

使用LDAP的ISE基於角色的訪問控制

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[組態](#)

[將ISE加入LDAP](#)

[為LDAP使用者啟用管理訪問](#)

[將管理員組對映到LDAP組](#)

[設定選單訪問的許可權](#)

[設定資料存取的許可權](#)

[設定管理員組的RBAC許可權](#)

[驗證](#)

[使用AD憑證訪問ISE](#)

[疑難排解](#)

[一般資訊](#)

[封包擷取分析](#)

[日誌分析](#)

[驗證prrt-server.log](#)

[驗證ise-psc.log](#)

簡介

本文檔介紹使用輕量級目錄訪問協定(LDAP)作為外部身份庫對思科身份服務引擎(ISE)管理GUI進行管理訪問的配置示例。

必要條件

思科建議您瞭解以下主題：

- 思科ISE版本3.0的配置
- LDAP (輕量級目錄訪問協定)

需求

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE版本3.0
- Windows Server 2016

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

組態

使用以下部分配置基於LDAP的使用者，以獲取ISE GUI的管理/自定義訪問許可權。以下配置使用LDAP協定查詢從Active directory提取使用者以執行身份驗證。

將ISE加入LDAP

1. 導航到**管理>身份管理>外部身份源> Active Directory > LDAP**。
2. 在**General**頁籤下，輸入LDAP的名稱，然後選擇架構Active Directory。

The screenshot shows the Cisco ISE Administration interface for Identity Management. The breadcrumb trail is Administration > Identity Management > External Identity Sources > LDAP Identity Sources List > LDAP_Server. The left sidebar shows a tree view of External Identity Sources, with LDAP selected. The main content area displays the configuration for the LDAP Identity Source 'LDAP_Server' under the 'General' tab. The configuration includes: Name: LDAP_Server, Description: (empty), and Schema: Active Directory (selected from a dropdown menu). Other tabs like Connection, Directory Organization, Groups, Attributes, and Advanced Settings are visible but not active. A warning icon and 'Evaluation' text are in the top right corner.

配置連線型別和LDAP配置

1. 導航到**ISE >管理>身份管理>外部身份源> LDAP**。
2. 配置主LDAP伺服器的主機名以及埠389(LDAP)/636(LDAP-Secure)。
3. 輸入管理員唯一判別名(DN)的路徑，並輸入LDAP伺服器的管理員密碼。
4. 點選Test Bind Server以測試從ISE訪問LDAP伺服器的能力。

Identities Groups **External Identity Sources** Identity Source Sequences Settings

> Certificate Authentication F

- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

General **Connection** Directory Organization Groups Attributes Advanced Settings

| Primary Server | | Secondary Server | |
|----------------|----------------|------------------|-----|
| * Hostname/IP | 10.127.197.180 | Hostname/IP | |
| * Port | 389 | Port | 389 |

Enable Secondary Server

Specify server for each ISE node

Access Anonymous Access Authenticated Access

Admin DN * cn=Administrator,cn=Users,dc=

Password *

配置目錄組織、組和屬性

1. 根據LDAP伺服器中儲存的使用者的層次結構選擇正確的使用者組織組。

Identities Groups **External Identity Sources** Identity Source Sequences Settings

> Certificate Authentication F

- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

General Connection **Directory Organization** Groups Attributes Advanced Settings

* Subject Search Base dc=anshsinh,dc=local [Naming Contexts...](#)

* Group Search Base dc=anshsinh,dc=local [Naming Contexts...](#)

Search for MAC Address in Format xx-xx-xx-xx-xx-xx

Strip start of subject name up to the last occurrence of the separator \

Strip end of subject name from the first occurrence of the separator

為LDAP使用者啟用管理訪問

完成以下步驟即可啟用密碼型驗證。

1. 導航到ISE > Administration > System > Admin Access > Authentication。
2. 在Authentication Method頁籤下，選擇Password-Based選項。
3. 從Identity Source下拉選單中選擇LDAP。
4. 按一下Save Changes。

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE', 'Administration - System', and a warning for 'Evaluation Mode 64 Days'. The main navigation menu has tabs for Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, **Admin Access**, and Settings. The left sidebar contains 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The main content area is titled 'Authentication Method' and includes sub-links for 'Password Policy', 'Account Disable Policy', and 'Lock/Suspend Settings'. Under 'Authentication Type', 'Password Based' is selected. The 'Identity Source' is set to 'LDAP:LDAP_Server'. There are 'Save' and 'Reset' buttons at the bottom right.

將管理員組對映到LDAP組

在ISE上配置管理組並將其對映到AD組。這允許配置的使用者根據基於組成員資格的管理員配置的RBAC許可權的授權策略獲得訪問許可權。

The screenshot shows the Cisco ISE Administration console, specifically the 'Admin Groups' configuration page. The navigation and sidebar are the same as in the previous screenshot. The main content area is titled 'Admin Groups > LDAP_User_Group' and 'Admin Group'. The 'Name' field is 'LDAP_User_Group'. The 'Type' is 'External'. The 'External Identity Source Name' is 'LDAP_Server'. Under 'External Groups', a group 'CN=employee,CN=Users,DC=a' is listed. The 'Member Users' section is empty, showing a table with columns for Status, Email, Username, First Name, and Last Name, and a note 'No data available'.

