Конфигурация Active Directory для одиночного входа в систему - для гостевого сервера NAC

Содержание

Введение

Единая точка входа Active Directory (AD SSO) функция использует Kerberos между web-браузером клиента и гостевым сервером Cisco NAC для автоматической аутентификации гостя против Контроллера доменов Active Directory.

Примечание: В целях этого документа NTP и серверы DNS находятся также на DC, но это - возможно не случай в вашей среде.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- DNS должен быть настроен и работать на гостевой сервер Cisco NAC.
- DNS должен быть настроен и работать на Контроллер домена.
- Записи DNS для гостевого сервера Cisco NAC должны быть определены:ЗаписьЗапись *PTR*
- Записи DNS для Контроллера домена должны быть определены:ЗаписьЗапись *PTR*
- Настройки времени Гостевого сервера Cisco NAC должны синхронизироваться с Доменом Active Directory.

Используемые компоненты

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

- Гостевой сервер NAC 2.0
- Microsoft Windows XP с Internet Explorer 6.0
- Windows Server 2003

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.

Условные обозначения

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

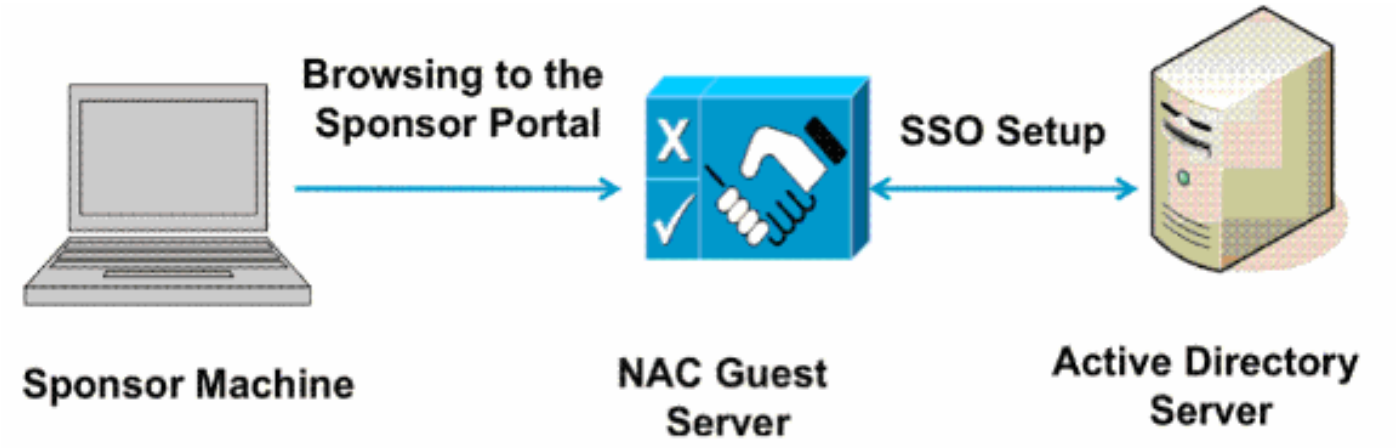
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:



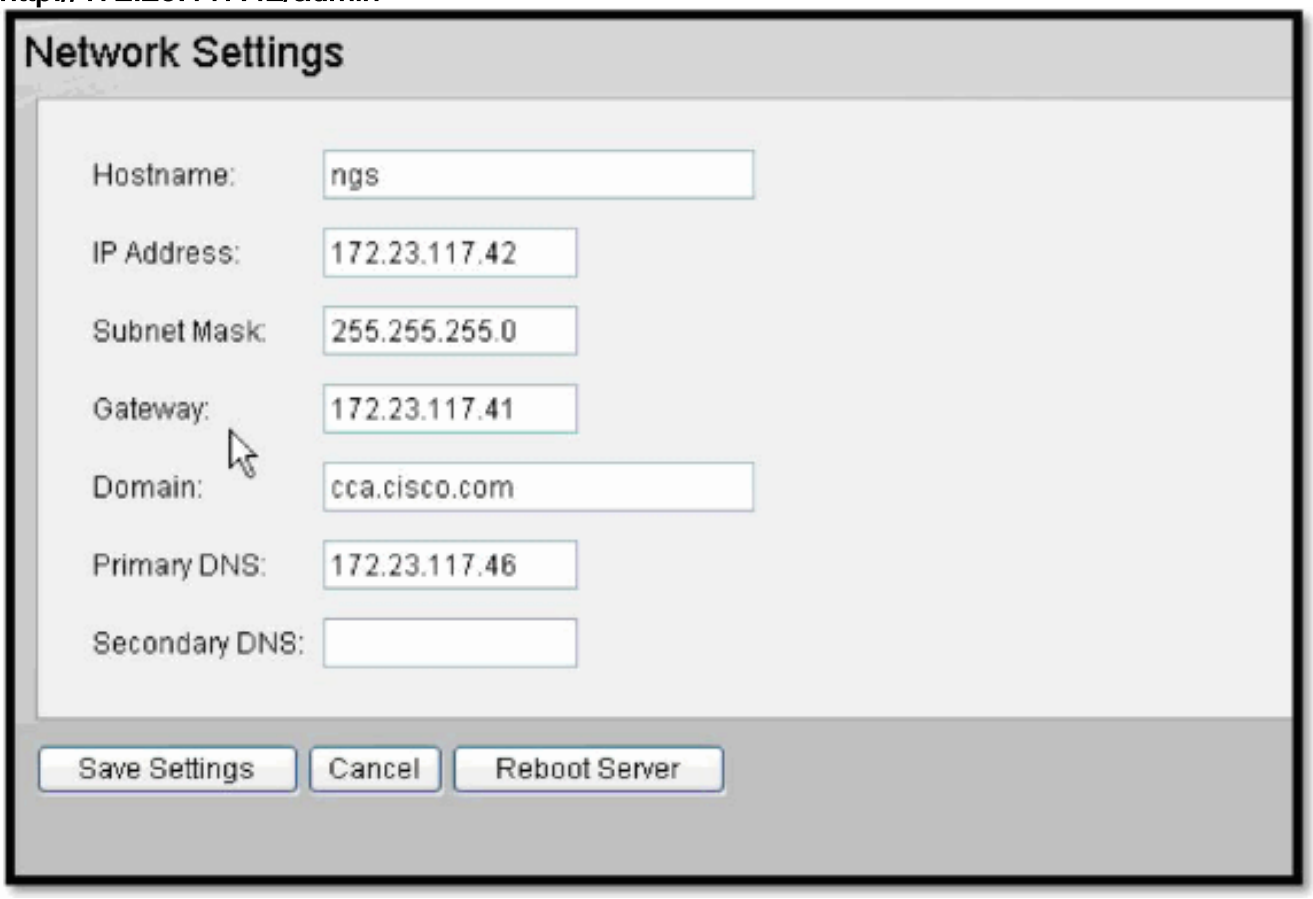
Конфигурации

Этот документ использует эти IP-адреса:

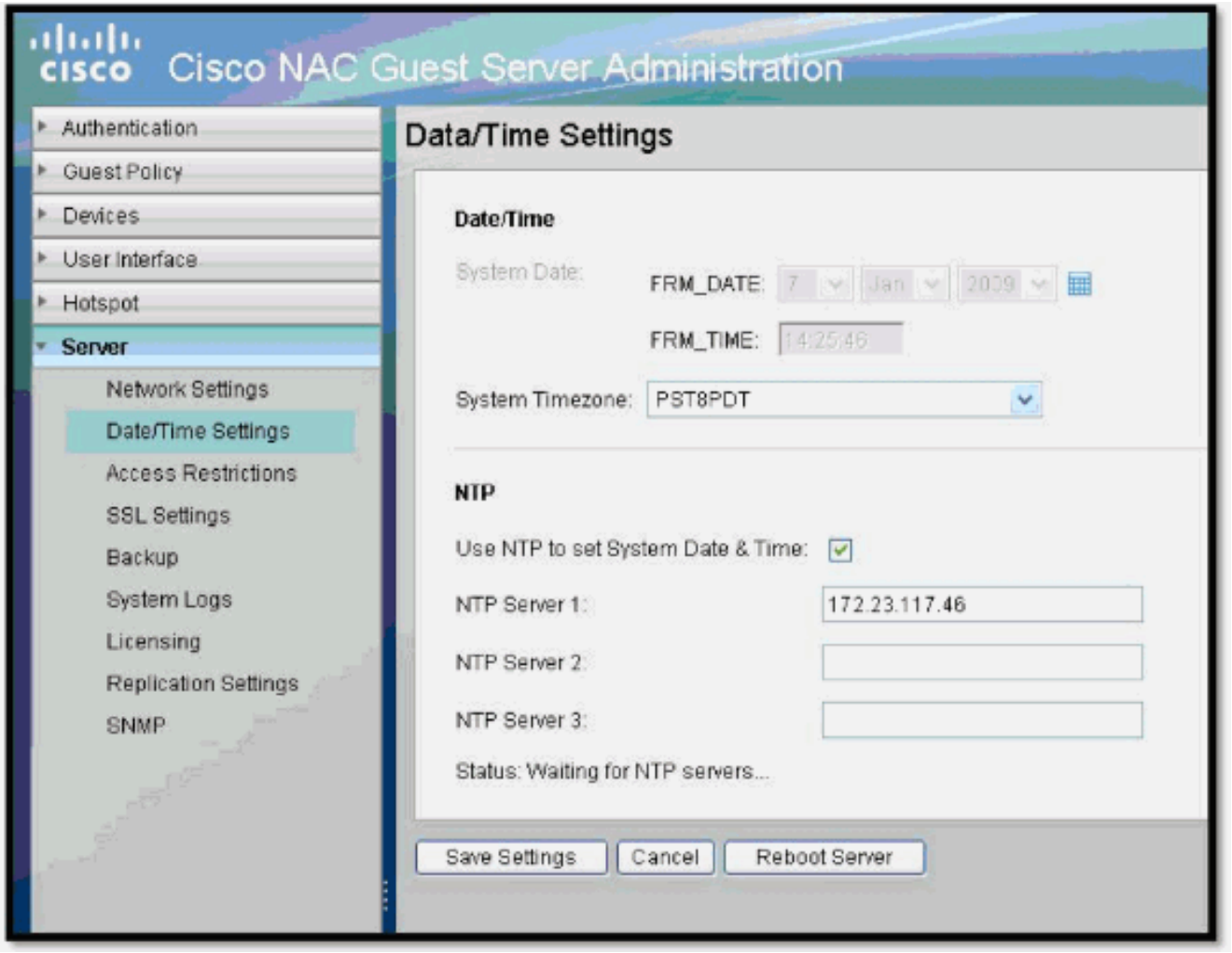
- Контроллер домена — 172.23.117.46 (w2k3-server.cca. cisco . com)
- Гостевой сервер NAC — 172.23.117.42 (ngs.cca. cisco . com)
- Машина спонсора — 172.23.117.45

Выполните следующие действия:

1. Обратитесь к Интерфейсу Admin НАНОГРАММОВ. От браузера перейдите **к http://172.23.117.42/admin**



