Konto verwalten

Astra Control Center

NetApp
November 27, 2023

Inhalt

Konto verwalten

Managen Sie lokale Benutzer und Rollen

Sie können Benutzer Ihrer Astra Control Center-Installation über die Astra Control-Benutzeroberfläche hinzufügen, entfernen und bearbeiten. Sie können die Astra Control UI oder verwenden "Astra Control API" Um Benutzer zu managen.

Sie können LDAP auch zur Authentifizierung für ausgewählte Benutzer verwenden.

LDAP verwenden

LDAP ist ein branchenübliches Protokoll für den Zugriff auf verteilte Verzeichnisinformationen und eine beliebte Wahl für die Unternehmensauthentifizierung. Sie können Astra Control Center mit einem LDAP-Server verbinden, um die Authentifizierung für ausgewählte Astra Control-Benutzer durchzuführen. Auf hohem Niveau beinhaltet die Konfiguration die Integration von Astra mit LDAP und die Definition der Astra Control Benutzer und Gruppen entsprechend der LDAP-Definitionen. Sie können die Astra Control API oder die Web-Benutzeroberfläche verwenden, um die LDAP-Authentifizierung und LDAP-Benutzer und -Gruppen zu konfigurieren. Weitere Informationen finden Sie in der folgenden Dokumentation:

- "Mit der Astra Control API können Sie die Remote-Authentifizierung und -Benutzer verwalten"
- "Verwenden Sie die Astra Control-Benutzeroberfläche, um Remote-Benutzer und -Gruppen zu verwalten"
- "Verwenden Sie die Astra Control-Benutzeroberfläche, um die Remote-Authentifizierung zu verwalten"

Benutzer hinzufügen

Kontoinhaber und -Administratoren können weitere Benutzer zur Installation des Astra Control Center hinzufügen.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Wählen Sie die Registerkarte **Benutzer** aus.
3. Wählen Sie **Benutzer Hinzufügen**.
4. Geben Sie den Namen des Benutzers, die E-Mail-Adresse und ein temporäres Kennwort ein.

   Der Benutzer muss das Passwort bei der ersten Anmeldung ändern.

5. Wählen Sie eine Benutzerrolle mit den entsprechenden Systemberechtigungen aus.

   Jede Rolle bietet die folgenden Berechtigungen:

   - Ein **Viewer** kann Ressourcen anzeigen.
   - Ein **Mitglied** verfügt über Berechtigungen für Viewer-Rollen und kann Apps und Cluster verwalten, Apps verwalten und Snapshots und Backups löschen.
   - Ein **Admin** verfügt über Berechtigungen für die Mitgliederrolle und kann alle anderen Benutzer außer dem Eigentümer hinzufügen und entfernen.
   - Ein **Owner** hat Administratorrechte und kann beliebige Benutzerkonten hinzufügen und entfernen.
6. Um einem Benutzer mit einer Mitglied- oder Viewer-Rolle Einschränkungen hinzuzufügen, aktivieren Sie

das Kontrollkästchen * Rolle auf Einschränkungen beschränken*.

Weitere Informationen zum Hinzufügen von Einschränkungen finden Sie unter "Managen Sie lokale Benutzer und Rollen".

7. Wählen Sie **Hinzufügen**.

Passwörter verwalten

Sie können Passwörter für Benutzerkonten im Astra Control Center verwalten.

Passwort ändern

Sie können das Passwort Ihres Benutzerkontos jederzeit ändern.

Schritte

1. Klicken Sie oben rechts auf dem Bildschirm auf das Symbol Benutzer.
2. Wählen Sie **Profil**.
3. Wählen Sie im Menü Optionen in der Spalte **Aktionen** die Option **Passwort ändern** aus.
4. Geben Sie ein Passwort ein, das den Anforderungen des Passworts entspricht.
5. Geben Sie das Kennwort zur Bestätigung erneut ein.
6. Wählen Sie **Passwort ändern**.

Kennwort eines anderen Benutzers zurücksetzen

Wenn Ihr Konto über Berechtigungen für die Administrator- oder Eigentümerrolle verfügt, können Sie Passwörter für andere Benutzerkonten sowie für Ihre eigenen zurücksetzen. Wenn Sie ein Kennwort zurücksetzen, weisen Sie ein temporäres Kennwort zu, das der Benutzer bei der Anmeldung ändern muss.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Wählen Sie die Dropdown-Liste **Aktionen** aus.
3. Wählen Sie **Passwort Zurücksetzen**.
4. Geben Sie ein temporäres Kennwort ein, das den Anforderungen des Passworts entspricht.
5. Geben Sie das Kennwort zur Bestätigung erneut ein.

