УТВЕРЖДЕН

ЦМДА.00011-01 32-ЛУ

ПРОГРАММА

«DNSTAP2CLCK. ПРОГРАММА СБОРА И СОХРАНЕНИЯ СТАТИСТИКИ ЗАПРОСОВ К DNS-СЕРВЕРАМ»

Руководство системного программиста

ЦМДА.00011-01 32 01

Листов 10

2022

Инв. N подл.	Подп. и дата	Взам. Инв. N	Инв. N дубл.	Подп. и дата

АННОТАЦИЯ

Настоящий документ руководство системного программиста ЦМДА.00011-01 32 01 разработан на программу «Dnstap2clck. Программа сбора и сохранения статистики запросов к DNS-серверам» ЦМДА.00011-01.

В документе содержатся основные сведения о назначении программы «Dnstap2clck. Программа сбора и сохранения статистики запросов к DNS-серверам» ЦМДА.00011-01, приведены сведения о порядке установки, настройки и эксплуатации.

СОДЕРЖАНИЕ

1. Общие сведения 4
1.1. Назначение и функции 4
1.2. Сведения о программных и технических средствах 4
1.3. Квалификация персонала 4
2. Структура программы 5
3. Установка и настройка 6
3.1. Описание получения программы с сайта правообладателя 6
3.2. Установка 6
3.3. Запуск 6
3.4. Настройка 6
4. Регламент эксплуатации 8
Перечень принятых сокращений 9

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение и функции

Программа «Dnstap2clck. Программа сбора и сохранения статистики запросов к DNS-серверам» ЦМДА.00011-01 (далее по тексту – программа Dnstap2clck) предназначена для сбора и сохранения статистики запросов к DNS-серверам в СУБД.

1.2. Сведения о программных и технических средствах

Программа Dnstap2clck функционирует под управлением ОС семейства UNIX. Для хранения данных используется СУБД Clickhouse.

Для организации доступа к СУБД используется язык структурированных запросов в соответствии со стандартом SQL.

Программа Dnstap2clck разработана на языке программирования GO.

Параметры технических средств, требуемых для функционирования программы Dnstap2clck, должны быть не ниже приведенных в таблице 1.

Таблица 1 – Параметры технических средств

Наименование	**Параметр**
Процессор Intel	2 шт. по 2,2 ГГц
Объем оперативной памяти	8 Гб (RAM)
Объем ПЗУ	80 Гб

1.3. Квалификация персонала

Для обеспечения выполнения изложенных в руководстве системного программиста функций по эксплуатации программы Dnstap2clck обслуживающий персонал должен иметь квалификацию инженера, системного программиста или системного администратора и обладать необходимыми знаниями по настройке операционной системы, сетей и сетевых служб.

Перечень функций и режимы работы должны быть регламентированы должностными инструкциями. Персонал выполняет свои функции в соответствии с требованиями норм охраны труда и техники безопасности.

2. СТРУКТУРА ПРОГРАММЫ

Программа Dnstap2clck функционирует в автономном режиме, не связана с другими программами. Программа Dnstap2clck обеспечивает:

– получение данные из unix- или tcp-сокета;

– накопление данных DNS-запросов (таблица 2);

– запись с установленной периодичностью данных DNS-запросов в СУБД. Периодичность настраивается в конфигурационном файле или при запуске (см. раздел 3).

Таблица 2 – Поля таблицы для хранения данных статистики запросов к DNS-серверам

Наименование поля	Тип данных	Описание
timestamp	DateTime	Время получения (отправления) пакета
src_port	UInt32	Номер порта источника
dst_port	UInt32	Номер порта назначения
src_addr	String	Адрес источника
dst_addr	String	Адрес назначения
protocol	UInt8	Тип протокола (TCP/UDP)
qname	String	Запрашиваемое доменное имя
msg_id	UInt16	Идентификатор запроса
opcode	UInt8	Вид запроса
rcode	UInt8	Код результата
qd_count	UInt16	Количество записей в секции question
an_count	UInt16	Количество записей в секции answer
ns_count	UInt16	Количество NS-записей в секции authority
ar_count	UInt16	Количество ресурсных записей в секции additional
qtype	UInt16	Тип запроса
qclass	UInt16	Класс запроса
aa	UInt8	Значение флага Authoritative Answer
tc	UInt8	Значение флага TrunCation
rd	UInt8	Значение флага Recursion Desired
cd	UInt8	Значение флага checking disabled
ra	UInt8	Значение флага Recursion Available
ad	UInt8	Значение флага authentic data
do	UInt8	Значение флага DNSSEC OK
qr	UInt8	Тит запроса
node	String	Имя сервера, задается в настройках dnstap

В общем случае алгоритм работы программы Dnstap2clck: опросить по очереди список адресов для выдачи данных (указывается при запуске или в конфигурационном файле (см. раздел 3)), записать данные по первому доступному адресу; если не удается записать данные, то протоколируется сообщение об ошибке, данные записываются в файл.

