ACS 5.x AAA, кэширующийся в примере конфигурации Cisco IOS

Содержание

Введение

Этот документ описывает шаги, необходимые для настройки кэширования TACACS + учетные данные пользователя с правами администратора для Telnet и доступа линии VTY. Авторизация и Опознавательное Кэширование были интегрированы в Cisco IOS® Version 15.0 (1) M. Эта функция позволяет маршрутизатору сохранить учетные данные Аутентификации, авторизации и учета (AAA) в своем кэше после того, как она получает TACACS +, отвечают на запрос AAA. Кэш используется, чтобы повысить производительность и уменьшить сумму запросов, отправленных к AAA-серверу, или как метод аутентификации нейтрализации в случае, если AAA-сервер недостижим.

Предварительные условия

Требования

Компания Cisco рекомендует следующее:

- Подтвердите возможность подключения с помощью IP-адреса между маршрутизатором и сервером Cisco Secure Access Control Server (ACS) Версия 5. x.
- Определите маршрутизатор на ACS как Клиент AAA (Сетевые устройства) с тем же общим секретным ключом.

Используемые компоненты

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

- Версия ACS 5
- Маршрутизаторы, которые выполняют версию Cisco IOS 15.1

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

Конфигурация на маршрутизаторе Cisco IOS

1. Введите эти команды для определения Сервера tacacs и предварительного общего ключа:
```
Router(config)#tacacs-server host 192.168.159.41
Router(config)#tacacs-server timeout 4
Router(config)#tacacs-server key SECRET12345
```

2. Введите эти команды для определения групп профиля кэша.
Примечание: Каждое имя профиля должно совпасть с AAA username.
```
Router(config)#aaa cache profile admin
Router(config-profile-map)# profile peteradmin
```

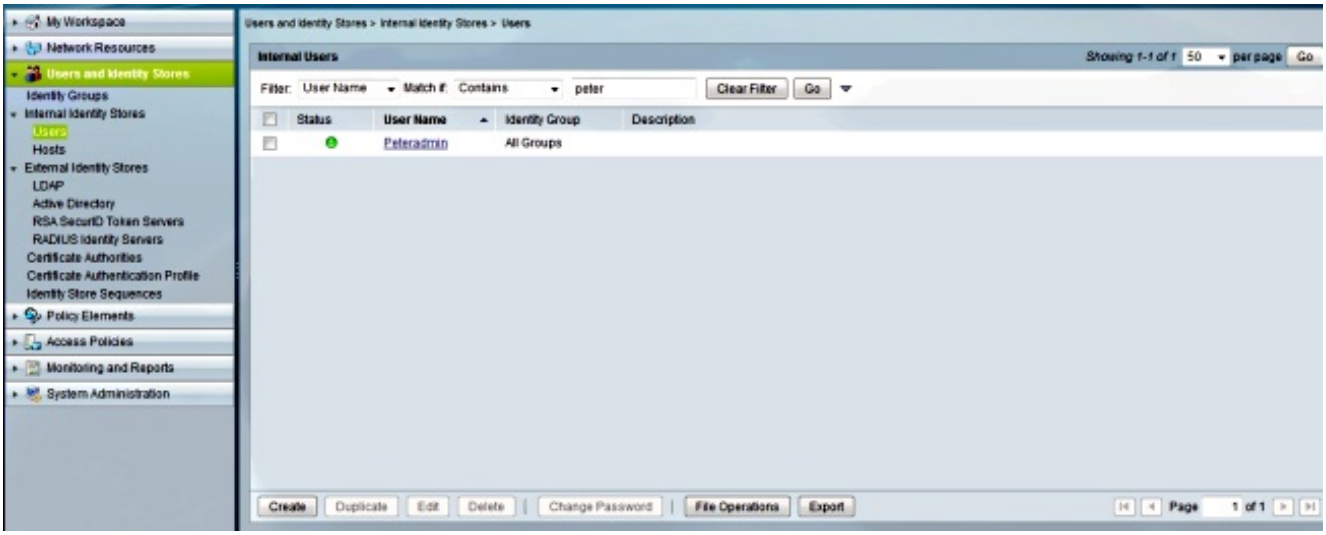
3. Введите эти команды для присвоения проверки подлинности и авторизация, кэширующей правила к группам AAA-серверов:
```
Router(config-profile-map)# aaa group server tacacs+ admin-tac
Router(config-sg-tacacs+)# server 192.168.159.41
Router(config-sg-tacacs+)# cache authentication profile admin
Router(config-sg-tacacs+)# cache authorization profile admin
```

4. Определите списки методов проверки подлинности и авторизация, которые содержат метод кэша. Если AAA-серверы не отвечают, в этом примере конфигурации только используется кэш. Если заказ коммутирован для **кэширования tac admin группы tac admin**, кэш смотрят первым.
Примечание: Enable password от TACACS не кэшируется.
```
aaa authentication login mtac group admin-tac cache admin-tac local
aaa authorization exec default group admin-tac cache admin-tac local
aaa accounting exec default start-stop group admin-tac
```

