КИБЕРПРОТЕКТ

КИБЕР
Бэкап Облачный

Версия 26.03

Регистрация событий в частном облаке

Редакция: 24.07.2026

Оглавление

Введение

В настоящем документе описаны технические меры по регистрации событий информационной безопасности, а также событий, связанных с изменением конфигурации.

Регистрация событий

Кибер Бэкап Облачный поддерживает возможность передачи событий из журнала аудита в SIEM-систему. В Руководстве администратора компании приведены более подробные сведения о журнале аудита и инструкции по настройке отправления записей журнала аудита на удаленный Syslog-сервер. Перечень регистрируемых событий приведён в разделе *Регистрируемые события*.

> **Примечание**
>
> Регистрация событий Кибер Инфраструктуры не поддерживается.

На уровне операционной системы регистрация событий обеспечивается стандартным пакетом auditd для РЕД ОС. Правила устанавливаются в конфигурационном файле (см. *приложение*).

Для передачи данных в централизованное хранилище или SIEM-систему на виртуальных машинах настроен анализатор сетевых пакетов Auditbeat, который пересылает данные в СУБД Redis. Данные из неё получает серверный конвейер обработки данных Logstash, на уровне которого можно настроить правила выгрузки событий безопасности во внешнюю систему.

Например, для выгрузки событий во внешние системы по стандарту Syslog необходимо добавить в блок `output` конфигурации Logstash следующие строки:

```
if ”auditd” in [service][type] {
    udp {
        <параметры_подключения>
    }
}
```

Где `<параметры_подключения>` — это параметры подключения ко внешней системе по стандарту Syslog.

Регистрируемые события

В журнале аудита Кибер Бэкапа Облачного фиксируются события следующих категорий:

- оповещения;
- действия с планами защиты;
- действия с устройствами и их группами;
- аутентификация и авторизация;
- действия с тенантами;
- резервное копирование;
- лицензирование;
- регистрация агентов;
- действия с хранилищами;
- действия с архивами.

Более подробная информация о записываемых в журнал событиях приведена в таблицах далее.

События оповещений

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Оповещение создано (Alert created)	Информация (info)	Alert-Management	Alert	Имя ресурса	• Plan: имя (идентификатор) плана; • resource: имя (идентификатор) ресурса.	Service-Account	—	Создать (Create)	200	Имя отдела	<IP-адрес инициатора>:<порт>
Оповещение обновлено (Alert updated)	Информация (info)	Alert-Management	Alert	Имя ресурса	• Plan: имя (идентификатор) плана; • resource: имя (идентификатор) ресурса.	Service-Account	—	Обновить (Update)	200	Имя отдела	<IP-адрес инициатора>:<порт>
Оповещение отменено (Alert reset)[1]	Информация (info)	Alert-Management	Alert	Имя ресурса	• Plan: имя (идентификатор) плана; • resource: имя (идентификатор) ресурса.	Service-Account или user	Имя пользователя	Удалить (Delete)	204	Имя отдела	<IP-адрес инициатора>:<порт>

События действий с планами защиты

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
План защиты создан (Backup plan created)	Информация (info)	Policy-Management	Policy	Имя плана	Location: имя хранилища	User	Имя пользователя	Создать (Create)	20x	Имя тенанта	<IP-адрес инициатора>:<порт>
План защиты обновлён (Backup plan updated)	Информация (info)	Policy-Management	Policy	Имя плана	• Resource: имя (идентификатор) ресурса; • location: имя хранилища.	User	Имя пользователя	Обновить (Update)	20x	Имя тенанта	<IP-адрес инициатора>:<порт>
План защиты удалён (Backup plan deleted)	Информация (info)	Policy-Management	Policy	Имя плана	• Resource: имя (идентификатор) ресурса; • location: имя хранилища.	User	Имя пользователя	Удалить (Delete)	204	Имя тенанта	<IP-адрес инициатора>:<порт>

(продолжается на следующей странице)

[1] При использовании массового действия с оповещениями, например, **Очистить всё**, для каждого оповещения будет создана отдельная запись в журнале аудита.

