

# Konfigurieren der rollenbasierten ISE-Zugriffskontrolle mit Lightweight Directory Access Protocol

## Inhalt

---

### [Einleitung](#)

### [Voraussetzungen](#)

#### [Anforderungen](#)

### [Konfigurationen](#)

#### [Beitritt der ISE zum LDAP](#)

#### [Administrator-Zugriff für LDAP-Benutzer aktivieren](#)

#### [Zuordnen der Admin-Gruppe zur LDAP-Gruppe](#)

##### [Festlegen von Berechtigungen für den Menüzugriff](#)

##### [Festlegen von Berechtigungen für den Datenzugriff](#)

##### [RBAC-Berechtigungen für die Admin-Gruppe festlegen](#)

### [Überprüfung](#)

#### [Zugriff auf die ISE mit AD-Anmeldeinformationen](#)

### [Fehlerbehebung](#)

#### [Allgemeine Informationen](#)

#### [Paketerfassungsanalyse](#)

#### [Protokollanalyse](#)

##### [Überprüfen Sie den Wert für "rt-server.log".](#)

##### [Verifizieren Sie theise-psc.log](#)

---

## Einleitung

In diesem Dokument wird ein Konfigurationsbeispiel für die Verwendung des Lightweight Directory Access Protocol (LDAP) als externer Identitätsspeicher für den Administratorzugriff auf die Management-GUI der Cisco Identity Services Engine (ISE) beschrieben.

## Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration der Cisco ISE Version 3.0
- LDAP

## Anforderungen

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE Version 3.0
- Windows Server 2016

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Konfigurationen

In diesem Abschnitt können Sie einen LDAP-basierten Benutzer konfigurieren, um administrativen/benutzerdefinierten Zugriff auf die ISE-GUI zu erhalten. In der folgenden Konfiguration werden LDAP-Protokollabfragen verwendet, um den Benutzer aus dem Active Directory für die Authentifizierung abzurufen.

### Beitritt der ISE zum LDAP

1. Navigieren Sie zu Administration > Identity Management > External Identity Sources > Active Directory > LDAP.
2. Geben Sie auf der Registerkarte Allgemein den Namen des LDAP ein, und wählen Sie das Schema Active Directory aus.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation is Administration > Identity Management > External Identity Sources > LDAP. The left sidebar shows a tree view of External Identity Sources, with LDAP selected. The main content area displays the configuration for an LDAP Identity Source named 'LDAP\_Server'. The 'General' tab is active, showing fields for Name (LDAP\_Server), Description, and Schema (Active Directory).

### Verbindungstyp und LDAP-Konfiguration konfigurieren

1. Navigieren Sie zu ISE > Administration > Identity Management > External Identity Sources > LDAP.
2. Konfigurieren Sie den Hostnamen des primären LDAP-Servers zusammen mit dem Port 389(LDAP)/636 (LDAP-Secure) .

3. Geben Sie den Pfad für den Distinguished Name (DN) des Administrators mit dem Administratorkennwort für den LDAP-Server ein.

4. Klicken Sie auf Test Bind Server, um die Erreichbarkeit des LDAP-Servers von der ISE zu testen.

The screenshot shows the Cisco ISE Administration interface for Identity Management. The 'External Identity Sources' tab is active, and the 'LDAP' source is selected. The 'Connection' sub-tab is chosen, displaying configuration for a Primary Server and a Secondary Server. The Primary Server is configured with Hostname/IP 10.127.197.180 and Port 389. The Secondary Server is currently disabled. Access is set to 'Authenticated Access' for both servers. The Admin DN for the Primary Server is 'cn=Administrator,cn=Users,dc='.

Konfigurieren der Verzeichnisorganisation, der Gruppen und der Attribute

1. Wählen Sie die richtige Organisationsgruppe des Benutzers basierend auf der Hierarchie der im LDAP-Server gespeicherten Benutzer aus.

The screenshot shows the Cisco ISE Administration interface for Identity Management, specifically the 'Directory Organization' sub-tab. The 'Subject Search Base' and 'Group Search Base' are both set to 'dc=anshsinh,dc=local'. There are 'Naming Contexts...' buttons next to these fields. The 'Search for MAC Address in Format' is set to 'xx-xx-xx-xx-xx-xx'. There are two checkboxes for stripping parts of the subject name based on a separator, both of which are currently unchecked.

