アカウントを管理
Element Software

NetApp
October 01, 2024

目次

アカウントを管理

SolidFire ストレージシステムでは、テナントはアカウントを使用してクライアントがクラスタ上のボリュームに接続できるようにすることができます。ボリュームは、作成時に特定のアカウントに割り当てられます。SolidFire ストレージシステムのクラスタ管理者アカウントを管理することもできます。

- "CHAPを使用してアカウントを操作します"
- "クラスタ管理者のユーザアカウントを管理します"

詳細情報

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

CHAPを使用してアカウントを操作します

SolidFire ストレージシステムでは、テナントはアカウントを使用してクライアントがクラスタ上のボリュームに接続できるようにすることができます。アカウントには、割り当てられているボリュームへのアクセスに必要なChallenge Handshake Authentication Protocol（CHAP；チャレンジハンドシェイク認証プロトコル）認証が含まれています。ボリュームは、作成時に特定のアカウントに割り当てられます。

アカウントには最大 2 、 000 個のボリュームを関連付けることができますが、 1 つのボリュームが属することのできるアカウントは 1 つだけです。

CHAPアルゴリズム

Element 12.7以降では、FIPS準拠のセキュアなCHAPアルゴリズムSHA1、SHA-256、およびSHA3-256がサポートされています。Element 12.7では、ホストiSCSIイニシエータがElement iSCSIターゲットを使用してiSCSIセッションを作成している場合、使用するCHAPアルゴリズムのリストを要求します。Element のiSCSIターゲットは、ホストのiSCSIイニシエータが要求したリストから、最初にサポートするアルゴリズムを選択します。ElementのiSCSIターゲットが最もセキュアなアルゴリズムを選択することを確認するには、ホストのiSCSIイニシエータを設定して、最もセキュアなアルゴリズム（SHA-256など）から最もセキュアでないアルゴリズムのリストを送信する必要があります。たとえば、次のようになります。 SHA1またはMD5。ホストのiSCSIイニシエータからSHAアルゴリズムが要求されない場合は、ホストから提示されたアルゴリズムのリストにMD5が含まれていれば、Element iSCSIターゲットによってMD5が選択されます。セキュアなアルゴリズムのサポートを有効にするために、ホストのiSCSIイニシエータ設定の更新が必要になる場合があります。

Element 12.7のアップグレード時に、ストレージノードの再起動時に、SHAアルゴリズムを含むリストを含むセッション要求を送信するようにホストiSCSIイニシエータ設定がすでに更新されている場合は、 新しいセキュア・アルゴリズムがアクティブ化され、最もセキュアなプロトコルを使用して、新規または再接続されたiSCSIセッションが確立されます。アップグレード時に、既存のすべてのiSCSIセッションがMD5からSHAに移行します。SHAを要求するためにホストiSCSIイニシエータの設定を更新しない場合、既存のiSCSIセッションでは引き続きMD5が使用されます。ホストのiSCSIイニシエータCHAPアルゴリズムをあとで更新したあと、iSCSIセッションは、iSCSIセッションの再接続になるメンテナンス作業に基づいて、時間の経過とと

もにMD5からSHAに徐々に移行する必要があります。

たとえば、Red Hat Enterprise Linux（RHEL）8.3のデフォルトのホストiSCSIイニシエータの設定はコメントアウトされている `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5`ため、iSCSIイニシエータではMD5のみが使用されます。ホストでこの設定のコメントを解除し、iSCSIイニシエータを再起動すると、そのホストからのiSCSIセッションがSHA-256を使用し始めるようになります。

必要に応じて、APIメソッドを使用して、各セッションで使用されているCHAPアルゴリズムを確認できます "ListISCSISessions"。

アカウントの作成

アカウントを作成して、ボリュームへのアクセスを許可することができます。

システム内のアカウント名はそれぞれ一意である必要があります。

1. [* 管理 **>] > [** アカウント] を選択します。
2. ［ * アカウントの作成 * ］ をクリックします。
3. * ユーザー名 * を入力します。
4. [* CHAP 設定 * （ * CHAP Settings * ）] セクションで、次の情報を入力します。

   パスワードを自動生成する場合は、クレデンシャルフィールドを空白のままにします。

   - * イニシエータシークレット * - CHAP ノードセッション認証用
   - * Target Secret * ： CHAP ノードセッション認証用
5. ［ * アカウントの作成 * ］ をクリックします。

