Ip admission ISR и LDAP для веб-Перенаправления к веб-Примеру Конфигурации безопасности ScanSafe/Облака

Содержание

Введение

Этот документ описывает, как настроить Маршрутизаторы ISR Cisco G2 Series (ISR). В то время как конфигурация IP Admission и Протокола LDAP может использоваться просто для аутентификации прокси-сервера на ISR, это, как правило, используется в сочетании с функцией перенаправления Облачной веб-безопасности (CWS) Cisco. Также, этот документ предназначен, чтобы быть ссылкой для добавления документации конфигурации и устранения проблем перенаправления CWS относительно ISR.

Предварительные условия

Требования

Cisco рекомендует, чтобы ваша система удовлетворила эти требования перед попыткой конфигураций, которые описаны в этом документе:

- ISR должен выполнить версию кода 15.2 (1) T1 или позже.
- Ваша система должна иметь образы с набором характеристики безопасности (SEC) лицензия, которые доступны в (универсальном) Cisco IOS®.
- Клиентская рабочая станция на домене Active Directory (AD) должна иметь возможность выполнить активную аутентификацию через web-браузер.
- У вас должна быть подписка CWS.

Используемые компоненты

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

- Internet Explorer, Google Chrome, Mozilla Firefox (требует дополнительной настройки для прозрачного LAN Manager NT (NTLM) аутентификация),
- Cisco G2 800, 1900, 2900 и ISR серии 3900.

- Контроллер домена AD Microsoft Windows (ADDC)

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.

> **Примечание:** Cisco G1 1800, 2800 и маршрутизаторы серии 3800 не поддерживаются.

Общие сведения

Много администраторов, которые устанавливают ISR Cisco G2 Series, которые не имеют устройств адаптивной защиты Cisco (ASA) в их сетях, принимают решение использовать CWS ISR (раньше ScanSafe) функциональность перенаправления для использования преимуществ решения для CWS для веб-фильтрации. Как часть того решения, большинство администраторов также хочет использовать текущую AD инфраструктуру для передачи информации об идентичности пользователя к башням CWS в целях пользователя - или основанная на группе принудительная политика для веб-политики фильтрации в портале CWS.

Общее понятие подобно интеграции между ASA и Агентом каталога контекста (CDA) с несколькими различиями. Большая часть примечательного различия - то, что ISR фактически не поддерживает пассивного пользователя к IP, сопоставляющего базу данных, таким образом, пользователи должны пройти через некоторый тип аутентификации, чтобы передать транзитом ISR и передать пользователю или информации о группе к порталу CWS.

> **Совет:** См. раздел **Методов аутентификации** этого документа для получения дополнительной информации о различиях между различными методами аутентификации, которые доступны.