> Wenn sich der Benutzer beim nächsten Mal anmeldet, wird er aufgefordert, das Passwort zu ändern.

6. Wählen Sie **Passwort zurücksetzen**.

Benutzer entfernen

Benutzer mit der Eigentümer- oder Administratorrolle können jederzeit andere Benutzer aus dem Konto entfernen.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.

2. Aktivieren Sie auf der Registerkarte **Benutzer** das Kontrollkästchen in der Zeile jedes Benutzers, den Sie entfernen möchten.
3. Wählen Sie im Menü Optionen in der Spalte **Aktionen** die Option **Benutzer/s entfernen** aus.
4. Wenn Sie aufgefordert werden, bestätigen Sie den Löschvorgang, indem Sie das Wort "Entfernen" eingeben und dann **Ja, Benutzer entfernen** wählen.

Ergebnis

Astra Control Center entfernt den Benutzer aus dem Konto.

Rollen managen

Sie können Rollen managen, indem Sie Namespace-Einschränkungen hinzufügen und Benutzerrollen auf diese Einschränkungen beschränken. So können Sie den Zugriff auf Ressourcen in Ihrem Unternehmen kontrollieren. Sie können die Astra Control UI oder verwenden "Astra Control API" Rollen managen.

Fügen Sie einer Rolle eine Namespace-Einschränkung hinzu

Ein Administrator oder Benutzer des Eigentümers kann den Mitglied- oder Viewer-Rollen Namespace-Einschränkungen hinzufügen.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Wählen Sie die Registerkarte **Benutzer** aus.
3. Wählen Sie in der Spalte **Actions** die Menü-Schaltfläche für einen Benutzer mit der Rolle Mitglied oder Viewer.
4. Wählen Sie **Rolle bearbeiten**.
5. Aktivieren Sie das Kontrollkästchen * Rolle auf Einschränkungen beschränken*.

   Das Kontrollkästchen ist nur für Mitglieder- oder Viewer-Rollen verfügbar. Aus der Dropdown-Liste **Rolle** können Sie eine andere Rolle auswählen.

6. Wählen Sie **Bedingung hinzufügen**.

   Sie können die Liste der verfügbaren Einschränkungen nach Namespace oder Namensraum-Bezeichnung anzeigen.

7. Wählen Sie in der Dropdown-Liste **Constraint type** je nach Konfiguration Ihrer Namespaces entweder **Kubernetes Namespace** oder **Kubernetes Namespace Label** aus.
8. Wählen Sie eine oder mehrere Namespaces oder Labels aus der Liste aus, um eine Beschränkung zu erstellen, die Rollen auf diese Namespaces beschränkt.
9. Wählen Sie **Bestätigen**.

   Auf der Seite * Rolle bearbeiten* wird die Liste der für diese Rolle ausgewählten Einschränkungen angezeigt.

10. Wählen Sie **Bestätigen**.

    Auf der Seite **Konto** können Sie die Einschränkungen für beliebige Mitglieder- oder Viewer-Rollen in der Spalte **Role** anzeigen.

Wenn Sie Einschränkungen für eine Rolle aktivieren und **Bestätigen** wählen, ohne dass Einschränkungen hinzugefügt werden müssen, gilt die Rolle als uneingeschränkt eingeschränkt (die Rolle wird dem Zugriff auf alle Ressourcen verweigert, die Namespaces zugewiesen sind).

Entfernen Sie eine Namespace-Beschränkung aus einer Rolle

Ein Administrator oder Benutzer eines Eigentümers kann eine Namespace-Einschränkung aus einer Rolle entfernen.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Wählen Sie die Registerkarte **Benutzer** aus.
3. Wählen Sie in der Spalte **Aktionen** die Menütaste für einen Benutzer mit der Rolle Mitglied oder Viewer mit aktiven Einschränkungen.
4. Wählen Sie **Rolle bearbeiten**.

   Im Dialogfeld **Rolle bearbeiten** werden die aktiven Einschränkungen für die Rolle angezeigt.
5. Wählen Sie das **X** rechts neben der Bedingung aus, die Sie entfernen müssen.
6. Wählen Sie **Bestätigen**.