アカウントの詳細を表示します

個々のアカウントのパフォーマンスアクティビティをグラフ形式で表示できます。

グラフには、アカウントの I/O とスループットの情報が表示されます。Average と Peak のアクティビティレベルが、 10 秒間隔で表示されます。これらの統計には、アカウントに割り当てられているすべてのボリュームのアクティビティが含まれます。

1. [* 管理 **>] > [** アカウント] を選択します。
2. アカウントの [アクション] アイコンをクリックします。
3. [* 詳細の表示 *] をクリックします。

以下に詳細を示します。

- * ステータス * ：アカウントのステータス。有効な値：
  - active ：アクティブアカウント。
  - locked ：ロック済みアカウント。
  - removed ：削除およびパージされたアカウント。
- * Active Volumes * ：アカウントに割り当てられているアクティブなボリュームの数。

- * Compression * ：アカウントに割り当てられているボリュームの圧縮による削減率。
- * 重複排除機能 * ：アカウントに割り当てられているボリュームの重複排除による削減率。
- * シンプロビジョニング * ：アカウントに割り当てられたボリュームのシンプロビジョニングによる削減率。
- * 全体的な削減率 * ：アカウントに割り当てられているボリュームの全体的な削減率。

アカウントを編集します

アカウントを編集して、ステータス、 CHAP シークレット、またはアカウント名を変更できます。

アカウントの CHAP 設定を変更したり、アクセスグループからイニシエータやボリュームを削除したりすると、原因イニシエータがボリュームにアクセスできなくなることがあります。ボリュームへのアクセスが突然失われないようにするには、アカウントまたはアクセスグループの変更の影響を受ける iSCSI セッションを必ずログアウトし、イニシエータやクラスタの設定に対する変更が完了したあとにイニシエータからボリュームに再接続できることを確認してください。

管理サービスに関連付けられた永続ボリュームは、インストールまたはアップグレード時に作成された新しいアカウントに割り当てられます。永続ボリュームを使用している場合は、関連付けられているアカウントを変更または削除しないでください。

1. [* 管理 **>] > [** アカウント] を選択します。
2. アカウントの [アクション] アイコンをクリックします。
3. 表示されたメニューで、「 * 編集 * 」を選択します。
4. * オプション： * ユーザー名 * を編集します。
5. * オプション： * Status * ドロップダウンリストをクリックして、別のステータスを選択します。

ステータスを * locked * に変更すると、アカウントへのすべての iSCSI 接続が切断され、アカウントにアクセスできなくなります。アカウントに関連付けられているボリュームは維持されますが、 iSCSI で検出できなくなります。

6. * オプション： * CHAP Settings * で、 * Initiator Secret * および * Target Secret * クレデンシャルを編集し、ノードセッション認証に使用します。

CHAP 設定 * のクレデンシャルを変更しない場合、クレデンシャルは変更されません。クレデンシャルのフィールドを空白にすると、システムによって新しいパスワードが生成されます。

7. [変更の保存 *] をクリックします。

アカウントを削除します

不要になったアカウントを削除できます。

アカウントを削除する前に、そのアカウントに関連付けられているボリュームを削除およびパージします。

管理サービスに関連付けられた永続ボリュームは、インストールまたはアップグレード時に作成された新しいアカウントに割り当てられます。永続ボリュームを使用している場合は、関連付けられているアカウントを変更または削除しないでください。

1. [* 管理 **>] > [** アカウント] を選択します。
2. 削除するアカウントの [アクション] アイコンをクリックします。
3. 表示されたメニューで、 * 削除 * を選択します。
4. 操作を確定します。

詳細情報

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

クラスタ管理者のユーザアカウントを管理します

SolidFire ストレージシステムのクラスタ管理者アカウントの管理では、クラスタ管理者アカウントの作成、削除、編集、クラスタ管理者パスワードの変更、およびユーザのシステムアクセスを管理するための LDAP の設定を行います。

ストレージクラスタ管理者アカウントのタイプ

NetApp Element ソフトウェアを実行するストレージクラスタには、プライマリクラスタ管理者アカウントとクラスタ管理者アカウントの 2 種類の管理者アカウントがあります。

