Gérez votre compte

Astra Control Center

NetApp
March 12, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/astra-control-center-2310/use/manage-local-users-and-roles.html on March 12, 2024. Always check docs.netapp.com for the latest.

Sommaire

Gérez votre compte

Gérez les utilisateurs et les rôles locaux

Vous pouvez ajouter, supprimer et modifier les utilisateurs de votre installation Astra Control Center à l'aide de l'interface utilisateur Astra Control. Vous pouvez utiliser l'interface utilisateur de contrôle Astra ou "API de contrôle Astra" pour gérer les utilisateurs.

Vous pouvez également utiliser LDAP pour effectuer l'authentification pour certains utilisateurs.

Utiliser LDAP

LDAP est un protocole standard de l'industrie pour l'accès aux informations d'annuaires distribués et un choix populaire pour l'authentification d'entreprise. Vous pouvez connecter Astra Control Center à un serveur LDAP pour effectuer l'authentification de certains utilisateurs Astra Control. À un niveau élevé, la configuration implique l'intégration d'Astra avec LDAP et la définition des utilisateurs et des groupes Astra Control correspondant aux définitions LDAP. Vous pouvez utiliser l'API de contrôle Astra ou l'interface utilisateur Web pour configurer l'authentification LDAP et les utilisateurs et groupes LDAP. Pour plus d'informations, reportez-vous à la documentation suivante :

- "Utilisez l'API de contrôle Astra pour gérer l'authentification à distance et les utilisateurs"
- "Utilisez l'interface utilisateur Astra Control pour gérer les utilisateurs et les groupes distants"
- "Utilisez l'interface utilisateur Astra Control pour gérer l'authentification à distance"

Ajouter des utilisateurs

Les propriétaires et administrateurs de comptes peuvent ajouter d'autres utilisateurs à l'installation d'Astra Control Center.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **utilisateurs**.
3. Sélectionnez **Ajouter utilisateur**.
4. Entrez le nom de l'utilisateur, son adresse e-mail et son mot de passe temporaire.

   L'utilisateur doit modifier le mot de passe lors de sa première connexion.

5. Sélectionnez un rôle d'utilisateur avec les autorisations système appropriées.

   Chaque rôle offre les autorisations suivantes :

   - Un **Viewer** peut afficher les ressources.
   - Un **membre** dispose des autorisations de rôle Viewer et peut gérer les applications et les clusters, annuler la gestion des applications et supprimer des instantanés et des sauvegardes.
   - Un **Admin** dispose des autorisations de rôle de membre et peut ajouter et supprimer d'autres utilisateurs, à l'exception du propriétaire.
   - Un **propriétaire** possède des autorisations de rôle d'administrateur et peut ajouter et supprimer des

comptes d'utilisateur.

6. Pour ajouter des contraintes à un utilisateur avec un rôle membre ou visualiseur, activez la case à cocher **restreindre le rôle aux contraintes**.

   Pour plus d'informations sur l'ajout de contraintes, voir "Gérez les utilisateurs et les rôles locaux".

7. Sélectionnez **Ajouter**.

Gérer les mots de passe

Vous pouvez gérer les mots de passe des comptes utilisateur dans Astra Control Center.

Changer votre mot de passe

Vous pouvez modifier le mot de passe de votre compte utilisateur à tout moment.

Étapes

1. Sélectionnez l'icône utilisateur en haut à droite de l'écran.
2. Sélectionnez **Profile**.
3. Dans le menu Options de la colonne **actions**, sélectionnez **changer mot de passe**.
4. Saisissez un mot de passe conforme aux exigences de mot de passe.
5. Saisissez à nouveau le mot de passe pour le confirmer.
6. Sélectionnez **changer mot de passe**.

Réinitialiser le mot de passe d'un autre utilisateur

Si votre compte dispose des autorisations de rôle Administrateur ou propriétaire, vous pouvez réinitialiser les mots de passe des autres comptes utilisateur ainsi que les vôtres. Lorsque vous réinitialisez un mot de passe, vous attribuez un mot de passe temporaire que l'utilisateur devra modifier lors de la connexion.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez la liste déroulante **actions**.
3. Sélectionnez **Réinitialiser le mot de passe**.
4. Saisissez un mot de passe temporaire conforme aux exigences de mot de passe.
5. Saisissez à nouveau le mot de passe pour le confirmer.