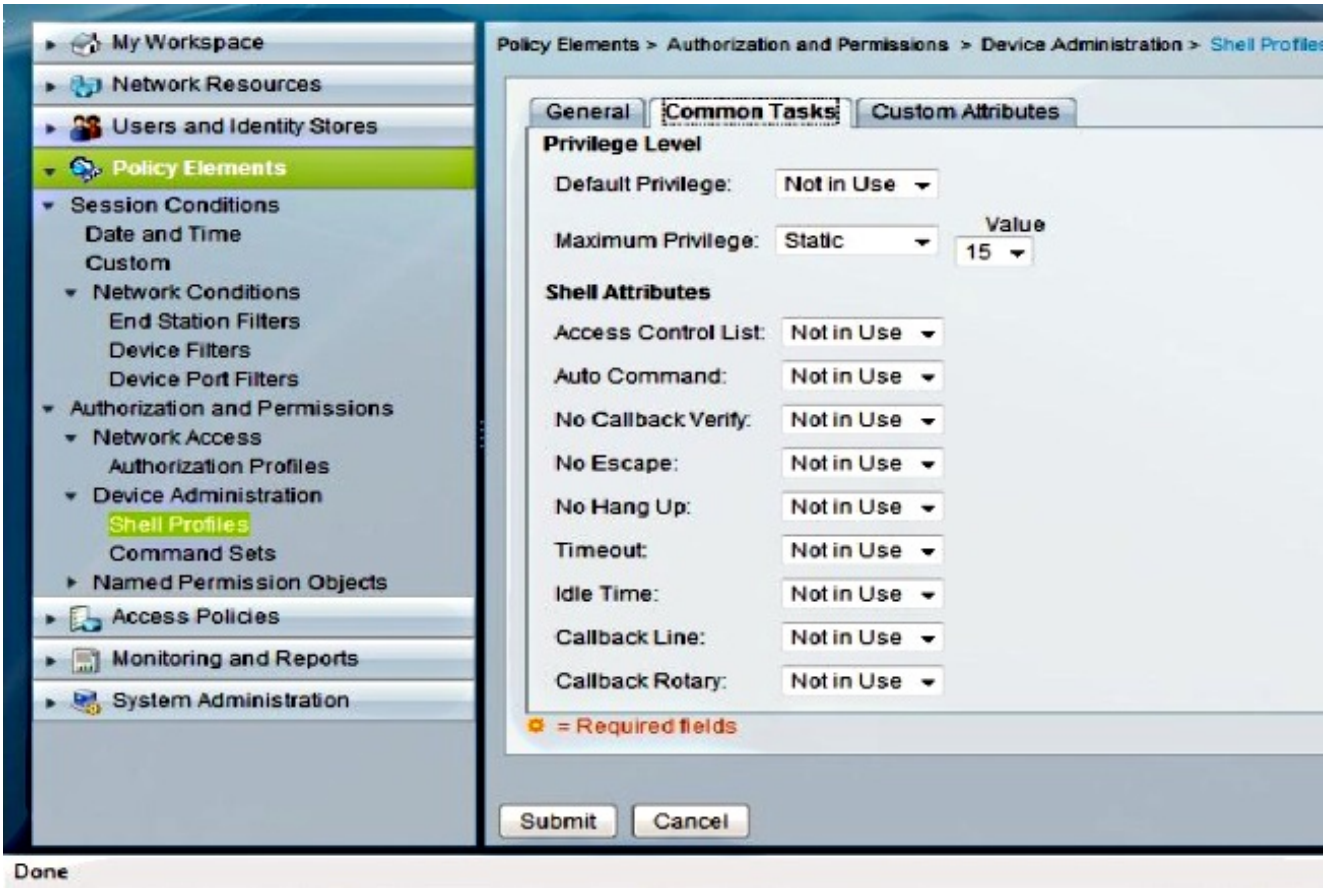
5. Введите эти команды для настройки TACACS + на линиях VTY:
```
Router(config)#line vty 0 4
Router(config-line)#login authentication mtac
```

