Gérer les comptes

Element Software

NetApp
November 12, 2025

Sommaire

Gérer les comptes

Gérer les comptes

Dans les systèmes de stockage SolidFire , les locataires peuvent utiliser des comptes pour permettre aux clients de se connecter aux volumes d'un cluster. Lorsque vous créez un volume, celui-ci est affecté à un compte spécifique. Vous pouvez également gérer les comptes d'administrateur de cluster pour un système de stockage SolidFire .

- "Travailler avec des comptes utilisant CHAP"
- "Gérer les comptes d'utilisateurs administrateurs du cluster"

Pour plus d'informations

- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Travailler avec des comptes utilisant CHAP

Dans les systèmes de stockage SolidFire , les locataires peuvent utiliser des comptes pour permettre aux clients de se connecter aux volumes d'un cluster. Un compte contient l'authentification par protocole CHAP (Challenge-Handshake Authentication Protocol) requise pour accéder aux volumes qui lui sont attribués. Lorsque vous créez un volume, celui-ci est affecté à un compte spécifique.

Un compte peut se voir attribuer jusqu'à deux mille volumes, mais un volume ne peut appartenir qu'à un seul compte.

Algorithmes CHAP

À partir de l'élément 12.7, les algorithmes CHAP sécurisés conformes à la norme FIPS SHA1, SHA-256 et SHA3-256 sont pris en charge. Lorsqu'un initiateur iSCSI hôte crée une session iSCSI avec une cible iSCSI Element, il demande une liste d'algorithmes CHAP à utiliser. La cible iSCSI Element choisit le premier algorithme qu'elle prend en charge parmi la liste demandée par l'initiateur iSCSI hôte. Pour confirmer que la cible iSCSI Element choisit l'algorithme le plus sécurisé, vous devez configurer l'initiateur iSCSI hôte pour envoyer une liste d'algorithmes classés du plus sécurisé, par exemple SHA3-256, au moins sécurisé, par exemple SHA1 ou MD5. Lorsque les algorithmes SHA ne sont pas demandés par l'initiateur iSCSI hôte, la cible iSCSI Element choisit MD5, en supposant que la liste d'algorithmes proposée par l'hôte contienne MD5. Vous devrez peut-être mettre à jour la configuration de l'initiateur iSCSI hôte pour activer la prise en charge des algorithmes sécurisés.

Lors d'une mise à niveau vers Element 12.7 ou une version ultérieure, si vous avez déjà mis à jour la configuration de l'initiateur iSCSI de l'hôte pour envoyer une requête de session avec une liste incluant les algorithmes SHA, lors du redémarrage des nœuds de stockage, les nouveaux algorithmes sécurisés sont activés et les sessions iSCSI nouvelles ou reconnectées sont établies à l'aide du protocole le plus sécurisé. Toutes les sessions iSCSI existantes passeront de MD5 à SHA lors de la mise à niveau. Si vous ne mettez pas à jour la configuration de l'initiateur iSCSI hôte pour demander SHA, les sessions iSCSI existantes continueront d'utiliser MD5. Ultérieurement, après la mise à jour des algorithmes CHAP de l'initiateur iSCSI hôte, les sessions iSCSI devraient passer progressivement de MD5 à SHA au fil du temps en fonction des

activités de maintenance qui entraînent des reconnexions de session iSCSI.

Par exemple, l'initiateur iSCSI hôte par défaut dans Red Hat Enterprise Linux (RHEL) 8.3 possède le `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5` Le paramètre a été commenté, ce qui a pour conséquence que l'initiateur iSCSI utilise uniquement MD5. Décommenter ce paramètre sur l'hôte et redémarrer l'initiateur iSCSI déclenche l'utilisation de SHA3-256 par les sessions iSCSI de cet hôte.

Si nécessaire, vous pouvez utiliser le "Liste des sessions ISCSI" Méthode API permettant de visualiser les algorithmes CHAP utilisés pour chaque session.

Créer un compte

Vous pouvez créer un compte pour autoriser l'accès aux volumes.

Chaque nom de compte dans le système doit être unique.

1. Sélectionnez **Gestion** > **Comptes**.
2. Cliquez sur **Créer un compte**.
3. Veuillez saisir un **nom d'utilisateur**.
4. Dans la section **Paramètres CHAP**, saisissez les informations suivantes :

   Laissez les champs d'identification vides pour générer automatiquement un mot de passe.

   - **Secret de l'initiateur** pour l'authentification de session du nœud CHAP.
   - **Secret cible** pour l'authentification de session du nœud CHAP.
5. Cliquez sur **Créer un compte**.

Afficher les détails du compte

Vous pouvez consulter les performances de chaque compte sous forme graphique.

Les informations graphiques fournissent des données sur les E/S et le débit du compte. Les niveaux d'activité moyens et de pointe sont affichés par incréments de périodes de rapport de 10 secondes. Ces statistiques incluent l'activité de tous les volumes attribués au compte.

