Contrôle d'accès basé sur les rôles ISE avec LDAP

Contenu

Introduction

Ce document décrit un exemple de configuration pour l'utilisation du protocole LDAP (Lightweight Directory Access Protocol) comme magasin d'identité externe pour l'accès administratif à l'interface utilisateur graphique de gestion de Cisco Identity Services Engine (ISE).

Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de Cisco ISE version 3.0
- LDAP (Lightweight Directory Access Protocol)

Conditions requises

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ISE version 3.0
- Windows Server 2016

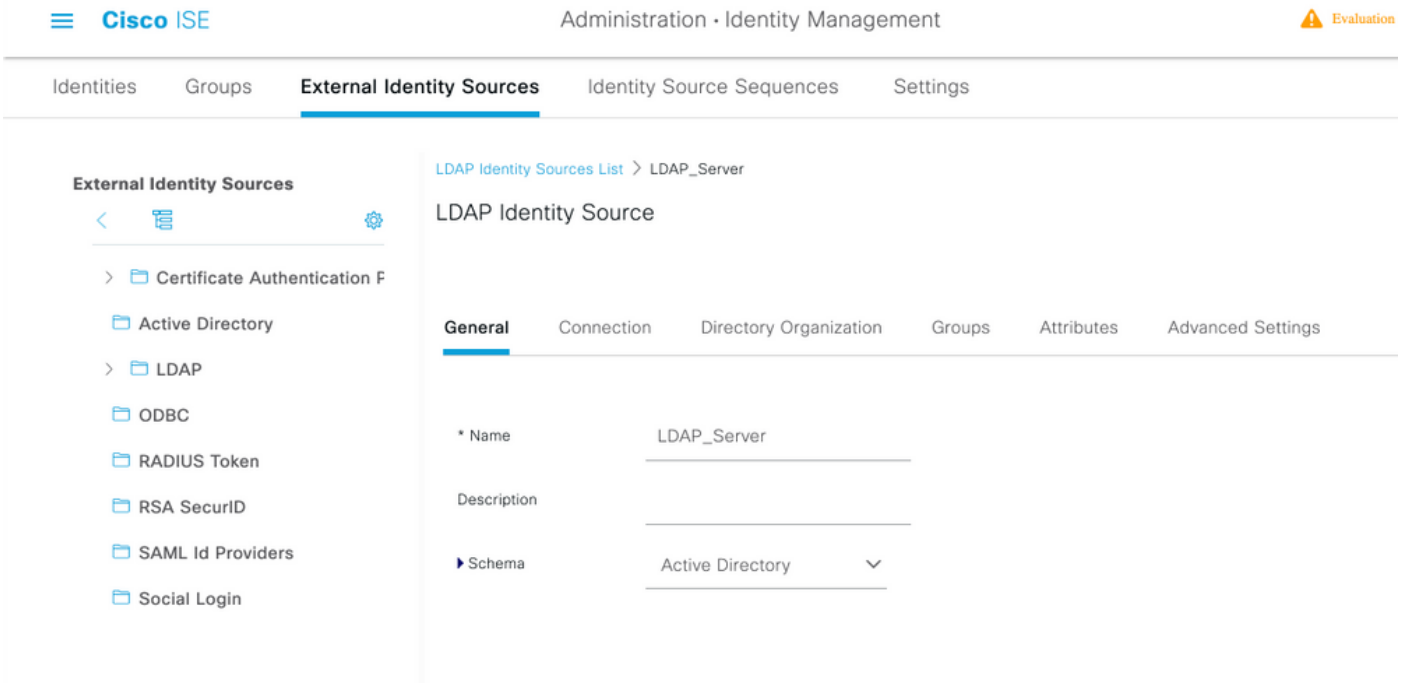
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurations

Utilisez la section ci-dessous pour configurer un utilisateur LDAP afin d'obtenir l'accès administratif / personnalisé à l'interface utilisateur graphique ISE . La configuration ci-dessous utilise les requêtes de protocole LDAP afin de récupérer l'utilisateur à partir d'Active Directory pour effectuer l'authentification.

Rejoindre ISE à LDAP

1. Accédez à **Administration > Identity Management > External Identity Sources > Active Directory > LDAP.**
2. Sous l'onglet **Général**, entrez le nom du LDAP et choisissez le schéma Active Directory.