Administrator-Zugriff für LDAP-Benutzer aktivieren

Führen Sie diese Schritte aus, um die kennwortbasierte Authentifizierung zu aktivieren.

1. Navigieren Sie zu ISE > Administration > System > Admin Access > Authentication.
2. Wählen Sie auf der Registerkarte Authentifizierungsmethode die Option Kennwortbasiert aus.
3. Wählen Sie LDAP aus dem Dropdown-Menü Identitätsquelle aus.
4. Klicken Sie auf Änderungen speichern.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb path is Administration > System > Admin Access > Authentication. The left sidebar has a menu with Authentication, Authorization, Administrators, and Settings. The main content area is titled 'Authentication Method' and includes sub-sections for Password Policy, Account Disable Policy, and Lock/Suspend Settings. Under 'Authentication Type', the 'Password Based' option is selected. Below it, the 'Identity Source' is set to 'LDAP:LDAP\_Server' via a dropdown menu. The 'Client Certificate Based' option is unselected. At the bottom right, there are 'Save' and 'Reset' buttons.

## Zuordnen der Admin-Gruppe zur LDAP-Gruppe

Konfigurieren Sie die Administratorgruppe auf der ISE, und ordnen Sie sie der AD-Gruppe zu. Dadurch erhält der konfigurierte Benutzer auf Basis der Autorisierungsrichtlinien, die auf den konfigurierten RBAC-Berechtigungen für den Administrator basieren, Zugriff auf Basis der Gruppenmitgliedschaft.

The screenshot shows the Cisco ISE Administration interface for configuring an Admin Group. The breadcrumb path is Administration > System > Admin Access > Admin Groups. The left sidebar has a menu with Authentication, Authorization, Administrators, and Settings. The main content area is titled 'Admin Group' and shows the configuration for 'LDAP\_User\_Group'. The 'Name' field is filled with 'LDAP\_User\_Group'. The 'Description' field is empty. The 'Type' is set to 'External'. The 'External Identity Source' is 'LDAP\_Server'. Under 'External Groups', the group 'CN=employee,CN=Users,DC=a' is selected. At the bottom, there is a 'Member Users' section with 'Add' and 'Delete' buttons and a table with columns for Status, Email, Username, First Name, and Last Name. The table currently shows 'No data available'.

## Festlegen von Berechtigungen für den Menüzugriff

1. Navigieren Sie zu ISE > Administration > System > Authorization > Permissions > Menu Access.

2. Legen Sie den Menüzugriff für den Administrator fest, der auf die ISE-GUI zugreifen soll. Sie können die untergeordneten Entitäten so konfigurieren, dass sie in der GUI angezeigt oder ausgeblendet werden, damit ein Benutzer bei Bedarf nur eine Reihe von Vorgängen ausführen kann.

3. Klicken Sie auf Speichern.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration · System' and a menu with options: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, **Admin Access**, and Settings. The left sidebar shows a tree view with 'Permissions' expanded to 'Menu Access'. The main content area is titled 'Edit Menu Access Permission' for 'LDAP\_Menu\_Access'. It features a 'Name' field with the value 'LDAP\_Menu\_Access' and a 'Description' text area. Below this is the 'Menu Access Privileges' section, which includes a tree view of the 'ISE Navigation Structure' and a 'Permissions for Menu Access' section with radio buttons for 'Show' (selected) and 'Hide'.

## Festlegen von Berechtigungen für den Datenzugriff

1. Navigieren Sie zu ISE > Administration > System > Authorization > Permissions > Data Access.

2. Definieren Sie den Datenzugriff für den Administrator, damit dieser vollständigen oder schreibgeschützten Zugriff auf die Identitätsgruppen in der ISE-GUI hat.

