Controllo degli accessi basato sui ruoli ISE con LDAP

Sommario

Introduzione

Questo documento descrive un esempio di configurazione per l'uso del protocollo LDAP (Lightweight Directory Access Protocol) come archivio identità esterno per l'accesso amministrativo all'interfaccia utente di gestione di Cisco Identity Services Engine (ISE).

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Cisco ISE versioni 3.0
- LDAP (Lightweight Directory Access Protocol)

Requisiti

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE versione 3.0
- Windows Server 2016

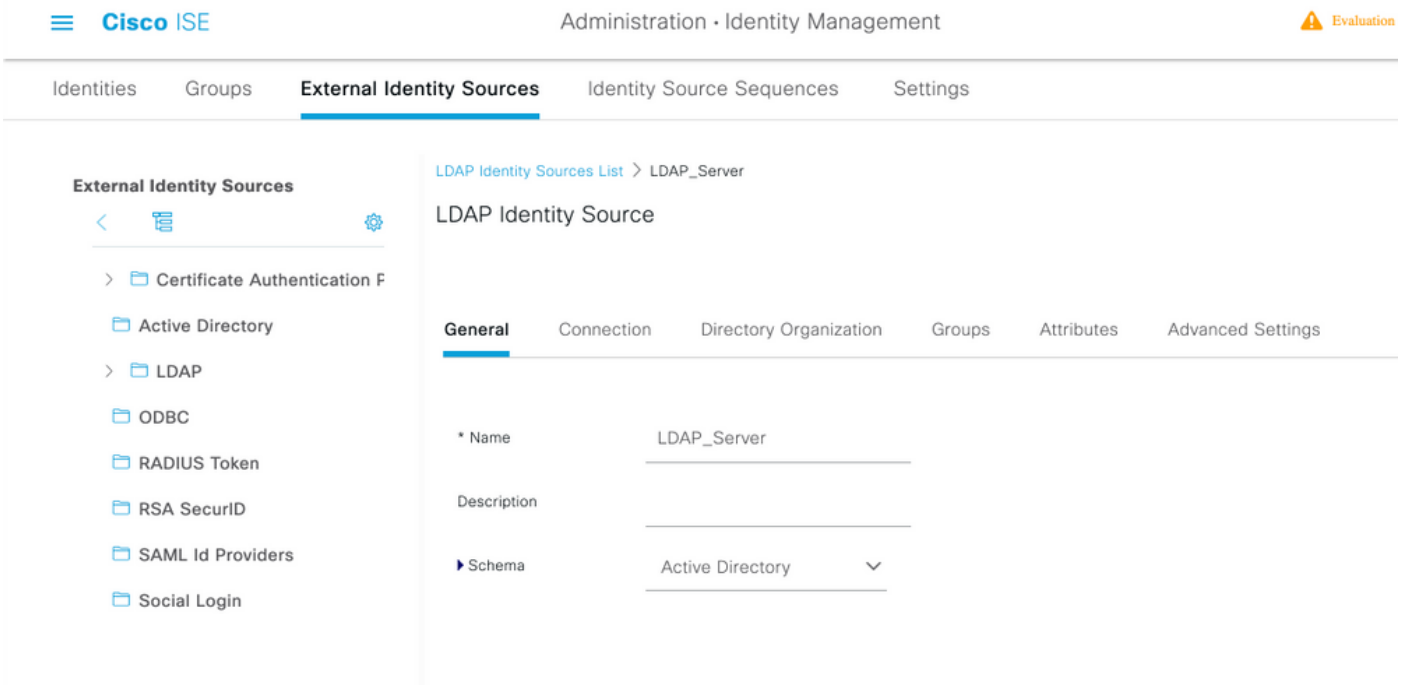
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazioni

Utilizzare la sezione seguente per configurare un utente basato su LDAP in modo da ottenere l'accesso amministrativo/personalizzato all'interfaccia grafica di ISE. La configurazione seguente utilizza le query del protocollo LDAP per recuperare l'utente da Active Directory per eseguire l'autenticazione.

Unisci ISE a LDAP

1. Passare a **Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory > LDAP.**
2. Nella scheda **Generale**, immettere il nome del server LDAP e scegliere lo schema Active Directory.



