LDAPによるISEロールベースアクセスコントロール

内容

概要

このドキュメントでは、Cisco Identity Services Engine(ISE)管理GUIへの管理アクセス用の外部IDストアとしてLightweight Directory Access Protocol(LDAP)を使用するための設定例について説明します。

前提条件

次の項目に関する知識があることが推奨されます。

- Cisco ISEバージョン3.0の設定
- LDAP(Lightweight Directory Access Protocol)

要件

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE バージョン 3.0
- Windows Server 2016

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

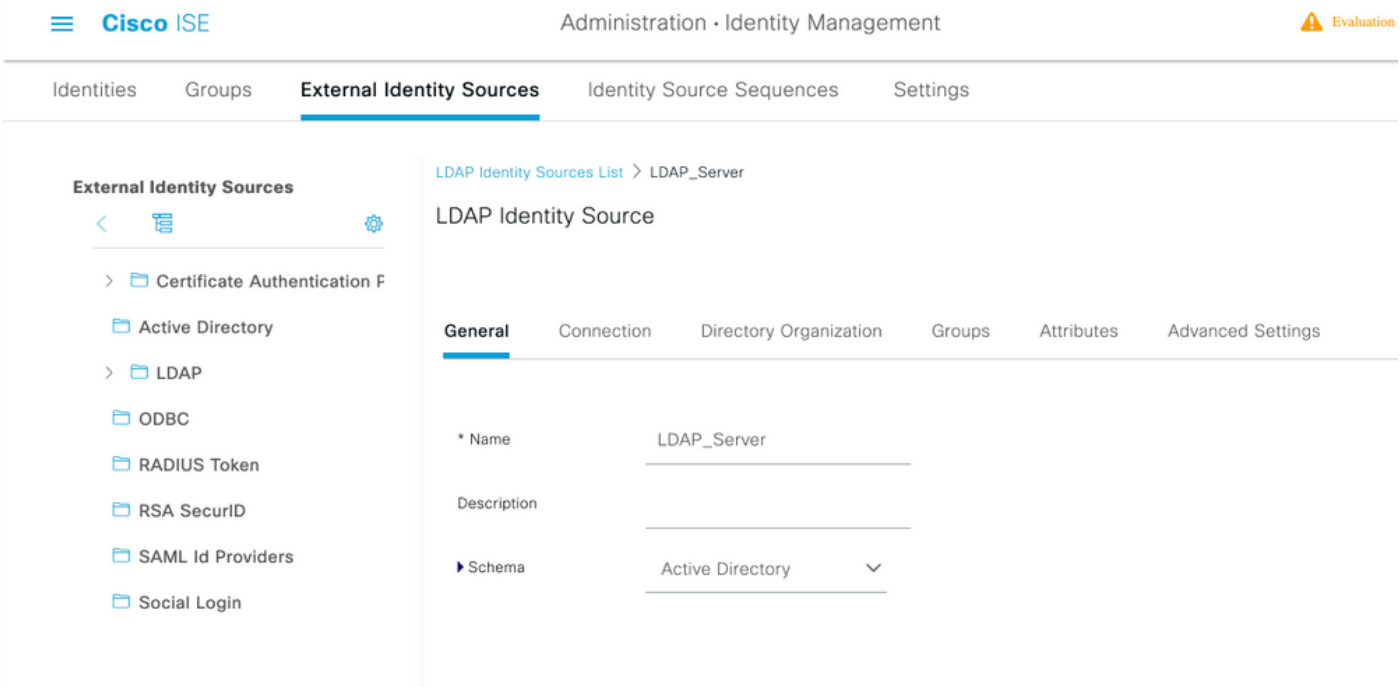
キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

ISE GUIへの管理/カスタムベースのアクセスを取得するようにLDAPベースのユーザを設定するには、次のセクションを使用します。次の設定では、LDAPプロトコルクエリを使用して、Active Directoryからユーザを取得し、認証を実行します。

ISEからLDAPへの参加

1. **[Administration] > [Identity Management] > [External Identity Sources] > [Active Directory] > [LDAP]に移動します。**
2. [General]タブで、LDAPの名前を入力し、スキーマの[Active Directory]を選択します。



