Gestion des comptes

Element Software

NetApp
October 01, 2024

Sommaire

Gestion des 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, il 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 à l'aide du protocole CHAP"
- "Gérez les comptes utilisateurs d'administrateur du cluster"

Pour en savoir plus

- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Travailler avec des comptes à l'aide du protocole 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 CHAP (Challenge-Handshake Authentication Protocol) requise pour accéder aux volumes qui lui sont affectés. Lorsque vous créez un volume, il est affecté à un compte spécifique.

Un compte peut comporter jusqu'à deux milliers de volumes qui lui sont attribués, mais un volume ne peut appartenir qu'à un seul compte.

Algorithmes CHAP

Depuis Element 12.7, les algorithmes CHAP sécurisés conformes à la norme FIPS SHA1, SHA-256 et SHA3-256 sont pris en charge. Avec l'élément 12.7, lorsqu'un initiateur iSCSI hôte crée une session iSCSI avec une cible iSCSI Element, il demande la liste des algorithmes CHAP à utiliser. La cible iSCSI de l'élément choisit le premier algorithme qu'il prend en charge dans la liste demandée par l'initiateur iSCSI de l'hôte. Pour confirmer que la cible iSCSI de l'élément choisit l'algorithme le plus sécurisé, vous devez configurer l'initiateur iSCSI hôte pour qu'il envoie une liste d'algorithmes ordonnés de MOST Secure, par exemple, SHA3-256, pour le moins sécuriser, par exemple, SHA1 ou MD5. Lorsque les algorithmes SHA ne sont pas demandés par l'initiateur iSCSI hôte, la cible iSCSI de l'élément choisit MD5, en supposant que la liste d'algorithmes proposée par l'hôte contient 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 d'Element 12.7, si vous avez déjà mis à jour la configuration de l'initiateur iSCSI hôte afin d'envoyer une demande de session avec une liste incluant des algorithmes SHA, au redémarrage des nœuds de stockage, Les nouveaux algorithmes sécurisés sont activés et les nouvelles sessions iSCSI ou les sessions reconnectées sont établies à l'aide du protocole le plus sécurisé. Toutes les sessions iSCSI existantes passent de MD5 à SHA pendant la mise à niveau. Si vous ne mettez pas à jour la configuration de l'initiateur iSCSI hôte pour demander le SHA, les sessions iSCSI existantes continueront à utiliser MD5. À une date ultérieure, après la mise à jour des algorithmes CHAP de l'initiateur iSCSI de l'hôte, les sessions iSCSI devraient passer progressivement de MD5 à SHA au fil du temps en fonction des activités de maintenance qui entraînent une reconnexion de session iSCSI.

Par exemple, l'initiateur iSCSI de l'hôte par défaut dans Red Hat Enterprise Linux (RHEL) 8.3 a le `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5` paramètre commenté, ce qui fait que l'initiateur iSCSI n'utilise que MD5. Annuler la suppression de ce paramètre sur l'hôte et redémarrer l'initiateur iSCSI déclenche des sessions iSCSI à partir de cet hôte pour démarrer l'utilisation de SHA3-256.

Si nécessaire, vous pouvez utiliser la "ListISCSISessions" méthode API pour voir les algorithmes CHAP utilisés pour chaque session.

Créez 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. Saisissez un **Nom d'utilisateur**.
4. Dans la section **CHAP Settings**, entrez les informations suivantes :

   Laissez les champs d'informations d'identification vides pour générer automatiquement l'un ou l'autre des mots de passe.

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

Afficher les détails du compte

Vous pouvez afficher l'activité de performances des comptes individuels dans un format graphique.

Le graphique fournit des informations d'E/S et de débit pour le compte. Les niveaux d'activité moyenne et maximale sont indiqués par incréments de périodes de déclaration de 10 secondes. Ces statistiques comprennent l'activité de tous les volumes affectés au compte.