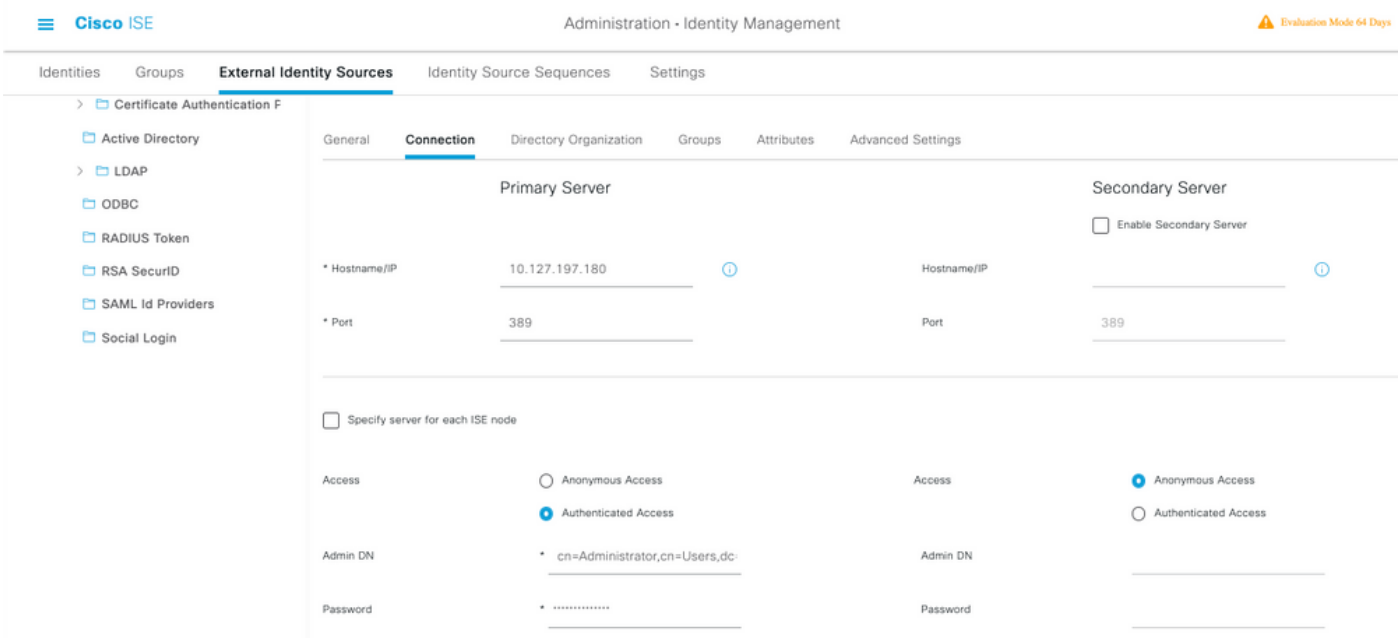
Configura tipo di connessione e configurazione LDAP

1. Passare a **ISE > Amministrazione > Gestione delle identità > Origini identità esterne > LDAP.**

2. Configurare il nome host del server LDAP primario insieme alla porta 389(LDAP)/636 (LDAP-Secure).

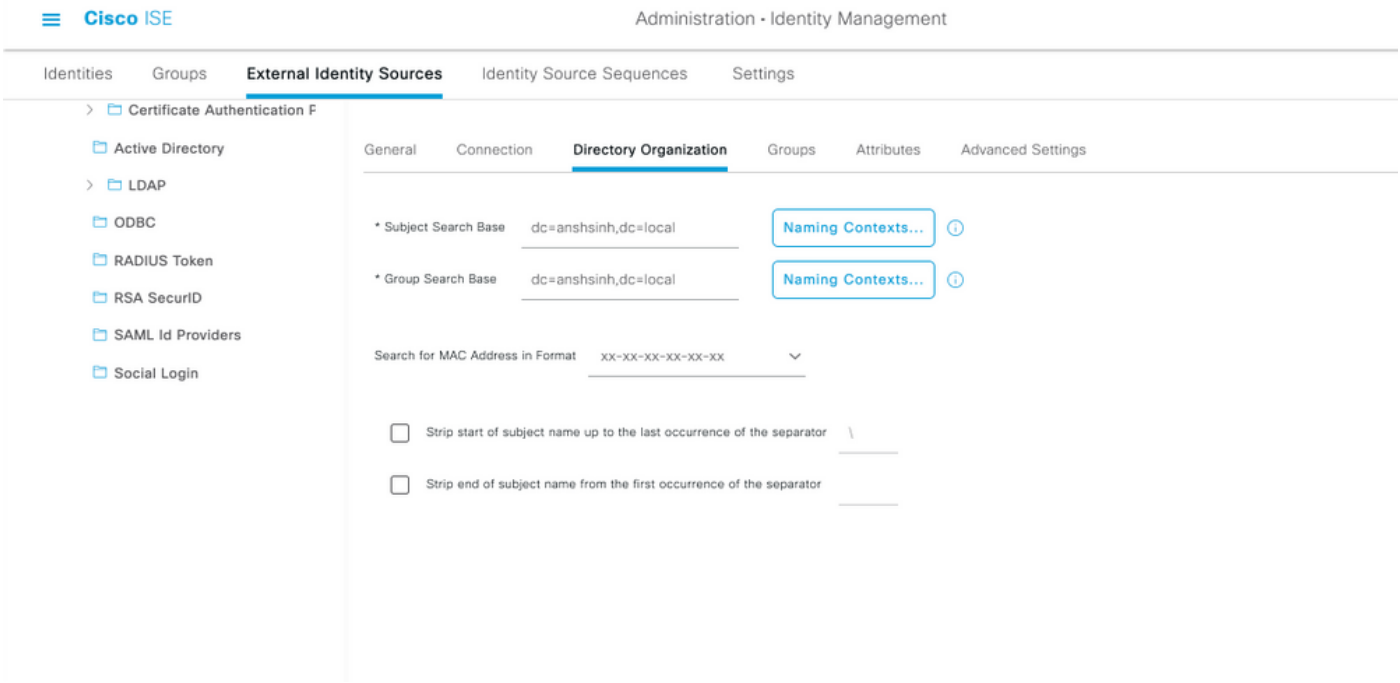
3. Immettere il percorso per il nome distinto (DN) dell'amministratore con la password dell'amministratore per il server LDAP.

