



Configurer les intégrations et les services de NetApp Console

NetApp Console local deployment

NetApp
August 10, 2026

Sommaire

- Configurer les intégrations et les services de NetApp Console 1
 - Intégrer le déploiement local de la NetApp Console avec Active Directory 1
 - Avant de commencer 1
 - Désactiver ou activer une intégration Active Directory 2
 - Supprimer une intégration Active Directory 2
 - Connectez votre LLM et activez l'assistant NetApp Console dans le déploiement local de NetApp Console 3
 - Rassemblez ce dont vous avez besoin avant de connecter un LLM 3
 - Connectez un LLM au déploiement local de la NetApp Console 4
 - Vérifiez que l'intégration LLM fonctionne 4
 - Protégez les identifiants et surveillez l'utilisation du LLM 4
 - Résoudre les problèmes d'intégration LLM dans le déploiement local de la NetApp Console 5
 - Résolvez rapidement les problèmes d'intégration LLM 5
 - Dépanner par symptôme 5
 - Répondez à l'exposition ou à l'utilisation abusive d'un identifiant LLM 6
 - Configurez les canaux de distribution des notifications dans le déploiement local de la NetApp Console . . . 6
 - Configurer un serveur de messagerie 6
 - Configurer un webhook 8

Configurer les intégrations et les services de NetApp Console

Intégrer le déploiement local de la NetApp Console avec Active Directory

Intégrez le déploiement local de NetApp Console à Active Directory pour la connexion et la recherche d'utilisateurs via l'annuaire. Utilisez votre service d'annuaire pour authentifier les utilisateurs, puis attribuez des accès à ces utilisateurs dans le déploiement local de NetApp Console.

Rôles d'accès requis

Super administrateur ou administrateur de l'organisation. ["Découvrez les rôles d'accès"](#).

Lorsque vous intégrez Active Directory, le déploiement local de la Console authentifie les utilisateurs via votre annuaire existant. Après avoir ajouté un utilisateur à l'annuaire, attribuez des rôles d'accès à la Console pour contrôler ce à quoi cet utilisateur peut accéder.

L'intégration d'Active Directory vous aide également à répondre aux exigences de conformité en appliquant vos contrôles, journaux d'audit et politiques existants à l'accès au déploiement local de NetApp Console.



- L'intégration d'Active Directory ne crée pas de groupes fédérés, ne synchronise pas les affectations de groupes d'annuaire et n'accorde pas automatiquement l'accès. Les administrateurs ajoutent toujours les utilisateurs de l'annuaire à l'organisation et attribuent des rôles dans le déploiement local de la Console.
- Une seule intégration Active Directory est prise en charge à la fois. Une fois une intégration configurée, le bouton **Ajouter une intégration** est désactivé. Pour passer à un autre annuaire, désactivez ou supprimez d'abord l'intégration existante.
- Les utilisateurs de l'annuaire ne configurent ni n'utilisent l'authentification multifacteur (MFA). Le déploiement local de la console prend en charge la MFA uniquement pour les utilisateurs locaux. ["Apprenez à gérer les paramètres de sécurité des membres"](#).

Avant de commencer

Avant d'intégrer Active Directory, assurez-vous de disposer des éléments suivants :

- Un domaine Active Directory et des identifiants permettant d'interroger l'annuaire
- L'adresse du serveur LDAP et le nom unique (DN) de base de l'arborescence d'annuaire
- Accès réseau depuis le déploiement local de NetApp Console vers votre serveur LDAP sur le port 389 (LDAP) ou 636 (LDAPS)
- Certificats SSL/TLS, si vous prévoyez d'utiliser LDAPS

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Directory services** pour ouvrir la page Federations.
3. Sélectionnez **Ajouter une intégration**.

4. Saisissez les informations de connexion à votre serveur Active Directory :
 - Un nom descriptif pour l'intégration.
 - **Hôte LDAP** : nom d'hôte ou adresse IP de votre serveur LDAP. Pour plusieurs serveurs, saisissez le principal.
 - Le port : 389 pour LDAP ou 636 pour LDAPS.
 - Délai d'expiration de la connexion en millisecondes. La valeur par défaut est de 1000 ms.
5. Sélectionnez **Utiliser SSL/TLS** pour utiliser LDAPS. Vérifiez que votre serveur LDAP prend en charge LDAPS et que la NetApp Console peut accéder aux certificats requis.
6. Testez la connexion. En cas d'échec, vérifiez l'hôte LDAP, le port, la connectivité réseau et les certificats SSL/TLS.
7. Une fois le test réussi, saisissez le répertoire et les informations de l'utilisateur :
 - **Liaison DN de base** : Saisissez le nom unique de liaison (Bind DN) du compte LDAP/AD que cette application utilisera pour se connecter à l'annuaire, ainsi que l'identifiant (mot de passe) de ce compte. NetApp Console utilise ces informations pour se lier à LDAP et valider la connexion.
 - **DN utilisateur** : un compte utilisateur autorisé à interroger l'annuaire. Par exemple, CN=ldap-reader,OU=Service Accounts,DC=example,DC=com.
8. Sélectionnez **Ajouter** pour enregistrer l'intégration.