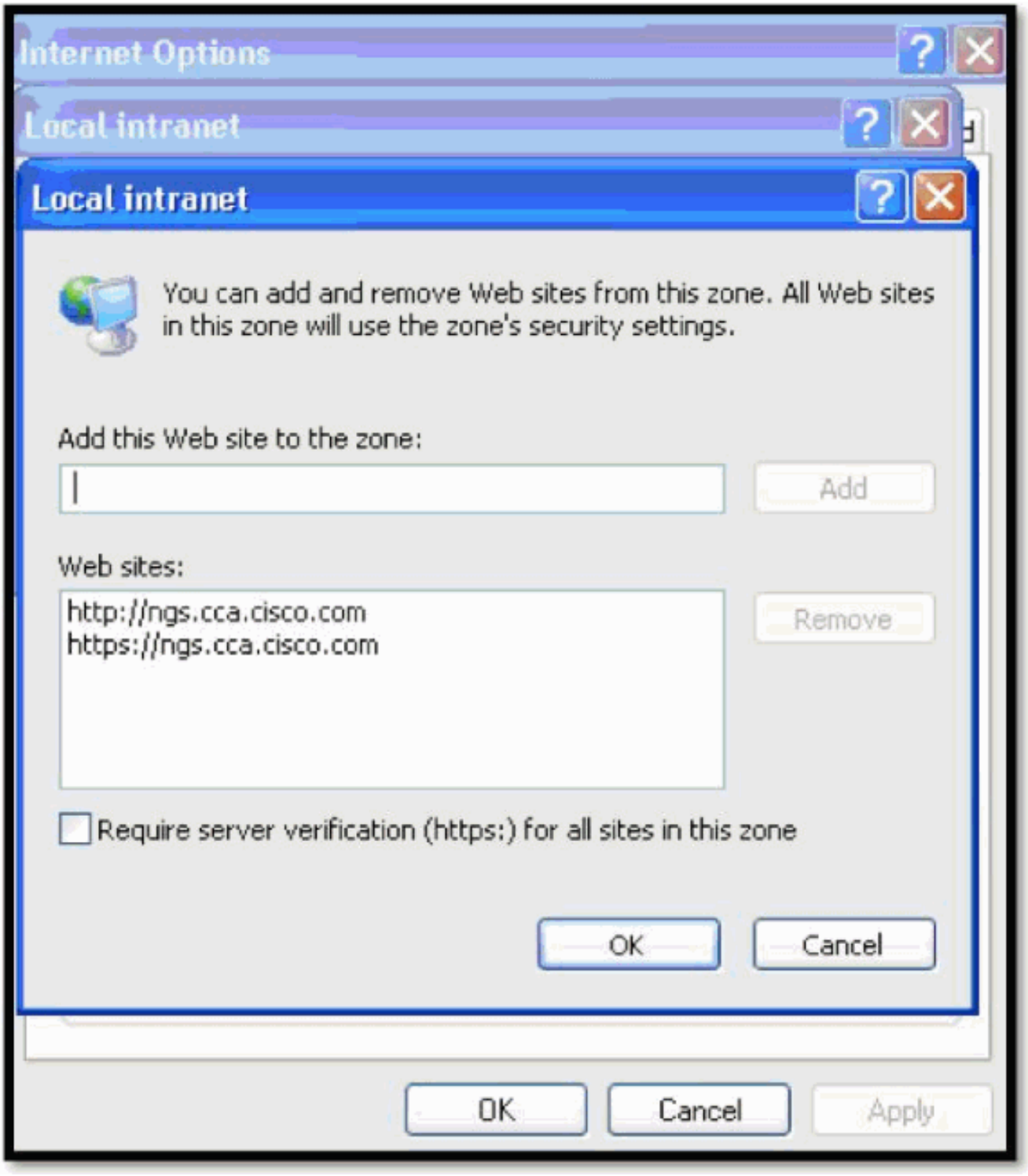
2. **Конфигурация сети НАНОГРАММОВ**Выберите **Server> Network Settings**.Host nameDomain — cca. cisco . comОсновной DNS — 172.23.117.46
3. **Настройка NTP**В **Дате/Времени Server>** настройте сервер NTP к IP DC **172.23.117.46**.