4.Fare clic su Test Bind Server per verificare la raggiungibilità del server LDAP da ISE.



Configurare l'organizzazione della directory, i gruppi e gli attributi

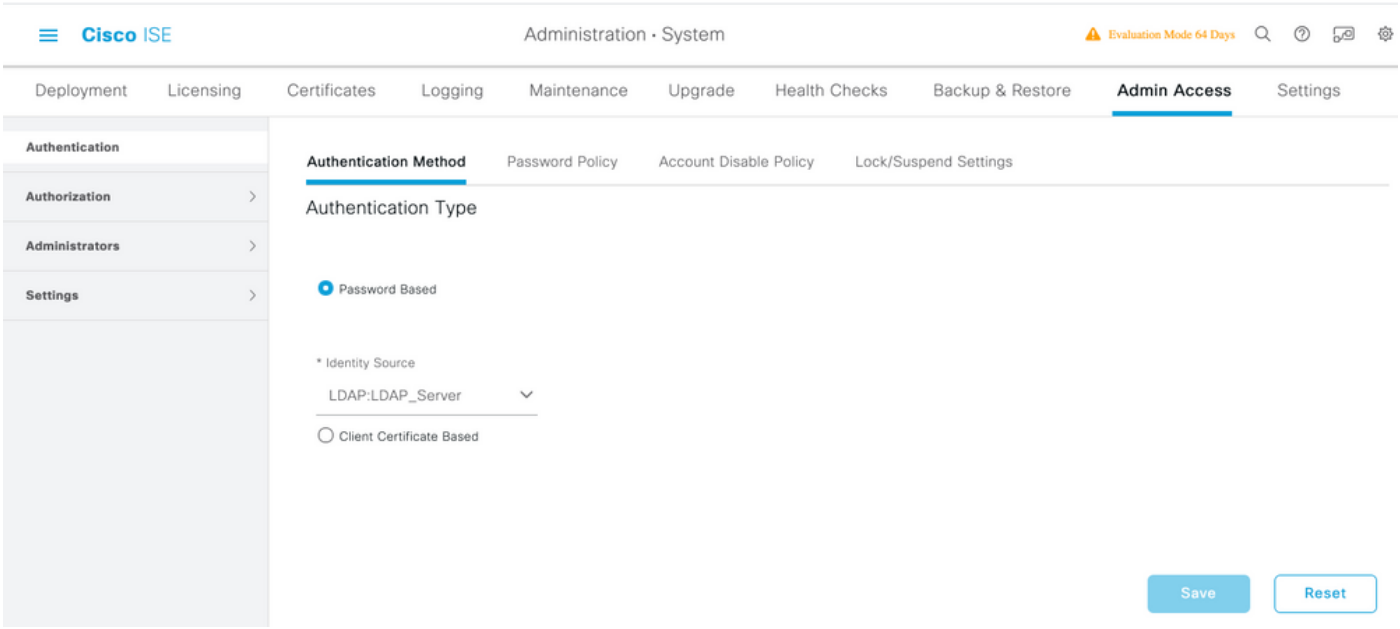
1. Scegliere il gruppo di organizzazioni corretto dell'utente in base alla gerarchia degli utenti memorizzati nel server LDAP.