3. Klicken Sie auf Speichern.

The screenshot displays the Cisco ISE Administration interface. The top navigation bar includes 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The left sidebar shows a menu with 'Authentication', 'Authorization', 'Permissions', 'Menu Access', 'Data Access', 'RBAC Policy', 'Administrators', and 'Settings'. The main content area is titled 'Edit Data Access Permission' and shows the configuration for 'LDAP\_Data\_Access'. The '\* Name' field is set to 'LDAP\_Data\_Access'. Below it is a 'Description' text area. The 'Data Access Privileges' section is expanded to show a list of groups: 'Admin Groups', 'User Identity Groups', 'Endpoint Identity Groups', and 'Network Device Groups'. To the right of this list, the 'Permissions for Data Access' are set to 'Full Access' (selected with a radio button), with 'Read Only Access' and 'No Access' as unselected options.

## RBAC-Berechtigungen für die Admin-Gruppe festlegen

1. Navigieren Sie zu ISE > Administration > System > Admin Access > Authorization > Policy.
2. Wählen Sie im Dropdown-Menü "Aktionen" auf der rechten Seite die Option Neue Richtlinie einfügen aus, um eine neue Richtlinie hinzuzufügen.
3. Erstellen Sie eine neue Regel mit der Bezeichnung LDAP\_RBAC\_policy, ordnen Sie sie der im Abschnitt Admin-Zugriff für AD aktivieren definierten Admin-Gruppe zu, und weisen Sie ihr Berechtigungen für den Menü- und Datenzugriff zu.
4. Klicken Sie auf Save Changes (Änderungen speichern), um die Bestätigung der gespeicherten Änderungen in der unteren rechten Ecke der GUI anzuzeigen.

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... × 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

 Hinweis: Der Administrator kann die vom System generierten Standardrichtlinien und -berechtigungen für die rollenbasierte Zugriffskontrolle nicht ändern. Hierzu müssen Sie neue RBAC-Richtlinien mit den erforderlichen Berechtigungen erstellen, die auf Ihren Anforderungen basieren, und diese Richtlinien einer Admin-Gruppe zuordnen.

 Hinweis: Nur ein Admin-Benutzer aus der Standard-Super Admin-Gruppe kann andere Admin-Benutzer ändern oder löschen. Selbst ein extern zugeordneter Benutzer, der Teil einer Admin-Gruppe ist, die mit den Menü- und Datenzugriffsberechtigungen der Super Admin-Gruppe geklont wurde, kann einen Admin-Benutzer nicht ändern oder löschen.

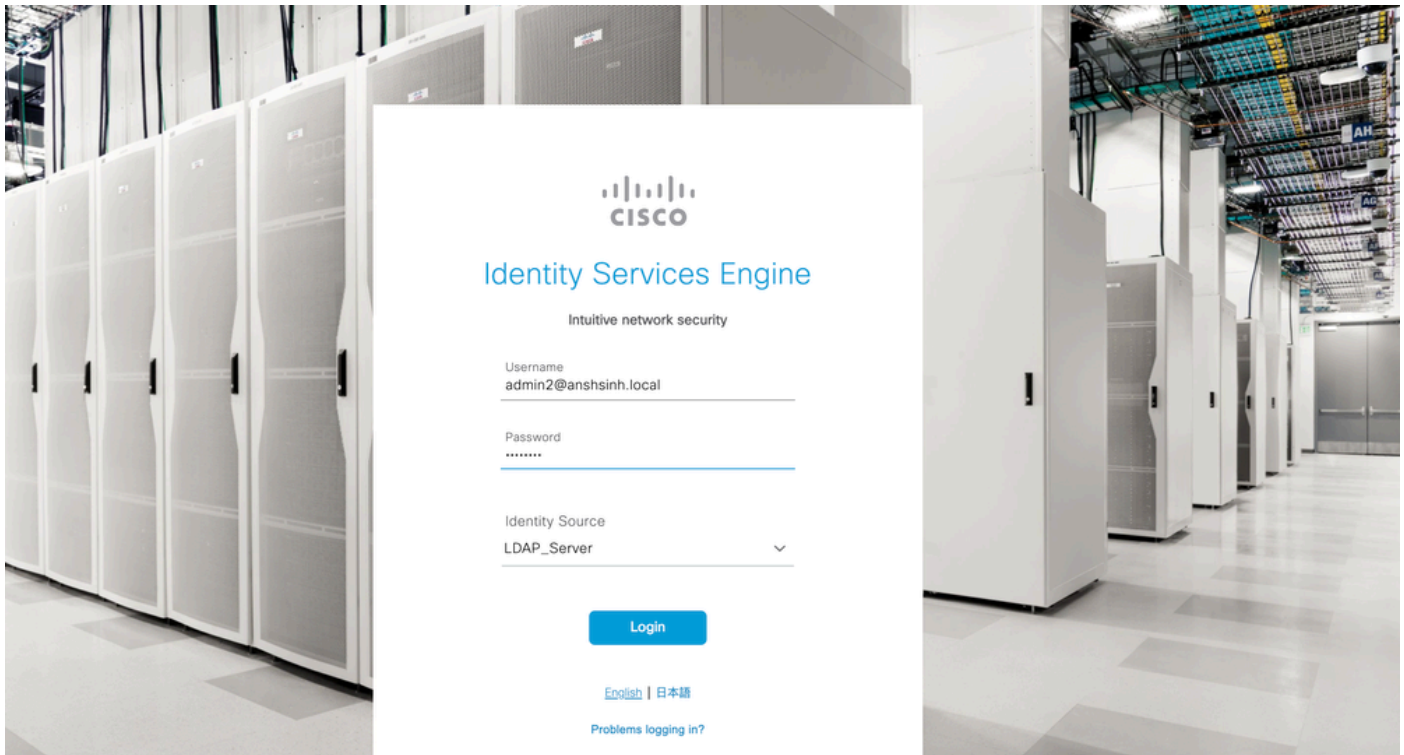
## Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

