

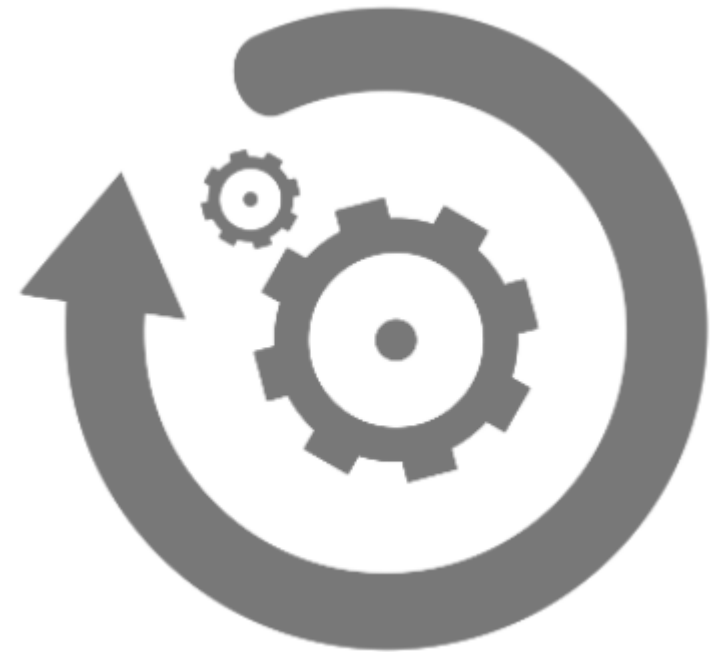
Система анализа и мониторинга состояния ИБ DATARK

Тема 8. Обновление. Диагностика и устранение
неисправностей

Обновление ПО DATARK

Обновление ПО DATARK – процесс установки более свежей версии DATARK.

В новых версиях продукта добавляются новые функции, устраняются ошибки функционирования.



Выход новых релизов

О выпуске новых релизов DATAPK производитель уведомляет по электронной почте ответственных лиц.

Новая версия DATAPK выкладывается на файловый ресурс (tar-архив, документация, правила обнаружения вторжений, корреляции, сканеры сбора данных, базы уязвимостей...).

Обновления контента (правила обнаружения вторжений, корреляции, сканеры сбора, базы уязвимостей) выкладываются чаще (ориентировочно раз в месяц).

Интеграторы/заказчики принимают решения об обновлении на новую версию. При необходимости макетируют обновление на стендах.

Вместе с релизом DATAPK предоставляется пошаговая инструкция по обновлению в составе документации.



Nextcloud

Частота обновлений

Мажорная версия (3.0, 3.1, ...) выпускается ориентировочно 1 раз в полгода. В данной версии **добавляется новый функционал**.

Выпуск **минорных версий** м.б. чаще. В данных версиях **не меняется API, однако содержатся исправления ошибок и потенциальных уязвимостей** (в редких случаях добавляется небольшой функционал).



Поддержка разных версий ПО

Поддержка мажорной версии DATAPK осуществляется в течении 1 года с момента выпуска. В дальнейшем необходимо произвести обновление до актуальной версии ПО.

Более старые версии поддерживаются ограниченно. В случае архитектурных проблем, решенных в более новых версиях, будет рекомендовано обновление. Выпуск исправлений программного кода производиться не будет.

Поддержка сертифицированной версии DATAPK осуществляется дольше 1 года (либо до внесения изменений в сертифицированный дистрибутив).



Поддержка разных версий ПО

В линейке **1.x** поддерживаемая версия на сегодня 1.19.0.4 (остальные на ограниченной поддержке). Версия 1.x в новые инсталляции **не продается** (в старые инсталляции для дооснащения – **решается индивидуально**). В любом случае нужно **менять узловую ОС**, актуализировать набор лицензий.

В линейке **3.x** – актуальная сертифицированная версия 3.0.0.0 (в конце марта-апреле ожидается релиз 3.1.0.0, который не планируется сертифицировать).

Обновления Альт СП предоставляются Базальт СПО – производитель DATAPK может только порекомендовать обновления, т.к. DATAPK базируется на пакетной базе Альт СП (но не предоставляет Альт СП).



