Configuration du contrôle d'accès basé sur les rôles ISE avec le protocole allégé d'accès aux répertoires

Table des matières

- Introduction
- Conditions préalables
  - Exigences
- Configurations
  - Joindre ISE à LDAP
  - Activer l'accès administratif pour les utilisateurs LDAP
  - Mapper le groupe Admin au groupe LDAP
    - Définir les autorisations pour l'accès au menu
    - Définir les autorisations d'accès aux données
    - Définir les autorisations RBAC pour le groupe Admin
- Vérifier
  - Accès à ISE avec identifiants AD
- Dépannage
  - Informations générales
  - Analyse de capture de paquets
  - Analyse des journaux
    - Vérifiez le fichier port-server.log
    - Vérifiez theise-psc.log

Introduction

Ce document décrit un exemple de configuration pour l'utilisation du protocole LDAP (Lightweight Directory Access Protocol) comme magasin d'identités 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 Versions 3.0
- LDAP

Exigences

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

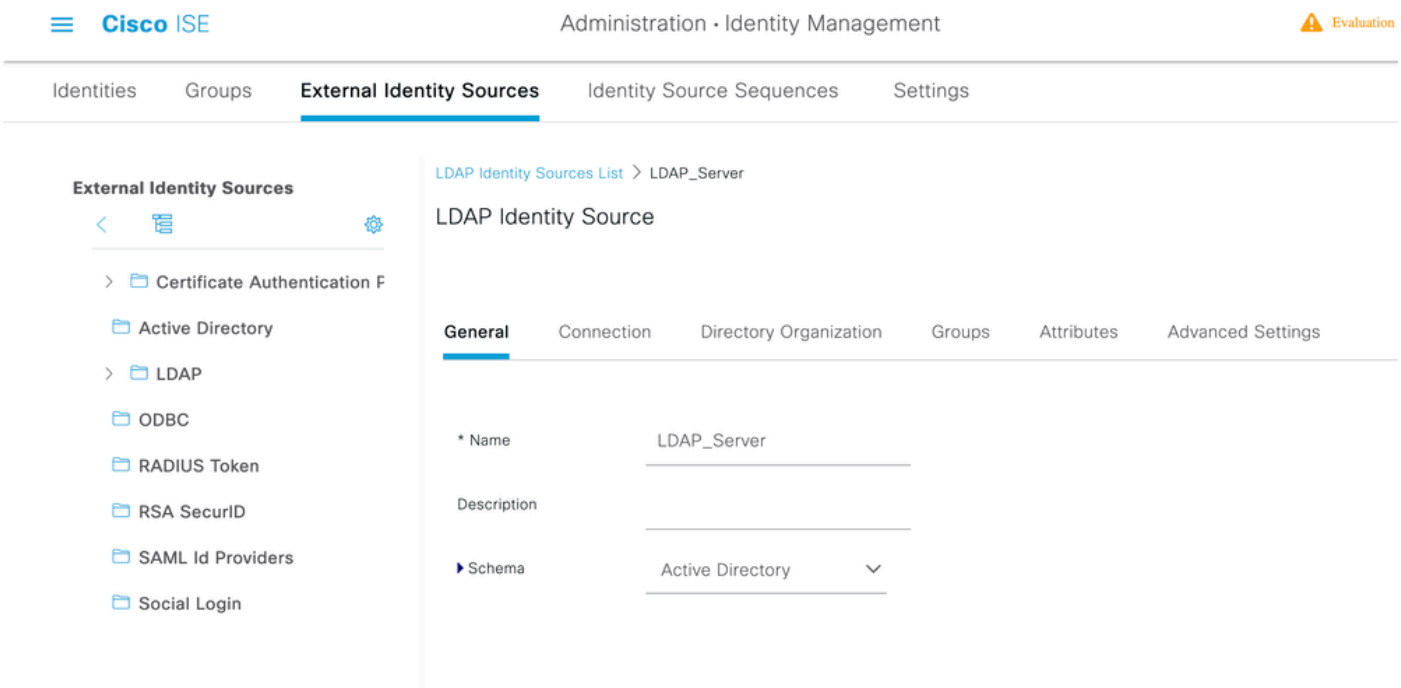
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurations

