

ACS 4.2 TACACS와의 Prime Infrastructure 통합 컨피그레이션 예

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[구성](#)

[PI에서 ACS를 TACACS 서버로 추가](#)

[PI의 AAA 모드 설정](#)

[PI에서 사용자 역할 특성 검색](#)

[ACS 4.2 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 TACACS+(Terminal Access Controller Access-Control System)의 컨피그레이션 예에 대해 설명합니다

Cisco Prime Infrastructure(PI) 애플리케이션에 대한 인증 및 권한 부여

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ACS(Access Control Server)에서 PI를 클라이언트로 정의
- ACS 및 PI에서 IP 주소 및 동일한 공유 비밀 키를 정의합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ACS 버전 4.2
- Prime Infrastructure 릴리스 3.0

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

구성

PI에서 ACS를 TACACS 서버로 추가

ACS를 TACACS 서버로 추가하려면 다음 단계를 완료합니다.

1단계. 다음으로 이동합니다. **관리 > 사용자 > 사용자, 역할 및 AAA PI**에서

2단계. 왼쪽 사이드바 메뉴에서 **TACACS+ 서버**를 선택하고 **Add TACACS+ servers(TACACS+ 서버 추가)**에서 **Go(이동)**를 클릭하면 이미지가 표시된 것처럼 페이지가 나타납니다.

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

Add TACACS+ Server

* IP Address

* DNS Name

* Port: 49

Shared Secret Format: ASCII

* Shared Secret

* Confirm Shared Secret

* Retransmit Timeout: 5 (secs)

* Retries: 1

Authentication Type: PAP

Local Interface IP: 10.106.68.130

Save Cancel

3단계. ACS 서버의 IP 주소를 추가합니다.

4단계. ACS 서버에 구성된 TACACS+ 공유 암호를 입력합니다.

5단계. 공유 암호 확인 텍스트 상자에 공유 암호를 다시 입력합니다.

6단계. 나머지 필드는 기본 설정으로 둡니다.

7단계. Submit(제출)을 클릭합니다.

PI의 AAA 모드 설정

AAA(Authentication, Authorization, and Accounting) 모드를 선택하려면 다음 단계를 완료하십시오.

1단계. Administration(관리) > AAA로 이동합니다.

2단계. 왼쪽 사이드바 메뉴에서 **AAA Mode(AAA 모드)**를 선택하면 이미지에 표시된 대로 페이지를

볼 수 있습니다.

Administration / Users / Users, Roles & AAA ★

AAA Mode Settings

AAA Mode ? Local RADIUS TACACS+ SSO

Enable fallback to Local ONLY on no server respons

Save

3단계. TACACS+를 선택합니다.

4단계. ACS 서버에 연결할 수 없을 때 관리자가 로컬 데이터베이스를 사용하도록 하려면 Enable Fallback to Local(로컬로 대체 사용) 상자를 선택합니다. 권장되는 설정입니다.

PI에서 사용자 역할 특성 검색

1단계. Administration(관리) > AAA > User Groups(사용자 그룹)로 이동합니다. 이 예에서는 관리자 인증을 보여줍니다. 목록에서 Admin Group Name(관리 그룹 이름)을 찾고 이미지에 표시된 대로 오른쪽의 Task List(작업 목록) 옵션을 클릭합니다.

Administration / Users / Users, Roles & AAA ★

Group Name	Members	Audit Trail	View Task
Admin	virtual		Task List
Config Managers			Task List
Lobby Ambassador			Task List
Monitor Lite			Task List
NBI Credential			Task List
NBI Read			Task List
NBI Write			Task List
North Bound API			Task List
Root	root		Task List
Super Users			Task List
System Monitoring	virtual		Task List

작업 목록 옵션을 클릭하면 다음과 같이 창이 나타납니다.

Task List

Please copy and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

TACACS+ Custom Attributes

```
role0=Admin
task0=View Alerts and Events
task1=Run Job
task2=Device Reports
task3=Alarm Stat Panel Access
task4=RADIUS Servers
task5=Raw NetFlow Reports
task6=Credential Profile Delete Access
task7=Compliance Audit Fix Access
task8=Network Summary Reports
task9=Discovery View Privilege
task10=Configure ACS View Servers
task11=Run Reports List
task12=View CAS Notifications Only
task13=Administration Menu Access
task14=Monitor Clients
task15=Configure Guest Users
task16=Monitor Media Streams
task17=Configure Lightweight Access Point
Templates
task18=Monitor Chokepoints
task19=Maps Read Write
task20=Administrative privileges under Manage and
```