Процесс обновления

Общий процесс обновления:

- Разослать обновления (скопировать на все DATAPK дистрибутивы) + подключить репозитории Альт СП
- Сделать актуальные резервные копии
- Обновить уровень Supervision (при наличии)
- Обновить уровень Management
- Обновить подключенные к нему уровни Sensor
- Аналогично для остальных Managements/Sensors

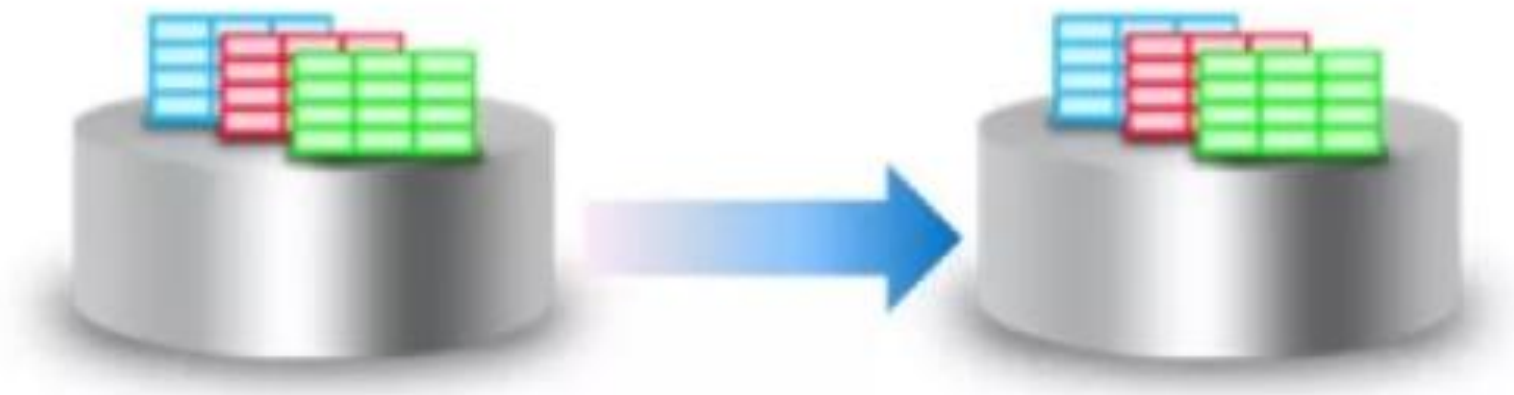
Миграция данных

Миграция данных – изменение структуры базы данных от одной версии к другой.

В DATAPK 3.x миграции происходят автоматически при обновлении.

В нагруженных инсталляциях миграции данных могут занимать продолжительное время. Во время проведения миграций нельзя останавливать и перезапускать DATAPK.

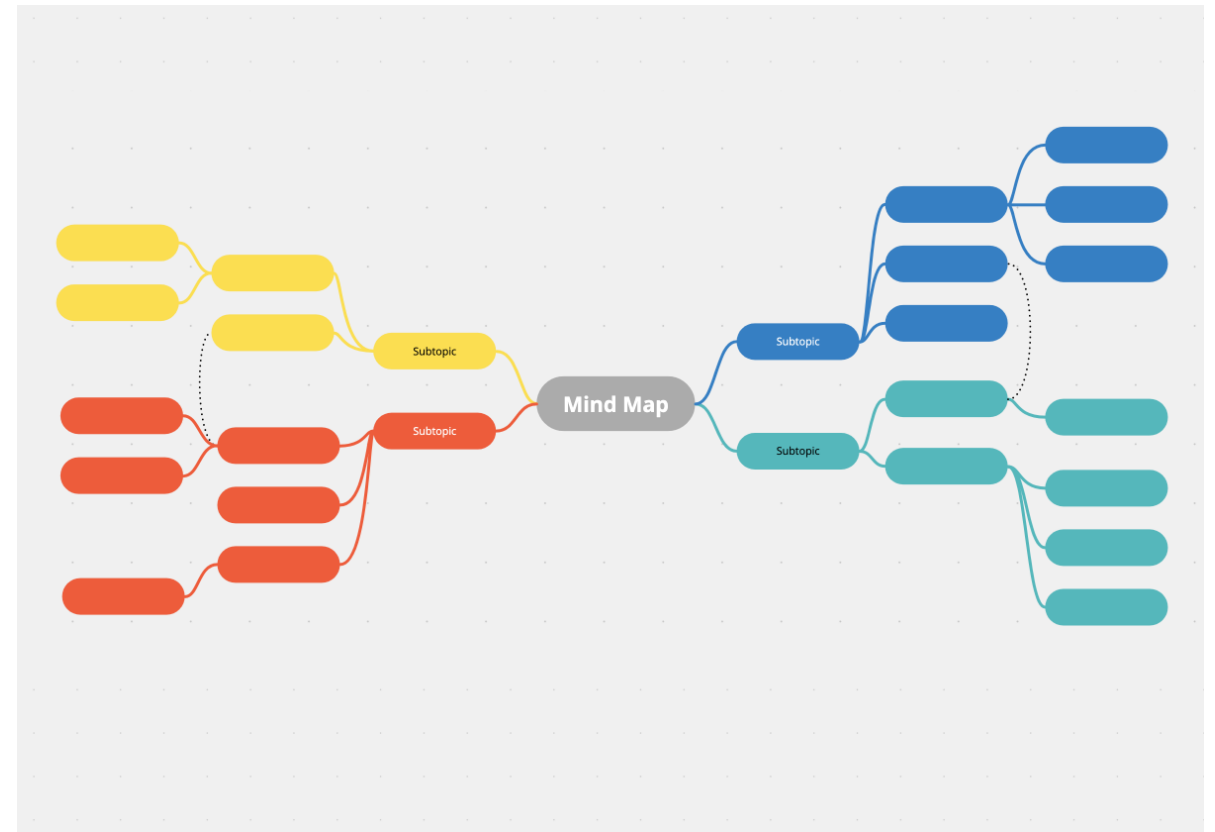
Перенос данных с релизов 1.x до 3.x возможен в ручном режиме (инструкции предоставляются по запросу).



