TACACS + и атрибуты RADIUS для различной Cisco и примера конфигурации устройств не марки CISCO

Содержание

Введение

Этот документ предоставляет компиляцию атрибутов, которые различная Cisco и продукты не-Cisco ожидают получать от аутентификации, авторизации и учета (AAA); в этом случае AAA-сервером является Access Control Server (ACS). ACS может возвратить эти атрибуты наряду с Access-Accept как часть профиля оболочки (TACACS +) или профиля авторизации (RADIUS).

Этот документ предоставляет пошаговые инструкции о том, как добавить настраиваемые атрибуты для окружения профилей авторизации и профилей. Этот документ также содержит список устройств и TACACS + и атрибуты RADIUS, которые устройства ожидают видеть, возвратился из AAA-сервера. Все темы включают примеры.

Список атрибутов, предоставленных в этом документе, не является исчерпывающим или авторитетным и может измениться в любое время без обновления этого документа.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Версии ACS 5.2/5.3.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Создайте профиль Shell (TACACS +)

Профиль оболочки является основным контейнером разрешений для TACACS, +-based обращаются. Можно задать, какой TACACS + атрибуты и значения атрибута должны быть возвращены с Access-Accept, в дополнение к уровню привилегий Cisco® IOS, превышению времени ожидания сеанса и другим параметрам.

Выполните эти шаги для добавления настраиваемых атрибутов к новому профилю оболочки:

1. Войдите к интерфейсу ACS.
2. Перейдите к **Элементам Политики> Авторизация и Разрешения> Администрирование устройств> Профили Shell**.
3. Нажмите кнопку **Create**.
4. Назовите профиль оболочки.
5. Нажмите вкладку **Custom Attributes**.
6. Введите название атрибута в поле **Attribute**.
7. Выберите, является ли требование **Обязательным** или **Дополнительным** от выпадающего списка Требования.
8. Оставьте выпадающее для набора значения атрибута к **Статическому**. Если значение статично, можно ввести значение в следующее поле. Если значение является динамичным, вы не можете ввести атрибут вручную; вместо этого приписанный сопоставлен с атрибутом в одном из идентификационных хранилищ.
9. Введите значение атрибута в последнем поле.
10. Нажмите **кнопку Add** для добавления записи в таблицу.
11. Повторитесь для настройки всех атрибутов, в которых вы нуждаетесь.
12. **Нажмите кнопку «Submit» (Отправить) внизу экрана.**