- * プライマリクラスタ管理者アカウント *

  この管理者アカウントは、クラスタ作成時に作成されます。このアカウントは、クラスタへの最高レベルのアクセス権を持つプライマリの管理アカウントです。このアカウントは、 Linux システムの root ユーザに相当します。この管理者アカウントのパスワードを変更できます。

- * クラスタ管理者アカウント *

  クラスタ管理者アカウントには、クラスタ内で特定のタスクを実行するための限定的な管理アクセスを付与できます。各クラスタ管理者アカウントに割り当てられたクレデンシャルを使用して、ストレージシステム内での API や Element UI の要求が認証されます。

ノード UI からクラスタ内のアクティブノードにアクセスするには、ローカル（ LDAP 以外）のクラスタ管理者アカウントが必要です。まだクラスタに含まれていないノードにアクセスする場合、アカウントのクレデンシャルは必要ありません。

クラスタ管理者の詳細を表示

1. クラスタ全体（ LDAP 以外）のクラスタ管理者アカウントを作成するには、次の操作を実行します。
   a. [**Users**>*Cluster Admins] をクリックします。

2. Users タブの Cluster Admins ページで、次の情報を表示できます。
   - * ID * ：クラスタ管理者アカウントに割り当てられたシーケンシャル番号。
   - * Username * ：クラスタ管理者アカウントの作成時に指定した名前。
   - * アクセス * ：ユーザアカウントに割り当てられたユーザ権限。有効な値：
     - 読み取り
     - レポート作成
     - ノード
     - ドライブ
     - ボリューム
     - アカウント
     - clusterAdmin の権限が必要です
     - 管理者
     - supportAdmin

     administrator アクセスタイプには、すべての権限が割り当てられています。
   - * タイプ * ：クラスタ管理者のタイプ。有効な値：
     - クラスタ
     - LDAP
   - * 属性 * ： Element API を使用して作成されたクラスタ管理者アカウントに対し、作成時に設定された名前と値のペアが表示されます。

     を参照して "NetApp Element ソフトウェア API リファレンス"

クラスタ管理者アカウントを作成

新しいクラスタ管理者アカウントを作成し、ストレージシステムの特定の領域へのアクセスを許可または制限する権限を付与できます。クラスタ管理者アカウントの権限を設定すると、割り当てていない権限については読み取り専用権限が付与されます。

LDAP クラスタ管理者アカウントを作成する場合は、作成を開始する前にクラスタで LDAP が設定されていることを確認します。

"Element ユーザインターフェイスで LDAP 認証を有効にします"

レポート作成、ノード、ドライブ、ボリューム、アカウント用のクラスタ管理者アカウントの権限をあとから変更することができます。 クラスタレベルのアクセスとアクセス許可を有効にすると、そのレベルの書き込みアクセスが割り当てられます。選択しなかったレベルについては、読み取り専用アクセスが付与されます。

システム管理者が作成したクラスタ管理者ユーザアカウントをあとから削除することもできます。クラスタの作成時に作成されたプライマリクラスタ管理者アカウントを削除することはできません。

1. クラスタ全体（ LDAP 以外）のクラスタ管理者アカウントを作成するには、次の操作を実行します。

a. [**Users**>*Cluster Admins] をクリックします。
b. Create Cluster Admin をクリックします。
c. ユーザタイプとして「 * Cluster * 」を選択します。
d. アカウントのユーザ名とパスワードを入力し、確認のためにパスワードをもう一度入力します。
e. アカウントに適用するユーザ権限を選択します。
f. チェックボックスをオンにして、エンドユーザライセンス契約に同意します。
g. Create Cluster Admin をクリックします。

2. LDAP ディレクトリにクラスタ管理者アカウントを作成するには、次の操作を実行します。

a. [**Cluster**>*LDAP*] をクリックします。
b. LDAP認証が有効になっていることを確認します。
c. [ユーザー認証のテスト] をクリックし、ユーザーまたはユーザーがメンバーになっているグループのいずれかに表示される識別名をコピーして、後で貼り付けることができます。
d. [**Users**>*Cluster Admins] をクリックします。
e. Create Cluster Admin をクリックします。
f. LDAP ユーザタイプを選択します。
g. [Distinguished Name] フィールドのテキストボックスの例に従って、ユーザまたはグループの完全な識別名を入力します。または、前の手順でコピーした識別名を貼り付けます。