### Zugriff auf die ISE mit AD-Anmeldeinformationen

Gehen Sie wie folgt vor, um mit AD-Anmeldeinformationen auf die ISE zuzugreifen:

1. Öffnen der ISE-GUI zur Anmeldung beim LDAP-Benutzer
2. Wählen Sie LDAP\_Server aus dem Dropdown-Menü Identitätsquelle aus.
3. Geben Sie den UPN und das Kennwort aus der LDAP-Datenbank ein, und melden Sie sich an.



Überprüfen Sie die Anmeldung für die Administratoranmeldungen in Audit Reports (Überwachungsberichte). Navigieren Sie zu ISE > Operations > Reports > Audit > Administrators Logins.

Cisco ISE Operations · Reports Evaluation Mode 64 Days

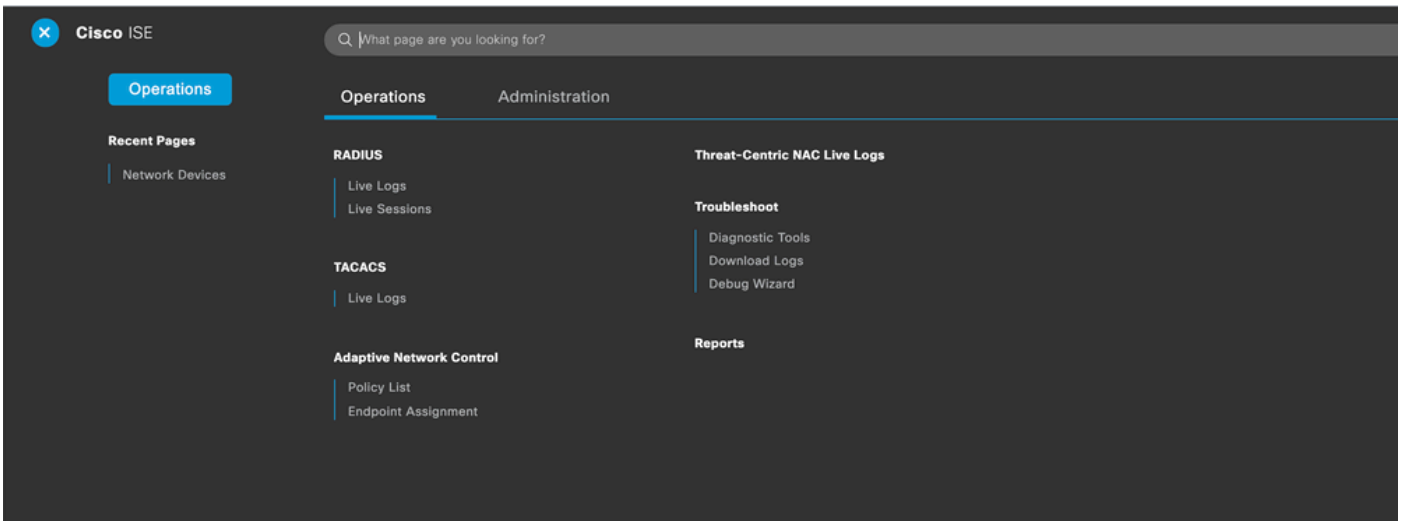
### Administrator Logins

From 2020-10-10 00:00:00.0 To 2020-10-10 10:58:13.0  
Reports exported in last 7 days: 0

Logged At	Administrator	IP Address	Server	Event	Event Details
Today	Administrator		Server		
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

Um sicherzustellen, dass diese Konfiguration ordnungsgemäß funktioniert, überprüfen Sie den authentifizierten Benutzernamen oben rechts in der ISE-GUI. Definieren Sie einen benutzerdefinierten Zugriff mit eingeschränktem Zugriff auf das Menü, wie hier gezeigt:





## Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

### Allgemeine Informationen

Um den RBAC-Prozess zu beheben, müssen diese ISE-Komponenten beim Debuggen auf dem ISE-Admin-Knoten aktiviert werden:

RBAC - Diese Meldung druckt die RBAC-bezogene Nachricht, wenn wir uns anmelden (ise-psc.log).

access-filter - Gibt den Zugriff auf den Ressourcenfilter aus (ise-psc.log)

runtime-AAA - Gibt die Protokolle für Anmelde- und LDAP-Interaktionsmeldungen aus (prtt-server.log)

### Paketerfassungsanalyse

No.	Time	Source	Destination	Protocol	Length	User-Name	Ct. Info