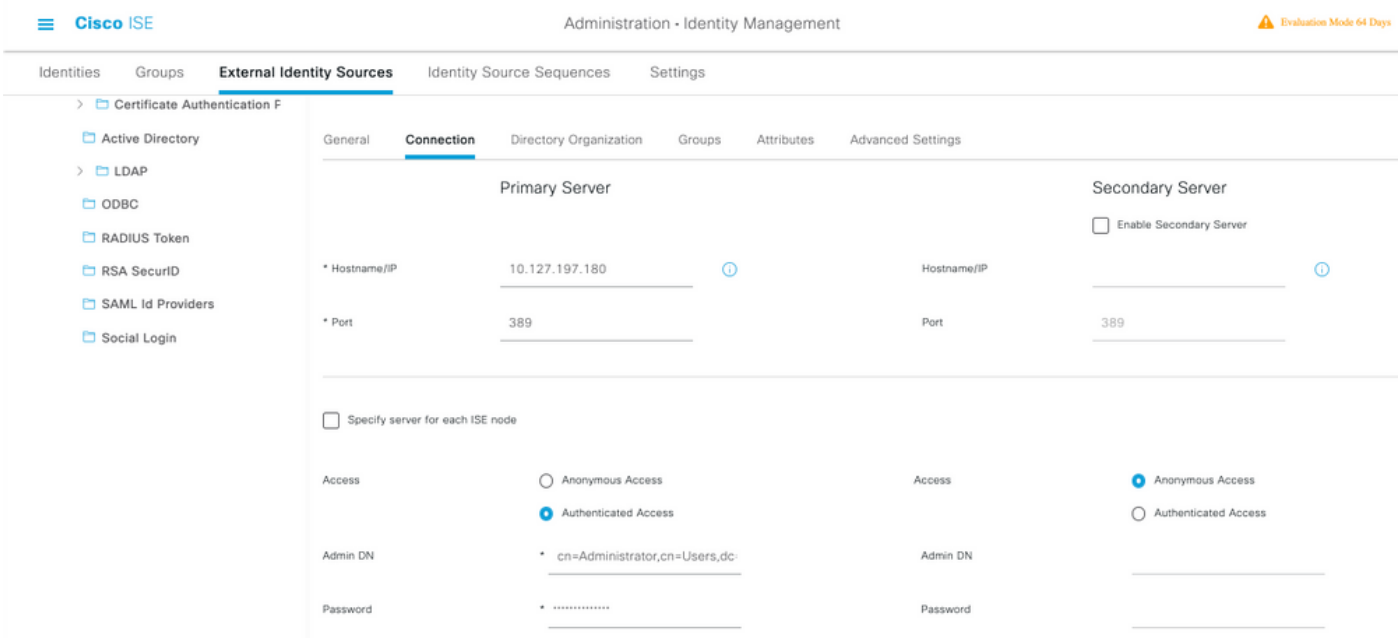
Configurer le type de connexion et la configuration LDAP

1. Accédez à **ISE > Administration > Identity Management > External Identity Sources > LDAP.**

2. Configurez le nom d'hôte du serveur LDAP principal avec le port 389(LDAP)/636 (LDAP-Secure).

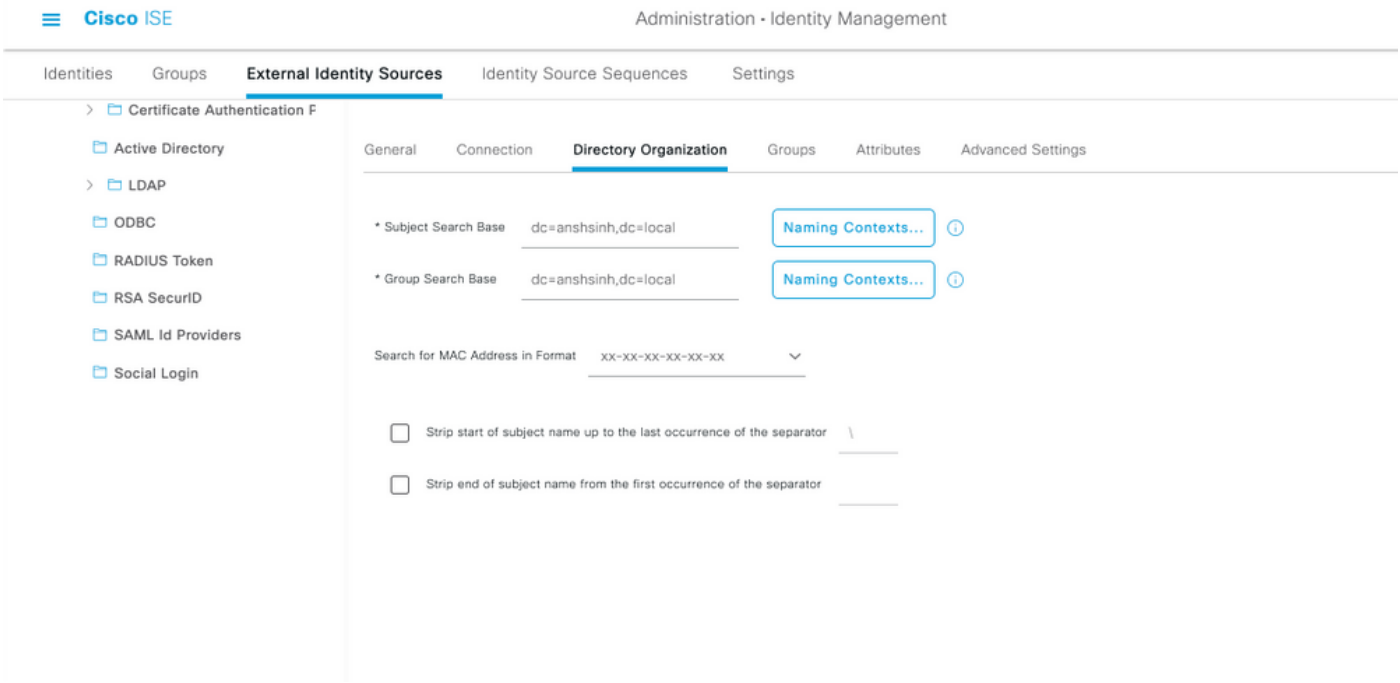
3. Entrez le chemin d'accès du nom unique d'administrateur (DN) avec le mot de passe admin pour le serveur LDAP .

