Configura le integrazioni e i servizi della NetApp Console

NetApp Console local deployment

NetApp
August 10, 2026

Sommario

Configura le integrazioni e i servizi della NetApp Console . . . 1
Integra NetApp Console distribuzione locale con Active Directory . . . 1
Prima di iniziare . . . 1
Disabilita o abilita l’integrazione con Active Directory . . . 2
Elimina un’integrazione di Active Directory . . . 2
Collega il tuo LLM e abilita l’assistente della NetApp Console nella distribuzione locale di NetApp Console . . . 3
Raccogli tutto il necessario prima di connetterti a un LLM . . . 3
Connetti un LLM alla distribuzione locale della NetApp Console . . . 3
Verifica che l’integrazione con LLM funzioni . . . 4
Proteggi le credenziali e monitora l’utilizzo di LLM . . . 4
Risolvi i problemi di integrazione LLM nella distribuzione locale di NetApp Console . . . 5
Gestisci rapidamente i problemi di integrazione LLM . . . 5
Risolvi i problemi in base ai sintomi . . . 5
Rispondi alla divulgazione o all’uso improprio delle credenziali LLM . . . 6
Configura i canali di consegna delle notifiche nella distribuzione locale di NetApp Console . . . 6
Configura un server di posta elettronica . . . 6
Configura un webhook . . . 8

Configura le integrazioni e i servizi della NetApp Console

Integra NetApp Console distribuzione locale con Active Directory

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

Ruoli di accesso richiesti

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

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

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

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

Prima di iniziare

Prima di integrare Active Directory, verifica di avere:

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

Passaggi

1. Seleziona **Amministrazione > Identità e accesso**.
2. Seleziona **Directory services** per aprire la pagina Federations.
3. Seleziona **Aggiungi integrazione**.
4. Inserisci i dettagli di connessione per il tuo server Active Directory:

- Un nome descrittivo per l'integrazione.
- L'host LDAP: nome host o indirizzo IP del LDAP server. Per più server, inserisci quello principale.
- La porta: 389 per LDAP o 636 per LDAPS.
- Il **timeout di connessione** in millisecondi. Il valore predefinito è 1000 ms.

5. Seleziona **Usa SSL/TLS** per utilizzare LDAPS. Verifica che il tuo LDAP server supporti LDAPS e che la Console possa accedere ai certificati necessari.
6. Verifica la connessione. Se non riesce, controlla l'host LDAP, la porta, la connettività di rete e i certificati SSL/TLS.
7. Dopo che il test ha esito positivo, inserisci la directory e i dettagli dell'utente:
   - **Associazione DN di base**: Inserisci il Bind DN per l'account LDAP/AD che questa app userà per connettersi alla directory e inserisci la Bind credential (password) per quell'account. NetApp Console usa questi dettagli per associarsi a LDAP e convalidare la connessione.
   - **DN utente**: un account utente con l'autorizzazione a interrogare la directory. Ad esempio, `CN=ldap-reader,OU=Service Accounts,DC=example,DC=com`.
8. Seleziona **Aggiungi** per salvare l'integrazione.

Dopo aver finito

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

Disabilita o abilita l'integrazione con Active Directory

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

Passaggi

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

Elimina un'integrazione di Active Directory

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

Passaggi

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

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

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

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

Ruoli di accesso richiesti

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

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

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

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

Raccogli tutto il necessario prima di connetterti a un LLM

Prima di collegare il tuo LLM, raccogli quanto segue:

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

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

Connetti un LLM alla distribuzione locale della NetApp Console

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

Passaggi

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

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

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

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

"Risolvi i problemi di integrazione di LLM".

Verifica che l'integrazione con LLM funzioni

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

Passaggi

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

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

Proteggi le credenziali e monitora l'utilizzo di LLM

- Quando possibile, usa una chiave API dedicata per l'integrazione della distribuzione locale della Console.
- Ruota le chiavi API in base alle policy della tua organizzazione.
- Limita la possibilità di modificare le impostazioni di AI Tools solo ai ruoli amministrativi necessari.
- Monitora l'utilizzo delle API lato provider e gli avvisi per individuare attività anomale o picchi di costo.

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

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

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

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

Gestisci rapidamente i problemi di integrazione LLM

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

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

2. Verifica la disponibilità dell'assistente sulla dashboard.

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

3. Convalida il comportamento in fase di esecuzione.

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

Risolvi i problemi in base ai sintomi

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

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

Rispondi alla divulgazione o all'uso improprio delle credenziali LLM

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

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

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

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

Ruoli di accesso richiesti

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

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

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

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

Configura un server di posta elettronica

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

Passaggi

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

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

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

Aggiorna la configurazione del server di posta elettronica

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

Passaggi

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

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

Rimuovi la configurazione del server di posta elettronica

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

Passaggi

1. Seleziona **Administration > Console**.
2. Seleziona **Configuration** per aprire la pagina di configurazione dei sistemi.

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

Configura un webhook

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

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

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

Prima di iniziare

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

Passaggi

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

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

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

Informazioni sul copyright

Informazioni sul marchio commerciale