Инструкция по развертыванию ПК Cyberlympha ITM на ОС Альт СП Сервер

ООО «СайберЛимфа» <support@cyberlympha.com>, Ганжа Владислав

Version 1.7.0.0, 14.03.2024

Оглавление

1. Дистрибутивы	1
1.1. Состав и назначение дистрибутивов	1
1.2. Контрольные суммы файлов	1
2. Требования и рекомендации	3
2.1. Общие	3
2.2. ОС Альт Сервер 10	3
3. Предварительная подготовка	4
3.1. Обновление ОС Альт	4
3.2. Настройка NTP-сервера	4
3.3. Установка дополнительных пакетов ОС	4
3.4. Подготовка СУБД PostgreSQL	4
3.5. Подготовка iptables.	5
4. Установка CL ITM-VM	6
5. Установка СL ITM-М	0
6. Установка CL ITM-RM 1	5
7. Установка агента CL ITM на ОС Альт	7

1. Дистрибутивы

1.1. Состав и назначение дистрибутивов

Название дистрибутива (файла)	Версия	Назначение
alt-sp-server-20230529-x86_64.iso	CП Server	сертифицированный дистрибутив для развертывания CL ITM (Сервер)
alt-sp-workstation-20230528- x86_64.iso	СП Workstation	сертифицированный дистрибутив для развертывания CL ITM (Рабочая станция)
alt-server-10.2-x86_64.iso	10.2 Server	дистрибутив для развертывания CL ITM
alt-workstation-10.2-x86_64.iso	10.2 Workstation	дистрибутив для развертывания агента CL ITM
iptables	1.0	файл с правилами iptables
itm-agent2_v.1.2.0.alt_amd64.rpm	1.2.0	агент CL ITM для ОС Альт
clitm_cert_generator.sh	1.0	генератор сертификатов веб- сервера
udv_itm-vm_1.7.0.0.tar.gz	1.7.0.0	образ CL ITM-VM
docker-compose.release.yaml	1.7.0.0	compose-файл CL ITM-VM
env_generator.sh	1.7.0.0	генератор env для CL ITM-VM
udv_itm-k_v1.6.0.2.tar.gz	1.6.0.2	образ CL ITM-M
docker-compose.release.yaml	1.6.0.2	compose-файл CL ITM-M
env_generator.sh	1.6.0.2	генератор env для CL ITM-M
udv_itm-rm_v1.3.0.1.tar.gz	1.3.0.1	образ CL ITM-RM
docker-compose.release.yaml	1.3.0.1	compose-файл CL ITM-RM
env_generator.sh	1.3.0.1	генератор env для CL ITM-RM

1.2. Контрольные суммы файлов

Название дистрибутива (файла)	Контрольная сумма SHA1
alt-sp-server-20230529-x86_64.iso	23ADBB8B18BB3C8C5D6E91E961911368DC4ECA2A
alt-sp-workstation-20230528-x86_64.iso	228F15415DCEDAF15C7C459FB3ED4C668BAC6F89
alt-server-10.2-x86_64.iso	417BC81B813F5E5674DF738626BCA80D0635D8C3
alt-workstation-10.2-x86_64.iso	44847D1C1F29D5678368A65C9586548485381E27
iptables	2DB0D94E4A3666A4F5CE24580B7E769E6F99D7F4
<pre>itm-agent2_v.1.2.0.alt_amd64.rpm</pre>	030014DADCF6FAB77ABBF3BBD4954E96234B7178
clitm_cert_generator.sh	CCB28BB5EFF6D60219C9B4C22B888673EB2E2E6A
udv_itm-vm_1.7.0.0.tar.gz	0FA148DF8A4152FAB50F22CDBDA44CCD0E00FB51
docker-compose.release.yaml	E6129F7A7850EA866B453099AB74151341AEE93A
env_generator.sh	52B1B9EE8F0EBCC3D85E3DCEF3FFB55935487AF2
udv_itm-k_v1.6.0.2.tar.gz	663AF2F6BBEC2BE50C1658DC7A7072D1B265F928
docker-compose.release.yaml	7C29E6F57A39579605073F1AFD557FC69BEF44FA
env_generator.sh	E44E0E56DC186C936E82F75CF305ED0A71CA7BA1
udv_itm-rm_v1.3.0.1.tar.gz	07B71D1B5830893E5B32E45BD06467F5BB6AFA78
docker-compose.release.yaml	FF368C2D6D2A1ECE86ED52967FBD2629E33FCEEC
env_generator.sh	E12B63301EC466BD14E7E4B837CF7E182E93C81B