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

Joindre ISE à LDAP

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



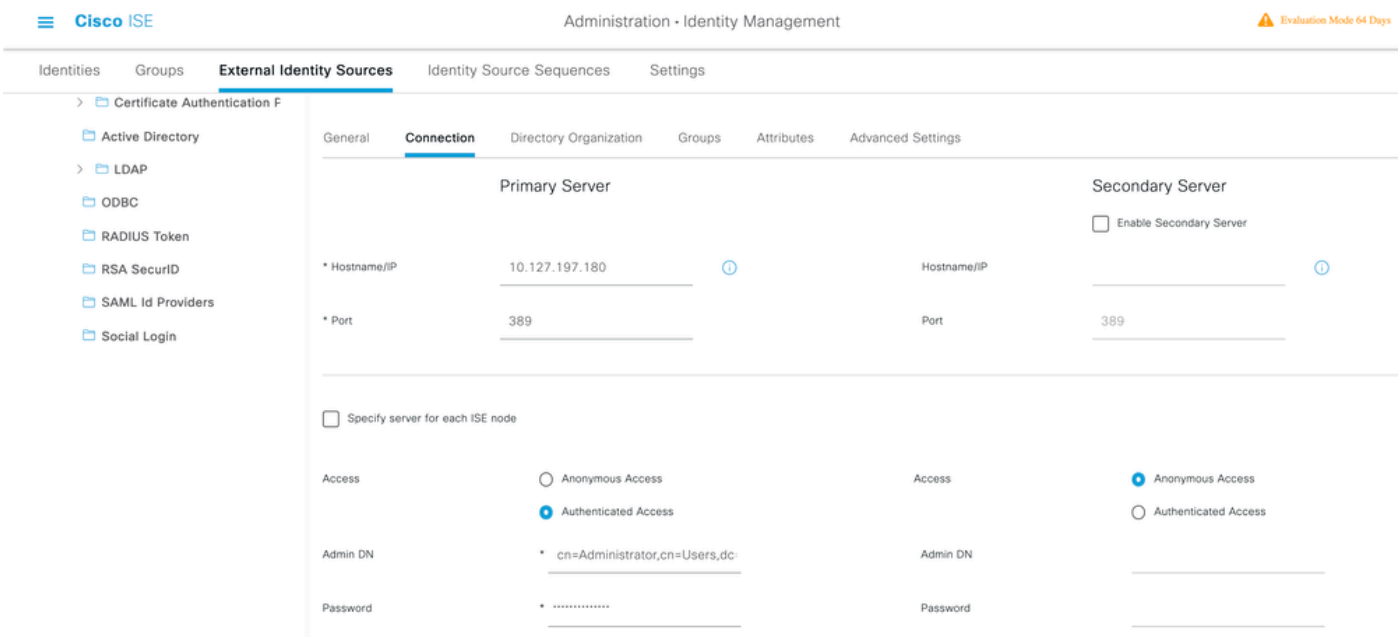
Configurer le type de connexion et la configuration LDAP

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) .

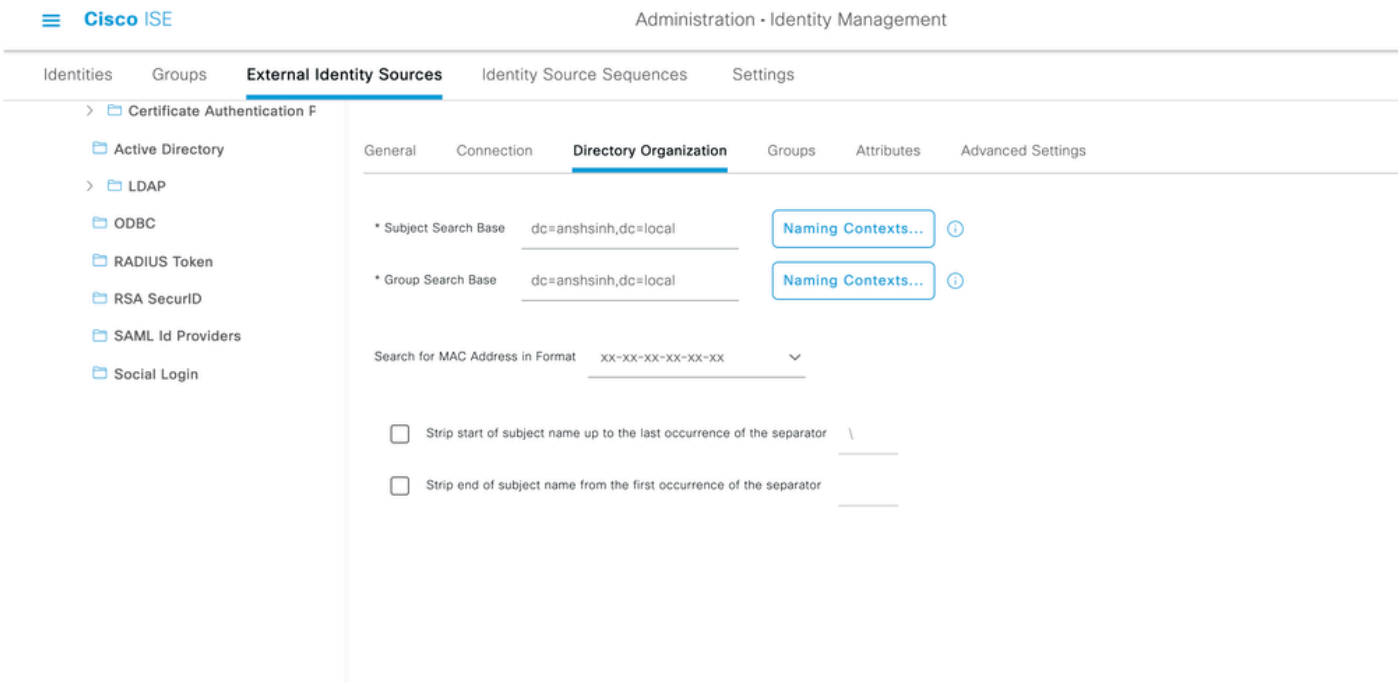
3. Entrez le chemin d'accès du nom distinctif (DN) Admin avec le mot de passe admin pour le serveur LDAP .

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 stockée dans le serveur LDAP .