Finden Sie weitere Informationen

- "Benutzerrollen und Namespaces"

Managen Sie die Remote-Authentifizierung

LDAP ist ein branchenübliches Protokoll für den Zugriff auf verteilte Verzeichnisinformationen und eine beliebte Wahl für die Unternehmensauthentifizierung. Sie können Astra Control Center mit einem LDAP-Server verbinden, um die Authentifizierung für ausgewählte Astra Control-Benutzer durchzuführen.

Auf hohem Niveau beinhaltet die Konfiguration die Integration von Astra mit LDAP und die Definition der Astra Control Benutzer und Gruppen entsprechend der LDAP-Definitionen. Sie können die Astra Control API oder die Web-Benutzeroberfläche verwenden, um die LDAP-Authentifizierung und LDAP-Benutzer und -Gruppen zu konfigurieren.

Astra Control Center verwendet das bei aktivierter Remote-Authentifizierung konfigurierte Attribut für die Benutzeranmeldung, um Remote-Benutzer zu suchen und zu verfolgen. Für jeden Remote-Benutzer, den Sie im Astra Control Center anzeigen möchten, muss in diesem Feld ein Attribut einer E-Mail-Adresse („Mail“) oder eines Hauptnamens des Benutzers („userPrincipalName“) vorhanden sein. Dieses Attribut wird als Benutzername in Astra Control Center für die Authentifizierung und bei der Suche nach Remote-Benutzern verwendet.

Fügen Sie ein Zertifikat für die LDAPS-Authentifizierung hinzu

Fügen Sie das private TLS-Zertifikat für den LDAP-Server hinzu, damit sich Astra Control Center bei Verwendung einer LDAPS-Verbindung mit dem LDAP-Server authentifizieren kann. Sie müssen dies nur einmal tun, oder wenn das Zertifikat, das Sie installiert haben, abläuft.

Schritte

1. Gehen Sie zu **Konto**.
2. Wählen Sie die Registerkarte **Zertifikate** aus.
3. Wählen Sie **Hinzufügen**.
4. Laden Sie entweder die hoch `.pem` Datei oder fügen Sie den Inhalt der Datei aus der Zwischenablage ein.
5. Aktivieren Sie das Kontrollkästchen * Trusted*.
6. Wählen Sie **Zertifikat hinzufügen**.

Aktivieren Sie die Remote-Authentifizierung

Sie können die LDAP-Authentifizierung aktivieren und die Verbindung zwischen Astra Control und dem Remote LDAP-Server konfigurieren.

Bevor Sie beginnen

Wenn Sie LDAPS verwenden möchten, stellen Sie sicher, dass das private TLS-Zertifikat für den LDAP-Server im Astra Control Center installiert ist, damit sich Astra Control Center mit dem LDAP-Server authentifizieren kann. Siehe Fügen Sie ein Zertifikat für die LDAPS-Authentifizierung hinzu Weitere Anweisungen.

Schritte

1. Gehen Sie zu **Konto > Verbindungen**.
2. Wählen Sie im Fenster **Remote Authentication** das Konfigurationsmenü aus.
3. Wählen Sie **Verbinden**.
4. Geben Sie die IP-Adresse, den Port und das bevorzugte Verbindungsprotokoll (LDAP oder LDAPS) des Servers ein.

   Verwenden Sie als Best Practice LDAPS, wenn Sie eine Verbindung zum LDAP-Server herstellen. Vor der Verbindung mit LDAPS müssen Sie das private TLS-Zertifikat des LDAP-Servers in Astra Control Center installieren.

5. Geben Sie die Anmeldeinformationen für das Servicekonto im E-Mail-Format ein (administrator@example.com). Astra Control verwendet diese Anmeldeinformationen, wenn Sie eine Verbindung mit dem LDAP-Server herstellen.
6. Gehen Sie im Abschnitt **User Match** wie folgt vor:
   a. Geben Sie den Basis-DN und einen entsprechenden Benutzersuchfilter ein, der beim Abrufen von Benutzerinformationen vom LDAP-Server verwendet werden soll.
   b. (Optional) Wenn Ihr Verzeichnis das Benutzeranmeldungsattribut verwendet `userPrincipalName` Statt `mail`, Geben Sie ein `userPrincipalName` Geben Sie im Feld **User Login Attribut** das richtige Attribut ein.
7. Geben Sie im Abschnitt **Gruppenvergleich** den Gruppen-Suchsockel-DN und einen entsprechenden benutzerdefinierten Gruppensuchfilter ein.