Après avoir terminé

Après avoir enregistré l'intégration, ajoutez les utilisateurs de l'annuaire à votre organisation et attribuez-leur des rôles. Vous devez configurer et activer au moins une intégration Active Directory avant de pouvoir ajouter des utilisateurs de l'annuaire. ["Découvrez comment ajouter des utilisateurs à l'annuaire et attribuer des rôles"](#).

Désactiver ou activer une intégration Active Directory

Désactivez une intégration pour suspendre temporairement l'authentification par annuaire sans supprimer la configuration. Lorsque vous désactivez un service d'annuaire, les utilisateurs de l'annuaire ne peuvent pas se connecter via l'annuaire.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Directory services** pour ouvrir la page Federations.
3. Dans la liste des intégrations, repérez l'intégration et sélectionnez le menu d'actions correspondant à cette ligne.
4. Sélectionnez **Désactiver** pour suspendre l'intégration, ou **Activer** pour la rétablir.

Supprimer une intégration Active Directory

Supprimez une intégration pour supprimer définitivement la configuration du service d'annuaire. Avant de supprimer, vérifiez les avertissements concernant les utilisateurs d'annuaire liés à l'intégration, car leur accès sera affecté.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Directory services** pour ouvrir la page Federations.
3. Dans la liste des intégrations, repérez l'intégration et sélectionnez le menu d'actions correspondant à cette

ligne.

4. Sélectionnez **Supprimer** et confirmez la suppression.

Connectez votre LLM et activez l'assistant NetApp Console dans le déploiement local de NetApp Console

Connectez votre grand modèle de langage (LLM) au déploiement local de NetApp Console pour activer l'assistant de la Console et la gestion du stockage assistée par l'IA.



Cette documentation relative à la connexion d'un LLM à l'assistant Console pour activer les fonctionnalités d'IA est fournie à titre d'aperçu technologique. Dans le cadre de cette offre d'aperçu, NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de cette offre avant sa disponibilité générale.

Rôles d'accès requis

Super administrateur ou administrateur de l'organisation. ["Découvrez les rôles d'accès"](#).

Une fois la configuration terminée, les utilisateurs ouvrent l'assistant Console depuis le tableau de bord et choisissent un mode d'accès :

- En mode **Lecture seule**, l'assistant répond aux questions et fournit des conseils sans apporter de modifications.
- En mode **Lecture/écriture**, l'assistant peut interagir avec l'infrastructure de stockage. Il affiche les détails pour vérification et confirmation avant chaque modification. Pour les opérations asynchrones, telles que la création de volume, il crée une tâche que les utilisateurs peuvent vérifier depuis l'assistant.

Pour connecter votre LLM, sélectionnez un chemin de fournisseur, saisissez les détails de l'endpoint et la clé API, puis sélectionnez un modèle dans **Administration > AI Tools**. Les actions de l'assistant restent conformes à vos politiques de stockage et à vos contrôles d'accès basés sur les rôles.

Rassemblez ce dont vous avez besoin avant de connecter un LLM

Avant de connecter votre LLM, rassemblez les éléments suivants :

- Votre choix de type de fournisseur : OpenAI ou compatible OpenAI. ["Découvrez les choix de fournisseurs."](#)
- Une clé API valide pour le chemin du fournisseur que vous sélectionnez.
- L'URL du point de terminaison pour le chemin de votre fournisseur.
- L'URL de votre proxy ou de votre passerelle, si votre organisation en exige une.
- Votre nom d'utilisateur ou votre identifiant d'authentification unique (SSO) pour le compte fournisseur LLM, si nécessaire.
- Accès réseau depuis le déploiement local de NetApp Console vers le point de terminaison sélectionné.
- Classes de stockage et contrôles d'accès basés sur les rôles pour les actions de l'assistant que vous prévoyez d'autoriser.