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Статус установки плана (Plan deployment state)	Информация (info)	Policy-Management	Policy	Имя плана	• Location: имя хранилища; • Deployment-State : идентификатор статуса.	User	—	Применить (Apply)	200	Имя пользователя[2]	—
Политика применена к устройству (Policy applied to workload)	Информация (info)	Policy-Management	Policy-Application	Имя плана	• Resource: имя (идентификатор) ресурса; • location: имя хранилища.	User	Имя пользователя	Обновить (Update)	20x	Имя тенанта	<IP-адрес инициатора>:<порт>

[2] Если действие выполняется на уровне тенанта типа **Клиент**, то в поле **Имя тенанта** будет указано имя учётной записи администратора отдела.

События действий с устройствами и их группами

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Устройство создано (Workload created)	Информация (info)	Workload-Management	Workload	Имя ресурса	Agent: имя (идентификатор) агента	User	—	Создать (Create)	200	Имя пользователя	—
Устройство обновлено (Workload updated)	Информация (info)	Workload-Management	Workload	Имя ресурса	Agent: имя (идентификатор) агента	User	—	Обновить (Update)	200	Имя пользователя	—
Устройство удалено (Workload deleted)	Информация (info)	Workload-Management	Workload	Имя ресурса	Agent: имя (идентификатор) агента	User	—	Удалить (Delete)	200	Имя пользователя	—
Группа устройств создана (Workload group created)	Информация (info)	Workload-Management	Group-Membership	Имя группы	Нет	User	Имя пользователя	Создать (Create)	201	Имя тенанта	<IP-адрес инициатора>:<порт>

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Участники добавлены в статическую группу устройств (Workload static group member added)	Информация (info)	Workload-Management	Group-Membership	Имя группы	Resource: имя (идентификатор) ресурса	User	—	Добавить (Add)	200	Имя тенанта	—
Участники добавлены в динамическую группу устройств (Workload dynamic group member added)	Информация (info)	Workload-Management	Group-Membership	Имя группы	Resource: имя (идентификатор) ресурса	User	—	Добавить (Add)	200	Имя тенанта	—
Участники удалены из статической группы устройств (Workload static group member removed)	Информация (info)	Workload-Management	Group-Membership	Имя группы	Resource: имя (идентификатор) ресурса	User	—	Удалить (Remove)	200	Имя тенанта	—

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Участники удалены из динамической группы устройств (Workload dynamic group member removed)	Информация (info)	Workload-Management	Group-Membership	Имя группы	Resource: имя (идентификатор) ресурса	User	—	Удалить (Remove)	200	Имя тенанта	—
Группа устройств удалена (Workload group deleted)	Информация (info)	Workload-Management	Group-Membership	Имя группы	Нет	User	Имя пользователя	Удалить (Delete)	200	Имя тенанта	<IP-адрес инициатора>:<порт>

События аутентификации и авторизации

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Успешный вход в систему (Logged in)	Информация (info)	Auth	Session	Имя пользователя	User: имя (идентификатор) пользователя	User	Имя пользователя	Вход в систему (Login)	200	Имя учётной записи	IP-адрес машины, с которой был выполнен вход
Превышено число попыток войти в систему (Exceeded the number of login attempts)	Критично (critical)	Auth	Session	Имя пользователя	User: имя (идентификатор) пользователя	Service-Account	Имя пользователя	Вход в систему временно заблокирован (Login::-Temporary-Lock)	429	Имя тенанта, имя отдела	IP-адрес машины, с которой был выполнен вход
Успешный выход из системы (Logged out)	Информация (info)	Auth	Session	Имя пользователя	User: имя (идентификатор) пользователя	User	Имя пользователя	Выход из системы (Logout)	200	Имя учётной записи	IP-адрес машины, с которой был выполнен выход

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Документ был подписан (Legal document signed)	Информация (info)	Auth	Legal-Document	—	User: имя (идентификатор) пользователя	User	Имя пользователя	Подписать (Sign)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Токен доступа выписан (Access token issued)	Информация (info)	Auth	Token	—	User: имя (идентификатор) пользователя	Service-Account	—	Выписать (Issue)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие

События действий с тенантами

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Тенант создан (Tenant created)	Информация (info)	IAM	Tenant	Имя созданного тенанта	Нет	User	Имя пользователя	Создать (Create)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Тенант обновлён (Tenant updated) (При обновлении тенанта типа **Клиент**).	Информация (info)	IAM	Tenant	Имя обновлённого тенанта	Нет	User	Имя пользователя	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Тенант обновлён (Tenant updated) (При обновлении родительского тенанта).	Информация (info)	IAM	Tenant	Имя обновлённого тенанта	User: имя пользователя	User	—	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Тенант обновлён (Tenant updated) (При обновлении имени тенанта или при включении тенанта).	Информация (info)	IAM	Tenant	Имя обновлённого тенанта	Нет	User	Имя пользователя	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Тенант отключён (Tenant disabled)	Предупреждение (warning)	IAM	Tenant	Имя обновлённого тенанта	Нет	User	Имя пользователя	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Тенант удалён (Tenant deleted)	Предупреждение (warning)	IAM	Tenant	Имя удалённого тенанта	Нет	User	Имя пользователя	Удалить (Delete)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Изменение привилегий пользователя (User privileges updated) (При назначении привилегий пользователю).	Информация (info)	IAM	UserPrivileges	—	User: имя (идентификатор) пользователя, для которого назначаются привилегии	User	Имя пользователя, совершившего действие	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Изменение привилегий пользователя (User privileges updated) (При отзыве привилегий пользователя).	Информация (info)	IAM	UserPrivileges	—	User: имя (идентификатор) пользователя, у которого отзываются привилегии	User	Имя пользователя, совершившего действие	Обновить (Update)	200	Имя пользователя	IP-адрес машины, с которой было совершено действие

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Учётная запись пользователя создана (User created)	Информация (info)	IAM	User	Имя пользователя	Нет	User	Имя пользователя	Создать (Create)	200	Имя пользователя	IP-адрес машины, с которой было совершено действие
Учётная запись пользователя обновлена (User updated)	Информация (info)	IAM	User	Имя (логин) обновлённого пользователя	Нет	User	Имя пользователя	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Учётная запись пользователя отключена (User disabled)	Предупреждение (warning)	IAM	User	Имя обновлённого пользователя	Нет	User	Имя пользователя	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Учётная запись пользователя включена (User enabled)	Предупреждение (warning)	IAM	User	Имя изменённого пользователя	Нет	User	Имя пользователя, совершившего действие	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Пароль сброшен (User reset)	Предупреждение (warning)	IAM	User	Имя обновлённого пользователя	Нет	User	Имя пользователя	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Учётная запись пользователя удалена (User deleted)	Критично (critical)	IAM	User	Имя пользователя	Нет	User	Имя пользователя	Удалить (Delete)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Служебная учётная запись создана (Account created) (При работе с API-клиентами).	Информация (info)	IAM	Service-Account	Имя API-клиента	Нет	User	Имя пользователя	Создать (Create)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Служебная учётная запись обновлена (Account updated) (При работе с API-клиентами).	Информация (info)	IAM	Service-Account	Имя API-клиента	Нет	User	Имя пользователя	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Служебная учётная запись удалена (Account deleted) (При работе с API-клиентами).	Информация (info)	IAM	Service-Account	Имя API-клиента	Нет	User	Имя пользователя	Удалить (Delete)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Секрет служебной учётной записи сброшен (Account secret reset) (При работе с API-клиентами).	Информация (info)	IAM	Service-Account	Имя API-клиента	Нет	User	Имя пользователя	Сбросить (Reset)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Юридический документ добавлен (Legal document created) (При работе с лицензионными документами).	Информация (info)	Auth	Legal-Document	Версия документа (например, Version 2024-04-03)	Нет	User	Имя пользователя	Создать (Create)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Юридический документ опубликован (Legal document published) (При работе с лицензионными документами).	Информация (info)	Auth	Legal-Document	Версия документа (например, Version 2024-04-03)	Нет	User	Имя пользователя	Опубликовать (Publish)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Юридический документ удалён (Legal document deleted) (При работе с лицензионными документами).	Информация (info)	Auth	Legal-Document	Версия документа (например, Version 2024-04-03)	Нет	User	Имя пользователя	Удалить (Delete)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Документ был подписан (Legal document signed) (При работе с лицензионными документами).	Информация (info)	Auth	Legal-Document	Версия документа (например, Version 2024-04-03)	Нет	User	Имя пользователя	Подписать (Sign)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Служба добавлена для тенанта (Service added for tenant) При добавлении функциональности Кибер Инфраструктуры.	Информация (info)	License-Management	Application	Cyber Infrastructure	Нет	User	Имя пользователя	Включение (Enable)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Служба удалена для тенанта (Service removed from tenant) При отключении функциональности Кибер Инфраструктуры.	Информация (info)	License-Management	Application	Cyber Infrastructure	Нет	User	Имя пользователя	Отключение (Disable)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Служба добавлена для тенанта (Service added for tenant) При включении у тенанта прочих консолей (Cyber Protection).	Информация (info)	License-Management	Application	Cyber Protection	Нет	User	Имя пользователя	Включение (Enable)	200	Имя тенанта	IP-адрес машины, с которой было совершено
Служба удалена для тенанта (Service removed from tenant) При отключении у тенанта прочих консолей (Cyber Protection).	Информация (info)	License-Management	Application	Cyber Protection	Нет	User	Имя пользователя	Отключение (Disable)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие

События резервного копирования

Примечание

IP-адрес инициатора отсутствует.

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант
Резервное копирование помещено в очередь (Backup queued)	Информация (info)	Task-Management	Task	Имя ресурса	• Plan: имя (идентификатор) плана; • resource: имя (идентификатор) ресурса.	Service-Account или User	• Имя пользователя, если тип инициатора — **User**; • '-', если тип инициатора — **ServiceAccount**.	Создать (Create)	200	Имя пользователя

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант
Резервное копирование назначено агенту (Backup assigned to agent)	Информация (info)	Task-Management	Task	Имя ресурса	• Plan: имя (идентификатор) плана; • resource: имя (идентификатор) ресурса.	Service-Account или User	• Имя пользователя, если тип инициатора — **User**; • '-', если тип инициатора — **ServiceAccount**.	Назначить (Assign)	200	Имя пользователя
Ошибка при назначении резервного копирования агенту (Error assigning backup to agent)	Критично (critical)[3]	Task-Management	Task	Имя ресурса	• Plan: имя (идентификатор) плана; • resource: имя (идентификатор) ресурса.	Service-Account или User	• Имя пользователя, если тип инициатора — **User**; • '-', если тип инициатора — **ServiceAccount**.	Назначить (Assign)	500	Имя пользователя

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант
Резервное копирование начато (Backup started)	Информация (info)	Task-Management	Task	Имя ресурса	• Plan: имя (идентификатор) плана; • resource: имя (идентификатор) ресурса.	Service-Account или User	• Имя пользователя, если тип инициатора — **User**; • '-', если тип инициатора — **ServiceAccount**.	Начать (Start)	200	Имя пользователя
Резервное копирование выполнено (Backup completed)	Информация (info)	Task-Management	Task	Имя ресурса	• Plan: имя (идентификатор) плана; • resource: имя (идентификатор) ресурса.	Service-Account или User	• Имя пользователя, если тип инициатора — **User**; • '-', если тип инициатора — **ServiceAccount**.	Завершить (Complete)	200	Имя пользователя

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант
Резервное копирование завершилось с предупреждением (Backup finished with warning)	Предупреждение (warning)[c. 26, 3]	Task-Management	Task	Имя ресурса	• Plan: имя (идентификатор) плана; • resource: имя (идентификатор) ресурса.	Service-Account или User	• Имя пользователя, если тип инициатора — **User**; • '-', если тип инициатора — **ServiceAccount**.	Завершить (Complete)	200	Имя пользователя
Резервное копирование завершилось с ошибкой (Backup failed)	Критично (critical)[c. 26, 3]	Task-Management	Task	Имя ресурса	• Plan: имя (идентификатор) плана; • resource: имя (идентификатор) ресурса.	Service-Account или User	• Имя пользователя, если тип инициатора — **User**; • '-', если тип инициатора — **ServiceAccount**.	Завершить (Complete)	500	Имя пользователя

