ディレクトリサービスを使用する
SANtricity 11.8

NetApp
December 16, 2024

目次

ディレクトリサービスを使用する

ディレクトリサーバの追加

アクセス管理用の認証を設定するには、LDAPサーバとUnified ManagerのWebサービスプロキシを実行するホストの間の通信を確立します。次に、LDAPユーザグループをローカルユーザロールにマッピングします。

開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- ユーザグループがディレクトリサービスに定義されている必要があります。
- LDAPサーバのクレデンシャルを確認しておく必要があります。ドメイン名とサーバのURLのほか、必要に応じてバインドアカウントのユーザ名とパスワードも指定できます。
- セキュアなプロトコルを使用するLDAPSサーバの場合は、LDAPサーバの証明書チェーンをローカルマシンにインストールする必要があります。

タスクの内容

ディレクトリサーバの追加は、2つの手順で行います。最初にドメイン名とURLを入力します。サーバでセキュアなプロトコルを使用している場合は、認証用のCA証明書もアップロードする必要があります（標準の署名機関によって署名されている場合）。バインドアカウントのクレデンシャルがある場合は、ユーザアカウント名とパスワードも入力できます。次に、LDAPサーバのユーザグループをローカルユーザロールにマッピングします。

手順

1. アクセス管理*を選択します。
2. [ディレクトリサービス]タブで、[ディレクトリサーバーの追加]を選択します。

   [ディレクトリサーバーの追加]ダイアログボックスが開きます。
3. [サーバー設定]タブで、LDAPサーバーの資格情報を入力します。

フィールドの詳細

設定	製品説明
構成設定	ドメイン
LDAPサーバのドメイン名を入力します。ドメインを複数入力する場合は、カンマで区切って入力します。ドメイン名は、ログイン（*username@domain*）で、認証するディレクトリサーバを指定するために使用されます。	サーバURL
LDAPサーバにアクセスするためのURLをの形式で入力し`ldap[s]://**host**:*port*`ます。	証明書のアップロード（オプション）
このフィールドは、上記の[Server URL]フィールドでLDAPSプロトコルが指定されている場合にのみ表示されます。 [**Browse**]をクリックして、アップロードするCA証明書を選択します。これは、LDAPサーバの認証に使用される信頼された証明書または証明書チェーンです。	バインドアカウント（オプション）

設定	製品説明
LDAPサーバに対する検索クエリおよびグループ内の検索に使用する読み取り専用ユーザアカウントを入力します。アカウント名はLDAPタイプの形式で入力します。たとえば、バインドユーザの名前が「bindacct」の場合は、などの値を入力します `CN=bindacct,CN=Users,DC=cpoc,DC=local`。	バインドパスワード（オプション）
このフィールドは、バインドアカウントを入力すると表示されます。 バインドアカウントのパスワードを入力します。	追加する前にサーバ接続をテストする
入力したLDAPサーバの設定でシステムと通信できるかどうかを確認するには、このチェックボックスを選択します。このテストは、ダイアログボックスの下部にある*追加*（* Add *）をクリックした後に実行されます。 このチェックボックスを選択してテストに失敗した場合、設定は追加されません。設定を追加するには、エラーを解決するか、チェックボックスを選択解除してテストをスキップする必要があります。	権限の設定

設定	製品説明
検索ベースDN	ユーザを検索するLDAPコンテキストを入力します。通常はの形式で入力します `CN=Users, DC=cpoc, DC=local`。
ユーザ名属性	認証用のユーザIDにバインドされた属性を入力します。例： `sAMAccountName`。
グループ属性	グループとロールのマッピングに使用される、ユーザの一連のグループ属性を入力します。例： `memberOf, managedObjects`。

4. [役割マッピング（Role Mapping *）]タブをクリックします。
5. 事前定義されたロールにLDAPグループを割り当てます。1つのグループに複数のロールを割り当てることができます。

フィールドの詳細

設定	製品説明
マッピング	グループDN
マッピングするLDAPユーザグループの識別名（DN）を指定します。正規表現がサポートされています。正規表現パターンに含まれていない場合は、これらの特殊な正規表現文字をバックスラッシュ（\）でエスケープする必要がありま す。\.[]{}()<>*+-=!?^$	
役割	フィールド内をクリックし、グループDNにマッピングするローカルユーザロールを1つ選択します。このグループに含めるロールをそれぞれ個別に選択する必要があります。MonitorロールはSANtricity Unified Managerにログインするため必要なロールであり、他のロールと一緒に指定する必要があります。各ロールの権限は次のとおりです。 • * Storage admin *--アレイ上のストレージ・オブジェクトへの読み取り/書き込みのフル・アクセスを提供しますが'セキュリティ構成へのアクセスはありません • * Security admin *--アクセス管理と証明書管理のセキュリティ設定へのアクセス。 • * Support admin *--ストレージアレイ上のすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。 • *Monitor *--すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

Monitorロールは、管理者を含むすべてのユーザに必要です。

6. 必要に応じて、*別のマッピングを追加*をクリックして、グループとロールのマッピングをさらに入力します。
7. マッピングが終了したら、*追加*をクリックします。

   システムによって検証が実行され、ストレージアレイとLDAPサーバが通信できるかどうかが確認されます。エラーメッセージが表示された場合は、ダイアログボックスで入力したクレデンシャルを確認し、必要に応じて情報を再入力します。

ディレクトリサーバの設定とロールマッピングの編集

アクセス管理でディレクトリサーバをすでに設定している場合は、その設定をいつでも変更できます。設定には、サーバ接続情報とグループとロールのマッピングが含まれます。

開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- ディレクトリサーバを定義する必要があります。

手順

1. アクセス管理*を選択します。
2. [ディレクトリサービス]タブを選択します。
3. 複数のサーバが定義されている場合は、編集するサーバを表から選択します。
4. 「表示/設定の編集」を選択します。

   [ディレクトリサーバーの設定]ダイアログボックスが開きます。

5. サーバー設定*タブで、必要な設定を変更します。

フィールドの詳細

設定	製品説明
構成設定	ドメイン
LDAPサーバのドメイン名。ドメインを複数入力する場合は、カンマで区切って入力します。ドメイン名は、ログイン（*username*@*domain*）で、認証するディレクトリサーバを指定するために使用されます。	サーバURL
LDAPサーバにアクセスするためのURL（の形式）`ldap[s]://host:port`。	バインドアカウント（オプション）
LDAPサーバに対する検索クエリおよびグループ内の検索に使用する読み取り専用ユーザアカウント。	バインドパスワード（オプション）
バインドアカウントのパスワード。（このフィールドは、バインドアカウントを入力すると表示されます）。	保存する前にサーバ接続をテストする
システムがLDAPサーバ設定と通信できることを確認します。[保存（Save）]をクリックすると、テストが実行されます。このチェックボックスを選択してテストに失敗した場合、設定は変更されません。設定を編集するには、エラーを解決するか、チェックボックスを選択解除してテストをスキップする必要があります。	権限の設定

設定	製品説明
検索ベースDN	ユーザを検索するLDAPコンテキスト。通常はの形式です。 `CN=Users, DC=cpoc, DC=local`
ユーザ名属性	認証用のユーザIDにバインドされた属性。例： `sAMAccountName`。
グループ属性	ユーザのグループ属性のリスト。グループとロールのマッピングに使用されます。例： `memberOf, managedObjects`。

6. [役割マッピング]タブで、目的のマッピングを変更します。

フィールドの詳細

設定	製品説明
マッピング	グループDN
マッピングするLDAPユーザグループのドメイン名。正規表現がサポートされています。これらの特殊正規表現文字が正規表現パターンに含まれていない場合は、バックスラッシュ（\）でエスケープする必要があります。 \.[]{}()<>*+-=！？^$	
役割	グループDNにマッピングするロール。このグループに含めるロールをそれぞれ個別に選択する必要があります。MonitorロールはSANtricity Unified Managerにログインするため必要なロールであり、他のロールと一緒に指定する必要があります。ロールには次のものがあります。 • * Storage admin *--アレイ上のストレージ・オブジェクトへの読み取り/書き込みのフル・アクセスを提供しますがセキュリティ構成へのアクセスはありません • * Security admin *--アクセス管理と証明書管理のセキュリティ設定へのアクセス。 • * Support admin *--ストレージアレイ上のすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。 • *Monitor *--すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

Monitorロールは、管理者を含むすべてのユーザに必要です。

7. 必要に応じて、*別のマッピングを追加*をクリックして、グループとロールのマッピングをさらに入力します。
8. [保存（ Save ）] をクリックします。

結果

このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザーセッションのみが保持されます。

ディレクトリサーバの削除

ディレクトリサーバとWebサービスプロキシの間の接続を解除するには、[アクセス管理]ページでサーバ情報を削除します。このタスクは、新しいサーバを設定したあとに古いサーバを削除する場合に実行できます。

開始する前に

Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

タスクの内容

このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザーセッションのみが保持されます。

手順

1. アクセス管理*を選択します。
2. [ディレクトリサービス]タブを選択します。
3. リストから、削除するディレクトリサーバを選択します。
4. [削除（ Remove ）] をクリックします。

   [ディレクトリサーバーの削除]ダイアログボックスが開きます。

5. フィールドにと入力し `remove`、*[削除]*をクリックします。

   ディレクトリサーバの構成設定、権限設定、およびロールのマッピングが削除されます。ユーザは、このサーバのクレデンシャルを使用してログインできなくなります。

著作権に関する情報

商標に関する情報