

# Cisco Identity Services Engine(ISE)2.4による ASR9K TACACSの設定

## 内容

[概要](#)

[背景説明](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[IOS® XRの定義済みコンポーネント](#)

[定義済みユーザグループ](#)

[事前定義されたタスクグループ](#)

[ユーザ定義タスクグループ](#)

[ルータのAAA設定](#)

[ISE サーバの設定](#)

[確認](#)

[Operator](#)

[AAAを使用するオペレータ](#)

[Sysadmin](#)

[ルートシステム](#)

[トラブルシューティング](#)

## 概要

このドキュメントでは、Cisco Identity Services Engine(ISE)2.4サーバでTACACS+を介して認証および認可するためのASR 9000シリーズアグリゲーションサービスルータ(ASR)の設定について説明します。

## 背景説明

この例では、Cisco IOS® XRソフトウェアシステムでユーザアクセスを制御するために使用される、タスクベースの認可の管理モデルの実装を示します。タスクベースの承認を実装するために必要な主なタスクには、ユーザグループとタスクグループの設定方法が含まれます。ユーザグループとタスクグループは、認証、許可、アカウントिंग(AAA)サービスに使用されるCisco IOS® XRソフトウェアコマンドセットを使用して設定されます。認証コマンドは、ユーザまたはプリンシパルのIDを確認するために使用されます。認証コマンドは、特定のタスクを実行するために、認証されたユーザ(またはプリンシパル)に権限が付与されていることを確認するために使用されます。アカウントングコマンドは、セッションのロギングや、特定のユーザまたはシステムが生成したアクションを記録して監査証跡を作成するために使用されます。

## 前提条件

## 要件

次の項目に関する知識があることが推奨されます。

- ASR 9000の導入と基本設定
- TACACS+プロトコル
- ISE 2.4の導入と設定

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS® XRソフトウェアを搭載したASR 9000、バージョン5.3.4
- Cisco ISE 2.4

このドキュメントの情報は、特定のラボ環境にあるデバイスから作成されます。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。ネットワークが稼働中の場合は、設定変更による潜在的な影響を完全に理解していることを確認します。

## 設定

### IOS® XRの定義済みコンポーネント

IOS® XRには、事前定義されたユーザグループとタスクグループがあります。管理者は、これらの定義済みグループを使用するか、要件に従ってカスタムグループを定義できます。

### 定義済みユーザグループ

IOS® XRでは、次のユーザグループが事前定義されています。

#### ユーザグループ 権限

Ciscoサポート	デバッグ機能とトラブルシューティング機能（通常、シスコテクニカルサポート担当者）
netadmin	Open Shortest Path First(OSPF)などのネットワークプロトコルを設定します（通常はネットワークエンジニア）
会社名	日常的な監視アクティビティを実行し、設定権限を制限します。
root-lr	1つのRP内のすべてのコマンドを表示および実行します。
ルートシステム	システム内のすべてのRPのすべてのコマンドを表示および実行します。
sysadmin	コアダンプの格納場所の維持や、ネットワークタイムプロトコル(NTP)クロックの設定など
serviceadmin	セッションボーダーコントローラ(SBC)などのサービス管理タスクを実行します。

事前定義された各ユーザグループには、特定のタスクグループがマッピングされており、変更することはできません。事前定義されたユーザグループを確認するには、次のコマンドを使用します。

```
RP/0/RSP0/CPU0:ASR9k#sh aaa usergroup ?
```

```
|          Output Modifiers
root-lr   Name of the usergroup
netadmin  Name of the usergroup
operator  Name of the usergroup
sysadmin  Name of the usergroup
```

```

retrieval      Name of the usergroup
maintenance    Name of the usergroup
root-system    Name of the usergroup
provisioning   Name of the usergroup
read-only-tg   Name of the usergroup
serviceadmin   Name of the usergroup
cisco-support  Name of the usergroup
WORD           Name of the usergroup
<cr>