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант
Задача на восстановление создана (Recovery task created)	Информация (info)	Task-Management	Activity	Имя ресурса	• Plan: имя (идентификатор) плана; • resource: имя (идентификатор) ресурса.	User	Имя пользователя	Создать (Create)	200	Имя пользователя
Задача на восстановление запущена (Recovery task started)	Информация (info)	Task-Management	Activity	Имя ресурса	• Plan: имя (идентификатор) плана; • resource: имя (идентификатор) ресурса.	User	Имя пользователя	Начать (Start)	200	Имя пользователя
Задача на восстановление выполнена (Recovery task completed)	Информация (info)	Task-Management	Activity	Имя ресурса	• Plan: имя (идентификатор) плана; • resource: имя (идентификатор) ресурса.	User	Имя пользователя	Завершать (Complete)	200	Имя пользователя

[3] Серьёзность зависит от кода задачи: если она завершена с кодом **warning**, то Серьёзность — **предупреждение** (**warning**); если с кодом **error**, то Серьёзность — **критично** (**critical**).

События лицензирования

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Лицензия для тенанта включена (Tenant license enabled)	Информация (info)	License-Management	Offering-ItemCount	pw_pack... или pg_pack...	Нет	User	Имя тенанта	Создать (Create)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Лицензия для тенанта включена (Tenant license enabled)	Информация (info)	License-Management	Offering-ItemCount	local_-storage	Нет	User	Имя тенанта	Создать (Create)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие
Успешное выключение лицензии для тенанта (Tenant license disabled)	Предупреждение (warning)	License-Management	Offering-ItemCount	pw_pack... или pg_pack...	Нет	User	Имя пользователя	Удалить (Delete)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Квота для тенанта установлена (Tenant quota set)	Информация (info)	License-Management	Tenant-Quota	pw_base... или pg_base...	• Applica-tion : идентификатор приложения; • tenant: имя (идентификатор) тенанта.	User	Имя тенанта	Обновить (Update)	200	Имя тенанта	IP-адрес машины, с которой было совершено действие

События регистрации агентов

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Регистрация агента завершена (Agent registered)	Информация (info)	Software-Management	Agent	Имя агента (имя хоста)	Нет	Service-Account	—	Зарегистрировать (Register)	200	Имя отдела, в котором регистрируется агент	IP-адрес машины с агентом
Регистрация агента отозвана (Agent unregistered) (При удалении агента с помощью интерфейса командной строки).	Информация (info)	Software-Management	Agent	Имя агента (имя хоста)	Нет	Service-Account	—	Отменить регистрацию (Unregister)	200	Имя отдела, в котором отменяется регистрация агента	IP-адрес машины с агентом

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Связанные объекты	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Регистрация агента отозвана (Agent unregistered) (При удалении агента с помощью консоли службы).	Информация (info)	Software-Management	Agent	Имя агента (имя хоста)	Нет	User	Имя пользователя, инициировавшего удаление	Отменить регистрацию (Unregister)	200	Имя отдела, в котором отменяется регистрация агента	IP-адрес машины с агентом

События действий с хранилищами

Примечание

Связанные объекты отсутствуют.

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Хранилище создано (Storage created)	Информация (info)	Vault-Management	Vault	Имя хранилища	Service-Account	—	Создать (Create)	200	Имя пользователя	IP-адрес сервера управления
Хранилище обновлено (Storage updated)	Информация (info)	Vault-Management	Vault	Имя хранилища	User или Service-Account	• Имя пользователя, если тип инициатора — **User**; • '-', если тип инициатора — **ServiceAccount**.	Обновить (Update)	200	Имя пользователя	IP-адрес сервера управления
Хранилище удалено (Storage deleted)	Информация (info)	Vault-Management	Vault	Имя хранилища	Service-Account	—	Удалить (Delete)	200	Название тенанта	IP-адрес сервера управления

События действий с архивами

Примечание

Связанные объекты отсутствуют.

