Настройка отправки журналов с устройства Cisco Prime AR

В данной статье описано, как настроить отправку журналов с Cisco Prime Access Registrar (Prime AR).

Общие сведения

Cisco Prime Access Registrar (Prime AR) поддерживает централизованное логирование через протокол **Syslog**, что позволяет собирать диагностические и аудиторские сообщения на удаленном сервере. Локальное и Syslog-логирование можно включать или отключать в любой момент, редактируя файл конфигурации **$INSTALLPATH/conf/car.conf**.

Для приема Syslog-сообщений требуется UNIX-хост с запущенным демоном **Syslogd**. Сервер Prime AR и Syslog-демон могут работать как на одном, так и на разных хостах.

Формат Syslog-сообщений

Сообщения из следующих журналов передаются на Syslog-сервер:

- **aregcmd_log**;
- **config_mcd_[1..n]_log**;
- **name_radius_[1..n]_log**;
- **agent_server_[1..n]_log**.

Стандартный формат (до 1024 байт):

MMM DD hh:mm:ss hostname %Prime AR-[severity]-[mnemonic]: [#n], [System|Server]: message_description

Параметры:

- **MMM DD hh:mm:ss** — дата и время получения сообщения на Syslog-сервере;
- **hostname** — имя хоста Syslog-сервера;
- **severity** — уровень важности (0–7):
  - 0 — emergency;
  - 1 — alert;
  - 2 — critical;
  - 3 — error;
  - 4 — warning;
  - 5 — notification;
  - 6 — informational;
  - 7 — debugging.
- **mnemonic** — идентификатор подсистемы: **aregcmd**, **name_radius**, **agent_server**, **config_mcd**;
- **#n** — идентификатор экземпляра компонента;
- **message_description** — текстовое описание события.

Пример:

May 19 14:28:44 dwlau-ultra2.cisco.com %Prime AR-3-name_radius: #1, System: Remote LDAP Server.Unable to bind.
May 19 14:28:45 dwlau-ultra2.cisco.com %Prime AR-6-name_radius: #1, Server: Stopping server

Длинные сообщения (>1024 байт) разбиваются на несколько строк. Каждая строка, кроме последней, завершается троеточием (**...**). Следующая часть начинается с **...** .

Настройка логирования сообщений

Для настройки выполните следующие шаги:

Шаг 1. Для того чтобы настроить логирование сообщений, необходимо включить прием Syslog на сервере:

1. для систем на базе RHEL < 7.0:
   - Отредактируйте **/etc/sysconfig/syslog** и добавьте флаг **-r**:

     SYSLOGD_OPTIONS="-r -m 0"

     Флаг **-r** разрешает прием сообщений от удаленных хостов на порту **514/UDP**.
2. для RHEL 7.0 и выше:
   - Отредактируйте **/etc/rsyslog.conf** и добавьте:

     $ModLoad imudp.so
     $UDPServerRun 514
     SYSLOGD_OPTIONS="-r -m 0"
     localn.info <tab> <tab> <tab> /var/log/filename.log

   - Укажите правило маршрутизации (см. ниже).

Шаг 2. Перезапустите службу:

systemctl restart rsyslog.service

Настройка демона syslogd

Для настройки выполните следующие шаги:

Шаг 1. В файле **/etc/syslog.conf** (или **/etc/rsyslog.conf**) укажите, куда сохранять сообщения от Prime AR:

localn.info /var/log/filename.log

Используйте табуляцию как разделитель между **facility** и путем к файлу.

Параметры:

- **localn** — facility (n = 0–7), должен совпадать со значением **FACILITY_LOCAL_NUMBER** в **car.conf**;
- **/var/log/filename.log** — путь и имя файла журнала (выбирается администратором).

Шаг 2. Создание файла журнала:

1. Войдите под пользователем **root**.
2. Создайте файл:

   touch /var/log/filename.log

3. Установите права:

   chmod 664 /var/log/filename.log

Изменение каталога локальных журналов

Для изменения каталога выполните следующие шаги:

Шаг 1. Чтобы изменить каталог для локальных журналов (не Syslog!), добавьте в **$INSTALLPATH/conf/car.conf**:

LOGDIR /полный/путь/к/каталогу

Пример:

LOGDIR /var/log/AICar1

- Перед изменением остановите сервер Prime AR.
- После правки скопируйте существующие журналы в новый каталог.
- Эта настройка не влияет на расположение syslog-файлов на удаленном сервере.