1. Sélectionnez **gestion** > **comptes**.
2. Cliquez sur l'icône actions d'un compte.
3. Cliquez sur **Afficher les détails**.

Voici quelques-uns des détails :

- **Statut** : état du compte. Valeurs possibles :
  - Active : un compte actif.
  - Verrouillé : un compte verrouillé.
  - Supprimé : compte supprimé et purgé.
- **Volumes actifs** : nombre de volumes actifs affectés au compte.
- **Compression** : le score d'efficacité de compression pour les volumes affectés au compte.
- **Déduplication** : score d'efficacité de la déduplication pour les volumes affectés au compte.

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

Modifier un compte

Vous pouvez modifier un compte pour modifier son statut, modifier les secrets CHAP ou modifier le nom du compte.

La modification des paramètres CHAP d'un compte ou la suppression d'initiateurs ou de volumes d'un groupe d'accès peut entraîner une perte inattendue de l'accès aux volumes. Pour vérifier que l'accès au volume ne sera pas perdu de façon inattendue, déconnectez toujours les sessions iSCSI qui seront affectées par une modification de compte ou de groupe d'accès. Vérifiez également que les initiateurs peuvent se reconnecter aux volumes après la modification des paramètres de l'initiateur et des paramètres du cluster.

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

1. Sélectionnez **gestion** > **comptes**.
2. Cliquez sur l'icône actions d'un compte.
3. Dans le menu qui s'affiche, sélectionnez **Modifier**.
4. **Facultatif:** modifiez le **Nom d'utilisateur**.
5. **Facultatif :** cliquez sur la liste déroulante **Statut** et sélectionnez un autre état.

   Si vous changez l'état à **Locked**, toutes les connexions iSCSI au compte sont résiliées et le compte n'est plus accessible. Les volumes associés au compte sont conservés, mais ils ne sont pas détectables iSCSI.

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

   Si vous ne modifiez pas les informations d'identification **CHAP Settings**, elles restent les mêmes. Si vous ne renseignez pas les champs d'informations d'identification, 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 supprimez tous les volumes associés au compte avant de supprimer le compte.

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

1. Sélectionnez **gestion** > **comptes**.
2. Cliquez sur l'icône actions du compte à supprimer.

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

Trouvez plus d'informations

- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Gérez les comptes utilisateurs d'administrateur du cluster

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

Types de compte d'administrateur du cluster de stockage

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

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

  Ce compte administrateur est créé lors de la création du cluster. Il s'agit du compte administratif principal avec le niveau d'accès le plus élevé au cluster. Ce compte est similaire à un utilisateur root dans un système Linux. Vous pouvez modifier le mot de passe de ce compte administrateur.

- **Compte administrateur de cluster**

  Vous pouvez donner à un administrateur de cluster une plage limitée d'accès administratif afin d'effectuer des tâches spécifiques au sein d'un cluster. Les identifiants attribués à chaque compte d'administrateur du cluster sont utilisés pour authentifier les demandes d'interface utilisateur d'API et d'éléments du système de stockage.

> Un compte d'administrateur de cluster local (non LDAP) est nécessaire 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 à l'échelle du cluster (non LDAP), effectuez les opérations suivantes :
   a. Cliquez sur **utilisateurs** > **administrateurs de cluster**.
2. Sur la page administrateurs de cluster de l'onglet utilisateurs, vous pouvez afficher les informations suivantes.
   - **ID** : numéro séquentiel attribué au compte administrateur de cluster.
   - **Nom d'utilisateur** : nom donné au compte administrateur de cluster lors de sa création.
   - **Accès** : les autorisations d'utilisateur attribuées au compte d'utilisateur. Valeurs possibles :

- lecture
- création de rapports
- nœuds
- disques
- volumes
- comptes
- ClusterAdmins
- administrateur
- SupportAdmin

> Toutes les autorisations sont disponibles pour le type d'accès administrateur.