2. Требования и рекомендации

2.1. Общие

- В закрытом сетевом контуре АСУ ТП должен быть настроен, по меньшей мере, один NTP сервер (рекомендуется 2-3 независимых NTP сервера);
- Из закрытого сетевого контура АСУ ТП необходимо обеспечить доступ к Интернет репозиторию для обновления пакетной базы ОС Альт либо, используя ЦУС, развернуть отдельный сервер с зеркалом репозитория.

2.2. ОС Альт Сервер 10

- Сервер для развертывания ПК **CL ITM** должен иметь, как минимум, один сетевой интерфейс.
- Рекомендуемый объем ОЗУ для развертывания ПК СL ITM не менее 16 ГБ.
- Рекомендуемый объем свободного места на диске не менее 240 ГБ.
- Рекомендуемое число ядер ЦП не менее 4.
- На новых серверах предпочтительно использовать UEFI загрузку.
- ОС Альт Сервер 10 устанавливается с минимальным профилем, в процессе установки конфигурируется только один сетевой интерфейс для управления комплексом, при этом не следует менять используемую по умолчанию подсистему управления сетью Etcnet.
- Для работы ПК **CL ITM** рекомендуется разбивать диск вручную с использованием LVM и файловой системы XFS, размещать все данные на одном разделе вместе с системой, место для SWAP-раздела также стоит предусмотреть.

3. Предварительная подготовка

3.1. Обновление ОС Альт

После установки ОС Альт должна быть обновлена до актуального состояния

3.2. Настройка NTP-сервера

Для корректной работы ПК **CL ITM** на ОС Альт СП Сервер должен быть настроен NTP-сервер, часы должны быть синхронизированы. Рекомендуется настроить синхронизацию времени средствами Альт СП Сервер.

3.3. Установка дополнительных пакетов ОС

Для работы CL ITM необходимо установить пакеты docker-ce, docker-compose, net-snmp, netsnmp-utils, fping, postgresql15-server.

После установки необходимо запустить docker и добавить его в автозагрузку:

systemctl enable --now docker

3.4. Подготовка СУБД PostgreSQL

Для корректной работы CL ITM необходимо настроить запуск СУБД после docker на 10265 порту.

Для этого перейдите в режим редактирования службы СУБД:

systemctl edit postgresql

Добавьте блоки [Unit] и [Service]:

```
[Unit]
After=docker.service
BindsTo=docker.service
ReloadPropagatedFrom=docker.service
[Service]
```

_

Environment=PGPORT=10265

Примените изменения:

systemctl daemon-reload

Инициируйте СУБД. Для этого выполните команды:

```
# /etc/init.d/postgresql initdb
# systemctl enable --now postgresql
```

Подключитесь к СУБД, установите пароль для пользователя postgresql:

```
# psql -U postgres -p 10265
# ALTER USER postgres WITH PASSWORD '[пароль]';
# \q
```

Отредактируйте файл /var/lib/pgsql/data/postgresql.conf. Поменяйте значение переменных listen_addresses, port, shared_buffers (раскомментируйте переменные при необходимости):

```
listen_addresses = '127.0.0.1,172.17.0.1'
port = 10265
shared_buffers = 86B
```

Отредактируйте файл /var/lib/pgsql/data/pg_hba.conf. Измените метод аутентификации в строке host all all 127.0.0.1/32 [текущий метод аутентификации] на md5.