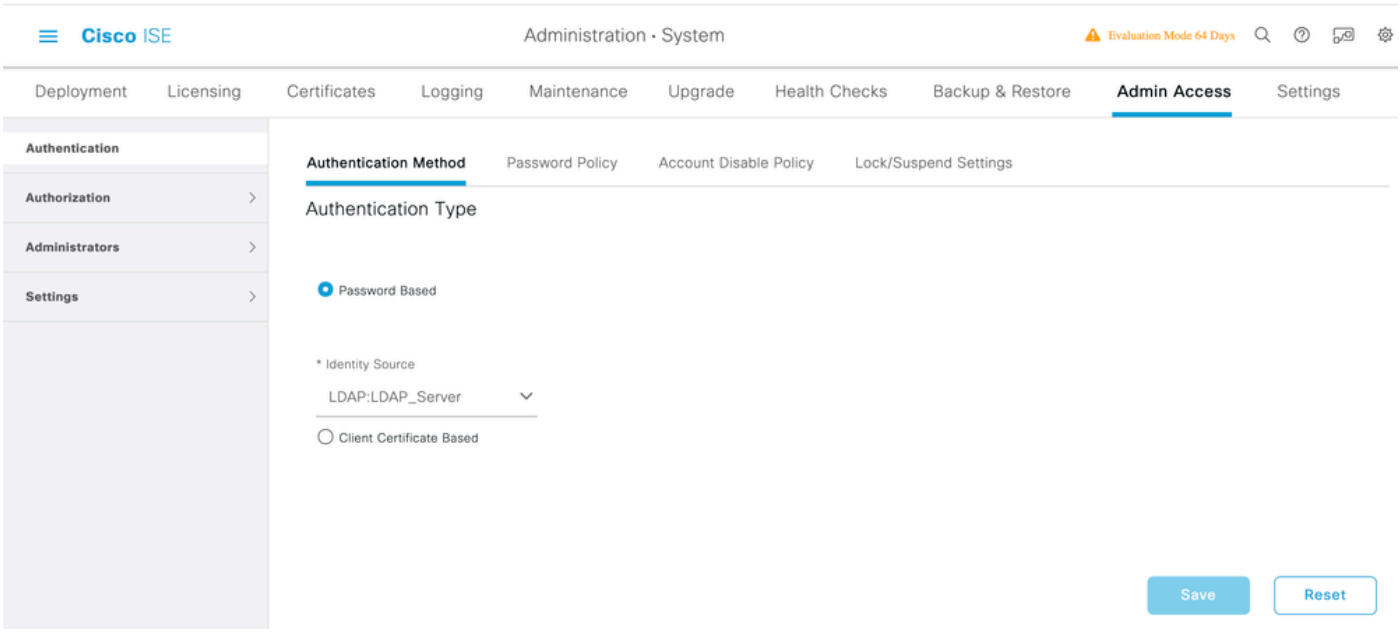


Activer l'accès administratif pour les utilisateurs LDAP

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

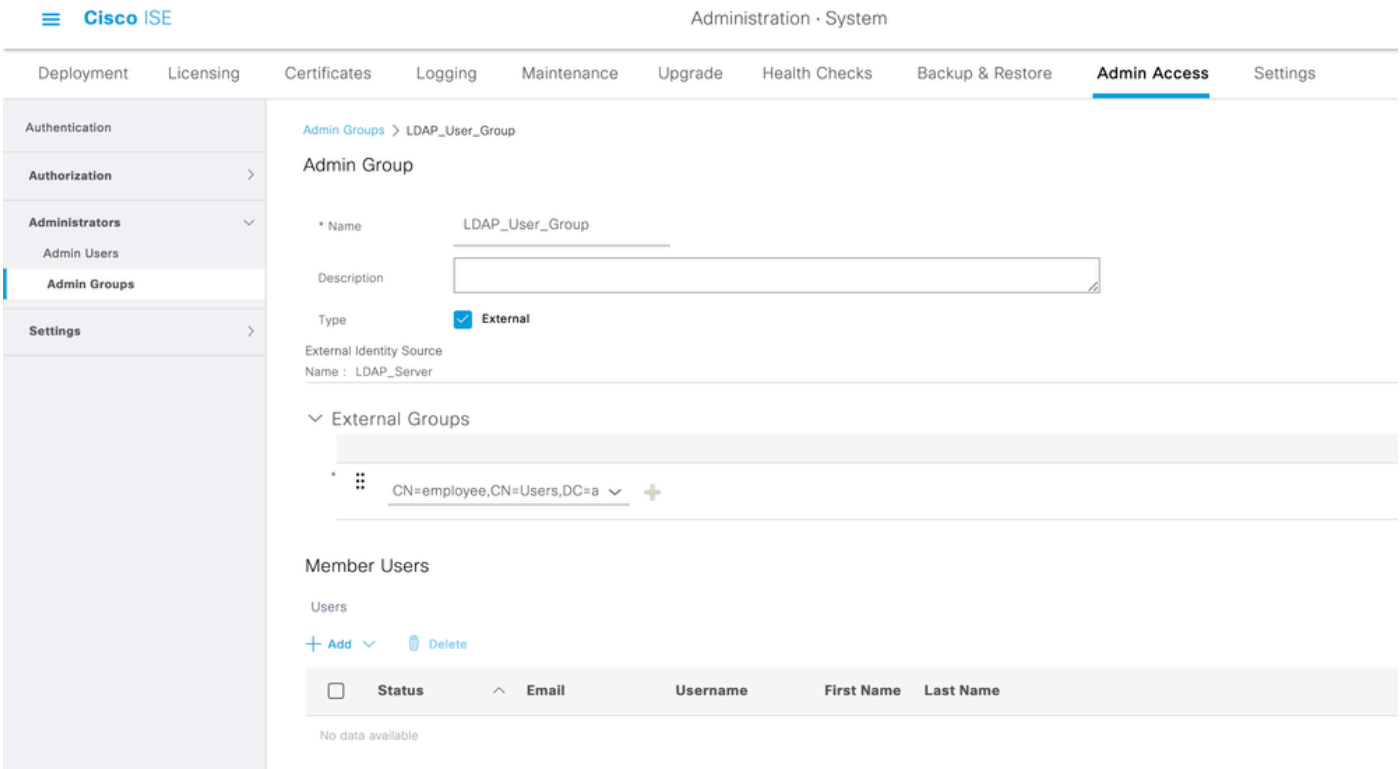
1. Accédez à ISE > Administration > System > Admin Access > Authentication.
2. Sous l'onglet Authentication Method, sélectionnez l'option Password-Based.
3. Sélectionnez LDAP dans le menu déroulant Identity Source.