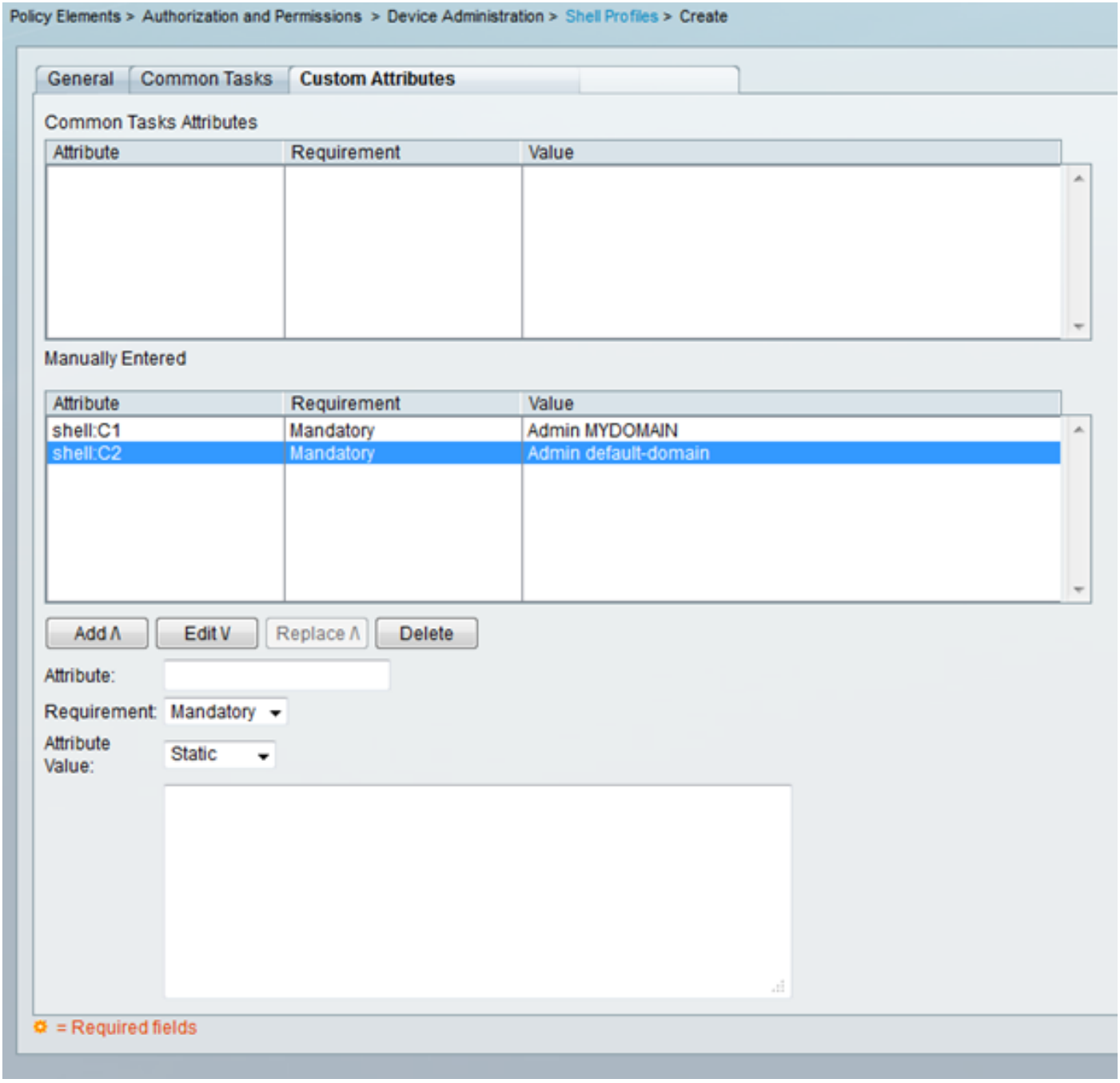
Пример конфигурации

Устройство: Ядро управления приложениями (ACE)

Атрибут `shell:<context-name>`

Значение (значения): `<Role-name> <domain-name1>`

Использование: роль и домен разделены пробелом. Можно настроить пользователя (например, USER1), чтобы быть назначенными роль (например, ADMIN) и домен (например, MYDOMAIN) когда входы пользователя в систему в к контексту (например, C1).



Создайте профиль авторизации (RADIUS)

Профиль авторизации является основным контейнером разрешений для основанного на RADIUS доступа. Можно задать, какие атрибуты RADIUS и значения атрибута должны быть возвращены с Access-Accept, в дополнение к VLAN, Списки контроля доступа (ACL) и другие параметры.

Выполните эти шаги для добавления настраиваемых атрибутов к новому профилю авторизации:

1. Войдите к интерфейсу ACS.
2. Перейдите к **Элементам Политики> Авторизация и Разрешения> Доступ к сети> Профили Авторизации**.
3. Нажмите кнопку **Create**.
4. Назовите профиль авторизации.
5. Нажмите вкладку **атрибутов RADIUS**.
6. Выберите словарь от раскрывающегося меню **Типа словаря**.
7. Для установки выбора атрибут для поля атрибута RADIUS нажмите кнопку **Select**. Новое окно появляется.
8. Рассмотрите доступные атрибуты, сделайте ваш выбор и нажмите **OK**. Значение **Типа атрибута** установлено по умолчанию, на основе выбора атрибута, который вы просто сделали.
9. Оставьте выпадающее для набора значения атрибута к **Статическому**. Если значение статично, можно ввести значение в следующее поле. Если значение является динамичным, вы не можете ввести атрибут вручную; вместо этого приписанный сопоставлен с атрибутом в одном из идентификационных хранилищ.
10. Введите значение атрибута в последнем поле.
11. Нажмите **кнопку Add** для добавления записи в таблицу.
12. Повторитесь для настройки всех атрибутов, в которых вы нуждаетесь.
13. **Нажмите кнопку «Submit» (Отправить) внизу экрана.**