Прочие неисправности

Типовые категории неисправностей были рассмотрены в предыдущих темах, а также частично смоделированы в ходе лабораторных работ.

Так же ряд неисправностей описан в документации на ПО DATAPK.



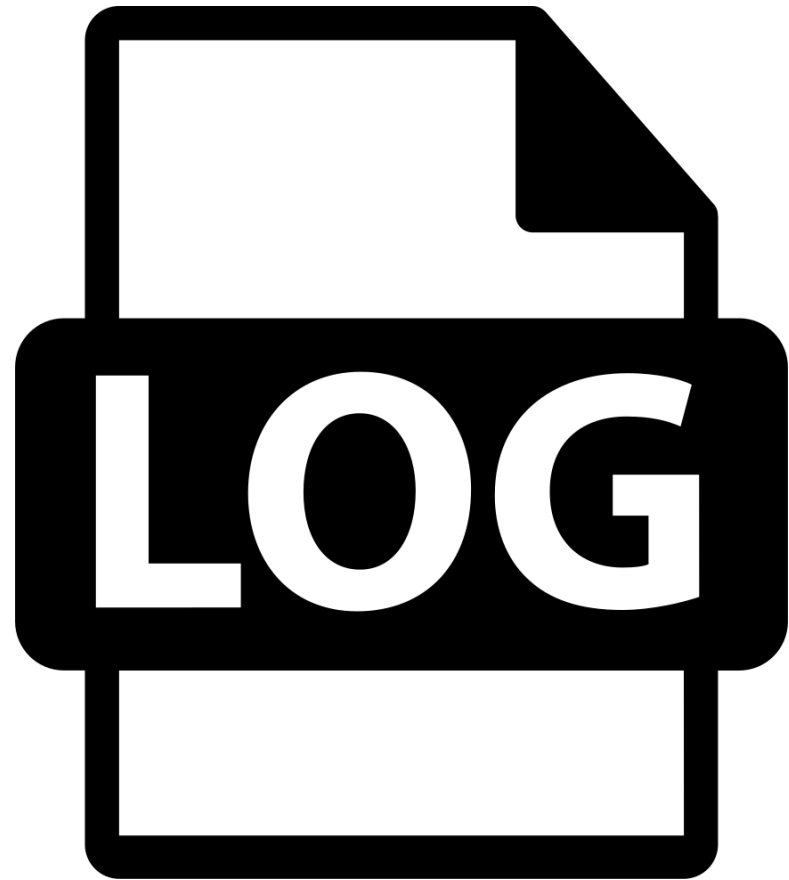
Сбор и анализ логов

Для сбора логов сервисов необходимо использовать команду **journalctl** с указанием сервиса, для которого планируется просмотр и анализ отладочных сообщений. Так же временно можно повышать уровень логирования сервисов (на постоянку не рекомендуется оставлять debug-режим – большая нагрузка на ОС)

Для централизованного сбора логов можно воспользоваться поставляемым производителем DATAPK скриптом **dtpk_get_logs-3_o.bash**.

Данный скрипт:

- собирает логи всех сервисов за указанный в аргументе период;
- собирает общие сведения о системе (свободное место, настройки сетевых интерфейсов, ...)
- формирует каталог **logs-hostname-date + tar.gz архив** с собранными данными в структурированном виде.