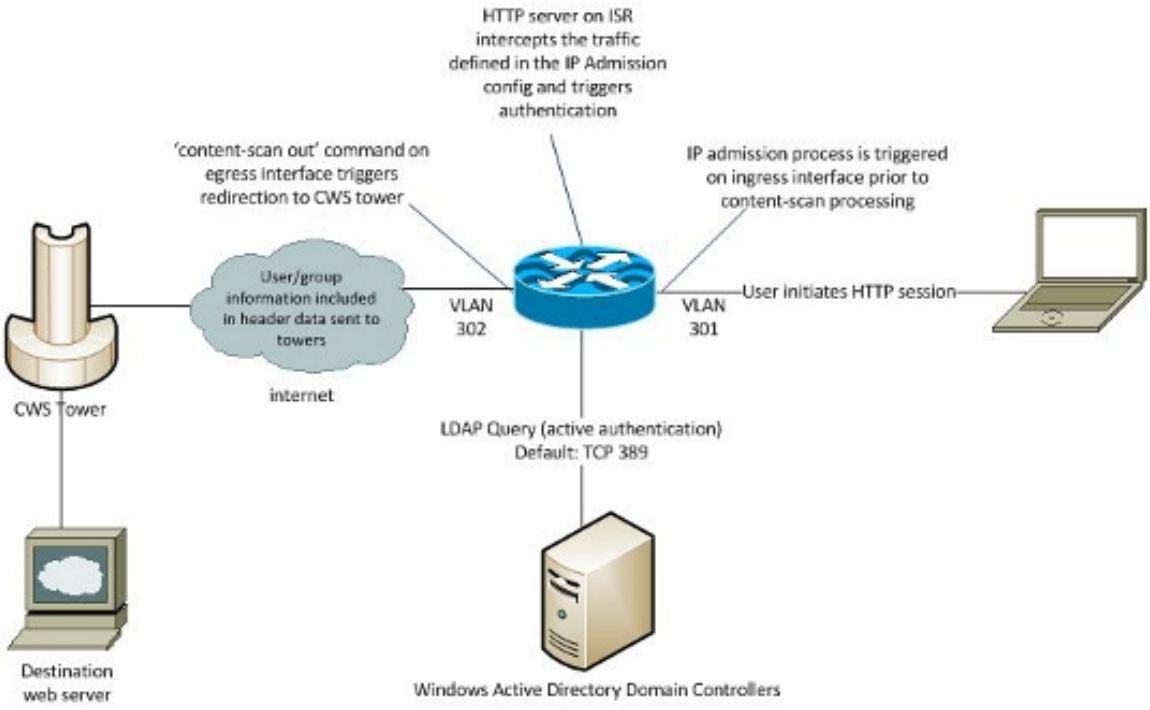
В то время как часть перенаправления CWS конфигурации, которая описана в этом документе, является относительно прямой, некоторые администраторы могли бы встретиться с трудностью с попытками настроить опознавательную часть. Эта часть работает с **командой ip admission**, которая ссылается на Серверы LDAP и объявления проверки подлинности Аутентификации, авторизации и учета (AAA), которые должны также быть настроены. Цель этого документа состоит в том, чтобы предоставить операторам сети источник полного справочника, чтобы настроить или устранить неполадки Ip admission и частей LDAP этой конфигурации на ISR Cisco G2 Series.

Настройка

Используйте информацию, которая описана в этом разделе для настройки ISR Cisco.

> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети



Настройте LDAP

Выполните эти шаги для настройки свойств LDAP AAA-сервера (AAA-серверов):

1. Настройте Карту атрибутов LDAP для принуждения имени пользователя, которое введено пользователем для соответствия **с sAMAccountName** свойством в AD:
   ```
   C-881(config)#ldap attribute-map ldap-username-map map type sAMAccountName
    username
   C-881(config-attr-map)#map type sAMAccountName username
   ```
   Примечание: Эта конфигурация требуется, потому что атрибут **sAMAccountName** является уникальным значением в AD, в отличие от атрибута Общего имени (CN), который иначе используется для соответствия по умолчанию. Например, могут быть множественные случаи *Джона Смита* в AD, но может только быть один пользователь с **sAMAccountName** *jsmith*, который является также входом в систему учетной записи пользователя. Другие учетные записи *Джона Смита* имеют **sAMAccountNames**, такой как *jsmith1* или *jsmith2*.
   Команда **атрибутов show ldap** может также использоваться для просмотра списка атрибутов LDAP и связанных атрибутов AAA.

2. Настройте группу Сервера LDAP:
   ```
   C-881(config)#aaa group server ldap LDAP_GROUP
   C-881(config-ldap-sg)#server DC01
   ```
3. Настройте Серверы LDAP:
   ```
   C-881(config)#ldap server DC01
   C-881(config-ldap-server)# ipv4 10.10.10.150
   C-881(config-ldap-server)#attribute map ldap-username-map
   C-881(config-ldap-server)# bind authenticate root-dn CN=Csco_Service,CN=Users,
   DC=lab,DC=cisco,DC=com password Cisco12345!

   C-881(config-ldap-server)#base-dn DC=lab,DC=cisco,DC=com
   ```

```
C-881(config-ldap-server)#search-filter user-object-type top
C-881(config-ldap-server)#authentication bind-first
```

Эта конфигурация обычно не требует модификации, пока нет потребность внедрить пользовательский поисковый фильтр. Только администраторы, которые являются сведущими в LDAP и знают, как должным образом ввести эту информацию, должны использовать пользовательские поисковые фильтры. Если вы не уверены в поисковом фильтре, который должен использоваться, просто использовать описанный фильтр; это определяет местоположение пользователей в обычной AD среде.