```

## 事前定義されたタスクグループ

管理者が使用できる定義済みのタスクグループは、通常は初期設定に使用できます。

- cisco-support:シスコのサポート担当者タスク
- netadmin:ネットワーク管理者タスク
- [operator] : オペレータの日常業務 ( デモンストレーション用 )
- root-lr:セキュアドメインルータ管理者タスク
- root-system:システム全体の管理者タスク
- sysadmin:システム管理者タスク
- serviceadmin:サービス管理タスク

定義済みのタスクグループを確認するには、次のコマンドを使用します。

```
RP/0/RSP1/CPU0:ASR9k#show aaa taskgroup ?
```

```

|           Output Modifiers
root-lr     Name of the taskgroup
netadmin    Name of the taskgroup
operator    Name of the taskgroup
sysadmin    Name of the taskgroup
root-system Name of the taskgroup
serviceadmin Name of the taskgroup
cisco-support Name of the taskgroup
WORD        Name of the taskgroup
<cr>

```

```
RP/0/RSP1/CPU0:ASR9k#show aaa task supported
```

[AAA]	ACL	[管理 ( Admin ) ]	Ancp	ATM	基本サービス	Bcdl
Boot	バンドル	call-home	CDP	CEF	Cgn	Ciscoサポ-
暗号化	Diag	不許可	ドライバ	Dwdm	EEM	eigrp
ファブリック	fault-mgr	ファイルシステム	Firewall	FR	Hdlc	ホストサー
インベントリ	ip-services	Ipv4	Ipv6	isis	L2vpn	LI
LPTS	モニタ	mpls-ldp	mpls-static	mpls-te	マルチキャスト	NetFlow
ospf	桜井	Pbr	pkg-mgmt	pos-dpt	Ppp	QoS
rip	root-lr	ルートシステム	ルートマ ップ	route-policy	SBC	snmp
sysmgr	システム	トランスポート	ttyアクセス	Tunnel (トンネル)	ユニバーサル	VLAN

上記の各タスクには、次のいずれか、または4つのすべての権限を付与できます。

read 読み取り操作のみを許可する指定を指定します。  
write 変更操作を許可し、暗黙的に読み取り操作を許可する指定を指定します。

実行 アクセス操作を許可する指定を指定します。たとえば、pingとTelnetなどです。  
デバッグ デバッグ操作を許可する指定を指定します。

## ユーザ定義タスクグループ

管理者は、特定のニーズを満たすようにカスタムタスクグループを構成できます。次に設定例を示します。

```
RP/0/RSP1/CPU0:ASR9k(config)#taskgroup TAC-Defined-TASK
RP/0/RSP1/CPU0:ASR9k(config-tg)#task ?
  debug      Specify a debug-type task ID
  execute    Specify a execute-type task ID
  read       Specify a read-type task ID
  write      Specify a read-write-type task ID
```

```
RP/0/RSP1/CPU0:ASR9k(config-tg)#task read aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task write aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task execute aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task debug aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task read acl
RP/0/RSP1/CPU0:ASR9k(config-tg)#task write acl
RP/0/RSP1/CPU0:ASR9k(config-tg)#task execute acl
RP/0/RSP1/CPU0:ASR9k(config-tg)#commit
```

```
RP/0/RSP1/CPU0:ASR9k#show aaa taskgroup TAC-Defined-TASK
Task group 'TAC-Defined-TASK'
```

```
Task IDs included directly by this group:
Task:          aaa  : READ    WRITE    EXECUTE  DEBUG
Task:          acl  : READ    WRITE    EXECUTE
```

```
Task group 'TAC-Defined-TASK' has the following combined set
of task IDs (including all inherited groups):
Task:          aaa  : READ    WRITE    EXECUTE  DEBUG
Task:          acl  : READ    WRITE    EXECUTE
```

**describe**コマンドを使用すると、特定のコマンドに必要なタスクグループと権限を検索できます。

例 1 :

```
RP/0/RSP1/CPU0:ASR9k#describe show aaa usergroup
Package:
.....
User needs ALL of the following taskids:

aaa (READ)
RP/0/RSP1/CPU0:ASR9k#
```