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Архив создан (Archive created)	Информация (info)	Archive-Management	Archive	Имя файла резервной копии	Service-Account	—	Создать (Create)	200	Имя пользователя	IP-адрес сервера управления
Архив обновлён (Archive updated)	Информация (info)	Archive-Management	Archive	Имя файла резервной копии	User или Service-Account	• Имя пользователя, если тип инициатора — **User**; • '-', если тип инициатора — **ServiceAccount**.	Обновить (Update)	200	Имя пользователя	IP-адрес сервера управления
Архив удалён (Archive deleted)	Информация (info)	Archive-Management	Archive	Имя файла резервной копии	Service-Account	—	Удалить (Delete)	200	Название тенанта	IP-адрес сервера управления
Точка восстановления создана (Recovery point created)	Информация (info)	Archive-Management	Recovery-Point	Имя точки восстановления (см. далее)	Service-Account	—	Удалить (Delete)	200	Название тенанта	IP-адрес сервера управления

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Категория (домен)	Тип объекта события	Название объекта	Тип инициатора	Инициатор события	Действие	Результат действия	Тенант	IP-адрес инициатора
Точка восстановления удалена (Recovery point deleted)	Информация (info)	Archive-Management	Recovery-Point	Имя точки восстановления (см. далее)	Service-Account	—	Удалить (Delete)	200	Название тенанта	IP-адрес сервера управления

Имя точки восстановления задаётся в формате `<ГГГГ>-<ММ>-<ДД> <чч>:<мм>:<сс> <смещение> UTC`.

В этом выражении:

- `<ГГГГ>` — год четырьмя цифрами (например, `2026`).
- `<ММ>` — месяц двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, `06`).
- `<ДД>` — день двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, `02`).
- `<чч>` — часы двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, `09`).
- `<мм>` — минуты двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, `07`).
- `<сс>` — секунды двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, `05`).
- `<смещение>` — смещение времени относительно UTC (например, `+0000`).

Пример: `2026-06-02 09:07:05 +0000 UTC`.

Описание формата сообщений Syslog

Сообщения CEF (RFC 3164)

Сообщение состоит из Syslog-заголовка (Syslog RFC 3164 header) и CEF-сообщения (CEF msg) и имеет следующую структуру:

```
<PRI> TIMESTAMP HOSTNAME TAG: CEF:Version|Device Vendor|Device Product|Device Version|Device
↪Event Class Id|Name|Severity|[Extension]
```

Ниже приведено описание компонентов сообщения.

К Syslog-заголовку относятся:

- `<PRI>` — приоритет сообщения, значение которого определяется формулой:

  ```
  <PRI> = <Facility> x 8 + <Severity>
  ```

  Где:

  - `<Facility>` — параметр, который может принимать следующие значения:

Значение	Назначение
0	Kernel
1	User-level
2	Mail
3	Daemon
4	Security
5	Syslog
6	Printer
7	News
16—23	Local0—local7 (прикладное ПО)

  - `<Severity>` — параметр, который может принимать следующие значения:

Значение	Уровень	Условия использования
0	Emergency	Аварийное состояние
1	Alert	Необходимо срочное вмешательство
2	Critical	Критическая ошибка
3	Error	Ошибка

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Значение	Уровень	Условия использования
4	Warning	Предупреждение
5	Notice	Значимое событие
6	Info	Информационное сообщение
7	Debug	Отладочная информация

Например, если `<Facility>` = 16 (local0), `<Severity>` = 6 (info), то `<PRI>` = `<Facility>` x 8 + `<Severity>` = 16 x 8 + 6 = 134.

- `TIMESTAMP` — временная метка в формате BSD без указания года и часового пояса, имеющая вид: `<MMM> <ДД> <чч>:<мм>:<сс>`.

  В этом выражении:

  - `<MMM>` — первые три буквы названия месяца на английском языке, первая буква является заглавной.
  - `<ДД>` — день месяца одной или двумя цифрами. Если значение меньше 10, то день отделяется от месяца двумя пробелами, при этом ноль перед днём месяца не указывается.
  - `<чч>` — часы двумя цифрами (если значение меньше 10, то перед ним указывается ноль).
  - `<мм>` — минуты двумя цифрами (если значение меньше 10, то перед ним указывается ноль).
  - `<сс>` — секунды двумя цифрами (если значение меньше 10, то перед ним указывается ноль).