識別名がグループの一部である場合、 LDAP サーバ上でそのグループのメンバーであるユーザには、この管理者アカウントの権限が与えられます。

LDAP クラスタ管理者ユーザまたはグループを追加する場合、ユーザ名の一般的な形式は「 LDAP ： <Full Distinguished Name>` 」です。

a. アカウントに適用するユーザ権限を選択します。
b. チェックボックスをオンにして、エンドユーザライセンス契約に同意します。
c. Create Cluster Admin をクリックします。

クラスタ管理者の権限を編集します

レポート作成、ノード、ドライブ、ボリューム、アカウント用のクラスタ管理者アカウントの権限を変更できます。 クラスタレベルのアクセスとアクセス許可を有効にすると、そのレベルの書き込みアクセスが割り当てられます。選択しなかったレベルについては、読み取り専用アクセスが付与されます。

1. [**Users**>*Cluster Admins] をクリックします。
2. 編集するクラスタ管理者の操作アイコンをクリックします。
3. [編集（ Edit ）] をクリックします。
4. アカウントに適用するユーザ権限を選択します。
5. [変更の保存 *] をクリックします。

クラスタ管理者アカウントのパスワードを変更します

Element UI を使用してクラスタ管理者のパスワードを変更できます。

1. [**Users**>*Cluster Admins] をクリックします。
2. 編集するクラスタ管理者の操作アイコンをクリックします。
3. [編集（ Edit ）] をクリックします。
4. Change Password フィールドに新しいパスワードを入力し、確認のためにもう一度入力します。
5. [変更の保存 *] をクリックします。

詳細情報

- "Element ユーザインターフェイスで LDAP 認証を有効にします"
- "LDAPを無効にする"
- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

LDAPの管理

Lightweight Directory Access Protocol （ LDAP ）を設定して、 SolidFire ストレージへのセキュアなディレクトリベースのログイン機能を有効にすることができます。LDAP をクラスタレベルで設定し、 LDAP ユーザおよびグループを許可することができます。

LDAP を管理するには、既存の Microsoft Active Directory 環境を使用して SolidFire クラスタへの LDAP 認証を設定し、設定をテストします。

IPv4 アドレスと IPv6 アドレスの両方を使用できます。

LDAP を有効にする手順の概要を次に示します。

1. * LDAP サポート * の設定前の手順を完了します。LDAP 認証の設定に必要な詳細情報がすべて揃っていることを確認します。
2. * LDAP 認証を有効にします * 。Element UI または Element API を使用します。
3. * LDAP 設定を確認します。 *必要に応じて、 GetLdapConfiguration API メソッドを実行するか、 Element UI を使用して LCAP 設定をチェックし、クラスタが正しい値で設定されていることを確認します。
4. * LDAP認証*をテストします（ユーザとともに `readonly`）。TestLdapAuthentication API メソッドを実行するか、 Element UI を使用して、 LDAP 構成が正しいことをテストします。この最初のテストでは、ユーザのユーザ名「`sAMAccountName`」を使用し `readonly`ます。これにより、クラスタが`LDAP`認証用に正しく設定されているかどうかと、クレデンシャルとアクセスが正しいかどうかが検証されます `readonly`。この手順が失敗した場合は、手順 1~3 を繰り返します。
5. * LDAP 認証をテストします * （追加するユーザアカウントを使用）。Element クラスタ管理者として追加するユーザアカウントに対して setp 4 を繰り返します。名前（DN）またはユーザ（またはグループ）をコピーします `distinguished`。この DN はステップ 6 で使用されます。
6. * LDAP クラスタ管理者を追加します * （ LDAP 認証のテスト手順で DN をコピーして貼り付けます

）。Element UI または AddLdapClusterAdmin API メソッドを使用して、適切なアクセスレベルで新しいクラスタ管理者ユーザを作成します。ユーザ名には、手順 5 でコピーした完全な DN を貼り付けます。これにより、 DN が正しくフォーマットされます。

7. * クラスタ管理者アクセスをテストします。 *新しく作成した LDAP クラスタ管理者ユーザを使用してクラスタにログインします。LDAP グループを追加した場合は、そのグループの任意のユーザとしてログインできます。

LDAP サポートの設定前の手順を実行します

Element で LDAP サポートを有効にする前に、 Windows Active Directory Server をセットアップし、その他の設定前のタスクを実行する必要があります。