Перезагрузите СУБД:

```
# systemctl restart postgresql
```

3.5. Подготовка iptables

Для корректной работы CL ITM необходимо использовать iptables, efw необходимо отключить. Для удобства настройки можно скопировать файл iptables, подготовленный производителем CL ITM, в /etc/sysconfig/iptables, внести изменения при необходимости, активировать iptables. В примере файл iptables от производителя CL ITM был помещен в каталог /home/[имя пользователя OC]:

```
# cp /home/[имя пользователя OC]/iptables /etc/sysconfig/iptables
# systemctl enable --now iptables
# systemctl restart docker
```



После любых правок iptables необходимо перезапустить службы iptables и docker.

4. Установка CL ITM-VM



Перед установкой необходимо выполнить предварительную подготовку (разделы 2-3 настоящей инструкции).

1. Создайте каталог /opt/itm-vm:

```
# mkdir /opt/itm-vm
```

- 2. Скопируйте в указанный каталог файлы env_generator.sh, clitm_cert_generator, dockercompose.release.yaml, udv_itm-vm_1.7.0.0.tar.gz.
- 3. Создайте учетную запись в СУБД для CL ITM-VM:

```
# psql -U postgres -p 10265
# CREATE USER itmm_user WITH createdb PASSWORD '[пароль]';
# \q
```

4. Отредактируйте файл /var/lib/pgsql/data/pg_hba.conf. Добавьте в секцию ipv4localconnections строки:

host	all	itmm_user	172.17.0.0/24	md5
host	all	itmm_user	172.15.0.0/24	md5

5. Перезапустите СУБД:

```
# systemctl restart postgresql
```



В момент перезапуска СУБД все docker-контейнеры на машине должны быть остановлены.

6. Создайте файл /etc/sysctl.d/98-itm.conf, добавьте в него строку vm.overcommit_memory=1.

Примените изменения командой sysctl -p /etc/sysctl.d/98-itm.conf

7. Перейдите в каталог /opt/itm-vm, запустите генератор env-файла env_generator.sh. Настраивайте все предложенные параметры (у в диалоговом окне в момент запросов). Настройки оставляйте по умолчанию за исключением пароля пользователя СУБД (необходимо указать пароль, заданный при создании учетной записи в СУБД). В случае, если планируете на этом же сервере разворачивать также CL ITM-M, то необходимо в качестве порта для подключения к веб-серверу указать 8081, в качестве SSL порта для подключения к веб-интерфейсу - 8443:

bash env_generator.sh

8. Выполните загрузку образов и сгенерируйте сертификаты для веб-сервера, создайте парольную фразу по запросу скрипта генерации сертификатов:

```
# docker load -i udv_itm-vm_1.7.0.0.tar.gz
# bash clitm_cert_generator.sh vm
```

9. Запустите все сервисы ПК СL ITM-VM и дождитесь окончания их запуска:

```
$ su -c 'cd /opt/itm-vm && docker-compose up -d'
```

- 10. При помощи команды su -c 'docker ps' убедитесь, что все сервисы ПК CL ITM-VM запущены имеют статус «up» и не имеют статуса «restarting».
- Проверьте возможность подключения к ПК CL ITM-VM по протоколу HTTPS. Для этого откройте браузер и введите IP-адрес интерфейса управления CL ITM-VM, например: https://10.51.203.102:8443.
- 12. Если в браузере появится предупреждение о незащищенном подключении (по причине того, что созданный серверный сертификат не является доверенным для браузера), нажмите на кнопку «Дополнительно...» (Рисунок 1).



Рисунок 1 – Окно предупреждения о незащищенном подключении

13. Для продолжения подключения к CL ITM-VM нажмите кнопку «Принять риск и продолжить» (Рисунок 2).