3. УСТАНОВКА И НАСТРОЙКА

3.1. Описание получения программы с сайта правообладателя

Для получения программы Dnstap2clck необходимо:

– пройти по ссылке: https://kb.msk-ix.ru/software/ ;

– нажать на гиперссылку «Программное обеспечение»;

– ввести логин и пароль в окне автаутентификации.

3.2. Установка

Для сборки программы Dnstap2clck из исходного кода требуется GO версии 1.13 или выше.

Команды для компиляции программы Dnstap2clck:

```
mkdir -p $HOME/go/src/dnstap2clck
[переместить файлы из архива с программой в созданный каталог]
make
```

Рекомендуется при установке программы Dnstap2clck скомпилировать исходный код в директорию: /usr/local/bin

3.3. Запуск

Для запуска программы Dnstap2clck необходимо выполнить:

```
./dt2clck -c /path/to/config
```

Опции команды запуска программы Dnstap2clck:

– **-c <path>** – указывается путь к конфигурационному файлу;

– **-i <path>** – указывается источник данных (в виде: «*unix:///path/to/socket*» или «*tcp://1.2.3.4:5678*»);

– **-o <url>,<url>** – указывается список, адресов для выдачи данных (задается в виде: «*tcp://1.2.3.4:5678?username=user&password=qwerty&database=clicks&debug=true*», или «*http(s)://1.2.3.4:5678?username=user&password=qwerty&database=clicks&debug=true*», или «*file:///path/to/file*» (в первых двух случаях выполняются sql-запросы, в последнем – в файл сохраняются запросы в формате json, по одному на строку));

– **-t <table>** – указывается имя таблицы в СУБД;

– **-v** – включение функции протоколирования в стандартный поток stderr.

3.4. Настройка

Конфигурационный файл dt2clck.conf позволяет настроить параметры, указанные в таблице 3.

Таблица 3 – Настраиваемые параметры конфигурационного файла программы Dnstap2clck

Наименование параметра	Пример значения	Описание
output	http://localhost:9134; file:///tmp/dnstap.log	Список адресов, куда по очереди пытается писать программа Dnstap2clck, как только получилось, попытки останавливаются
input	unix:///tmp/dnstap.sock	Адрес, с которого программа Dnstap2clck получает данные (unix- или tcp-сокет)
table	dnstap	Имя таблицы в СУБД, в которую программа Dnstap2clck записывает данные
period	30	Периодичность записи данных в СУБД, в секундах

4. РЕГЛАМЕНТ ЭКСПЛУАТАЦИИ

Эксплуатация программы Dnstap2clck осуществляется 24 ч в день ежесуточно в течение всего календарного года.

После запуска программы Dnstap2clck необходимо осуществлять проверку работоспособности программы Dnstap2clck: убедиться, что в таблицу СУБД записываются данные, и при этом отсутствуют сообщения об ошибках в log-файлах.

При эксплуатации программы Dnstap2clck следует обращать внимание на ситуации, приводящие к неисправностям:

– DNS-сервер функционирует в chroot, а программа Dnstap2clck создает сокет за его пределами. Рекомендуется задать правильный путь к сокету;

– DNS-сервер и программа Dnstap2clck работают под разными пользователями. Рекомендуется запускать DNS-сервер и программу Dnstap2clck из-под одного и того же пользователя.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

ОС	–	операционная система
ПЗУ	–	постоянное запоминающее устройство
СУБД	–	система управления базой данных

Лист регистрации изменений									
Номера листов (страниц)					*Всего листов (страниц) в докум.*	*№ документа*	*Входящий № сопроводительного докум. и дата*	*Подл.*	*Дата*
Изм.	*измененных*	*замененных*	*новых*	*аннулированных*					