Control de acceso basado en roles ISE con LDAP

Contenido

Introducción

Este documento describe un ejemplo de configuración para el uso del protocolo ligero de acceso a directorios (LDAP) como almacén de identidad externo para el acceso administrativo a la GUI de administración de Cisco Identity Services Engine (ISE).

Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de las versiones 3.0 de Cisco ISE
- LDAP (protocolo ligero de acceso a directorios)

Requirements

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ISE versión 3.0
- Windows Server 2016

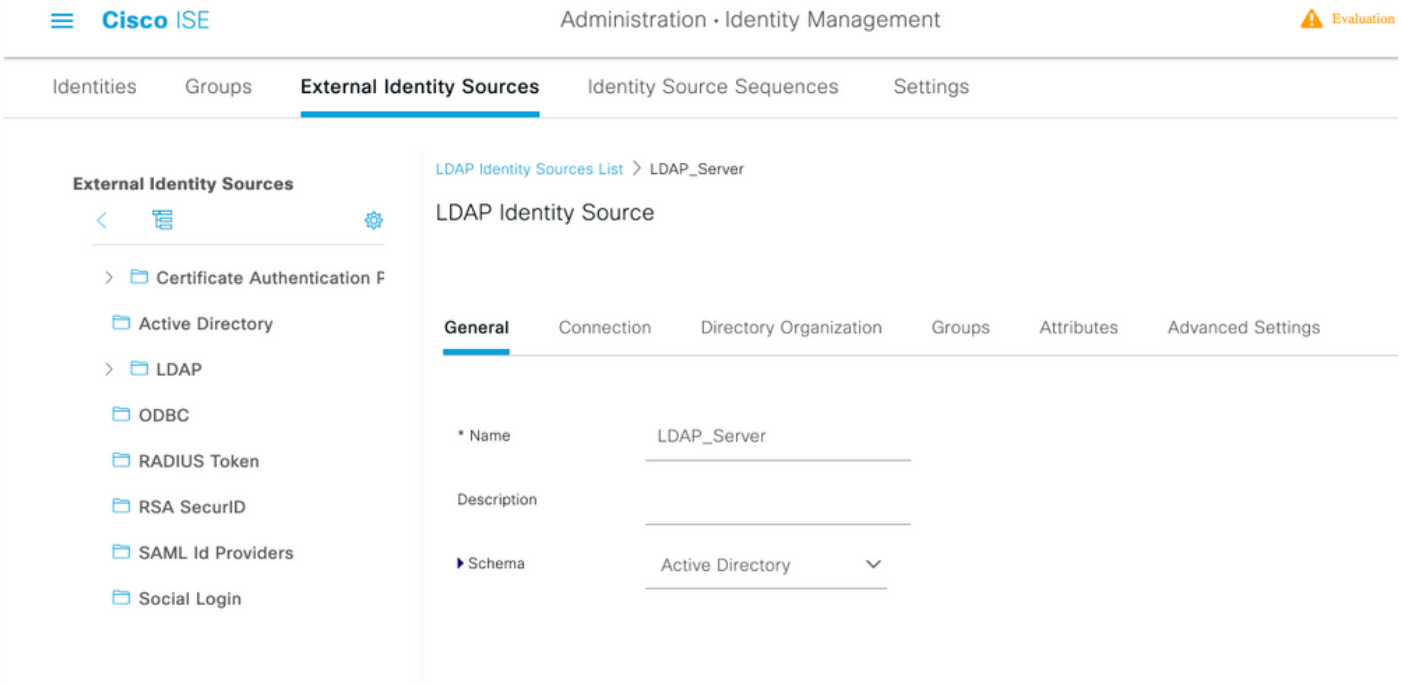
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuraciones

Utilice la siguiente sección para configurar un usuario basado en LDAP para obtener el acceso administrativo/personalizado basado en la GUI de ISE . La siguiente configuración utiliza las consultas del protocolo LDAP para obtener al usuario del directorio activo para realizar la autenticación.

Unir ISE a LDAP

1. Vaya a **Administration > Identity Management > External Identity Sources > Active Directory > LDAP.**
2. Bajo la ficha **General**, ingrese el nombre del LDAP y elija el esquema Active Directory.