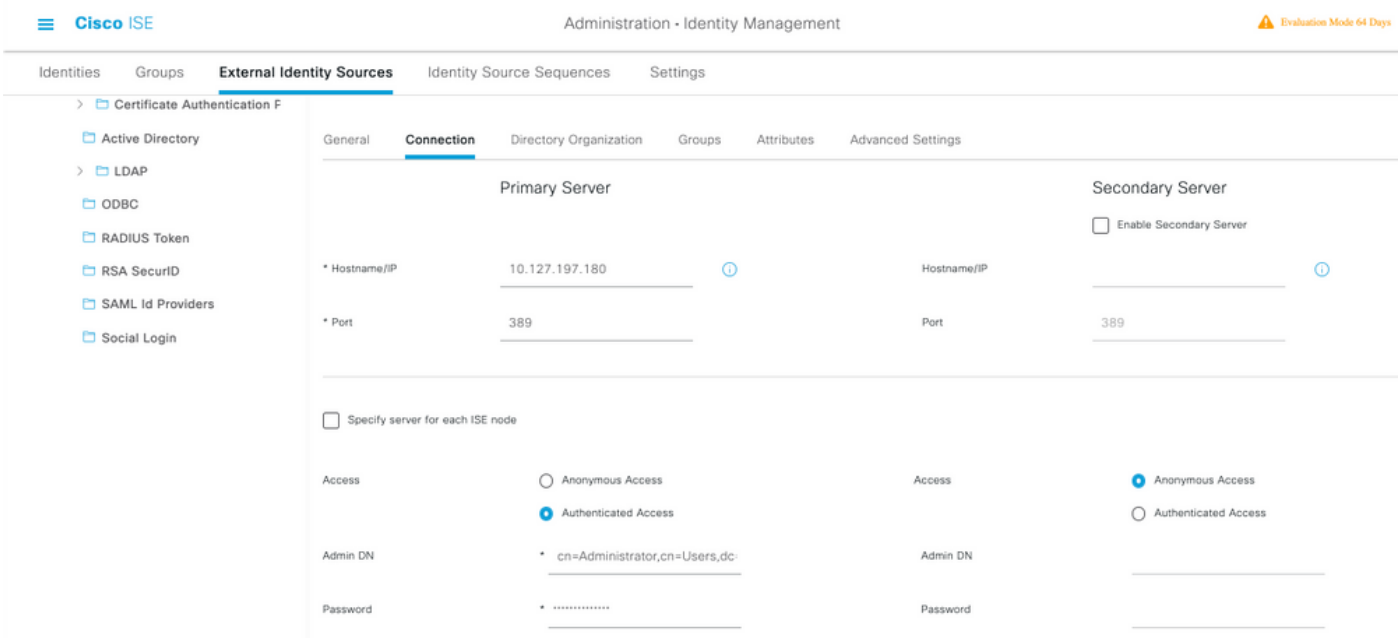
接続タイプとLDAP設定の設定

1. [ISE] > **[Administration] > [Identity Management] > [External Identity Sources] > [LDAP]に移動します。**

2.プライマリLDAPサーバのホスト名を、ポート389(LDAP)/636(LDAP-Secure)とともに設定します。

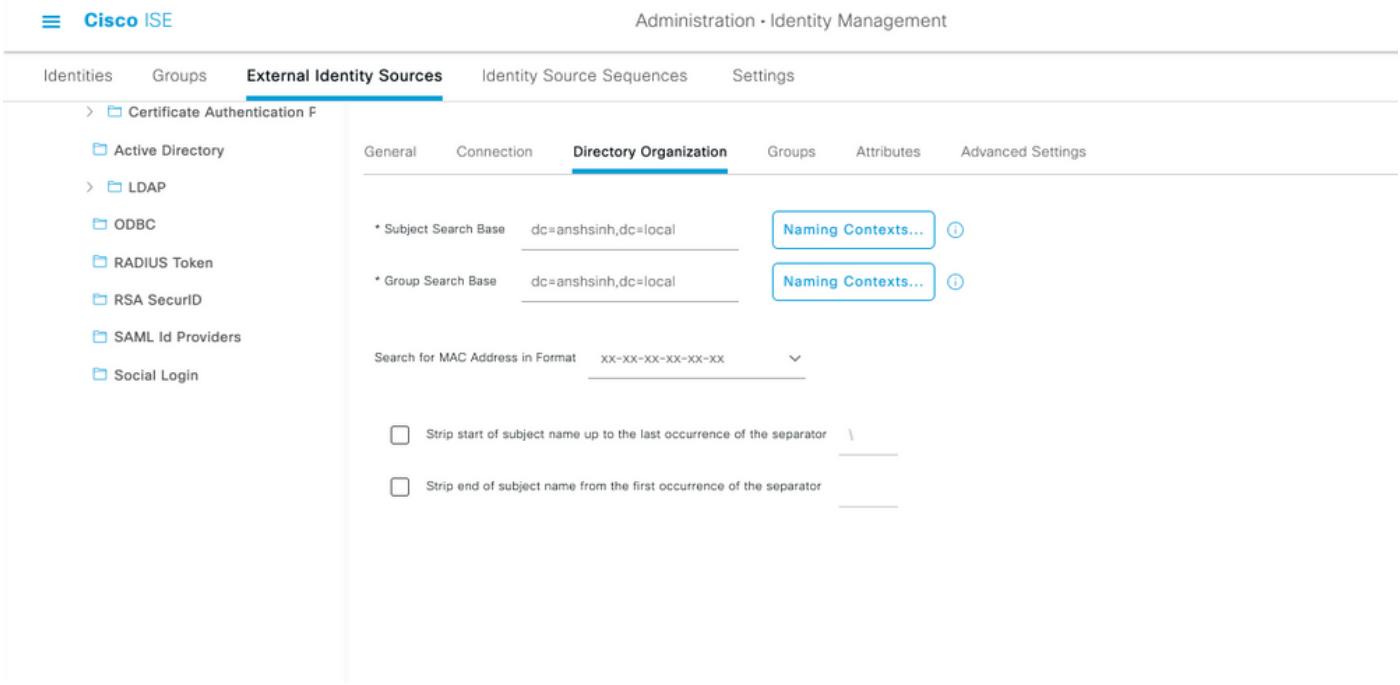
3. LDAPサーバの管理パスワードを使用して、管理識別名(DN)のパスを入力します。