Другой частью Конфигурации LDAP, которая также требует, чтобы особое внимание детализировало, являются Составные имена (DN), которые требуются в **командах bind-authenticate-root-dn и base-dn**. Они должны быть введены точно, поскольку они появляются в Сервере LDAP или сбое запросов LDAP. Кроме того, **команда base-dn** должна быть самой низкой частью дерева LDAP, где находятся все пользователи, которые аутентифицируются.

Рассмотрите сценарий, в котором **команда base-dn** в предыдущей конфигурации модифицируется, такие как это:

```
base-dn OU=TestCompany,DC=lab,DC=cisco,DC=com
```

В этом случае запрос для пользователей, которые включены в **Cn=Users, DC=lab, DC=cisco, DC=com**, не возвращает результатов, так как Сервер LDAP только ищет Подразделение (OU) TestCompany и дочерние объекты в нем. В результате аутентификация всегда отказывает для тех пользователей, пока они или не перемещены в TestCompany OU или его поддерево, или если **команда base-dn** изменена для включения его в запрос.

> **Совет:** См. **Определение Объектов DN в AD - ADSI Редактирует** раздел этого документа для подробных данных о том, как определить надлежащие DN для основных и корневых команд.

Настройте AAA

Теперь, когда Серверы LDAP настроены, необходимо сослаться на них в соответствующих операторах AAA, которые используются процессом IP Admission:

```
C-881(config)#aaa authentication login SCANSAFE_AUTH group LDAP_GROUP
C-881(config)#aaa authorization network SCANSAFE_AUTH group LDAP_GROUP
```

> **Примечание:** Если эти команды не доступны, то **команда aaa new-model**, возможно, должна была бы быть введена для добавления этой функциональности AAA, потому что это не включено по умолчанию.

Настройте IP Admission

Часть IP Admission инициирует процесс, который побуждает пользователя для аутентификации (или выполняет прозрачную аутентификацию), и затем выполняет запросы LDAP на основе учетных данных пользователя и AAA-серверов, которые определены в конфигурации. Если пользователи аутентифицируются успешно, информацию об идентичности пользователя тогда вытягивает процесс просмотра содержания и отсылают в башни CWS, наряду с перенаправленным потоком. Процесс IP Admission не активирован, пока ***команда ip admission name*** не введена во входной интерфейс маршрутизатора.

Поэтому эта часть конфигурации может быть внедрена без любого влияния трафика.

```
C-881(config)#ip admission virtual-ip 1.1.1.1 virtual-host ISR_PROXY
C-881(config)#ip admission name SCANSAFE_ADMISSION ntlm
C-881(config)#ip admission name SCANSAFE_ADMISSION method-list authentication
 SCANSAFE_AUTH authorization SCANSAFE_AUTH
```

Включите IP Admission

Вот конфигурация, которая используется для включения IP Admission:

> **Примечание:** Это вынуждает пользователей аутентифицироваться, который вызывает прерывание трафика, если отказывает аутентификация.

```
C-881(config)#int vlan301 (internal LAN-facing interface)
C-881(config-if)#ip admission SCANSAFE_ADMISSION
```

Освобожденные внутренние хосты от аутентификации

Некоторые администраторы могли бы желать освободить некоторые внутренние хосты от процесса проверки подлинности по различным причинам. Например, это мог бы быть нежелательный для внутренних серверов или устройств, которые не способны к аутентификации NTLM или базовой проверке подлинности, на которую будет влиять процесс Ip admission. В этих экземплярах Список контроля доступа (ACL) может быть применен к конфигурации IP Admission, чтобы препятствовать тому, чтобы определенные IP - адреса хоста или подсети инициировали IP Admission.

В то время как аутентификация все еще требуется для всех других хостов, в данном примере внутренний хост **10.10.10.150** освобожден от требования аутентификации:

```
C-881(config)#ip access-list extended NO_ADMISSION
C-881(config-ext-nacl)#deny ip host 10.10.10.150 any
C-881(config-ext-nacl)#permit ip any any
C-881(config)#ip admission name SCANSAFE_ADMISSION ntlm list NO_ADMISSION
```

Включите сервер HTTP на ISR

Требуется, что вы включаете сервер HTTP, чтобы перехватить сеансы HTTP и инициировать процесс проверки подлинности:

```
Ip http server
Ip http secure-server
```

> **Примечание:** Если перенаправление к HTTPS для аутентификации требуется, **Ip http secure-server** только необходим.