4. Cliquez sur Enregistrer les modifications.



Mapper le groupe Admin au groupe LDAP

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

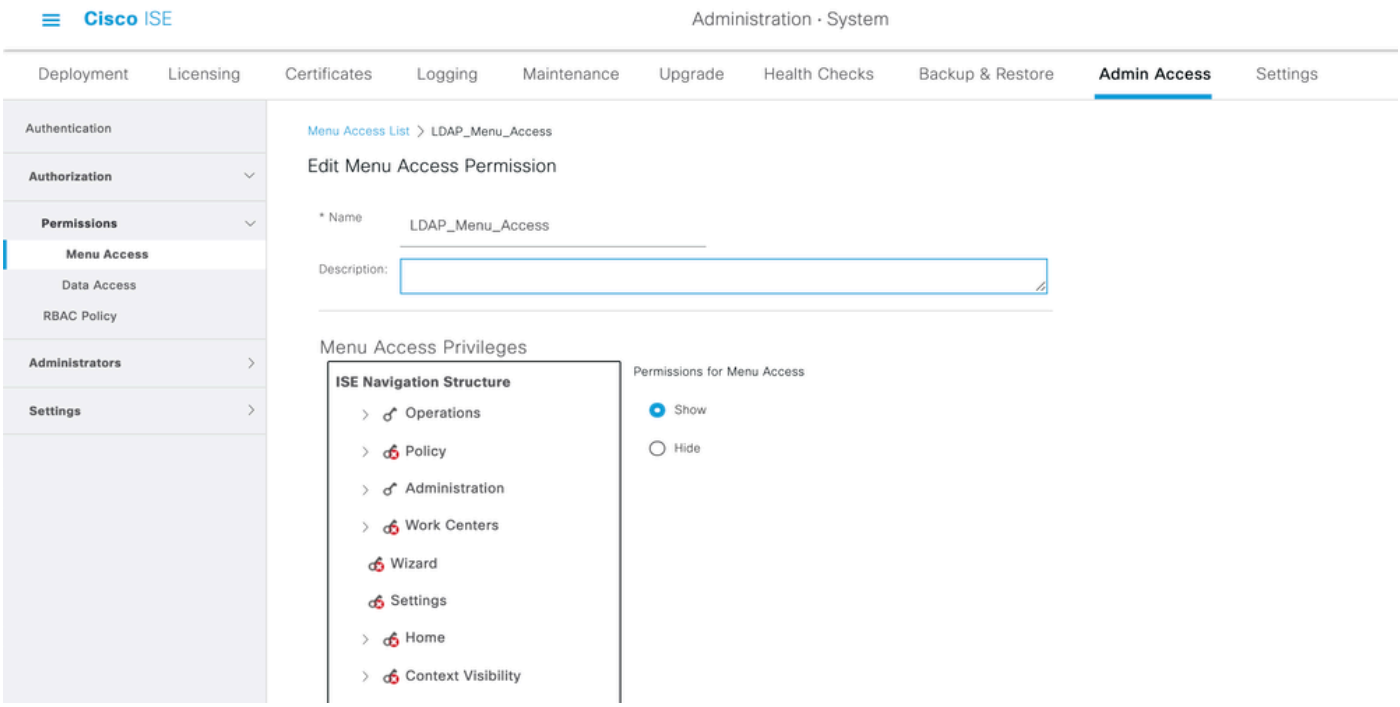


Définir les autorisations pour l'accès au menu

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

2. Définissez l'accès au menu pour que l'utilisateur admin puisse accéder à l'interface utilisateur graphique ISE. Vous pouvez configurer les sous-entités à afficher ou masquer sur l'interface utilisateur graphique pour un accès personnalisé permettant à un utilisateur d'effectuer uniquement un ensemble d'opérations si nécessaire.