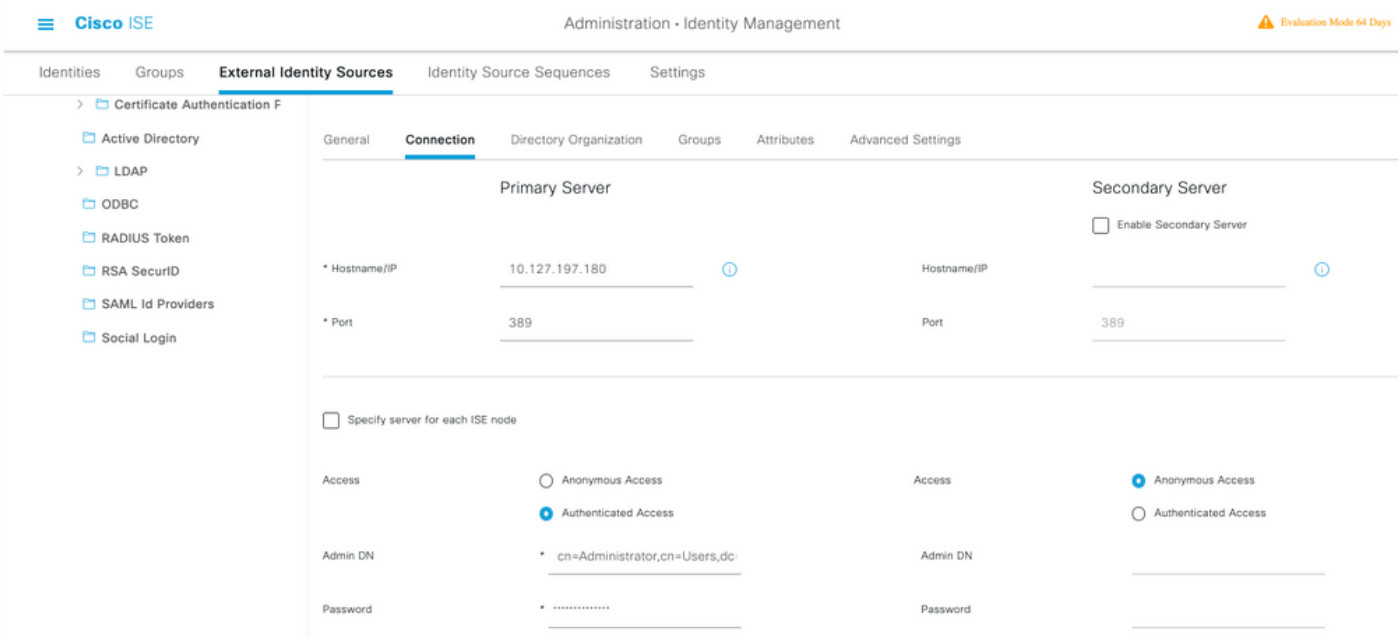
Configurar el tipo de conexión y la configuración LDAP

1. Vaya a **ISE > Administration > Identity Management > External Identity Sources > LDAP.**

2. Configure el nombre de host del servidor LDAP primario junto con el puerto 389(LDAP)/636 (LDAP-Secure) .

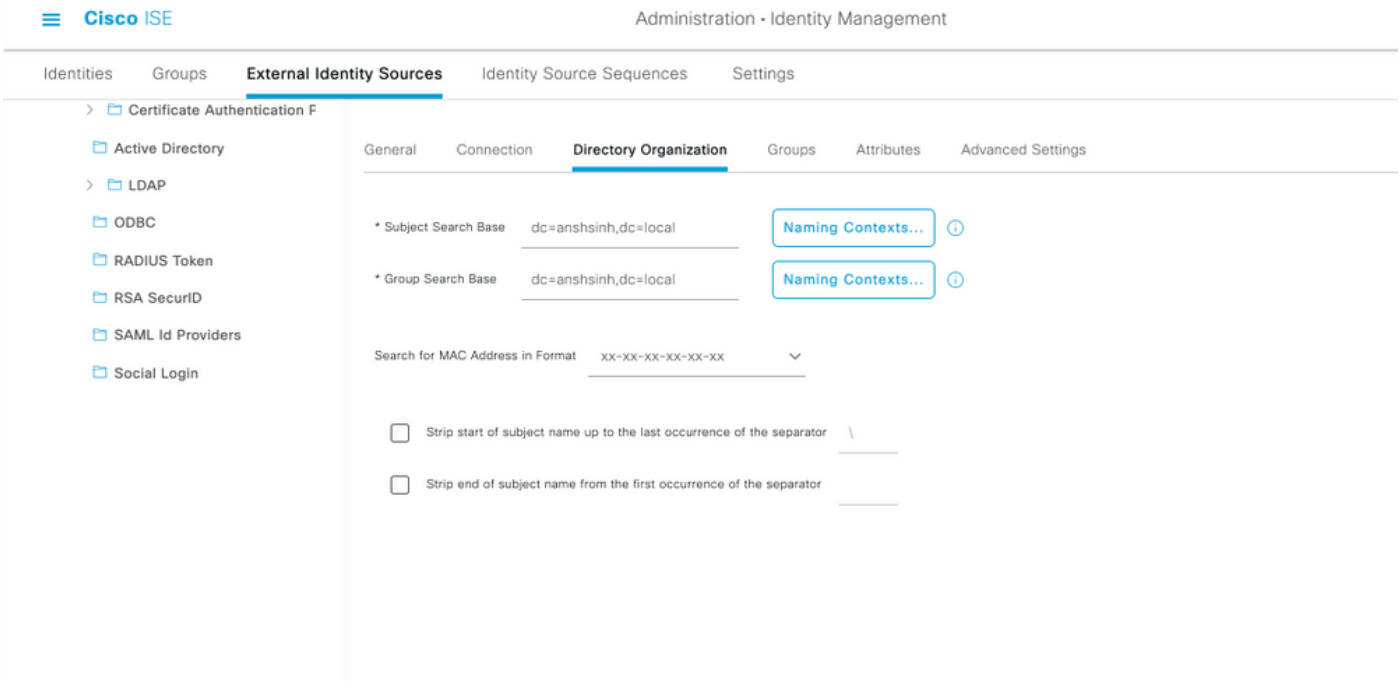
3. Introduzca la ruta del nombre distinguido del administrador (DN) con la contraseña del administrador para el servidor LDAP .