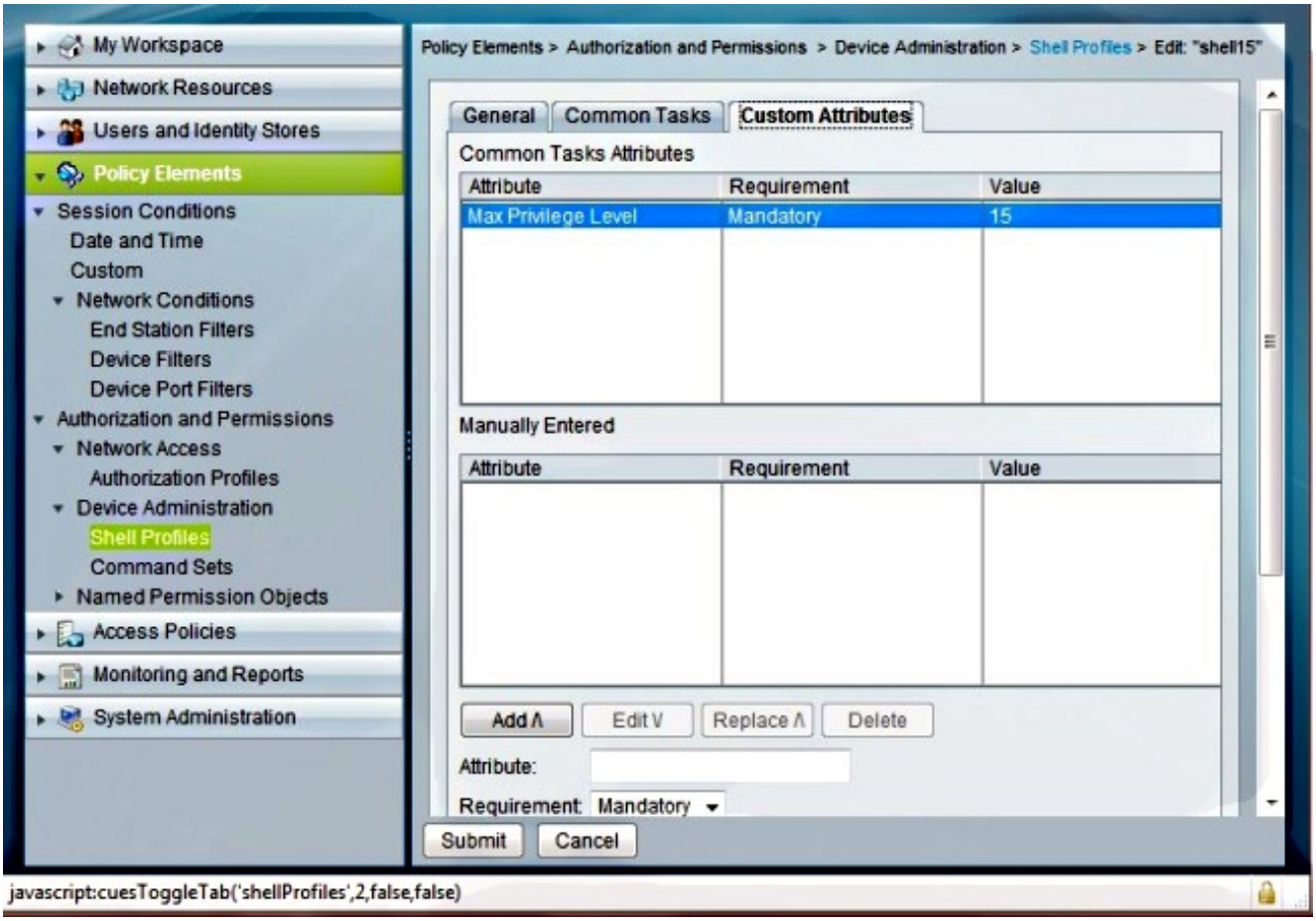
Конфигурация на ACS

1. Создайте пользователя в ACS. Перейдите **Пользователям, и Идентификационные Хранилища> Создают Пользователя**. Данный пример использует **тестового пользователя Петерэдмина**.

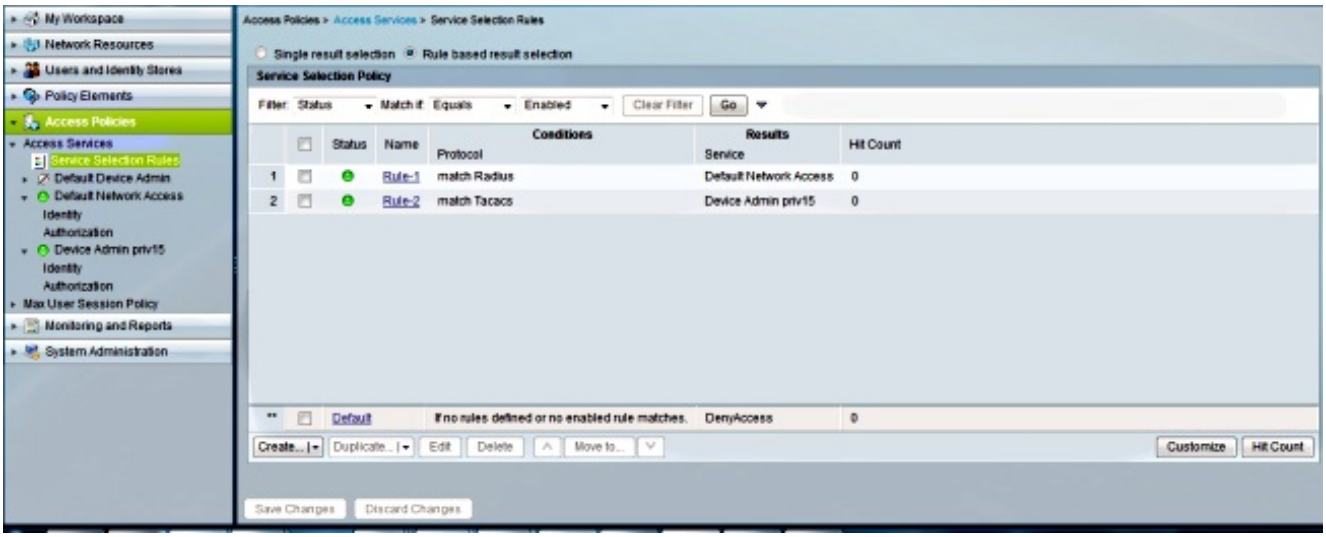


2. TACACS + пользователям с правами администратора нужен профиль оболочки, который позволяет им уровень привилегий **15** так, чтобы они могли войти **в привилегированный режим**. Для настройки профиля оболочки перейдите к **Элементам Политики> Авторизация и Разрешения> Администрирование устройств> Профили Shell**.