Abilita accesso amministrativo per utenti LDAP

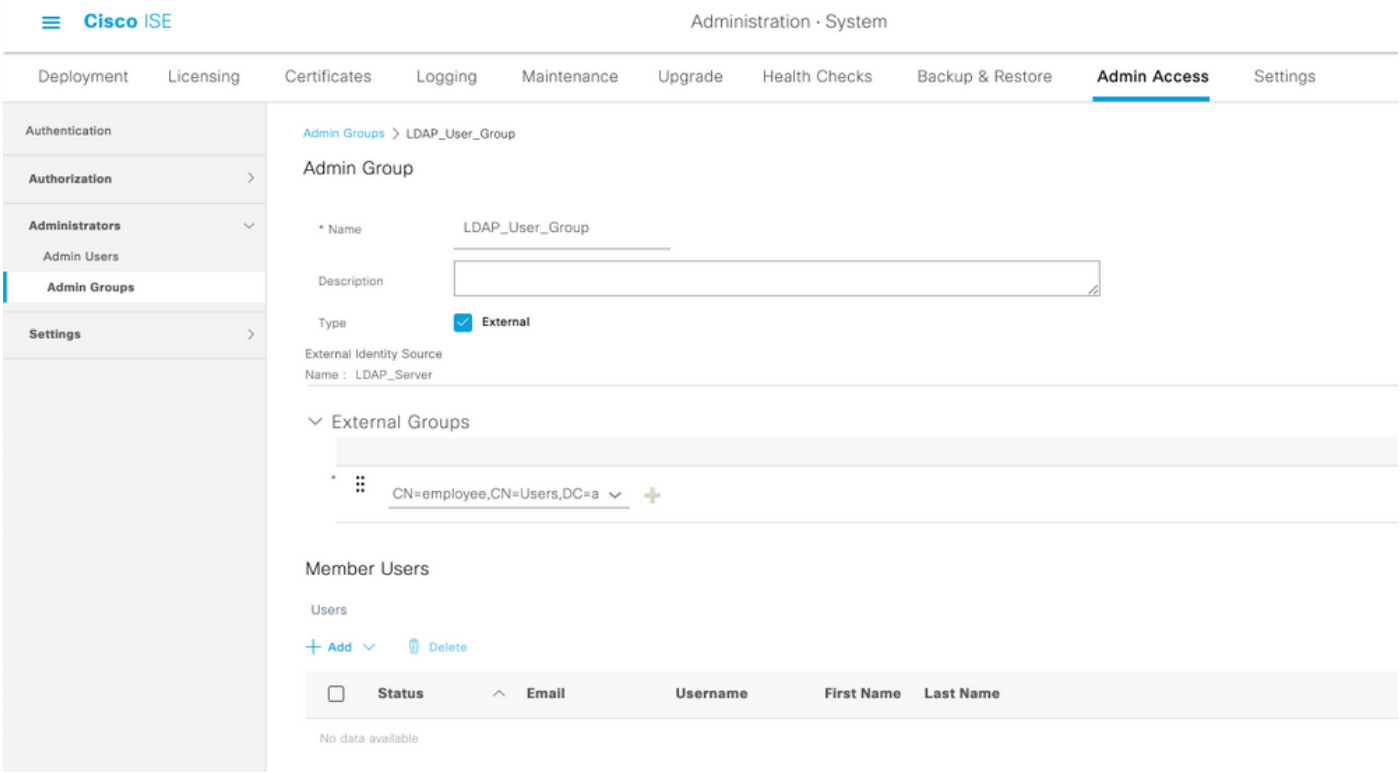
Completare questa procedura per abilitare l'autenticazione basata su password.

1. Selezionare **ISE > Amministrazione > Sistema > Accesso amministratore > Autenticazione**.
2. Nella scheda **Metodo di autenticazione** selezionare l'opzione **Basato su password**.
3. Selezionare **LDAP** dal menu a discesa **Origine identità**.
4. Fare clic su **Salva modifiche**.



Mappare il gruppo amministrativo al gruppo LDAP

Configurare il gruppo Admin sull'ISE e mapparlo al gruppo AD. Ciò consente all'utente configurato di ottenere l'accesso in base ai criteri di autorizzazione basati sulle autorizzazioni RBAC configurate per l'amministratore in base all'appartenenza ai gruppi.