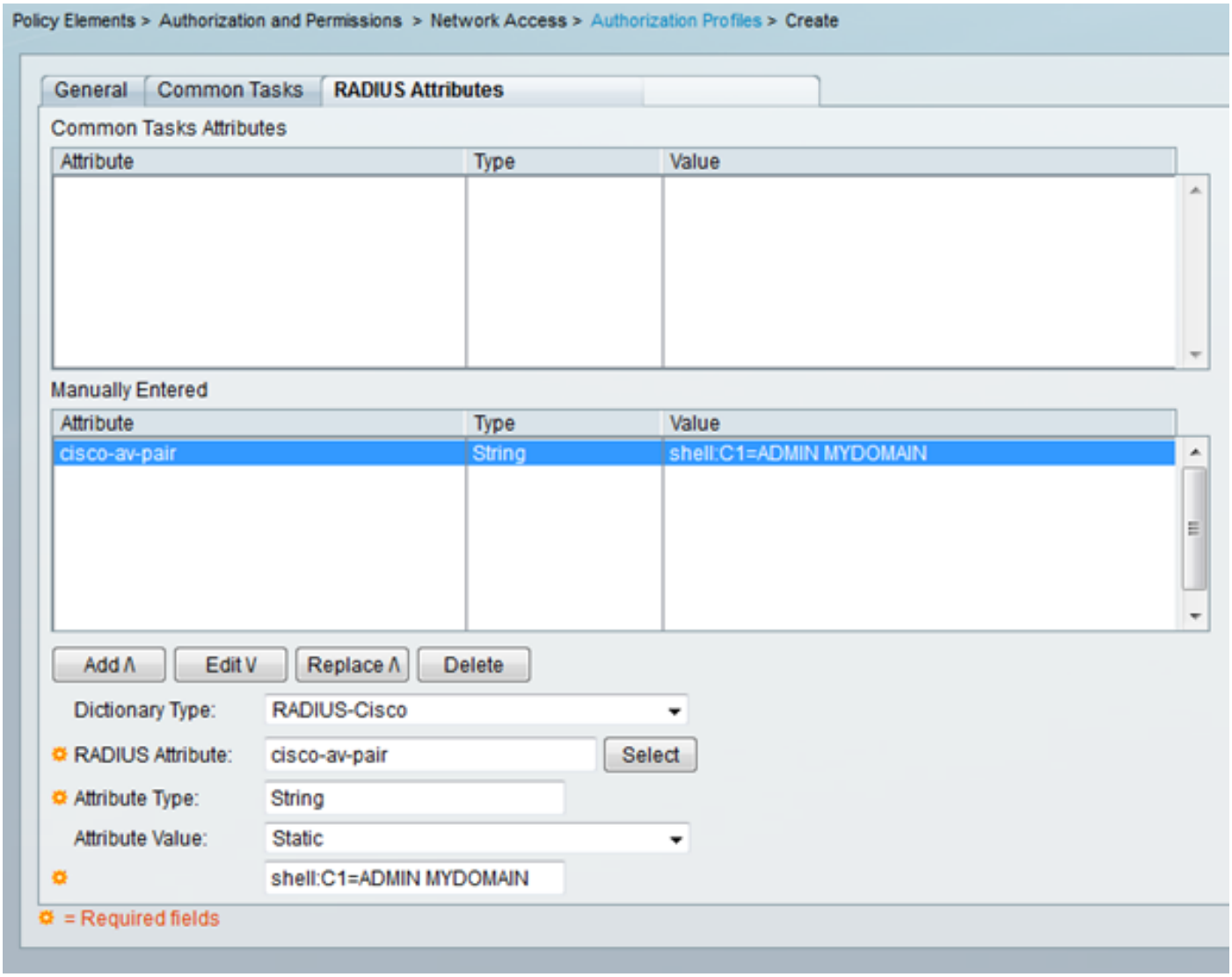
Пример конфигурации

Устройство: ACE

Атрибут `cisco-av-pair`

Значение (значения): `shell:<context-name>=<Role-name> <domain-name1> <domain-name2>`