ユーザがshow aaa usergroupコマンドを実行できるようにするには、タスクグループ : task read aaaをユーザグループに割り当てる必要があります。

例 2 :

```
RP/0/RSP1/CPU0:ASR9k(config)#describe aaa authentication login default group tacacs+
Package:
.....
User needs ALL of the following taskids:

aaa (READ WRITE)
RP/0/RSP1/CPU0:ASR9k(config)#
```

ユーザがコンフィギュレーションモードから `authentication login default group tacacs+` コマンドを実行できるようにするには、`task group: task read write aaa` をユーザグループに割り当てる必要があります。

管理者は、複数のタスクグループを継承できるユーザグループを定義できます。次に設定の例を示します。

```
RP/0/RSP1/CPU0:ASR9k#show aaa usergroup TAC-Defined
Tue Feb 16 00:50:56.799 UTC
User group 'TAC-Defined'
  Inherits from task group 'operator'

User group 'TAC-Defined' has the following combined set
of task IDs (including all inherited groups):
Task:      basic-services  : READ      WRITE      EXECUTE      DEBUG
Task:      cdp             : READ
Task:      diag           : READ
Task:      ext-access     : READ              EXECUTE
Task:      logging        : READ
```

```
RP/0/RSP1/CPU0:ASR9k#conf t
RP/0/RSP1/CPU0:ASR9k(config)#usergroup TAC-Defined
RP/0/RSP1/CPU0:ASR9k(config-ug)#taskgroup TAC-Defined-TASK
RP/0/RSP1/CPU0:ASR9k(config-ug)#commit
```

```
RP/0/RSP1/CPU0:ASR9k#show aaa usergroup TAC-Defined
Tue Feb 16 00:51:31.494 UTC
User group 'TAC-Defined'
  Inherits from task group 'operator'
  Inherits from task group 'TAC-Defined-TASK'

User group 'TAC-Defined' has the following combined set
of task IDs (including all inherited groups):
Task:      aaa           : READ      WRITE      EXECUTE      DEBUG
Task:      acl           : READ      WRITE      EXECUTE
Task:      basic-services : READ      WRITE      EXECUTE      DEBUG
Task:      cdp           : READ
Task:      diag          : READ
Task:      ext-access    : READ              EXECUTE
Task:      logging       : READ
```

## ルータのAAA設定

ASRルータのTACACSサーバに、使用するIPアドレスと共有秘密を設定します。

```
RP/0/RSP1/CPU0:ASR9k(config)#tacacs-server host 10.106.73.233 port 49
RP/0/RSP1/CPU0:ASR9k(config-tacacs-host)#key 0 cisco
RP/0/RSP1/CPU0:ASR9k(config-tacacs-host)#commit
```

```
!  
tacacs-server host 10.127.196.160 port 49  
key 7 14141B180F0B
```

！  
設定されたTACACSサーバを使用するように、認証と認可を設定します。

```
#aaa authentication login default group tacacs+ local  
#aaa authorization exec default group tacacs+ local
```

設定されたTACACSサーバを使用するようにコマンド許可を設定します ( オプション )。

**注：** 認証と認可が期待どおりに動作することを確認し、コマンド認可を有効にする前にコマンドセットが正しく設定されていることを確認します。正しく設定されていない場合、ユーザはデバイスでコマンドを入力できない可能性があります。

```
#aaa authorization commands default group tacacs+
```

設定されたTACACSサーバを使用するために、コマンドアカウントリングを設定します ( オプション )。

```
#aaa accounting commands default start-stop group tacacs+  
#aaa accounting update newinfo
```

## ISE サーバの設定

ステップ1: ISEサーバのAAAクライアントリストでルータIPを定義するには、[Administration] > [N]に移動します **Network Resources > Network Devices** 図に示すように、共有秘密は、図に示すようにASRルータに設定されている共有秘密と同じである必要があります。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices List > New Network Device