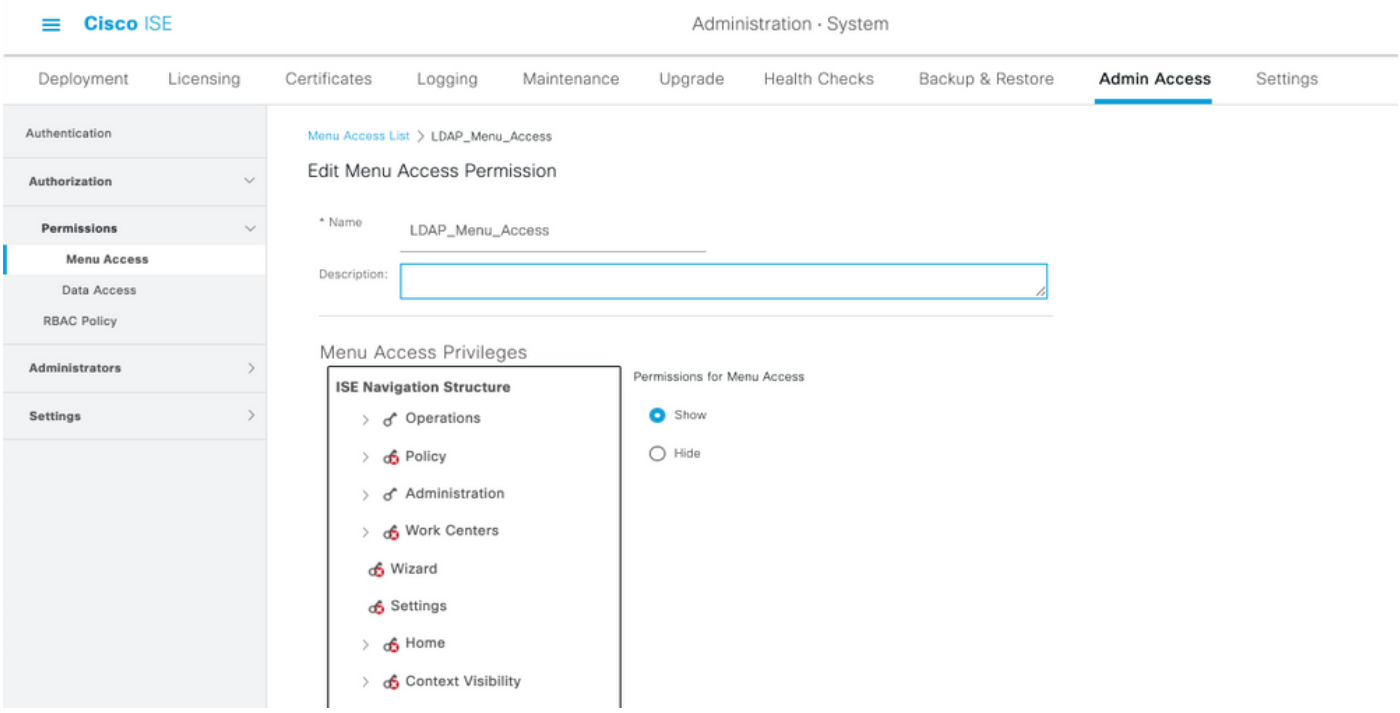


Imposta autorizzazioni per accesso menu

1. Selezionare **ISE > Amministrazione > Sistema > Autorizzazione > Autorizzazioni > Accesso al menu**

2. Definire l'accesso al menu per l'utente amministratore per accedere all'interfaccia grafica di ISE. È possibile configurare le entità secondarie da visualizzare o nascondere sulla GUI per consentire a un utente di eseguire solo un insieme di operazioni, se necessario.