•	Предупреждение: Вероятная угроза безопасности — Mozilla Firefox				
▲ Предупреждение: Вероятна:×	+				
$\leftarrow \rightarrow$ C \textcircled{a}	A Не защищено https://10.51.203.102:8443	☆	¢	Ð	≡
	Корее всего, эта проолема связана с самим вео-саитом, и вы ничего не сможете сэтим сделать. Сли вы находитесь в корпоративной сети или используете антивирусную программу, вы можете связаться со службой поддержки для получения помощи. Вы также можете сообщить администратору веб-сайта об этой проблеме. Подробнее Вернуться назад (рекомендуется) Ополнительно Кто-то может пытаться подменить настоящий сайт и вам лучше не продолжать. Кеб-сайты подтверждают свою подлинность с помощью сертификатов. Firefox не доверяет 10.51.203.102:8443, потому что издатель его сертификата неизвестен, сертификат является самоподписанным, или сервер не отправляет корректные промежуточные сертификат. Код ошибки: SEC_ERROR_UNKNOWN_ISSUER Просмотреть сертификат Мезад (рекомендуется) Оринять риск и продолжить		6	2	
меню 📷 😐	Предупреждение: Вероят	🗄 🔂 en 📐	🌒) 📄 🚅 Cp, 13	мар,	17:07

Рисунок 2 – Подключение к CL ITM-VM по HTTPS

- 14. При успешном подключении к ПК **CL ITM-VM** в браузере отобразится окно авторизации (Рисунок 3).
- 15. Подключитесь к ПК CL ITM-VM. Для этого:
 - 1. Откройте браузер.
 - 2. В адресной строке введите IP-адрес интерфейса управления ПК **CL ITM-VM**.
 - 3. В окне авторизации (Рисунок 3) в поля «Логин», «Пароль» введите имя и пароль учетной записи администратора ПК CL ITM-VM (itm/P@ssw0rd1234):

e	ITM-VM — Mozilla Firefox		
$\leftarrow \rightarrow$ C $\widehat{\square}$ \bigcirc $\widehat{\square}$ https://10.51.203.102:844	13/login		☆ 🛛 🗢
	Авторизация логин * пароль * 		
👯 Меню 📷 🧉 😜 ITM-VM — Mozilla Firefox		to en	🚬 (())) 📑 🛒 Ср, 13 мар, 17:0

Рисунок 3 – Окно авторизации в ПК CL ITM-VM

•	ITM-VM — Mozilla Firefox	
TTM-VM × +		
\leftarrow \rightarrow C \textcircled{a}	○ ▲ •~ https://10.51.203.102:8443/dashboard ☆	⊚ ≡
ITM-VM	Панель информации Обновлено: 13.03.2024 17:15 (-каждую 1 мин.)	
Панель информации	Филиал/ТК Все v	📱 Виджеты
 Серверы мониторинга 	Количество объектов мониторинга по статусу	÷
Объекты мониторинга	Bcero 1 OM	
К ИТ-услуги	• Мониторинг - 1	
🛦 Проблемы	Изменение количества объектов мониторинга 🕚	+‡+
🏟 Администрирование 🗸	По статусу По проблемности Час День Неделя Месяц М	(вартал Год
🔦 Настройки 🗸 🗸	0.75	
	14.02.2024 18.02.2024 22.02.2024 26.02.2024 01.03.2024 05.03.2024 09.03.2024	13.03.2024
17:16:30 (UTC+05) 13.03.2024		
1 D Đ		
<	Количество объектов мониторинга по проблемности	+
📆 Меню 📷 😜 П	📕	📔 🚅 Ср, 13 мар, 17:15

Рисунок 4 – Веб-интерфейс ПК CL ITM-VM

5. Установка CL ITM-М



Перед установкой необходимо выполнить предварительную подготовку (разделы 2-3 настоящей инструкции).

1. Создайте каталог /opt/itm-k:

```
# mkdir /opt/itm-k
```

- Скопируйте в указанный каталог файлы env_generator.sh, clitm_cert_generator, dockercompose.release.yaml, udv_itm-k_v1.6.0.2.tar.gz.
- 3. Создайте учетную запись в СУБД для CL ITM-VM и создайте БД datapkitm:

```
# psql -U postgres -p 10265
# CREATE USER datapkitm WITH PASSWORD '[пароль]';
# CREATE DATABASE datapkitm OWNER datapkitm;
# \q
```

4. Отредактируйте файл /var/lib/pgsql/data/pg_hba.conf. Добавьте в секцию ipv4localconnections строку:

host datapkitm datapkitm 172.16.239.0/24 md5

5. Перезапустите СУБД:

systemctl restart postgresql



В момент перезапуска СУБД все docker-контейнеры на машине д.б. остановлены.