4.Cliquez sur Test Bind Server pour tester l'accessibilité du serveur LDAP à partir d'ISE .



Configurer l'organisation, les groupes et les attributs du répertoire

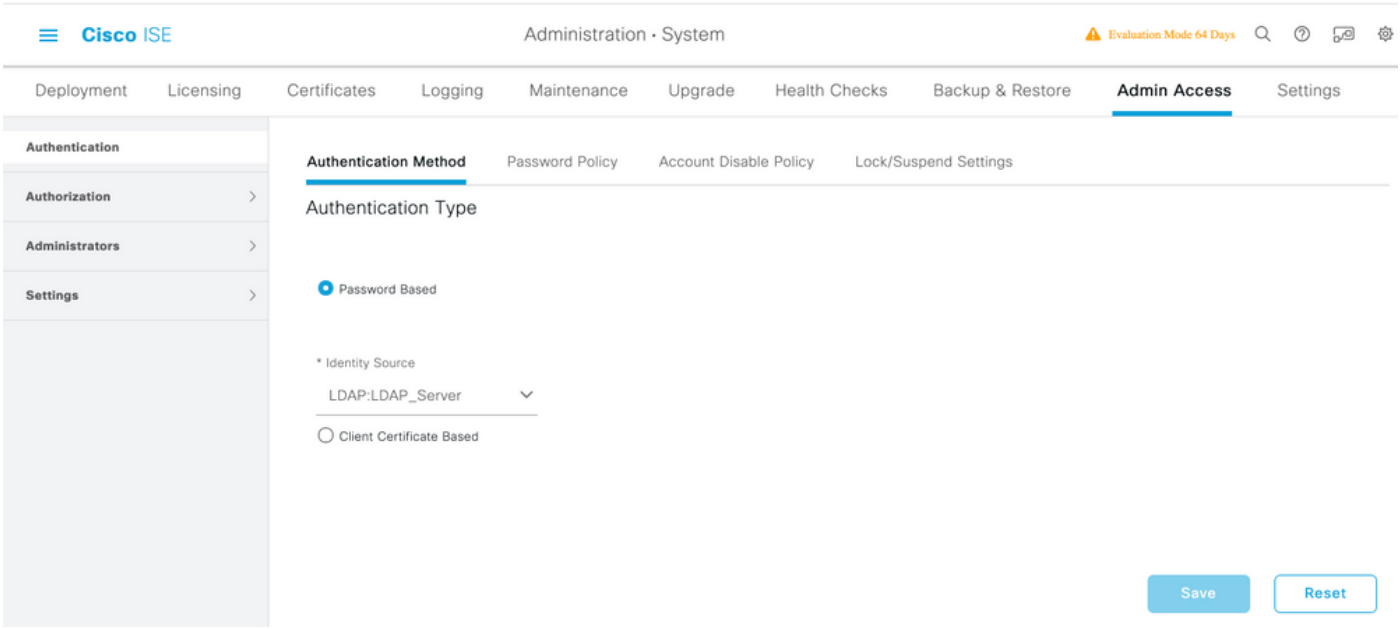
1. Choisissez le groupe Organisation correct de l'utilisateur en fonction de la hiérarchie des utilisateurs stockés dans le serveur LDAP .