   Verwenden Sie unbedingt den richtigen Basisnamen (DN) und einen entsprechenden Suchfilter für **User Match** und **Group Match**. Der Basis-DN teilt Astra Control mit, auf welcher Ebene der Verzeichnisstruktur die Suche gestartet werden soll, und der Suchfilter begrenzt die Teile des Verzeichnisbaums Astra Control Suchanfragen.

8. Wählen Sie **Senden**.

Ergebnis

Der Fensterstatus **Remote-Authentifizierung** wechselt zu **Ausstehend** und dann zu **verbunden**, wenn die Verbindung zum LDAP-Server hergestellt wird.

Deaktivieren Sie die Remote-Authentifizierung

Sie können eine aktive Verbindung zum LDAP-Server vorübergehend deaktivieren.

> Wenn Sie eine Verbindung zu einem LDAP-Server deaktivieren, werden alle Einstellungen gespeichert und alle Remote-Benutzer und -Gruppen, die von diesem LDAP-Server zu Astra Control hinzugefügt wurden, bleiben erhalten. Sie können jederzeit eine Verbindung zu diesem LDAP-Server herstellen.

Schritte

1. Gehen Sie zu **Konto > Verbindungen**.
2. Wählen Sie im Fenster **Remote Authentication** das Konfigurationsmenü aus.
3. Wählen Sie **Deaktivieren**.

Ergebnis

Der Status des Fensterbereichs **Remote Authentication** wechselt zu **deaktivierte**. Alle Einstellungen für die Remote-Authentifizierung, Remote-Benutzer und Remote-Gruppen bleiben erhalten, und Sie können die Verbindung jederzeit wieder aktivieren.

Remote-Authentifizierungseinstellungen bearbeiten

Wenn Sie die Verbindung zum LDAP-Server deaktiviert haben oder sich der Fensterbereich **Remote Authentication** im Status „Verbindungsfehler“ befindet, können Sie die Konfigurationseinstellungen bearbeiten.

> Sie können die URL oder IP-Adresse des LDAP-Servers nicht bearbeiten, wenn sich der Bereich **Remote Authentication** im Status „deaktiviert“ befindet. Sie müssen Trennen Sie die Remote-Authentifizierung Zunächst.

Schritte

1. Gehen Sie zu **Konto > Verbindungen**.
2. Wählen Sie im Fenster **Remote Authentication** das Konfigurationsmenü aus.
3. Wählen Sie **Bearbeiten**.
4. Nehmen Sie die erforderlichen Änderungen vor, und wählen Sie **Bearbeiten**.

Trennen Sie die Remote-Authentifizierung

Sie können die Verbindung zu einem LDAP-Server trennen und die Konfigurationseinstellungen von Astra Control entfernen.

Wenn Sie ein LDAP-Benutzer sind und die Verbindung trennen, wird Ihre Sitzung sofort beendet Wenn Sie die Verbindung zum LDAP-Server trennen, werden alle Konfigurationseinstellungen für diesen LDAP-Server aus Astra Control sowie alle Remote-Benutzer und -Gruppen entfernt, die diesem LDAP-Server hinzugefügt wurden.

Schritte

1. Gehen Sie zu **Konto > Verbindungen**.
2. Wählen Sie im Fenster **Remote Authentication** das Konfigurationsmenü aus.
3. Wählen Sie **Trennen**.

Ergebnis

Der Status des Fensterbereichs **Remote Authentication** wechselt zu **nicht verbunden**. Remote-Authentifizierungseinstellungen, Remote-Benutzer und Remote-Gruppen werden aus Astra Control entfernt.

Verwalten von Remote-Benutzern und -Gruppen

Wenn Sie die LDAP-Authentifizierung auf Ihrem Astra Control System aktiviert haben, können Sie nach LDAP-Benutzern und -Gruppen suchen und diese in die genehmigten Benutzer des Systems aufnehmen.

Fügen Sie einen Remote-Benutzer hinzu

Kontoinhaber und -Administratoren können Remote-Benutzer zu Astra Control hinzufügen. Astra Control Center unterstützt bis zu 10,000 LDAP Remote-Benutzer.