設定選單訪問的許可權

1. 導航到ISE > 管理 > 系統 > 授權 > 許可權 > 選單訪問

2. 定義管理員使用者訪問ISE GUI的選單訪問。我們可以配置要在GUI上顯示或隱藏的子實體，以便使用者進行自定義訪問，從而僅在需要時執行一組操作。

3. 按一下Save。

The screenshot shows the Cisco ISE Admin Access configuration page for editing a Menu Access Permission. The breadcrumb is "Menu Access List > LDAP_Menu_Access". The page title is "Edit Menu Access Permission". The "Name" field is "LDAP_Menu_Access" and the "Description" field is empty. Below, the "Menu Access Privileges" section shows the "ISE Navigation Structure" with a tree view containing: Operations, Policy, Administration, Work Centers, Wizard, Settings, Home, and Context Visibility. To the right, "Permissions for Menu Access" has radio buttons for "Show" (selected) and "Hide".

設定資料存取的許可權

1. 導航到 ISE > Administration > System > Authorization > Permissions > Data access

2. 為管理員使用者定義資料存取許可權，使其對 ISE GUI 上的身份組具有完全訪問許可權或只讀訪問許可權。

3. 按一下 Save。

The screenshot shows the Cisco ISE Admin Access configuration page for editing a Data Access Permission. The breadcrumb is "Data Access List > LDAP_Data_Access". The page title is "Edit Data Access Permission". The "Name" field is "LDAP_Data_Access" and the "Description" field is empty. Below, the "Data Access Privileges" section shows a list of groups: Admin Groups, User Identity Groups, Endpoint Identity Groups, and Network Device Groups. To the right, "Permissions for Data Access" has radio buttons for "Full Access" (selected), "Read Only Access", and "No Access".

設定管理員組的RBAC許可權

1. 導航到 ISE > Administration > System > Admin Access > Authorization > Policy。
2. 從右側的 Actions 下拉選單中，選擇 Insert New Policy Below 以新增新策略。

3. 建立一個名為LDAP_RBAC_policy的新規則，並將其與「為AD啟用管理訪問」部分中定義的管理組進行對映，然後為其分配選單訪問和資料存取的許可權。
4. 按一下**Save Changes**,GUI的右下角將顯示對已儲存更改的確認。

Cisco ISE Administration · System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Authentication

Authorization

Permissions

Menu Access

Data Access

RBAC Policy

Administrators

Settings

Create Role Based Access Control policies by configuring rules based on Admin groups, Menu Access permissions (menu items), Data Access permissions (identity group data elements) and other condition not allowed on a single policy. You can copy the default policies shown below, then modify them as needed. Note that system-created and default policies cannot be updated, and default policies cannot be evaluated. The subject's permissions will be the aggregate of all permissions from each applicable policy. Permit overrides Deny. (The policies are displayed in alphabetical order of the policy name).

RBAC Policies

| Rule Name | Admin Groups | Permissions |
|--|--------------------------|--|
| <input checked="" type="checkbox"/> Customization Admin Policy | If Customization Admin | + then Customization Admin Menu ... + Actions |
| <input checked="" type="checkbox"/> Elevated System Admin Poli | If Elevated System Admin | + then System Admin Menu Access... + Actions |
| <input checked="" type="checkbox"/> ERS Admin Policy | If ERS Admin | + then Super Admin Data Access + Actions |
| <input checked="" type="checkbox"/> ERS Operator Policy | If ERS Operator | + then Super Admin Data Access + Actions |
| <input checked="" type="checkbox"/> ERS Trustsec Policy | If ERS Trustsec | + then Super Admin Data Access + Actions |
| <input checked="" type="checkbox"/> Helpdesk Admin Policy | If Helpdesk Admin | + then Helpdesk Admin Menu Access + Actions |
| <input checked="" type="checkbox"/> Identity Admin Policy | If Identity Admin | + then Identity Admin Menu Access... + Actions |
| <input checked="" type="checkbox"/> LDAP_RBAC_Rule | If LDAP_User_Group | + then LDAP_Menu_Access and L... X Actions |
| <input checked="" type="checkbox"/> MnT Admin Policy | If MnT Admin | + then LDAP_Menu_Access + |
| <input checked="" type="checkbox"/> Network Device Policy | If Network Device Admin | + then LDAP_Data_Access |
| <input checked="" type="checkbox"/> Policy Admin Policy | If Policy Admin | + then RBAC Admin Menu Access ... + Actions |
| <input checked="" type="checkbox"/> RBAC Admin Policy | If RBAC Admin | + then RBAC Admin Menu Access ... + Actions |