Network Devices

\* Name LAB\_ASR  
Description LAB\_ASR device

IP Address \* IP: 10.106.37.160 / 32

\* Device Profile Cisco  
Model Name  
Software Version

\* Network Device Group  
Location LAB Set To Default  
IPSEC Is IPSEC Device Set To Default  
Device Type ASR Set To Default

RADIUS Authentication Settings  
 TACACS Authentication Settings  
Shared Secret Show  
Enable Single Connect Mode  
 Legacy Cisco Device  
 TACACS Draft Compliance Single Connect Support

SNMP Settings  
 Advanced TrustSec Settings

Submit Cancel

## ネットワークデバイスの設定

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> LAB_ASR	10.106.37.16...	Cisco	LAB	ASR	LAB_ASR device

## ネットワークデバイスの設定

ステップ2：要件に従ってユーザグループを定義します。この例では、4つのグループを使用します。[Administration] > [Identity Management] > [Groups] > [User Identity Groups]でグループを定義できます。この例で作成するグループは次のとおりです。

1. ASR-Operator
2. ASR-Operator-AAA
3. ASR-RootSystem
4. ASR-Sysadmin

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> ASR-Operator	
<input type="checkbox"/> ASR-Operator-AAA	
<input type="checkbox"/> ASR-RootSystem	
<input type="checkbox"/> ASR-Sysadmin	
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_SocialLogin (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

ID グループステップ3：図に示すように、ユーザを作成し、以前に作成した各ユーザグループにマッピングします。

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled	ASRaaa					ASR-Operator-AAA	
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled	ASRRead					ASR-Operator	
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled	ASRRoot					ASR-RootSystem	
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled	ASRwrite					ASR-Sysadmin	

## アイデンティティ/ユーザ

注：この例では、ISE内部ユーザが認証と認可に使用されます。外部IDソースを使用した認証と認可は、このドキュメントの範囲外です。

ステップ4：各ユーザにプッシュするシェルプロファイルを定義します。そのためには、[Work Centers] > [Device Administration] > [Policy Elements] > [Results] > [TACACS Profiles]に移動します。新しいシェルプロファイルは、図に示すように、以前のバージョンのISEにも設定できます。この例で定義されているシェルプロファイルは次のとおりです。

1. ASR\_Operator
2. ASR\_RootSystem
3. ASR\_Sysadmin
4. Operator\_with\_AAA

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	ASR_Operator	Shell	
<input type="checkbox"/>	ASR_RootSystem	Shell	
<input type="checkbox"/>	ASR_Sysadmin	Shell	
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	Operator_with_AAA	Shell	
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR

## TACACSのシェルプロファイル

[Add]ボタンをクリックして、[Type]、[Name]、および[Value]フィールドを入力できます([Custom Attributes]セクションの下の図を参照)。

オペレータの役割：

<input type="checkbox"/>	Type	Name	Value
<input type="checkbox"/>	MANDATORY	task	nwx,#operator

ASRオペレータシェルプロファイルルートシステムロールの場合：

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

TACACS Profiles > ASR\_RootSystem

**TACACS Profile**

Name: ASR\_RootSystem

Description:

Task Attribute View Raw View

**Common Tasks**

Common Task Type: Shell

- Default Privilege (Select 0 to 15)
- Maximum Privilege (Select 0 to 15)
- Access Control List
- Auto Command
- No Escape (Select true or false)
- Timeout (Minutes (0-9999))
- Idle Time (Minutes (0-9999))

**Custom Attributes**

+ Add Trash Edit

Type	Name	Value
<input type="checkbox"/> MANDATORY	task	nwc,#root-system

Cancel Save

ASRルートシステムシェルプロファイルsysadminロールの場合 :

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassivID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

TACACS Profiles > ASR\_Sysadmin

**TACACS Profile**

Name ASR\_Sysadmin

Description

Task Attribute View Raw View

**Common Tasks**

Common Task Type Shell

Default Privilege (Select 0 to 15)  
 Maximum Privilege (Select 0 to 15)  
 Access Control List  
 Auto Command  
 No Escape (Select true or false)  
 Timeout Minutes (0-9999)  
 Idle Time Minutes (0-9999)