4.Haga clic en Test Bind Server para probar el alcance del servidor LDAP desde ISE .



Configuración de la organización, grupos y atributos del directorio

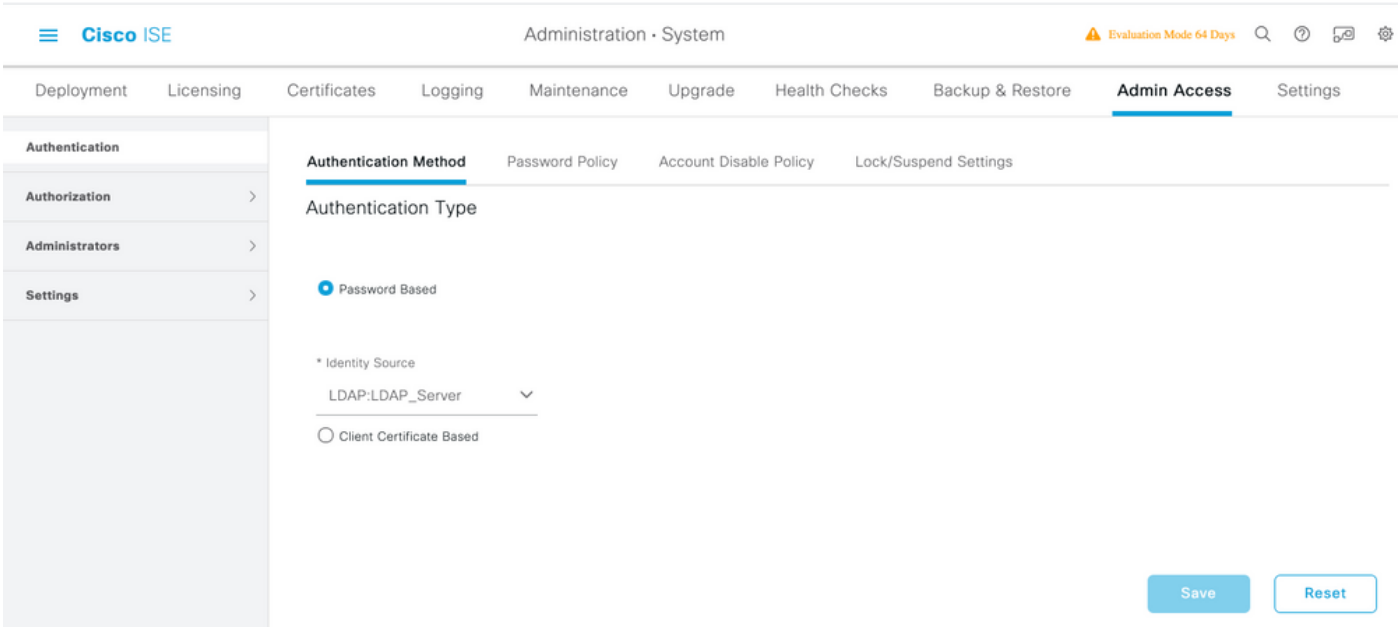
1. Elija el grupo de organización correcto del usuario basado en la jerarquía de usuarios almacenados en el servidor LDAP .