Использование: Каждое значение после равного сигнала разделено пробелом. Можно настроить пользователя (например, USER1), чтобы быть назначенными роль (например, ADMIN) и домен (например, MYDOMAIN) когда входы пользователя в систему в к контексту (например, C1).



Список устройств

Маршрутизаторы агрегации (ASR)

RADIUS (профиль авторизации)

Атрибут `cisco-av-pair`

Значение (значения): `shell:tasks="#<role-name>,<permission>:<process>"`

Использование: Установите значения `of <role-name> to` название роли, локально определенной на маршрутизаторе. Иерархия роли может быть описана с точки зрения дерева, где role `#root` наверху дерева, и role `#leaf` добавляет дополнительные команды. Эти две роли могут объединяться и пасоваться назад если: `shell:tasks="#root,#leaf"`.

Разрешения могут также пасоваться назад на основе отдельного процесса, так, чтобы пользователю можно было предоставить чтение, запишите и выполните привилегии для определенных процессов. Например, для предоставления пользовательского чтения и привилегий записи для процесса BGP, установите значение в: `shell:tasks="#root,rw:bgp"`. Заказ атрибутов не имеет значения; результатом является то же, установлено ли значение в `shell:tasks="#root,rw:bgp"` или го `shell:tasks="rw:bgp,#root"`.

Пример – *добавляет атрибут к профилю авторизации*

Тип словаря	Атрибут RADIUS	Тип атрибута	Значение атрибута
Cisco RADIUS	`cisco-av-pair`	Строка	`shell:tasks="#root,#leaf,rwx:bgp,r:ospf"`

Ядро управления приложениями (ACE)

TACACS + (профиль Shell)

Атрибут `shell:<context-name>`

Значение (значения): `<Role-name> <domain-name1>`

Использование: роль и домен разделены пробелом. Можно настроить пользователя (например, USER1), чтобы быть назначенными роль (например, ADMIN) и домен (например, MYDOMAIN) когда входы пользователя в систему в к контексту (например, C1).

Пример – *добавляет атрибут к профилю Shell*

Атрибут	Требование	Значение атрибута
`shell:C1`	Обязательный	`Admin MYDOMAIN`

Если USER1 входит через контекст C1, тому пользователю автоматически назначают роль ADMIN и домен MYDOMAIN (при условии, что правило авторизации было настроено, где, как только USER1 входит, им назначают этот профиль авторизации).

Если USER1 входит через другой контекст, который не возвращен в значении атрибута, который передает обратно ACS, тому пользователю автоматически назначают роль по умолчанию (Сетевой монитор) и домен по умолчанию (домен по умолчанию).

RADIUS (профиль авторизации)

Атрибут `cisco-av-pair`

Значение (значения): `shell:<context-name>=<Role-name> <domain-name1> <domain-name2>`

Использование: Каждое значение после равного сигнала разделено пробелом. Можно настроить пользователя (например, USER1), чтобы быть назначенными роль (например, ADMIN) и домен (например, MYDOMAIN) когда входы пользователя в систему в контекст (например, C1).

Пример – *добавляет атрибут к профилю авторизации*

Тип словаря	Атрибут RADIUS	Тип атрибута	Значение атрибута
Cisco RADIUS	`cisco-av-pair`	Строка	`shell:C1=ADMIN MYDOMAIN`

Если USER1 входит через контекст C1, тому пользователю автоматически назначают роль ADMIN и домен MYDOMAIN (при условии, что правило авторизации было настроено, где, как только USER1 входит, им назначают этот профиль авторизации).