**Custom Attributes**

+ Add Trash Edit

Type	Name	Value
<input type="checkbox"/> MANDATORY	task	rwc_#sysadmin

Cancel Save

ASR SysadminシェルプロファイルオペレータおよびAAAロール :

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > Reports > Settings

TACACS Profiles > Operator\_with\_AAA

**TACACS Profile**

Name: Operator\_with\_AAA

Description:

Task Attribute View | Raw View

**Common Tasks**

Common Task Type: Shell

- Default Privilege: (Select 0 to 15)
- Maximum Privilege: (Select 0 to 15)
- Access Control List:
- Auto Command:
- No Escape: (Select true or false)
- Timeout: Minutes (0-9999)
- Idle Time: Minutes (0-9999)

**Custom Attributes**

+ Add | Trash | Edit

Type	Name	Value
<input type="checkbox"/> MANDATORY	task	nwc:aaa,#operator

Cancel Save

AAAシェルプロファイルを持つオペレータステップ5:[Administration] > [Identity Management] > [Identity Source Sequences]で内部ユーザーを使用するようにアイデンティティ・ソース・シーケンスを構成します。新しいアイデンティティ・ソース・シーケンスを追加するか、使用可能なアイデンティティ・ソース・シーケンスを編集できます。

The screenshot shows the 'Identity Source Sequence' configuration page in Cisco ISE. The sequence name is 'All\_User\_ID\_Stores' and its description is 'A built-in Identity Source Sequence to include all User Identity Stores'. Under 'Certificate Based Authentication', the 'Preloaded\_Certificate' profile is selected. The 'Authentication Search List' section shows a list of available identity stores ('Internal Endpoints') and a list of selected identity stores ('Internal Users', 'All\_AD\_Join\_Points', 'Guest Users'). The 'Advanced Search List Settings' section has the option 'Treat as if the user was not found and proceed to the next store in the sequence' selected. At the bottom, there are 'Save' and 'Reset' buttons.

ステップ6:[Work Centers] > [Device Administration] > [Device Admin Policy Sets] > [Choose Policy Set]で認証ポリシーを設定し、内部ユーザを含むIDストアシーケンスを使用します。前に作成したユーザIDグループを使用して要件に基づいて認可を設定し、それぞれのシェルフプロファイルをマップします ( 図を参照 )。

The screenshot shows the 'Device Admin Policy Sets' configuration page. A policy set named 'ASR TACACS policy' is shown with the following conditions: 'DEVICE Device Type EQUALS All Device Types#ASR' and 'DEVICE Location EQUALS All Locations#LAB'. The policy set is associated with the 'Default Device Admin' profile. Below the policy set, the 'Authentication Policy (1)' section shows a 'Default' policy set with the 'All\_User\_ID\_Stores' identity source sequence mapped to it.

## 認証ポリシー

認可ポリシーは、要件に基づいてさまざまな方法で設定できます。図に示すルールは、デバイスの場所、タイプ、および特定の内部ユーザIDグループに基づいています。選択したシェルフプロファイルは、許可の時点でコマンドセットとともにプッシュされます。

Authorization Policy - Local Exceptions			Authorization Policy - Global Exceptions				
Authorization Policy (5)							
+	Status	Rule Name	Conditions	Results		Hits	Actions
				Command Sets	Shell Profiles		
	ASR_Root-System_Rule	AND	InternalUser IdentityGroup EQUALS User Identity Groups ASR-RootSystem DEVICE Location EQUALS All Locations#LAB DEVICE Device Type EQUALS All Device Types#ASR	PermitAllCommands	ASR_RootSystem	0	
	ASR_Sysadmin-Rule	AND	InternalUser IdentityGroup EQUALS User Identity Groups ASR-Sysadmin DEVICE Location EQUALS All Locations#LAB DEVICE Device Type EQUALS All Device Types#ASR	PermitAllCommands	ASR_Sysadmin	0	
	ASR_Operator_AAA_Rule	AND	InternalUser IdentityGroup EQUALS User Identity Groups ASR-Operator-AAA DEVICE Location EQUALS All Locations#LAB DEVICE Device Type EQUALS All Device Types#ASR	PermitAllCommands	Operator_with_AAA	0	
	ASR_Operator_Rule	AND	InternalUser IdentityGroup EQUALS User Identity Groups ASR-Operator DEVICE Location EQUALS All Locations#LAB DEVICE Device Type EQUALS All Device Types#ASR	PermitAllCommands	ASR_Operator	0	
	Default			DenyAllCommands	Deny All Shell Profile	0	