3. Fare clic su **Save** (Salva).

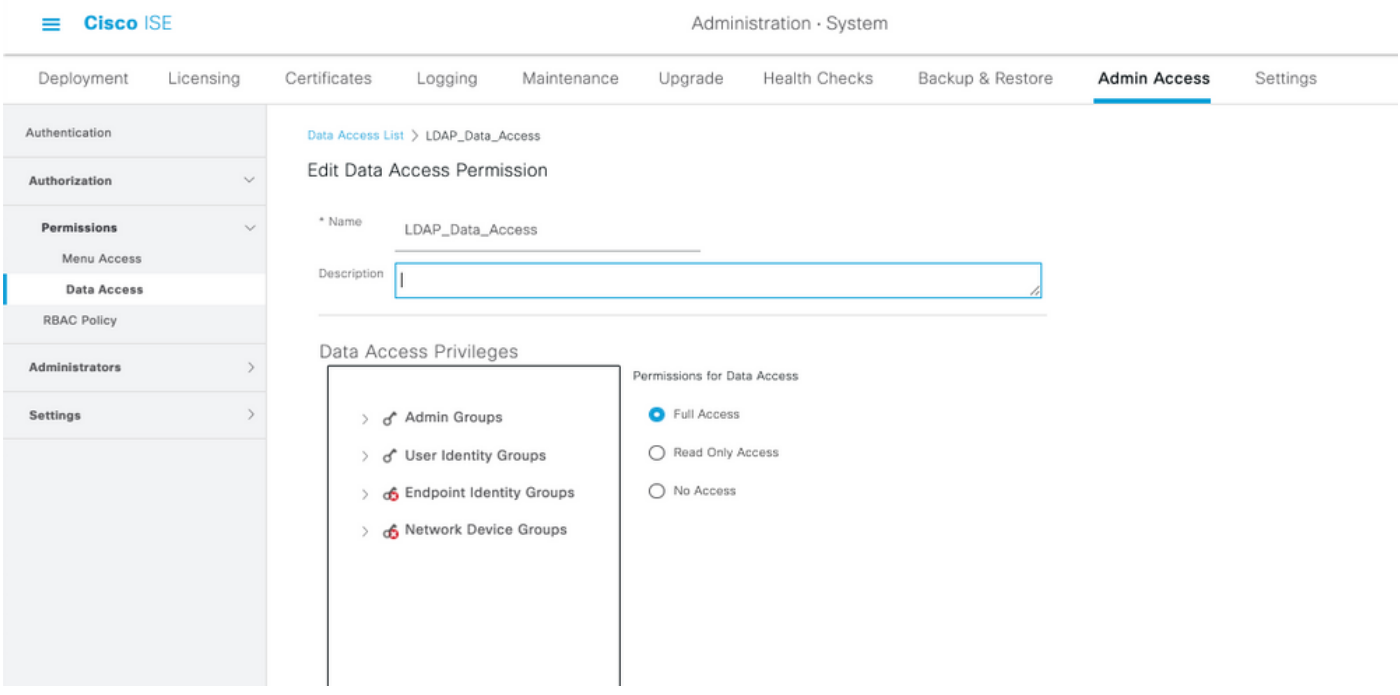


Impostare le autorizzazioni per l'accesso ai dati

1. Selezionare **ISE > Amministrazione > Sistema > Autorizzazione > Autorizzazioni > Accesso ai dati**

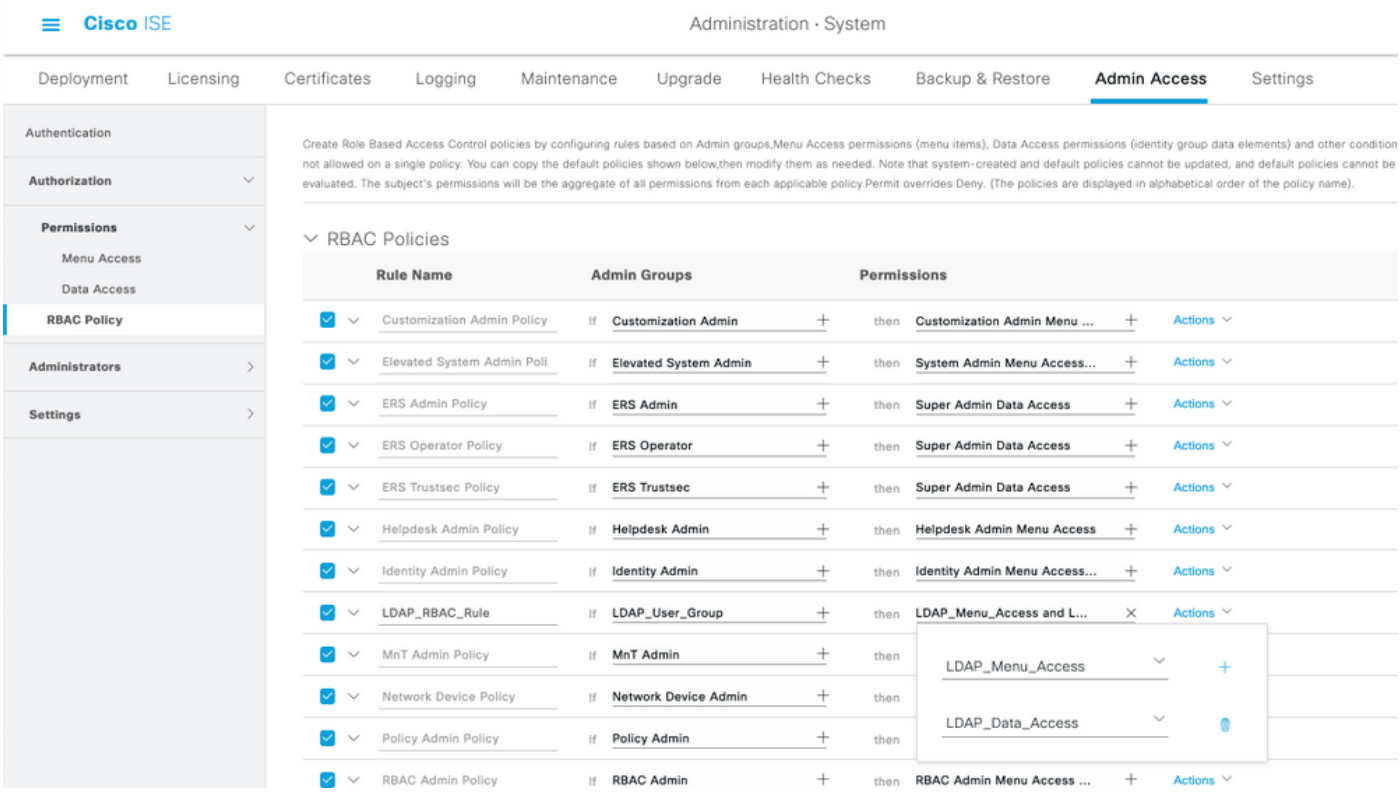
2. Definire l'accesso ai dati per l'utente amministratore in modo che abbia accesso completo o di sola lettura ai gruppi di identità sull'interfaccia grafica ISE.

3. Fare clic su **Save** (Salva).



Impostare le autorizzazioni RBAC per il gruppo Admin

1. Selezionare **ISE > Amministrazione > Sistema > Accesso amministratore > Autorizzazione > Criteri**.
2. Dal menu a discesa **Azioni** a destra, selezionare **Inserisci nuovo criterio sotto** per aggiungere un nuovo criterio.
3. Creare una nuova regola denominata LDAP_RBAC_policy e mapparla al gruppo Admin definito nella sezione Abilita accesso amministrativo per AD e assegnarle le autorizzazioni per l'accesso ai menu e ai dati.
4. Fare clic su **Save Changes** (Salva modifiche). Nell'angolo inferiore destro dell'interfaccia grafica viene visualizzata la conferma delle modifiche salvate.