  Примеры значений `TIMESTAMP`: `Jan 29 03:09:27`, `Nov 7 11:15:17`.

- `HOSTNAME` — имя хоста (например, `cp1`).
- `TAG` — источник процесса. В его качестве может быть `app[pid]` (например, `event-store[3924]`).

> **Примечание**
>
> После `TAG` обязательно двоеточие.

К CEF-сообщению относятся:

- `CEF:Version` — номер версии формата CEF (например, `CEF:1`).
- `Device Vendor` — вендор продукта (например, `Cyberprotect`).
- `Device Product` — название продукта (например, `CyberBackupCloud`).
- `Device Version` — версия продукта (например, `18.5`).

- `Device Event Class Id` — идентификатор типа события (например, `BackupStart`).
- `Name` — название события в человекочитаемом формате (например, `Backup job started`).
- `Severity` — параметр `CEF-severity`, принимающий значения, приведённые в таблице.

Значение	Уровень серьёзности
0—3	Low
4—6	Medium
7—8	High
9—10	Critical

- `[Extension]` (необязательно) — параметры сообщения в формате `key=value` (например, `src=10.0.0.1 dst=10.0.0.5 suser=admin msg=Backup started`).

  Более подробное описание параметров сообщений приведено в документе Implementing ArcSight Common Event Format (CEF).

Пример сообщения:

```
<134> Feb 24 06:31:14 dev01-cloud-event-store-744996bf97-5sp5r event-store[1]:¬
↪CEF:1|Cyberprotect|CyberBackupCloud|25.11|Session|Logged in|3|cat=Command flexString1=2c448d4d-
↪876d-432f-ab2d-e1e2973a76c5 flexString1Label=eventTenantUUID flexString2=S_admin¬
↪flexString2Label=eventTenantName src= requestClientApplication= act=Login cn1=200¬
↪cn1Label=eventStatus end=2026-02-24 06:31:14.376999 +0000 UTC outcome=success msg=Logged in¬
↪dvc= dvchost=dev01-cloud-event-store-744996bf97-5sp5r dvcExternalId= reportedResourceID=¬
↪reportedResourceName=user cs6=Auth cs6Label=objectDomain reportedResourceType=Session cs4=¬
↪cs4Label=objectSubtype dst= cs7=00000000-0000-0000-0000-000000000000 cs7Label=localityID¬
↪sourceServiceName=management suid=d7638075-ad65-4378-83a5-d32d568453bb cs3=User¬
↪cs3Label=principalType suser=user spid=00000000-0000-0000-0000-000000000000 cs1=¬
↪cs1Label=oldValue cs2= cs2Label=newValue cs5= cs5Label=changedField
```

Сообщения Syslog (RFC 5424)

Сообщение Syslog (SYSLOG-MSG) состоит из заголовка (header), параметров сообщения (structured-data) и самого сообщения (MSG). Оно имеет следующую структуру:

```
HEADER STRUCTURED-DATA MSG
```

Где:

- `HEADER` — компонент, включающий в себя:
  - `<PRI>` — приоритет сообщения, значение которого определяется формулой:

```
<PRI> = <Facility> x 8 + <Severity>
```

В этом выражении:

- `<Facility>` — параметр, который может принимать следующие значения:

Значение	Назначение
0	Kernel
1	User-level
2	Mail
3	Daemon
4	Security
5	Syslog
6	Printer
7	News
16—23	Local0—local7 (прикладное ПО)

- `<Severity>` — параметр, который может принимать следующие значения:

Значение	Уровень	Условия использования
0	Emergency	Аварийное состояние
1	Alert	Необходимо срочное вмешательство
2	Critical	Критическая ошибка
3	Error	Ошибка
4	Warning	Предупреждение
5	Notice	Значимое событие
6	Info	Информационное сообщение
7	Debug	Отладочная информация

- `VERSION` — версия (например, `1`).
- `TIMESTAMP` — временная метка в соответствии с RFC3339 или ISO 8601, имеющая вид: `<ГГГГ>-<ММ>-<ДД>T<чч>:<мм>:<сс><ЧАСОВОЙ ПОЯС>`.