Pour plus de détails sur les modèles pris en charge, voir ["Découvrez les fournisseurs et modèles LLM pris en charge dans le déploiement local de NetApp Console"](#).

Connectez un LLM au déploiement local de la NetApp Console

Saisissez les paramètres du fournisseur, la clé API et le modèle pour connecter votre LLM au déploiement local de NetApp Console.

Étapes

1. Connectez-vous au déploiement local de la NetApp Console.
2. Sélectionnez **Administration > Outils d'IA**.
3. Sélectionnez le menu, puis sélectionnez **Modifier**.
4. Dans **Type de fournisseur**, sélectionnez un type de fournisseur.

["Découvrez l'intégration LLM dans le déploiement local de NetApp Console"](#).

5. Si le système vous demande un point de terminaison de fournisseur, saisissez l'URL du point de terminaison du fournisseur pour le chemin que vous avez sélectionné.
6. Saisissez l'URL du proxy ou de la passerelle et les identifiants.
7. Dans le champ **Nom d'utilisateur**, saisissez votre nom d'utilisateur ou votre identifiant SSO si le chemin de votre fournisseur l'exige.
8. Dans le champ **clé API**, collez la clé API provenant du chemin de votre fournisseur sélectionné.
9. Sélectionnez un modèle dans la liste.
10. Vérifiez la configuration, puis sélectionnez **Enregistrer**.

Si l'enregistrement ou le test échoue, vérifiez le type de fournisseur, l'URL du point de terminaison, la clé API et le modèle sélectionné, puis réessayez.

["Résolvez les problèmes liés à l'intégration de votre LLM"](#).

Vérifiez que l'intégration LLM fonctionne

Après avoir enregistré la configuration, vérifiez la disponibilité et le comportement de l'assistant.

Étapes

1. Vérifiez que le bouton **Assistant Console** apparaît sur le tableau de bord de déploiement local de la NetApp Console.
2. Ouvrez l'assistant en mode **Lecture seule** et exécutez une requête de base.
3. Ouvrez l'assistant en mode **Lecture/écriture** et vérifiez que les actions modifiant le stockage nécessitent une confirmation de l'utilisateur avant leur exécution.
4. Vérifiez que les utilisateurs qui ont besoin de flux de travail d'actions disposent des contrôles d'accès basés sur les rôles requis.

Une fois la validation terminée, les utilisateurs peuvent ouvrir l'assistant Console depuis le tableau de bord et décrire les tâches en langage clair. Pour des exemples d'utilisation et des flux de travail pour les utilisateurs finaux, consultez ["Utilisez l'assistant de la console NetApp"](#).

Protégez les identifiants et surveillez l'utilisation du LLM

- Utilisez une clé API dédiée pour l'intégration du déploiement local de Console lorsque cela est possible.
- Renouvelez les clés API conformément à la politique de votre organisation.

- Restreindre la modification des paramètres des outils d'IA aux seuls rôles d'administrateur requis.
- Surveillez l'utilisation des API côté fournisseur et les alertes afin de détecter les activités anormales ou les pics de coûts.

Résoudre les problèmes d'intégration LLM dans le déploiement local de la NetApp Console

Utilisez ce flux de triage rapide pour diagnostiquer et résoudre les problèmes d'intégration LLM courants dans le déploiement local de la NetApp Console.



Cette documentation relative à la connexion d'un LLM à l'assistant Console pour activer les fonctionnalités d'IA est fournie à titre d'aperçu technologique. Dans le cadre de cette offre d'aperçu, NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de cette offre avant sa disponibilité générale.

Si vous n'avez pas terminé la configuration, consultez ["Connectez votre LLM et activez l'assistant NetApp Console"](#).

Résolvez rapidement les problèmes d'intégration LLM

1. Validez la configuration des outils d'IA dans **Administration > Outils d'IA**.

Confirmez le type de fournisseur, l'URL du point de terminaison, la clé API, le modèle sélectionné et l'accès au réseau sortant.

2. Vérifiez la disponibilité de l'assistant sur le tableau de bord.

Confirmez que le bouton **Console assistant** apparaît pour les utilisateurs et organisations attendus.

3. Validez le comportement lors de l'exécution.

Exécutez une simple requête en lecture seule et confirmez l'accessibilité du point de terminaison du fournisseur, la disponibilité du modèle et l'état du service du fournisseur.