Если USER1 входит через другой контекст, который не возвращен в значении атрибута, который передает обратно ACS, тому пользователю автоматически назначают роль по умолчанию (Сетевой монитор) и домен по умолчанию (домен по умолчанию).

Пакетный формирователь BlueCoat

RADIUS (профиль авторизации)

Атрибут `Packeteer-AVPair`

Значение (значения): `access=<level>`

Использование: `<level>` является уровнем доступа к предоставлению. В то время как доступ взгляда эквивалентен только для чтения, сенсорный доступ эквивалентен чтению-записи.

BlueCoat VSA не существует в словарях ACS по умолчанию. Для использования атрибута BlueCoat в профиле авторизации необходимо создать словарь BlueCoat и добавить, что BlueCoat приписывает тому словарю.

Создайте словарь:

1. Перейдите к **Администрированию системы> Конфигурация> Словари> Протоколы> RADIUS > VSA RADIUS**.
2. **Нажмите кнопку Create.**
3. Введите подробные данные словаря:Name: BlueCoatИденификатор поставщика: 2334Префикс атрибута: Packeteer-
4. **Нажмите кнопку Submit (Отправить).**

Создайте атрибут в новом словаре:

1. Перейдите к **Администрированию системы> Конфигурация> Словари> Протоколы> RADIU S> VSA RADIUS> BlueCoat**.
2. **Нажмите кнопку Create.**
3. Введите подробные данные атрибута:Атрибут: `Packeteer-AVPair`Описание: Используемый для определения уровня доступаID атрибута поставщика: 1Направление: ИСХОДЯЩИЙМножественный позволенный: FALSEВключайте атрибут в журнал: ПроверенныйТип атрибута: строка
4. **Нажмите кнопку Submit (Отправить).**

Пример – ***Добавляет Атрибут к Профилю Авторизации (для доступа только на чтение)***

Тип словаря	Атрибут RADIUS	Тип атрибута	Значение атрибута
Солдат RADIUS	`Packeteer-AVPair`	Строка	`access=look`

Пример – ***Добавляет Атрибут к Профилю Авторизации (для доступа для чтения-записи)***

Тип словаря	Атрибут RADIUS	Тип атрибута	Значение атрибута

Солдат RADIUS	`Packeteer-AVPair`	Строка	`access=touch`

Коммутаторы Brocade

RADIUS (профиль авторизации)

Атрибут `Tunnel-Private-Group-ID`

Значение (значения): `U:<VLAN1>`; `T:<VLAN2>`

Использование: Установите `<VLAN1>` в значение VLAN для передачи данных. Установите `<VLAN2>` в значение голосового VLAN. В данном примере VLAN для передачи данных является VLAN 10, и голосовой VLAN является VLAN 21.

Пример – ***добавляет атрибут к профилю авторизации***

Тип словаря	Атрибут RADIUS	Тип атрибута	Значение атрибута
IETF RADIUS	`Tunnel-Private-Group-ID`	Тэговая строка	`U:10;T:21`

Cisco Unity Express (CUE)

RADIUS (профиль авторизации)

Атрибут `cisco-av-pair`

Значение (значения): `fndn:groups=<group-name>`

Использование: `<group-name>` является названием группы с привилегиями, что вы хотите предоставить пользователю. Эта группа должна быть настроена на Cisco Unity Express (CUE).

Пример – ***добавляет атрибут к профилю авторизации***

Тип словаря	Атрибут RADIUS	Тип атрибута	Значение атрибута
Cisco RADIUS	`cisco-av-pair`	Строка	`fndn:groups=Administrators`

Infoblox

RADIUS (профиль авторизации)

Атрибут `Infoblox-Group-Info`

Значение (значения): `<group-name>`

Использование: `<group-name>` является названием группы с привилегиями, что вы хотите

предоставить пользователю. Эта группа должна быть настроена на устройстве Infoblox. В этом примере конфигурации именем группы является MyGroup.

