Gestisci il tuo account

Astra Control Center

NetApp
August 11, 2025

This PDF was generated from https://docs.netapp.com/it-it/astra-control-center-2304/use/manage-local-users-and-roles.html on August 11, 2025. Always check docs.netapp.com for the latest.

Sommario

Gestisci il tuo account . . . 1
- Gestire utenti e ruoli locali . . . 1
  - Utilizzare LDAP . . . 1
  - Aggiungere utenti . . . 1
  - Gestire le password . . . 2
  - Rimuovere gli utenti . . . 2
  - Gestire i ruoli . . . 3
  - Per ulteriori informazioni . . . 4
- Gestire l’autenticazione remota . . . 4
  - Aggiungere un certificato per l’autenticazione LDAPS . . . 4
  - Abilitare l’autenticazione remota . . . 5
  - Disattiva autenticazione remota . . . 5
  - Modificare le impostazioni di autenticazione remota . . . 6
  - Disconnettere l’autenticazione remota . . . 6
- Gestire utenti e gruppi remoti . . . 6
  - Aggiungere un utente remoto . . . 7
  - Aggiungere un gruppo remoto . . . 7
- Visualizzare e gestire le notifiche . . . 8
- Aggiungere e rimuovere le credenziali . . . 9
  - Aggiungere credenziali . . . 9
  - Rimuovere le credenziali . . . 9
- Monitorare l’attività dell’account . . . 9
- Aggiornare una licenza esistente . . . 10
  - Per ulteriori informazioni . . . 11

Gestisci il tuo account

Gestire utenti e ruoli locali

È possibile aggiungere, rimuovere e modificare gli utenti dell'installazione di Astra Control Center utilizzando l'interfaccia utente di Astra Control. È possibile utilizzare l'interfaccia utente di Astra Control o. "L'API Astra Control" per gestire gli utenti.

È inoltre possibile utilizzare LDAP per eseguire l'autenticazione per gli utenti selezionati.

Utilizzare LDAP

LDAP è un protocollo standard di settore per l'accesso alle informazioni di directory distribuite e una scelta popolare per l'autenticazione aziendale. È possibile collegare Astra Control Center a un server LDAP per eseguire l'autenticazione per gli utenti Astra Control selezionati. Ad alto livello, la configurazione prevede l'integrazione di Astra con LDAP e la definizione degli utenti e dei gruppi Astra Control corrispondenti alle definizioni LDAP. È possibile utilizzare l'API Astra Control o l'interfaccia utente Web per configurare l'autenticazione LDAP e gli utenti e i gruppi LDAP. Per ulteriori informazioni, consultare la seguente documentazione:

- "Utilizzare l'API Astra Control per gestire l'autenticazione remota e gli utenti"
- "Utilizzare l'interfaccia utente di Astra Control per gestire utenti e gruppi remoti"
- "Utilizzare l'interfaccia utente di Astra Control per gestire l'autenticazione remota"

Aggiungere utenti

Gli account Owner e gli amministratori possono aggiungere altri utenti all'installazione di Astra Control Center.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **utenti**.
3. Selezionare **Aggiungi utente**.
4. Immettere il nome dell'utente, l'indirizzo e-mail e una password temporanea.

   L'utente dovrà modificare la password al primo accesso.

5. Selezionare un ruolo utente con le autorizzazioni di sistema appropriate.

   Ciascun ruolo fornisce le seguenti autorizzazioni:

   - Un **Viewer** può visualizzare le risorse.
   - Un **Member** dispone delle autorizzazioni per il ruolo Viewer e può gestire app e cluster, annullare la gestione delle app ed eliminare snapshot e backup.
   - Un **Admin** dispone delle autorizzazioni di ruolo membro e può aggiungere e rimuovere qualsiasi altro utente ad eccezione del Proprietario.
   - Un **Owner** dispone delle autorizzazioni di ruolo Admin e può aggiungere e rimuovere qualsiasi account utente.

6. Per aggiungere vincoli a un utente con ruolo membro o visualizzatore, attivare la casella di controllo **limita**

ruolo ai vincoli.

Per ulteriori informazioni sull'aggiunta di vincoli, fare riferimento a. "Gestire utenti e ruoli locali".