Настройте перенаправление CWS

Вот основная итоговая конфигурация для перенаправления CWS:

```
Ip http server
```

```
Ip http secure-server
```

Конфигурация полной выборки

Этот раздел предоставляет завершенные примеры конфигурации для предыдущих разделов.

LDAP

```
Ip http server
Ip http secure-server
```

AAA

```
Ip http server
Ip http secure-server
```

IP Admission

```
Ip http server
Ip http secure-server
```

Сервер HTTP

```
Ip http server
Ip http secure-server
```

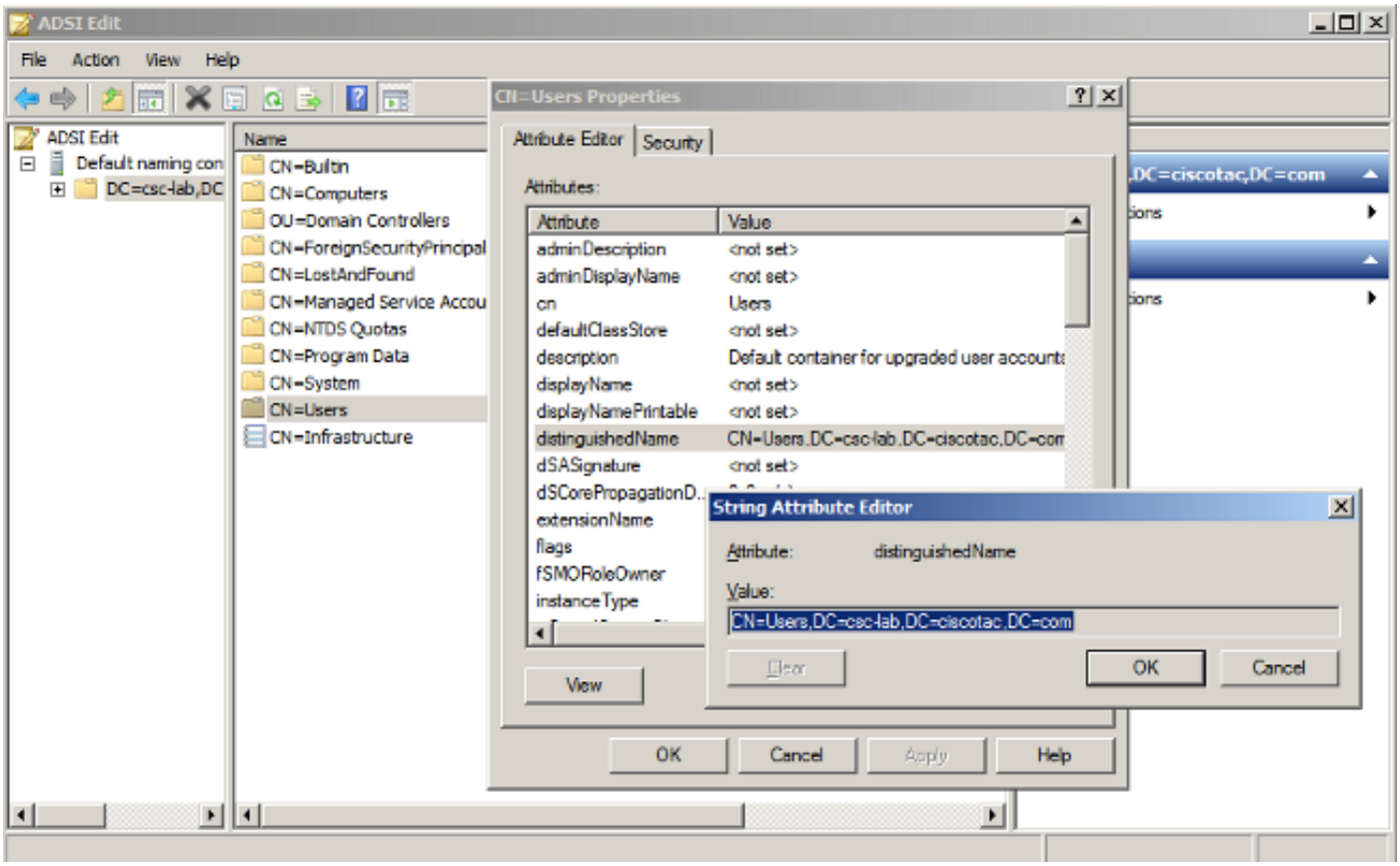
Просмотр содержания и CWS

```
Ip http server
Ip http secure-server
```