   Lors de la prochaine connexion de l'utilisateur, l'utilisateur est invité à modifier le mot de passe.

6. Sélectionnez **Réinitialiser le mot de passe**.

Supprimer des utilisateurs

Les utilisateurs disposant du rôle propriétaire ou administrateur peuvent à tout moment supprimer d'autres utilisateurs du compte.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Dans l'onglet **Users**, cochez la case de la ligne de chaque utilisateur que vous souhaitez supprimer.
3. Dans le menu Options de la colonne **actions**, sélectionnez **Supprimer utilisateur/s**.
4. Lorsque vous y êtes invité, confirmez la suppression en saisissant le mot "supprimer", puis sélectionnez **Oui, Supprimer l'utilisateur**.

Résultat

Astra Control Center supprime l'utilisateur du compte.

Gérez les rôles

Vous pouvez gérer les rôles en ajoutant des contraintes d'espace de noms et en restreignant les rôles des utilisateurs à ces contraintes. Cela vous permet de contrôler l'accès aux ressources de votre organisation. Vous pouvez utiliser l'interface utilisateur de contrôle Astra ou "API de contrôle Astra" pour gérer les rôles.

Ajoutez une contrainte d'espace de noms à un rôle

Un administrateur ou un propriétaire peut ajouter des contraintes d'espace de noms aux rôles de membre ou de visualiseur.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **utilisateurs**.
3. Dans la colonne **actions**, sélectionnez le bouton de menu d'un utilisateur ayant le rôle membre ou visualiseur.
4. Sélectionnez **Modifier le rôle**.
5. Activez la case à cocher **restreindre le rôle aux contraintes**.

   La case à cocher n'est disponible que pour les rôles de membre ou de visualiseur. Vous pouvez sélectionner un autre rôle dans la liste déroulante **role**.

6. Sélectionnez **Ajouter une contrainte**.

   Vous pouvez afficher la liste des contraintes disponibles par espace de noms ou par étiquette d'espace de noms.

7. Dans la liste déroulante **Type de contrainte**, sélectionnez **espace de noms Kubernetes** ou **étiquette d'espace de noms Kubernetes** selon la configuration de vos espaces de noms.
8. Sélectionnez un ou plusieurs espaces de noms ou étiquettes dans la liste pour composer une contrainte qui restreint les rôles à ces espaces de noms.
9. Sélectionnez **confirmer**.

   La page **Modifier rôle** affiche la liste des contraintes que vous avez choisies pour ce rôle.

10. Sélectionnez **confirmer**.

    Sur la page **compte**, vous pouvez afficher les contraintes pour n'importe quel rôle de membre ou de visualiseur dans la colonne **rôle**.

Si vous activez des contraintes pour un rôle et que vous sélectionnez **confirmer** sans ajouter de contraintes, le rôle est considéré comme étant soumis à des restrictions complètes (le rôle est refusé l'accès aux ressources affectées aux espaces de noms).

Supprime une contrainte d'espace de noms d'un rôle

Un utilisateur Admin ou propriétaire peut supprimer une contrainte d'espace de noms d'un rôle.

Étapes

1. Dans la zone de navigation **gérer votre compte**, sélectionnez **compte**.
2. Sélectionnez l'onglet **utilisateurs**.
3. Dans la colonne **actions**, sélectionnez le bouton de menu d'un utilisateur ayant le rôle membre ou visualiseur ayant des contraintes actives.
4. Sélectionnez **Modifier le rôle**.

   La boîte de dialogue **Modifier le rôle** affiche les contraintes actives du rôle.

5. Sélectionnez **X** à droite de la contrainte à supprimer.
6. Sélectionnez **confirmer**.

Pour en savoir plus

- "Rôles et espaces de noms d'utilisateur"

Gérer l'authentification à distance

LDAP est un protocole standard de l'industrie pour l'accès aux informations d'annuaires distribués et un choix populaire pour l'authentification d'entreprise. Vous pouvez connecter Astra Control Center à un serveur LDAP pour effectuer l'authentification de certains utilisateurs Astra Control.

À un niveau élevé, la configuration implique l'intégration d'Astra avec LDAP et la définition des utilisateurs et des groupes Astra Control correspondant aux définitions LDAP. Vous pouvez utiliser l'API de contrôle Astra ou l'interface utilisateur Web pour configurer l'authentification LDAP et les utilisateurs et groupes LDAP.

