

ПРОТОКОЛ № 15200/2023

проведения совместных испытаний программного обеспечения «Deckhouse» версии 1.52.3 и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7)

г. Москва

09.11.2023

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 02.11.2023 по 08.11.2023 совместных испытаний программного обеспечения «Deckhouse» версии 1.52.3 (далее – ПО), разработанного АО «Флант», и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) (далее – Astra Linux SE 1.7.0), разработанной ООО «РусБИТех-Астра», включая Astra Linux SE 1.7.0 с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2023-0426SE17 (оперативное обновление 1.7.4) (далее – Astra Linux SE 1.7.4).

2 Объект испытаний

2.1 Перечень компонентов, эксплуатировавшихся в ходе проведения данных испытаний, относящихся к ПО, представлен в Таблице 1.

Таблица 1 – Перечень компонентов, относящихся к ПО

Описание	Наименование	MD5	Источник
Файл программного пакета дистрибутива ПО	Deckhouse ce v. 1.52.3	1cfe94b9eec3f1f8fd177d60 37b4d31e3c501a9a35b0058 f4c73d26d1755eed0	Ресурс в сети «Интернет», адрес: «registry.deckhouse.io/deckhouse/ce/install:v1.52.3»
Официальное руководство по эксплуатации ПО в электронном формате	Deckhouse Platform на bare metal	-	https://deckhouse.ru/gs/bm/step2.html



3 Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки корректности функционирования ПО в средах: Astra Linux SE 1.7.0, Astra Linux SE 1.7.4, – в объеме, указанном в Приложении 1.

3.2 Перечень официальных репозиторий ПО, эксплуатировавшихся в упомянутых средах:

- в среде Astra Linux SE 1.7.0: base;
- в среде Astra Linux SE 1.7.4: base, update, extended.

3.3 Неофициальные репозитории ПО для указанных сред не эксплуатировались.

3.4 Проверка корректности функционирования ПО при включённом режиме замкнутой программной среды (далее — ЗПС) в указанных средах не проводилась по причине отсутствия поддержки ПО соответствующей функциональности ОС. Информация об отсутствии упомянутой поддержки была заявлена стороной разработчика ПО.

3.5 Проверка корректности функционирования ПО в условиях ненулевого уровня конфиденциальности механизма мандатного разграничения доступа (далее – МРД) указанных сред не проводилась по причине отсутствия поддержки ПО соответствующей функциональности ОС. Информация об отсутствии упомянутой поддержки была заявлена стороной разработчика ПО.

3.6 Установка ПО производится с отдельного установочного узла на целевой узел под управлением тестируемой ОС, данная информация отражена в Приложении 2. При этом оба узла должны находиться в одной подсети и быть доступными друг для друга по ssh.

3.7 Не удалось установить ПО в среде ALSE 1.7.0. После перезагрузки мастер узла в процессе установки не запускается Kubernetes API и установка не может быть продолжена.



4 Результаты испытаний

4.1 ПО корректно функционирует в среде Astra Linux SE 1.7.4.

4.2 ПО не функционирует в среде Astra Linux SE 1.7.0.

5 Вывод

5.1 ПО и операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) совместимы, принимая во внимание информацию, содержащуюся в разделах 3, 4 и Приложении 2.

6 Состав рабочей группы и подписи сторон

6.1 Данный протокол составлен участниками рабочей группы:

Проканюк Д.С. – начальник сектора отдела технологической совместимости департамента развития технологического сотрудничества ДВиС ООО «РусБИТех-Астра»;

Словцов С.Ю. – младший инженер отдела технологической совместимости департамента развития технологического сотрудничества ДВиС ООО «РусБИТех-Астра».

ООО «РусБИТех-Астра»	
начальник сектора отдела технологической совместимости департамента развития технологического сотрудничества ДВиС	
(должность)	
(подпись)	Проканюк Д.С. (фамилия, инициалы)



Перечень проверок совместимости ПО и Astra Linux SE 1.7.0, Astra Linux SE 1.7.4

№ п/п	Наименование проверки	Результат проверки ПО и Astra Linux SE									
		1.7.0 с ядром ОС		1.7.4 с ядром ОС							
		5.4.0-54-generic	5.4.0-54-hardened	5.4.0-162-generic	5.4.0-162-hardened	5.10.190-1-generic	5.10.190-1-hardened	5.15.0-83-generic	5.15.0-83-hardened	5.15.0-83-lowlatency	6.1.50-1-generic
1.	Установка ПО	Неуспешно	Неуспешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
2.	Запуск, остановка выполнения ПО	Неуспешно	Неуспешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
3.	Эксплуатация минимальной базовой функциональности ПО	Неуспешно	Неуспешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
4.	Функционирование ПО в условиях низкого уровня целостности механизма МКЦ ОС	Не проводилась	Не проводилась	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
5.	Функционирование ПО в условиях ненулевого уровня конфиденциальности механизма МРД ОС	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась
6.	Отсутствие нарушений требований подраздела 17.3 «Руководство по КСЗ Ч. 1»	Не проводилась	Не проводилась	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
7.	Соответствие объектов ФС ОС дистрибутиву ОС при эксплуатации ПО	Не проводилась	Не проводилась	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
8.	Удаление ПО	Не проводилась	Не проводилась	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
9.	Функционирование ПО в условиях включённого механизма ЗПС ОС	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась
10.	Отсутствие нарушений требований подраздела 17.2 «Руководство по КСЗ Ч. 1»	Не проводилась	Не проводилась	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно



**Инструкция по установке и удалению ПО в средах: Astra Linux SE 1.7.0, Astra
Linux SE 1.7.4**

1 Установка ПО:

1.1 выполнить системные команды, действия:

#Выполнить команды на отдельном узле.

#В качестве <master_ip> - подставить ip-адрес целевого (мастер) узла, на который будет производиться установка ПО.

```
ssh-keygen
```

```
ssh-copy-id u@<master_ip-address>
```

```
echo "# Секция с общими параметрами кластера.
```

```
# https://deckhouse.ru/documentation/v1/installing/configuration.html#clusterconfiguration
```

```
apiVersion: deckhouse.io/v1
```

```
kind: ClusterConfiguration
```

```
clusterType: Static
```

```
# Адресное пространство подов кластера.
```

```
podSubnetCIDR: 10.111.0.0/16
```

```
# Адресное пространство сети сервисов кластера.
```

```
serviceSubnetCIDR: 10.222.0.0/16
```

```
kubernetesVersion: "Automatic"
```

```
# Домен кластера.
```

```
clusterDomain: "cluster.local"
```

```
---
```

```
# Секция первичной инициализации кластера Deckhouse.
```

```
# https://deckhouse.ru/documentation/v1/installing/configuration.html#initconfiguration
```

```
apiVersion: deckhouse.io/v1
```

```
kind: InitConfiguration
```

```
deckhouse:
```

```
  releaseChannel: Stable
```

```
  configOverrides:
```



```

global:
  modules:
    # Шаблон, который будет использоваться для составления адресов системных
приложений в кластере.
    # Например, Grafana для %s.test.test будет доступна на домене 'grafana.test.test'.
    # Можете изменить на свой сразу, либо следовать шагам руководства и сменить
его после установки.
    publicDomainTemplate: "%s.test.test"
    # Имя storage class, который будет использоваться для всех компонентов
Deckhouse (Prometheus, Grafana, OpenVPN и т. д.).
    storageClass: localpath-deckhouse-system
  userAuthn:
    controlPlaneConfigurator:
      dexCAMode: DoNotNeed
    # Включение доступа к API-серверу Kubernetes через Ingress.
    #
https://deckhouse.ru/documentation/v1/modules/150-user-authn/configuration.html#param
eters-publishapi
    publishAPI:
      enable: true
      https:
        mode: Global
        global:
          kubeconfigGeneratorMasterCA: ""
    # Включить модуль cni-cilium
    cniCiliumEnabled: true
    # Настройки модуля cni-cilium
    # https://deckhouse.ru/documentation/v1/modules/021-cni-cilium/configuration.html
    cniCilium:
      tunnelMode: VXLAN
---
# Секция с параметрами статического кластера.
#
https://deckhouse.ru/documentation/v1/installing/configuration.html#staticclusterconfigurati

```



on

apiVersion: deckhouse.io/v1

kind: StaticClusterConfiguration

Список внутренних сетей узлов кластера (например, '10.0.4.0/24'), который
используется для связи компонентов Kubernetes (kube-apiserver, kubelet...) между
собой.

Если каждый узел в кластере имеет только один сетевой интерфейс,

ресурс StaticClusterConfiguration можно не создавать.

internalNetworkCIDRs:

- 192.168.56.0/24 # (!!!) PUT THE ADDRESS OF THE LOCAL NETWORK HERE (!!!) # "
> /home/astralinux.ru/\$USER/config.yml

docker run --pull=always -it -v "\$PWD/config.yml:/config.yml" -v "\$HOME/.ssh:/tmp/.ssh/"
registry.deckhouse.io/deckhouse/ce/install:v1.52.3 bash

dhctl bootstrap --ssh-user=<username> --ssh-host=<master_ip> --ssh-agent-private-
keys=/tmp/.ssh/id_rsa --config=/config.yml --ask-become-pass

#Дальнейшие команды выполняются на целевом (мастер) узле !

sudo /opt/deckhouse/bin/kubectl patch nodegroup master --type json -p [{"op": "remove",
"path": "/spec/nodeTemplate/taints"}]

echo "# Секция, описывающая параметры NGINX Ingress controller.