## 認可ポリシー

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

## Operator

ユーザグループと、ユーザがルータにログインしたときに割り当てられたタスクグループを確認します。

```
username: ASRread
```

```
password:
```

```
RP/0/RSP1/CPU0:ASR9k#show user
```

```
ASRread
```

```
RP/0/RSP1/CPU0:ASR9k#show user group
```

```
operator
```

```
RP/0/RSP1/CPU0:ASR9k#show user tasks
```

```
Task:          basic-services  : READ    WRITE    EXECUTE  DEBUG
```

```
Task:                cdp      : READ
```

```
Task:                diag     : READ
```

```
Task:          ext-access  : READ          EXECUTE
```

```
Task:                logging  : READ
```

## AAAを使用するオペレータ

ユーザグループと、割り当てられたタスクグループを確認します。アスラア ユーザがルータにログインします。

**注:**オペレータのタスクがTACACSサーバからプッシュされ、AAAタスクの読み取り、書き込み、および実行権限とともに実行されます。

```
username: asraaa
```

password:

```
RP/0/RSP1/CPU0:ASR9k#sh user
asraaa
```

```
RP/0/RSP1/CPU0:ASR9k#sh user group
operator
```

```
RP/0/RSP1/CPU0:ASR9k#sh user tasks
Task:          aaa      : READ      WRITE      EXECUTE
Task:    basic-services : READ      WRITE      EXECUTE      DEBUG
Task:          cdp      : READ
Task:          diag     : READ
Task:    ext-access    : READ          EXECUTE
Task:    logging      : READ
```

## Sysadmin

ユーザグループと、割り当てられたタスクグループを確認します。 **asrwrite** ユーザがルータにログインします。

```
username: asrwrite
password:
```

```
RP/0/RSP1/CPU0:ASR9k#sh user
asrwrite
```

```
RP/0/RSP1/CPU0:ASR9k#sh user group
sysadmin
```

```
RP/0/RSP1/CPU0:ASR9k#sh user tasks
Task:          aaa      : READ
Task:          acl      : READ      WRITE      EXECUTE      DEBUG
Task:          admin    : READ
Task:          ancp     : READ
Task:          atm      : READ
Task:    basic-services : READ      WRITE      EXECUTE      DEBUG
Task:          bcdl     : READ
Task:          bfd      : READ
Task:          bgp      : READ
Task:          boot     : READ      WRITE      EXECUTE      DEBUG
Task:          bundle   : READ
Task:    call-home     : READ
Task:          cdp      : READ      WRITE      EXECUTE      DEBUG
Task:          cef      : READ
Task:          cgn      : READ
Task:    config-mgmt   : READ      WRITE      EXECUTE      DEBUG
Task:    config-services : READ      WRITE      EXECUTE      DEBUG
Task:          crypto   : READ      WRITE      EXECUTE      DEBUG
Task:          diag     : READ      WRITE      EXECUTE      DEBUG
Task:          drivers  : READ
Task:          dwdm     : READ
Task:          eem      : READ      WRITE      EXECUTE      DEBUG
Task:          eigrp    : READ
Task:    ethernet-services : READ
```

--More--

(output omitted )

