Nexus N5500, 5600 и Управление доступом ядра роли (RBAC) N6000

Содержание

Введение

Этот документ описывает, как ограничить пользователя для доступа к Nexus 5500, Nexus 5600 и коммутаторам Nexus 6000 с помощью Управления доступом ядра роли (RBAC).

RBAC позволяет вам определять правила для роли назначенного пользователя для ограничения авторизации пользователя, который имеет доступ к операциям управления коммутатором.

Можно создать и управлять учетной записью пользователя и назначить роли, которые ограничивают доступ к Nexus 5500, Nexus 5600 и коммутаторам Nexus 6000.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Nexus 5500, Nexus 5600, Nexus 6000 переключает команды конфигурации интерфейса командой строки
- Cisco Fabric Services (CFS).

Используемые компоненты

Сведения в этом документе основываются на Nexus 5500, Nexus 5600 и коммутаторах

Nexus 6000 рабочий NXOS 5.2 (1) N1 (9) 7.3 (1) N1 (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.

Требования пользователя

Это некоторые требования пользователя, которые являются потребностью, которая будет выполнена:

- Только пользователи с ролью сетевого admin могут создать роли.
- Только пользователи с ролью сетевого admin могут просмотреть выходные данные **show role**.
- Даже если пользователям разрешают выполнить все команды показа, им не разрешают просмотреть **выходные данные show role**, пока этим пользователям не назначают роль сетевого admin.
- Учетная запись пользователя должна иметь по крайней мере одну роль пользователя.

Роли пользователя

Каждая роль может быть назначена на несколько пользователей, и каждый пользователь может быть частью множественных ролей.

Например, роль пользователям разрешают выполнить команды показа, и роль B пользователи позволены изменить конфигурацию.

Если пользователя назначают и на роль A и на Роль B, этот пользователь может выполнить команду показа и внести изменения в конфигурацию.

Команда доступа разрешения принимает приоритет, запрещают команду доступа.

Например, если вы принадлежите роли, которая запрещает доступ к командам настройки.

Однако, если вы также принадлежите роли, которая имеет доступ к командам настройки, у вас тогда есть доступ к командам настройки.

Существует пять ролей пользователя по умолчанию:

- сетевой администратор- Завершенный доступ с правом чтения и записи к целостному коммутатору.
- оператор сети - Завершенный доступ для чтения к целостному коммутатору.
- vdc-admin - Доступ с правом чтения и записи, ограниченный VDC
- оператор vdc - Доступ для чтения, ограниченный VDC
- san-admin - Завершенный доступ с правом чтения и записи SAN администраторам.

Примечание: Вы не можете модифицировать/удалять роли пользователя по умолчанию.

Примечание: команда show role отобразит роль, доступную на коммутаторе

Правила роли пользователя

Правило является основным элементом роли.

Правило определяет, какие операции роль позволяет пользователю выполнять.

Можно применить правила для этих параметров:

- Команда - команда или группа команд определены в регулярном выражении.
- Функция - Команды, которые применяются к функции, предоставленной программным обеспечением NX-OS.
- Телефонная группа - или определяемая пользователем группа По умолчанию функций.

Эти параметры создают иерархические отношения. Самый основной параметр управления является командой.

Следующий параметр управления является функцией, которая представляет все команды, привязанные к функции.

Последний параметр управления является телефонной группой. Телефонная группа сочетает отнесенные функции и позволяет вам легко управлять правилами.

Заданный пользователями номер правила определяет заказ, в котором применены правила.

Правила применены в порядке убывания.

Например, правило 1 применено перед правилом 2, которое применено перед правилом 3 и так далее.

Команда правила задает операции, которые могут быть выполнены определенной ролью. Каждое правило состоит из номера правила, тип правила (permit or deny),

тип команды (например, конфигурация, показывают, exec, отладка), и название дополнительной функции (например, FCOE, HSRP, VTP, интерфейс).

Распределение роли пользователя

Основанные на роли конфигурации используют инфраструктуру Cisco Fabric Services (CFS), чтобы включить эффективное управление базой данных и предоставить одиночную точку конфигурации в сети.

При включении распределения CFS для функции на устройстве устройство принадлежит CFS region, содержащему другие устройства в сети, которую вы также включили для распределения CFS для функции. Распределение CFS для функции роли пользователя отключено по умолчанию.

Необходимо включить CFS для ролей пользователя на каждом устройстве, которому вы

хотите распределить изменения конфигурации.

После включения распределения CFS для ролей пользователя на коммутаторе первая команда настройки роли пользователя, которую вы вводите, заставляет программное обеспечение NX-OS коммутатора принимать эти меры:

1. Создает сеанс CFS на коммутаторе.
2. Блокирует конфигурацию роли пользователя на всех коммутаторах в CFS region с CFS, включенным для функции роли пользователя.
3. Сохраняет изменения конфигурации роли пользователя во временном буфере на коммутаторе.

Изменения остаются во временном буфере на коммутаторе, пока вы явно не передаете их, чтобы быть распределенными устройствам в CFS region.

При фиксации изменений программное обеспечение NX-OS принимает эти меры:

1. Применяет изменения к рабочей конфигурации на коммутаторе.
2. Распределяет обновленную конфигурацию роли пользователя другим коммутаторам в CFS region.
3. Разблокировал конфигурацию роли пользователя в устройствах в CFS region.
4. Завершает сеанс CFS.