VSA Infoblox не существует в словарях ACS по умолчанию. Для использования атрибута Infoblox в профиле авторизации необходимо создать словарь Infoblox и добавить, что Infoblox приписывает тому словарю.

Создайте словарь:

1. Перейдите к **Администрированию системы> Конфигурация> Словари> Протоколы> RADIU S> VSA RADIUS**.
2. **Нажмите кнопку Create.**
3. Нажмите маленькую стрелку затем для **Использования Усовершенствованных Параметров поставщика**.
4. Введите подробные данные словаря:Name: InfobloxИденификатор поставщика: 7779Размер длины поля поставщика: 1Размер поля типа поставщика: 1
5. **Нажмите кнопку Submit (Отправить).**

Создайте атрибут в новом словаре:

1. Перейдите к **Администрированию системы> Конфигурация> Словари> Протоколы> RADIU S> VSA RADIUS> Infoblox**.
2. **Нажмите кнопку Create.**
3. Введите подробные данные атрибута:Атрибут: `Infoblox-Group-Info`ID атрибута поставщика: 009Направление: ИСХОДЯЩИЙМножественный позволенный: FALSEВключайте атрибут в журнал: ПроверенныйТип атрибута: строка
4. **Нажмите кнопку Submit (Отправить).**

Пример – ***добавляет атрибут к профилю авторизации***

Тип словаря	**Атрибут RADIUS**	**Тип атрибута**	**Значение атрибута**
RADIUS-Infoblox	`Infoblox-Group-Info`	Строка	`MyGroup`

Система предотвращения вторжений (IPS)

RADIUS (профиль авторизации)

Атрибут `ips-role`

Значение (значения): `<role name>`

Использование: значение `<role name>` может быть любой из четырех ролей пользователя Системы предотвращения вторжений (IPS): средство просмотра, оператор, администратор или сервис. См. руководство по конфигурации для вашей версии IPS для подробных данных разрешений, данных к каждому типу роли пользователя.

- Менеджер устройств системы предотвращения вторжений Cisco (IPS) руководство по конфигурации для IPS 7.0
- Менеджер устройств системы предотвращения вторжений Cisco (IPS) руководство по

конфигурации для IPS 7.1

Пример – *добавляет атрибут к профилю авторизации*

Тип словаря	Атрибут RADIUS	Тип атрибута	Значение атрибута
Cisco RADIUS	`cisco-av-pair`	Строка	`ips-role:administrator`

Juniper

TACACS + (профиль Shell)

Атрибут `allow-commands`; `allow-configuration`; `local-user-name`; `deny-commands`; `deny-configuration`; `user-permissions`

Значение (значения): `<allow-commands-regex>`; `<allow-configuration-regex>`; `<local-username>`; `<deny-commands-regex>`; `<deny-configuration-regex>`

Использование: Установите значение `<local-username>` (т.е. значение атрибута имени локального пользователя) к имени пользователя, которое существует локально на устройстве Juniper. Например, можно настроить пользователя (например, USER1), чтобы быть назначенными тот же шаблон пользователя как пользователь (например, JUSER), который существует локально на устройстве Juniper, когда вы устанавливаете значение атрибута имени локального пользователя к JUSER. Значения позволять-команд, позволять-конфигурации, запрещать-команд и запрещать-атрибутов-конфигурации могут быть введены в формат regex. Значения, в которые установлены эти атрибуты, в дополнение к в рабочем состоянии командам / командам режима конфигурации, авторизовавшим битами полномочий класса входа в систему пользователя.