4.[Test Bind Server]をクリックして、ISEからのLDAPサーバの到達可能性をテストします（LDAPサーバの到達可能性をテストします）。



ディレクトリの編成、グループ、および属性の設定

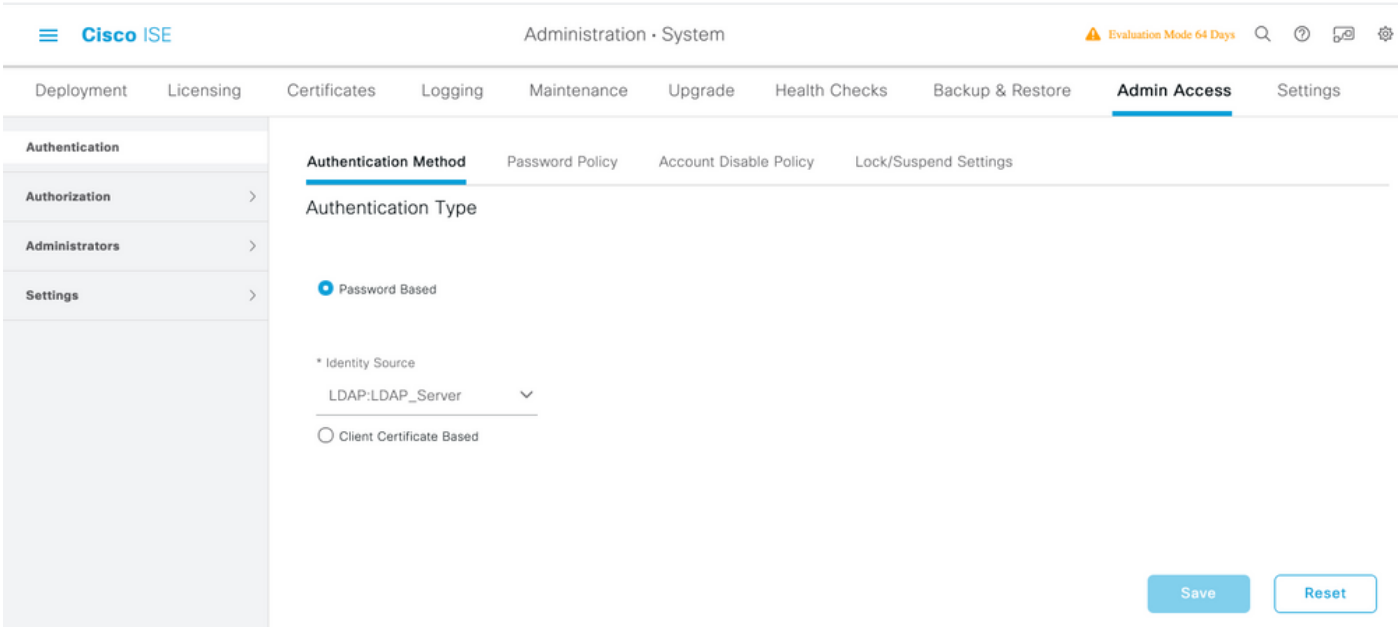
1. LDAPサーバに保存されているユーザの階層に基づいて、ユーザの正しい組織グループを選択します（図2を参照）。



LDAPユーザの管理アクセスの有効化

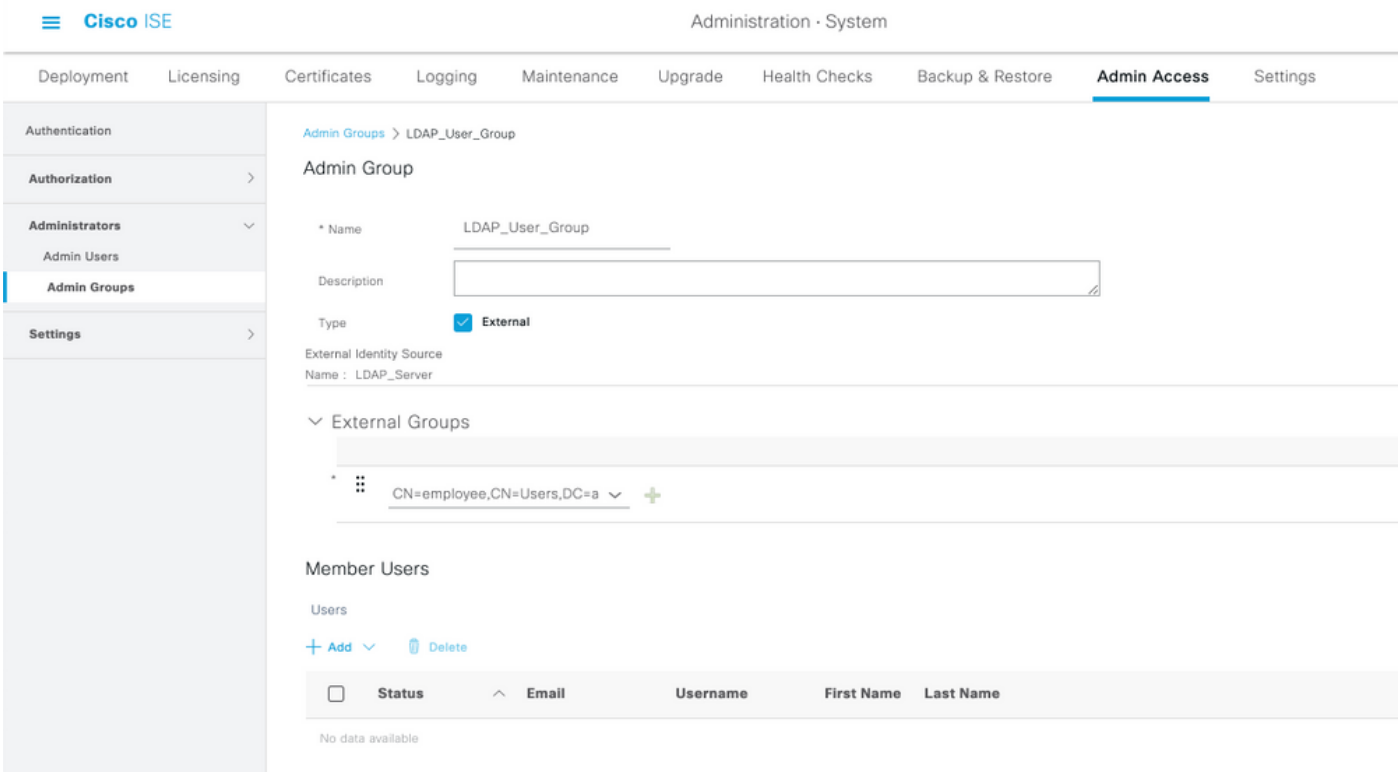
パスワードベースの認証を有効にするには、次の手順を実行します。

1. [ISE] > [Administration] > [System] > [Admin Access] > [Authentication]に移動します。
2. [Authentication Method]タブで、[Password-Based]オプションを選択します。
3. [IDソース]ドロップダウンメニューから[LDAP]を選択します。
4. [Save Changes] をクリックします。