Определите объекты DN в AD - ADSI редактирует

В случае необходимости возможно просмотреть AD структуру чтобы к DN поиска для использования с пользователем или базой поиска группы. Администраторы могут использовать программное средство, названное *ADSI, Редактируют*, который встроен в AD контроллеры домена. Для открытия, ADSI Редактируют, выбирают **Start> Run** на AD контроллере домена и вводят **adsiedit.msc**.

Как только Редактирование ADSI открыто, щелкните правой кнопкой мыши любой объект, такой как OU, группа или пользователь, и выберите **Properties** для просмотра DN того объекта. Строка DN может тогда быть легко скопирована и вставлена к конфигурации маршрутизатора во избежание любых опечаток. Этот образ иллюстрирует процесс:



Методы аутентификации

Существует четыре различных типа методов аутентификации, доступных, которые используют IP Admission, и они часто неправильно понимаются, особенно различие между прозрачным и пассивным NTLM. Следующие разделы описывают различия между этими типами аутентификации.

Активный NTLM

Когда прозрачная аутентификация NTLM отказывает, активный метод аутентификации NTLM побуждает пользователей для аутентификации. Это обычно вследствие того, что клиентский браузер не поддерживает интегрированную аутентификацию Microsoft Windows или потому что пользователь вошел в рабочую станцию с локальными (недоменными) учетными данными. Активная аутентификация NTLM выполняет запросы LDAP к контроллеру домена, чтобы гарантировать, что предоставленные учетные данные корректны.

> **Примечание:** Со всеми типами аутентификации NTLM учетные данные не передают через открытый текст. Однако Версия 1 (NTLMv1) NTLM хорошо задокументировала уязвимости. ISR NTLMv2-способен, невзирая на то, что по умолчанию, более старый Windows версий Microsoft IE мог бы выполнить согласование через NTLMv1. Это поведение зависит от AD политики аутентификации.

Прозрачный NTLM

Прозрачная аутентификация NTLM происходит, когда пользователь зарегистрирован в рабочую станцию с доменными учетными данными, и те учетные данные передает прозрачно браузер к маршрутизатору IOS. Маршрутизатор IOS тогда выполняет запрос LDAP для проверки учетных данных пользователя. Это обычно - самая желаемая форма проверки подлинности для этой функции.

Базовая проверка подлинности (через HTTP в открытом тексте)

Когда аутентификация NTLM отказывает или не возможна для клиентов, таких как Macintosh, основанные на Linux устройства или мобильные устройства, эта форма проверки подлинности, как правило, используется в качестве механизма восстановления. С этим методом, если Защищенный сервер HTTP не включен, то эти учетные данные передают через HTTP в (очень неуверенном) открытом тексте.

Пассивный NTLM

Пассивная аутентификация NTLM запрашивает учетные данные от пользователей, но фактически не аутентифицирует пользователя против контроллера домена. В то время как это может избежать связанных с LDAP проблем, где запросы отказывают против контроллера домена, он также представляет пользователей в среде к угрозе безопасности. Если прозрачная аутентификация отказывает или не возможна, то пользователям предлагают для учетных данных. Однако пользователь может ввести любые учетные данные, которые они выбирают, которые передают в башню CWS. В результате политика не могла бы быть применена соответственно.

Например, Пользователь A может использовать Firefox (который по умолчанию не позволяет прозрачный NTLM без дополнительной настройки), и введите имя пользователя Пользователя Б с любым паролем, и политика для пользователя Б применена к Пользователю A. Рискозависимость может быть смягчена, если пользователи все вынуждены использовать браузеры, которые поддерживают прозрачную аутентификацию NTLM, но в большинстве случаев, не рекомендуется использование пассивной аутентификации.