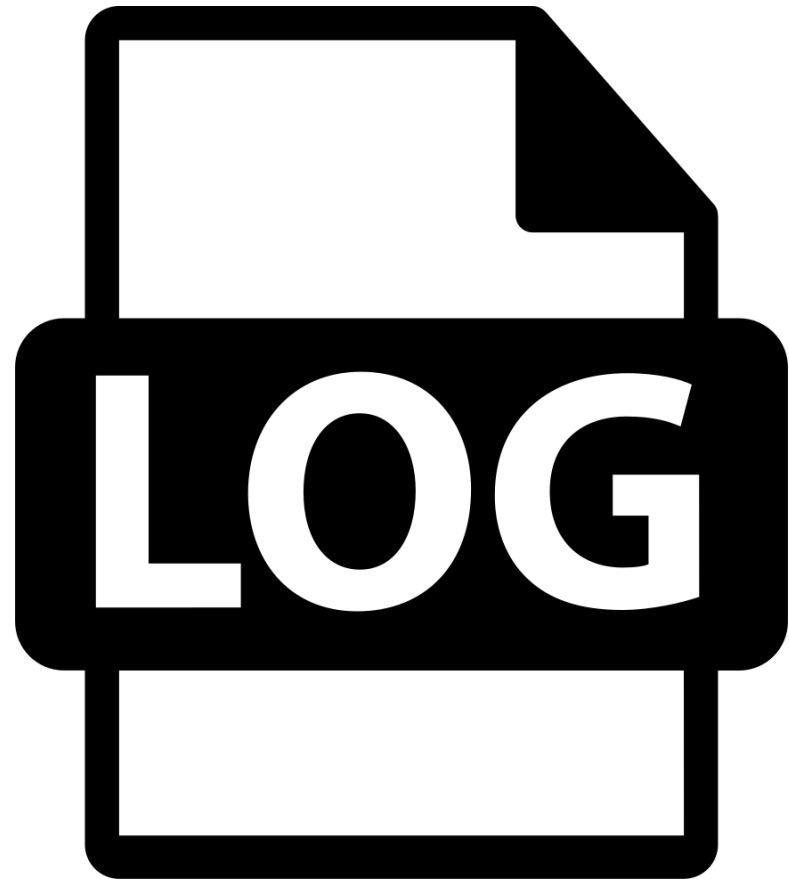
Сбор и анализ логов

Данный каталог в виде архива рекомендуется прикладывать к сервисным запросам на техподдержку. Запуск скрипта необходимо делать при запущенном DATAPK.

Для запуска скрипта нужно:

- положить файл **get_logs.bash** в произвольный каталог на узловой машине;
- перейти в каталог из предыдущего пункта в консоли ОС (команда cd);
- выполнить команду **bash get_logs.bash 6** (в примере собираются логи за последние 6 часов, данный интервал времени можно менять);
- дождаться выполнения команды, начать работать с получившимся каталогом

Скрипт нужно выполнять на всех участвующих Management и Sensor (если ошибка сбора данных – выполнять на Management и Sensor, который выполняет сканер сбора)



Обращение в техподдержку

Основной канал подачи заявок – support@udv.group. При обращении необходимо указывать **номер действующего сертификата техподдержки** (или лицензии, если в нее уже входит ТП, некоторые примеры внизу).

По умолчанию ТП оказывается в режиме 8x5, есть возможность ТП 24x7 (условия обговариваются индивидуально).

Альтернативные каналы – только для партнерских тестирований/пилотов, обговариваются отдельно на установочной встрече.

При обращении в ТП необходимо подробно описать проблему, указать используемую версию ПО, приложить скриншоты (в т.ч. будут полезны скрины проверки доступности, запись сетевого трафика и пр.), логи. Дополнительные сведения м.б. запрошены отдельно. В документации так же есть форма анкеты при обращении в сервисный центр, можно использовать ее. Для чувствительных данных есть возможность шифровать архив, пароль передавать отдельным каналом. При необходимости производитель DATAPK может выделить квоту на своем локальном файлообменнике для загрузки логов.

Название

Комплекс DATAPK базового уровня с поддержкой на 1 год (лицензия)

Артикул

DATAPK-ENT-03-1Y (лицензия)

Серийный номер

CI-0114

Название

Сертификат на базовую техническую поддержку программного обеспечения CyberLympha DATAPK, модуль «DATAPK-Management Enterprise», 1 год

Серийный номер

TS-CL-01

Вопросы?