Habilitar acceso administrativo para usuarios LDAP

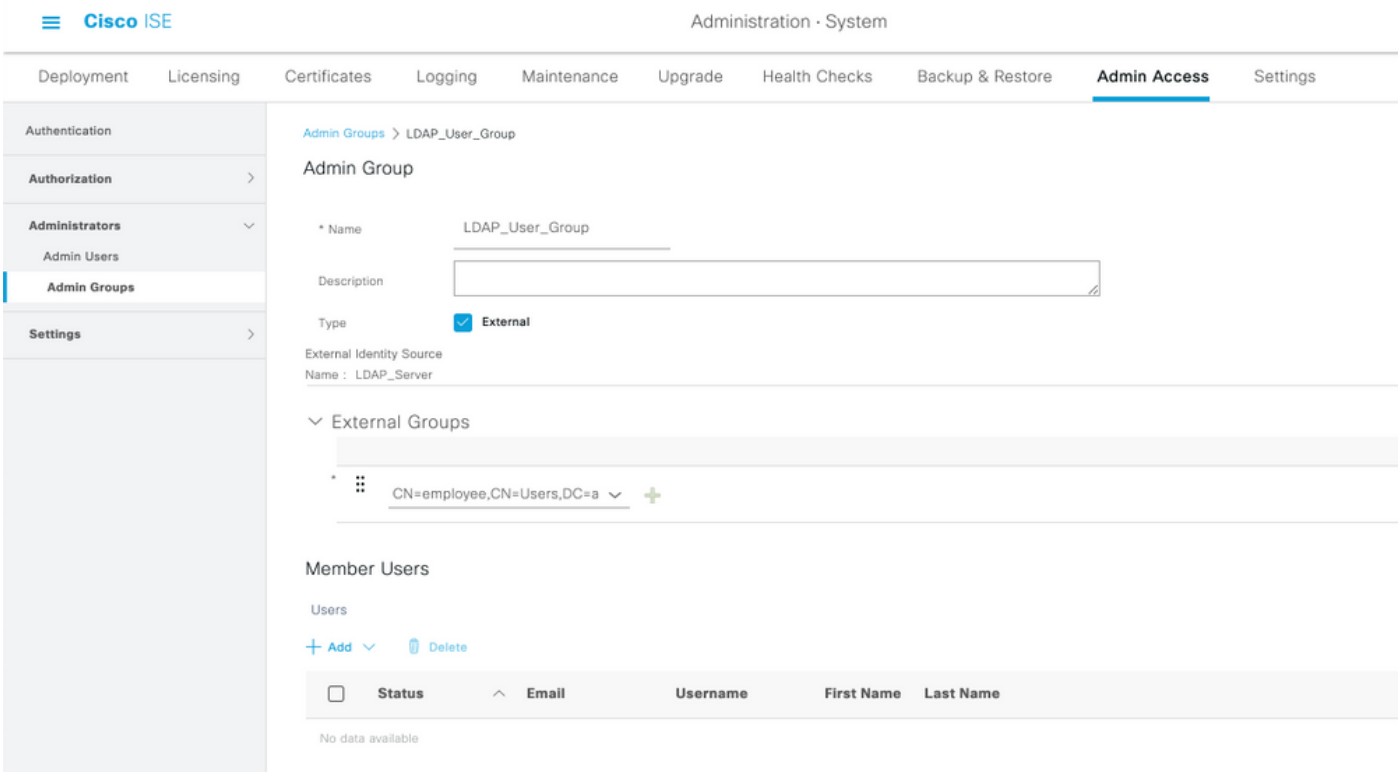
Complete estos pasos para habilitar la autenticación basada en contraseña.

1. Vaya a **ISE > Administration > System > Admin Access > Authentication**.
2. En la ficha **Authentication Method**, seleccione la **opción Password-Based**.
3. Seleccione **LDAP** en el menú desplegable **Origen de identidad**.
4. Haga clic en **Guardar cambios**.



Asigne el Grupo Admin al Grupo LDAP

Configure el grupo de administración en el ISE y asígnelo al grupo de AD. Esto permite al usuario configurado obtener acceso en función de las políticas de autorización basadas en los permisos RBAC configurados para el administrador en función de la pertenencia al grupo.