6. Перейдите в каталог /opt/itm-k, запустите генератор env-файла env_generator.sh. Настраивайте все предложенные параметры (у в диалоговом окне в момент запросов). Синхронизацию с DATAPK необходимо пропустить при отсутствии CL DATAPK в инфраструктуре. Настройки оставляйте по умолчанию за исключением пароля пользователя СУБД (необходимо указать пароль, заданный при создании учетной записи в СУБД):

```
# cd /opt/itm-k
# bash env_generator.sh
```

7. Выполните загрузку образов и сгенерируйте сертификаты для веб-сервера, создайте парольную фразу по запросу скрипта генерации сертификатов:

```
# docker load -i udv_itm-k_v1.6.0.2.tar.gz
# bash clitm_cert_generator.sh k
```

8. Запустите все сервисы ПК СС ІТМ-М и дождитесь окончания их запуска:

\$ su -c 'cd /opt/itm-k && docker-compose up -d'

- 9. При помощи команды su -c 'docker ps' убедитесь, что все сервисы ПК CL ITM-VM запущены имеют статус «up» и не имеют статуса «restarting».
- 10. Проверьте возможность подключения к ПК **CL ITM-M** по протоколу HTTPS. Для этого откройте браузер и введите IP-адрес интерфейса управления CL ITM-M, например: https://10.51.203.102.
- 11. Если в браузере появится предупреждение о незащищенном подключении (по причине того, что созданный серверный сертификат не является доверенным для браузера), нажмите на кнопку «Дополнительно...» (Рисунок 5).

۵	Предупреждение: Вероятная угроза безопасности — Mozilla Firefox	_ 🗆 🗙
▲ Предупреждение: Вероятна:×	+	
$\leftarrow \rightarrow$ C \textcircled{a}	Ане защищено https://10.51.203.102	ය
4	Предупреждение: Вероятная угроза безопасности	
	Firefox обнаружил вероятную угрозу безопасности и не стал открывать 10.51.203.102. Если вы посетите	
	этот сайт, злоумышленники могут попытаться похитить вашу информацию, такую как пароли, адреса электронной почты или данные банковских карт.	
	Как вы можете это исправить?	
	Скорее всего, эта проблема связана с самим веб-сайтом, и вы ничего не сможете с этим сделать.	
	Если вы находитесь в корпоративной сети или используете антивирусную программу, вы можете	
	связаться со службой поддержки для получения помощи. Вы также можете сообщить администратору веб-сайта об этой проблеме.	
	Подробнее	
	Вернуться назад (рекомендуется) Дополнительно	
🍇 Меню 📷 💊	Предупреждение: Вероят	🔋 🕞 en 🗽 🐠 🗎 🚅 Ср, 13 мар, 17:10

Рисунок 5 – Окно предупреждения о незащищенном подключении

12. Для продолжения подключения к CL ITM-М нажмите кнопку «Принять риск и продолжить» (Рисунок 6).