Dépanner par symptôme

Symptôme	Cause probable	Que vérifier	Prochaine action
Échec de l'enregistrement ou du test dans AI Tools	Incompatibilité de configuration ou de connectivité	Type de fournisseur, URL du point de terminaison, format de clé API, modèle sélectionné et accès sortant	Corrigez la valeur qui n'est pas validée et enregistrez à nouveau
Le bouton Console assistant est manquant	État d'intégration défaillant, incompatibilité d'organisation ou incompatibilité RBAC	Enregistrement réussi des outils d'IA, état d'intégration, organisation actuelle et rôle d'accès attendu	Actualisez la session et vérifiez avec un compte administrateur valide

Symptôme	Cause probable	Que vérifier	Prochaine action
L'assistant s'ouvre mais la requête échoue	Problème de chemin d'accès au fournisseur ou à l'exécution	Accessibilité du point de terminaison, disponibilité du modèle sur ce point de terminaison, limites du fournisseur et statut temporaire du fournisseur	Réessayez après avoir corrigé les problèmes de correspondance entre l'endpoint/le modèle ou les problèmes de limite côté fournisseur
La réponse de l'assistant est lente ou incohérente	Taille de l'invite, performances du point de terminaison ou instabilité du réseau/proxy	Test rapide, état du service du fournisseur et stabilité du réseau/proxy	Utilisez une invite plus courte, essayez un autre modèle pris en charge et stabilisez le routage réseau ou proxy

Répondez à l'exposition ou à l'utilisation abusive d'un identifiant LLM

Si vous soupçonnez une exposition ou une utilisation non autorisée de la clé API :

1. Révoquez la clé API existante dans votre système fournisseur.
2. Créez une nouvelle clé API.
3. Mettez à jour la clé dans **Administration > Outils d'IA**.
4. Vérifiez la réussite de la reconnexion avec un test d'assistant en lecture seule.

Configurez les canaux de distribution des notifications dans le déploiement local de la NetApp Console

Dans le déploiement local de NetApp Console, vous pouvez configurer plusieurs canaux pour les notifications d'alerte, notamment par e-mail et par webhooks.

Rôles d'accès requis

Super administrateur ou administrateur de l'organisation. ["Découvrez les rôles d'accès"](#).

Par défaut, le déploiement local de la Console affiche les notifications via son système de notifications intégré. La configuration de canaux de diffusion supplémentaires vous permet de recevoir les notifications de la manière la plus adaptée à votre flux de travail.

Vous pouvez envoyer toutes les notifications par les mêmes canaux ou utiliser des canaux différents pour différents types de notifications. Par exemple, vous pouvez envoyer des alertes de stockage urgentes par e-mail tout en acheminant d'autres alertes vers un outil de surveillance tiers via un webhook.

Une fois les canaux de diffusion des notifications configurés, vous pouvez configurer les règles de notification et les affecter à différents canaux. ["Apprenez à configurer les règles de notification"](#).

Configurer un serveur de messagerie

Lorsque vous configurez un serveur de messagerie, le déploiement local de Console envoie des notifications, des alertes et des invitations d'utilisateurs via ce serveur. Le déploiement local de Console prend en charge les serveurs de messagerie SMTP, qu'il s'agisse de votre serveur de messagerie d'entreprise existant ou d'un service de messagerie tiers.

Étapes

1. Sélectionnez **Administration > Console**.
2. Sélectionnez **Configuration** pour ouvrir la page des configurations système.
3. Dans la section **Serveur de messagerie**, sélectionnez **Configurer**.
4. Saisissez les informations de connexion de votre serveur de messagerie :
 - Ajoutez un nom d'expéditeur et une adresse e-mail d'expéditeur.
 - Le **serveur SMTP** : nom d'hôte ou adresse IP de votre serveur SMTP. Pour plusieurs serveurs, indiquez le serveur principal.
 - Sélectionnez le protocole de connexion dans la liste déroulante **Sécurité de la connexion**. Le port est configuré pour vous et est en lecture seule : 25 pour SMTP avec STARTTLS, ou 465 pour SMTPS.

Le protocole SMTPS (port 465) établit immédiatement une connexion chiffrée et est recommandé pour les environnements sensibles à la sécurité. Le protocole STARTTLS (port 25) permet de passer d'une connexion non chiffrée à une connexion chiffrée, mais peut revenir à une transmission non chiffrée si la négociation du chiffrement échoue.

5. Sélectionnez **E-mail de test** pour envoyer un e-mail de test à un destinataire que vous spécifiez.
6. Après la réussite du test, sélectionnez **Enregistrer** pour enregistrer la configuration.