管理グループをLDAPグループにマッピングします。

ISEで管理グループを設定し、ADグループにマッピングします。これにより、設定されたユーザは、グループメンバーシップに基づいて管理者に設定されたRBAC権限に基づいて、許可ポリシーに基づいてアクセスできるようになります。

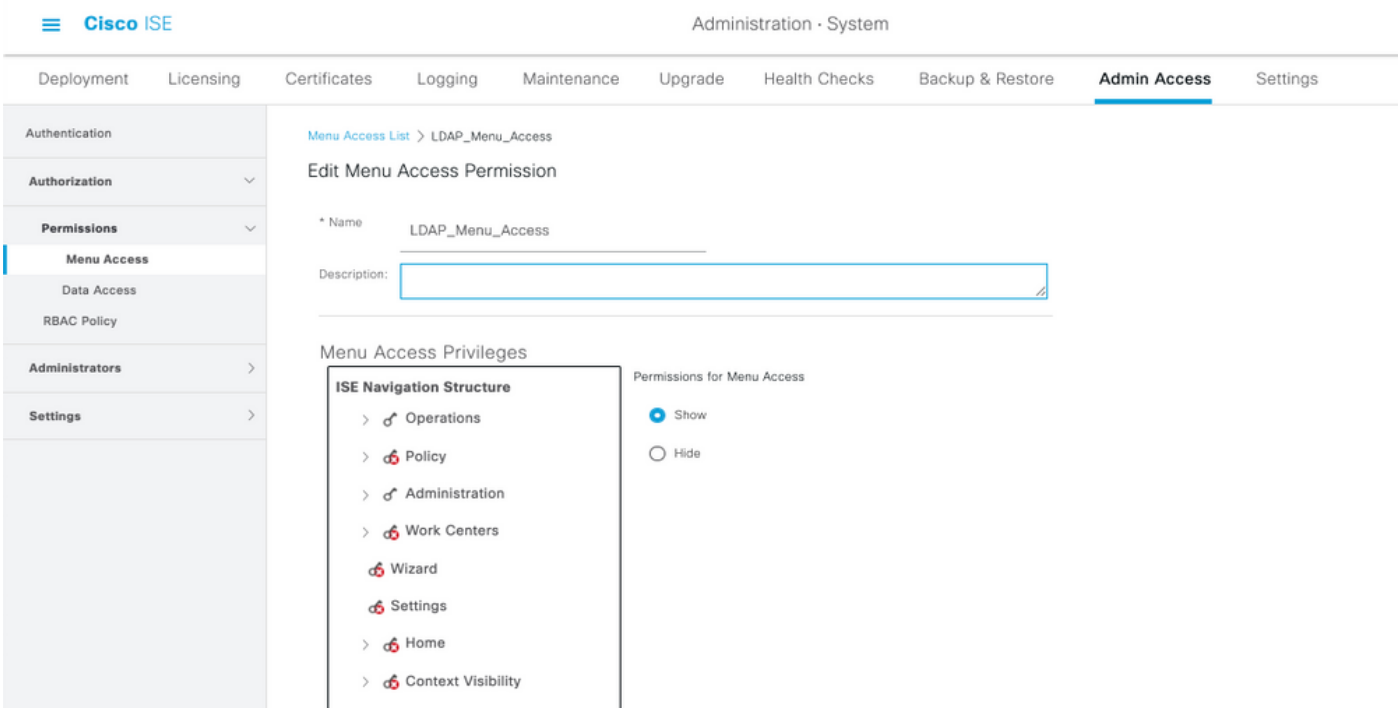


メニューアクセス権限の設定

1. [ISE] > [Administration] > [System] > [Authorization] > [Permissions] > [Menu access]に移動します