579	2028-09-30 01:21:08.848523	10.106.32.184	10.127.197.188	LDAP	73		unbindRequest(4)
1840	2028-09-30 01:21:13.346421	10.106.32.184	10.127.197.188	LDAP	140		bindRequest(1) "CN=Administrator,CN=Users,DC=anshshih,DC=local" simple
1841	2028-09-30 01:21:13.348424	10.127.197.188	10.106.32.184	LDAP	88		bindResponse(1) success
1842	2028-09-30 01:21:13.348723	10.106.32.184	10.127.197.188	LDAP	191		searchRequest(1) "dc=anshshih,dc=local" wholesubtree
1844	2028-09-30 01:21:13.349581	10.127.197.188	10.106.32.184	LDAP	475		searchResEntry(2) "CN=admin2,CN=Users,DC=anshshih,DC=local"   searchRes
1848	2028-09-30 01:21:13.351826	10.106.32.184	10.127.197.188	LDAP	127		bindRequest(1) "CN=admin2,CN=Users,DC=anshshih,DC=local" simple
1849	2028-09-30 01:21:13.352809	10.127.197.188	10.106.32.184	LDAP	88		bindResponse(1) success
15320	2028-09-30 01:21:40.068100	10.106.32.184	10.127.197.188	LDAP	191		searchRequest(3) "dc=anshshih,dc=local" wholesubtree
15325	2028-09-30 01:21:40.069045	10.127.197.188	10.106.32.184	LDAP	475		searchResEntry(3) "CN=admin2,CN=Users,DC=anshshih,DC=local"   searchRes
15330	2028-09-30 01:21:40.069756	10.106.32.184	10.127.197.188	LDAP	127		bindRequest(2) "CN=admin2,CN=Users,DC=anshshih,DC=local" simple
15337	2028-09-30 01:21:40.071884	10.127.197.188	10.106.32.184	LDAP	88		bindResponse(2) success

### Protokollanalyse

Überprüfen Sie den Port-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

Überprüfen Sie das ise-psc.log.

Aus diesen Protokollen können Sie die RBAC-Richtlinie überprüfen, die für den Benutzer admin2 beim Zugriff auf die Netzwerkgeräteressource verwendet wird.

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

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.