Содержание

Введение

Этот документ предоставляет сведения о проверке конфигурации Протокола LDAP на Комплекте Управления системой унифицированных коммуникаций (UCSM) и шагает для исследования проблем сбоя проверки подлинности LDAP.

РУКОВОДСТВА ПО КОНФИГУРАЦИИ:

[Аутентификация Настройки UCSM](#)

[Типовая конфигурация Active Directory (AD)](#)

Проверьте Конфигурацию LDAP UCSM

Удостоверьтесь, что UCSM развернул конфигурацию успешно путем проверки статуса Блока конечных состояний (FSM), и это показывает завершенный в 100%.

От контекста Интерфейса командной строки (CLI) UCSM

От Операционной системы Nexus (NX-OS) контекст CLI

Оптимальные методы конфигурации LDAP

1. Создайте дополнительные опознавательные домены вместо того, чтобы изменить область "Собственного компонента Отэниткэйшна"

2. Всегда используйте локальную сферу для 'консольной аутентификации', В случае, если пользователь блокирован из использования 'собственной аутентификации', admin все еще был бы в состоянии обратиться к нему от консоли.

3. Если все серверы в данном подлинном домене были не в состоянии отвечать во время попытки входа (не применимый для команды test aaa), UCSM всегда возвращается к состоянию до сбоя к локальной проверке подлинности.

Проверка Конфигурации LDAP

Протестируйте проверку подлинности LDAP с помощью команды NX-OS. команда 'тестового aaa' доступна только от CLI - интерфейса NX-OS.

1. Проверьте группу LDAP определенная конфигурация.

Следующая команда проходит список всех настроенных Серверов LDAP на основе их настроенного порядка.

2. Проверьте определенную конфигурацию Сервера LDAP

Примечание: строка <password> будет отображена на терминале.

В этом случае, если нет никакого фильтра, настроенного для указанного Сервера LDAP, UCSM тестирует аутентификацию против определенного сервера и может отказать.

Устранение проблем ошибок регистрации в системе LDAP

Этот раздел предоставляет сведения о диагностировании проблем проверки подлинности LDAP.

Сценарий проблемы #1 - не Может войти

Не может войти как пользователь LDAP и через Графический пользовательский интерфейс (GUI) UCSM и через CLI

Пользователь получает **"Ошибку при аутентификации на сервере"** при тестировании проверки подлинности LDAP.

Рекомендация
Проверьте сетевое подключение между интерфейсом управления Сервера LDAP и Центрального устройства (FI) эхо-запросом Протокола ICMP и соединением TELNET установления от контекста локального mgmt

Исследуйте сетевое подключение Протокола IP, если UCSM не может пропинговать Сервер

LDAP или открыть сеанс Telnet для Сервера LDAP.

Проверьте, возвращает ли Сервис доменных имен (DNS) правильный IP-адрес к UCS для имени хоста Сервера LDAP, и удостоверьтесь, что трафик LDAP не заблокирован между этими двумя устройствами.

Сценарий проблемы #2 - Может войти в GUI, не может войти в SSH

Пользователь LDAP может войти через GUI UCSM, но не может открыть Сеанс SSH для FI.

Рекомендация

При установлении Сеанса SSH к FI как пользователь LDAP UCSM требует, чтобы "ucs-" предварительно ожидался перед domain-name LDAP

* От Linux / машина MAC

* От клиента шпаклевки

Примечание: Доменное имя учитывает регистр и должно совпасть с domain-name, настроенным в UCSM. Максимальная длина имени пользователя может быть 32 char, который включает доменное имя.

"ucs-<domain-name> \<имя пользователя>" = 32 char.

Сценарий проблемы #3 - у Пользователя есть привилегии только для чтения

Пользователь LDAP может войти, но имеет привилегии только для чтения даже при том, что карты группы ldap правильно настроены в UCSM.

Рекомендация

Если никакие роли не были получены во время процесса регистрации в системе LDAP, удаленный пользователь или позволен с ролью по умолчанию (доступ только для чтения) или запрещенный доступ (никакой вход в систему) для входа в систему к UCSM, на основе политики удаленного входа в систему.

Когда удаленный пользователь входит, и пользователю дали доступ только на чтение, В этом случае проверьте подробные данные членства группы пользователей в LDAP/AD. Например, мы можем использовать Служебную программу ADSIEdit для Active Directory MS. или ldapserach в случае Linux/Mac.

Это может также быть проверено с командой "тестового aaa" от оболочки NX-OS.

Сценарий проблемы #4 - не Может войти с 'Удаленной аутентификацией'

Когда "Собственная Аутентификация" была изменена на механизм удаленной

аутентификации (LDAP и т.д.), пользователь не может войти или имеет доступ только на чтение к UCSM как удаленный пользователь

Рекомендация
Как UCSM fallsback к локальной проверке подлинности для консольного доступа, когда это не может достигнуть сервера удаленной аутентификации, мы можем придержаться ниже шагов для восстановления его.