<https://deckhouse.ru/documentation/v1/modules/402-ingress-nginx/cr.html>

apiVersion: deckhouse.io/v1

kind: IngressNginxController

metadata:

name: nginx

spec:

ingressClass: nginx

Способ поступления трафика из внешнего мира.



```

inlet: HostPort
hostPort:
  httpPort: 80
  httpsPort: 443
# Описывает, на каких узлах будет находиться Ingress-контроллер.
# Возможно, захотите изменить.
nodeSelector:
  node-role.kubernetes.io/control-plane: ""
tolerations:
- operator: Exists " > /home/astralinux.ru/$USER/ingress-nginx-controller.yml

```

```
sudo /opt/deckhouse/bin/kubectl create -f ingress-nginx-controller.yml
```

```
sudo apt install nginx
```

```
#Подождать около 7 минут
```

```
sudo /opt/deckhouse/bin/kubectl create -f ingress-nginx-controller.yml
```

```
#Подождать около 3х минут
```

```
sudo /opt/deckhouse/bin/kubectl -n d8-ingress-nginx get po -l app=controller
```

```
#Дождаться, пока в результате вывода предыдущей команды будет статус 3\3
```

```
sudo /opt/deckhouse/bin/kubectl create -f - << EOF
```

```
apiVersion: deckhouse.io/v1alpha1
```

```
kind: LocalPathProvisioner
```

```
metadata:
```

```
  name: localpath-deckhouse-system
```

```
spec:
```

```
  nodeGroups:
```

```
  - worker
```

```
  path: "/opt/local-path-provisioner"
```

```
EOF
```

```
echo "apiVersion: deckhouse.io/v1
```

```
kind: ClusterAuthorizationRule
```

```
metadata:
```




```
name: admin
spec:
  # список учётных записей Kubernetes RBAC
  subjects:
  - kind: User
    name: admin@test.test
  # предустановленный шаблон уровня доступа
  accessLevel: SuperAdmin
  # разрешить пользователю делать kubectl port-forward
  portForwarding: true
---
# секция, описывающая параметры статического пользователя
# используемая версия API Deckhouse
apiVersion: deckhouse.io/v1
kind: User
metadata:
  name: admin
spec:
  # e-mail пользователя
  email: admin@test.test
  # это хэш пароля 039ssumuyu, сгенерированного сейчас
  # сгенерируйте свой или используйте этот, но только для тестирования
  # echo "039ssumuyu" | htpasswd -BinC 10 "" | cut -d: -f2 | base64 -w0
  # возможно, захотите изменить
  password:
'JDJhJDEwJGtCd094RDg2ZlplnSGhTSGZ0SHQ4UmVObkpPNUI5Z295bjI4Q01NVTIxQ3V
GeUxlaWJydk4y"' > /home/astralinux.ru/$USER/user.yml

sudo /opt/deckhouse/bin/kubectl create -f user.yml

sudo nano /etc/hosts

#add:
```



```
<master-ip> api.test.test argocd.test.test cdi-uploadproxy.test.test dashboard.test.test  
documentation.test.test dex.test.test grafana.test.test hubble.test.test istio.test.test istio-  
api-proxy.test.test kubeconfig.test.test openvpn-admin.test.test prometheus.test.test  
status.test.test upmeter.test.test
```

#save and exit

2 Удаление ПО:

2.1 выполнить системные команды, действия:

```
sudo sh /var/lib/bashible/cleanup_static_node.sh --yes-i-am-sane-and-i-understand-  
what-i-am-doing  
sudo apt purge nginx  
sudo apt autoremove
```



Перечень используемых сокращений

«Руководство по КСЗ Ч. 1» – документ «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1» РУСБ.10015-01 97 01-1;

Astra Linux SE 1.7.0 – операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7);

Astra Linux SE 1.7.4 – операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2023-0426SE17 (оперативное обновление 1.7.4);

ДВиС – дирекция внедрения и сопровождения;

ЗПС – замкнутая программная среда;

КСЗ – комплекс средств защиты;

МКЦ – мандатный контроль целостности;



МРД – мандатное управление доступом;

ОС – операционная система;

ПО – программное обеспечение «Deckhouse» версии 1.52.3.

Идентификатор документа d99de1bf-c2ef-4fea-8689-597daf5699d0

Документ подписан и передан через оператора ЭДО АО «ПФ «СКБ Контур»

Подписи отправителя:	 ООО "РУСБИТЕХ-АСТРА" Проханок Дмитрий Сергеевич	 Не приложена при подписании	Доверенность: рег. номер, период действия и статус Сертификат: серийный номер, период действия 03B5A6850058AF999442C11D88 AD01026B с 25.11.2022 10:56 по 25.11.2023 10:56 GMT+03:00	Дата и время подписания 13.11.2023 18:14 GMT+03:00 Подпись соответствует файлу документа
-------------------------	--	---	--	---