3. Cliquez sur Enregistrer.

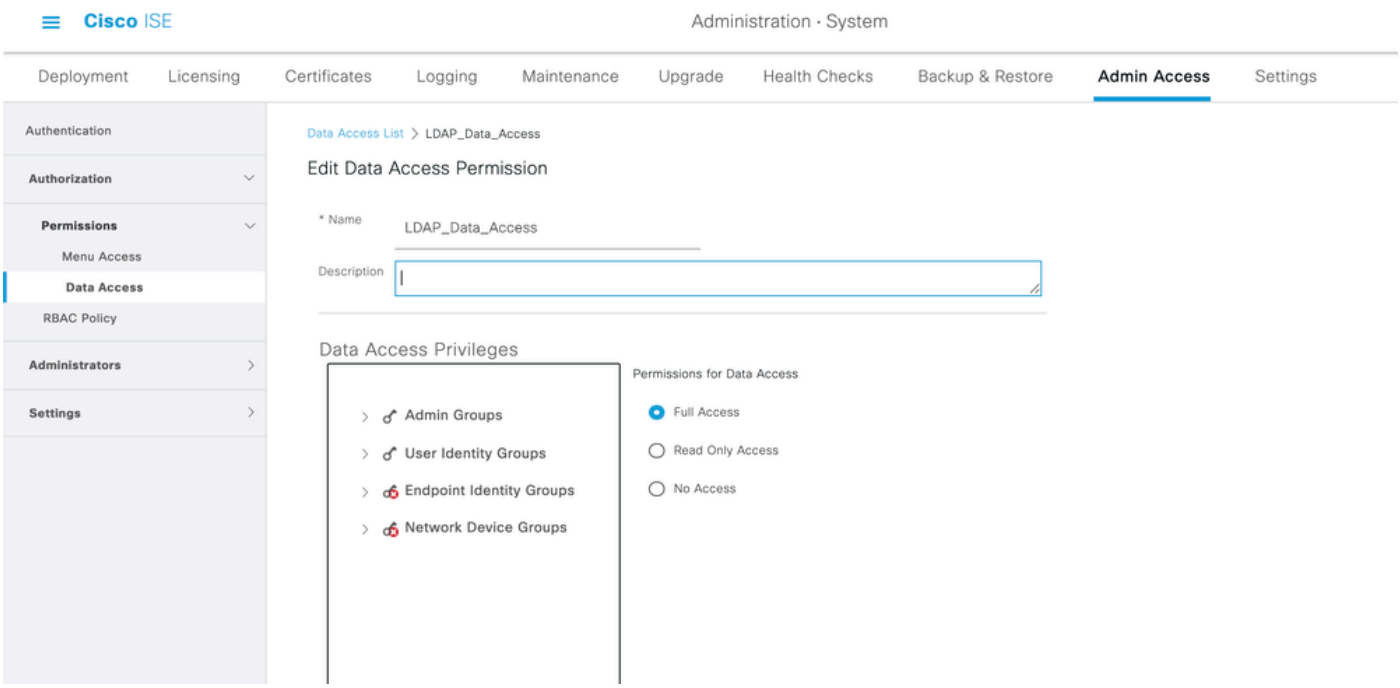


Définir les autorisations d'accès aux données

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

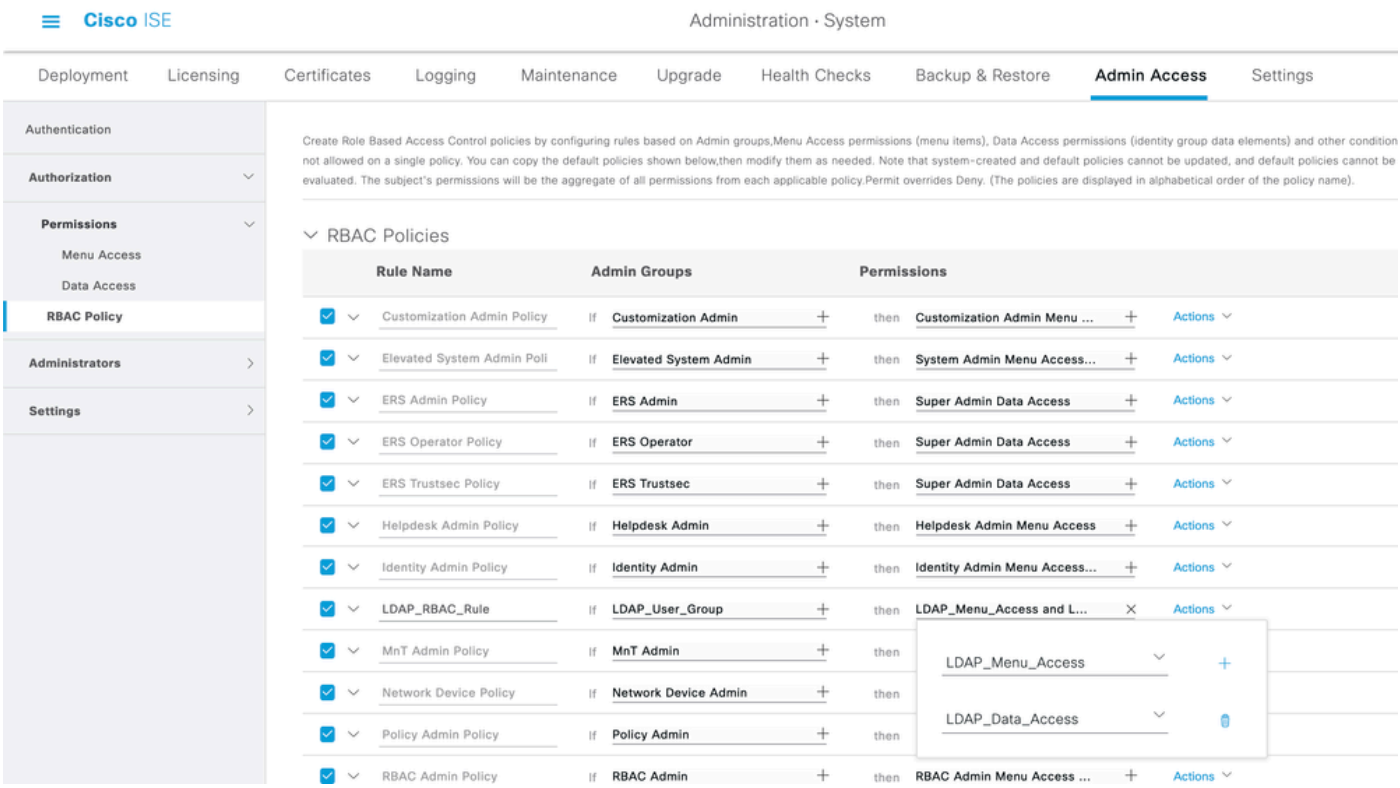
2. Définissez l'accès aux données pour que l'utilisateur admin dispose d'un accès complet ou en lecture seule aux groupes d'identité sur l'interface utilisateur graphique ISE.