ASTRA Control Center utilise l'attribut de connexion utilisateur, configuré lorsque l'authentification à distance est activée, pour rechercher et garder le suivi des utilisateurs distants. Un attribut d'adresse e-mail (« mail ») ou de nom principal d'utilisateur (« userPrincipalName ») doit exister dans ce champ pour tout utilisateur distant que vous souhaitez voir apparaître dans Astra Control Center. Cet attribut est utilisé comme nom d'utilisateur dans Astra Control Center pour l'authentification et pour les recherches d'utilisateurs distants.

Ajoutez un certificat pour l'authentification LDAPS

Ajoutez le certificat TLS privé pour le serveur LDAP afin que Astra Control Center puisse s'authentifier auprès du serveur LDAP lorsque vous utilisez une connexion LDAPS. Vous ne devez le faire qu'une seule fois, ou lorsque le certificat que vous avez installé expire.

Étapes

1. Accédez à **compte**.
2. Sélectionnez l'onglet **certificats**.
3. Sélectionnez **Ajouter**.
4. Téléchargez le `.pem` importez ou collez le contenu du fichier à partir du presse-papiers.
5. Cochez la case **approuvé**.
6. Sélectionnez **Ajouter un certificat**.

Activez l'authentification à distance

Vous pouvez activer l'authentification LDAP et configurer la connexion entre Astra Control et le serveur LDAP distant.

Avant de commencer

Si vous prévoyez d'utiliser LDAPS, assurez-vous que le certificat TLS privé pour le serveur LDAP est installé dans Astra Control Center afin que le centre de contrôle Astra puisse s'authentifier auprès du serveur LDAP. Voir Ajoutez un certificat pour l'authentification LDAPS pour obtenir des instructions.

Étapes

1. Accédez à **compte > connexions**.
2. Dans le volet **authentification à distance**, sélectionnez le menu de configuration.
3. Sélectionnez **connexion**.
4. Entrez l'adresse IP du serveur, le port et le protocole de connexion préféré (LDAP ou LDAPS).

> Il est recommandé d'utiliser LDAPS lors de la connexion au serveur LDAP. Vous devez installer le certificat TLS privé du serveur LDAP dans Astra Control Center avant de vous connecter avec LDAPS.

5. Saisissez les informations d'identification du compte de service au format e-mail (administrator@example.com). Astra Control utilisera ces informations d'identification lors de la connexion au serveur LDAP.
6. Dans la section **correspondance utilisateur**, procédez comme suit :
   a. Entrez le DN de base et un filtre de recherche d'utilisateur approprié à utiliser lors de la récupération des informations utilisateur à partir du serveur LDAP.
   b. (Facultatif) si votre répertoire utilise l'attribut de connexion utilisateur `userPrincipalName` au lieu de `mail`, entrez `userPrincipalName` Dans l'attribut correct dans le champ **User login attribute**.
7. Dans la section **correspondance de groupe**, entrez le nom unique de base de recherche de groupe et un filtre de recherche de groupe personnalisé approprié.

> Veillez à utiliser le nom unique de base (DN) correct et un filtre de recherche approprié pour **User Match** et **Group Match**. Le DN de base indique à Astra Control à quel niveau de l'arborescence de répertoire démarrer la recherche, et le filtre de recherche limite les parties de l'arborescence de répertoires Astra Control à partir de.

8. Sélectionnez **soumettre**.

Résultat

L'état du volet **authentification à distance** passe à **en attente**, puis à **connecté** lorsque la connexion au serveur LDAP est établie.

Désactiver l'authentification à distance

Vous pouvez désactiver temporairement une connexion active au serveur LDAP.

> Lorsque vous désactivez une connexion à un serveur LDAP, tous les paramètres sont enregistrés et tous les utilisateurs et groupes distants ajoutés à Astra Control à partir de ce serveur LDAP sont conservés. Vous pouvez vous reconnecter à ce serveur LDAP à tout moment.

Étapes

1. Accédez à **compte > connexions**.
2. Dans le volet **authentification à distance**, sélectionnez le menu de configuration.
3. Sélectionnez **Désactiver**.