驗證

使用AD憑證訪問ISE

完成以下步驟，以便使用AD憑證訪問ISE:

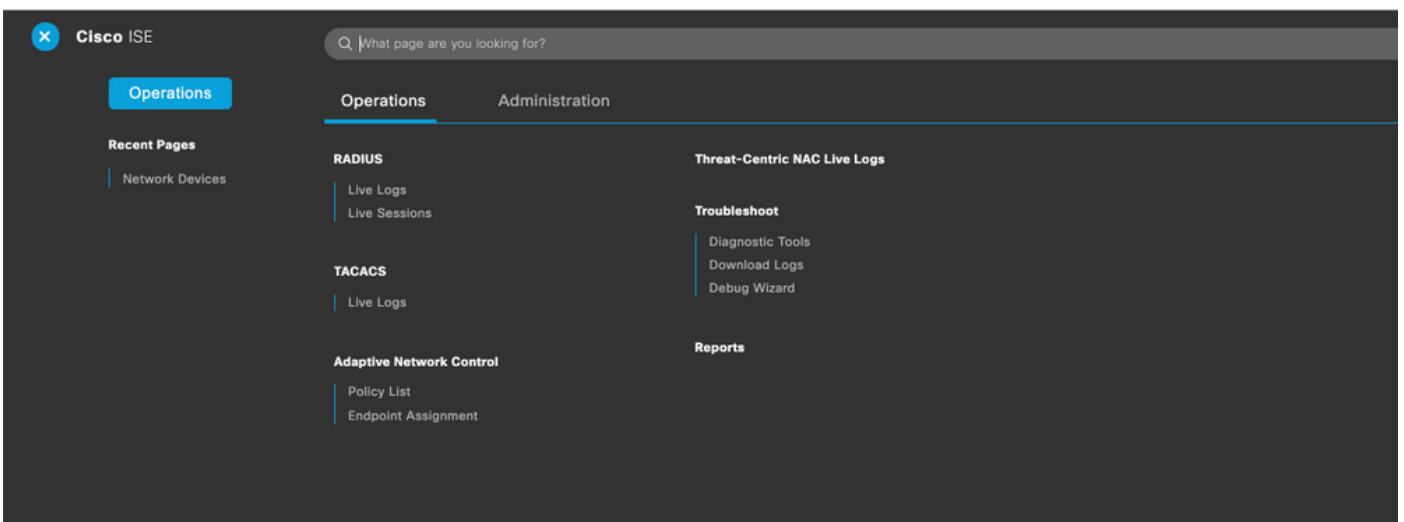
1. 開啟ISE GUI以使用LDAP使用者登入。
2. 從Identity Source下拉選單中選擇LDAP_Server。
3. 從LDAP資料庫輸入使用者名稱和密碼，然後登入。



在「審計報告」中驗證管理員登入的登入。導航到ISE > Operations > Reports > Audit > Administrators Logins。

| Logged At | Administrator | IP Address | Server | Event | Event Details |
|-------------------------|-----------------------|-------------|--------|--|---|
| 2020-10-10 10:57:41.217 | admin | 10.65.37.52 | ise30 | Administrator authentication succeeded | Administrator authentication successful |
| 2020-10-10 10:57:32.098 | admin2@anshsinh.local | 10.65.37.52 | ise30 | Administrator logged off | User logged out |
| 2020-10-10 10:56:47.668 | admin2@anshsinh.local | 10.65.37.52 | ise30 | Administrator authentication succeeded | Administrator authentication successful |

為了確認此配置正常工作，請驗證ISE GUI右上角的身份驗證使用者名稱。定義對選單具有有限訪問許可權的基於自定義的訪問，如下所示：



疑難排解

一般資訊

為了對RBAC流程進行故障排除，必須在ISE管理節點的調試中啟用這些ISE元件：

RBAC — 這將在嘗試登入時列印RBAC相關消息(ise-psc.log)

access-filter — 這將列印資源過濾器訪問許可權(ise-psc.log)

runtime-AAA — 這將列印登入和LDAP互動消息的日誌(prrt-server.log)

封包擷取分析

The image shows a Wireshark network traffic capture of LDAP operations. The packet list pane on the left shows several LDAP packets. Three callout boxes highlight specific packets:

- Bind Request and response using LDAP for the administrator.** This box points to packets 140 and 141, which are bindRequest(1) and bindResponse(1) respectively.
- Search request and response Entry for the username to the mapped LDAP group.** This box points to packets 127 and 128, which are searchRequest(1) and searchResEntry(1) respectively.
- Bind success for the username search** This box points to packet 129, which is bindResponse(2) success.

The packet details pane on the right shows the structure of these LDAP messages, including fields like 'simple', 'wholeSubtree', and 'success'.

日誌分析

驗證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
```

驗證ise-psc.log

從這些日誌中，您可以驗證在嘗試訪問網路裝置資源 —

```
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
```