

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Настройка](#)

[Конфигурации](#)

[Добавьте ACS как СЕРВЕР TACACS в PI](#)

[Параметры настройки режима AAA в PI](#)

[Получите атрибуты роли пользователя из PI](#)

[Настройте ACS 4.2](#)

[Проверка](#)

[Устранение неполадок](#)

Введение

Этот документ описывает пример конфигурации для Terminal Access Controller Access Control System (TACACS) (TACACS +)

проверка подлинности и авторизация на приложении Главной инфраструктуры (PI) Cisco.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Определите PI как клиента в Access Control Server (ACS)
- Определите IP-адрес и идентичный разделяемый секретный ключ на ACS и PI

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версия ACS 4.2
- Главный выпуск 3.0 Инфраструктуры

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

Конфигурации

Добавьте ACS как СЕРВЕР TACACS в PI

Выполните эти шаги для добавления ACS как Сервера tacacs:

Шаг 1. Перейдите к > Users администрирования в PI

Шаг 2. Из левого меню боковой панели выберите **TACACS +, Серверы**, под **Добавляют TACACS +, серверы** нажимают **Go**, и страница появляется как показано в образе:

The screenshot shows the Cisco Prime Infrastructure web interface. The breadcrumb navigation is Administration / Users / Users, Roles & AAA. The left sidebar contains a menu with items: AAA Mode Settings, Active Sessions, Change Password, Local Password Policy, RADIUS Servers, SSO Server Settings, SSO Servers, TACACS+ Servers, User Groups, and Users. The main content area is titled "Add TACACS+ Server" and contains the following fields:

- * IP Address (text input)
- * DNS Name (text input)
- * Port: 49 (text input)
- Shared Secret Format: ASCII (dropdown menu)
- * Shared Secret: (text input with a help icon)
- * Confirm Shared Secret: (text input)
- * Retransmit Timeout: 5 (secs) (text input)
- * Retries: 1 (text input)
- Authentication Type: PAP (dropdown menu)
- Local Interface IP: 10.106.68.130 (dropdown menu)

At the bottom of the form are "Save" and "Cancel" buttons.

Шаг 3. Добавьте IP-адрес сервера ACS.

Шаг 4. Введите TACACS + общий секретный ключ, настроенный в сервере ACS.

Шаг 5. Повторно введите общий секретный ключ в **Подтвердить** текстовом поле **Общего секретного ключа**.

Шаг 6. Остаток выхода полей на их настройке по умолчанию.

Шаг 7. Нажмите кнопку **Submit (Отправить)**.

Параметры настройки режима AAA в PI

Для выбора режима Authentication, Authorization, and Accounting (AAA) выполните эти шаги:

Шаг 1. Перейдите к администрированию > AAA.

Шаг 2. Выберите **AAA Mode** из левого меню боковой панели, вы видите страницу как показано в образе:

Шаг 3. Выберите TACACS +.

Шаг 4. Проверьте Разрешать Нейтрализацию к Локальной коробке, если вы хотите, чтобы администратор использовал локальную базу данных, когда сервер ACS не достижим. Это - рекомендуемая настройка.

Получите атрибуты роли пользователя из PI

Шаг 1. Перейдите к администрированию> AAA> Группы пользователей. Данный пример показывает проверку подлинности администратора. Ищите Название Admin Group в списке и нажмите опцию Task List справа, как показано в образе:

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

Как только вы нажимаете опцию Task List, окно появляется, как показано в образе:

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
```

Шаг 2. Скопируйте эти атрибуты и сохраните его на файле блокнота.

Шаг 3. Вы, возможно, должны добавить пользовательские действительные доменные атрибуты в сервере ACS. Пользовательские действительные доменные атрибуты доступны в нижней части той же страницы Листа задач.

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

Шаг 4. Нажмите по щелчку [здесь](#) опцию для получения страницы атрибута виртуального

домена, и вы видите страницу, как показано в образе:

TACACS+ Custom Attributes

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

RADIUS Custom Attributes

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

Настройте ACS 4.2

Шаг 1. Войдите к **GUI Admin ACS** и перейдите к странице **Interface Configuration> TACACS +**.

Шаг 2. Создайте новый сервис для начала. Данный пример показывает имя сервиса, настроенное с названием **NCS**, как показано в образе:

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"/>		

Шаг 3. Добавьте все атрибуты из блокнота, созданного в Шаге 2 в пользователя или Конфигурацию группы. Убедитесь для добавления действительно-доменных атрибутов.

- 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
```

Шаг 4 Нажмите кнопку ОК.

Проверка

Войдите к началу с новым пользователем, называют вас созданными и подтверждают, что у вас есть роль **Admin**.

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Рассмотрите `usermgmt.log` от главного корневого CLI, доступного в `/opt/CSCOlumos/logs` каталоге. Проверьте, существуют ли какие-либо сообщения об ошибках.

Данный пример показывает выборку сообщения об ошибках, которое могло произойти из-за различных причин как соединение, которому отказывает межсетевой экран или любое промежуточное устройство и т.д.