Activer l'accès administratif pour les utilisateurs LDAP

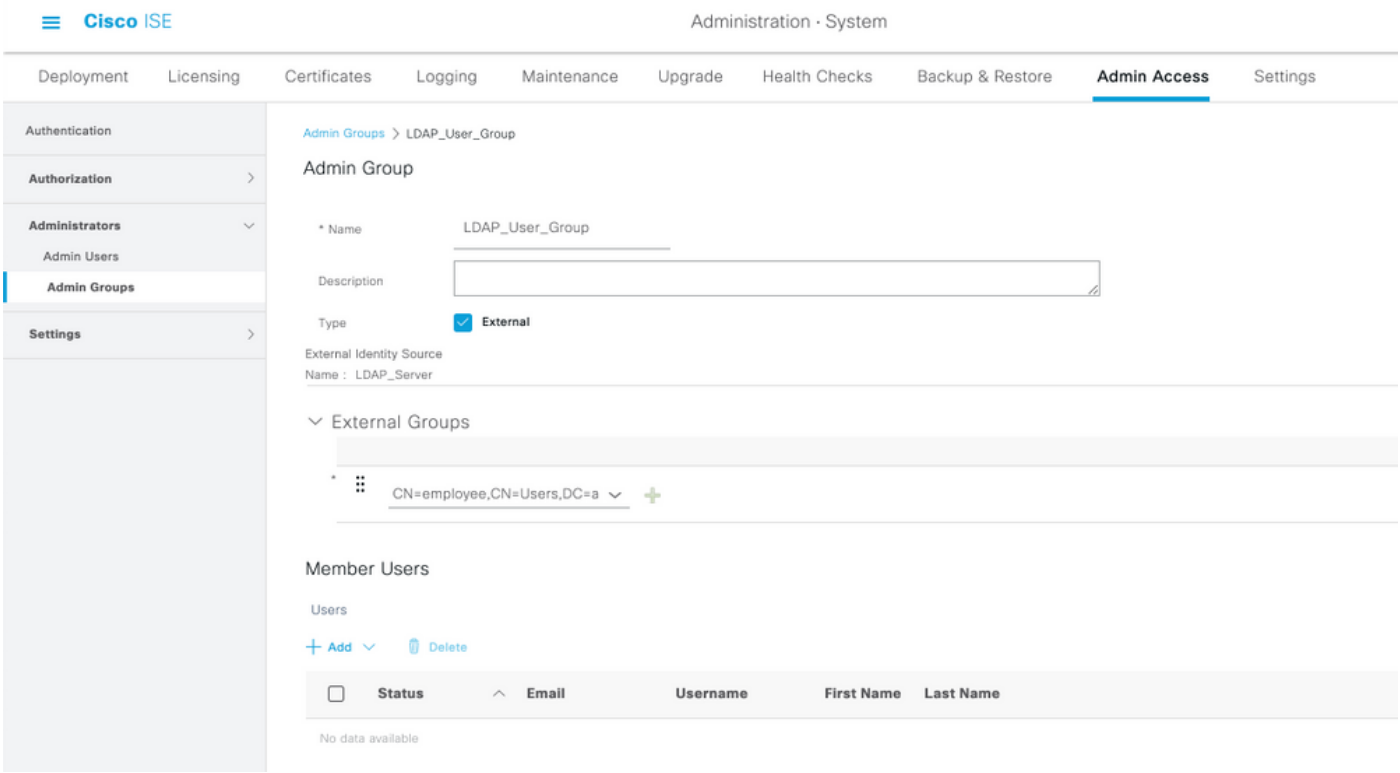
Complétez ces étapes afin d'activer l'authentification basée sur un mot de passe.

1. Accédez à **ISE > Administration > System > Admin Access > Authentication**.
2. Sous l'onglet **Authentication Method**, sélectionnez l'option **Password-Based**.
3. Sélectionnez **LDAP** dans le menu déroulant **Source d'identité**.
4. Cliquez sur **Enregistrer les modifications**.



Mapper le groupe Admin au groupe LDAP

Configurez le groupe Admin sur l'ISE et associez-le au groupe AD. Cela permet à l'utilisateur configuré d'obtenir un accès en fonction des stratégies d'autorisation en fonction des autorisations RBAC configurées pour l'administrateur en fonction de l'appartenance au groupe.