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 pour ajouter une nouvelle stratégie.
3. Créez une nouvelle règle appelée LDAP_RBAC_policy, mappez-la avec le groupe Admin défini dans la section Activer l'accès administratif pour AD, et attribuez-lui des autorisations d'accès au menu et aux données.
4. Cliquez sur Save Changes et la confirmation des modifications enregistrées s'affiche dans le coin inférieur droit de l'interface utilisateur graphique.



Remarque : L'utilisateur super admin ne peut pas modifier les stratégies et autorisations RBAC générées par le système par défaut. Pour ce faire, vous devez créer de nouvelles stratégies RBAC avec les autorisations nécessaires en fonction de vos besoins, et mapper ces stratégies à un groupe d'administrateurs.

Remarque : seul un utilisateur administrateur du groupe Super Admin par défaut peut modifier ou supprimer d'autres utilisateurs administrateur. Même un utilisateur mappé en externe qui fait partie d'un groupe d'administrateurs cloné avec les privilèges Menu et Accès aux données du groupe Super Admin ne peut pas modifier ou supprimer un utilisateur admin.

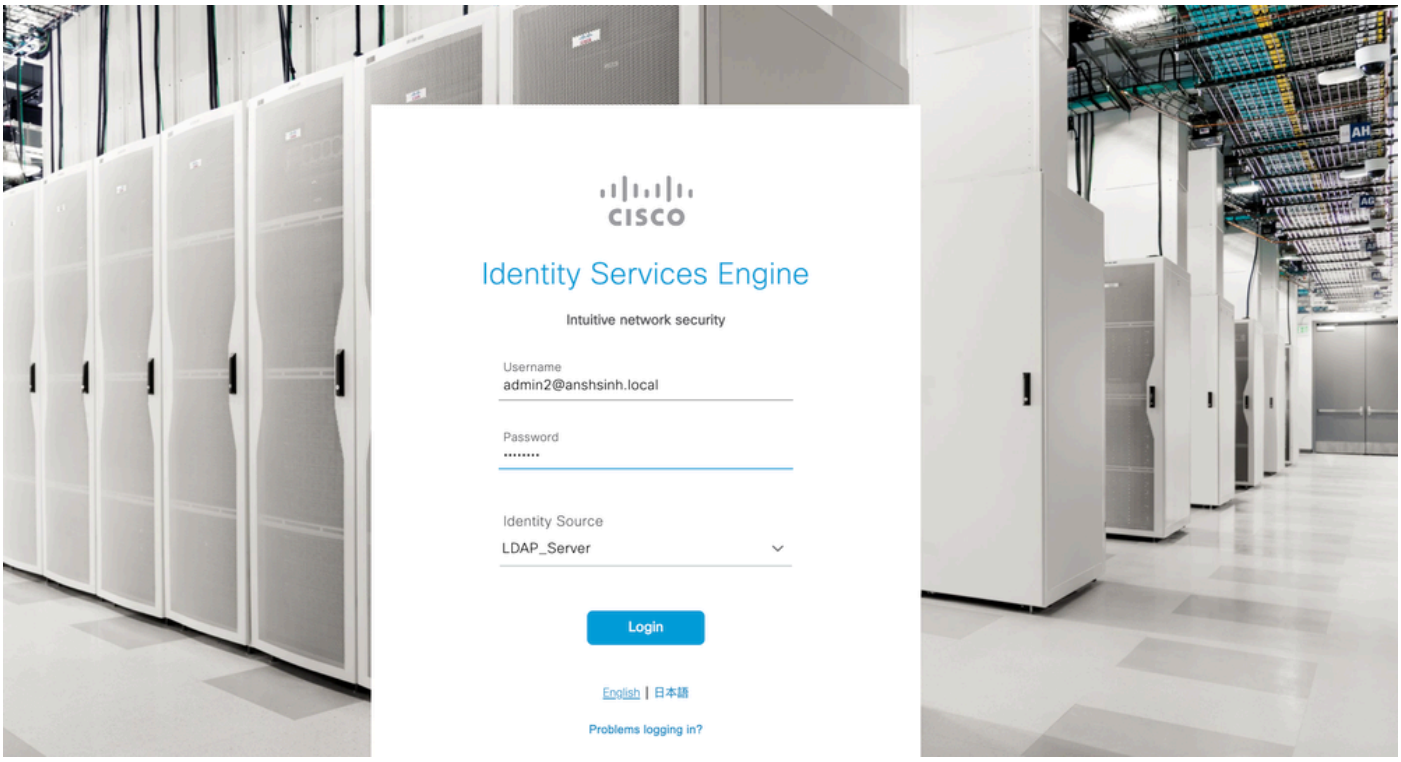
Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