e	Предупреждение: Вероятная угроза безопасности — Mozilla Firefox			
🛕 Предупреждение: Вероятна: ×	+			
\leftarrow \rightarrow C \textcircled{a}	🔒 Не защищено https://10.51.203.102	☆	\boxtimes	≡
	№ Не защищено https://10.51.203.102 Скорее всего, эта проолема связана с самим вео-саитом, и вы ничего не сможете с этим сделать. Если вы находитесь в корпоративной сети или используете антивирусную программу, вы можете связаться со службой поддержки для получения помощи. Вы также можете сообщить администратору веб-сайта об этой проблеме. Подробнее Вернуться назад (рекомендуется) Дополнительно Кто-то может пытаться подменить настоящий сайт и вам лучше не продолжать. Веб-сайты подтверждают свою подлинность с помощью сертификатов. Firefox не доверяет 10.51.203.102, потому что издатель его сертификата неизвестен, сертификат является самоподписанным, или сервер не отправляят корректные промежуточные сертификаты. Код ошибки: SEC_ERROR_UNKNOWN_ISSUER Просмотреть сертификат Вернуться назад (рекомендуется) Принять риск и продолжить			H
🐺 Меню 📷 💊 🕴	Предупреждение: Вероят	🛛 🔂 en 📐 (🐠)) 💼 🛒 Ср, 13 м	ap, 17:11

Рисунок 6 – Подключение к CL ITM-M по HTTPS

- 13. При успешном подключении к ПК **CL ITM-M** в браузере отобразится окно авторизации (Рисунок 7).
- 14. Подключитесь к ПК CL ITM-М. Для этого:
 - 1. Откройте браузер.
 - 2. В адресной строке введите IP-адрес интерфейса управления ПК **CL ITM-VM**.
 - 3. В окне авторизации (Рисунок 7) в поля «Логин», «Пароль» введите имя и пароль учетной записи администратора ПК CL ITM-VM (datapkitm/datapkitm).

۵	v1.6.0.2 — Mozilla Firefox	
••• v1.6.0.2 × +		
$\leftarrow \rightarrow$ C \textcircled{a} https://10	51.203.102	☆ 🛛 🖘
	ГТМ ГОМОЦЬ	v18.0.2
🎘 Меню 📷 🧕 👘 V1.6.0.2 — Mozilla Firefox		📑 🔂 еп 📐 🍥 🚰 🛃 Ср, 13 мар, 17:1

Рисунок 7 – Окно авторизации в ПК CL ITM-М

0					V	1.6.0.2: Панель	— Mozilla Firefox							
🚾 v	1.6.0.2: Панель	×	+											
~	\rightarrow C \textcircled{a}			O 🔒 https://10.51.203.102/zabbix.p	hp?actior	n=dashboard.view	/&dashboardid=1					ş	2	⊚ ≡
	ITM-M v1.6.0.2	~ 1	9	Главная панель										Изменить па
		c	ર	Все панели / Главная панель										
•	Мониторинг Панель		^	Информация о системе Количество узлов сети (активированных/деактивированных)	1	1/0	1			0	0		1	
	Проблемы			Количество шаблонов	167		доступен			едоступен	Неизвестно	0	BCelo	
	Узлы сети			Количество элементов данных	127	116/0/11								
	Обзор	ор (а		(активированных/деактивированных /неподдерживаемых)										
	Последние данные			Количество триггеров 58 (активированных/деактивированных Горобовиных/	58	58 / 0 [0 / 58]	0	0	,	0	0	0	0	1
	Комплексные экраны		(активированных/деактивированных				Чрезвычайная	Высс	, окая	Средняя	Предупреждение	О Информация	Не лассифицирован	
	Карты сетей			Количество пользователей (в сети)	2	1								
	Обнаружение				2	•								
	Услуги			Проблемы										Избранны
:≡	Инвентаризация		~	Время 🔻 Инфо Узел (сети	Проблема • Ваз	жность	Длит	ельност	ъ Под	дтверждено	Действия	Теги	Карты сети
	Отчеты		~				Данные не н	чайдены	I.					
5														
	Настройка		ř											
•	Администрирование		×											
9	Поддержка													
atty. N	Іеню 📷 💊		v1.	5.0.2: Панель — Mozill								🗄 🔂 en 🕒	🗏 📣 🌔 🚔 c	р, 13 мар, 17:14

Рисунок 8 – Веб-интерфейс ПК CL ITM-М

- 15. Установите агент CL ITM, чтобы сервер мог снимать свои метрики производительности. Для этого скопируйте пакет itm-agent2_v.1.2.0.alt_amd64.rpm на узловую OC.
- 16. Выполните установку пакета:

rpm -Uvh itm-agent2_v.1.2.0.alt_amd64.rpm

В случае ошибки ввиду отсутствия зависимостей сперва поставьте пакет zabbix-common и повторите команду выше.