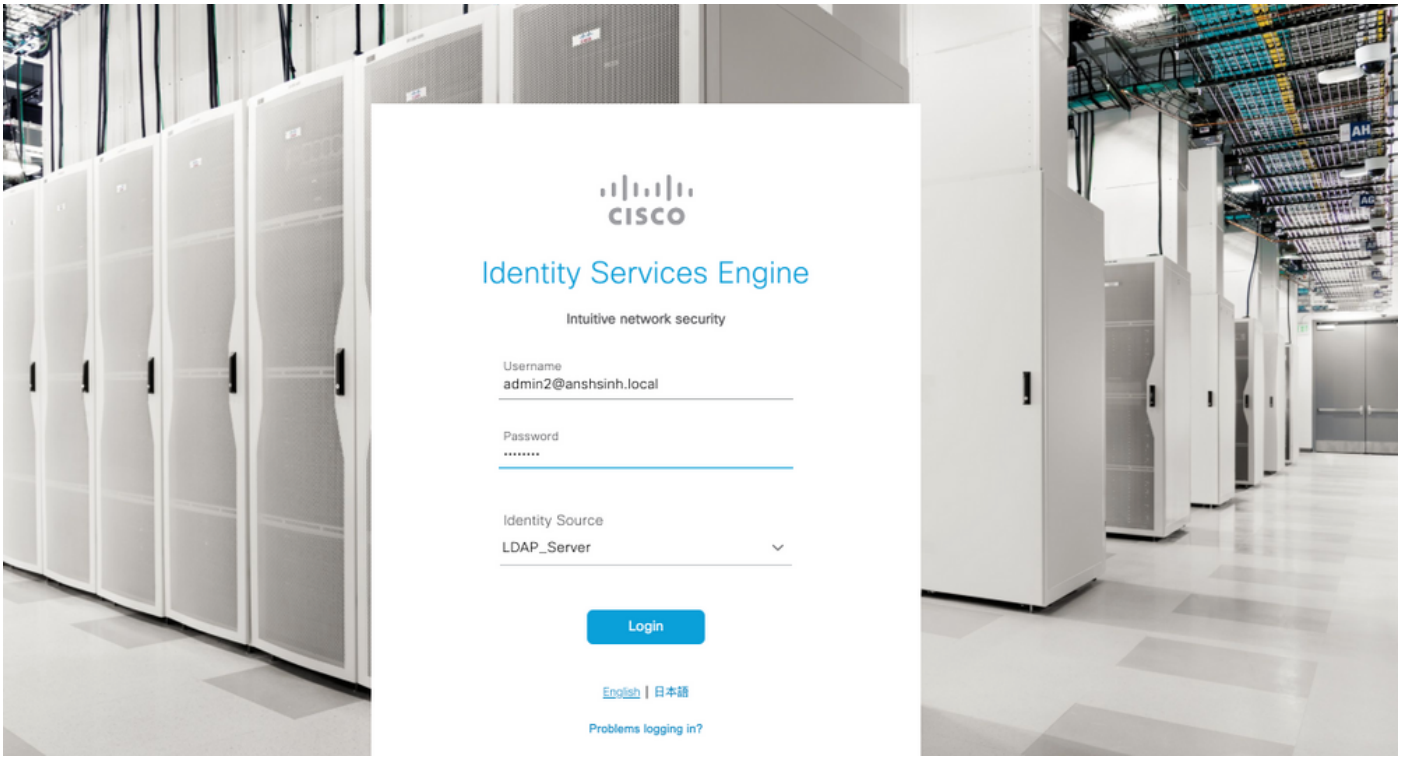


Verifica

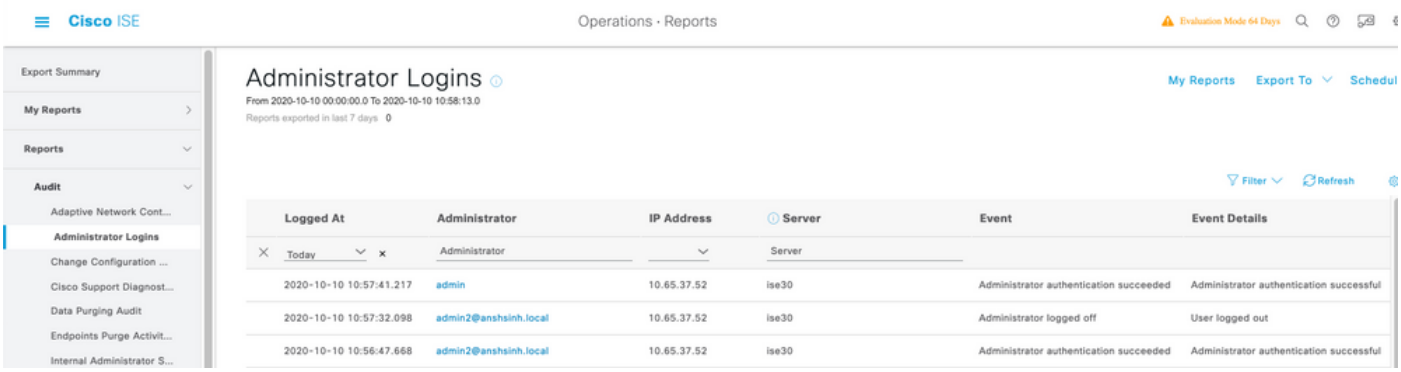
Accesso ad ISE con credenziali AD

Per accedere ad ISE con le credenziali di AD, completare la procedura seguente:

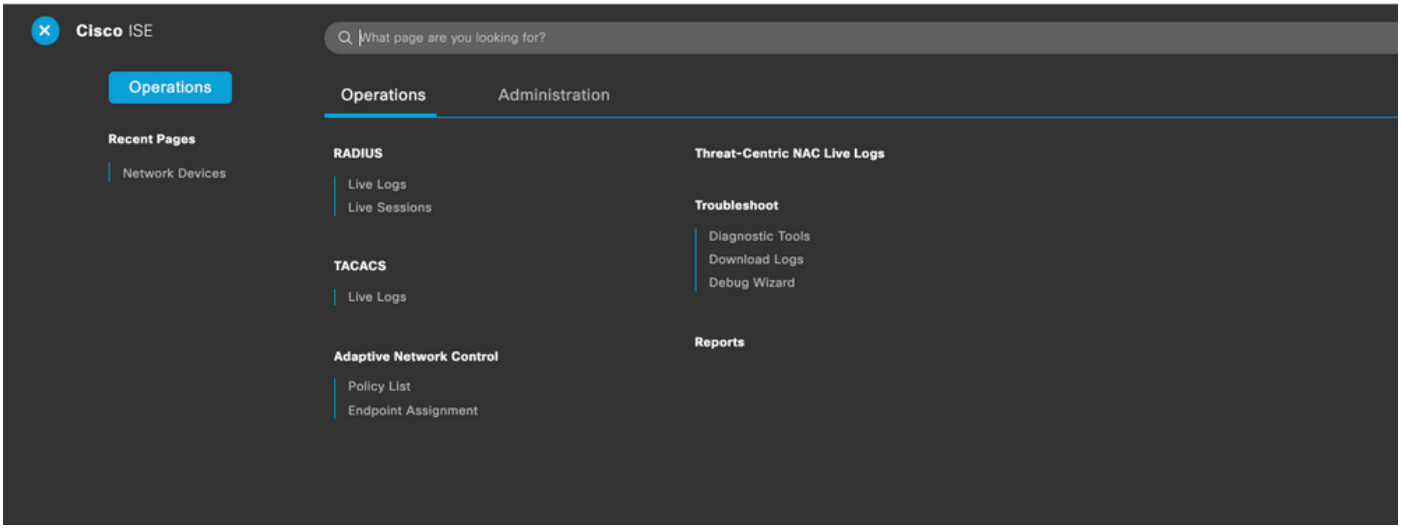
1. Aprire ISE GUI per accedere con l'utente LDAP.
2. Selezionare LDAP_Server dal menu a discesa **Origine identità**.
3. Immettere il nome utente e la password dal database LDAP ed effettuare l'accesso.



Verificare l'accesso per gli account di accesso dell'amministratore nei report di verifica. Passare a **ISE > Operazioni > Report > Audit > Login amministratori.**



Per verificare che la configurazione funzioni correttamente, verificare il nome utente autenticato nell'angolo in alto a destra dell'interfaccia utente di ISE. Definire un accesso personalizzato con accesso limitato al menu, come illustrato di seguito:



Risoluzione dei problemi

Informazioni generali

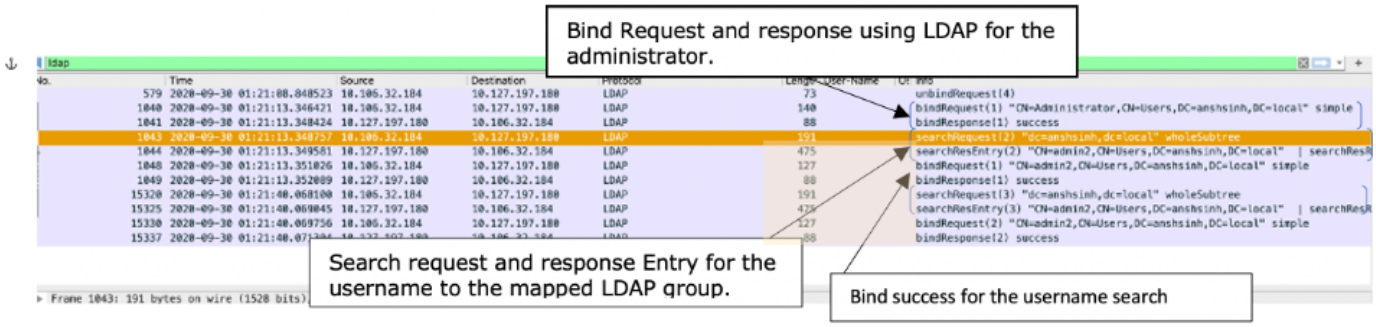
Per risolvere i problemi relativi al processo RBAC, questi componenti ISE devono essere abilitati nel debug sul nodo ISE Admin:

RBAC - Stampa il messaggio relativo a RBAC quando si prova a eseguire il login (ise-psc.log)

access-filter - Stampa l'accesso al filtro risorse (ise-psc.log)

runtime-AAA - Stampa i log per i messaggi di accesso e interazione LDAP (prt-server.log)

Analisi acquisizione pacchetti



Analisi log

Verificare il file 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
```

Verificare il file ise-psc.log

Da questi registri è possibile verificare il criterio RBAC utilizzato per l'utente admin2 quando tenta di accedere alla risorsa Dispositivo di rete -

```
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
```