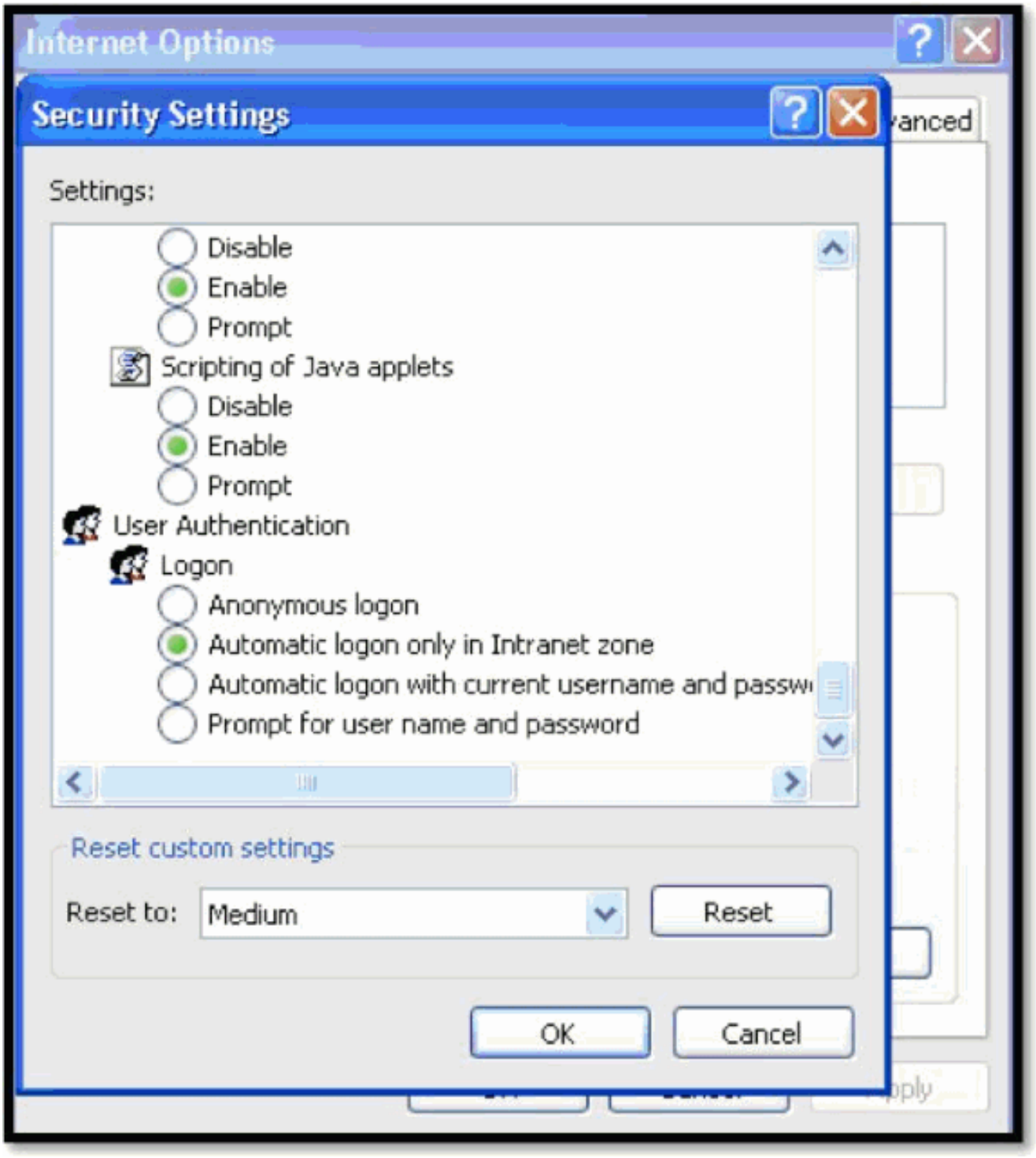


4. **AD настройка SSO**Перед настройкой раздела SSO удостоверьтесь, A и записи PTR существуют для контроллера домена и Гостевого сервера NAC.B AuthServer> Подлинный раздел SSO, настройте
это:

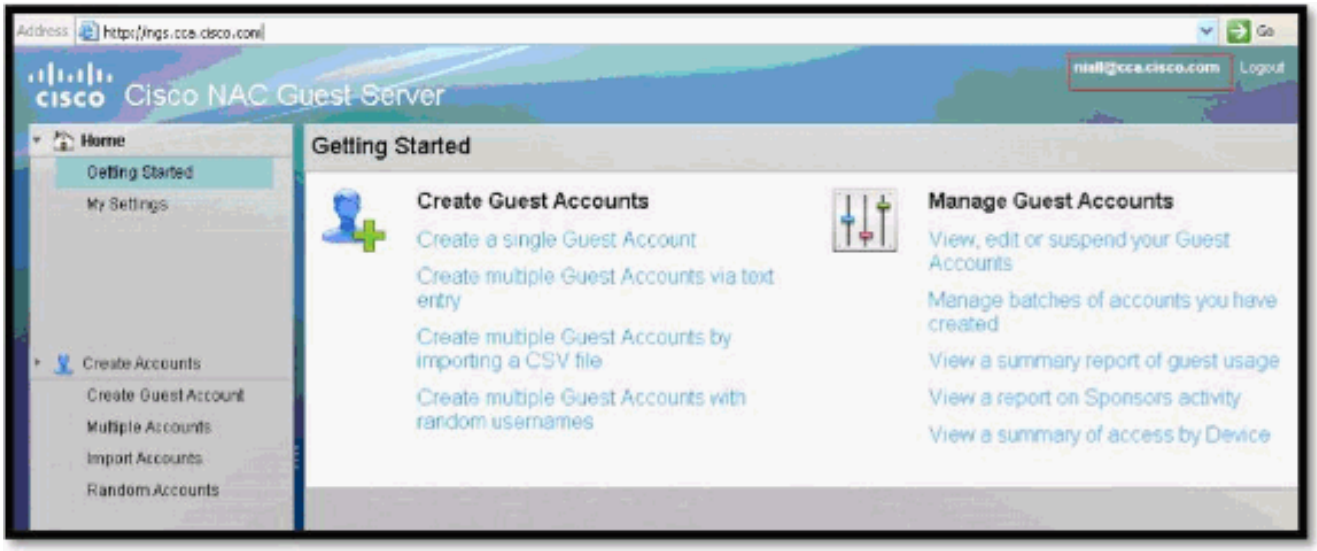
Если конфигурация успешна, необходимо видеть сообщение об успешном завершении.