1. Sélectionnez **Gestion** > **Comptes**.
2. Cliquez sur l'icône Actions pour un compte.
3. Cliquez sur **Afficher les détails**.

Voici quelques détails :

- **Statut** : Le statut du compte. Valeurs possibles :
  - actif : Un compte actif.
  - verrouillé : Un compte verrouillé.
  - supprimé : Un compte qui a été supprimé et purgé.
- **Volumes actifs** : Le nombre de volumes actifs attribués au compte.
- **Compression** : Score d'efficacité de la compression pour les volumes attribués au compte.
- **Déduplication** : Score d'efficacité de la déduplication pour les volumes attribués au compte.

- **Provisionnement fin** : Score d'efficacité du provisionnement fin pour les volumes affectés au compte.
- **Efficacité globale** : Score d'efficacité global pour les volumes attribués au compte.

Modifier un compte

Vous pouvez modifier un compte pour en changer le statut, les secrets CHAP ou le nom.

La modification des paramètres CHAP dans un compte ou la suppression d'initiateurs ou de volumes d'un groupe d'accès peut entraîner une perte d'accès inattendue aux volumes pour les initiateurs. Pour éviter toute perte d'accès inattendue aux volumes, déconnectez systématiquement les sessions iSCSI qui seront affectées par une modification de compte ou de groupe d'accès, et vérifiez que les initiateurs peuvent se reconnecter aux volumes une fois les modifications apportées aux paramètres d'initiateur et aux paramètres de cluster terminées.

Les volumes persistants associés aux services de gestion sont affectés à un nouveau compte créé lors de l'installation ou de la mise à niveau. Si vous utilisez des volumes persistants, ne modifiez ni ne supprimez le compte associé.

1. Sélectionnez **Gestion** > **Comptes**.
2. Cliquez sur l'icône Actions pour un compte.
3. Dans le menu qui s'affiche, sélectionnez **Modifier**.
4. **Facultatif :** Modifier le **nom d'utilisateur**.
5. **Facultatif :** Cliquez sur la liste déroulante **Statut** et sélectionnez un autre statut.

   Le passage au statut **verrouillé** met fin à toutes les connexions iSCSI vers le compte, et celui-ci n'est plus accessible. Les volumes associés au compte sont conservés ; cependant, ces volumes ne sont pas détectables via iSCSI.

6. **Facultatif :** Dans les **Paramètres CHAP**, modifiez les informations d'identification **Secret de l'initiateur** et **Secret cible** utilisées pour l'authentification de la session du nœud.

   Si vous ne modifiez pas les informations d'identification **Paramètres CHAP**, elles restent inchangées. Si vous laissez les champs d'identification vides, le système génère de nouveaux mots de passe.

7. Cliquez sur **Enregistrer les modifications**.

Supprimer un compte

Vous pouvez supprimer un compte lorsqu'il n'est plus nécessaire.

Supprimez et purgez tous les volumes associés au compte avant de supprimer le compte.

Les volumes persistants associés aux services de gestion sont affectés à un nouveau compte créé lors de l'installation ou de la mise à niveau. Si vous utilisez des volumes persistants, ne modifiez ni ne supprimez le compte associé.

1. Sélectionnez **Gestion** > **Comptes**.
2. Cliquez sur l'icône Actions du compte que vous souhaitez supprimer.

3. Dans le menu qui s'affiche, sélectionnez **Supprimer**.
4. Confirmez l'action.

Trouver plus d'informations

- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Gérer les comptes d'utilisateurs administrateurs du cluster

Vous pouvez gérer les comptes d'administrateur de cluster pour un système de stockage SolidFire en créant, supprimant et modifiant les comptes d'administrateur de cluster, en changeant le mot de passe de l'administrateur de cluster et en configurant les paramètres LDAP pour gérer l'accès au système pour les utilisateurs.

types de comptes d'administrateur de cluster de stockage

Il existe deux types de comptes d'administrateur pouvant exister dans un cluster de stockage exécutant le logiciel NetApp Element : le compte d'administrateur principal du cluster et un compte d'administrateur de cluster.

- **Compte d'administrateur principal du cluster**

  Ce compte administrateur est créé lors de la création du cluster. Ce compte est le compte d'administration principal disposant du niveau d'accès le plus élevé au cluster. Ce compte est analogue à un utilisateur root dans un système Linux. Vous pouvez modifier le mot de passe de ce compte administrateur.

- **Compte d'administrateur de cluster**

  Vous pouvez accorder à un compte d'administrateur de cluster un accès administratif limité pour effectuer des tâches spécifiques au sein d'un cluster. Les identifiants attribués à chaque compte d'administrateur de cluster sont utilisés pour authentifier les requêtes API et Element UI au sein du système de stockage.