Пример – *добавляет, что атрибуты к Shell представляют 1*

Атрибут	Требование	Значение атрибута
`allow-commands`	Дополнительно	`"(request system) | (show rip neighbor)"`
`allow-configuration`	Дополнительно	
`local-user-name`	Дополнительно	`sales`
`deny-commands`	Дополнительно	`"<^clear"`
`deny-configuration`	Дополнительно	

Пример – *добавляет, что атрибуты к Shell представляют 2*

Атрибут	Требование	Значение атрибута
`allow-commands`	Дополнительно	`"monitor | help | show | ping | traceroute"`
`allow-configuration`	Дополнительно	
`local-user-name`	Дополнительно	`engineering`
`deny-commands`	Дополнительно	`"configure"`

deny-configuration	Дополнительно	

Коммутаторы Nexus

RADIUS (профиль авторизации)

Атрибут `cisco-av-pair`

Значение (значения): `shell:roles="<role1> <role2>"`

Использование: Установите значения `<role1>` и `<role2>` к названиям ролей, локально определенных на коммутаторе. Когда вы добавляете множественные роли, разделяете их пробелом. Когда множественные роли пасуются назад от AAA-сервера до коммутатора Nexus, результат состоит в том, что у пользователя есть доступ к командам, определенным объединением всех трех ролей.

Встроенные роли определены в Учетных записях пользователя Настройки и RBAC.

Пример – ***добавляет атрибут к профилю авторизации***

Тип словаря	Атрибут RADIUS	Тип атрибута	Значение атрибута
Cisco RADIUS	cisco-av-pair	Строка	shell:roles="network-admin vdc-admin vdc-operator"

Riverbed

TACACS + (профиль Shell)

Атрибут `service`; `local-user-name`

Значение (значения): `rbt-exec`; `<username>`

Использование: для предоставления пользовательского доступа только на чтение значение `<username>` должно собираться контролировать. Для предоставления пользовательского доступа для чтения-записи значение `<username>` должно быть установлено в admin. Если вы имеете другую учетную запись, определенную в дополнение к admin и монитору, настраиваете то название, которое будет возвращено.

Пример – ***Добавляет Атрибуты к Профилю Shell (для доступа только на чтение)***

Атрибут	Требование	Значение атрибута
service	Обязательный	rbt-exec
local-user-name	Обязательный	monitor

Пример – ***Добавляет Атрибуты к Профилю Shell (для доступа для чтения-записи)***

Атрибут	Требование	Значение атрибута
service	Обязательный	rbt-exec

`local-user-name`	Обязательный	`admin`

Контроллер беспроводной локальной сети (WLC)

RADIUS (профиль авторизации)

Атрибут `Service-Type`

Значение (значения): `Administrative (6)` / `NAS-Prompt (7)`

Использование: для предоставления пользовательского доступа для чтения-записи к Контроллеру беспроводной локальной сети (WLC) значение должно быть Административным; для доступа только на чтение значение должно быть Приглашением NAS.

Для получения дополнительной информации посмотрите аутентификацию сервера RADIUS Пользовательских интерфейсов управления на Примере конфигурации Контроллера беспроводной локальной сети (WLC)

Пример – ***Добавляет Атрибут к Профилю Авторизации (для доступа только на чтение)***

Тип словаря	Атрибут RADIUS	Тип атрибута	Значение атрибута
IETF RADIUS	`Service-Type`	Перечисление	`NAS-Prompt`

Пример – ***Добавляет Атрибут к Профилю Авторизации (для доступа для чтения-записи)***

Тип словаря	Атрибут RADIUS	Тип атрибута	Значение атрибута
IETF RADIUS	`Service-Type`	Перечисление	`Administrative`

Data Center Network Manager (DCNM)

DCNM должен быть перезапущен после того, как метод аутентификации изменен. В противном случае это может назначить привилегию оператора сети вместо сетевого admin.

Роль DCNM	Cisco-av-pair RADIUS	Cisco-av-pair tacacs
User	`shell:roles = "network-operator"`	`cisco-av-pair=shell:roles="network-operator"`
Администратор	`shell:roles = "network-admin"`	`cisco-av-pair=shell:roles="network-admin"`

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация
- Terminal Access Controller Access Control System (TACACS+)
- Служба удаленной аутентификации пользователей коммутируемого доступа (RADIUS)

- Запросы комментариев (RFC)