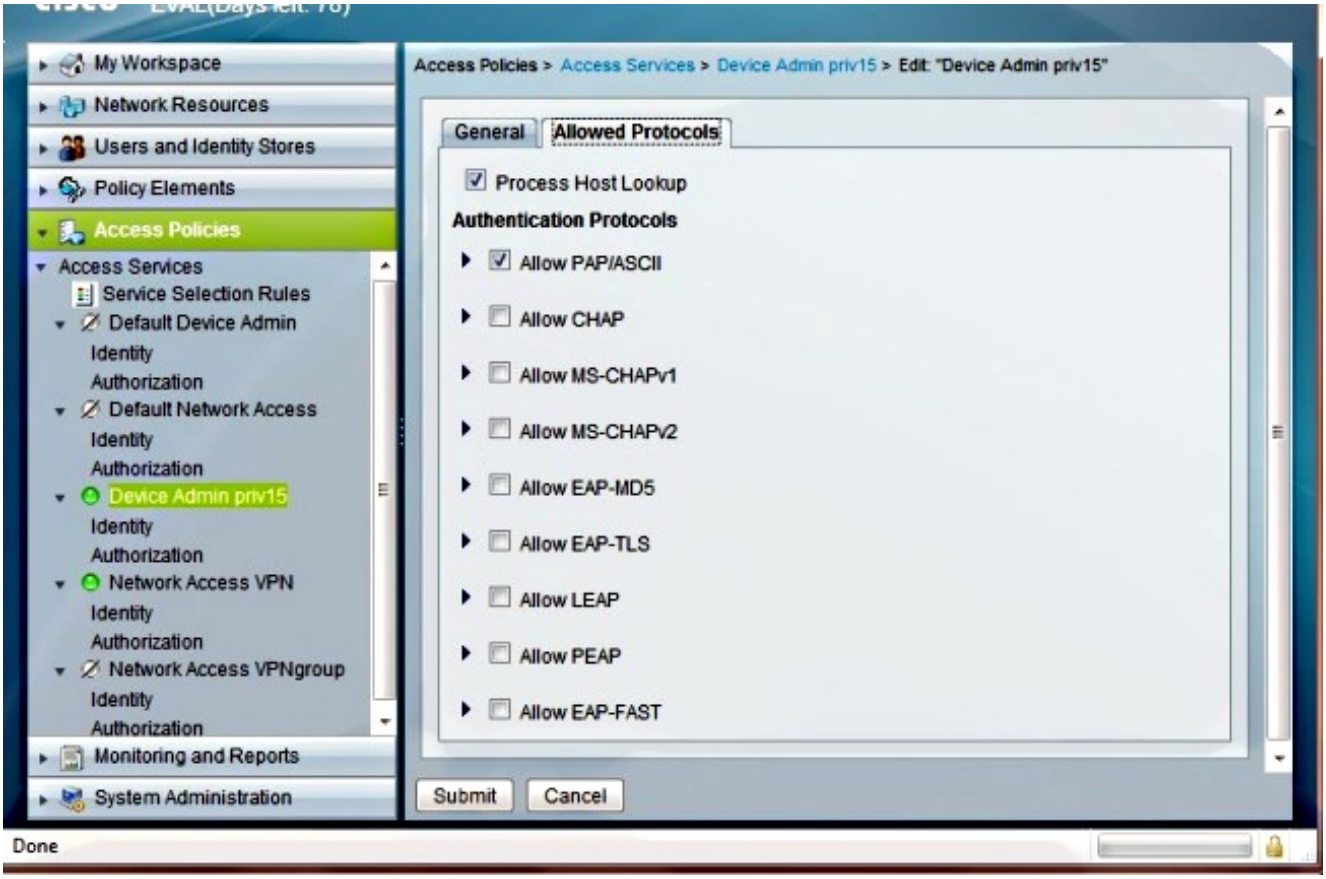




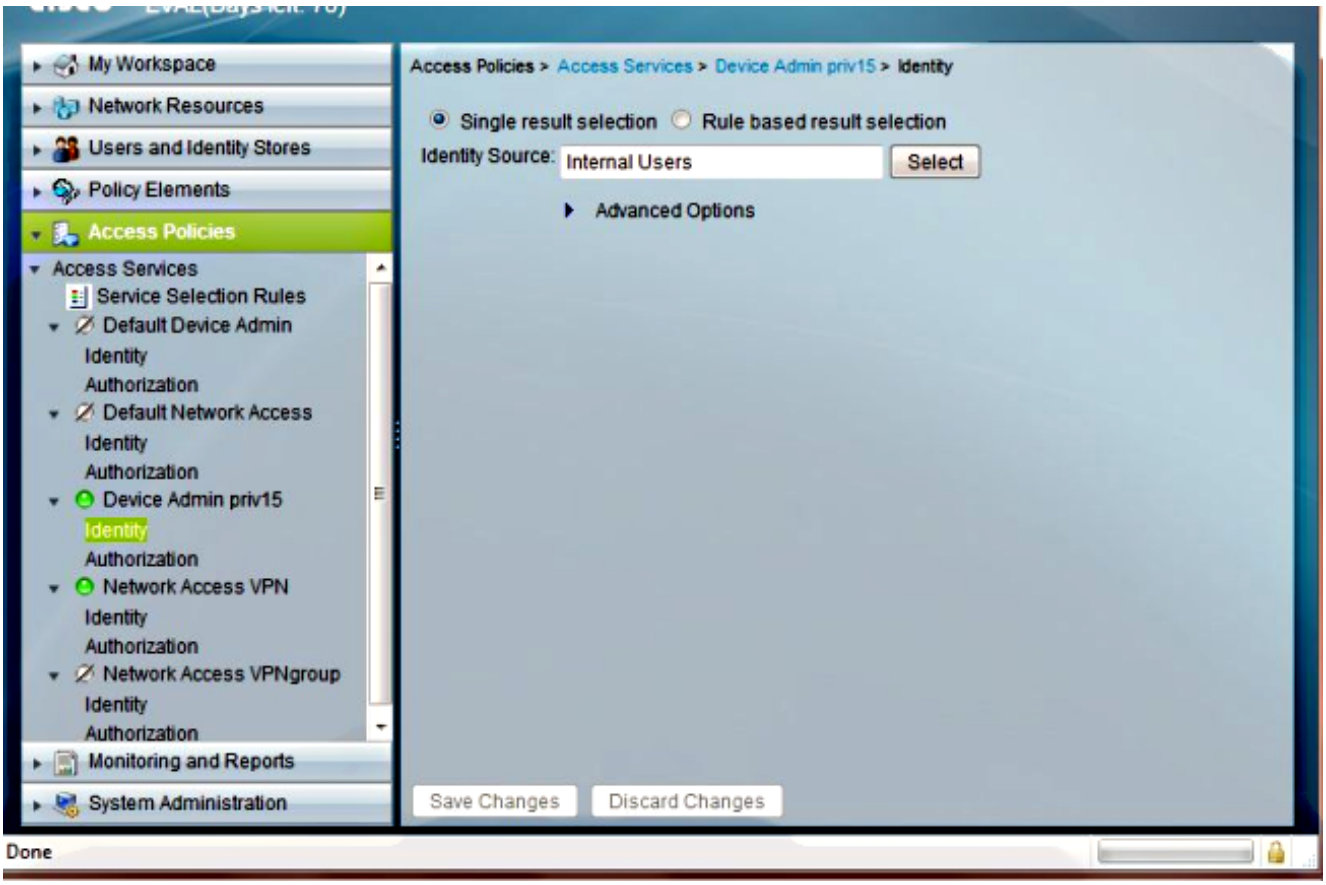
3. Создайте Сервисное Правило выбора под **Политикой доступа> Службы доступа** для соответствия с TACACS:



4. Перейдите к **устройству Admin priv15>, Разрешенные протоколы> Выбирают Authentication Protocols** и настраивают **Разрешенные протоколы**. Данный пример использует **PAP/ASCII**.