Astra Control Center verwendet das bei aktivierter Remote-Authentifizierung konfigurierte Attribut für die Benutzeranmeldung, um Remote-Benutzer zu suchen und zu verfolgen. Für jeden Remote-Benutzer, den Sie im Astra Control Center anzeigen möchten, muss in diesem Feld ein Attribut einer E-Mail-Adresse („Mail“) oder eines Hauptnamens des Benutzers („userPrincipalName“) vorhanden sein. Dieses Attribut wird als Benutzername in Astra Control Center für die Authentifizierung und bei der Suche nach Remote-Benutzern verwendet.

Sie können keinen Remote-Benutzer hinzufügen, wenn bereits ein lokaler Benutzer mit derselben E-Mail-Adresse (basierend auf dem Attribut „Mail“ oder „user principal Name“) auf dem System vorhanden ist. Um den Benutzer als Remote-Benutzer hinzuzufügen, löschen Sie zuerst den lokalen Benutzer aus dem System.

Schritte

1. Gehen Sie zum Bereich **Konto**.
2. Wählen Sie die Registerkarte **Benutzer & Gruppen** aus.
3. Wählen Sie rechts auf der Seite die Option **Remote Users**.
4. Wählen Sie **Hinzufügen**.
5. Sie können auch nach einem LDAP-Benutzer suchen, indem Sie die E-Mail-Adresse des Benutzers im Feld **Filtern nach E-Mail** eingeben.
6. Wählen Sie einen oder mehrere Benutzer aus der Liste aus.
7. Weisen Sie dem Benutzer eine Rolle zu.

Wenn Sie einem Benutzer und der Gruppe des Benutzers verschiedene Rollen zuweisen, hat die Rolle eine größere Priorität.

8. Weisen Sie diesem Benutzer optional eine oder mehrere Namespace-Einschränkungen zu und wählen Sie **Rolle auf Einschränkungen beschränken** aus, um sie durchzusetzen. Sie können eine neue Namespace-Einschränkung hinzufügen, indem Sie **Bedingung hinzufügen** auswählen.

Wenn einem Benutzer mehrere Rollen durch die LDAP-Gruppenmitgliedschaft zugewiesen werden, sind die Einschränkungen in der am stärksten permissivsten Rolle die einzigen, die wirksam werden. Wenn z. B. ein Benutzer mit einer lokalen Viewer-Rolle drei Gruppen verbindet, die an die Rolle Mitglied gebunden sind, wird die Summe der Einschränkungen aus den Mitgliederrollen wirksam, und alle Einschränkungen aus der Viewer-Rolle werden ignoriert.

9. Wählen Sie **Hinzufügen**.

Ergebnis

Der neue Benutzer wird in der Liste der Remote-Benutzer angezeigt. In dieser Liste können Sie aktive Einschränkungen für den Benutzer sehen und den Benutzer über das Menü **Aktionen** verwalten.

Fügen Sie eine externe Gruppe hinzu

Wenn Sie viele Remote-Benutzer gleichzeitig hinzufügen möchten, können Kontoinhaber und -Administratoren Remote-Gruppen zu Astra Control hinzufügen. Wenn Sie eine Remote-Gruppe hinzufügen, können sich alle Remote-Benutzer in dieser Gruppe bei Astra Control anmelden und übernehmen die gleiche Rolle wie die Gruppe.

Astra Control Center unterstützt bis zu 5,000 LDAP-Remote-Gruppen.

Schritte

1. Gehen Sie zum Bereich **Konto**.
2. Wählen Sie die Registerkarte **Benutzer & Gruppen** aus.
3. Wählen Sie rechts auf der Seite **Remote-Gruppen** aus.
4. Wählen Sie **Hinzufügen**.

   In diesem Fenster sehen Sie eine Liste der gemeinsamen Namen und Distinguished Names der LDAP-Gruppen, die Astra Control aus dem Verzeichnis abgerufen hat.

5. Suchen Sie optional nach einer LDAP-Gruppe, indem Sie den gemeinsamen Namen der Gruppe in das Feld **Filter nach gemeinsamem Namen** eingeben.
6. Wählen Sie eine oder mehrere Gruppen aus der Liste aus.
7. Weisen Sie den Gruppen eine Rolle zu.