2. ISE GUIにアクセスするadminユーザのメニューアクセスを定義します。ユーザが必要に応じて一連の操作のみを実行できるように、GUIで表示または非表示になるようにサブエンティティを設定できます。

3. [Save]をクリックします。

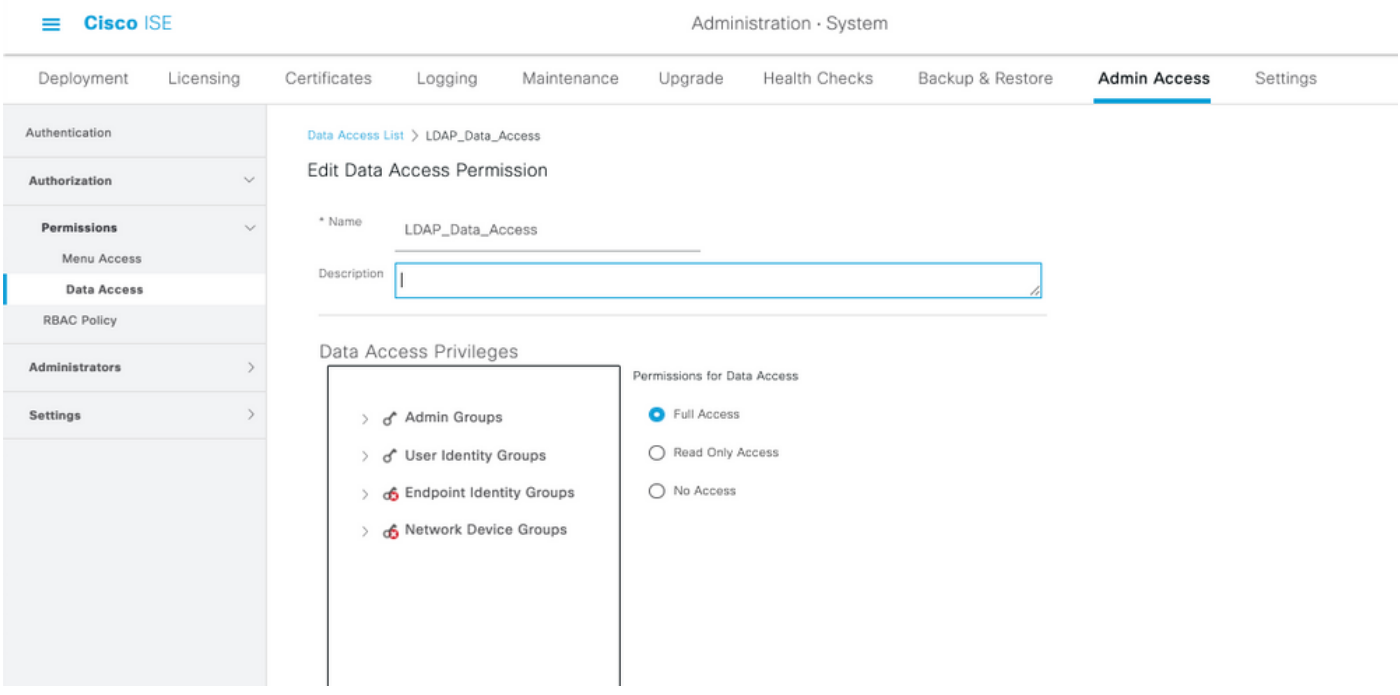


データアクセスの権限の設定

1. [ISE] > [Administration] > [System] > [Authorization] > [Permissions] > [Data access]に移動します

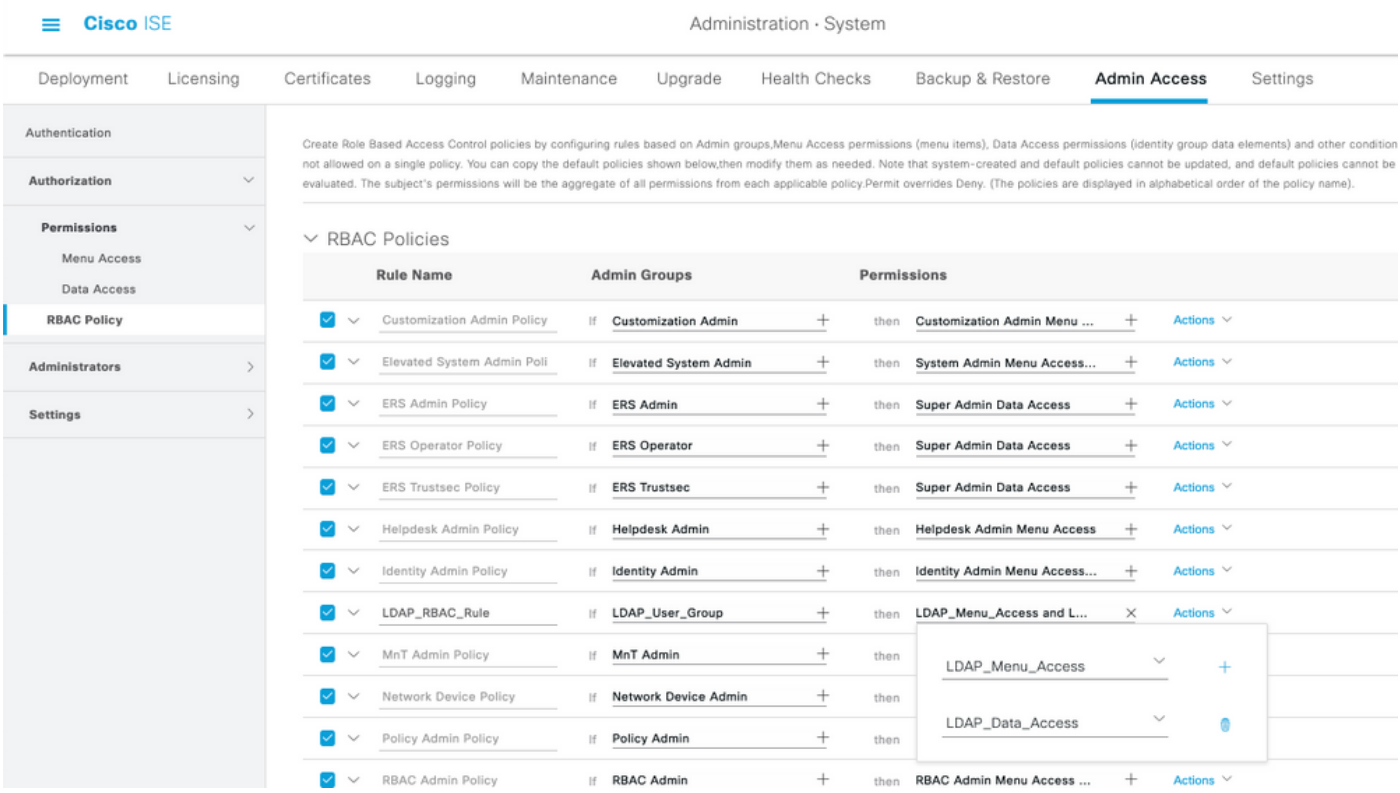
2. ISE GUIでアイデンティティグループへのフルアクセスまたは読み取り専用アクセス権を持つ管理者ユーザのデータアクセスを定義します。

3. 「保存」をクリックします。



管理グループの RBAC アクセス許可の設定

1. [ISE] > [Administration] > [System] > [Admin Access] > [Authorization] > [Policy]に移動します。
2. 右側にある [Actions] ドロップダウン メニューから [Insert New Policy Below] を選択して、新しいポリシーを追加します。
3. LDAP_RBAC_policyという名前の新しいルールを作成し、[Enable Administrative Access for AD]セクションで定義した管理グループにマッピングし、メニューアクセスとデータアクセスに権限を割り当てます。
4. [Save Changes] をクリックすると、保存された変更の確認が GUI の右下隅に表示されます。

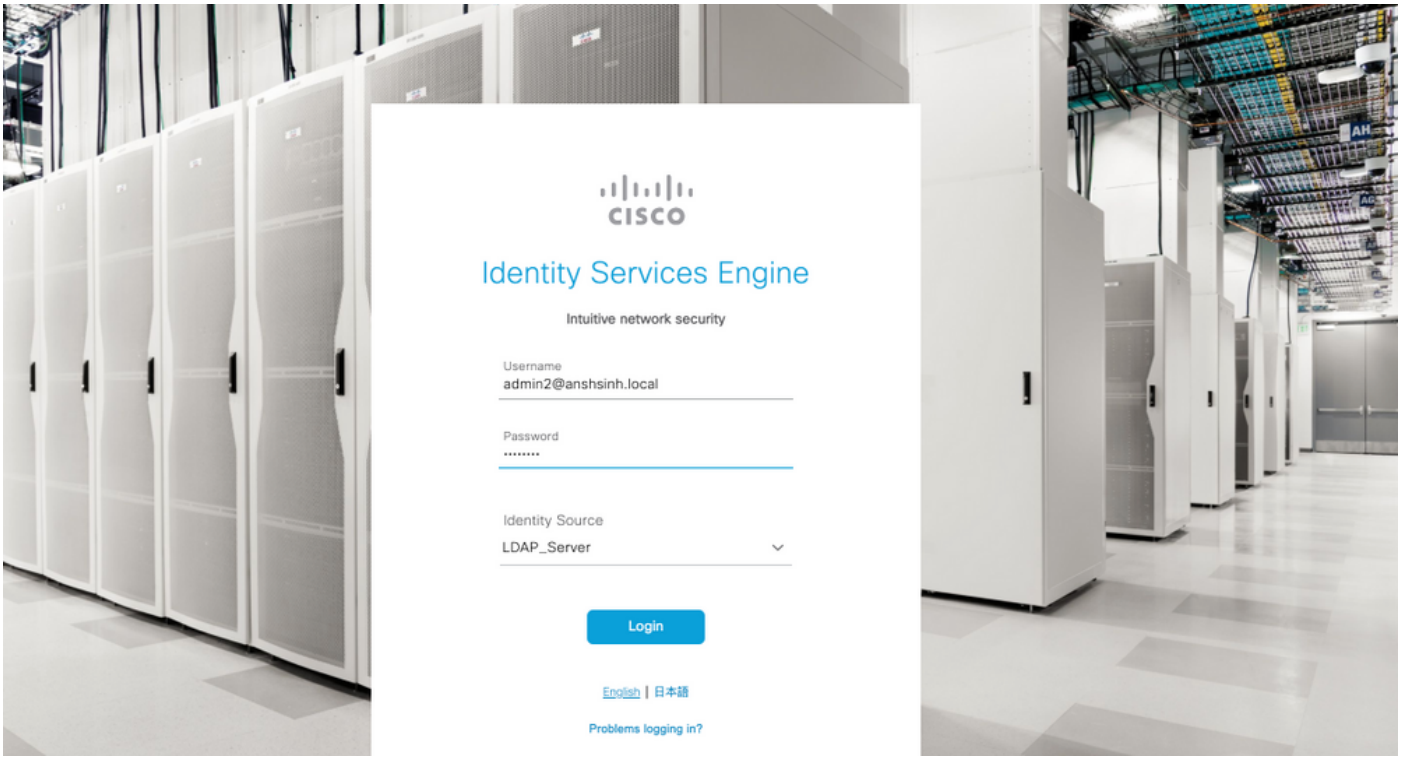


確認

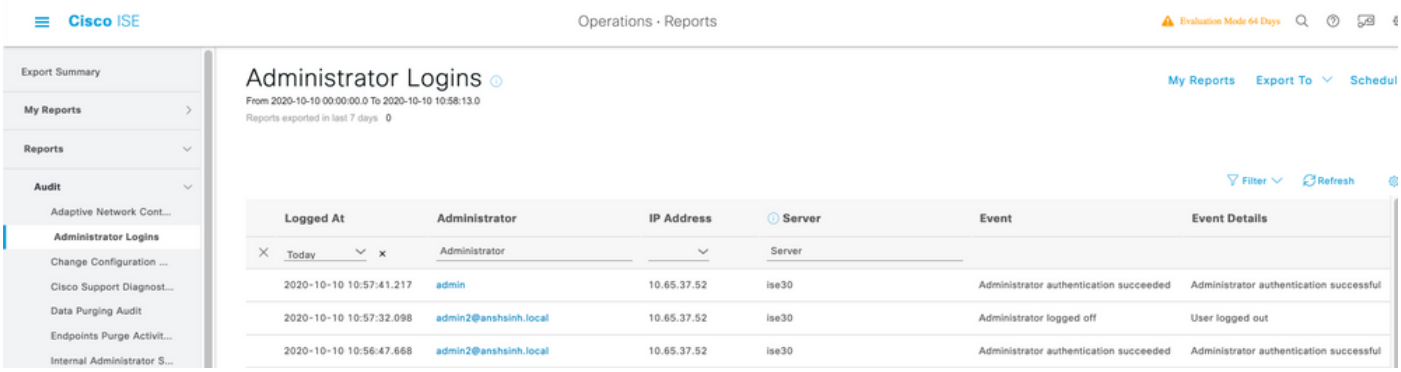
AD クレデンシャルでの ISE へのアクセス

AD クレデンシャルを使用して ISE にアクセスするには、次の手順を実行してください。