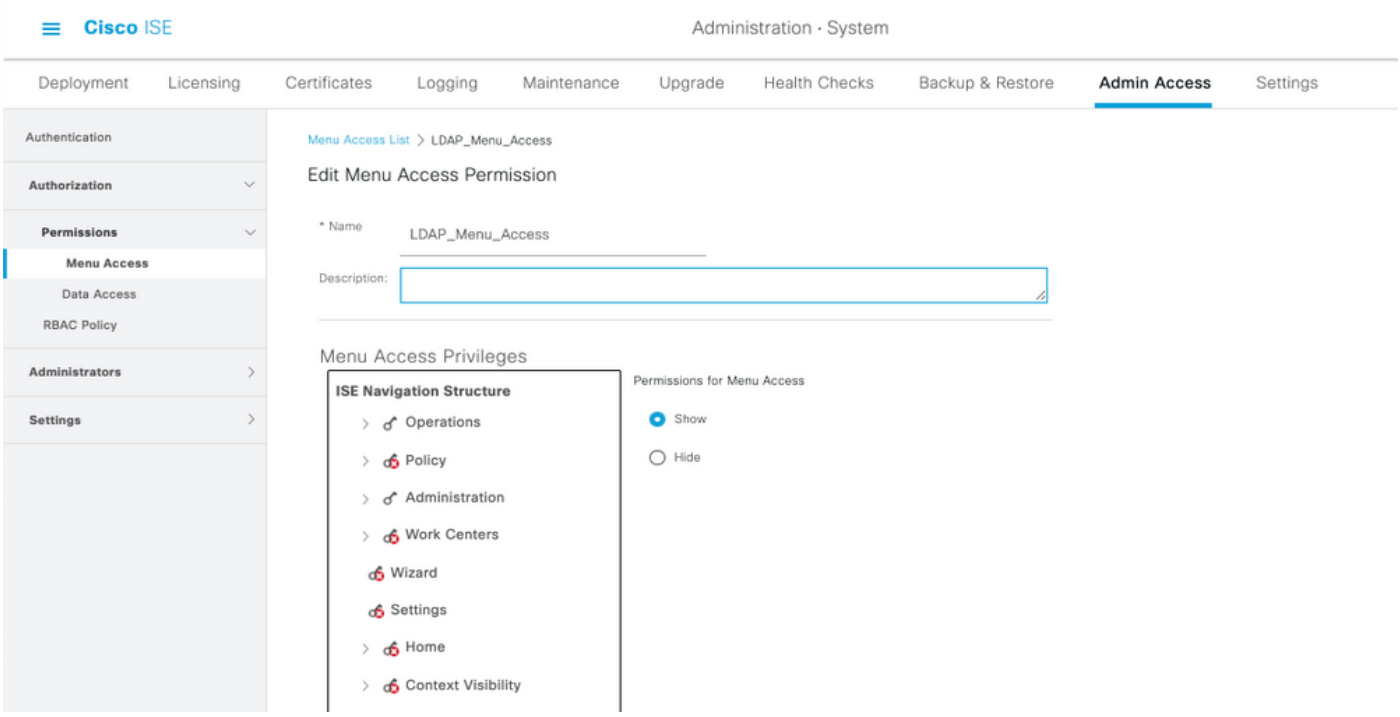


Establecer permisos para acceso a menús

1. Vaya a **ISE > Administration > System > Authorization > Permissions > Menu access**

2. Defina el acceso al menú para que el usuario administrador acceda a la GUI de ISE. Podemos configurar las subentidades que se mostrarán u ocultarán en la GUI para que un usuario pueda acceder a ellas de forma personalizada y realizar únicamente un conjunto de operaciones si es necesario.

3. Haga clic en **Guardar**.

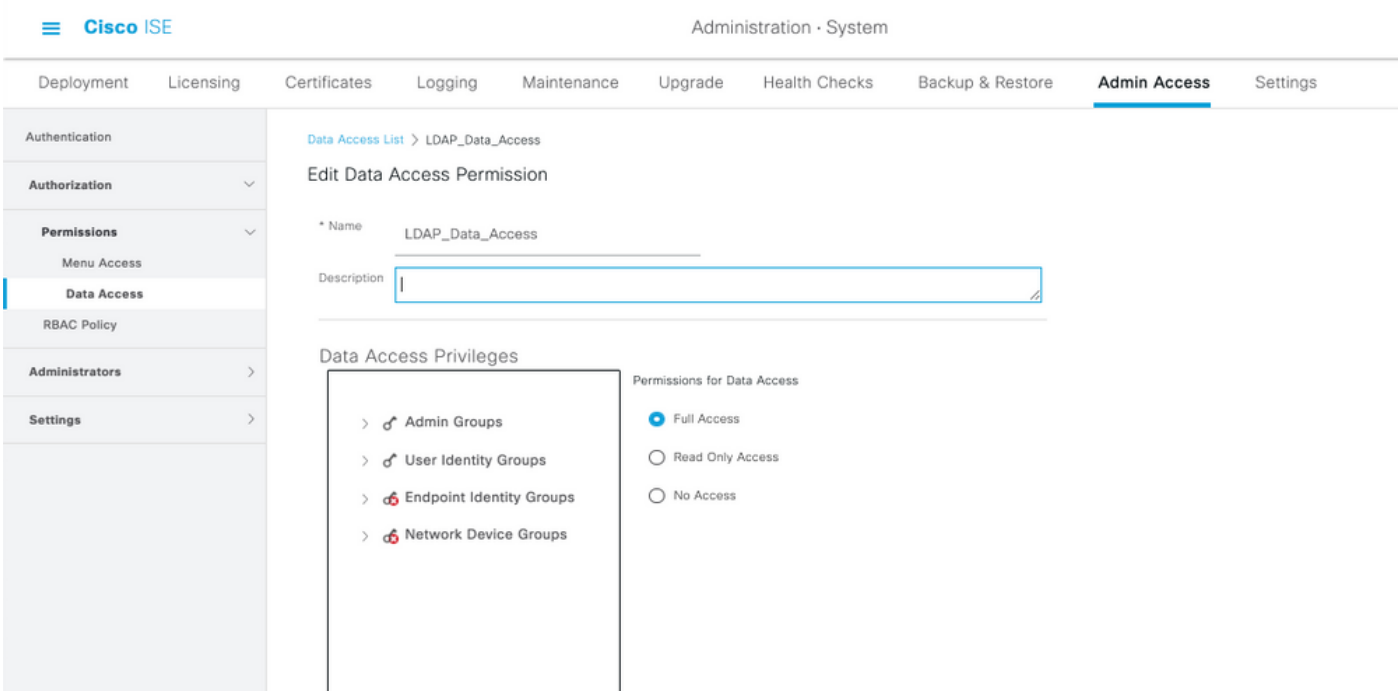


Establecer permisos para acceso a datos

1. Vaya a **ISE > Administration > System > Authorization > Permissions > Data Access**

2. Defina el acceso a los datos para que el usuario administrador tenga acceso completo o acceso de sólo lectura a los grupos de identidad en la GUI de ISE.