5. **Проверьте функцию SSO**От пользовательской машины войдите в домен. В данном примере эта машина является частью домена cca. Только Internet Explorer поддерживается для функции SSO. Необходимо удостовериться, что Гостевой сервер NAC является частью локального Intranet, и автовход в систему **включен**.**Примечание:** Используйте FQDN для гостевого сервера для тестирования SSO от браузера. Например, IP-адрес не работает.Проверьте настройки веб-браузера:

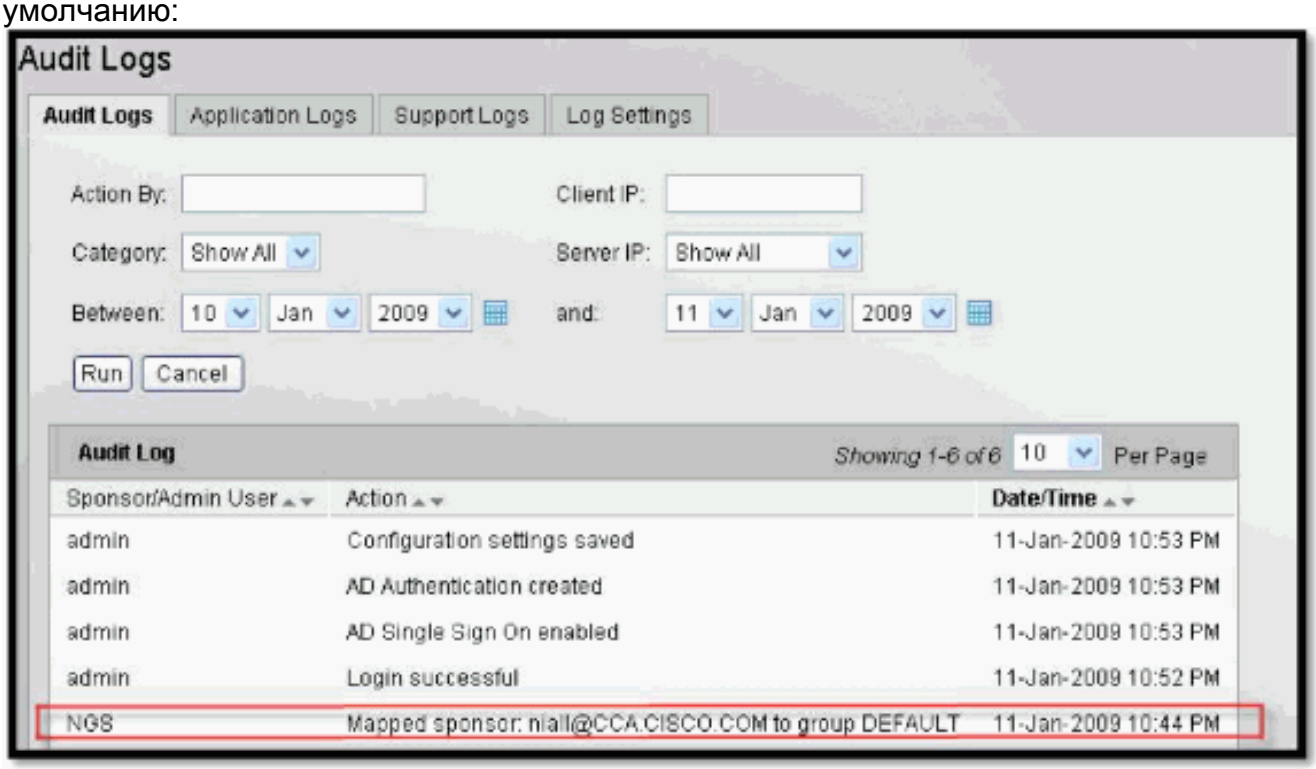

Internet Options
Local intranet
Local intranet
You can add and remove Web sites from this zone. All Web sites in this zone will use the zone's security settings.
Add this Web site to the zone:
Add
Web sites:
http://ngs.cca.cisco.com
https://ngs.cca.cisco.com
Remove
Require server verification (https:) for all sites in this zone
OK
Cancel
OK
Cancel
Apply



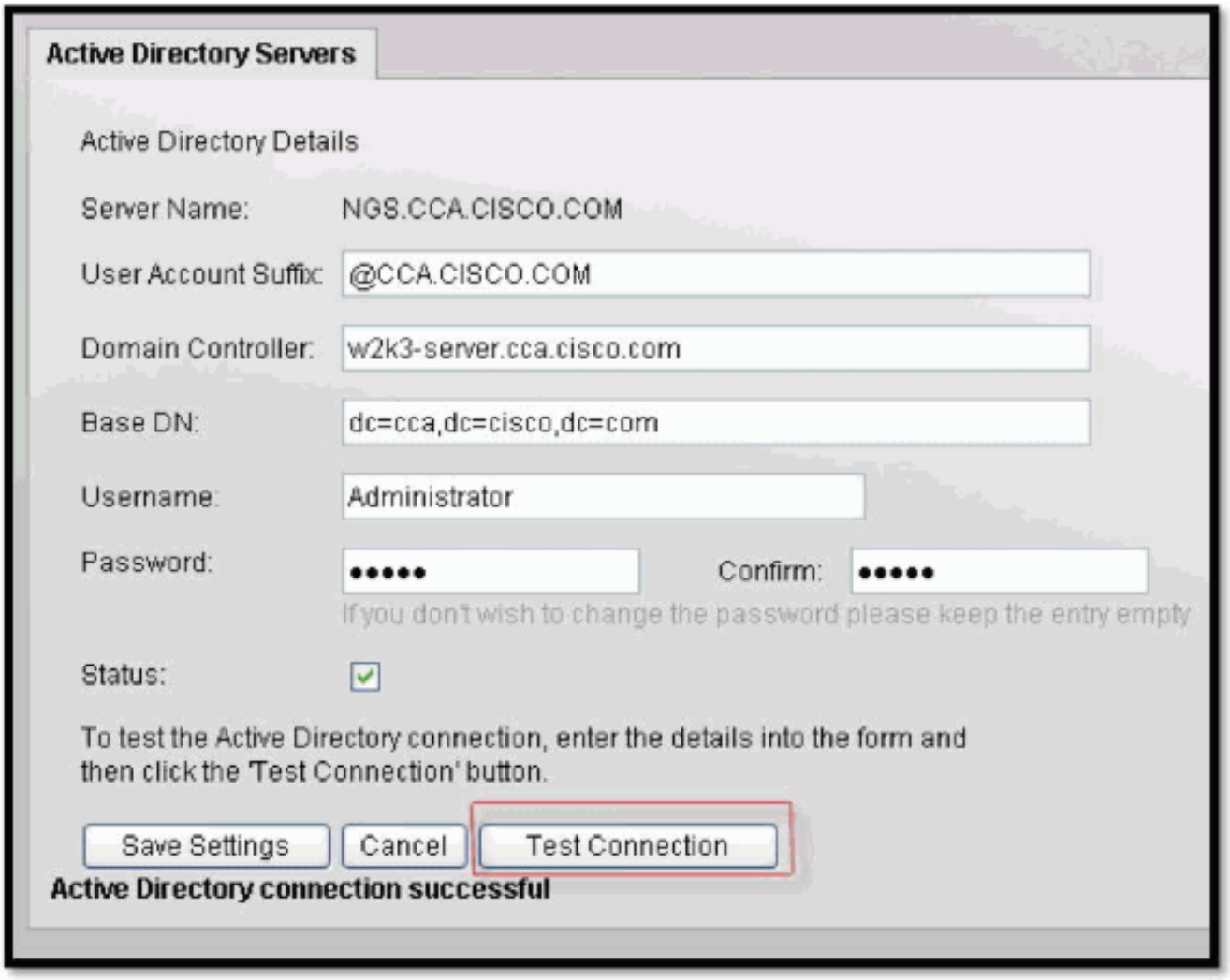
От web-браузера перейдите **к http://ngs.cca. cisco . com**. В вас нужно автоматически войти к нанограммам с доменными учетными данными.**Примечание:** Ссылка **http://ngs.cca. cisco . com** будет только работать при настройке NAC в режиме администрирования с учетными данными пользователя.