- 17. Отредактируйте файл /etc/zabbix/zabbix_agent2.conf. Закомментируйте строку ServerActive, в строке Server укажите значение 172.16.239.0/24. Раскомментируйте строку ListenPort=10050.
- 18. Запустите агент CL ITM:

```
# systemctl enable --now zabbix_agent2
```

19. Посмотреть статус агента можно в веб-интерфейсе CL ITM-M (вкладка "Узлы сети", узел "datapkitm server") через 3-5 минут после запуска агента.

6. Установка CL ITM-RM



Перед установкой необходимо выполнить предварительную подготовку (разделы 2-3 настоящей инструкции).

1. Создайте каталог /opt/itm-a:

```
# mkdir /opt/itm-a
```

- Скопируйте в указанный каталог файлы env_generator.sh, docker-compose.release.yaml, udv_itm-rm_v1.3.0.1.tar.gz.
- 3. Создайте учетную запись в СУБД для CL ITM-VM и создайте БД datapkitm:

```
# psql -U postgres -p 10265
# CREATE USER itma_user WITH PASSWORD '[пароль]';
# CREATE DATABASE itma_db WITH OWNER 'itma_user';
# \q
```

4. Отредактируйте файл /var/lib/pgsql/data/pg_hba.conf. Добавьте в секцию ipv4localconnections строку:

host itma_db itma_user 172.16.240.0/24 md5

5. Перезапустите СУБД:

systemctl restart postgresql



В момент перезапуска СУБД все docker-контейнеры на машине д.б. остановлены.

- 6. Перейдите в каталог /opt/itm-a, запустите генератор env-файла env_generator.sh. Настройки оставляйте по умолчанию за исключением пароля пользователя СУБД (необходимо указать пароль, заданный при создании учетной записи в СУБД) и адреса ITM-K (необходимо указать IP-адрес сервера CL ITM-M):
 - # cd /opt/itm-a
 # bash env_generator.sh
- 7. Выполните загрузку образов:

docker load -i udv_itm-rm_v1.3.0.1.tar.gz

8. Запустите все сервисы ПК CL ITM-RM и дождитесь окончания их запуска:

\$ su -c 'cd /opt/itm-a && docker-compose up -d'

- 9. Подключите прокси через веб-интерфейс CL ITM-М. Для этого:
 - 1. Откройте веб-интерфейс сервера мониторинга.
 - 2. Перейдите в меню «Администрирование» → «Прокси».
 - 3. В правом верхнем углу нажмите на кнопку «Создать прокси».
 - 4. В появившемся окне заполните поля:
 - і. Имя прокси введите имя сервера удаленного мониторинга.
 - іі. Режим прокси выберите «Пассивный».
 - ііі. Интерфейс укажите IP-адрес, оставьте значения «Подключаться через IP» и «Порт 10051».
 - 5. Нажмите на кнопку «Добавить».

Подождите несколько минут, обновите веб-страницу.

•	🔽 v1.6.0.2: Настройка прокси 🛛 🗙	+					\sim \odot \otimes \otimes
*	\leftrightarrow C @	🔿 🗛 https://10.51.203.102/zabbix.php?action=proxy.list				☆	ල දු ≡
0	<mark>™ ITM-M</mark> << ™	Прокси					Создать прокси
	হ						Фильтр 🏹
•	Э Мониторинг ~		Имя	Режим Любое Активн	ый Пассивный		
	🚍 Инвентаризация 🗸 🗸			менить Сбросить			
0	I. Отчеты ~			Copocario			
3	Настройка ~	Имя Режим Шифрование Сжатие Г	Тоследний раз был доступен (возраст)	Количество узлов сети	Количество элементов данных	Требуемое быстродействие (знч/сек)	Узлы сети
ε	Администрирование ^		ic.	0	0		Отображено 1 из 1 найденных
	Общие	0 выбрано Активировать узлы сети Деактивировать узлы сети :					
	Прокси						
	Аутентификация						
	Группы пользователей						
	Роли пользователей						
	Способы оповещений						
	Скрипты						
	Очередь						
4	Э Поддержка						
	Настройки пользователя						
	9 Выход						
	Maura 🔽 🚺	1.6.0.7: Hactonika move		ITM		: A 🕅	n da) 🍋 🛲 Ur. 14 yap. 12:04
-3		note the permetipercent				: 🗋 en 💆	1, 14 map, 12:04