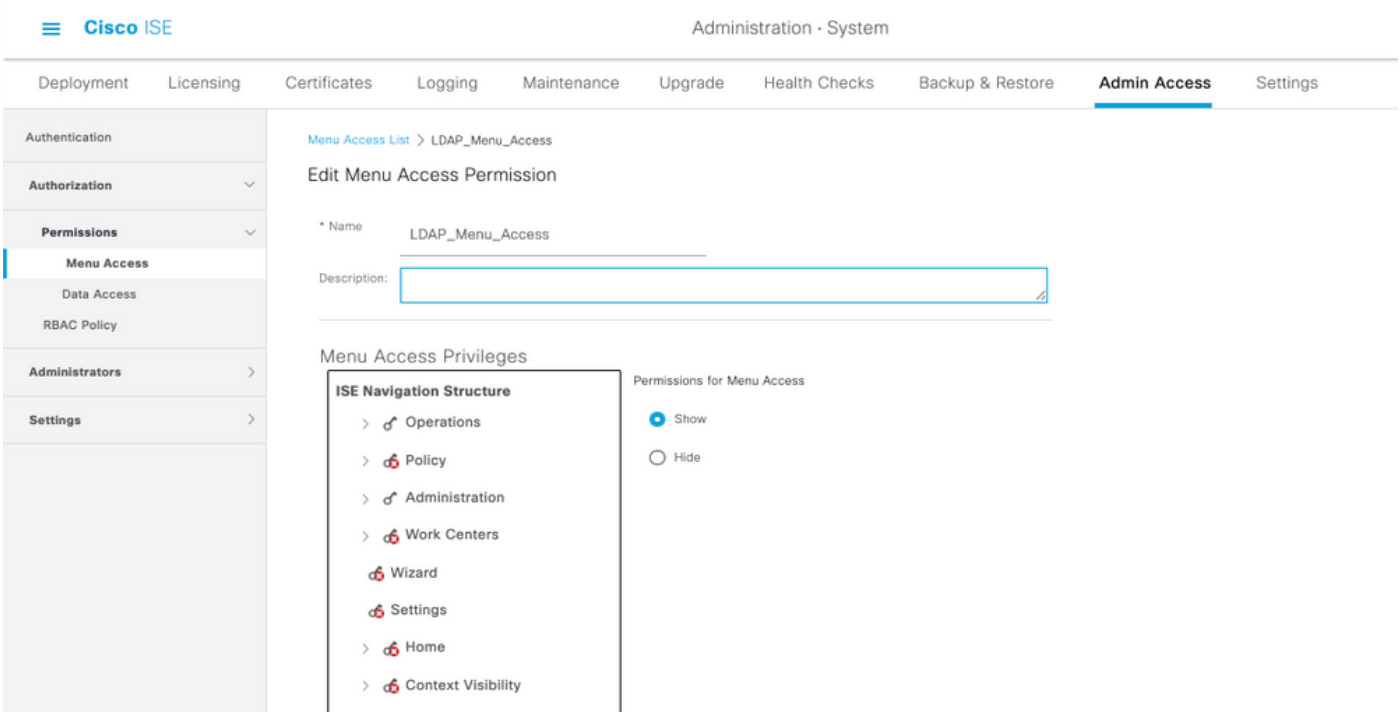


Définir les autorisations d'accès au menu

1. Accédez à **ISE > Administration > System > Authorization > Permissions > Menu access.**

2. Définissez l'accès au menu pour que l'utilisateur administrateur puisse accéder à l'interface utilisateur graphique ISE. Nous pouvons configurer les sous-entités à afficher ou masquer sur l'interface utilisateur graphique pour qu'un utilisateur puisse accéder à un jeu d'opérations uniquement si nécessaire.

3. Cliquez sur **Enregistrer**.

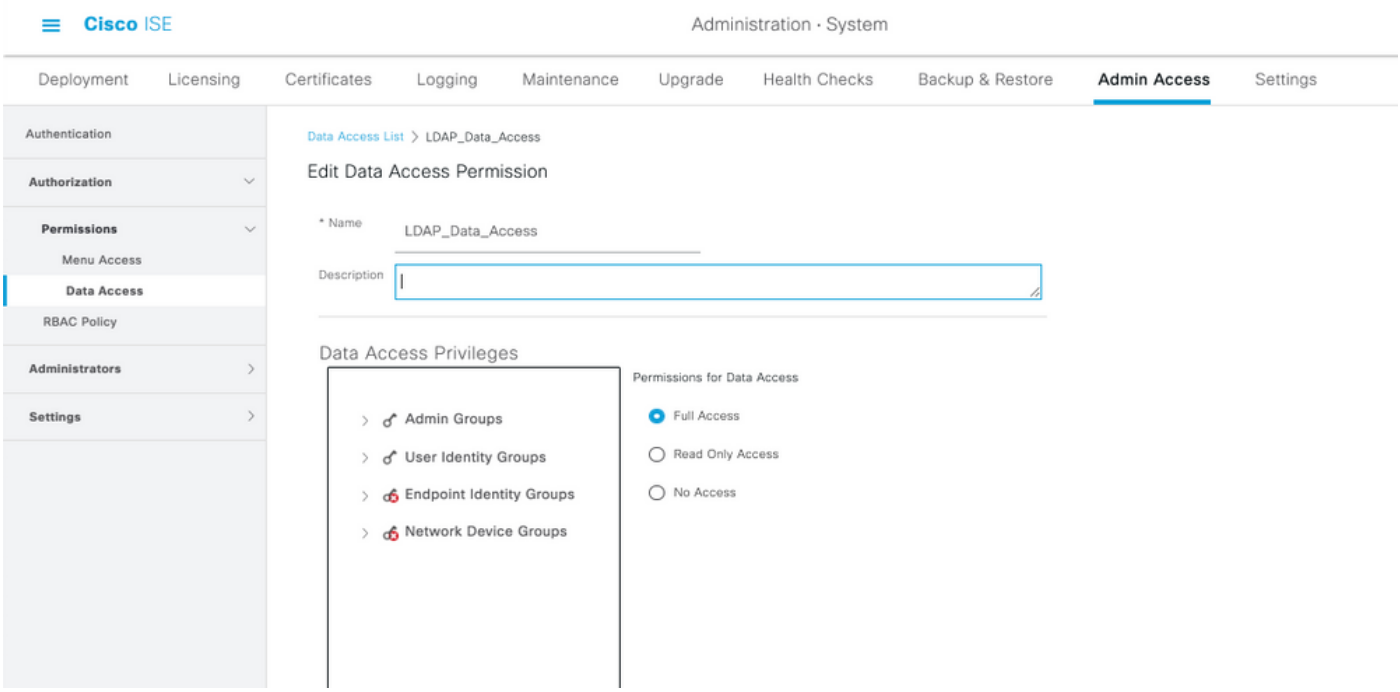


Définir les autorisations d'accès aux données

1. Accédez à **ISE > Administration > System > Authorization > Permissions > Data access.**

2. Définissez l'accès aux données pour que l'utilisateur administrateur dispose d'un accès complet ou en lecture seule aux groupes d'identité sur l'interface utilisateur graphique ISE.