Résultat

L'état du volet **authentification à distance** passe à **Désactivé**. Tous les paramètres d'authentification à distance, les utilisateurs distants et les groupes distants sont conservés et vous pouvez réactiver la connexion à tout moment.

Modifier les paramètres d'authentification à distance

Si vous avez désactivé la connexion au serveur LDAP ou si le volet **authentification à distance** est à l'état "erreur de connexion", vous pouvez modifier les paramètres de configuration.

> Vous ne pouvez pas modifier l'adresse IP ou l'URL du serveur LDAP lorsque le volet **authentification distante** est à l'état "Désactivé". Vous devez le faire Déconnectez l'authentification à distance tout d'abord.

Étapes

1. Accédez à **compte > connexions**.
2. Dans le volet **authentification à distance**, sélectionnez le menu de configuration.
3. Sélectionnez **Modifier**.
4. Apportez les modifications nécessaires et sélectionnez **Modifier**.

Déconnectez l'authentification à distance

Vous pouvez vous déconnecter d'un serveur LDAP et supprimer les paramètres de configuration d'Astra Control.

> Si vous êtes un utilisateur LDAP et que vous vous déconnectez, votre session prend fin immédiatement Lorsque vous vous déconnectez du serveur LDAP, tous les paramètres de configuration de ce serveur LDAP sont supprimés d'Astra Control, ainsi que tous les utilisateurs et groupes distants ajoutés à partir de ce serveur LDAP.

Étapes

1. Accédez à **compte > connexions**.

2. Dans le volet **authentification à distance**, sélectionnez le menu de configuration.
3. Sélectionnez **déconnecter**.

Résultat

L'état du volet **authentification à distance** passe à **déconnecté**. Les paramètres d'authentification à distance, les utilisateurs distants et les groupes distants sont supprimés d'Astra Control.

Gérez des utilisateurs et des groupes distants

Si vous avez activé l'authentification LDAP sur votre système Astra Control, vous pouvez rechercher des utilisateurs et des groupes LDAP et les inclure dans les utilisateurs approuvés du système.

Ajouter un utilisateur distant

Les propriétaires et administrateurs de comptes peuvent ajouter des utilisateurs distants à Astra Control. ASTRA Control Center prend en charge jusqu'à 10,000 utilisateurs distants LDAP.

ASTRA Control Center utilise l'attribut de connexion utilisateur, configuré lorsque l'authentification à distance est activée, pour rechercher et garder le suivi des utilisateurs distants. Un attribut d'adresse e-mail (« mail ») ou de nom principal d'utilisateur (« userPrincipalName ») doit exister dans ce champ pour tout utilisateur distant que vous souhaitez voir apparaître dans Astra Control Center. Cet attribut est utilisé comme nom d'utilisateur dans Astra Control Center pour l'authentification et pour les recherches d'utilisateurs distants.

Vous ne pouvez pas ajouter un utilisateur distant si un utilisateur local avec la même adresse e-mail (basée sur l'attribut « mail » ou « nom principal de l'utilisateur ») existe déjà sur le système. Pour ajouter l'utilisateur en tant qu'utilisateur distant, supprimez d'abord l'utilisateur local du système.

Étapes

1. Accédez à la zone **compte**.
2. Sélectionnez l'onglet **utilisateurs et groupes**.
3. À l'extrême droite de la page, sélectionnez **utilisateurs distants**.
4. Sélectionnez **Ajouter**.
5. Vous pouvez également rechercher un utilisateur LDAP en saisissant l'adresse e-mail de l'utilisateur dans le champ **Filter by email**.
6. Sélectionnez un ou plusieurs utilisateurs dans la liste.
7. Attribuez un rôle à l'utilisateur.

   Si vous attribuez différents rôles à un utilisateur et au groupe de l'utilisateur, le rôle plus permissif est prioritaire.

8. Vous pouvez éventuellement attribuer une ou plusieurs contraintes d'espace de noms à cet utilisateur et sélectionner **restreindre le rôle aux contraintes** pour les appliquer. Vous pouvez ajouter une nouvelle contrainte d'espace de noms en sélectionnant **Ajouter une contrainte**.

Lorsqu'un utilisateur se voit attribuer plusieurs rôles via l'appartenance à un groupe LDAP, les contraintes du rôle le plus permissif sont les seules qui prennent effet. Par exemple, si un utilisateur avec un rôle de visualiseur local rejoint trois groupes liés au rôle membre, la somme des contraintes des rôles de membre prend effet et toutes les contraintes du rôle de visualiseur sont ignorées.