Управление размером Syslog-файлов

Без контроля размера Syslog-файлы могут заполнить все дисковое пространство, что приведёт к сбоям в работе Prime AR (особенно при записи данных сессий).

Рекомендации:

1. Размещайте каталог журналов на отдельном дисковом разделе, отличном от того, где хранятся данные сессий.
2. Используйте **cron** для автоматической ротации журналов.

Пример cron-задачи (еженедельная архивация):

```
# Каждое воскресенье в 02:01
01 02 * * 0 cd /var/log; \
if [ -f ar_syslog.log ]; then \
  if [ -f ar_syslog.log.1 ]; then \
    /bin/mv ar_syslog.log.1 ar_syslog.log.2; \
  fi; \
  /usr/bin/cp ar_syslog.log ar_syslog.log.1; \
  >ar_syslog.log; \
fi
```

Архивные файлы (**ar_syslog.log.1**, **.2**) лучше перемещать на другой диск для экономии места.

Логирование статуса RADIUS-серверов

Prime AR фиксирует изменения состояния удаленных RADIUS-серверов в файле **$INSTALL/logs/name_radius_1_log**.

Типы сообщений:

Событие	Формат сообщения
Сервер стал доступен	Remote Server <host> (<IP>:<port>) is UP
Сервер недоступен	Remote Server <host> (<IP>:<port>) is DOWN!
Сервер остается недоступен	Remote Server <host> (<IP>:<port>) remains DOWN!
Сервер медленно отвечает	Remote Server <host> (<IP>:<port>) is UP but slow!
Сервер очень медленно отвечает	Remote Server <host> (<IP>:<port>) is UP but very slow!
Сервер возвращен в пул	Remote Server <host> (<IP>:<port>) is being reactivated for later use.

Логирование данных абонентов

Абонентские данные (включая Diameter-запросы/ответы) записываются в файл **$INSTALLPATH/logs/Subscriber_log**.

Чтобы включить логирование для конкретного клиента, установите параметр:

UserLogEnabled = True

Формат записи:

Дата|Время|Тип_Diameter_сообщения|IMSI|MSISDN|Subscription-Id|Origin-Host|...|Result_Code|...

Логирование IP-адреса пользователя

Логирование IP-адреса пользователя включается параметром в секции **/Radius/Advanced**:

DisplayUserForFailedLogin = True

При активации:

- при неудачных попытках входа в **aregcmd_log** добавляется **имя пользователя**;
- для всех операций (конфигурация, вход, выход) в **aregcmd_log** записывается **IP-адрес пользователя** (первый хоп).

Логирование таймаутов пакетов

Prime AR теперь фиксирует пакеты, по которым не получено ответа в течение заданного времени.

Пример записи:

log
07/04/2020 14:08:35.904 name/radius/1 Info System 0 Remote Server REM_76 has not responded Cmd code: 303 request for user-name 97000000051 in 1 try

Логирование системной статистики

Логирование системной статистики включается параметром в **car.conf**:

/RADIUS/Advanced/Diameter/TransportManagement/SystemStatsLogFrequencyInSecs = N

(где `N > 0` — интервал в секундах). Статистика сохраняется в файл **system_stats_log**.

Собираемые метрики:

- Общие:
  - Загрузка CPU и памяти;
  - NFS I/O статистика;
  - Число таймаутов (MAR/SAR/UDR);
  - Количество отброшенных/дублирующих пакетов;
  - Счетчики запросов/ответов (входящих/исходящих);
  - Очередь таймеров.
- По соединению:
  - Входящие/исходящие запросы в секунду;
  - Повторные запросы;
  - Отброшенные ответы.

Логирование размера очереди рабочих потоков

Для логирования размера очереди рабочих потоков в файл **system_stats_log** добавляется метрика: **Peak Worker Thread Queue / sec**.

Она отображается только если за последний интервал наблюдалось состояние **"All Workers Temporarily Busy"**.

Заключение

Правильная настройка **Syslog** в Cisco Prime Access Registrar обеспечивает:

- централизованный сбор событий безопасности и диагностики;
- контроль доступности RADIUS/Diameter-серверов;
- мониторинг производительности и нагрузки;
- соответствие требованиям аудита.

Рекомендуется использовать отдельный диск для журналов и настроить автоматическую ротацию через **cron** или **logrotate**.

ID статьи: 1553
Последнее обновление: 31 мар., 2026
Обновлено от: Михалева А.
Ревизия: 12