手順

1. Windows Active Directory サーバをセットアップする。
2. * オプション： * LDAPS サポートを有効にします。
3. ユーザとグループを作成
4. LDAP ディレクトリの検索に使用する読み取り専用のサービスアカウント（「 'fsreadonly' 」など）を作成します。

Element ユーザインターフェイスで LDAP 認証を有効にします

ストレージシステムと既存の LDAP サーバの統合を設定できます。これにより、 LDAP 管理者はストレージシステムへのユーザアクセスを一元管理できます。

LDAP の設定には、 Element ユーザインターフェイスまたは Element API を使用できます。この手順では、 Element UI を使用して LDAP を設定する方法について説明します。

次に、SolidFireでLDAP認証を設定し、認証タイプとしてを使用する例を示し `SearchAndBind`ます。この例では、 1 つの Windows Server 2012 R2 Active Directory サーバを使用します。

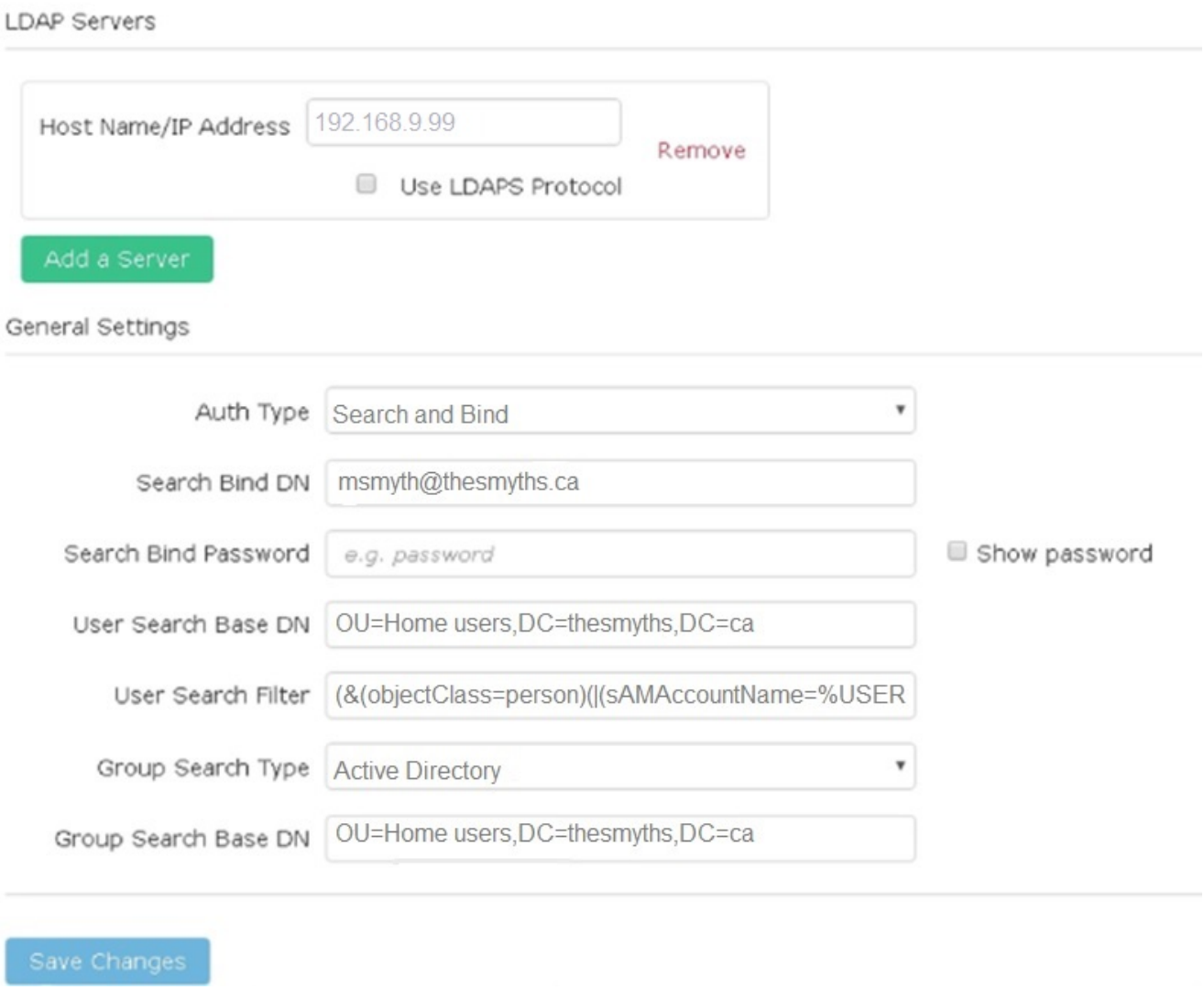
手順

1. [**Cluster**>*LDAP*] をクリックします。
2. [* Yes* （はい）] をクリックして、 LDAP 認証を有効
3. [サーバーの追加] をクリックします。
4. ホスト名 /IP アドレス * を入力します。