9. Sélectionnez **Ajouter**.

Résultat

Le nouvel utilisateur apparaît dans la liste des utilisateurs distants. Dans cette liste, vous pouvez voir les contraintes actives sur l'utilisateur et gérer l'utilisateur à partir du menu **actions**.

Ajouter un groupe distant

Pour ajouter plusieurs utilisateurs distants à la fois, les propriétaires et administrateurs de comptes peuvent ajouter des groupes distants à Astra Control. Lorsque vous ajoutez un groupe distant, tous les utilisateurs distants de ce groupe peuvent se connecter à Astra Control et héritent du même rôle que le groupe.

ASTRA Control Center prend en charge jusqu'à 5,000 groupes distants LDAP.

Étapes

1. Accédez à la zone **compte**.
2. Sélectionnez l'onglet **utilisateurs et groupes**.
3. À l'extrême droite de la page, sélectionnez **Remote Groups**.
4. Sélectionnez **Ajouter**.

   Dans cette fenêtre, vous pouvez voir une liste des noms communs et des noms distinctifs des groupes LDAP récupérés par Astra Control à partir du répertoire.

5. Vous pouvez également rechercher un groupe LDAP en saisissant le nom commun du groupe dans le champ **Filter by common name**.
6. Sélectionnez un ou plusieurs groupes dans la liste.
7. Attribuez un rôle aux groupes.

   Le rôle que vous sélectionnez est attribué à tous les utilisateurs de ce groupe. Si vous attribuez différents rôles à un utilisateur et au groupe de l'utilisateur, le rôle plus permissif est prioritaire.

8. Vous pouvez éventuellement attribuer une ou plusieurs contraintes d'espace de noms à ce groupe et sélectionner **restreindre le rôle aux contraintes** pour les appliquer. Vous pouvez ajouter une nouvelle contrainte d'espace de noms en sélectionnant **Ajouter une contrainte**.

   Lorsqu'un utilisateur se voit attribuer plusieurs rôles via l'appartenance à un groupe LDAP, les contraintes du rôle le plus permissif sont les seules qui prennent effet. Par exemple, si un utilisateur avec un rôle de visualiseur local rejoint trois groupes liés au rôle membre, la somme des contraintes des rôles de membre prend effet et toutes les contraintes du rôle de visualiseur sont ignorées.

9. Sélectionnez **Ajouter**.

Résultat

Le nouveau groupe apparaît dans la liste des groupes distants. Les utilisateurs distants de ce groupe n'apparaissent pas dans la liste des utilisateurs distants tant que chaque utilisateur distant ne se connecte pas. Dans cette liste, vous pouvez afficher les détails du groupe et gérer le groupe à partir du menu **actions**.

Afficher et gérer les notifications

Astra vous avertit lorsque les actions sont terminées ou en échec. Par exemple, vous verrez une notification si une sauvegarde d'une application a réussi.

Vous pouvez gérer ces notifications en haut à droite de l'interface :

Étapes

1. Sélectionnez le nombre de notifications non lues en haut à droite.
2. Examinez les notifications, puis sélectionnez **Marquer comme lu** ou **Afficher toutes les notifications**.

   Si vous avez sélectionné **Afficher toutes les notifications**, la page Notifications se charge.

3. Sur la page **Notifications**, affichez les notifications, sélectionnez celles que vous souhaitez marquer comme lu, sélectionnez **action** et **Marquer comme lu**.

Ajouter et supprimer des informations d'identification

Ajoutez et supprimez des identifiants pour les fournisseurs de cloud privé local, comme ONTAP S3, les clusters Kubernetes gérés avec OpenShift ou les clusters Kubernetes non gérés depuis votre compte à tout moment. Astra Control Center utilise ces identifiants pour détecter les clusters Kubernetes et les applications sur les clusters et provisionner les ressources en votre nom.

Notez que tous les utilisateurs d'Astra Control Center partagent les mêmes informations d'identification.

Ajouter des informations d'identification

Vous pouvez ajouter des informations d'identification à Astra Control Center lorsque vous gérez des clusters. Pour ajouter des informations d'identification en ajoutant un nouveau cluster, reportez-vous à la section "Ajouter un cluster Kubernetes".