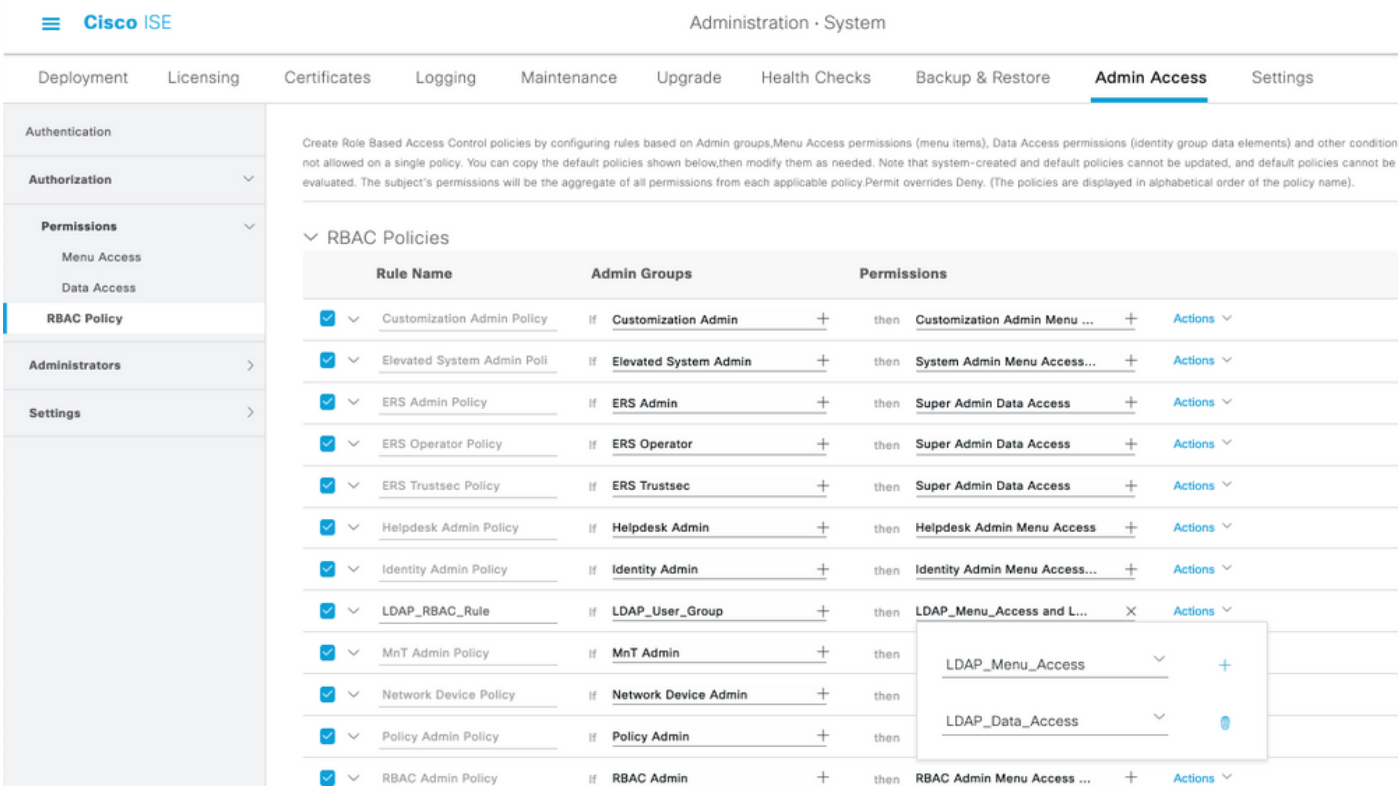
3. Haga clic en **Guardar**.



Establecer permisos RBAC para el grupo de administradores

1. Vaya a **ISE > Administration > System > Admin Access > Authorization > Policy**.

2. En el menú desplegable **Acciones** de la derecha, seleccione **Insertar nueva política abajo** para agregar una nueva política.
3. Cree una nueva regla llamada LDAP_RBAC_policy y asígnela con el Grupo de Administración definido en la sección Habilitar acceso administrativo para AD, y asígnele permisos para acceso a menús y acceso a datos.
4. Haga clic en **Guardar cambios**, y la confirmación de los cambios guardados se muestra en la esquina inferior derecha de la GUI.