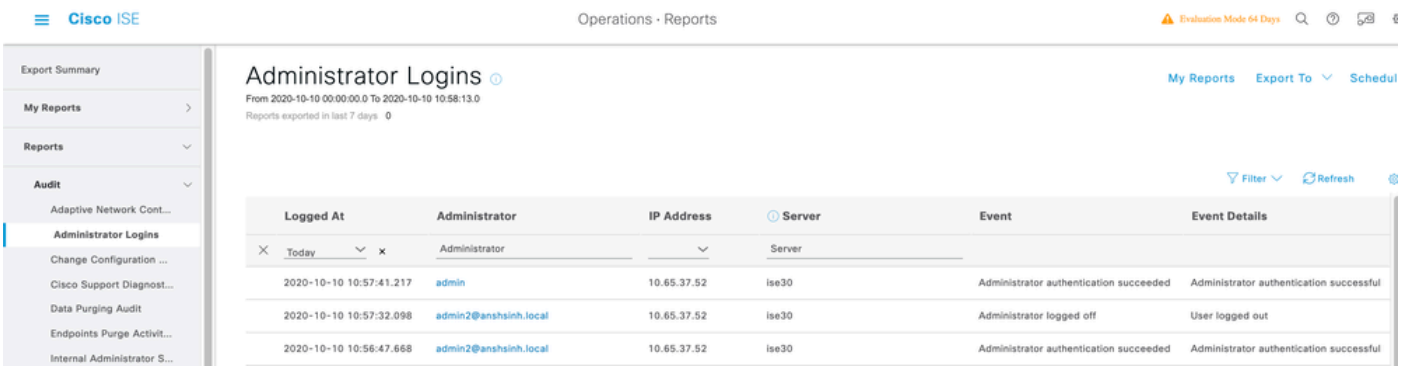
Accès à ISE avec identifiants AD

Suivez ces étapes pour accéder à ISE avec les informations d'identification AD :

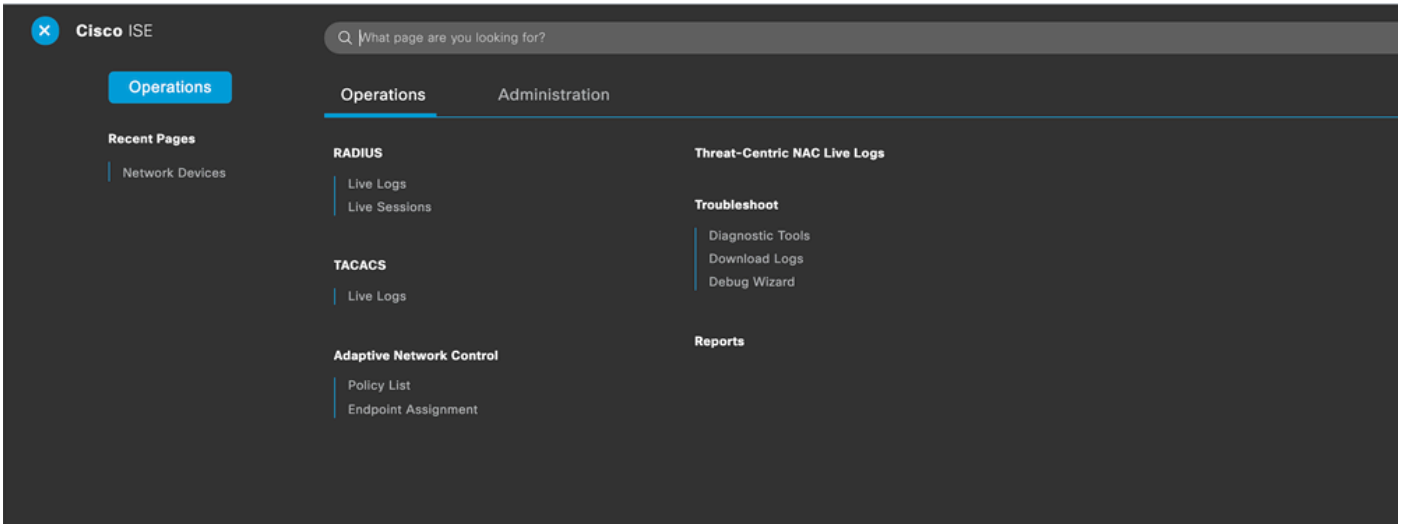
1. Ouvrez l'interface utilisateur graphique ISE pour vous connecter avec l'utilisateur LDAP.
2. Sélectionnez LDAP_Server dans le menu déroulant Identity Source.
3. Saisissez le nom UPN et le mot de passe de la base de données LDAP, puis connectez-vous.