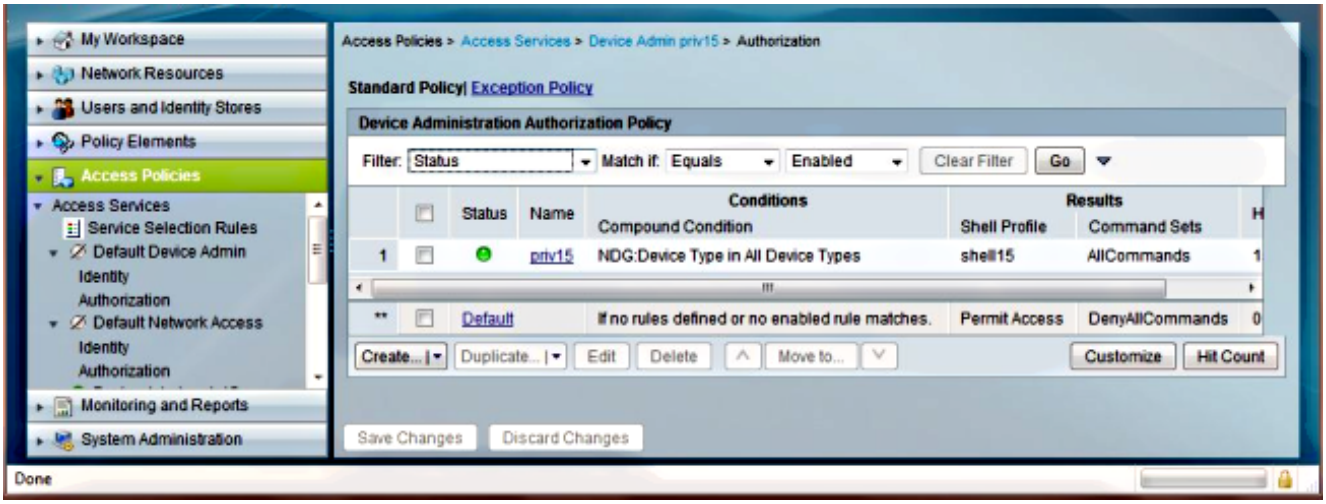


5. Перейдите к **Политике доступа> Службы доступа> устройство Admin priv15> Идентичность** и настройте Идентификационный Источник для **Внутренних пользователей**.



6. Настройте Политику авторизации под **Политикой доступа> Службы доступа>**

устройство Admin priv15> Авторизация.



Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Тестовый доступ Telnet

Эти отладки используются для проверки проверки подлинности и авторизация, кэширующейся для TACACS +:

- события debug tacacs
- debug aaa cache group

Telnet к маршрутизатору с ПОЛЬЗОВАТЕЛЕМ TACACS и enable password TACACS:

```
username: peteradmin
password: peteradmin

R102>en
password: cpeter
R102#

R102#debug tacacs events
R102#debug aaa cache group
R102#
11:35:47.151: TPLUS: Queuing AAA Authentication request 16 for processing
11:35:47.159: TPLUS: processing authentication start request id 16
11:35:47.163: TPLUS: Authentication start packet created for 16()
11:35:47.167: TPLUS: Using server 192.168.159.41
11:35:47.187: TPLUS(00000010)/0/NB_WAIT/69540BEC: Started 4 sec timeout
11:35:47.223: TPLUS(00000010)/0/NB_WAIT: wrote entire 37 bytes request
11:35:47.227: TPLUS: Would block while reading pak header
11:35:47.251: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 16
bytes)
11:35:47.255: TPLUS(00000010)/0/READ: read entire 28 bytes response
11:35:47.255: TPLUS(00000010)/0/69540BEC: Processing the reply packet
11:35:47.259: TPLUS: Received authen response status GET_USER (7)
11:35:47.263: AAA/AUTHEN/CACHE: No username in response
11:35:56.703: TPLUS: Queuing AAA Authentication request 16 for processing
```

```
11:35:56.711: TPLUS: processing authentication continue request id 1611:35:56.715:
TPLUS: Authentication continue packet generated for 16
11:35:56.719: TPLUS(00000010)/0/WRITE/69540BEC: Started 4 sec timeout
11:35:56.727: TPLUS(00000010)/0/WRITE: wrote entire 27 bytes request
11:35:56.751: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 16
bytes)
11:35:56.751: TPLUS(00000010)/0/READ: read entire 28 bytes response
11:35:56.755: TPLUS(00000010)/0/69540BEC: Processing the reply packet
11:35:56.759: TPLUS: Received authen response status GET_PASSWORD (8)
11:35:56.763: AAA/AUTHEN/CACHE: Request status = 8, cannot add to cache
11:36:02.943: TPLUS: Queuing AAA Authentication request 16 for processing
11:36:02.955: TPLUS: processing authentication continue request id 16
11:36:02.959: TPLUS: Authentication continue packet generated for 16
11:36:02.963: TPLUS(00000010)/0/WRITE/69540BEC: Started 4 sec timeout
11:36:02.967: TPLUS(00000010)/0/WRITE: wrote entire 27 bytes request
11:36:03.971: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 6
bytes)
11:36:03.975: TPLUS(00000010)/0/READ: read entire 18 bytes response