Последовательность сообщений для активной аутентификации NTLM

Вот последовательность сообщения о выполнении для активного метода аутентификации NTLM:

```
Browser --> ISR : GET / google.com
Browser <-- ISR : 302 Page moved http://1.1.1.1/login.html
Browser --> ISR : GET /login.html 1.1.1.1
Browser <-- ISR : 401 Unauthorized..Authenticate using NTLM
Browser --> ISR : GET /login.html + NTLM Type-1 msg
ISR    --> AD : LDAP Bind Request + NTLM Type-1 msg
```

ISR копирует сообщение Type1 от HTTP до LDAP, байта байтом без любого изменения данных.

```
ISR    <-- AD : LDAP Bind Response + NTLM Type-2 msg
Browser <-- ISR : 401 Unauthorized + NTLM Type-2 msg
```

Сообщение Type-2 является также скопированным байтом байтом от LDAP до HTTP. Таким

образом, в PCAP, это, кажется, происходит от **1.1.1.1**, но фактическое содержание от AD.

```
Browser --> ISR : GET /login.html + NTLM Type-3 msg
ISR    --> AD : LDAP Bind Request + NTLM Type-3 msg
ISR    <-- AD : LDAP Bind response - Success
Browser <-- ISR : 200OK + redirect to google.com
```

Когда активный NTLM настроен, ISR не вмешивается во время обмена NTLM. Однако, если пассивный NTLM настроен, то ISR генерирует свое собственное сообщение Type-2.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

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

Команды "show"

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

Можно использовать эти **команды показа** для устранения проблем конфигурации:

- **кэш show ip admission**
- **статус show ip admission**
- **статистика show ip admission**
- **сервер show ldap все**

Команды "debug"

> **Примечание:** Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Вот некоторые полезные команды отладки, которые можно использовать для устранения проблем конфигурации:

- **ldap отладки все** - Эта команда может использоваться для обнаружения причины та аутентификация сбои.
- **подробность ip admission отладки** - Эта команда очень многословна и с высокой загрузкой ЦПУ. Cisco рекомендует использовать ее только с одиночными тестовыми

клиентами, которые инициируют IP admission.

- **ip admission отладки ntlm** - Эта команда может использоваться для обнаружения причины, что инициирован процесс IP Admission.
- **ip admission отладки httpd**
- **debug ip http transaction**
- **debug aaa authorization debug aaa authentication**

Распространенные проблемы

В этом разделе описываются некоторые общие проблемы, с которыми встречаются с конфигурацией, описанной в этом документе.

IP Admission не Перехватывает Запросы HTTP

Эта проблема становится очевидной при просмотре выходных данных **команды statistics show ip admission**. Выходные данные не показывают перехват никаких запросов HTTP:

```
C-881#show ip admission statistics
Webauth HTTPd statistics:

HTTPd process 1
Intercepted HTTP requests: 0
```

Возможные решения

Существует два возможных решения к этой проблеме. Первое должно проверить, что включен **ip http server**.

Если сервер HTTP для ISR не включен, то IP Admission инициирует, но никогда фактически перехватывает сеанс HTTP. Поэтому это вызывает для аутентификации. В этой ситуации нет никаких выходных данных для команды **кэша show ip admission**, но много повторений этих линий замечены в выходных данных **подробной** команды **ip admission отладки**:

```
C-881#show ip admission statistics
Webauth HTTPd statistics:

HTTPd process 1
Intercepted HTTP requests: 0
```

Второе решение этой проблемы состоит в том, чтобы проверить, что пользовательский IP-адрес не освобожден от ACL в конфигурации IP Admission.

Пользователи получают *404 не найденная* ошибка

Эта проблема наблюдается, когда пользователи перенаправлены для аутентификации и **404 Не, Найденная** ошибка происходит в браузере.

Возможное решение

Гарантируйте, что название в **ip admission виртуальные IP 1.1.1.1 действительных хоста ISR_PROXY** может успешно решить с клиентским сервером Системы доменных имен (DNS). В этом случае клиент выполняет запрос DNS для **ISR_PROXY.lab. cisco . com** начиная с **лабораторной работы. cisco . com** является Полное доменное имя (FQDN) домена, к которому присоединяются к рабочей станции. Если запрос DNS отказывает, клиент передает запрос Локального для канала разрешения имен групповой адресации (LLMNR), придерживавшийся запросом NetBIOS, который передан к локальной подсети.