1. Разъедините интерфейсный кабель mgmt основного FI (состояние show cluster указало бы, который действует как Основной),
2. Соединитесь с консолью основного FI
3. Выполните следующие команды для изменения собственной аутентификации

4. Подключите интерфейсный кабель mgmt
5. Вход в систему через UCSM использование локальной учетной записи и создает подлинный домен для удаленной аутентификации (исключая LDAP) группа.
Примечание: Разъединение интерфейса mgmt НЕ влияло бы ни на какой трафик плоскости данных.

Сценарий проблемы #4 - Проверка подлинности LDAP работает, но не с включенным SSL

Когда параметр SSL включен, проверка подлинности LDAP хорошо работает без Протокола SSL, но отказывает.

Рекомендация
Клиент LDAP UCSM использует настроенные точки доверия (сертификаты Центра сертификации (CA)) при установлении подключения SSL.

1. Удостоверьтесь, что точка доверия была настроена правильно.

2. Определить поле в свидетельстве должно быть "именем хоста "Сервера LDAP. Удостоверьтесь, что имя хоста, настроенное в UCSM, совпадает с подарком имени хоста в сертификате и допустимо.

3. Удостоверьтесь, что UCSM настроен с 'именем хоста' не 'ipaddress' Сервера LDAP, и это recheable от интерфейса локального mgmt.

Сценарий проблемы #5 - Опознавательные сбои после изменений поставщика LDAP

Опознавательные сбои после удаления старого Сервера LDAP и добавления нового Сервера LDAP

Рекомендация
Когда LDAP используется в области аутентификации, удаление и добавление новых серверов не разрешены. От версии UCSM 2.1 это привело бы к сбою FSM.

Шаги для придержаний, когда удаление/добавление новых серверов в той же транзакции

1. Удостоверьтесь, что все области аутентификации с помощью ldap изменены на локальную переменную и сохранили конфигурацию.
2. Обновите Серверы LDAP и проверьте, что статус FSM завершил успешно.
3. Измените подлинные области доменов, модифицируемых в шаге 1 к LDAP.

Для всех других сценариев проблемы - Отладка LDAP

Включите отладки, попытайтесь войти как пользователь LDAP и собрать следующие журналы наряду с UCSM techsupport, который перехватывает отказавшее событие входа в систему.

1) Откройте Сеанс SSH для FI и входа в систему как локальный пользователь и изменитесь на контекст CLI NX-OS.

2) Включите следующие флаги отладки и сохраните выходные данные Сеанса SSH к файлу журнала.

3) Теперь откройте новый GUI или сеанс CLI и попытку войти как удаленные (LDAP) пользователь
4) Как только вы получили сообщение ошибки регистрации в системе, **выключите отладки.**

Пакет caputure трафика LDAP

В сценариях, где захват пакета требуется, Ethanalyzer может используемый для получения трафика LDAP между FI и Сервером LDAP.

В вышеупомянутой команде, pcap файл сохранен в/workspace/diagnostics каталоге и может быть получен из FI через контекст CLI локального mgmt

Выше команды может использоваться для получения пакетов для любого удаленного (LDAP, TACACS, RADIUS) authenitcation трафик.
5. Соответствующие журналы в UCSM techsupport связка (bundle)

В UCSM techsupport, соответствующие журналы расположены под **<FI>/var/sysmgr/sam_logs каталог**

Известные предупреждения

CSCth96721
rootdn сервера LDAP на sam должен позволить больше чем 128 символов

Версия UCSM ранее, чем 2.1 имеет ограничение 127 символов для основного DN / связывают строку DN.

http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/cli/config/guide/2.0/b_UCSM_CLI_Configuration_Guide_2_0_chapter_0111.html#task_0FC4E8245C6D4A64B5A1F575DAEC6127

фрагмент----------

Определенное составное имя в иерархии LDAP, где сервер должен начать поиск, когда удаленный пользователь входит и система, пытается получить DN пользователя на основе их имени пользователя. Максимальная поддерживаемая длина строки составляет 127 символов.

Проблема устранена в 2.1.1 и выше выпуска

CSCuf19514
Демон LDAP завершился катастрофическим отказом

Если вызов ldap_start_tls_s берет больше чем 60 secs для завершения инициализации, клиент LDAP может завершиться катастрофическим отказом при инициализации ssl библиотеки. Это могло произойти, только упаковывают недопустимой Записи DNS / задержки Разрешения DNS.

Предпримите шаги для адресации к задержкам Разрешения DNS и ошибкам.