7. Selezionare **Aggiungi**.

Gestire le password

Puoi gestire le password per gli account utente in Astra Control Center.

Modificare la password

È possibile modificare la password dell'account utente in qualsiasi momento.

Fasi

1. Selezionare l'icona User (utente) nella parte superiore destra della schermata.
2. Selezionare **Profilo**.
3. Dal menu Opzioni nella colonna **azioni** e selezionare **Modifica password**.
4. Immettere una password conforme ai requisiti.
5. Immettere nuovamente la password per confermare.
6. Selezionare **Cambia password**.

Reimpostare la password di un altro utente

Se l'account dispone delle autorizzazioni di ruolo Amministratore o Proprietario, è possibile reimpostare le password per altri account utente e per i propri. Quando si reimposta una password, si assegna una password temporanea che l'utente dovrà modificare al momento dell'accesso.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare l'elenco a discesa **azioni**.
3. Selezionare **Reset Password** (Ripristina password).
4. Immettere una password temporanea conforme ai requisiti della password.
5. Immettere nuovamente la password per confermare.

> Al successivo accesso, all'utente verrà richiesto di modificare la password.

6. Selezionare **Ripristina password**.

Rimuovere gli utenti

Gli utenti con il ruolo Owner (Proprietario) o Admin (Amministratore) possono rimuovere altri utenti dall'account in qualsiasi momento.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Nella scheda **utenti**, selezionare la casella di controllo nella riga di ciascun utente che si desidera rimuovere.

3. Dal menu Options (Opzioni) nella colonna **Actions** (azioni), selezionare **Remove user/s** (Rimuovi utenti).
4. Quando richiesto, confermare l'eliminazione digitando la parola "remove", quindi selezionare **Yes, Remove User** (Sì, Rimuovi utente).

Risultato

Astra Control Center rimuove l'utente dall'account.

Gestire i ruoli

È possibile gestire i ruoli aggiungendo vincoli dello spazio dei nomi e limitando i ruoli utente a tali vincoli. In questo modo è possibile controllare l'accesso alle risorse all'interno dell'organizzazione. È possibile utilizzare l'interfaccia utente di Astra Control o. "L'API Astra Control" per gestire i ruoli.

Aggiungere un vincolo dello spazio dei nomi a un ruolo

Un utente Admin o Owner può aggiungere vincoli di spazio dei nomi ai ruoli Member o Viewer.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **utenti**.
3. Nella colonna **azioni**, selezionare il pulsante di menu per un utente con ruolo membro o visualizzatore.
4. Selezionare **Modifica ruolo**.
5. Attivare la casella di controllo **limita ruolo ai vincoli**.

   La casella di controllo è disponibile solo per i ruoli Member o Viewer. È possibile selezionare un ruolo diverso dall'elenco a discesa **ruolo**.

6. Selezionare **Aggiungi vincolo**.

   È possibile visualizzare l'elenco dei vincoli disponibili in base allo spazio dei nomi o all'etichetta dello spazio dei nomi.

7. Nell'elenco a discesa **tipo di vincolo**, selezionare **spazio dei nomi Kubernetes** o **etichetta dello spazio dei nomi Kubernetes** a seconda della configurazione degli spazi dei nomi.
8. Selezionare uno o più spazi dei nomi o etichette dall'elenco per comporre un vincolo che limiti i ruoli a tali spazi dei nomi.
9. Selezionare **Conferma**.

   La pagina **Modifica ruolo** visualizza l'elenco dei vincoli scelti per questo ruolo.

10. Selezionare **Conferma**.

    Nella pagina **account**, è possibile visualizzare i vincoli per qualsiasi ruolo membro o visualizzatore nella colonna **ruolo**.

> Se si abilitano i vincoli per un ruolo e si seleziona **Conferma** senza aggiungere alcun vincolo, il ruolo viene considerato con restrizioni complete (al ruolo viene negato l'accesso a tutte le risorse assegnate agli spazi dei nomi).

Rimuovere un vincolo dello spazio dei nomi da un ruolo

Un utente Admin o Owner può rimuovere un vincolo dello spazio dei nomi da un ruolo.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **utenti**.
3. Nella colonna **azioni**, selezionare il pulsante di menu per un utente con ruolo membro o visualizzatore con vincoli attivi.
4. Selezionare **Modifica ruolo**.

   La finestra di dialogo **Modifica ruolo** visualizza i vincoli attivi per il ruolo.
5. Selezionare la **X** a destra del vincolo da rimuovere.
6. Selezionare **Conferma**.

Per ulteriori informazioni

- "Ruoli e spazi dei nomi degli utenti"

Gestire l'autenticazione remota

LDAP è un protocollo standard di settore per l'accesso alle informazioni di directory distribuite e una scelta popolare per l'autenticazione aziendale. È possibile collegare Astra Control Center a un server LDAP per eseguire l'autenticazione per gli utenti Astra Control selezionati.

Ad alto livello, la configurazione prevede l'integrazione di Astra con LDAP e la definizione degli utenti e dei gruppi Astra Control corrispondenti alle definizioni LDAP. È possibile utilizzare l'API Astra Control o l'interfaccia utente Web per configurare l'autenticazione LDAP e gli utenti e i gruppi LDAP.

> Astra Control Center utilizza l'indirizzo e-mail nell'attributo "mail" LDAP per cercare e tenere traccia degli utenti remoti. Questo attributo potrebbe essere un campo facoltativo o vuoto nella directory. In questo campo deve esistere un indirizzo e-mail per tutti gli utenti remoti che si desidera visualizzare in Astra Control Center. Questo indirizzo e-mail viene utilizzato come nome utente in Astra Control Center per l'autenticazione.

Aggiungere un certificato per l'autenticazione LDAPS

Aggiungere il certificato TLS privato per il server LDAP in modo che Astra Control Center possa autenticarsi con il server LDAP quando si utilizza una connessione LDAPS. Questa operazione deve essere eseguita una sola volta o alla scadenza del certificato installato.

Fasi

1. Vai a **account**.
2. Selezionare la scheda **certificati**.
3. Selezionare **Aggiungi**.
4. Caricare il `.pem` archiviare o incollare il contenuto del file dagli appunti.

5. Selezionare la casella di controllo **attendibile**.
6. Selezionare **Aggiungi certificato**.

Abilitare l'autenticazione remota

È possibile attivare l'autenticazione LDAP e configurare la connessione tra Astra Control e il server LDAP remoto.

Prima di iniziare

Se si intende utilizzare LDAPS, assicurarsi che il certificato TLS privato per il server LDAP sia installato in Astra Control Center in modo che Astra Control Center possa autenticarsi con il server LDAP. Vedere Aggiungere un certificato per l'autenticazione LDAPS per istruzioni.

Fasi

1. Accedere a **account > connessioni**.
2. Nel riquadro **Remote Authentication**, selezionare il menu di configurazione.
3. Selezionare **Connect**.
4. Inserire l'indirizzo IP del server, la porta e il protocollo di connessione preferito (LDAP o LDAPS).

> Come Best practice, utilizzare LDAPS per la connessione con il server LDAP. È necessario installare il certificato TLS privato del server LDAP in Astra Control Center prima di connettersi a LDAPS.

5. Inserire le credenziali dell'account di servizio nel formato e-mail (administrator@example.com). Astra Control utilizza queste credenziali per la connessione con il server LDAP.
6. Nella sezione **User Match** (corrispondenza utente), immettere il DN di base e un filtro di ricerca utente appropriato da utilizzare per il recupero delle informazioni utente dal server LDAP.
7. Nella sezione **corrispondenza gruppo**, immettere il DN della base di ricerca gruppo e un filtro di ricerca gruppo personalizzato appropriato.

> Assicurarsi di utilizzare il nome distinto (DN) di base corretto e un filtro di ricerca appropriato per **corrispondenza utente** e **corrispondenza gruppo**. Il DN di base indica ad Astra Control a quale livello della struttura di directory avviare la ricerca e il filtro di ricerca limita le parti della struttura di directory da cui Astra Control esegue la ricerca.

8. Selezionare **Invia**.

Risultato

Lo stato del riquadro **Remote Authentication** (autenticazione remota) passa a **Pending** (in sospeso), quindi a **Connected** (connesso) quando viene stabilita la connessione al server LDAP.

Disattiva autenticazione remota

È possibile disattivare temporaneamente una connessione attiva al server LDAP.

> Quando si disattiva una connessione a un server LDAP, vengono salvate tutte le impostazioni e vengono conservati tutti gli utenti e i gruppi remoti aggiunti ad Astra Control da tale server LDAP. È possibile riconnettersi a questo server LDAP in qualsiasi momento.

Fasi

1. Accedere a **account > connessioni**.
2. Nel riquadro **Remote Authentication**, selezionare il menu di configurazione.
3. Selezionare **Disable** (Disattiva).

Risultato

Lo stato del riquadro **Remote Authentication** passa a **Disabled**. Tutte le impostazioni di autenticazione remota, gli utenti remoti e i gruppi remoti vengono preservati e la connessione può essere riattivata in qualsiasi momento.

Modificare le impostazioni di autenticazione remota

Se la connessione al server LDAP è stata disattivata o il pannello **Remote Authentication** è in stato "Connection error" (errore di connessione), è possibile modificare le impostazioni di configurazione.

> Non è possibile modificare l'URL o l'indirizzo IP del server LDAP quando il pannello **Remote Authentication** (autenticazione remota) è in stato "Disabled" (Disattivato). È necessario Disconnettere l'autenticazione remota prima di tutto.

Fasi

1. Accedere a **account > connessioni**.
2. Nel riquadro **Remote Authentication**, selezionare il menu di configurazione.
3. Selezionare **Modifica**.
4. Apportare le modifiche necessarie e selezionare **Modifica**.

Disconnettere l'autenticazione remota

È possibile disconnettersi da un server LDAP e rimuovere le impostazioni di configurazione da Astra Control.

> Quando ci si disconnette dal server LDAP, tutte le impostazioni di configurazione per quel server LDAP vengono rimosse da Astra Control, così come tutti gli utenti e i gruppi remoti che sono stati aggiunti da quel server LDAP.

Fasi

1. Accedere a **account > connessioni**.
2. Nel riquadro **Remote Authentication**, selezionare il menu di configurazione.
3. Selezionare **Disconnect**.

Risultato

Lo stato del riquadro **Remote Authentication** (autenticazione remota) passa a **Disconnected** (disconnesso). Le impostazioni di autenticazione remota, gli utenti remoti e i gruppi remoti vengono rimossi da Astra Control.

Gestire utenti e gruppi remoti

Se è stata attivata l'autenticazione LDAP sul sistema Astra Control, è possibile cercare utenti e gruppi LDAP e includerli negli utenti approvati del sistema.

Aggiungere un utente remoto

Gli account Owner e gli amministratori possono aggiungere utenti remoti ad Astra Control.

> Non è possibile aggiungere un utente remoto se nel sistema esiste già un utente locale con lo stesso indirizzo e-mail. Per aggiungere l'utente come utente remoto, eliminare prima l'utente locale dal sistema.

> Astra Control Center utilizza l'indirizzo e-mail nell'attributo "mail" LDAP per cercare e tenere traccia degli utenti remoti. Questo attributo potrebbe essere un campo facoltativo o vuoto nella directory. In questo campo deve esistere un indirizzo e-mail per tutti gli utenti remoti che si desidera visualizzare in Astra Control Center. Questo indirizzo e-mail viene utilizzato come nome utente in Astra Control Center per l'autenticazione.

Fasi

1. Accedere all'area **account**.
2. Selezionare la scheda **utenti e gruppi**.
3. All'estrema destra della pagina, selezionare **utenti remoti**.
4. Selezionare **Aggiungi**.
5. In alternativa, cercare un utente LDAP inserendo l'indirizzo e-mail dell'utente nel campo **Filtra per email**.
6. Selezionare uno o più utenti dall'elenco.
7. Assegnare un ruolo all'utente.

   > Se si assegnano ruoli diversi a un utente e al gruppo dell'utente, il ruolo più permissivo ha la precedenza.

8. Facoltativamente, assegnare uno o più vincoli dello spazio dei nomi a questo utente e selezionare **limita ruolo ai vincoli** per applicarli. È possibile aggiungere un nuovo vincolo dello spazio dei nomi selezionando **Aggiungi vincolo**.

   > Quando a un utente vengono assegnati ruoli multipli tramite l'appartenenza al gruppo LDAP, i limiti nel ruolo più permissivo sono gli unici che hanno effetto. Ad esempio, se un utente con un ruolo Viewer locale unisce tre gruppi associati al ruolo Member, la somma dei vincoli dei ruoli Member ha effetto e tutti i vincoli del ruolo Viewer vengono ignorati.

9. Selezionare **Aggiungi**.

Risultato

Il nuovo utente viene visualizzato nell'elenco degli utenti remoti. In questo elenco, è possibile visualizzare i vincoli attivi sull'utente e gestire l'utente dal menu **azioni**.

Aggiungere un gruppo remoto

Per aggiungere più utenti remoti contemporaneamente, gli account Owners e gli amministratori possono aggiungere gruppi remoti ad Astra Control. Quando si aggiunge un gruppo remoto, tutti gli utenti remoti di tale gruppo vengono aggiunti ad Astra Control e ereditano lo stesso ruolo.

Fasi

1. Accedere all'area **account**.

2. Selezionare la scheda **utenti e gruppi**.
3. All'estrema destra della pagina, selezionare **gruppi remoti**.
4. Selezionare **Aggiungi**.

   In questa finestra, è possibile visualizzare un elenco dei nomi comuni e dei nomi distinti dei gruppi LDAP recuperati da Astra Control.

5. In alternativa, cercare un gruppo LDAP inserendo il nome comune del gruppo nel campo **Filtra per nome comune**.
6. Selezionare uno o più gruppi dall'elenco.
7. Assegnare un ruolo ai gruppi.

   Il ruolo selezionato viene assegnato a tutti gli utenti di questo gruppo. Se si assegnano ruoli diversi a un utente e al gruppo dell'utente, il ruolo più permissivo ha la precedenza.

8. Facoltativamente, assegnare uno o più vincoli dello spazio dei nomi a questo gruppo e selezionare **limita ruolo ai vincoli** per applicarli. È possibile aggiungere un nuovo vincolo dello spazio dei nomi selezionando **Aggiungi vincolo**.

   Quando a un utente vengono assegnati ruoli multipli tramite l'appartenenza al gruppo LDAP, i limiti nel ruolo più permissivo sono gli unici che hanno effetto. Ad esempio, se un utente con un ruolo Viewer locale unisce tre gruppi associati al ruolo Member, la somma dei vincoli dei ruoli Member ha effetto e tutti i vincoli del ruolo Viewer vengono ignorati.

9. Selezionare **Aggiungi**.

Risultato

Il nuovo gruppo viene visualizzato nell'elenco dei gruppi remoti e tutti gli utenti remoti di questo gruppo vengono visualizzati nell'elenco degli utenti remoti. In questo elenco, è possibile visualizzare i dettagli sul gruppo e gestire il gruppo dal menu **azioni**.

Visualizzare e gestire le notifiche

Astra informa l'utente quando le azioni sono state completate o non sono riuscite. Ad esempio, se il backup di un'applicazione è stato completato correttamente, viene visualizzata una notifica.

È possibile gestire queste notifiche dall'alto a destra dell'interfaccia:

Fasi

1. Selezionare il numero di notifiche non lette in alto a destra.
2. Esaminare le notifiche, quindi selezionare **Contrassegna come letto** o **Mostra tutte le notifiche**.

   Se si seleziona **Mostra tutte le notifiche**, viene caricata la pagina Notifiche.

3. Nella pagina **Notifiche**, visualizzare le notifiche, selezionare quelle che si desidera contrassegnare come lette, selezionare **azione** e selezionare **Contrassegna come letta**.

Aggiungere e rimuovere le credenziali

Aggiungi e rimuovi le credenziali per i provider di cloud privato locali, come ONTAP S3, i cluster Kubernetes gestiti con OpenShift o i cluster Kubernetes non gestiti dal tuo account in qualsiasi momento. Astra Control Center utilizza queste credenziali per scoprire i cluster Kubernetes e le applicazioni sui cluster e per eseguire il provisioning delle risorse per conto dell'utente.

Tutti gli utenti di Astra Control Center condividono gli stessi set di credenziali.