> Un compte d'administrateur de cluster local (non-LDAP) est requis pour accéder aux nœuds actifs d'un cluster via l'interface utilisateur par nœud. Les identifiants de compte ne sont pas nécessaires pour accéder à un nœud qui ne fait pas encore partie d'un cluster.

Afficher les détails de l'administrateur du cluster

1. Pour créer un compte d'administrateur de cluster (non-LDAP) à l'échelle du cluster, procédez comme suit :
   a. Cliquez sur **Utilisateurs** > **Administrateurs du cluster**.
2. Sur la page Administrateurs du cluster de l'onglet Utilisateurs, vous pouvez consulter les informations suivantes.
   - **ID** : Numéro séquentiel attribué au compte d'administrateur du cluster.
   - **Nom d'utilisateur** : Le nom donné au compte d'administrateur du cluster lors de sa création.
   - **Accès** : Les autorisations attribuées au compte utilisateur. Valeurs possibles :
     - lire

- reportage
- nœuds
- lecteurs
- volumes
- comptes
- Administrateurs de cluster
- administrateur
- supportAdmin

> Toutes les autorisations sont disponibles pour le type d'accès administrateur.
>
> Certains types d'accès disponibles via l'API ne sont pas disponibles dans l'interface utilisateur d'Element.

+

- **Type** : Le type d'administrateur de cluster. Valeurs possibles :
  - Cluster
  - LDAP
- **Attributs** : Si le compte d'administrateur du cluster a été créé à l'aide de l'API Element, cette colonne affiche toutes les paires nom-valeur définies à l'aide de cette méthode.

  Voir"Référence de l'API du logiciel NetApp Element" .

Créer un compte d'administrateur de cluster

Vous pouvez créer de nouveaux comptes d'administrateur de cluster avec des autorisations permettant d'autoriser ou de restreindre l'accès à des zones spécifiques du système de stockage. Lorsque vous définissez les autorisations du compte d'administrateur de cluster, le système accorde des droits de lecture seule pour toutes les autorisations que vous n'attribuez pas à l'administrateur de cluster.

Si vous souhaitez créer un compte d'administrateur de cluster LDAP, assurez-vous que LDAP est configuré sur le cluster avant de commencer.

"Activez l'authentification LDAP avec l'interface utilisateur Element."

Vous pourrez ultérieurement modifier les privilèges du compte d'administrateur de cluster pour la génération de rapports, les nœuds, les lecteurs, les volumes, les comptes et l'accès au niveau du cluster. Lorsque vous activez une autorisation, le système attribue un accès en écriture pour ce niveau. Le système accorde à l'utilisateur administrateur un accès en lecture seule pour les niveaux que vous ne sélectionnez pas.

Vous pouvez également supprimer ultérieurement tout compte utilisateur d'administrateur de cluster créé par un administrateur système. Vous ne pouvez pas supprimer le compte d'administrateur principal du cluster qui a été créé lors de la création du cluster.

1. Pour créer un compte d'administrateur de cluster (non-LDAP) à l'échelle du cluster, procédez comme suit :
   a. Cliquez sur **Utilisateurs** > **Administrateurs du cluster**.
   b. Cliquez sur **Créer un administrateur de cluster**.

c. Sélectionnez le type d'utilisateur **Cluster**.

d. Saisissez un nom d'utilisateur et un mot de passe pour le compte, puis confirmez le mot de passe.

e. Sélectionnez les autorisations utilisateur à appliquer au compte.

f. Cochez la case pour accepter le contrat de licence utilisateur final.

g. Cliquez sur **Créer un administrateur de cluster**.

2. Pour créer un compte d'administrateur de cluster dans l'annuaire LDAP, procédez comme suit :

a. Cliquez sur **Cluster** > **LDAP**.

b. Assurez-vous que l'authentification LDAP est activée.

c. Cliquez sur **Tester l'authentification de l'utilisateur** et copiez le nom distinctif qui apparaît pour l'utilisateur ou l'un des groupes dont il est membre afin de pouvoir le coller ultérieurement.

d. Cliquez sur **Utilisateurs** > **Administrateurs du cluster**.

e. Cliquez sur **Créer un administrateur de cluster**.

f. Sélectionnez le type d'utilisateur LDAP.

g. Dans le champ Nom distinctif, suivez l'exemple de la zone de texte pour saisir un nom distinctif complet pour l'utilisateur ou le groupe. Vous pouvez aussi le coller à partir du nom distinctif que vous avez copié précédemment.

Si le nom distinctif fait partie d'un groupe, alors tout utilisateur membre de ce groupe sur le serveur LDAP disposera des autorisations de ce compte administrateur.

Pour ajouter des utilisateurs ou des groupes d'administrateurs de cluster LDAP, le format général du nom d'utilisateur est « `LDAP:<Nom distinctif complet>` ».

a. Sélectionnez les autorisations utilisateur à appliquer au compte.

b. Cochez la case pour accepter le contrat de licence utilisateur final.

c. Cliquez sur **Créer un administrateur de cluster**.

Modifier les autorisations d'administrateur du cluster

Vous pouvez modifier les privilèges du compte d'administrateur de cluster pour la génération de rapports, les nœuds, les lecteurs, les volumes, les comptes et l'accès au niveau du cluster. Lorsque vous activez une autorisation, le système attribue un accès en écriture pour ce niveau. Le système accorde à l'utilisateur administrateur un accès en lecture seule pour les niveaux que vous ne sélectionnez pas.

1. Cliquez sur **Utilisateurs** > **Administrateurs du cluster**.
2. Cliquez sur l'icône Actions correspondant à l'administrateur du cluster que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. Sélectionnez les autorisations utilisateur à appliquer au compte.
5. Cliquez sur **Enregistrer les modifications**.

Modifier les mots de passe des comptes d'administrateur de cluster

Vous pouvez utiliser l'interface utilisateur Element pour modifier les mots de passe des administrateurs de cluster.

1. Cliquez sur **Utilisateurs** > **Administrateurs du cluster**.
2. Cliquez sur l'icône Actions correspondant à l'administrateur du cluster que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. Dans le champ « Changer le mot de passe », saisissez un nouveau mot de passe et confirmez-le.
5. Cliquez sur **Enregistrer les modifications**.

Informations connexes

- "Découvrez les types d'accès disponibles pour les API Element."
- "Activez l'authentification LDAP avec l'interface utilisateur Element."
- "Désactiver LDAP"
- "Module d'extension NetApp Element pour vCenter Server"

Gérer les LDAP

Vous pouvez configurer le protocole LDAP (Lightweight Directory Access Protocol) pour activer une fonctionnalité de connexion sécurisée basée sur un annuaire au stockage SolidFire . Vous pouvez configurer LDAP au niveau du cluster et autoriser les utilisateurs et les groupes LDAP.

La gestion du protocole LDAP implique la configuration de l'authentification LDAP auprès d'un cluster SolidFire à l'aide d'un environnement Microsoft Active Directory existant et le test de cette configuration.

Vous pouvez utiliser les adresses IPv4 et IPv6.

L'activation de LDAP implique les étapes générales suivantes, décrites en détail :

1. **Étapes complètes de préconfiguration pour la prise en charge LDAP**. Vérifiez que vous disposez de toutes les informations nécessaires à la configuration de l'authentification LDAP.
2. **Activer l'authentification LDAP**. Utilisez soit l'interface utilisateur d'Element, soit l'API d'Element.
3. **Valider la configuration LDAP**. Vous pouvez également vérifier que le cluster est configuré avec les valeurs correctes en exécutant la méthode API GetLdapConfiguration ou en vérifiant la configuration LCAP à l'aide de l'interface utilisateur Element.
4. **Testez l'authentification LDAP** (avec le `readonly` utilisateur). Vérifiez que la configuration LDAP est correcte soit en exécutant la méthode API TestLdapAuthentication, soit en utilisant l'interface utilisateur Element. Pour ce test initial, utilisez le nom d'utilisateur « `sAMAccountName` » du `readonly` utilisateur. Cela permettra de vérifier que votre cluster est correctement configuré pour l'authentification LDAP et de valider également que le `readonly` Les identifiants et l'accès sont corrects. Si cette étape échoue, répétez les étapes 1 à 3.
5. **Testez l'authentification LDAP** (avec un compte utilisateur que vous souhaitez ajouter). Répétez l'étape 4 avec un compte utilisateur que vous souhaitez ajouter en tant qu'administrateur du cluster Element. Copiez le `distinguished` nom (DN) ou l'utilisateur (ou le groupe). Ce DN sera utilisé à l'étape 6.
6. **Ajoutez l'administrateur du cluster LDAP** (copiez et collez le DN de l'étape de test d'authentification LDAP). Créez un nouvel utilisateur administrateur de cluster avec le niveau d'accès approprié, soit via l'interface utilisateur Element, soit via la méthode API AddLdapClusterAdmin. Pour le nom d'utilisateur, collez le DN complet que vous avez copié à l'étape 5. Cela garantit que le DN est correctement formaté.
7. **Tester l'accès administrateur du cluster**. Connectez-vous au cluster en utilisant l'utilisateur

administrateur du cluster LDAP nouvellement créé. Si vous avez ajouté un groupe LDAP, vous pouvez vous connecter en tant que n'importe quel utilisateur appartenant à ce groupe.

Étapes complètes de préconfiguration pour la prise en charge LDAP

Avant d'activer la prise en charge LDAP dans Element, vous devez configurer un serveur Active Directory Windows et effectuer d'autres tâches de préconfiguration.

Étapes

1. Configurer un serveur Active Directory Windows.
2. **Facultatif :** Activer la prise en charge LDAPS.
3. Créer des utilisateurs et des groupes.
4. Créez un compte de service en lecture seule (tel que « `sfreadonly` ») à utiliser pour la recherche dans l'annuaire LDAP.

Activez l'authentification LDAP avec l'interface utilisateur Element.

Vous pouvez configurer l'intégration du système de stockage avec un serveur LDAP existant. Cela permet aux administrateurs LDAP de gérer de manière centralisée l'accès des utilisateurs au système de stockage.

Vous pouvez configurer LDAP soit avec l'interface utilisateur d'Element, soit avec l'API d'Element. Cette procédure décrit comment configurer LDAP à l'aide de l'interface utilisateur Element.

Cet exemple montre comment configurer l'authentification LDAP sur SolidFire et l'utilise `SearchAndBind` comme type d'authentification. L'exemple utilise un seul serveur Active Directory Windows Server 2012 R2.

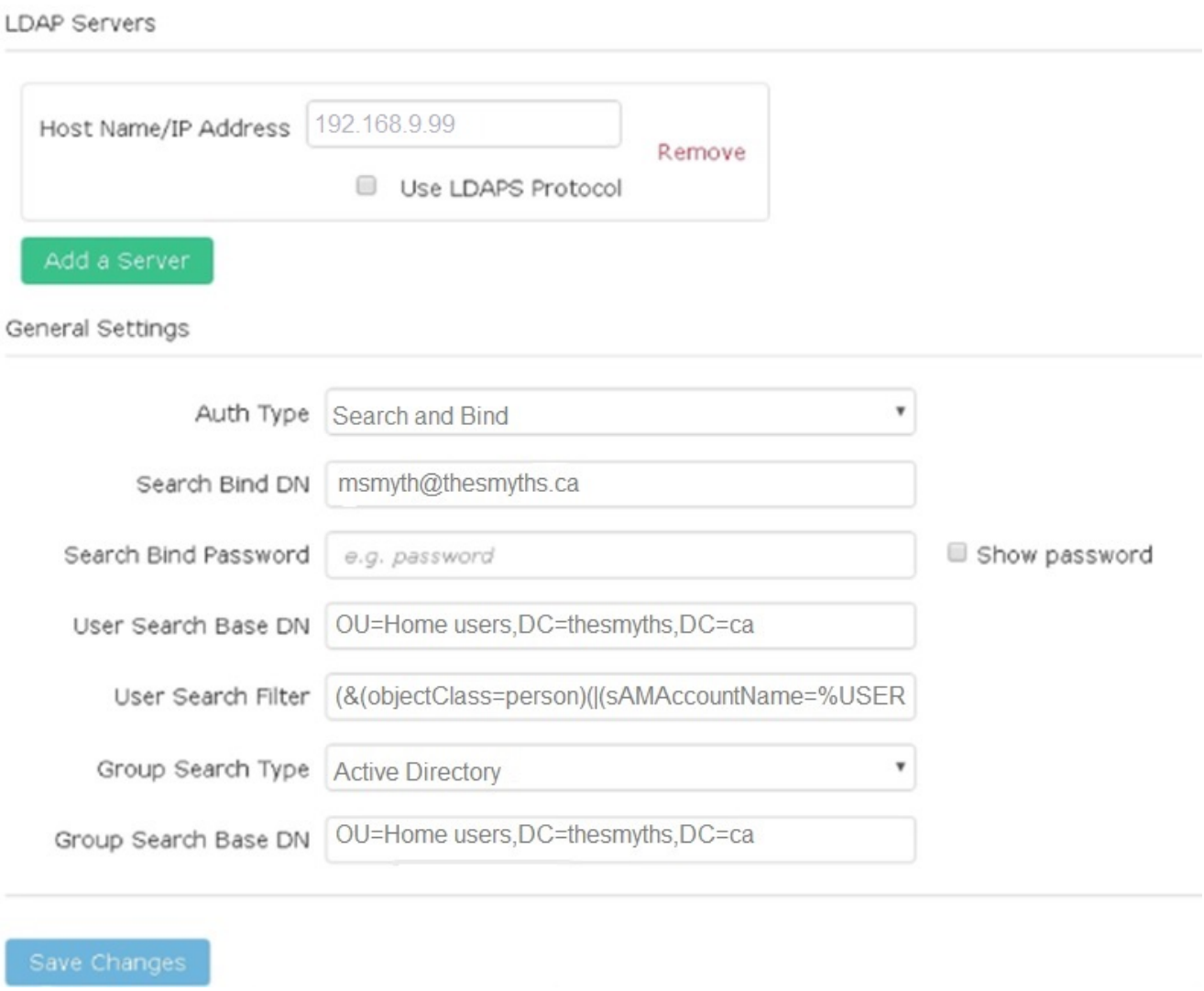
Étapes

1. Cliquez sur **Cluster** > **LDAP**.
2. Cliquez sur **Oui** pour activer l'authentification LDAP.
3. Cliquez sur **Ajouter un serveur**.
4. Saisissez le **nom d'hôte/l'adresse IP**.

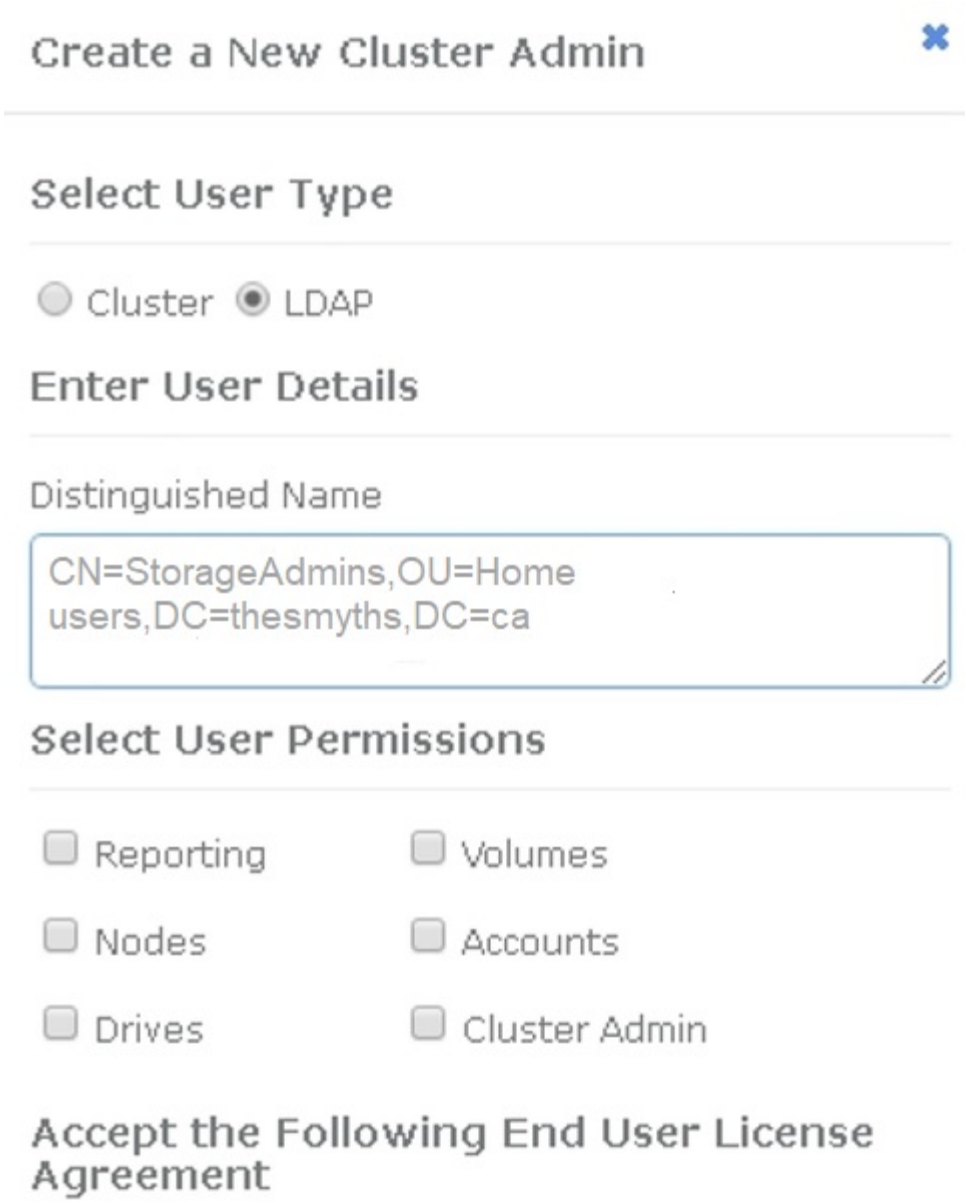
   Il est également possible de saisir un numéro de port personnalisé facultatif.

   Par exemple, pour ajouter un numéro de port personnalisé, saisissez <nom d'hôte ou adresse IP>:<numéro de port>

5. **Facultatif :** Sélectionnez **Utiliser le protocole LDAPS**.
6. Saisissez les informations requises dans **Paramètres généraux**.



7. Cliquez sur **Activer LDAP**.
8. Cliquez sur **Tester l'authentification de l'utilisateur** si vous souhaitez tester l'accès au serveur pour un utilisateur.
9. Copiez le nom distinctif et les informations du groupe d'utilisateurs qui apparaissent pour une utilisation ultérieure lors de la création d'administrateurs de cluster.
10. Cliquez sur **Enregistrer les modifications** pour enregistrer les nouveaux paramètres.
11. Pour créer un utilisateur dans ce groupe afin que n'importe qui puisse se connecter, veuillez procéder comme suit :
    a. Cliquez sur **Utilisateur** > **Afficher**.



b. Pour le nouvel utilisateur, cliquez sur **LDAP** pour le type d'utilisateur, puis collez le groupe que vous avez copié dans le champ Nom distinctif.
c. Sélectionnez les autorisations, généralement toutes les autorisations.
d. Faites défiler vers le bas jusqu'au Contrat de licence utilisateur final et cliquez sur **J'accepte**.
e. Cliquez sur **Créer un administrateur de cluster**.

   Vous disposez désormais d'un utilisateur ayant la valeur d'un groupe Active Directory.

Pour tester cela, déconnectez-vous de l'interface utilisateur d'Element et reconnectez-vous en tant qu'utilisateur de ce groupe.

Activez l'authentification LDAP avec l'API Element

Vous pouvez configurer l'intégration du système de stockage avec un serveur LDAP existant. Cela permet aux administrateurs LDAP de gérer de manière centralisée l'accès des utilisateurs au système de stockage.

Vous pouvez configurer LDAP soit avec l'interface utilisateur d'Element, soit avec l'API d'Element. Cette procédure décrit comment configurer LDAP à l'aide de l'API Element.

Pour utiliser l'authentification LDAP sur un cluster SolidFire , vous devez d'abord activer l'authentification LDAP sur le cluster à l'aide de `EnableLdapAuthentication` Méthode API.

Étapes

1. Activez d'abord l'authentification LDAP sur le cluster à l'aide de `EnableLdapAuthentication` Méthode API.
2. Veuillez saisir les informations requises.

```
{
     "method":"EnableLdapAuthentication",
     "params":{
          "authType": "SearchAndBind",
          "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
          "groupSearchType": "ActiveDirectory",
          "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
          "searchBindPassword": "ReadOnlyPW",
          "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
          "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
          "serverURIs": [
               "ldap://172.27.1.189",
          [
     },
  "id":"1"
}
```

3. Modifiez les valeurs des paramètres suivants :

Paramètres utilisés	Description
authType: SearchAndBind	Indique que le cluster utilisera le compte de service en lecture seule pour rechercher d'abord l'utilisateur à authentifier, puis pour lier cet utilisateur s'il est trouvé et authentifié.
groupSearchBaseDN : dc=prodtest,dc=solidfire,dc=net	Spécifie l'emplacement dans l'arborescence LDAP où commencer la recherche de groupes. Pour cet exemple, nous avons utilisé la racine de notre arbre. Si votre arborescence LDAP est très volumineuse, vous pouvez envisager de définir une sous-arborescence plus fine afin de réduire les temps de recherche.

Paramètres utilisés	Description
userSearchBaseDN : dc=prodtest,dc=solidfire,dc=net	Spécifie l'emplacement dans l'arborescence LDAP où commencer la recherche des utilisateurs. Pour cet exemple, nous avons utilisé la racine de notre arbre. Si votre arborescence LDAP est très volumineuse, vous pouvez envisager de définir une sous-arborescence plus fine afin de réduire les temps de recherche.
groupSearchType : ActiveDirectory	Utilise le serveur Active Directory Windows comme serveur LDAP.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Pour utiliser l'utilisateur principal (adresse e-mail de connexion), vous pouvez modifier l'utilisateurSearchFilter comme suit :
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
Ou, pour rechercher à la fois userPrincipalName et sAMAccountName, vous pouvez utiliser le filtre userSearchFilter suivant :
 	
`"(&(objectClass=person)(`
	(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))" ----

Utilise le sAMAccountName comme nom d'utilisateur pour se connecter au cluster SolidFire . Ces paramètres indiquent à LDAP de rechercher le nom d'utilisateur spécifié lors de la connexion dans l'attribut sAMAccountName et limitent également la recherche aux entrées qui ont « personne » comme valeur dans l'attribut objectClass.	searchBindDN
Il s'agit du nom distinctif de l'utilisateur en lecture seule qui sera utilisé pour effectuer la recherche dans l'annuaire LDAP. Pour Active Directory, il est généralement plus simple d'utiliser l'identifiant utilisateur principal (format adresse e-mail) pour l'utilisateur.	rechercherLierMotDePasse

Pour tester cela, déconnectez-vous de l'interface utilisateur d'Element et reconnectez-vous en tant

qu'utilisateur de ce groupe.

Afficher les détails du LDAP

Consultez les informations LDAP sur la page LDAP, dans l'onglet Cluster.

Vous devez activer LDAP pour afficher ces paramètres de configuration LDAP.