11:36:03.975: TPLUS(00000010)/0/69540BEC: Processing the reply packet
11:36:03.979: TPLUS: Received authen response status PASS (2)
11:36:03.983: AAA/AUTHEN/CACHE: SG profile admin
11:36:03.987: AAA/AUTHEN/CACHE: SG block for admin found
11:36:03.987: AAA/AUTHEN/CACHE: matching profile found for peteradmin in admin
11:36:03.991: AAA/AUTHEN/CACHE: Dealing with authen_type = 1
11:36:03.995: TPLUS: Error occurs in reading packet header, shutdown the single
connection
11:36:04.047: TPLUS: Queuing AAA Authorization request 16 for processing
11:36:04.055: TPLUS: processing authorization request id 16
11:36:04.059: TPLUS: Protocol set to None .....Skipping
11:36:04.063: TPLUS: Sending AV service=shell
11:36:04.067: TPLUS: Sending AV cmd*
11:36:04.067: TPLUS: Authorization request created for 16(peteradmin)
11:36:04.071: TPLUS: using previously set server 192.168.159.41 from group
admin-tac
11:36:04.091: TPLUS(00000010)/0/NB_WAIT/689C0FDC: Started 4 sec timeout
11:36:04.127: TPLUS(00000010)/0/NB_WAIT: wrote entire 66 bytes request
11:36:04.131: TPLUS: Would block while reading pak header
11:36:05.319: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 6
bytes)
11:36:05.323: TPLUS(00000010)/0/READ: read entire 18 bytes response
11:36:05.327: TPLUS(00000010)/0/689C0FDC: Processing the reply packet
11:36:05.327: TPLUS: received authorization response for 16: PASS
11:36:05.335: AAA/AUTHEN/CACHE: SG profile admin
11:36:05.335: AAA/AUTHEN/CACHE: SG block for admin found
11:36:05.339: AAA/AUTHEN/CACHE: matching profile found for peteradmin in admin
11:36:05.339: AAA/AUTHOR/CACHE(00000010): Existing entry no set for authorization
11:36:05.347: TPLUS: Error occurs in reading packet header, shutdown the single
connection
11:36:05.419: TPLUS: Queuing AAA Accounting request 16 for processing
11:36:05.431: TPLUS: processing accounting request id 16
11:36:05.439: TPLUS: Sending AV task_id=6
11:36:05.439: TPLUS: Sending AV timezone=UTC
11:36:05.443: TPLUS: Sending AV service=shell
11:36:05.443: TPLUS: Accounting request created for 16(peteradmin)
11:36:05.447: TPLUS: using previously set server 192.168.159.41 from group
admin-tac
11:36:05.471: TPLUS(00000010)/0/NB_WAIT/689C0FDC: Started 4 sec timeout
11:36:05.523: TPLUS(00000010)/0/NB_WAIT: wrote entire 85 bytes request
11:36:05.523: TPLUS: Would block while reading pak header
11:36:05.587: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 5
bytes)
11:36:05.591: TPLUS(00000010)/0/READ: read entire 17 bytes response
11:36:05.591: TPLUS(00000010)/0/689C0FDC: Processing the reply packet
11:36:05.595: TPLUS: Received accounting response with status PASS
```

```
11:36:05.603: TPLUS: Error occurs in reading packet header, shutdown the single
connection
R102#
```