RADIUS Custom Attributes

If the size of the RADIUS attributes on your AAA server is more than 4096 bytes, Please copy ONLY role retrieve the associated TASKS

```
NCS:role0=Admin
NCS:task0=View Alerts and Events
NCS:task1=Run Job
NCS:task2=Device Reports
NCS:task3=Alarm Stat Panel Access
NCS:task4=RADIUS Servers
NCS:task5=Raw NetFlow Reports
NCS:task6=Credential Profile Delete Access
NCS:task7=Compliance Audit Fix Access
NCS:task8=Network Summary Reports
NCS:task9=Discovery View Privilege
NCS:task10=Configure ACS View Servers
NCS:task11=Run Reports List
NCS:task12=View CAS Notifications Only
NCS:task13=Administration Menu Access
NCS:task14=Monitor Clients
NCS:task15=Configure Guest Users
NCS:task16=Monitor Media Streams
NCS:task17=Configure Lightweight Access Point
Templates
NCS:task18=Monitor Chokepoints
NCS:task19=Maps Read Write
NCS:task20=Administrative privileges under Manage
```

2단계. 이러한 특성을 복사하여 메모장 파일에 저장합니다.

3단계. ACS 서버에 사용자 지정 가상 도메인 특성을 추가해야 할 수 있습니다. 사용자 지정 가상 도메인 특성은 동일한 작업 목록 페이지 하단에서 사용할 수 있습니다.

Virtual Domain custom attributes are mandatory. To add custom attributes related to Virtual Domains, please click [here](#).

4단계. 여기 옵션을 클릭하여 가상 도메인 속성 페이지를 가져오면 다음 이미지와 같이 페이지를 볼 수 있습니다.

TACACS+ Custom Attributes

```
virtual-domain0=ROOT-DOMAIN
virtual-domain1=test1
```

RADIUS Custom Attributes

```
NCS:virtual-domain0=ROOT-DOMAIN
NCS:virtual-domain1=test1
```

ACS 4.2 구성

1단계. ACS Admin GUI에 로그인하고 Interface Configuration(인터페이스 컨피그레이션) > TACACS+ 페이지로 이동합니다.

2단계. prime에 대한 새 서비스를 생성합니다. 다음 예에서는 이미지에 표시된 대로 이름 NCS로 구성된 서비스 이름을 보여줍니다.

New Services

		Service	Protocol
<input checked="" type="checkbox"/>	<input type="checkbox"/>	ciscowlc	common
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Wireless-WCS	HTTP
<input checked="" type="checkbox"/>	<input type="checkbox"/>	NCS	HTTP
<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>		

3단계. 2단계에서 만든 메모장의 모든 특성을 사용자 또는 그룹 구성에 추가합니다. 가상 도메인 특성을 추가해야 합니다.

NCS HTTP

Custom attributes

```
virtual-domain0=ROOT-DOMAIN
role0=Admin
task0=View Alerts and Events
task1=Device Reports
task2=RADIUS Servers
task3=Alarm Stat Panel Access
```

4단계. 확인을 클릭합니다.

다음을 확인합니다.

생성한 새 사용자 이름으로 Prime에 로그인하고 **Admin** 역할이 있는지 확인합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

/opt/CSCOlumos/logs 디렉토리에서 사용 가능한 Prime 루트 CLI에서 usermgmt.log를 검토합니다. 오류 메시지가 있는지 확인합니다.

```
user entered username: 138527]
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - [          [TacacsLoginModule]
Primary server=172.18.70.243:49]
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - Thread Id : [835], Entering
Method : [login], Class : [com.cisco.xmp.jaas.tacacs.TacacsLoginClient].
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - Thread Id : [835], Entering
Method : [login], Class : [com.cisco.xmp.jaas.tacacs.SecondaryTacacsLoginClient].
2016-05-12 15:24:18,518 [http-bio-443-exec-10] INFO usermgmt - [Tacacs:connectTacacs()] :
[prepare to ping TACACS+ server (> 0):/172.18.70.243 (-1)].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] INFO usermgmt - [Tacacs:connectTacacs()] :
[Tacacs: Num of ACS is 3].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] INFO usermgmt - [Tacacs:connectTacacs()] :
[Tacacs:activeACSIndex is 0].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] INFO usermgmt - [Tacacs:connectTacacs()] :
[Tacacs: Unable to connect to Server 2: /172.18.70.243 Reason: Connection refused].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] DEBUG usermgmt - [          [Thu May 12 15:24:18
EST 2016] [TacacsLoginModule] exception in client.login( primaryServer, primaryPort,seconda...:
com.cisco.xmp.jaas.XmpAuthenticationServerException: Server Not Reachable: Connection refused]
이 예에서는 방화벽 또는 중간 장치 등에 의해 연결이 거부되는 다양한 이유로 인해 발생할 수 있는
오류 메시지의 예를 보여 줍니다.
```