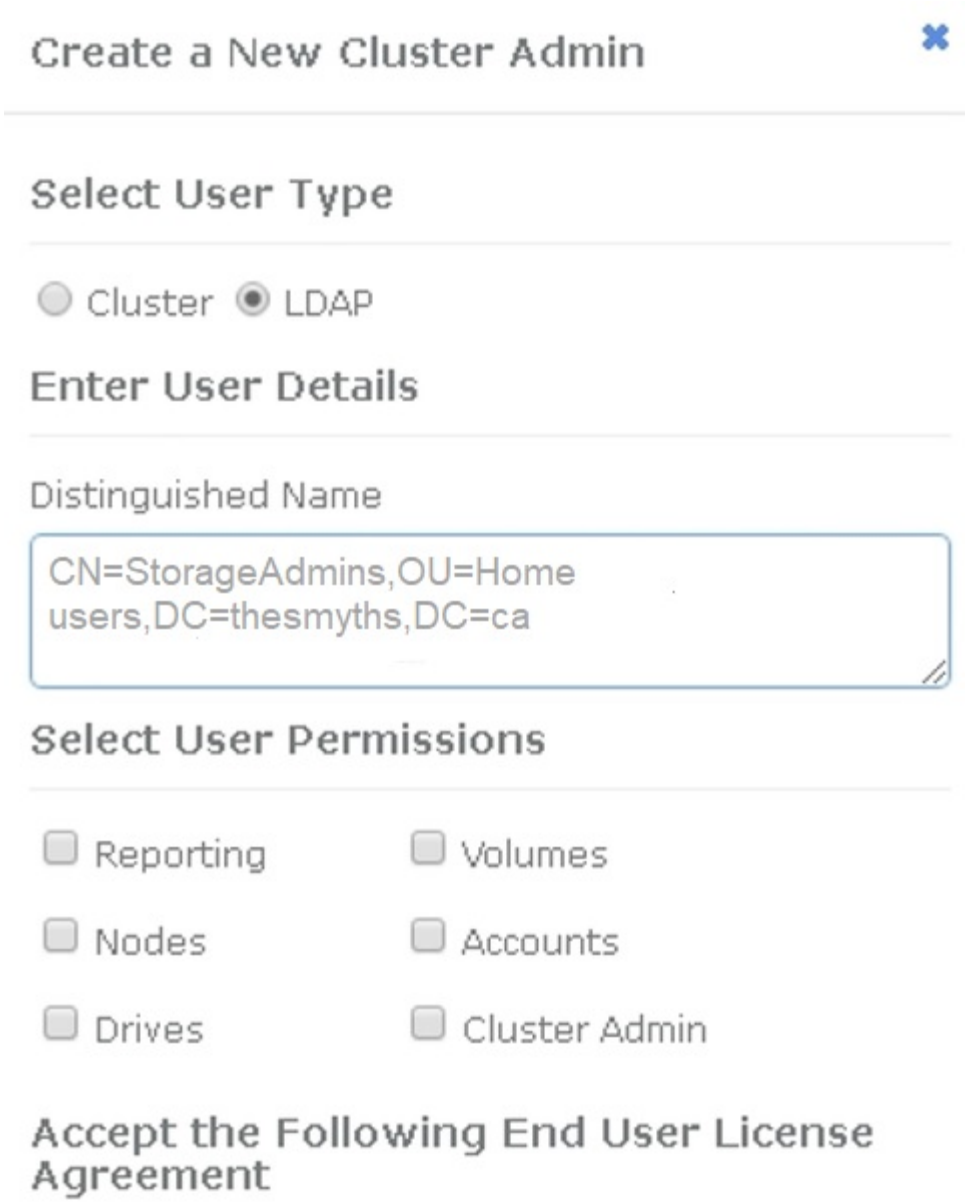
   オプションのカスタムポート番号を入力することもできます。

   たとえば、カスタムポート番号を追加するには、 <host name or IP address> ： <port number> と入力します

5. * オプション： * Use LDAPS Protocol * を選択します。
6. 「一般設定」に必要な情報を入力します。



7. [LDAPを有効にする]をクリックします。
8. ユーザーのサーバーアクセスをテストする場合は、 [ユーザー認証のテスト] をクリックします。
9. あとでクラスタ管理者を作成するときに使用できるように、表示された識別名とユーザグループの情報をコピーします。
10. [Save Changes] をクリックして、新しい設定を保存します。
11. 誰でもログインできるようにこのグループにユーザを作成するには、次の手順を実行します。
    a. [* ユーザー * （ * User * ）] > [* 表示（ * View ）]



b. 新しいユーザーの場合は、 [ユーザータイプ] の [*LDAP] をクリックし、 [識別名] フィールドにコピーしたグループを貼り付けます。
c. 権限を選択します。通常はすべての権限が選択されます。
d. エンドユーザライセンス契約までスクロールダウンし、 [* I accept （同意します）] をクリックします。
e. Create Cluster Admin をクリックします。

これで、 Active Directory グループの値を持つユーザが作成されました。

この問題をテストするには、 Element UI からログアウトし、そのグループにユーザとして再度ログインします。

Element API を使用して **LDAP** 認証を有効にします

ストレージシステムと既存の LDAP サーバの統合を設定できます。これにより、 LDAP 管理者はストレージシステムへのユーザアクセスを一元管理できます。

LDAP の設定には、 Element ユーザインターフェイスまたは Element API を使用できます。この手順では、 Element API を使用して LDAP を設定する方法について説明します。

SolidFireクラスタでLDAP認証を利用するには、まずAPIメソッドを使用してクラスタでLDAP認証を有効にし`EnableLdapAuthentication`ます。