Проверьте кэш

Введите эти команды, чтобы рассмотреть и очистить данные кэша:

- **show aaa cache group [имя группы кэша] все**
- **clear aaa cache group [имя группы кэша] все**

```
R102#show aaa cache group admin-tac all
-----------------------------------------------------------
Entries in Profile dB admin-tac for exact match
-----------------------------------------------------------
Profile: peteradmin
Updated: 00:00:42
Parse User: N
Authen User: Y
Query Count: 2
6731AF7C 0 00000009 username(422) 10 peteradmin, service shell, protocol none
6731AF8C 0 0000000A cmd(73) 0 , service shell, protocol none
-----------------------------------------------------------
Entries in Profile dB admin-tac for regexp match
-----------------------------------------------------------
No entries found for regexp match
```

Моделируйте сбой ACS

Разъедините сервер ACS от сети, чтобы моделировать сбой и вызвать проверку кэша.

Telnet к маршрутизатору с ПОЛЬЗОВАТЕЛЕМ TACACS и локальным enable password (enable password от TACACS не может кэшироваться):

```
username: peteradmin
password: peteradmin

R102>en
password:
R102#
11:39:10.723: TPLUS: Queuing AAA Authentication request 17 for processing
11:39:10.735: TPLUS: processing authentication start request id 17
11:39:10.739: TPLUS: Authentication start packet created for 17()
11:39:10.743: TPLUS: Using server 192.168.159.41
11:39:10.759: TPLUS(00000011)/0/NB_WAIT/68A4A820: Started 4 sec timeout
11:39:14.759: TPLUS(00000011)/0/NB_WAIT/68A4A820: timed out
11:39:14.763: TPLUS(00000011)/0/NB_WAIT/68A4A820: timed out, clean up
11:39:14.767: TPLUS(00000011)/0/68A4A820: Processing the reply packet
11:39:14.771: AAA/AUTHEN/CACHE: Don't cache responses with errors
11:39:14.779: AAA/AUTHEN/CACHE(00000011): GET_USER for username NULL
11:39:23.315: AAA/AUTHEN/CACHE(00000011): GET_PASSWORD for username peteradmin
11:39:25.191: AAA/AUTHEN/CACHE(00000011): Found a match
11:39:25.195: AAA/AUTHEN/CACHE(00000011): PASS for username peteradmin
11:39:25.215: TPLUS: Queuing AAA Authorization request 17 for processing
11:39:25.223: TPLUS: processing authorization request id 17
11:39:25.227: TPLUS: Protocol set to None .....Skipping
11:39:25.231: TPLUS: Sending AV service=shell
11:39:25.235: TPLUS: Sending AV cmd*
11:39:25.239: TPLUS: Authorization request created for 17(peteradmin)
```

```
11:39:25.239: TPLUS: Using server 192.168.159.41
11:39:25.243: TPLUS(00000011)/0/IDLE/689C3A0C: got immediate connect on new 0
11:39:25.247: TPLUS(00000011)/0/WRITE/689C3A0C: Started 4 sec timeout
11:39:25.251: TPLUS(00000011)/0/WRITE: write to 192.168.159.41 failed with errno
257((ENOTCONN))
11:39:25.255: TPLUS: Protocol set to None .....Skipping
11:39:25.259: TPLUS: Sending AV service=shell
11:39:25.259: TPLUS: Sending AV cmd*
11:39:25.263: TPLUS: Authorization request created for 17(peteradmin)
11:39:25.263: TPLUS(00000011): Start write failed
11:39:29.247: TPLUS(00000011)/0/WRITE/689C3A0C: timed out
11:39:29.251: TPLUS: Protocol set to None .....Skipping
11:39:29.255: TPLUS: Sending AV service=shell
11:39:29.255: TPLUS: Sending AV cmd*
11:39:29.259: TPLUS: Authorization request created for 17(peteradmin)
11:39:29.263: TPLUS(00000011)/0/WRITE/689C3A0C: timed out, clean up
11:39:29.267: TPLUS: Error occured while writing, shutdown the single