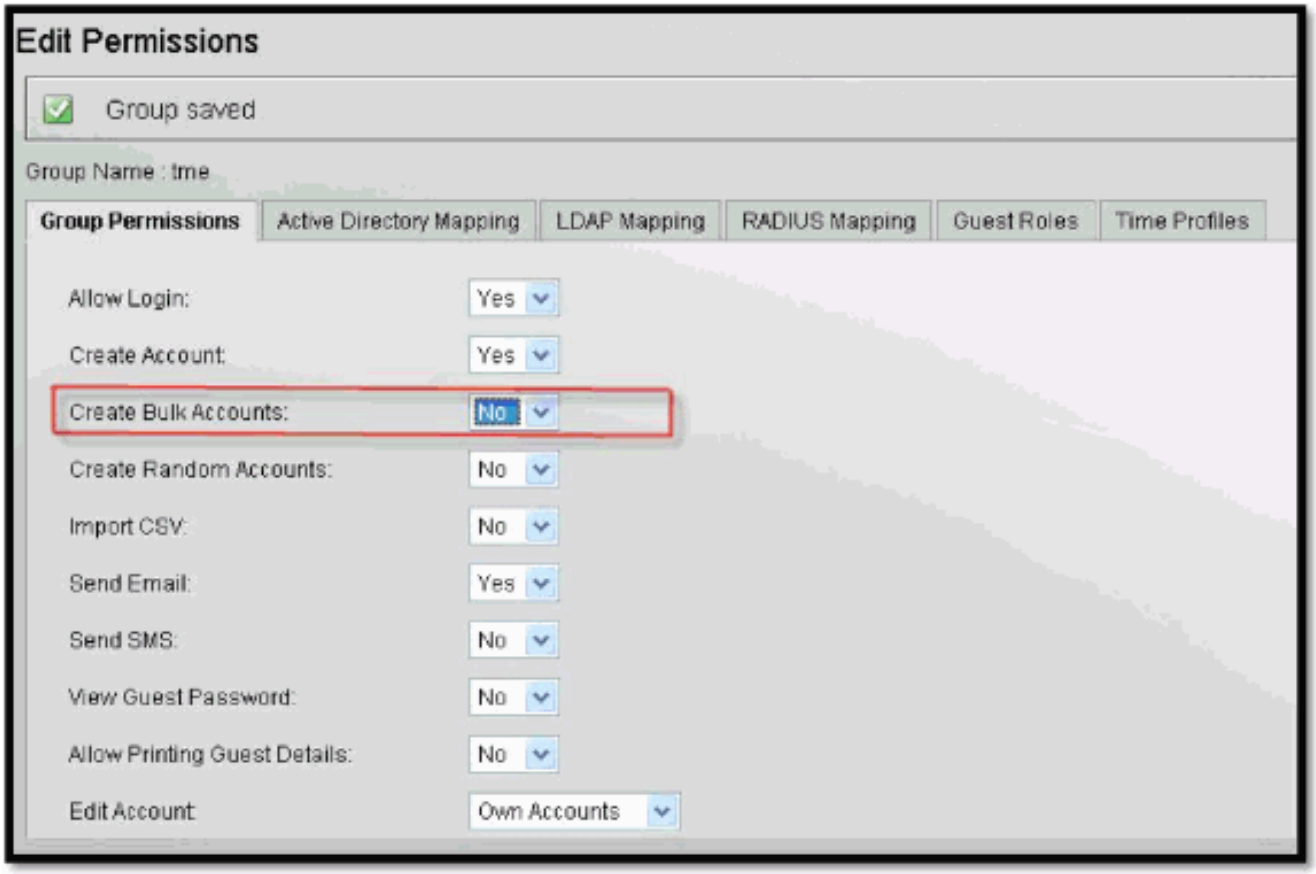
Под Журналами аудита Гостевого сервера NAC вы видите, что пользователь Найэл вошел в группу по
умолчанию:



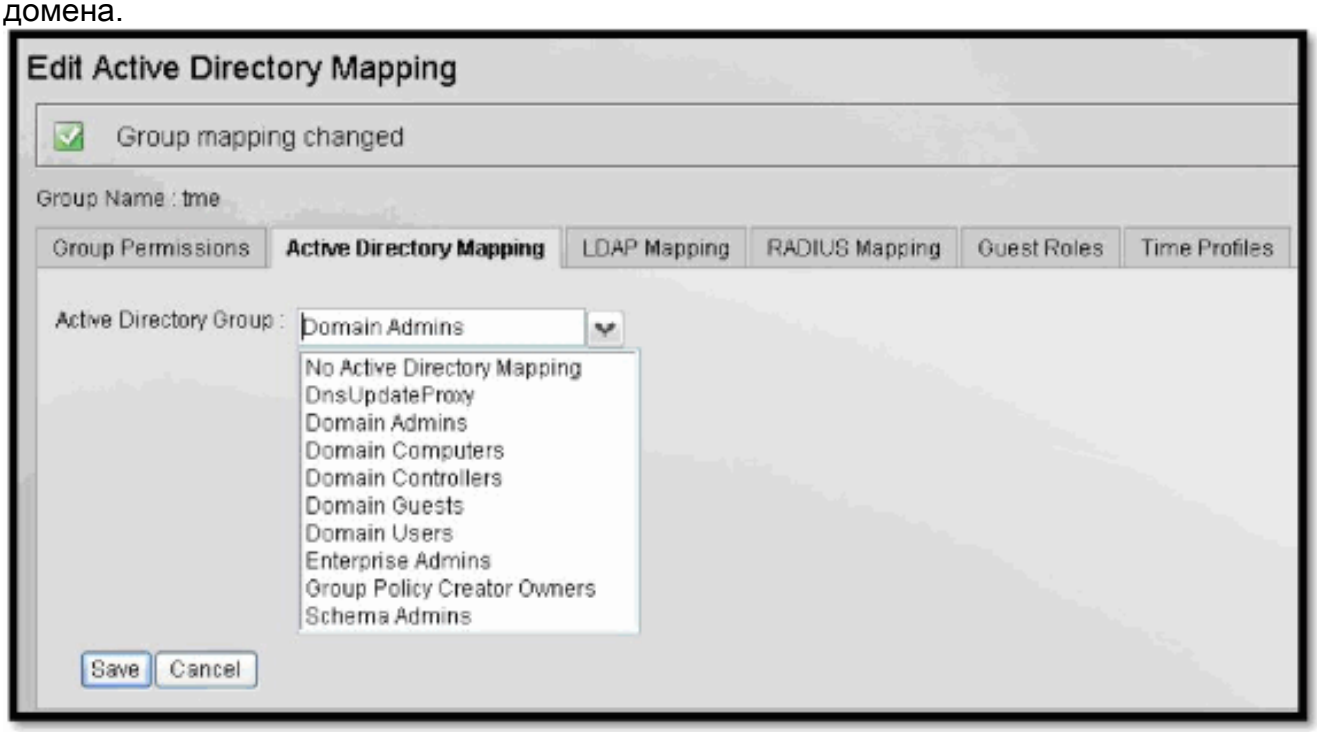
6. **Сопоставление группы пользователей с AD SSO (Необязательно)***В этом разделе вы будете учиться сопоставлять пользователя SSO с определенной группой кроме группы по умолчанию.*Для сопоставления группы пользователей с ADSSO необходимо настроить Сервер Active Directory как Сервер проверки подлинности и затем сопоставить AD группу с Группой пользователей Спонсора.Выберите **NGS (http://172.23.117.42/admin) Аутентификации> Спонсоры> Серверы Active Directory**. Добавьте новый контроллер
домена.



Опция тестового подключения была представлена в НАНОГРАММАХ 2.0 для простоты устранения проблем. Это говорит вам, настроили ли вы DC правильно.**Настройте группу пользователей**Имя группы Add a New User — **tme**. В данном примере вы выбираете **NO** для увеличения объема создания учетной записи. Таким образом, вы сразу знаете, был ли пользователь размещен в tme группу *или* группу по умолчанию.



В Сопоставлении Active Directory тестовый пользователь niall уже является частью Администраторов
домена.



Проверка

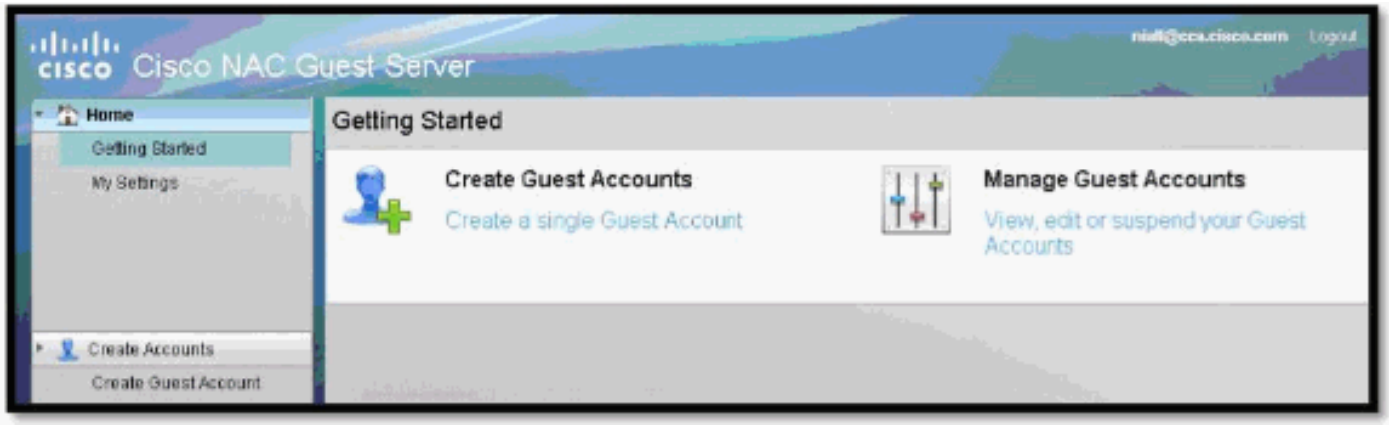
Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