Эти конфигурации распределены:

- Имена ролей и описания
- Список правил для ролей

Команды configuration и show

	Команда	Цель
Шаг 1.	**configure terminal** Пример: **switch#configure terminal** коммутатор (config) #	Вход в режим глобальной конфигурации.
Шаг 2.	*имя роли* **имени роли** Пример: коммутатор (config) # **имя роли Усера** коммутатор (роль config) #	Задает роль пользователя и вводит режим конфигурации роли.
Шаг 3.	**vlan policy deny** Пример: коммутатор (роль config) # **vlan policy deny**	Вводит режим конфигурации политики виртуальной локальной сети роли.

	коммутатор (vlan роли config) # *vlan-id* **permit vlan**	
Шаг 4. .	Пример: коммутатор (vlan роли config) # **permit vlan 1**	Задает vlan, к которому может обратиться роль. Повторите эту команду для как многие vlans по мере необходимости.
	exit	
Шаг 5. .	Пример: коммутатор (vlan роли config) # **выход**	Выходной режим конфигурации политики виртуальной локальной сети роли.
	коммутатор (роль config) # **show role**	
Шаг 6.	Пример: коммутатор (роль config) # **show role show role {ожидающий | diff в состоянии ожидания}**	(Необязательно) Показы конфигурация роли.
Шаг 7.	Пример: коммутатор (роль config) # **show role pending**	(Необязательно) Показы конфигурация роли пользователя, ожидающая для распределения
	role commit	Если вы включили распределение конфигурации CFS для функции роли пользователя, (Необязательно) Применяет изменения конфигурации роли пользователя во временной базе данных к рабочей конфигурации и распределяет конфигурацию роли пользователя другим коммутаторам.
Шаг 8.	Пример: коммутатор (роль config) # **role commit**	
	copy running-config startup-config	
Шаг 9.	Пример: **switch#copy running-config startup-config**	(Необязательно) Копии рабочая конфигурация к загрузочной конфигурации.

Эти шаги включают распределение конфигурации роли:

	Команда	Цель
Шаг 1.	**config t** switch# коммутатор (config) #	Вводит режим конфигурации.
Шаг 2.	коммутатор (config) # **role distribute**	Включает распределение конфигурации роли.
	коммутатор (config) **#no role distribute**	Отключает распределение конфигурации роли (по умолчанию).

Эти шаги передают изменения конфигурации роли:

	Команда	Цель
Шаг 1	**Config t** Nexus# Nexus (config) #	Вводит режим конфигурации.
Шаг 2	Nexus (config) # **role commit**	Передает изменения конфигурации роли.

Эти шаги сбрасывают от изменений конфигурации роли:

	Команда	Цель
Шаг 1	**Config t** Nexus# Nexus (config) #	Вводит режим конфигурации.
Шаг 2	Nexus (config) # **role abort**	Сбрасывает от изменений конфигурации роли и очищает базу данных конфигурации ожидания.

Для отображения учетной записи пользователя и сведений о конфигурации RBAC выполните одну из этих задач:

Команда	Цель
show role	Отображает конфигурацию роли пользователя.
show role feature	Отображает список функций.
show role feature-group	Отображает конфигурацию телефонной группы.

Очистите сеанс распределения роли пользователя

Можно очистить продолжающийся сеанс распределения Cisco Fabric Services (если таковые имеются) и разблокировать матрицу для функции роли пользователя.

> **Внимание. :** Любые изменения в базе данных в состоянии ожидания будут потеряны при выдаче этой команды.

	Команда	Цель
Шаг 1	switch# **очищают сеанс роли** **Пример:** switch# очищают сеанс роли	Очищает сеанс и разблокировал матрицу.
Шаг 2	**статус show role session** **Пример:** статус show role session switch#	(Необязательно) Показы статус сеанса CFS роли пользовате

Пример конфигурации

В данном примере мы переходим, создают TAC учетной записи пользователя с ними разрешение доступа:

- Доступ к команде clear
- Доступ к команде настройки
- Доступ к команде отладки
- Доступ к команде exec
- Доступ к команде показа

- Доступ к vlan 1-10 только

```
C5548P-1# config t
Enter configuration commands, one per line. End with CNTL/Z
C5548P-1(config)# role name Cisco
C5548P-1(config-role)# rule 1 permit command clear
C5548P-1(config-role)# rule 2 permit command config
C5548P-1(config-role)# rule 3 permit command debug
C5548P-1(config-role)# rule 4 permit command exec
C5548P-1(config-role)# rule 5 permit command show
C5548P-1(config-role)# vlan policy deny
C5548P-1(config-role-vlan)# permit vlan 1-10
C5548P-1(config-role-vlan)# end C5548P-1# show role name Cisco

Role: Cisco
 Description: new role
 vsan policy: permit (default)
 Vlan policy: deny
 Permitted vlans: 1-10
 Interface policy: permit (default)
 Vrf policy: permit (default)
 ----------------------------------------------------------------
 Rule   Perm   Type       Scope              Entity
 ----------------------------------------------------------------
 5      permit command                        show
 4      permit command                        exec
 3      permit command                        debug
 2      permit command                        config
 1      permit command                        clear


C5548P-1#
C5548P-1# config t
Enter configuration commands, one per line. End with CNTL/Z.
C5548P-1(config)# username TAC password Cisco123 role Cisco

C5548P-1(config)# show user-account TAC
user:TAC
       this user account has no expiry date
       roles:Cisco
```

Требования при лицензировании

Продукт	Лицензионное требование
NX-OS	Учетные записи пользователя и RBAC не требуют никакой лицензии.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

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