手順

1. 最初にAPIメソッドを使用して、クラスタでLDAP認証を有効にして `EnableLdapAuthentication`ください。
2. 必要な情報を入力します。

```
{
      "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. 次のパラメータの値を変更します。

使用するパラメータ	製品説明
authType ： SearchAndBind	では、クラスタで readonly サービスアカウントを使用して、認証されているユーザが最初に検索され、見つかったユーザが認証済みの場合はバインドされるように指定しています。
groupSearchBaseDN ： dc=prodtest 、 dc=solidfire 、 dc=net	グループの検索を開始する LDAP ツリー内の場所を指定します。この例では、ツリーのルートを使用しています。LDAP ツリーのサイズが非常に大きい場合は、検索時間を短縮するために、これをより詳細なサブツリーに設定することを推奨します。

使用するパラメータ	製品説明
userSearchBaseDN ： dc=prodtest 、 dc=solidfire 、 dc=net	ユーザの検索を開始する LDAP ツリー内の場所を指定します。この例では、ツリーのルートを使用しています。LDAP ツリーのサイズが非常に大きい場合は、検索時間を短縮するために、これをより詳細なサブツリーに設定することを推奨します。
groupSearchType ： ActiveDirectory	Windows Active Directory サーバを LDAP サーバとして使用します。

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
userPrincipalName （ログイン用の E メールアドレス）を使用するには、 userSearchFilter を次のように変更します。
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
または、 userPrincipalName と sAMAccountName の両方を検索するには、次の userSearchFilter を使用できます。
 	
`"(&(objectClass=person)(`
	（ sAMAccountName = %USERNAME% ）（ userPrincipalName = %USERNAME% ））」 -----

SolidFire クラスタにログインするには、 sAMAccountName をネットアップのユーザ名として使用します。これらの設定は 'sAMAccountName 属性でログイン中に指定されたユーザー名を検索するように LDAP に指示し ' さらに objectClass 属性の値として "person" を持つエントリにも検索を制限します	searchBindDN
LDAP ディレクトリの検索に使用される readonly ユーザの識別名を指定します。Active Directory の場合は、通常、ユーザに userPrincipalName （ E メールアドレス形式）を使用するのが最も簡単です。	searchBindPassword

この問題をテストするには、 Element UI からログアウトし、そのグループにユーザとして再度ログインします。

LDAP の詳細を確認します

クラスタタブの LDAP ページで LDAP 情報を表示します。

これらの LDAP 設定を表示するには、 LDAP を有効にする必要があります。

1. Element UI で LDAP の詳細を表示するには、 * Cluster * > * LDAP * をクリックします。
   - * Host Name/IP Address * ： LDAP または LDAPS ディレクトリサーバのアドレス。
   - * Auth Type * ：ユーザ認証方式。有効な値：
     - Direct Bind の
     - 検索とバインド
   - * Search Bind DN* ：ユーザの LDAP 検索を実行するためにログインで使用する完全修飾 DN （ LDAP ディレクトリへのバインドレベルのアクセスが必要）。
   - * Search Bind Password * ： LDAP サーバへのアクセスの認証に使用するパスワード。
   - * User Search Base DN* ：ユーザ検索を開始するツリーのベース DN 。指定した場所からサブツリーが検索されます。
   - * ユーザー検索フィルタ * ：ドメイン名を使用して次のように入力します。

