Настройка отправки журналов с устройства Cisco ISE

В данной статье описано, как настроить отправку системных событий с Cisco Identity Services Engine (ISE).

Общие сведения

Журналы ISE можно классифицировать по категориям и направлять на один или несколько удаленных получателей (targets), таких как UDP/TCP-серверы Syslog или защищенные TLS-серверы.

Журналы собираются узлами мониторинга (MnT) и хранятся локально. Для внешнего сбора необходимо настроить **удаленные цели (remote logging targets)** и привязать их к нужным категориям логирования.

Предварительные требования

1. Рекомендуемые знания:
   - основы работы с Cisco Identity Services Engine (ISE);
   - понимание принципов работы Syslog-серверов.
2. Используемое ПО:
   - Cisco ISE версии 3.3;
   - Kiwi Syslog Server v1.2.1.4 (в качестве примера).

Конфигурация выполнена в лабораторной среде с чистыми настройками. При работе в production-сети убедитесь, что понимаете влияние всех изменений.

Настройка удаленной цели (Remote Logging Target)

Добавление удаленного Syslog-сервера:

Шаг 1. В веб-интерфейсе ISE перейдите в **Menu → Administration → System → Logging → Remote Logging Targets → Add** .

Шаг 2. Заполните параметры:

Параметры	Описание
Name	Уникальное имя цели (например, Remote_Kiwi_Syslog)
Target Type	Тип подключения: • **UDP Syslog** — быстрая, но ненадежная передача; • **TCP Syslog** — надежная передача с подтверждением; • **Secure Syslog** — TCP + TLS-шифрование.
Status	Выберите **Enabled**
Description	(Опционально) Краткое описание
Host / IP Address	IPv4/IPv6-адрес или FQDN Syslog-сервера
Port	Порт назначения (по умолчанию **514** для UDP). Диапазон: 1–65535
Facility Code	Код facility (например, LOCAL6). Доступны LOCAL0–LOCAL7
Maximum Length	Максимальная длина сообщения (по умолчанию 1024, максимум 8192 байт)
Include Alarms	Отправлять ли системные оповещения на этот сервер
Comply to RFC 3164	Не экранировать спецсимволы (`;, {`, `}, \ и др.)

При использовании FQDN:

- Если указано доменное имя, обязательно включите DNS-кэширование, иначе производительность ISE сильно упадет из-за частых DNS-запросов.
- Команда для включения кэширования на всех PSN: **ise/admin(config)# service cache enable hosts ttl 180** .

Шаг 3. Нажмите **Save**. Система предупредит: **«You have chosen to create an unsecure (TCP/UDP) connection...»** — подтвердите **Yes**.

Привязка удаленной цели к категориям логирования

После создания цели ее нужно назначить на нужные категории событий.

Поддерживаемые категории журналов:

- Генерируются только на PSN-узлах:
  - AAA Audit;
  - AAA Diagnostics;
  - Accounting;
  - External MDM;
  - Passive ID;
  - Posture and Client Provisioning Audit/Diagnostics;
  - Profiler.
- Генерируются на всех узлах:
  - Administrative and Operational Audit;
  - System Diagnostics;
  - System Statistics.

Назначение цели на категорию:

Шаг 1. Перейдите в раздел **Menu → Administration → System → Logging → Logging Categories** .

Шаг 2. Выберите нужную категорию (например, **Passed Authentications**, **Failed Attempts**, **Radius Accounting** или **Administrative and Operational Audit**).

Шаг 3. Настройте параметры:

- **Log Severity Level** — уровень важности журналов;
- **FATAL** — аварийная ситуация;
- **ERROR** — критическая ошибка;
- **WARN** — предупреждение (часто используется по умолчанию);
- **INFO** — информационное сообщение;
- **DEBUG** — отладочная информация;
- **Local Logging** — сохранять ли журналы локально на PSN (рекомендуется оставить включенным);
- **Targets** — переместите вашу удаленную цель (например, **Remote_Kiwi_Syslog**) из списка **Available** в **Selected** с помощью стрелок.

Шаг 4. Повторите шаги для других категорий (например, **Failed Attempts**, **Radius Accounting** и т.д.).

Шаг 5. Убедитесь, что ваша цель отображается в списке выбранных для каждой нужной категории.

Структура категорий логирования

Категории организованы иерархически. Пример:

Родительская категория	Дочерние категории
AAA Audit	• Passed Authentication • Failed Attempts
AAA Diagnostics	• Authentication Flow Diagnostics • Identity Store Diagnostics • Policy Diagnostics • Radius Diagnostics • Administrator Authentication and Authorization
Accounting	• Radius Accounting
Administrative and Operational Audit	(без дочерних)
Posture and Ckient Provisioning Audit	(без дочерних)
System Diagnostics	• Distributed Management • Internal Operations Diagnostics

Проверка и устранение неполадок

Для того чтобы убедиться, что журналы отправляются, используйте встроенный TCP Dump на узле PSN, который обрабатывает аутентификацию:

Шаг 1. Перейдите в раздел **Menu → Operations → Troubleshoot → TCP Dump → Add** .

Шаг 2. Укажите фильтр:

ip host <IP_адрес_вашего_syslog_сервера>

Шаг 3. Запустите захват на том PSN, где происходят события (например, вход пользователя).

В результатах вы увидите исходящий Syslog-трафик от ISE к вашему серверу.

Заключение

После выполнения этих шагов Cisco ISE будет корректно отправлять выбранные категории системных журналов на внешний Syslog-сервер. Это позволяет централизованно собирать, анализировать и архивировать данные аудита, диагностики и учетных записей для целей безопасности и соответствия требованиям.

ID статьи: 1554
Последнее обновление: 26 мар., 2026
Обновлено от: Михалева А.
Ревизия: 9
База знаний Логикор -> Документация -> Система хранения и обработки данных «Логикор». Версия 2.5.0 -> Логикор. Руководство разработчика -> Подключение источников событий в Логикор -> Настройка источников -> Настройка отправки журналов с устройства Cisco ISE
https://docs.axel.pro/entry/1554/