Si le test échoue, revérifiez les paramètres que vous avez saisis et vérifiez que le déploiement local de NetApp Console dispose d'un accès réseau au serveur de messagerie.

Mettre à jour la configuration d'un serveur de messagerie

Vous pouvez mettre à jour la configuration d'un serveur de messagerie existant si vous souhaitez utiliser un serveur de messagerie différent.

Étapes

1. Sélectionnez **Administration > Console**.
2. Sélectionnez **Configuration** pour ouvrir la page des configurations système.
3. Dans la section **Serveur de messagerie**, sélectionnez **Configurer**.
4. Sélectionnez **Effacer les champs** pour effacer la configuration existante.
5. Saisissez les nouvelles informations de connexion pour votre serveur de messagerie.
6. Sélectionnez **E-mail de test** pour envoyer un e-mail de test à un destinataire que vous spécifiez.
7. Après la réussite du test, sélectionnez **Enregistrer** pour enregistrer la nouvelle configuration.

Si le test échoue, revérifiez les paramètres que vous avez saisis et vérifiez que le déploiement local de NetApp Console dispose d'un accès réseau au serveur de messagerie.

Supprimer une configuration de serveur de messagerie

Vous pouvez supprimer la configuration du serveur de messagerie si vous ne souhaitez plus que le déploiement local de Console envoie des e-mails.

Étapes

1. Sélectionnez **Administration > Console**.

2. Sélectionnez **Configuration** pour ouvrir la page de configuration des systèmes.
3. Dans la section **Serveur de messagerie**, sélectionnez **Configurer**.
4. Sélectionnez **Effacer les champs** pour effacer la configuration existante.
5. Sélectionnez **Enregistrer** pour sauvegarder la configuration effacée, ce qui supprime la configuration du serveur de messagerie du déploiement local de NetApp Console.

Configurer un webhook

Configurez des webhooks pour envoyer des notifications depuis le déploiement local de la Console vers d'autres outils ou services. Vous pouvez configurer plusieurs webhooks, chacun pointant vers un point de terminaison différent. Par exemple, un pour un SIEM et un autre pour un service de notification d'astreinte.

Une fois que vous avez créé un webhook, les utilisateurs disposant du rôle Storage admin peuvent l'assigner à des règles d'alerte spécifiques. Par exemple, ils peuvent envoyer les alertes critiques par e-mail tout en envoyant toutes les alertes à un outil de surveillance tiers via un webhook.



Le déploiement local de la Console n'applique aucun contrôle d'accès aux points de terminaison webhook. Tout utilisateur ou système pouvant accéder à l'URL du point de terminaison reçoit les données d'alerte. Assurez-vous que l'accès à l'application de réception est limité aux utilisateurs autorisés via les contrôles d'accès propres à cette application.

Avant de commencer

Vérifiez que le déploiement local de la Console peut atteindre l'application de réception via le réseau et recueillez l'URL du point de terminaison, la méthode HTTP et tous les paramètres d'authentification ou détails de certificat requis par cette application.

Étapes

1. Sélectionnez **Administration > Console**.
2. Sélectionnez **Configuration** pour ouvrir la page des configurations système.
3. Dans la section **Intégration Webhook**, sélectionnez **Configurer**.
4. Saisissez les informations requises pour le webhook :
 - Un nom descriptif pour le webhook.
 - L'URL du point de terminaison fournie par l'application réceptrice.
 - méthode HTTP
 - Facultatif : un certificat auto-signé au format PEM.
 - Tous les en-têtes ou secrets requis (paramètres d'authentification).
 - Format à utiliser pour l'envoi du webhook. Les formats JSON et OTEL (OpenTelemetry) sont pris en charge.

Utilisez JSON pour les webhooks génériques et les points de terminaison REST personnalisés. Utilisez OTEL pour les plateformes d'observabilité qui consomment nativement des signaux OpenTelemetry, telles que Grafana ou d'autres collecteurs compatibles OpenTelemetry.

5. Sélectionnez **Tester le webhook** pour tester la connexion webhook et vous assurer que le déploiement local de Console peut envoyer des messages avec succès à l'application de réception.
6. Une fois le test réussi, sélectionnez **Enregistrer** pour créer le webhook.

Une fois le webhook enregistré, il est disponible pour que les utilisateurs puissent le sélectionner là où les webhooks sont pris en charge, comme les options de diffusion des alertes. "[Apprenez à créer des règles d'alerte et à assigner des webhooks pour la diffusion des alertes.](#)"

Informations sur le copyright

Copyright © 2026 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 DÉLICTELLE (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.