Die ausgewählte Rolle ist allen Benutzern in dieser Gruppe zugewiesen. Wenn Sie einem Benutzer und der Gruppe des Benutzers verschiedene Rollen zuweisen, hat die Rolle eine größere Priorität.

8. Weisen Sie dieser Gruppe optional eine oder mehrere Namespace-Einschränkungen zu und wählen Sie **Rolle auf Einschränkungen beschränken** aus, um sie durchzusetzen. Sie können eine neue Namespace-Einschränkung hinzufügen, indem Sie **Bedingung hinzufügen** auswählen.

Wenn einem Benutzer mehrere Rollen durch die LDAP-Gruppenmitgliedschaft zugewiesen werden, sind die Einschränkungen in der am stärksten permissivsten Rolle die einzigen, die wirksam werden. Wenn z. B. ein Benutzer mit einer lokalen Viewer-Rolle drei Gruppen verbindet, die an die Rolle Mitglied gebunden sind, wird die Summe der Einschränkungen aus den Mitgliederrollen wirksam, und alle Einschränkungen aus der Viewer-Rolle werden ignoriert.

9. Wählen Sie **Hinzufügen**.

Ergebnis

Die neue Gruppe wird in der Liste der Remote-Gruppen angezeigt. Remote-Benutzer in dieser Gruppe werden erst dann in der Liste der Remote-Benutzer angezeigt, wenn sich jeder Remote-Benutzer anmeldet. In dieser Liste können Sie Details über die Gruppe anzeigen und die Gruppe über das Menü **Aktionen** verwalten.

Anzeigen und Managen von Benachrichtigungen

Astra benachrichtigt Sie, wenn Aktionen abgeschlossen oder fehlgeschlagen sind. Beispielsweise wird eine Benachrichtigung angezeigt, wenn ein Backup einer Anwendung erfolgreich abgeschlossen wurde.

Sie können diese Benachrichtigungen oben rechts auf der Schnittstelle verwalten:

Schritte

1. Wählen Sie oben rechts die Anzahl der ungelesenen Benachrichtigungen aus.
2. Überprüfen Sie die Benachrichtigungen und wählen Sie dann **als gelesen markieren** oder **Alle Benachrichtigungen anzeigen**.

   Wenn Sie **Alle Benachrichtigungen anzeigen** ausgewählt haben, wird die Seite Benachrichtigungen geladen.

3. Zeigen Sie auf der Seite **Benachrichtigungen** die Benachrichtigungen an, wählen Sie die Benachrichtigungen aus, die Sie als gelesen markieren möchten, wählen Sie **Aktion** und wählen Sie **als gelesen markieren**.

Anmeldeinformationen hinzufügen und entfernen

Fügen Sie Anmeldedaten für lokale Private-Cloud-Provider wie ONTAP S3, mit OpenShift gemanagte Kubernetes-Cluster oder nicht gemanagte Kubernetes-Cluster jederzeit in Ihrem Konto hinzu und entfernen Sie sie. Astra Control Center verwendet diese Zugangsdaten, um Kubernetes-Cluster und die Applikationen auf den Clustern zu erkennen und Ressourcen in Ihrem Auftrag bereitzustellen.

Beachten Sie, dass alle Benutzer im Astra Control Center dieselben Anmeldedaten verwenden.

Anmeldedaten hinzufügen

Wenn Sie Cluster verwalten, können Sie Astra Control Center Anmeldeinformationen hinzufügen. Informationen zum Hinzufügen von Anmeldeinformationen durch Hinzufügen eines neuen Clusters finden Sie unter "Fügen Sie einen Kubernetes-Cluster hinzu".

Wenn Sie Ihre eigene kubeconfig-Datei erstellen, sollten Sie nur **ein** Kontextelement in ihr definieren. Siehe "Kubernetes-Dokumentation" Für Informationen über das Erstellen von kubeconfig-Dateien.

Anmeldedaten entfernen

Entfernen Sie die Anmeldeinformationen jederzeit aus einem Konto. Sie sollten erst nach dem Entfernen von Anmeldeinformationen verwenden "Verwalten aller zugehörigen Cluster wird aufgehoben".

Der erste Satz von Anmeldeinformationen, die Sie dem Astra Control Center hinzufügen, wird immer verwendet, da Astra Control Center die Zugangsdaten für die Authentifizierung beim Backup-Bucket verwendet. Diese Anmeldedaten sollten am besten nicht entfernt werden.