Vérifiez la connexion pour les connexions administrateur dans Rapports d'audit. Accédez à ISE > Operations > Reports > Audit > Administrators Logins.



Pour 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 qui dispose d'un accès limité au menu, comme indiqué ici :



Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Informations générales

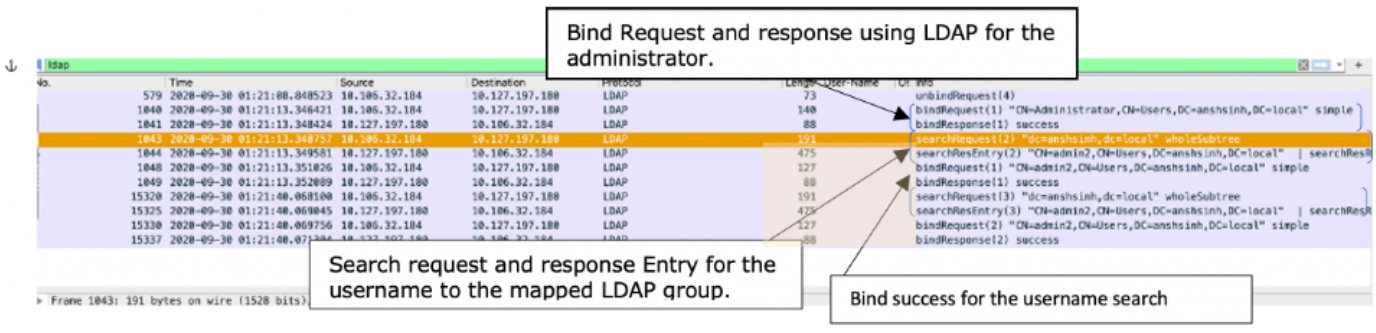
Pour dépanner le processus RBAC, ces composants ISE doivent être activés lors du débogage sur le noeud d'administration ISE :

RBAC : affiche le message RBAC lorsque nous essayons de nous connecter (ise-psc.log)

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

runtime-AAA - Affiche les journaux pour les messages de connexion et d'interaction LDAP (prt-server.log)

Analyse de capture de paquets



Analyse des journaux

Vérifiez le fichier prrt-server.log

```
PAPAuthenticator,2020-10-10 08:54:00,621,DEBUG,0x7f852bee3700,cntx=0002480105,sesn=ise30/389444264/3178

IdentitySequence,2020-10-10 08:54:00,627,DEBUG,0x7f852c4e9700,cntx=0002480105,sesn=ise30/389444264/3178

LDAPIDStore,2020-10-10 08:54:00,628,DEBUG,0x7f852c4e9700,cntx=0002480105,sesn=ise30/389444264/3178,CPMS

Server,2020-10-10 08:54:00,634,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessio

Connection,2020-10-10 08:54:00,634,DEBUG,0x7f85293b8700,LdapConnectionContext::sendSearchRequest(id = 1

Server,2020-10-10 08:54:00,635,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessio

Server,2020-10-10 08:54:00,635,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessio

Server,2020-10-10 08:54:00,636,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessio

Server,2020-10-10 08:54:00,636,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessio

Connection,2020-10-10 08:54:00,636,DEBUG,0x7f85293b8700,LdapConnectionContext::sendBindRequest(id = 122

Server,2020-10-10 08:54:00,640,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessio



LDAPIDStore,2020-10-10 08:54:00,641,DEBUG,0x7f852c6eb700,cntx=0002480105,sesn=ise30/389444264/3178,CPMS
```

Vérifiez le fichier ise-psc.log

À partir de ces journaux, vous pouvez vérifier la stratégie RBAC utilisée par l'utilisateur admin2 lorsqu'il tente d'accéder à la ressource Périphérique réseau.

```
2020-10-10 08:54:24,474 DEBUG  [admin-http-pool51][] com.cisco.cpm.rbacfilter.AccessUtil -:admin2@anshs

2020-10-10 08:54:24,524 INFO   [admin-http-pool51][] cpm.admin.ac.actions.NetworkDevicesLPInputAction -

2020-10-10 08:54:24,524 DEBUG  [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -:a
```

```
2020-10-10 08:54:24,526 DEBUG  [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImp
2020-10-10 08:54:24,526 DEBUG  [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImp
2020-10-10 08:54:24,528 DEBUG  [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -:a
2020-10-10 08:54:24,528 INFO   [admin-http-pool51][] cpm.admin.ac.actions.NetworkDevicesLPInputAction -
2020-10-10 08:54:24,534 INFO   [admin-http-pool51][] cisco.cpm.admin.license.TrustSecLicensingUIFilter
2020-10-10 08:54:24,593 DEBUG  [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -:a
2020-10-10 08:54:24,595 DEBUG  [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImp
2020-10-10 08:54:24,597 DEBUG  [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImp
2020-10-10 08:54:24,604 INFO   [admin-http-pool51][] cisco.cpm.admin.license.TrustSecLicensingUIFilter
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.