Aggiungere credenziali

È possibile aggiungere credenziali ad Astra Control Center quando si gestiscono i cluster. Per aggiungere credenziali aggiungendo un nuovo cluster, fare riferimento a. "Aggiungere un cluster Kubernetes".

> Se crei il tuo `kubeconfig` file, è necessario definire solo **un** elemento di contesto al suo interno. Vedere "Documentazione Kubernetes" per informazioni sulla creazione `kubeconfig` file.

Rimuovere le credenziali

Rimuovere le credenziali da un account in qualsiasi momento. Rimuovere le credenziali solo dopo "annullamento della gestione di tutti i cluster associati".

> Il primo set di credenziali aggiunto ad Astra Control Center è sempre in uso perché Astra Control Center utilizza le credenziali per l'autenticazione nel bucket di backup. Si consiglia di non rimuovere queste credenziali.

Fasi

1. Selezionare **account**.
2. Selezionare la scheda **credenziali**.
3. Selezionare il menu Opzioni nella colonna **Stato** per le credenziali che si desidera rimuovere.
4. Selezionare **Rimuovi**.
5. Digitare la parola "remove" per confermare l'eliminazione, quindi selezionare **Sì, Rimuovi credenziale**.

Risultato

Astra Control Center rimuove le credenziali dall'account.

Monitorare l'attività dell'account

Puoi visualizzare i dettagli delle attività nel tuo account Astra Control. Ad esempio, quando sono stati invitati nuovi utenti, quando è stato aggiunto un cluster o quando è stata acquisita una snapshot. È inoltre possibile esportare l'attività dell'account in un file CSV.

Se gestisci i cluster Kubernetes da Astra Control e Astra Control è connesso a Cloud Insights, Astra Control invia i registri degli eventi a Cloud Insights. Le informazioni di log, incluse le informazioni sull'implementazione del pod e sugli allegati PVC, vengono visualizzate nel registro delle attività di controllo Astra. Utilizza queste informazioni per identificare eventuali problemi sui cluster Kubernetes che stai gestendo.

Visualizza tutte le attività dell'account in Astra Control

1. Selezionare **Activity** (attività).
2. Utilizza i filtri per restringere l'elenco delle attività o utilizza la casella di ricerca per trovare esattamente ciò che stai cercando.
3. Selezionare **Export to CSV** (Esporta in CSV) per scaricare l'attività dell'account in un file CSV.

Visualizzare l'attività dell'account per un'applicazione specifica

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Activity** (attività).

Visualizzare l'attività dell'account per i cluster

1. Selezionare **Clusters**, quindi il nome del cluster.
2. Selezionare **Activity** (attività).

Intraprendere azioni per risolvere gli eventi che richiedono attenzione

1. Selezionare **Activity** (attività).
2. Selezionare un evento che richiede attenzione.
3. Selezionare l'opzione a discesa **take action**.

   Da questo elenco è possibile visualizzare le possibili azioni correttive da intraprendere, visualizzare la documentazione relativa al problema e ottenere supporto per risolvere il problema.

Aggiornare una licenza esistente

È possibile convertire una licenza di valutazione in una licenza completa oppure aggiornare una licenza di valutazione o una licenza completa esistente con una nuova licenza. Se non si dispone di una licenza completa, rivolgersi al contatto commerciale NetApp per ottenere una licenza completa e un numero di serie. È possibile utilizzare l'interfaccia utente di Astra Control Center o. "L'API Astra Control" per aggiornare una licenza esistente.

Fasi

1. Accedere a. "Sito di supporto NetApp".
2. Accedere alla pagina di download di Astra Control Center, inserire il numero di serie e scaricare il file di licenza NetApp completo (NLF).
3. Accedere all'interfaccia utente di Astra Control Center.
4. Dalla barra di navigazione a sinistra, selezionare **account** > **licenza**.
5. Nella pagina **account** > **licenza**, selezionare il menu a discesa dello stato della licenza esistente e selezionare **Sostituisci**.

6. Individuare il file di licenza scaricato.
7. Selezionare **Aggiungi**.

La pagina **account** > **licenze** visualizza le informazioni sulla licenza, la data di scadenza, il numero di serie della licenza, l'ID account e le unità CPU utilizzate.

Per ulteriori informazioni

- "Licenza Astra Control Center"

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.