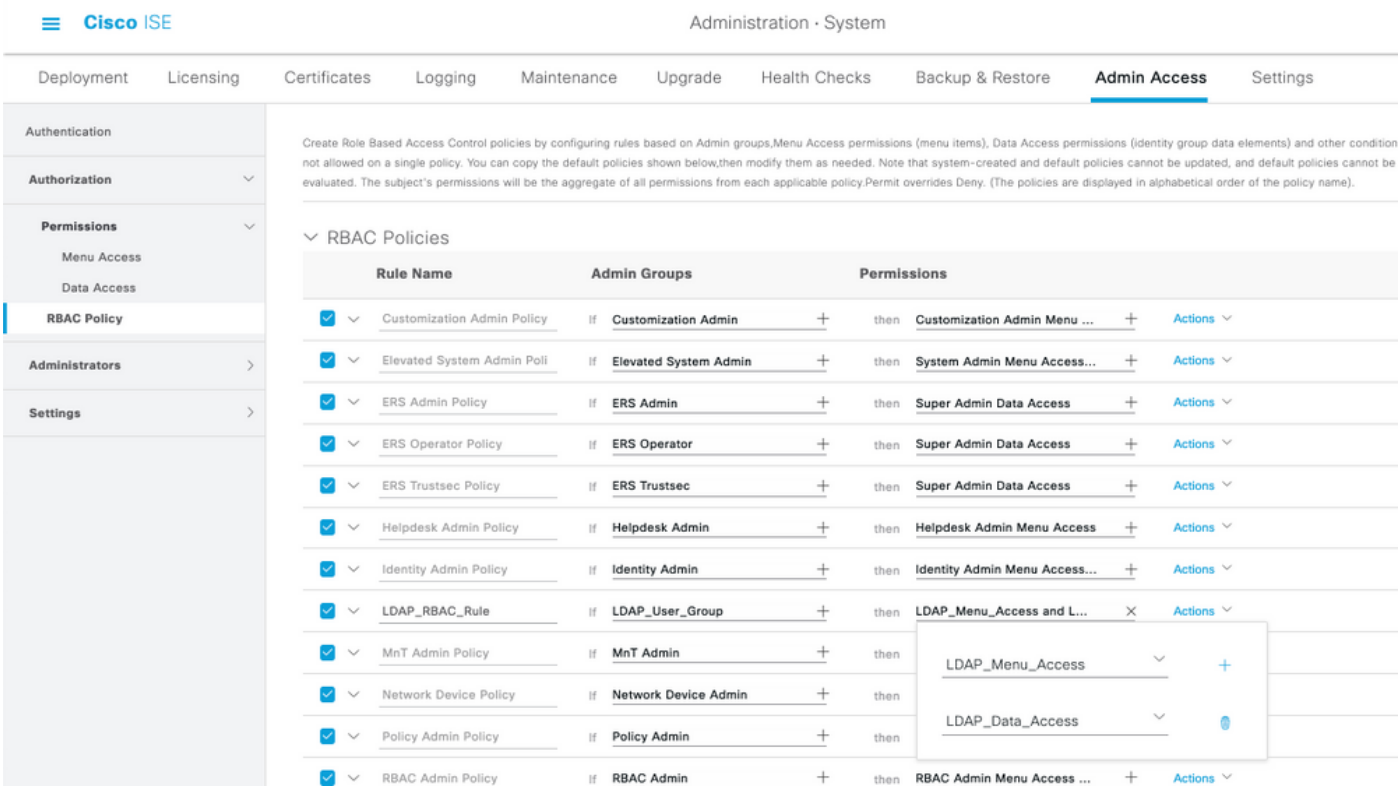
3. Cliquez sur **Enregistrer**.



Définir les autorisations RBAC pour le groupe Admin

1. Accédez à **ISE > Administration > System > Admin Access > Authorization > Policy**.

2. Dans le menu déroulant **Actions** à droite, sélectionnez **Insérer une nouvelle stratégie ci-dessous** afin d'ajouter une nouvelle stratégie.
3. Créez une nouvelle règle appelée LDAP_RBAC_policy et mappez-la avec le groupe d'administration défini dans la section Activer l'accès administratif pour AD, et affectez-lui des autorisations pour l'accès au menu et aux données.
4. Cliquez sur **Enregistrer les modifications**, et la confirmation des modifications enregistrées s'affiche dans le coin inférieur droit de l'interface utilisateur graphique.