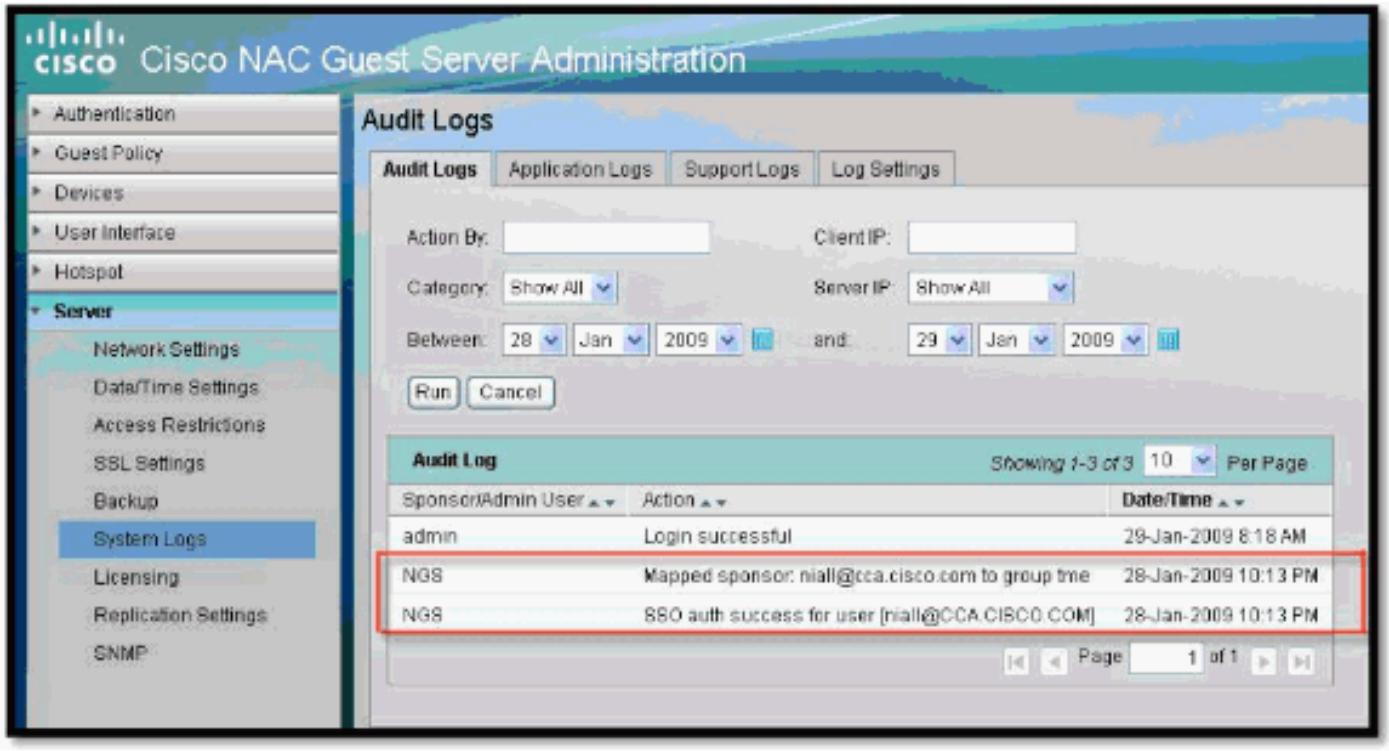
Проверьте сопоставление группы пользователей ADSSO

Для доступа к машине Спонсора откройте новый браузер и перейдите к http://ngs.cca. cisco . com.

Найэл должен быть размещен в tme группу без доступа для увеличения объема создания учетной записи.



При рассмотрении журналов аудита можно проверить, что Спонсор размещен в корректную Роль.



Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Это сообщения об ошибках в журналах. Ошибки Kerberos приводят к одной из этих ошибок:

- `Domain format incorrect / Domain Controller must be a FQDN, not an IP address` Домен не был введен в правильный формат (должен иметь CCA CISCO.COM формы).

- `Hostname must be a FQDN, not an IP address` Именем хоста Гостевого сервера NAC не может быть IP-адрес, это должно быть Полное доменное имя, например, nAC (CCA). cisco . com.
- `Cannot determine IP address for Domain Controller` Существует проблема Конфигурации DNS.
- `Cannot get DNS A record for Domain Controller` Существует проблема Конфигурации DNS.
- `Cannot get DNS A record for hostname` Существует проблема Конфигурации DNS.
- `Cannot get DNS PTR record for Domain Controller IP address` Существует проблема Конфигурации DNS.
- `Cannot get DNS PTR record for hostname IP address` Существует проблема Конфигурации DNS.
- `Failed to create computer account for this server on the Domain Controller. See application log for details .` Просмотрите журнал приложения для наблюдения полного изложения ошибки.
- `Invalid username/password` Имя пользователя администратора / пароль является неправильным.
- `Invalid Domain or cannot resolve network address for DC` На AD сервере существует Проблема DNS.
- `Domain Controller time does not match this server's time` Гарантируйте соответствие времен на сервере, рекомендуется использовать NTP для синхронизации времен на сервере.
- `The DC cannot determine the hostname for the Guest server by reverse lookup. There may be an issue with your DNS confiugration.` На вашем AD сервере существует проблема Конфигурации DNS.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация