momento.

Disattivare una federazione prima di eliminarla, ad esempio quando si dismette l'IdP o si interrompe la federazione. Ciò consente di riattivarlo in seguito, se necessario.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare la scheda **Federazione**.
3. Seleziona il menu azioni accanto alla federazione a cui vuoi aggiungere un dominio verificato e seleziona **Disabilita**.

Elimina una federazione

Se non hai più bisogno di una federazione, puoi eliminarla. In questo modo si rimuove la federazione e si impedisce agli utenti ad essa associati di accedere alla Console utilizzando le proprie credenziali aziendali. Ad esempio, se l'IdP viene dismesso o se la federazione non è più necessaria.

Non è possibile recuperare una federazione dopo averla eliminata. Devi creare una nuova federazione.

> È necessario disattivare una federazione prima di poterla eliminare. Non è possibile ripristinare una federazione dopo averla eliminata.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazioni** per visualizzare la pagina **Federazioni**.
3. Seleziona il menu azioni ⋮ accanto alla federazione a cui vuoi aggiungere un dominio verificato e seleziona **Elimina**.

Importa la tua federazione nella NetApp Console

Se in precedenza hai configurato la federazione tramite NetApp Cloud Central (un'applicazione esterna alla NetApp Console), la pagina Federazione ti chiederà di importare la tua connessione federata esistente nella Console, in modo da poterla gestire nella nuova interfaccia. Potrai quindi sfruttare i miglioramenti più recenti senza dover ricreare la tua connessione federata.

ⓘ Dopo aver importato la federazione esistente, puoi gestirla dalla pagina **Federazioni**."Scopri di più sulla gestione delle federazioni."

Ruolo richiesto

Amministratore dell'organizzazione o amministratore della federazione."Scopri di più sui ruoli di accesso."

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare la scheda **Federazione**.
3. Selezionare **Importa federazione**.

Applica le autorizzazioni ONTAP per ONTAP Advanced View (ONTAP System Manager)

Per impostazione predefinita, le credenziali dell'agente della console consentono agli utenti di accedere alla Visualizzazione avanzata (ONTAP System Manager). In alternativa, è possibile richiedere agli utenti le credenziali ONTAP . Ciò garantisce che le autorizzazioni ONTAP di un utente vengano applicate quando lavora con cluster ONTAP sia in Cloud Volumes ONTAP che in cluster ONTAP on-premises.

ⓘ Per modificare le impostazioni dell'agente della console, è necessario disporre del ruolo di amministratore dell'organizzazione.

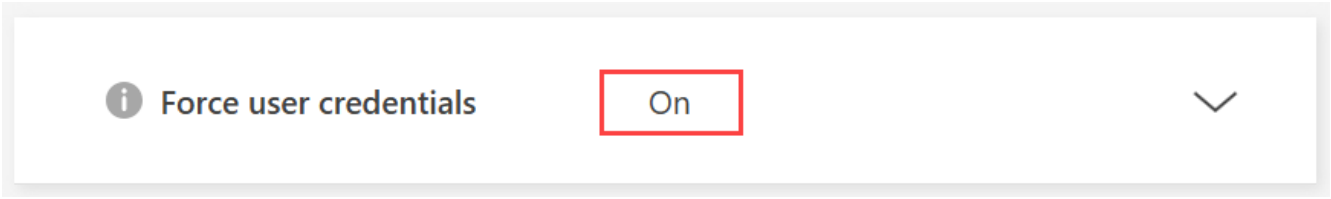
Passi

1. Selezionare **Amministrazione > Agenti**.
2. Nella pagina **Panoramica**, seleziona il menu azioni per un agente della console e seleziona **Modifica agente**.

   Per modificarlo, l'agente della console deve essere attivo.

3. Espandi l'opzione **Forza credenziali**.
4. Selezionare la casella di controllo per abilitare l'opzione **Forza credenziali**, quindi selezionare **Salva**.

5. Verificare che l'opzione **Forza credenziali** sia abilitata.



Abilita la modalità di sola lettura per un'organizzazione NetApp Console

Come misura di sicurezza, puoi abilitare la modalità di sola lettura per la tua organizzazione NetApp Console . In modalità di sola lettura, gli utenti possono visualizzare risorse e impostazioni, ma non possono apportare modifiche.

In modalità di sola lettura, gli utenti con ruoli di amministratore devono elevare manualmente le proprie autorizzazioni per apportare modifiche, il che garantisce che le modifiche siano intenzionali.

Ruoli di accesso richiesti

Super amministratore o amministratore dell'organizzazione.

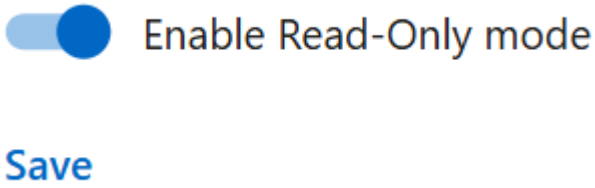
Abilita la modalità di sola lettura per l'organizzazione della tua console

Abilita la modalità di sola lettura per limitare le modifiche all'organizzazione della tua Console. Tutti gli utenti possono comunque visualizzare le risorse. Gli utenti con ruoli di amministratore non possono eseguire alcuna azione nella Console senza elevare manualmente le proprie autorizzazioni.

Quando la modalità di sola lettura è abilitata, gli utenti visualizzano un banner che li informa che l'organizzazione è in modalità di sola lettura. Gli utenti devono accedere alle Impostazioni utente per elevare il proprio ruolo.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Dalla scheda **Organizzazioni**, seleziona **Modifica impostazioni organizzazione** per l'organizzazione che desideri impostare in modalità di sola lettura.
3. Nella sezione **Modalità di sola lettura**, abilita la modalità di sola lettura spostando l'interruttore sulla posizione **On** e quindi seleziona **Salva**.



Registrati a NetApp Console come amministratore iniziale dell'organizzazione

Se la tua azienda non dispone di un'organizzazione NetApp Console , registrati per crearne una. Il primo utente è l'amministratore e gestisce gli account e le autorizzazioni. È possibile aggiornare i ruoli e aggiungere amministratori in un secondo momento.

Passi

1. Apri un browser web e vai su "NetApp Console"
2. Se disponi di un account NetApp Support Site, inserisci l'indirizzo e-mail associato al tuo account direttamente nella pagina **Accedi**.

   La Console ti registra come parte di questo accesso iniziale con le tue credenziali del sito di supporto NetApp .

3. Se vuoi registrarti creando un login alla Console, seleziona **Registrati**.
   a. Nella pagina **Iscriviti**, inserisci le informazioni richieste e seleziona **Avanti**.

      Nel modulo di registrazione sono ammessi solo caratteri inglesi.

   b. Controlla la tua casella di posta per trovare un'e-mail da NetApp che include le istruzioni per verificare il tuo indirizzo e-mail.

      Verifica il tuo indirizzo email per completare la registrazione.

4. Dopo aver effettuato l'accesso, leggere e accettare il Contratto di licenza con l'utente finale.
5. Nella pagina **Benvenuto**, crea un'organizzazione.
6. Seleziona **Iniziamo**.

+ Se sei un amministratore alle prime armi, segui la procedura guidata per aggiungere spazio di archiviazione, creare un agente della console e altro ancora. "Scopri come utilizzare l'Assistente Console."

Prossimi passi

In qualità di amministratore, dopo aver completato i passaggi inclusi in Console Assistant, dovresti pianificare la tua strategia di identità e accesso, aggiungere utenti alla tua organizzazione e assegnare ruoli. "Scopri di più sulla gestione dell'identità e degli accessi per NetApp Console"

Registrati o accedi alla NetApp Console quando esiste già un'organizzazione

Se la tua azienda ha già un'organizzazione NetApp Console , registrati o accedi per accedervi. Il metodo di registrazione o di accesso varia a seconda che la tua azienda utilizzi la federazione delle identità o disponga delle credenziali del sito di supporto NetApp . In caso contrario, creare un accesso NetApp Console .

Passi

1. Apri un browser web e vai su "NetApp Console"
2. Se disponi di un account NetApp Support Site o se la tua azienda ha configurato l'accesso singolo (SSO), inserisci l'indirizzo e-mail associato o le credenziali SSO nella pagina **Accedi**. Segui le istruzioni per completare l'accesso.

   In entrambi i casi, l'iscrizione alla Console avviene tramite questo accesso iniziale.

3. Se vuoi registrarti creando un login alla Console, seleziona **Registrati**.

a. Nella pagina **Iscriviti**, inserisci le informazioni richieste e seleziona **Avanti**.

   Nel modulo di registrazione sono ammessi solo caratteri inglesi.

b. Controlla la tua casella di posta per trovare un'e-mail da NetApp che include le istruzioni per verificare il tuo indirizzo e-mail.

   Verifica il tuo indirizzo email per completare la registrazione.

4. Dopo aver effettuato l'accesso, leggere e accettare il Contratto di licenza con l'utente finale.
5. Se il sistema ti chiede di creare un'organizzazione, chiudi la finestra di dialogo e contatta un amministratore della Console affinché possa aggiungerti all'organizzazione della Console e concederti l'accesso. "Scopri come contattare un amministratore dell'organizzazione."

Prossimi passi

Dopo aver ottenuto l'accesso alla tua organizzazione, puoi iniziare a gestire l'archiviazione e a utilizzare i servizi dati che ti sono stati assegnati.

Informazioni sul copyright

Informazioni sul marchio commerciale