connection
11:39:29.267: TPLUS(00000011)/0/689C3A0C: Processing the reply packet
11:39:29.271: AAA/AUTHEN/CACHE: Don't cache responses with errors
11:39:29.331: TPLUS: Queuing AAA Accounting request 17 for processing
11:39:29.343: TPLUS: processing accounting request id 17
11:39:29.351: TPLUS: Sending AV task_id=7
11:39:29.351: TPLUS: Sending AV timezone=UTC
11:39:29.355: TPLUS: Sending AV service=shell
11:39:29.359: TPLUS: Accounting request created for 17(peteradmin)
11:39:29.359: TPLUS: using previously set server 192.168.159.41 from group
admin-tac
11:39:29.379: TPLUS(00000011)/0/NB_WAIT/689C0FDC: Started 4 sec timeout
11:39:33.375: TPLUS(00000011)/0/NB_WAIT/689C0FDC: timed out
11:39:33.379: TPLUS: Choosing next server 192.168.159.41
11:39:33.383: TPLUS(00000011)/689C0FDC: releasing old socket 0
11:39:33.387: TPLUS(00000011)/0/NB_WAIT/689C0FDC: got immediate connect on
new 0
11:39:33.387: TPLUS(00000011)/0/WRITE/689C0FDC: Started 4 sec timeout
11:39:33.391: TPLUS(00000011)/0/WRITE: write to 192.168.159.41 failed with errno
257((ENOTCONN))
11:39:33.399: TPLUS: Sending AV task_id=7
11:39:33.399: TPLUS: Sending AV timezone=UTC
11:39:33.403: TPLUS: Sending AV service=shell
11:39:33.403: TPLUS: Accounting request created for 17(peteradmin)
11:39:33.407: TPLUS(00000011)/0/WRITE/689C0FDC: Write failed, this request
will be cleaned up after timeout
11:39:37.387: TPLUS(00000011)/0/WRITE/689C0FDC: timed out
11:39:37.395: TPLUS: Sending AV task_id=7
11:39:37.395: TPLUS: Sending AV timezone=UTC
11:39:37.399: TPLUS: Sending AV service=shell
11:39:37.403: TPLUS: Accounting request created for 17(peteradmin)
11:39:37.407: TPLUS: Choosing next server 192.168.159.41
11:39:37.407: TPLUS(00000011)/689C0FDC: releasing old socket 0
11:39:37.411: TPLUS(00000011)/0/WRITE/689C0FDC: got immediate connect on
new 0
11:39:37.415: TPLUS(00000011)/0/WRITE/689C0FDC: Started 4 sec timeout
11:39:37.415: TPLUS(00000011)/0/WRITE: write to 192.168.159.41 failed with errno
257((ENOTCONN))
11:39:37.423: TPLUS: Sending AV task_id=7
11:39:37.427: TPLUS: Sending AV timezone=UTC
11:39:37.427: TPLUS: Sending AV service=shell
11:39:37.431: TPLUS: Accounting request created for 17(peteradmin)
11:39:37.431: TPLUS(00000011)/0/WRITE/689C0FDC: Write failed, this request
will be cleaned up after timeout
11:39:41.411: TPLUS(00000011)/0/WRITE/689C0FDC: timed out
11:39:41.419: TPLUS: Sending AV task_id=7
11:39:41.423: TPLUS: Sending AV timezone=UTC
```

```
11:39:41.423: TPLUS: Sending AV service=shell
11:39:41.427: TPLUS: Accounting request created for 17(peteradmin)
11:39:41.431: TPLUS(00000011)/0/WRITE/689C0FDC: timed out, clean up
11:39:41.431: TPLUS: Error occured while writing, shutdown the single
connection
11:39:41.435: TPLUS(00000011)/0/689C0FDC: Processing the reply packet

Cached username and password works.

R102#clear aaa cache group admin-tac all
R102#show aaa cache group admin-tac all
-----------------------------------------------------------
Entries in Profile dB admin-tac for exact match
-----------------------------------------------------------
No entries found in Profile dB
```

Устранение неполадок

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Для этой конфигурации в настоящее время нет сведений об устранении проблем.