Schritte

1. Wählen Sie **Konto**.
2. Wählen Sie die Registerkarte **Anmeldeinformationen** aus.
3. Wählen Sie in der Spalte **Status** das Menü Optionen für die Anmeldeinformationen aus, die Sie entfernen möchten.
4. Wählen Sie **Entfernen**.
5. Geben Sie das Wort „Entfernen“ ein, um den Löschvorgang zu bestätigen, und wählen Sie dann **Ja, Anmeldedaten entfernen** aus.

Ergebnis

Astra Control Center entfernt die Anmeldeinformationen aus dem Konto.

Überwachen der Kontoaktivität

Details zu den Aktivitäten können Sie in Ihrem Astra Control Konto anzeigen. Beispiel: Beim Einladen neuer Benutzer, beim Hinzufügen eines Clusters oder beim Erstellen eines Snapshots. Sie haben auch die Möglichkeit, Ihre Kontoaktivität in eine CSV-Datei zu exportieren.

Wenn Sie Kubernetes-Cluster über Astra Control verwalten und Astra Control mit Cloud Insights verbunden ist, sendet Astra Control Ereignisprotokolle an Cloud Insights. Die Protokollinformationen, einschließlich Informationen über die Pod-Implementierung und PVC-Anhänge, werden im Astra Control Activity Log angezeigt. Mithilfe dieser Informationen können Sie alle zu verwaltenden Kubernetes-Cluster Fehler ermitteln.

Alle Kontoaktivitäten in Astra Control anzeigen

1. Wählen Sie **Aktivität**.
2. Verwenden Sie die Filter, um die Liste der Aktivitäten einzugrenzen, oder verwenden Sie das Suchfeld, um das gesuchte zu finden.

3. Wählen Sie **in CSV exportieren** aus, um Ihre Kontoaktivität in eine CSV-Datei herunterzuladen.

Zeigen Sie die Kontoaktivität für eine bestimmte App an

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie **Aktivität**.

Zeigen Sie die Kontoaktivität für Cluster an

1. Wählen Sie **Cluster** und dann den Namen des Clusters aus.
2. Wählen Sie **Aktivität**.

Ergreifen Sie Maßnahmen, um Ereignisse zu lösen, die Aufmerksamkeit erfordern

1. Wählen Sie **Aktivität**.
2. Wählen Sie ein Ereignis aus, das Aufmerksamkeit erfordert.
3. Wählen Sie die Dropdown-Option **Aktion** aus.

   In dieser Liste finden Sie mögliche Korrekturmaßnahmen, die Sie ergreifen können, eine Dokumentation zum Problem anzeigen und Support zur Behebung des Problems erhalten.

Aktualisieren einer vorhandenen Lizenz

Sie können eine Evaluierungslizenz in eine vollständige Lizenz umwandeln oder eine bestehende Evaluierung oder Volllizenz mit einer neuen Lizenz aktualisieren. Wenn Sie keine vollständige Lizenz besitzen, wenden Sie sich an Ihren NetApp Ansprechpartner, um eine vollständige Lizenz und eine Seriennummer zu erhalten. Sie können die Astra Control Center-UI oder verwenden "Astra Control API" Um eine vorhandene Lizenz zu aktualisieren.

Schritte

1. Melden Sie sich bei an "NetApp Support Website".
2. Rufen Sie die Download-Seite des Astra Control Center auf, geben Sie die Seriennummer ein und laden Sie die vollständige NetApp Lizenzdatei (NLF) herunter.
3. Melden Sie sich in der UI des Astra Control Center an.
4. Wählen Sie in der linken Navigationsleiste **Konto** > **Lizenz**.
5. Wählen Sie auf der Seite **Konto** > **Lizenz** das Dropdown-Menü Status der vorhandenen Lizenz aus und wählen Sie **Replace**.
6. Navigieren Sie zu der Lizenzdatei, die Sie heruntergeladen haben.
7. Wählen Sie **Hinzufügen**.

Auf der Seite **Konto** > **Lizenzen** werden Lizenzinformationen, Ablaufdatum, Lizenzseriennummer, Konto-ID und verwendete CPU-Einheiten angezeigt.

Finden Sie weitere Informationen

- "Astra Control Center-Lizenzierung"