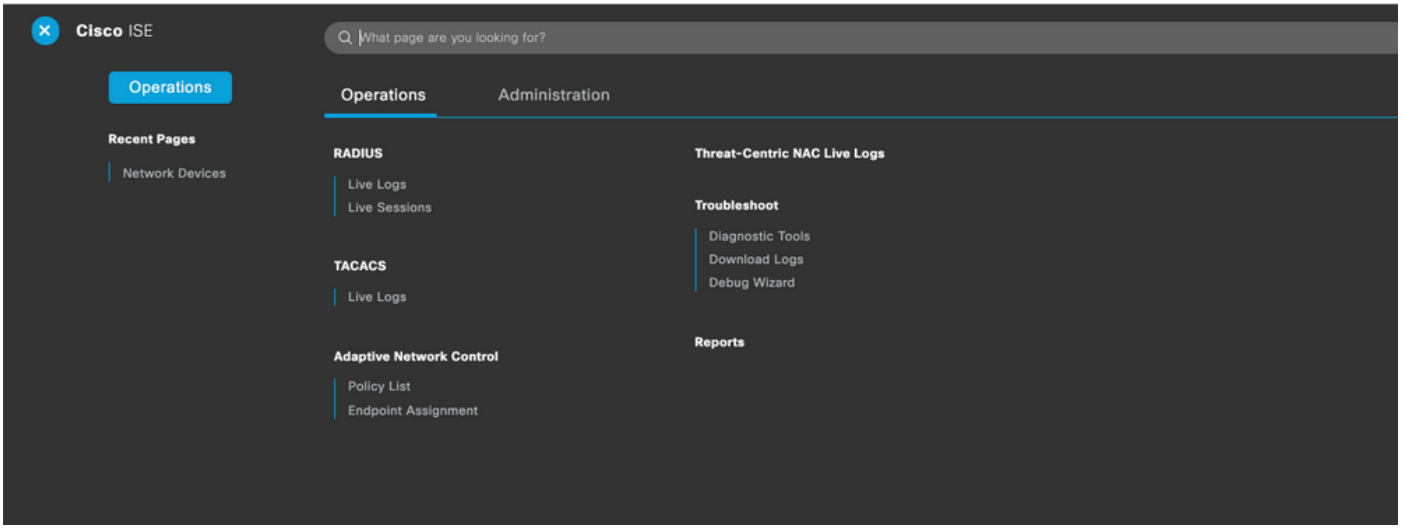
1. ISE GUIを開き、LDAPユーザでログインします。
2. [IDソース]ドロップダウンメニューからLDAP_Serverを選択します。
3. LDAPデータベースからユーザ名とパスワードを入力し、ログインします。



監査レポートで管理者ログインのログインを確認します。[ISE] > [Operations] > [Reports] > [Audit] > [Administrators Logins]に移動します。



この設定が正しく動作していることを確認するには、ISE GUIの右上隅にある認証済みユーザ名を確認します。次に示すように、メニューへのアクセスが制限されているカスタムベースのアクセスを定義します。



トラブルシュート

一般情報

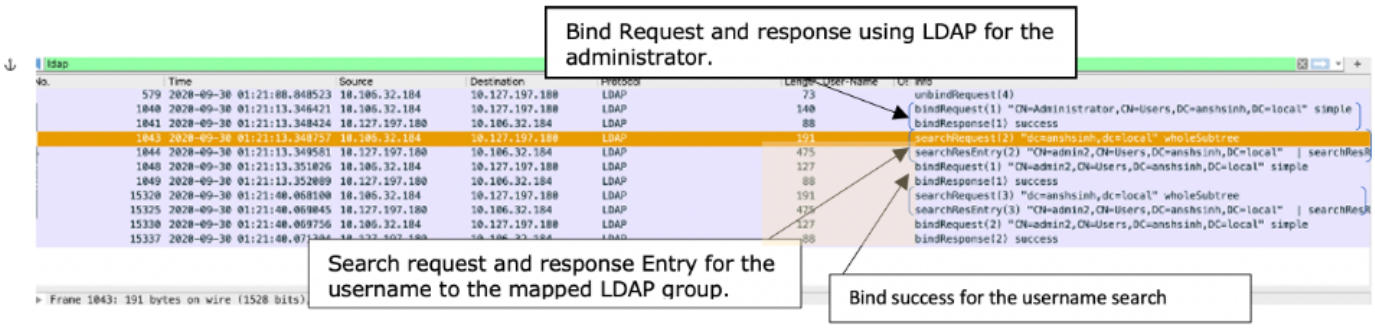
RBACプロセスのトラブルシューティングを行うには、ISE管理ノードのデバッグで次のISEコンポーネントを有効にする必要があります（ISEのデバッグはISE管理ノードで有効にする必要があります）。