Рисунок 10 – Отображение подключенного CL ITM-RM в ПК CL ITM-М

7. Установка агента CL ITM на ОС Альт

Для установки агента CL ITM на OC Альт Сервер или Рабочая станция необходимо наличие на машине пакета zabbix-common, также необходимо разрешить входящие подключения на порт 10050/tcp c IP-адреса CL ITM-M или CL ITM-RM.

- 1. Скопируйте пакет itm-agent2_v.1.2.0.alt_amd64.грм на узловую ОС.
- 2. Выполните установку пакета:

rpm -Uvh itm-agent2_v.1.2.0.alt_amd64.rpm

- 3. Отредактируйте файл /etc/zabbix/zabbix_agent2.conf. Закомментируйте строку ServerActive, в строке Server укажите значение IP-адреса сервера CL ITM-M или CL ITM-RM. Раскомментируйте строку ListenPort=10050.
- 4. Запустите агент CL ITM:

systemctl enable --now zabbix_agent2

5. Поставьте узел на мониторинг в веб-интерфейсе CL ITM-М.

0	💊 v1.6.0.2: Узлы сети — Mozilla Firefox										
🚾 v	1.6.0.2: Узлы сети	× +									
~	\rightarrow C C		🔿 🔒 https://10.5	1.203.102/zabbix.php?name=&ip	=&dns=&port=&sta	itus=-1&evaltype	=0&tags[0][tag]=	&tags[0][operator]	=0&tags[0][value]=&ma	☆	$\boxtimes \equiv$
m	ITM-M v1.6.0.2		Узлы сети								
		Q	<								
0	Мониторинг		Имя					Состояние Лю	бое Активировано	Деактивировано	
	Панель		Группы узлов сети	начните печатать для поиска		Выбрать		Теги или	ЛИ ИЛИ		
	Проблемы		IP			-		тег		Содержит Рав	ю значение
	Узлы сети		DNS					Доба	зить		
	Обзор		DNS				Узлы сети в об	іслуживании 🔽	Подавленны	е проблемы	
	Последние данные		Порт								
	Комплексные экраны		Важность	Не классифици… Предуп Информация Средня:	реждение Высо я Чреза	ая ычайная					
	Карты сетей								_		
	Обнаружение					Сохранить ка	Приме	Сбросит	ь		
	Услуги		имя 🔺	Интерфейс	Доступность	Теги	Проблемы	Состояние	Последние данные	Проблемы	Графики П
:=	Инвентаризация		Alt10-server	10.51.203.103: 10050	ZBX SNMP JMX	IPMI		Активировано	Последние данные	Проблемы	Графики 8 П
	Отцеты		Alt10-workstation	10.51.202.33: 10050	ZBX SNMP JMX	IPMI		Активировано	Последние данные	Проблемы	Графики 8 П
	Оцены		datapkitm server	host.docker.internal: 10050	ZBX SNMP JMX	IPMI		Активировано	Последние данные	Проблемы	Графики 25 П
્ય	Настройка										Отображено :
	Администрирование										
9	Поддержка						ITM				
att N	🐺 Меню 📷 💊 👘 👻 (4). 6.0.2: Узлы сети — Мог										

Рисунок 10 – Отображение объектов мониторинга под управлением ОС Альт в ПК СL ITM-М

ſ

После любых правок конфигурационного файла агента необходимо перезапустить службу zabbix_agent2.