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

   - **Group Search Type**: 使用されるデフォルトのグループ検索フィルタを制御する検索のタイプ。有効な値：
     - Active Directory ：あるユーザの LDAP グループをすべてネストしたメンバーシップ。
     - グループなし：グループはサポートされません。
     - Member DN ：メンバー DN 形式のグループ（シングルレベル）。
   - * Group Search Base DN* ：グループ検索を開始するツリーのベース DN 。指定した場所からサブツリーが検索されます。
   - * ユーザー認証のテスト * ： LDAP を構成した後、 LDAP サーバーのユーザー名とパスワード認証をテストするために使用します。この問題をテストするためにすでに存在するアカウントを入力してください。識別名とユーザグループの情報が表示されます。この情報をコピーして、あとでクラスタ管理者を作成する際に使用できます。

LDAP 設定をテストします

LDAPを設定したら、Element UIまたはElement APIメソッドを使用してLDAPをテストする必要があります `TestLdapAuthentication`。

手順

1. Element UI を使用して LDAP 設定をテストするには、次の手順を実行します。
   a. [**Cluster**>*LDAP*] をクリックします。
   b. [LDAP 認証のテスト *] をクリックします。
   c. 次の表に示す情報を使用して、問題を解決します。

エラーメッセージ	製品説明
`xLDAPUserNotFound`	• テスト対象のユーザが設定されたサブツリーに見つかりませんでした `userSearchBaseDN`。 • が `userSearchFilter`正しく設定されていません。
`xLDAPBindFailed (Error: Invalid credentials)`	• テスト中のユーザ名は有効な LDAP ユーザですが、入力したパスワードは正しくありません。 • テスト中のユーザ名は有効な LDAP ユーザですが、アカウントが現在無効になっています。
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	LDAP サーバの URI が正しくありません。
`xLDAPSearchBindFailed (Error: Invalid credentials)`	読み取り専用のユーザ名またはパスワードが正しく設定されていません。
`xLDAPSearchFailed (Error: No such object)`	が `userSearchBaseDN`LDAPツリー内の有効な場所ではありません。
`xLDAPSearchFailed (Error: Referral)`	• が `userSearchBaseDN`LDAPツリー内の有効な場所ではありません。 • と `groupSearchBaseDN` は `userSearchBaseDN` ネストされたOUにあります。これにより、原因権限の問題が発生する可能性がこの問題を回避するには、ユーザおよびグループのベースDNエントリにOUを含めます（例： `ou=storage, cn=company, cn=com`）。

2. Element API を使用して LDAP 設定をテストするには、次の手順を実行します。
   a. TestLdapAuthentication メソッドを呼び出します。

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

b. 結果を確認します。API 呼び出しに成功した場合は、指定したユーザの識別名とユーザがメンバーとなっているグループのリストが結果に含まれます。

```
{
"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"
     }
}
```

LDAPを無効にする

Element UI を使用して、 LDAP との統合を無効にすることができます。

LDAP を無効にするとすべての設定が消去されるため、作業を開始する前にすべての設定を書き留めておく必要があります。

手順

1. [**Cluster**>*LDAP*] をクリックします。
2. [* いいえ *] をクリックします。
3. [*LDAP を無効にする *] をクリックします

詳細情報

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

著作権に関する情報

商標に関する情報