> Si vous créez votre propre fichier kubeconfig, vous ne devez définir que l'élément de contexte **one**. Reportez-vous à la section "Documentation Kubernetes" pour plus d'informations sur la création de fichiers kubeconfig.

Supprimer les informations d'identification

Supprimez les informations d'identification d'un compte à tout moment. Vous ne devez supprimer les informations d'identification qu'après "annuler la gestion de tous les clusters associés".

Le premier ensemble d'informations d'identification que vous ajoutez à Astra Control Center est toujours utilisé car Astra Control Center utilise les informations d'identification pour s'authentifier auprès du compartiment de secours. Il est préférable de ne pas supprimer ces informations d'identification.

Étapes

1. Sélectionnez **compte**.
2. Sélectionnez l'onglet **informations d'identification**.
3. Sélectionnez le menu Options dans la colonne **État** pour les informations d'identification que vous souhaitez supprimer.
4. Sélectionnez **Supprimer**.
5. Tapez le mot "supprimer" pour confirmer la suppression, puis sélectionnez **Oui, Supprimer les informations d'identification**.

Résultat

Astra Control Center supprime les informations d'identification du compte.

Surveillez l'activité des comptes

Vous pouvez consulter les détails des activités de votre compte Astra Control. Par exemple, lorsque de nouveaux utilisateurs ont été invités, lorsqu'un cluster a été ajouté ou lorsqu'un snapshot a été créé. Vous pouvez également exporter votre activité de compte vers un fichier CSV.

Si vous gérez des clusters Kubernetes à partir d'Astra Control et qu'Astra Control est connecté à Cloud Insights, Astra Control envoie des journaux d'événements à Cloud Insights. Les informations du journal, y compris les informations sur le déploiement du pod et les pièces jointes en PVC, apparaissent dans le journal des activités de contrôle Astra. Utilisez ces informations pour identifier les problèmes éventuels sur les clusters Kubernetes que vous gérez.

Afficher toutes les activités du compte dans Astra Control

1. Sélectionnez **activité**.
2. Utilisez les filtres pour réduire la liste des activités ou utilisez la zone de recherche pour trouver exactement ce que vous recherchez.
3. Sélectionnez **Exporter au format CSV** pour télécharger l'activité de votre compte dans un fichier CSV.

Afficher l'activité d'un compte pour une application spécifique

1. Sélectionnez **applications**, puis le nom d'une application.
2. Sélectionnez **activité**.

Afficher l'activité des comptes pour les clusters

1. Sélectionnez **clusters**, puis le nom du cluster.
2. Sélectionnez **activité**.

Prenez des mesures pour résoudre les événements qui nécessitent votre attention

1. Sélectionnez **activité**.

2. Sélectionnez un événement qui nécessite une attention particulière.
3. Sélectionnez l'option de liste déroulante **prendre une action**.

   Dans cette liste, vous pouvez consulter les actions correctives possibles, consulter la documentation associée au problème et obtenir de l'aide pour résoudre ce dernier.

Mettre à jour une licence existante

Vous pouvez convertir une licence d'évaluation en licence complète, ou mettre à jour une évaluation existante ou une licence complète avec une nouvelle licence. Si vous ne disposez pas d'une licence complète, contactez votre contact commercial NetApp pour obtenir une licence complète et un numéro de série. Vous pouvez utiliser l'interface utilisateur du centre de contrôle Astra ou "API de contrôle Astra" pour mettre à jour une licence existante.

Étapes

1. Connectez-vous au "Site de support NetApp".
2. Accédez à la page de téléchargement d'Astra Control Center, entrez le numéro de série et téléchargez le fichier de licence NetApp complet (NLF).
3. Connectez-vous à l'interface utilisateur du centre de contrôle Astra.
4. Dans le menu de navigation de gauche, sélectionnez **compte** > **Licence**.
5. Dans la page **compte** > **Licence**, sélectionnez le menu déroulant d'état de la licence existante et sélectionnez **remplacer**.
6. Accédez au fichier de licence que vous avez téléchargé.
7. Sélectionnez **Ajouter**.

La page **compte** > **licences** affiche les informations de licence, la date d'expiration, le numéro de série de licence, l'ID de compte et les unités UC utilisées.

Pour en savoir plus

- "Licence Astra Control Center"

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.