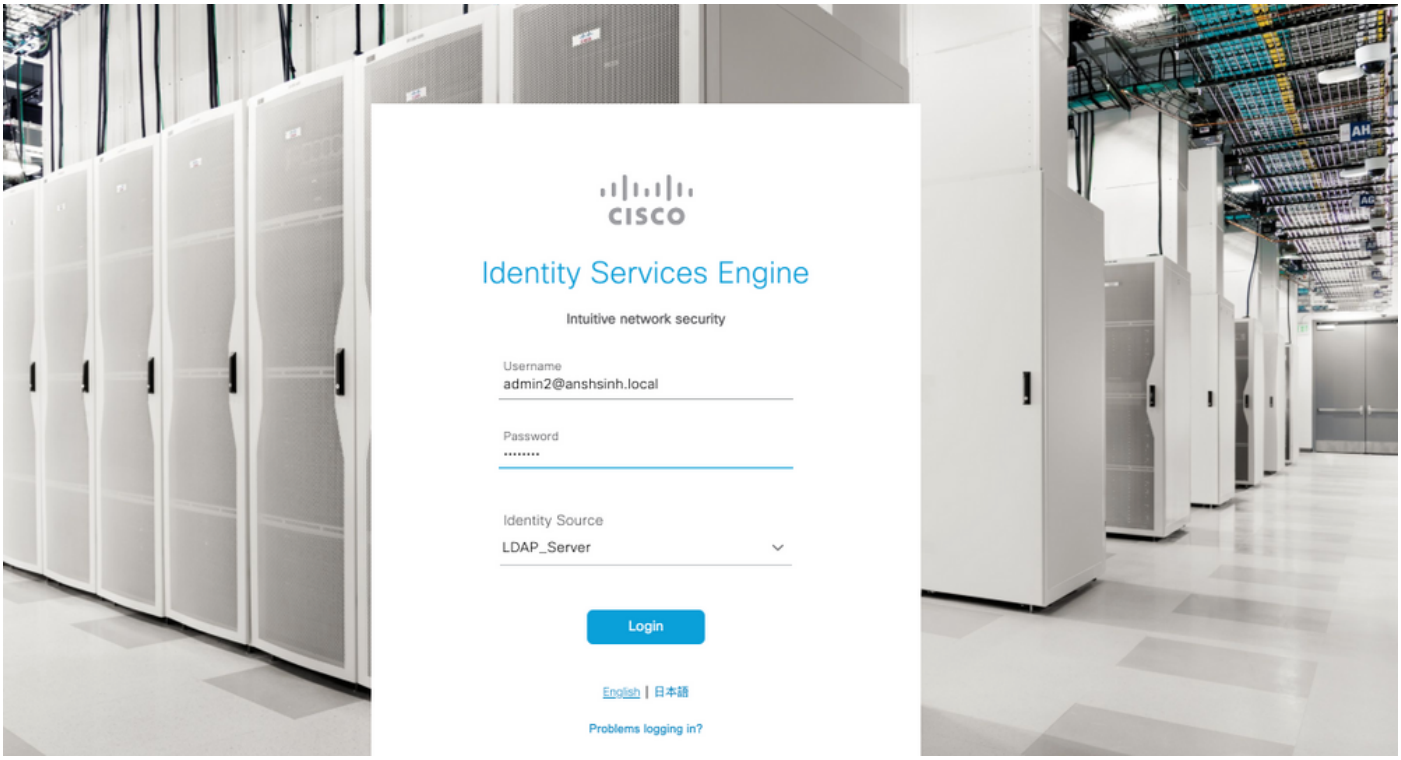


Vérification

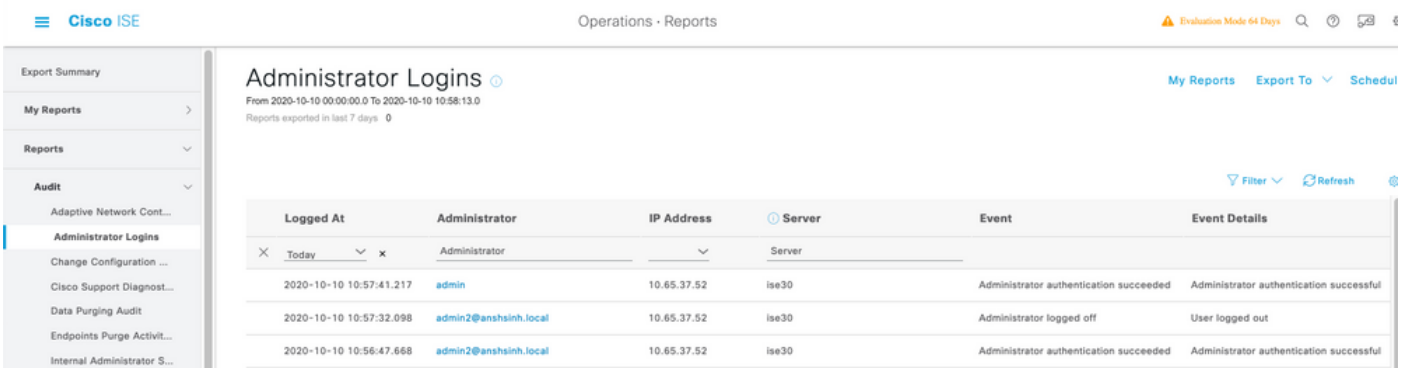
Accéder à ISE avec les identifiants AD

Complétez ces étapes afin d'accéder à ISE avec des informations d'identification AD :