. если все эти попытки разрешения сбой, в браузере, то **404, Не Найденные** или **Internet Explorer, не Могут Отобразить** ошибку **веб-страницы** отображены

Сбои проверки подлинности пользователя, когда предложено

Это может быть вызвано различными причинами, но обычно относится к Конфигурации LDAP на ISR или связи между ISR и Сервером LDAP. На ISR обычно наблюдается признак, когда пользователи застревают в **Состоянии инициализации**, как только инициирован IP Admission:

```
C-881(config)#do show ip admi cac
Authentication Proxy Cache
Client Name N/A, Client IP 10.10.10.152, Port 56674, timeout 60,
 Time Remaining 2, state INIT
```

Распространенные причины

Это типичные причины для этой проблемы:

- Неверное имя пользователя и/или пароль введены пользователем для активной аутентификации.
- Недопустимый **основной dn** используется в Конфигурации LDAP, которая приводит к поискам, которые не возвращают результатов.
- Недопустимое связывает опознавательного **корневого dn**, настроен для имени пользователя или пароля, которое вызывает LDAP, связывают для сбоя.
- Связь между ISR и сбоями Сервера LDAP. Проверьте, что Сервер LDAP слушает на указанном порте TCP для связи LDAP и что все межсетевые экраны между этими двумя позволяют трафик.
- Недопустимый поисковый фильтр не вызывает результатов для поиска LDAP.

LDAP устранения неполадок

Лучший способ определить причину, что опознавательные сбои должны использовать команды отладки LDAP на ISR. Следует иметь в виду, что отладки могут быть дорогими и опасными для работы ISR, если существуют избыточные выходные данные, и они могут

заставить маршрутизатор "зависать" и требовать цикла жесткой силы. Это особенно истинно для низкопроизводительных платформ.

Для устранения проблем Cisco рекомендует применить ACL к правилу IP Admission для подчинения только одиночной тестовой рабочей станции в сети к аутентификации. Таким образом, отладки могут быть включены с минимальным риском негативного воздействия к способности маршрутизатора передать трафик.

> **Совет:** См. **Освобожденные Внутренние хосты от Опознавательного** раздела этого документа для получения дополнительной информации о приложении ACL к конфигурации Ip admission.

При устренении связанных с LDAP проблем полезно понять шаги, в которых процессах LDAP запрашивает от ISR.

Высокоуровневые шаги для проверки подлинности LDAP

Вот высокоуровневые шаги для проверки подлинности LDAP:

1. Откройте соединение с Сервером LDAP на указанном порте. Порт по умолчанию является **TCP 389**.

2. Свяжите с Сервером LDAP со связыванием, аутентифицируют пользователя **корневого dn** и пароль.

3. Выполните поиск LDAP с использованием **основного dn** и поисковых фильтров, которые определены в Конфигурации LDAP для пользователя, который пытается аутентифицироваться.

4. Получите LDAP, следует из Сервера LDAP, и создайте запись в кэше IP Admission для пользователя, если аутентификация успешна, или перебыстра для учетных данных в случае ошибки проверки подлинности.

Анализ выходных данных отладки LDAP

Эти процессы могут быть просмотрены в выходных данных **ldap отладки вся** команда. Этот раздел предоставляет пример выходных данных отладки LDAP для аутентификации, которая отказывает из-за недопустимого **основного dn**. Рассмотрите выходные данные отладки и привязанные комментарии, которые описывают части выходных данных, которые показывают, где вышеупомянутые шаги могли бы встретиться со сбоем.

```
*Jan 30 20:51:50.818: LDAP: LDAP: Queuing AAA request 23 for processing
*Jan 30 20:51:50.818: LDAP: Received queue event, new AAA request
*Jan 30 20:51:50.818: LDAP: LDAP authentication request
*Jan 30 20:51:50.818: LDAP: Username sanity check failed
*Jan 30 20:51:50.818: LDAP: Invalid hash index 512, nothing to remove
*Jan 30 20:51:50.818: LDAP: New LDAP request
*Jan 30 20:51:50.818: LDAP: Attempting first next available LDAP server
*Jan 30 20:51:50.818: LDAP: Got next LDAP server :DC01
*Jan 30 20:51:50.818: LDAP: Free connection not available. Open a new one.
```

```
*Jan 30 20:51:50.818: LDAP: Opening ldap connection
( 10.10.10.150, 389 )ldap_open
```