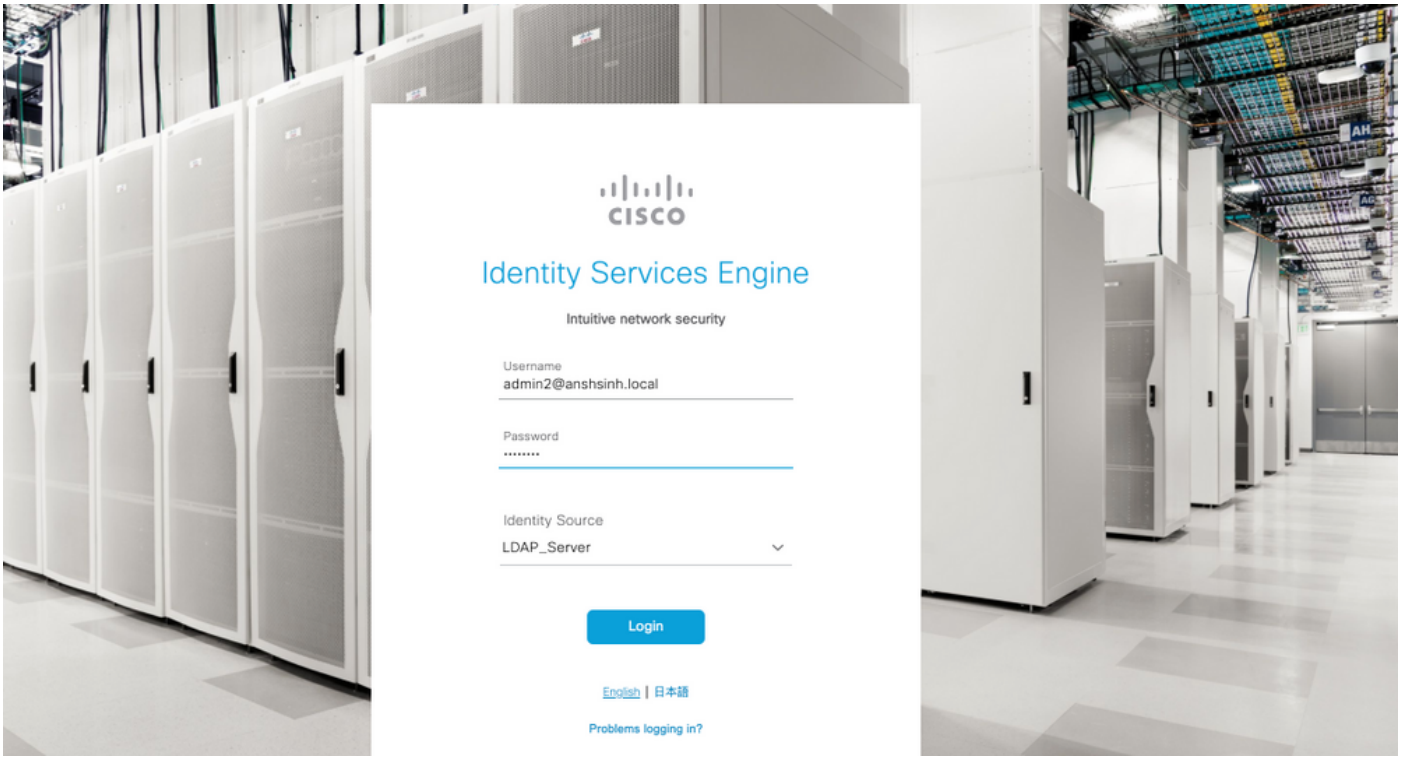


Verificación

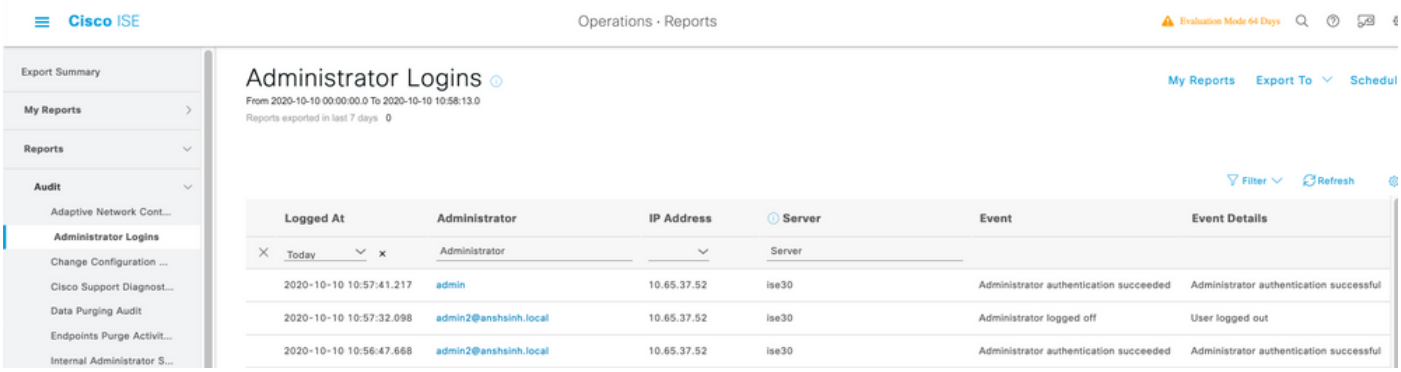
Acceso a ISE con credenciales AD

Complete estos pasos para acceder a ISE con credenciales AD:

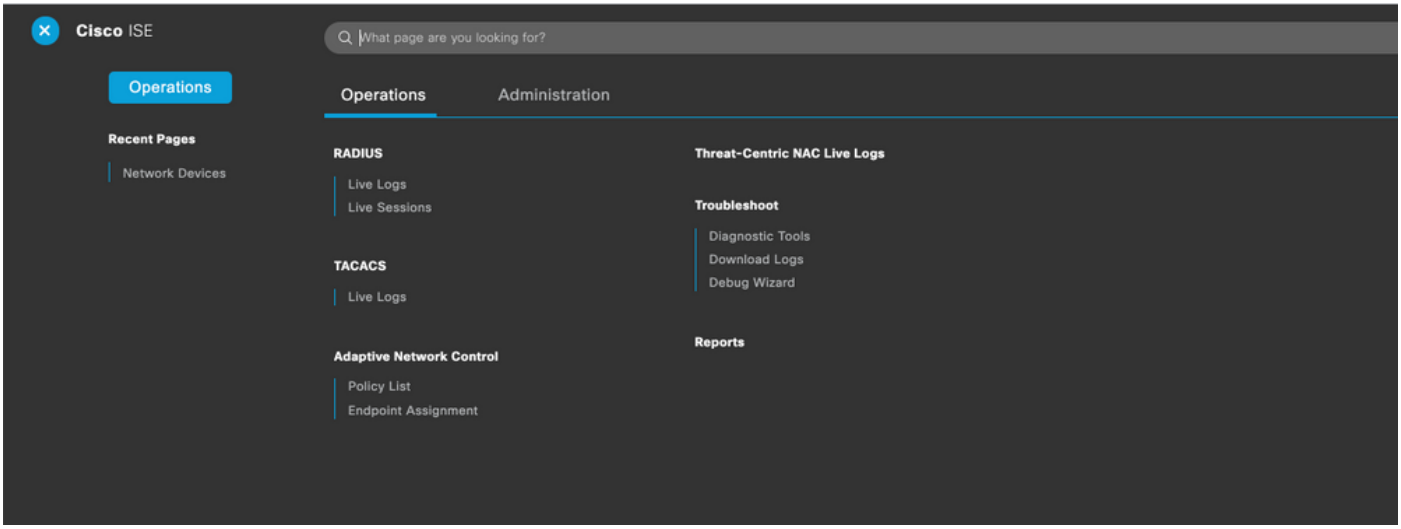
1. Abra la GUI de ISE para iniciar sesión con el usuario LDAP.
2. Seleccione LDAP_Server en el menú desplegable **Identity Source**.
3. Ingrese el nombre de usuario y la contraseña de la base de datos LDAP y conéctese.



Verifique el inicio de sesión del administrador en Informes de auditoría. Vaya a **ISE > Operaciones > Informes > Auditoría > Logins de administradores.**



Para confirmar que esta configuración funciona correctamente, verifique el nombre de usuario autenticado en la esquina superior derecha de la GUI de ISE. Defina un acceso basado en el cliente que tenga acceso limitado al menú como se muestra aquí:



Troubleshoot

Información general

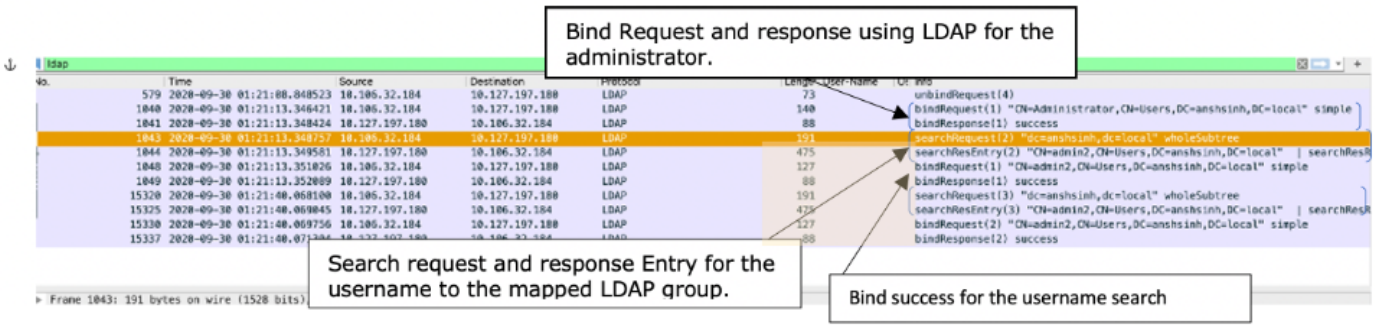
Para resolver problemas del proceso RBAC, estos componentes ISE deben estar habilitados en debug en el nodo de administrador ISE :

RBAC - Esto imprimirá el mensaje relacionado con RBAC cuando intentemos iniciar sesión (ise-psc.log)

access-filter - Esto imprimirá el acceso al filtro de recursos (ise-psc.log)

Runtime-AAA - Esto imprimirá los registros para los mensajes de interacción de login y LDAP (prrt-server.log)

Análisis de captura de paquetes



Análisis de registro

Verifique el 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
```

Verifique el ise-psc.log

Desde estos registros, puede verificar la política RBAC utilizada para el usuario admin2 cuando intente acceder al recurso de dispositivo de red -

```
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
```