RBAC：ログインを試みると、RBAC関連のメッセージが表示されます(ise-psc.log)

access-filter：リソースフィルタアクセス(ise-psc.log)を印刷します

runtime-AAA：ログインおよびLDAPインタラクションメッセージ(prrt-server.log)のログが出力されます

パケットキャプチャ分析



ログ分析

prrt-server.logを確認します

```
PAPAuthenticator,2020-10-10
08:54:00,621,DEBUG,0x7f852bee3700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,validateEvent: Username is [admin2@anshsinh.local]
bIsMachine is [0] isUtf8Valid is [1],PAPAuthenticator.cpp:86 IdentitySequence,2020-10-10
08:54:00,627,DEBUG,0x7f852c4e9700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,******* Authen
IDStoreName:LDAP_Server,IdentitySequenceWorkflow.cpp:377 LDAPIDStore,2020-10-10
08:54:00,628,DEBUG,0x7f852c4e9700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,Send event to LDAP_Server_924OqzxSbv_199_Primary
server,LDAPIDStore.h:205 Server,2020-10-10
08:54:00,634,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapServer::onAcquireConnectionResponse: succeeded to
acquire connection,LdapServer.cpp:724 Connection,2020-10-10
08:54:00,634,DEBUG,0x7f85293b8700,LdapConnectionContext::sendSearchRequest(id = 1221): base =
dc=anshsinh,dc=local, filter =
(&(objectclass=Person)(userPrincipalName=admin2@anshsinh.local)),LdapConnectionContext.cpp:516
Server,2020-10-10
08:54:00,635,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapSubjectSearchAssistant::processAttributes: found
CN=admin2,CN=Users,DC=anshsinh,DC=local entry matching admin2@anshsinh.local
subject,LdapSubjectSearchAssistant.cpp:268 Server,2020-10-10
```

```
08:54:00,635,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapSubjectSearchAssistant::processGroupAttr: attr =
memberOf, value = CN=employee,CN=Users,DC=anshsinh,DC=local,LdapSubjectSearchAssistant.cpp:389
Server,2020-10-10
08:54:00,636,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapServer::onAcquireConnectionResponse: succeeded to
acquire connection,LdapServer.cpp:724 Server,2020-10-10
08:54:00,636,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapServer::authenticate: user = admin2@anshsinh.local, dn
= CN=admin2,CN=Users,DC=anshsinh,DC=local,LdapServer.cpp:352 Connection,2020-10-10
08:54:00,636,DEBUG,0x7f85293b8700,LdapConnectionContext::sendBindRequest(id = 1223): dn =
CN=admin2,CN=Users,DC=anshsinh,DC=local,LdapConnectionContext.cpp:490 Server,2020-10-10
08:54:00,640,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapServer::handleAuthenticateSuccess: authentication of
admin2@anshsinh.local user succeeded,LdapServer.cpp:474 LDAPIDStore,2020-10-10
08:54:00,641,DEBUG,0x7f852c6eb700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LDAPIDStore::onResponse:
LdapOperationStatus=AuthenticationSucceeded -> AuthenticationResult=Passed,LDAPIDStore.cpp:336
```

ise-psc.logを確認します

これらのログから、ネットワークデバイスのリソースにアクセスしようとしたときにadmin2ユーザに使用されるRBACポリシーを確認できます。

```
2020-10-10 08:54:24,474 DEBUG [admin-http-pool51][] com.cisco.cpm.rbacfilter.AccessUtil -
:admin2@anshsinh.local:::- For admin2@anshsinh.local on /NetworkDevicesLPInputAction.do --
ACCESS ALLOWED BY MATCHING administration_networkresources_devices 2020-10-10 08:54:24,524 INFO
[admin-http-pool51][] cpm.admin.ac.actions.NetworkDevicesLPInputAction -
:admin2@anshsinh.local:::- In NetworkDevicesLPInputAction container method 2020-10-10
08:54:24,524 DEBUG [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -
:admin2@anshsinh.local:::- :::::::::Inside RBACAuthorization.getDataEntityDecision::::::
userName admin2@anshsinh.local dataType RBAC_NETWORK_DEVICE_GROUP permission ALL 2020-10-10
08:54:24,526 DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local:::- In DataPermissionEvaluator:hasPermission 2020-10-10 08:54:24,526
DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local:::- Data access being evaluated:LDAP_Data_Access 2020-10-10 08:54:24,528
DEBUG [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -
:admin2@anshsinh.local:::- :::::::::Inside RBACAuthorization.getDataEntityDecision::::::
permission retrieved false 2020-10-10 08:54:24,528 INFO [admin-http-pool51][]
cpm.admin.ac.actions.NetworkDevicesLPInputAction -:admin2@anshsinh.local:::- Finished with rbac
execution 2020-10-10 08:54:24,534 INFO [admin-http-pool51][]
cisco.cpm.admin.license.TrustSecLicensingUIFilter -:admin2@anshsinh.local:::- Should TrustSec be
visible :true 2020-10-10 08:54:24,593 DEBUG [admin-http-pool51][]
cisco.ise.rbac.authorization.RBACAuthorization -:admin2@anshsinh.local:::- :::::::::Inside
RBACAuthorization.getPermittedNDG:::::: userName admin2@anshsinh.local 2020-10-10 08:54:24,595
DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local:::- In DataPermissionEvaluator:getPermittedNDGMap 2020-10-10 08:54:24,597
DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local:::- processing data Access :LDAP_Data_Access 2020-10-10 08:54:24,604 INFO
[admin-http-pool51][] cisco.cpm.admin.license.TrustSecLicensingUIFilter -
:admin2@anshsinh.local:::- Should TrustSec be visible :true
```