  Где:

  - `<ГГГГ>` — год четырьмя цифрами (например, `2026`).
  - `<ММ>` — месяц двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, `01`).
  - `<ДД>` — день месяца двумя цифрами; если значение меньше 10, то перед ним указывается

ноль (например, `02`).

- `T` — разделитель времени.
- `<чч>` — часы двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, `03`).
- `<мм>` — минуты двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, `04`).
- `<сс>` — секунды двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, `05`).
- `<ЧАСОВОЙ ПОЯС>` — смещение времени, которое может быть указано в виде символа `Z` (для формата UTC) или в виде `±<чч>:<мм>` (например, `+03:00` или `-02:00`).

Примеры значений `TIMESTAMP`:

- `2026-01-29T03:09:23-08:00`;
- `2026-01-29T11:09:23Z`.

- `HOSTNAME` — имя узла (например, `cp1`).
- `APP-NAME` — название приложения (например, `CyberBackupCloud`).
- `PROCID` — идентификатор процесса (PID), например, `3924`.
- `MSGID` — тип или идентификатор события (например, `BackupStarted`).

- `STRUCTURED-DATA` — параметры события в формате `key=value` (например, `[backup@32473 job="daily" status="started"]`).

> **Примечание**
>
> Параметры определяются на уровне приложения.

Описание полей Syslog-сообщений приведено в таблице.

Категория	Ключ	SourceField	Описание
event	id	event.ID	Уникальный идентификатор события
event	category	event.Category	Категория события
event	version	event.Version	Версия
event	tenant_id	event.TenantUUID	Идентификатор тенанта
event	tracing_id	event.TracingUUID	Идентификатор трассировки
event	src_ip	event.SrcIP	IP-адрес инициатора действия

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Категория	Ключ	SourceField	Описание
event	dst_ip	event.DstIP	IP-адрес цели воздействия
event	user_agent	event.UserAgent	User-Agent клиента или приложения, выполнившего запрос
event	status	event.Status	Статус
object	id	object.ID	Уникальный идентификатор объекта
object	name	object.Name	Имя объекта в человекочитаемом формате
object	domain	object.Domain	Логический домен или пространство объекта
object	type	object.Type	Тип объекта
object	subtype	object.Subtype	Подтип и уточняющая классификация объекта
object	expr	object.Expr	Выражение, условие или фильтр, описывающие объект или набор объектов
object	scope_path	object.ScopePath	Расположение объекта в структуре
object	scope_expr	object.ScopeExpr	Выражение области действия (scope), определяющее группу объектов
principal	id	principal.ID	Уникальный идентификатор субъекта
principal	type	principal.Type	Тип субъекта (пользователь, сервис, роль и т. п.)
principal	name	principal.Name	Имя или логин субъекта
principal	session	principal.SessionUUID	Идентификатор сессии субъекта
locality	id	locality.ID	Идентификатор узла или локации выполнения события
locality	type	locality.Type	Тип локации (агент, сервер, кластер, узел и т. п.)
locality	version	locality.Version	Версия ПО или компонента, где произошло событие

- `HEADER` — описание события в человекочитаемом формате (например, `Backup started`).

Пример сообщения:

```
<134>1 2026-07-22T08:28:09Z test_hostname CyberBackupCloud 1 703711 [event category="Command" dst_
↪ip="" id="012f34f5-6a7f-8cf9-a012-ba34567db890" src_ip="1.1.1.1" status="200" tenant_id=
↪"1cbb23e4-5678-90ef-a123-ef4567ad890b" tracing_id="2e34d5e6-7890-1234-56f7-ca8bd90eab1a" user_
↪agent="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
↪150.0.0.0 Safari/537.36" version="1"][locality id="00000000-0000-0000-0000-000000000000" type=
↪"management" version=""][object domain="Auth" expr="" id="" name="root1" scope_expr="" scope_
↪path="" subtype="" type="Session"][principal id="a45f6789-ce0d-123c-45c6-789012345678" name=
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
↪"root1" session="00000000-0000-0000-0000-000000000000" type="User"] Session.Login.200
```

Приложение 1. Применяемые правила аудита

Правила доступны по ссылке.