- **Type** : le type d'administrateur de cluster. Valeurs possibles :
  - Cluster
  - LDAP
- **Attributes** : si le compte administrateur de cluster a été créé à l'aide de l'API d'élément, cette colonne affiche toutes les paires nom-valeur qui ont été définies à l'aide de cette méthode.

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

Créez un compte d'administrateur de cluster

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

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

"Activez l'authentification LDAP à l'aide de l'interface utilisateur Element"

Vous pouvez modifier ultérieurement les privilèges du compte administrateur du cluster pour les rapports, les nœuds, les disques, les volumes, les comptes, et l'accès au niveau du cluster. Lorsque vous activez une autorisation, le système attribue un accès en écriture à 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 tout compte utilisateur 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 à l'échelle du cluster (non LDAP), effectuez les opérations suivantes :
   a. Cliquez sur **utilisateurs** > **administrateurs de cluster**.
   b. Cliquez sur **Créer un administrateur de cluster**.
   c. Sélectionnez le type d'utilisateur **Cluster**.
   d. Entrez un nom d'utilisateur et un mot de passe pour le compte et confirmez le mot de passe.

e. Sélectionnez les autorisations utilisateur à appliquer au compte.

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

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

2. Pour créer un compte d'administrateur de cluster dans le répertoire LDAP, effectuez les opérations suivantes :

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

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

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

   d. Cliquez sur **utilisateurs** > **administrateurs de cluster**.

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

   f. Sélectionnez le type d'utilisateur LDAP.

   g. Dans le champ Nom unique, suivez l'exemple de la zone de texte pour entrer un nom distinctif complet pour l'utilisateur ou le groupe. Vous pouvez également 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 aura les autorisations de ce compte d'administrateur.

   Pour ajouter des utilisateurs ou des groupes LDAP Cluster Admin, le format général du nom d'utilisateur est « LDAP:<Nom unique complet> ».

   a. Sélectionnez les autorisations utilisateur à appliquer au compte.

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

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

Modifiez les autorisations d'administrateur de cluster

Vous pouvez modifier les privilèges du compte administrateur du cluster pour les comptes de rapports, les nœuds, les disques, les volumes, les comptes, et l'accès au niveau du cluster. Lorsque vous activez une autorisation, le système attribue un accès en écriture à 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 de cluster**.
2. Cliquez sur l'icône actions de l'administrateur de 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 du cluster

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

1. Cliquez sur **utilisateurs** > **administrateurs de cluster**.
2. Cliquez sur l'icône actions de l'administrateur de cluster que vous souhaitez modifier.

3. Cliquez sur **Modifier**.
4. Dans le champ Modifier le mot de passe, saisissez un nouveau mot de passe et confirmez-le.
5. Cliquez sur **Enregistrer les modifications**.

Trouvez plus d'informations

- "Activez l'authentification LDAP à l'aide de l'interface utilisateur Element"
- "Désactiver LDAP"
- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Gérer LDAP

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

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

Vous pouvez utiliser les adresses IPv4 et IPv6.

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

1. **Effectuer les étapes de pré-configuration pour la prise en charge du protocole LDAP**. Vérifiez que vous disposez de tous les détails nécessaires à la configuration de l'authentification LDAP.
2. **Activer l'authentification LDAP**. Utilisez l'interface utilisateur Element ou l'API Element.
3. **Valider la configuration LDAP**. Vous pouvez également vérifier que le cluster est configuré avec les valeurs correctes en exécutant la méthode GetLdapConfiguration API ou en vérifiant la configuration LCAP à l'aide de l'interface utilisateur Element.
4. **Testez l'authentification LDAP** (avec l' `readonly`utilisateur). Vérifiez que la configuration LDAP est correcte soit en exécutant la méthode TestLdapAuthentication API soit en utilisant l'interface utilisateur Element. Pour ce test initial, utilisez le nom d'utilisateur "`NomAccount'' de l' `readonly`utilisateur. Cela permet de vérifier que votre cluster est correctement configuré pour l'authentification LDAP et de vérifier que les `readonly` identifiants et l'accès sont corrects. Si cette étape échoue, répétez les étapes 1 à 3.
5. **Tester l'authentification LDAP** (avec un compte utilisateur que vous souhaitez ajouter). Répétez setp 4 avec un compte utilisateur que vous souhaitez ajouter en tant qu'administrateur de cluster Element. Copiez le `distinguished` nom (DN) ou l'utilisateur (ou le groupe). Ce DN sera utilisé à l'étape 6.
6. **Ajouter le cluster LDAP admin** (copiez et collez le DN à partir de l'étape d'authentification LDAP de test). En utilisant soit l'interface utilisateur Element soit la méthode de l'API AddapClusterAdmin, créez un nouvel utilisateur administrateur cluster avec le niveau d'accès approprié. Pour le nom d'utilisateur, collez le nom d'utilisateur complet que vous avez copié à l'étape 5. Cela garantit que le DN est correctement formaté.
7. **Tester l'accès admin du cluster**. Connectez-vous au cluster à l'aide du nouvel utilisateur administrateur de cluster LDAP. Si vous avez ajouté un groupe LDAP, vous pouvez vous connecter en tant qu'utilisateur

de ce groupe.

Suivez les étapes de pré-configuration pour la prise en charge du protocole LDAP

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

Étapes

1. Configurer un serveur Windows Active Directory.
2. **Facultatif:** activez 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 à l'aide de l'interface utilisateur Element

Vous pouvez configurer l'intégration du système de stockage avec un serveur LDAP existant. Les administrateurs LDAP peuvent ainsi gérer de façon centralisée l'accès au système de stockage pour les utilisateurs.

Vous pouvez configurer LDAP à l'aide de l'interface utilisateur Element ou de l'API Element. Cette procédure explique 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.

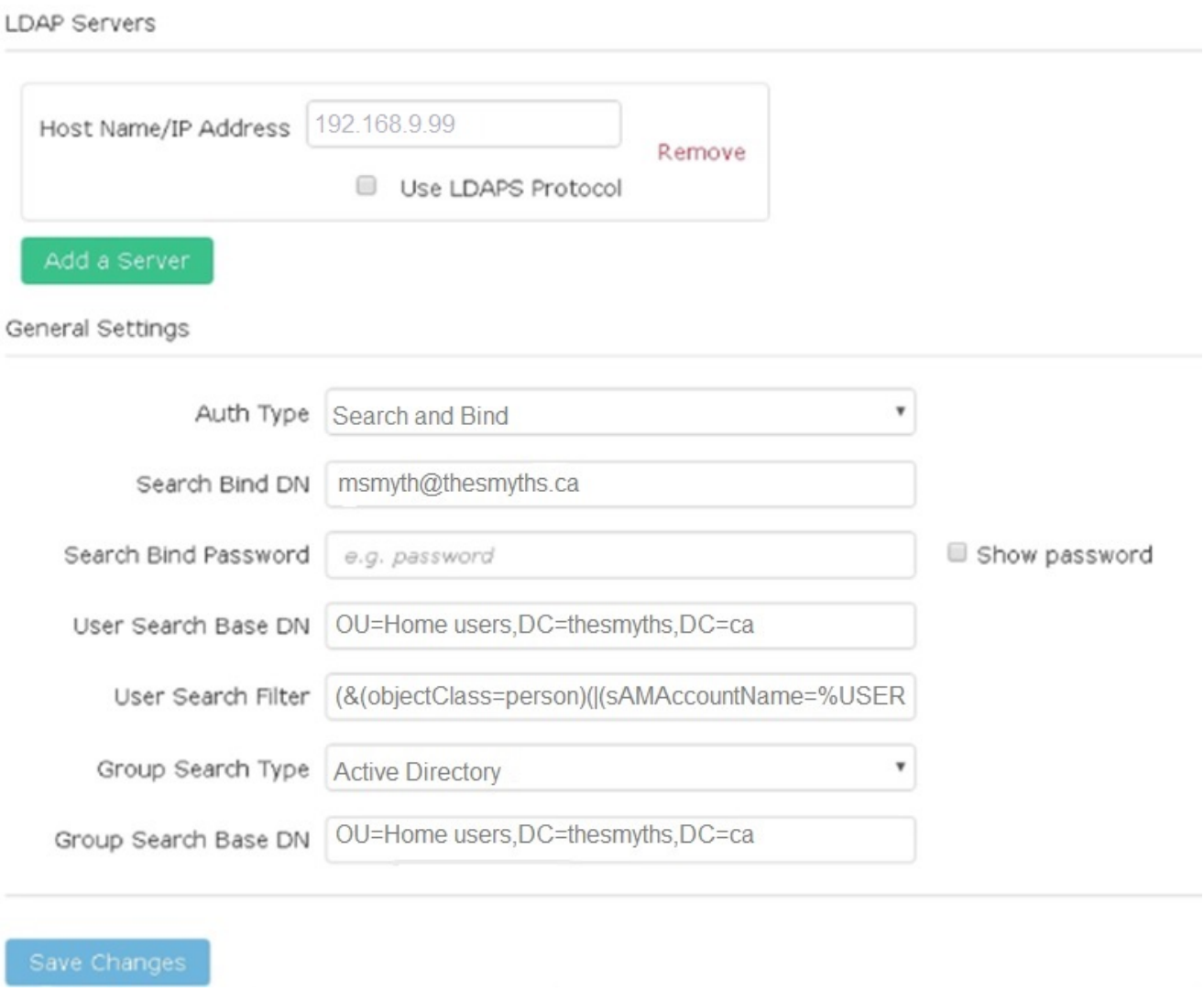
Étapes

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

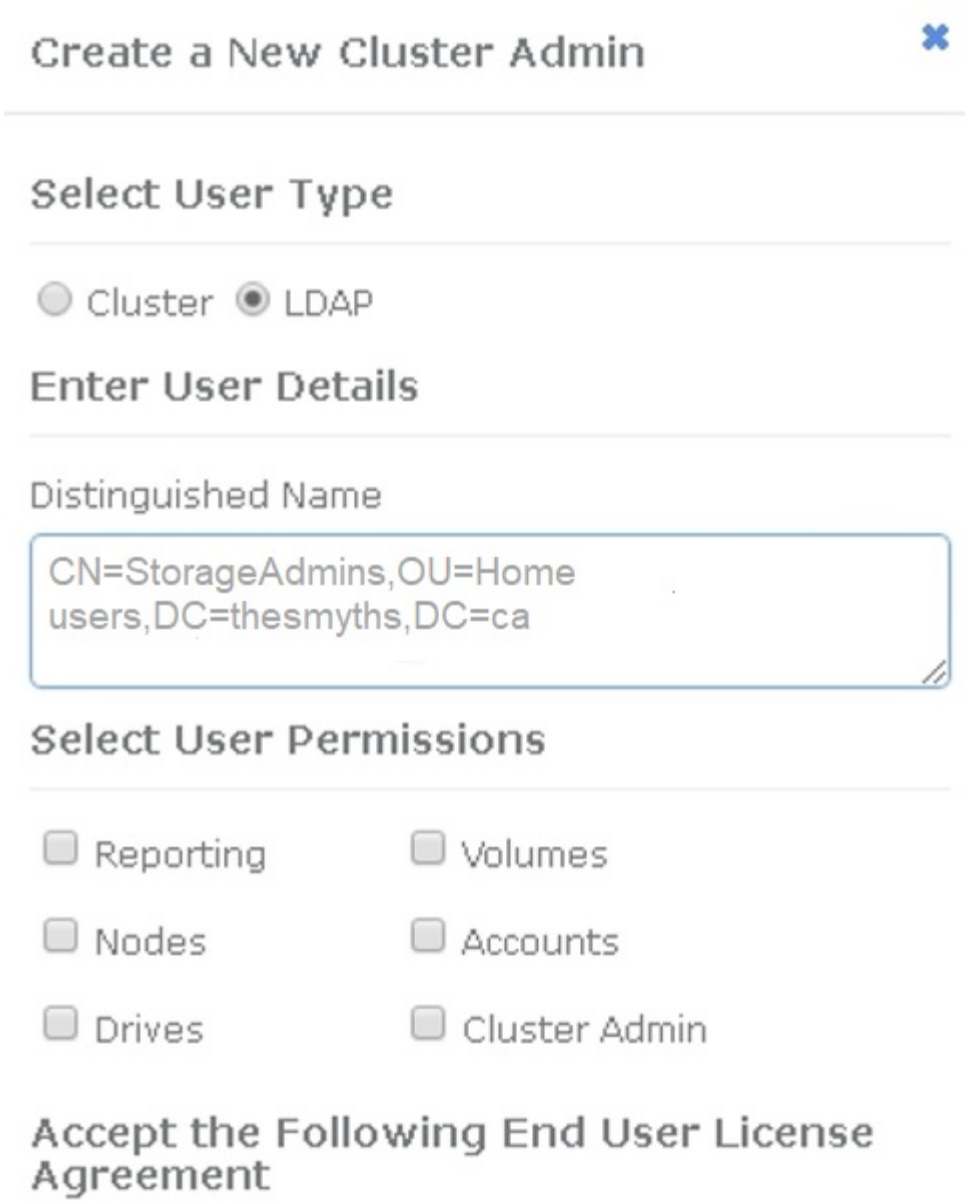
   Un numéro de port personnalisé facultatif peut également être saisi.

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

5. **Facultatif:** sélectionnez **utiliser le protocole LDAPS**.
6. Entrez les informations requises dans **Paramètres généraux**.



7. Cliquez sur **Activer LDAP**.
8. Cliquez sur **Tester l'authentification utilisateur** si vous souhaitez tester l'accès au serveur pour un utilisateur.
9. Copiez le nom distinctif et les informations sur le groupe d'utilisateurs qui s'affichent 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 tout le monde puisse se connecter, procédez comme suit :
    a. Cliquez sur **User** > **View**.



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

   Maintenant, vous avez un utilisateur avec la valeur d'un groupe Active Directory.

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

Activez l'authentification LDAP avec l'API Element

Vous pouvez configurer l'intégration du système de stockage avec un serveur LDAP existant. Les administrateurs LDAP peuvent ainsi gérer de façon centralisée l'accès au système de stockage pour les utilisateurs.

Vous pouvez configurer LDAP à l'aide de l'interface utilisateur Element ou de l'API Element. Cette procédure explique comment configurer LDAP à l'aide de l'API Element.

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

Étapes

1. Activez d'abord l'authentification LDAP sur le cluster à l'aide de la `EnableLdapAuthentication` méthode API.
2. Entrez 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 readonly pour rechercher d'abord l'utilisateur authentifié et lier ensuite cet utilisateur s'il est trouvé et authentifié.
GroupSearchBaseDN : dc=prodtest,dc=solidfire,dc=net	Spécifie l'emplacement dans l'arborescence LDAP pour commencer la recherche de groupes. Pour cet exemple, nous avons utilisé la racine de notre arbre. Si votre arborescence LDAP est très grande, vous pouvez le définir sur une sous-arborescence plus granulaire pour réduire les temps de recherche.

Paramètres utilisés	Description
UserSearchBaseDN : dc=prodtest,dc=solidfire,dc=net	Indique l'emplacement dans l'arborescence LDAP pour commencer la recherche d'utilisateurs. Pour cet exemple, nous avons utilisé la racine de notre arbre. Si votre arborescence LDAP est très grande, vous pouvez le définir sur une sous-arborescence plus granulaire pour réduire les temps de recherche.
GroupSearchType : ActiveDirectory	Utilise le serveur Windows Active Directory comme serveur LDAP.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Pour utiliser userPrincipalName (adresse e-mail pour la connexion), vous pouvez remplacer userSearchFilter par :
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
Ou, pour effectuer une recherche à la fois userPrincipalName et sAMAccountName, vous pouvez utiliser le userSearchFilter suivant :
 	
`"(&(objectClass=person)(`
	(SAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%))» ----

Utilise sAMAccountName comme nom d'utilisateur pour la connexion à la grappe 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 à des entrées dont la valeur est « personne » dans l'attribut objectClass.	SearchBindDN
Il s'agit du nom distinctif de l'utilisateur readonly qui sera utilisé pour effectuer une recherche dans l'annuaire LDAP. Pour le répertoire actif, il est généralement plus facile d'utiliser le nom d'utilisateur en titre (format d'adresse e-mail) pour l'utilisateur.	SearchBindPassword

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

qu'utilisateur dans ce groupe.

Afficher les détails du LDAP

Affichez les informations LDAP sur la page LDAP de l'onglet Cluster.

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

1. Pour afficher les détails LDAP avec l'interface utilisateur d'élément, 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
     - Rechercher et lier
   - **Rechercher un DN de liaison** : un DN complet pour se connecter avec pour effectuer une recherche LDAP pour l'utilisateur (nécessite un accès de niveau de liaison à l'annuaire LDAP).
   - **Search Bind Password** : mot de passe utilisé pour authentifier l'accès au serveur LDAP.
   - **Recherche utilisateur DN de base** : le DN de base de l'arborescence utilisée pour lancer la recherche utilisateur. Le système recherche la sous-arborescence à partir de l'emplacement spécifié.
   - **Filtre de recherche d'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.
     - Aucun groupe : aucun support de groupe.
     - DN du membre : groupes de style DN du membre (niveau unique).
   - **Recherche de groupe DN de base** : le DN de base de l'arborescence utilisée pour lancer la recherche de groupe. Le système recherche la sous-arborescence à partir de l'emplacement spécifié.
   - **Tester l'authentification utilisateur** : une fois le protocole LDAP configuré, utilisez-le pour tester le nom d'utilisateur et l'authentification par mot de passe pour le serveur LDAP. Saisissez un compte déjà existant pour le tester. Les informations relatives au nom distinctif et au groupe d'utilisateurs s'affichent, que vous pouvez copier pour une utilisation ultérieure lors de la création d'administrateurs de cluster.

Testez la configuration LDAP

Après avoir configuré LDAP, vous devez le tester à l'aide de l'interface utilisateur Element ou de la méthode API Element `TestLdapAuthentication`.

Étapes

1. Pour tester la configuration LDAP avec l'interface utilisateur Element, procédez comme suit :
   a. Cliquez sur **Cluster** > **LDAP**.
   b. Cliquez sur **Test authentification LDAP**.
   c. Pour résoudre les problèmes, utilisez les informations du tableau ci-dessous :

Message d'erreur	Description
`xLDAPUserNotFound`	• L'utilisateur testé est introuvable dans la sous-arborescence configurée `userSearchBaseDN`. • Le `userSearchFilter` n'est pas configuré correctement.
`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 incorrecte.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	Le nom d'utilisateur ou le mot de passe en lecture seule n'est pas configuré correctement.
`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. • Les `userSearchBaseDN` et `groupSearchBaseDN` se trouvent dans une UO imbriquée. Cela peut entraîner des problèmes de permission. La solution consiste à inclure l'UO 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. Passez en revue les résultats. Si l'appel API réussit, les résultats incluent le nom distinctif de l'utilisateur spécifié et une liste de groupes dans lesquels 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 à l'aide de l'interface utilisateur Element.

Avant de commencer, notez tous les paramètres de configuration, car la désactivation du protocole LDAP efface tous les paramètres.

Étapes

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

Trouvez plus d'informations

- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Informations sur le copyright

Informations sur les marques commerciales