1. Pour afficher les détails LDAP avec l'interface utilisateur Element, cliquez sur **Cluster** > **LDAP**.
   - **Nom d'hôte/Adresse IP** : Adresse d'un serveur d'annuaire LDAP ou LDAPS.
   - **Type d'authentification** : Méthode d'authentification de l'utilisateur. Valeurs possibles :
     - Liaison directe
     - Recherche et liaison
   - **DN de liaison de recherche** : DN complet permettant de se connecter pour effectuer une recherche LDAP pour l'utilisateur (nécessite un accès de niveau liaison à l'annuaire LDAP).
   - **Mot de passe de liaison de recherche** : Mot de passe utilisé pour authentifier l'accès au serveur LDAP.
   - **DN de base de la recherche utilisateur** : Le DN de base de l'arbre utilisé pour démarrer la recherche utilisateur. Le système effectue une recherche dans le sous-arbre à partir de l'emplacement spécifié.
   - **Filtre de recherche utilisateur** : Saisissez ce qui suit en utilisant votre nom de domaine :

     ```
     (&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))
     ```

   - **Type de recherche de groupe** : Type de recherche qui contrôle le filtre de recherche de groupe par défaut utilisé. Valeurs possibles :
     - Active Directory : Appartenance imbriquée à tous les groupes LDAP d'un utilisateur.
     - Pas de groupes : aucun soutien de groupe.
     - Membre DN : Groupes de type Membre DN (à un seul niveau).
   - **DN de base pour la recherche de groupe** : Le DN de base de l'arbre utilisé pour démarrer la recherche de groupe. Le système effectue une recherche dans le sous-arbre à partir de l'emplacement spécifié.
   - **Test d'authentification utilisateur** : Une fois LDAP configuré, utilisez cette procédure pour tester l'authentification par nom d'utilisateur et mot de passe du serveur LDAP. Saisissez un compte existant pour tester ceci. Le nom distinctif et les informations du groupe d'utilisateurs s'affichent ; vous pouvez les copier pour une utilisation ultérieure lors de la création d'administrateurs de cluster.

Tester la configuration LDAP

Après avoir configuré LDAP, vous devez le tester en utilisant soit l'interface utilisateur d'Element, soit l'API d'Element. `TestLdapAuthentication` méthode.

Étapes

1. Pour tester la configuration LDAP avec l'interface utilisateur Element, procédez comme suit :
   a. Cliquez sur **Cluster** > **LDAP**.
   b. Cliquez sur **Tester l'authentification LDAP**.

c. Résolvez tout problème en utilisant les informations du tableau ci-dessous :

Message d'erreur	Description
`xLDAPUserNotFound`	• L'utilisateur testé est introuvable dans la configuration. `userSearchBaseDN` sous-arbre. • Le `userSearchFilter` est mal configuré.
`xLDAPBindFailed (Error: Invalid credentials)`	• Le nom d'utilisateur testé est un utilisateur LDAP valide, mais le mot de passe fourni est incorrect. • Le nom d'utilisateur testé est un utilisateur LDAP valide, mais le compte est actuellement désactivé.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	L'URI du serveur LDAP est incorrect.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	Le nom d'utilisateur ou le mot de passe en lecture seule est mal configuré.
`xLDAPSearchFailed (Error: No such object)`	Le `userSearchBaseDN` n'est pas un emplacement valide dans l'arborescence LDAP.
`xLDAPSearchFailed (Error: Referral)`	• Le `userSearchBaseDN` n'est pas un emplacement valide dans l'arborescence LDAP. • Le `userSearchBaseDN` et `groupSearchBaseDN` sont dans une unité organisationnelle imbriquée. Cela peut entraîner des problèmes d'autorisation. La solution de contournement consiste à inclure l'unité organisationnelle dans les entrées DN de base de l'utilisateur et du groupe (par exemple : `ou=storage, cn=company, cn=com`)

2. Pour tester la configuration LDAP avec l'API Element, procédez comme suit :
   a. Appelez la méthode TestLdapAuthentication.

```
{
  "method":"TestLdapAuthentication",
     "params":{
        "username":"admin1",
        "password":"admin1PASS
      },
      "id": 1
}
```

b. Examinez les résultats. Si l'appel API réussit, les résultats incluent le nom distinctif de l'utilisateur spécifié et une liste des groupes dont l'utilisateur est membre.

```
{
"id": 1
     "result": {
         "groups": [

"CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
         ],
         "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
     }
}
```

Désactiver LDAP

Vous pouvez désactiver l'intégration LDAP via l'interface utilisateur d'Element.

Avant de commencer, vous devez noter tous les paramètres de configuration, car la désactivation de LDAP efface tous les paramètres.

Étapes

1. Cliquez sur **Cluster** > **LDAP**.
2. Cliquez sur **Non**.
3. Cliquez sur **Désactiver LDAP**.

Trouver plus d'informations

- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Informations sur le copyright

Informations sur les marques commerciales