Часть выходных данных, показанных полужирным, указывает, что это не проблема сетевого уровня, начиная с, соединение успешно открыто.

```
*Jan 30 20:51:50.822: LDAP: Root Bind on CN=Csco_Service,CN=Users,DC=lab,
DC=cisco,DC=com initiated.
*Jan 30 20:51:51.330: LDAP: Ldap Result Msg: SUCCESS, Result code =0
*Jan 30 20:51:51.330: LDAP: Root DN bind Successful on :CN=Csco_Service,
CN=Users,DC=lab,DC=cisco,DC=com
```

Связывать аутентифицировать-dn корректен в этих выходных данных. Если конфигурация является неправильной для этого, то свяжите сбои, замечены.

```
*Jan 30 20:51:50.822: LDAP: Root Bind on CN=Csco_Service,CN=Users,DC=lab,
DC=cisco,DC=com initiated.
*Jan 30 20:51:51.330: LDAP: Ldap Result Msg: SUCCESS, Result code =0
*Jan 30 20:51:51.330: LDAP: Root DN bind Successful on :CN=Csco_Service,
CN=Users,DC=lab,DC=cisco,DC=com
```

Часть выходных данных, показанных полужирным, указывает, что все связывать операции успешны, и это продолжает искать реального пользователя.

```
*Jan 30 20:51:51.854: LDAP: SASL NTLM authentication done..Execute search
*Jan 30 20:51:51.854: LDAP: Next Task: Send search req
*Jan 30 20:51:51.854: LDAP: Transaction context removed from list[ldap reqid=15]
*Jan 30 20:51:51.854: LDAP: Dynamic map configured
*Jan 30 20:51:51.854: LDAP: Dynamic map found for aaa type=username
*Jan 30 20:51:51.854: LDAP: Ldap Search Req sent
ld 2293572544
base dn     dc=lab1,dc=cisco,dc=comscope       2
filter (&(objectclass=top)(sAMAccountName=testuser5))
ldap_req_encode
put_filter "(&(objectclass=top)(sAMAccountName=testuser5))"
put_filter: AND
put_filter_list "(objectclass=top)(sAMAccountName=testuser5)"
put_filter "(objectclass=top)"
put_filter: simple
put_filter "(sAMAccountName=testuser5)"
put_filter: simple
Doing socket write
*Jan 30 20:51:51.854: LDAP: lctx conn index = 2
```

Первая линия (показанный полужирным) указывает, что начинаются выходные данные отладки Поиска LDAP. Кроме того, заметьте, что контроллер домена основного dn должен быть настроен для лабораторной работы, не lab1.

```
*Jan 30 20:51:52.374: LDAP: LDAP Messages to be processed: 1
*Jan 30 20:51:52.374: LDAP: LDAP Message type: 101
*Jan 30 20:51:52.374: LDAP: Got ldap transaction context from reqid
16ldap_parse_result
*Jan 30 20:51:52.374: LDAP: resultCode: 10 (Referral)
*Jan 30 20:51:52.374: LDAP: Received Search Response resultldap_parse_result
ldap_err2string
*Jan 30 20:51:52.374: LDAP: Ldap Result Msg: FAILED:Referral, Result code =10
*Jan 30 20:51:52.374: LDAP: LDAP Search operation result : failedldap_msgfree
*Jan 30 20:51:52.374: LDAP: Closing transaction and reporting error to AAA
*Jan 30 20:51:52.374: LDAP: Transaction context removed from list
[ldap reqid=16]
*Jan 30 20:51:52.374: LDAP: Notifying AAA: REQUEST FAILED
```

Часть выходных данных, показанных полужирным, указывает, что поиск не возвратил результатов, который в этом случае происходит из-за недопустимого основного dn.

RFC 4511

RFC 4511 (**Протокол LDAP: Протокол**), предоставляет сведения о сообщениях результирующего кода для LDAP и другой связанной с протоколом LDAP информации, на которую можно сослаться через веб-сайт IETF.