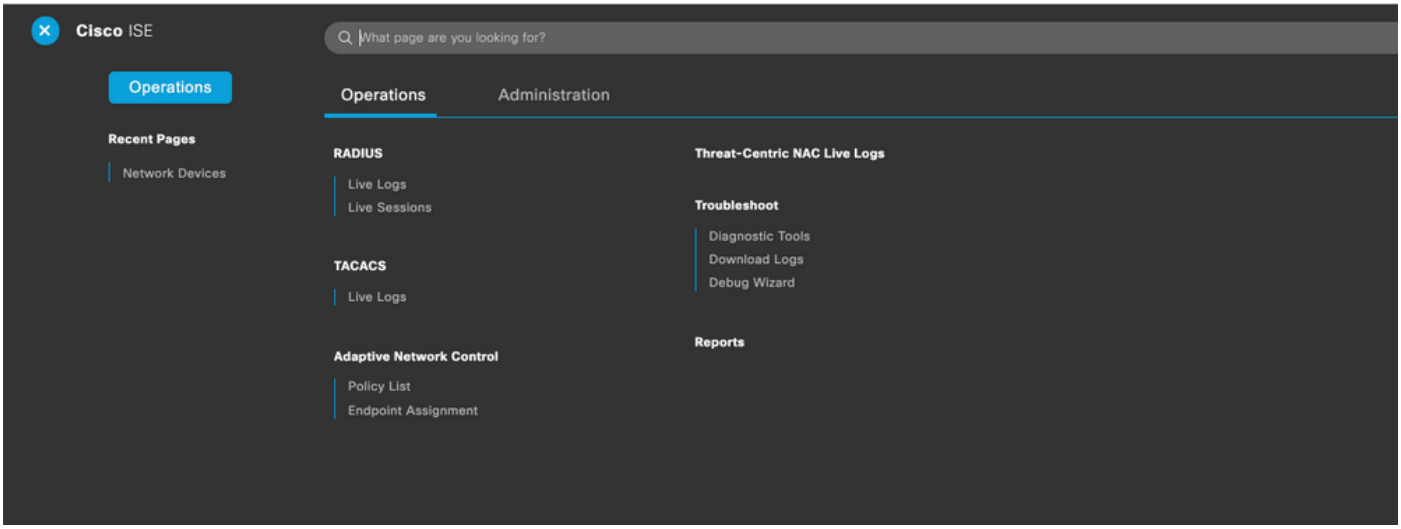
1. Ouvrez l'interface utilisateur ISE pour vous connecter à l'utilisateur LDAP.
2. Sélectionnez LDAP_Server dans le menu déroulant **Source d'identité**.
3. Saisissez le nom d'utilisateur et le mot de passe de la base de données LDAP, puis connectez-vous.



Vérifiez la connexion de l'administrateur dans Rapports d'audit. Accédez à **ISE > Operations > Reports > Audit > Administrators Logins.**



Afin de vérifier que cette configuration fonctionne correctement, vérifiez le nom d'utilisateur authentifié dans le coin supérieur droit de l'interface utilisateur graphique ISE. Définissez un accès personnalisé dont l'accès au menu est limité, comme indiqué ici :



Dépannage

Informations générales

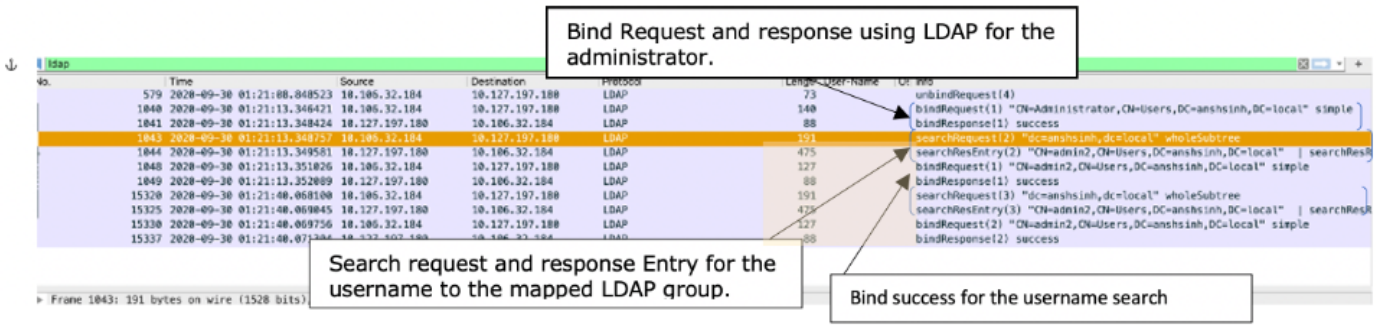
Afin de dépanner le processus RBAC, ces composants ISE doivent être activés dans debug sur le noeud d'administration ISE :

RBAC - Ce message s'affiche lorsque nous tentons de nous connecter (ise-psc.log).

access-filter - Permet d'imprimer l'accès au filtre de ressources (ise-psc.log)

runtime-AAA - Les journaux seront imprimés pour les messages d'interaction LDAP et de connexion (prrt-server.log)

Analyse de capture de paquets



Analyse des journaux

Vérifier le fichier prrt-server.log

```
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
```

Vérifier le fichier ise-psc.log

Àpartir de ces journaux, vous pouvez vérifier la stratégie RBAC utilisée pour l'utilisateur admin2 lors d'une tentative d'accès à la ressource Périphérique réseau -

```
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
```