## ルートシステム

ユーザグループと、割り当てられたタスクグループを確認します。asroot ユーザがルータにログインします。

```
username: asroot
password:
```

```
RP/0/RSP1/CPU0:ASR9k#show user
asroot
```

```
RP/0/RSP1/CPU0:ASR9k#show user group
root-system
```

```
RP/0/RSP1/CPU0:ios#show user tasks
Task:          aaa      : READ      WRITE      EXECUTE    DEBUG
Task:          acl      : READ      WRITE      EXECUTE    DEBUG
Task:          admin    : READ      WRITE      EXECUTE    DEBUG
Task:          ancp     : READ      WRITE      EXECUTE    DEBUG
Task:          atm      : READ      WRITE      EXECUTE    DEBUG
Task:          basic-services : READ    WRITE      EXECUTE    DEBUG
Task:          bcdl     : READ      WRITE      EXECUTE    DEBUG
Task:          bfd      : READ      WRITE      EXECUTE    DEBUG
Task:          bgp      : READ      WRITE      EXECUTE    DEBUG
Task:          boot     : READ      WRITE      EXECUTE    DEBUG
Task:          bundle   : READ      WRITE      EXECUTE    DEBUG
Task:          call-home : READ      WRITE      EXECUTE    DEBUG
Task:          cdp      : READ      WRITE      EXECUTE    DEBUG
Task:          cef      : READ      WRITE      EXECUTE    DEBUG
Task:          cgn      : READ      WRITE      EXECUTE    DEBUG
Task:          config-mgmt : READ    WRITE      EXECUTE    DEBUG
Task:          config-services : READ   WRITE      EXECUTE    DEBUG
Task:          crypto   : READ      WRITE      EXECUTE    DEBUG
Task:          diag     : READ      WRITE      EXECUTE    DEBUG
Task:          drivers  : READ      WRITE      EXECUTE    DEBUG
Task:          dwdm     : READ      WRITE      EXECUTE    DEBUG
Task:          eem      : READ      WRITE      EXECUTE    DEBUG
Task:          eigrp    : READ      WRITE      EXECUTE    DEBUG
```

```
--More--
(output omitted )
```

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

[Operations] > [TACACS] > [Live Logs]からISEレポートを確認します。詳細レポートを表示するには、虫眼鏡の記号をクリックします。

Refresh	Export To	Logged Time	Status	Details	Username	Type	Network Device IP	Remote Address	Authorization Policy	Authentication Policy	Ise Node
x					Username		Network Device IP	Remote Address	Authorization Policy	Authentication Policy	Ise Node
		May 14, 2018 03:35:25.792 PM	✓		ASRwrite	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >>> ASR Sysadmin Rulef		mumanika22
		May 14, 2018 03:35:25.695 PM	✓		ASRwrite	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >>> ASR Sysadmin Rulef		mumanika22
		May 14, 2018 03:35:25.597 PM	✓		ASRwrite	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >>> Default >>> Default	mumanika22
		May 14, 2018 03:35:12.959 PM	✓		ASRRoot	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >>> ASR Rootsystem rule		mumanika22
		May 14, 2018 03:35:12.859 PM	✓		ASRRoot	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >>> ASR Rootsystem rule		mumanika22
		May 14, 2018 03:35:12.771 PM	✓		ASRRoot	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >>> Default >>> Default	mumanika22
		May 14, 2018 03:34:53.788 PM	✓		ASRRead	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >>> ASR Operator Rule		mumanika22
		May 14, 2018 03:34:53.685 PM	✓		ASRRead	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >>> ASR Operator Rule		mumanika22
		May 14, 2018 03:34:53.581 PM	✓		ASRRead	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >>> Default >>> Default	mumanika22
		May 14, 2018 03:29:46.359 PM	✓		ASRaaa	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >>> ASR Operator AAA Rule		mumanika22
		May 14, 2018 03:29:46.257 PM	✓		ASRaaa	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >>> ASR Operator AAA Rule		mumanika22
		May 14, 2018 03:29:46.150 PM	✓		ASRaaa	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >>> Default >>> Default	mumanika22

ASRでのトラブルシューティングに役立つコマンドを次に示します。

- ユーザの表示
- show user group
- show user tasks
- show user all