

Общие сведения о Nova Container Platform SE

Данный раздел содержит общую вводную информацию о Nova Container Platform SE.

1. Введение

Nova Container Platform SE Special Edition (Nova SE) — комплексная платформа на базе Kubernetes версии 1.29, предназначенная для создания, управления и масштабирования приложений в контейнерах со встроенными средствами защиты от несанкционированного доступа.

В Nova SE привычные технологии Kubernetes дополнены множеством различных инструментов и решений для построения единой среды размещения приложений.

2. Назначение и область применения

Nova является средством контейнеризации, соответствующим требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (утв. Приказом ФСТЭК России № 76 от 2 июня 2020 г.) по 4 уровню доверия и требованиям по безопасности информации к средствам контейнеризации (утв. Приказом ФСТЭК России от 4 июля 2022 г. № 118) по 4 классу защиты.



Nova функционирует в единственном режиме – штатный режим (режим эксплуатации).

3. О Kubernetes

Kubernetes - открытое ПО для автоматизации развертывания, масштабирования и управления приложениями в контейнерах. В современной разработке контейнеры и образы, из которых они запускаются, являются основными структурными элементами. Для обеспечения масштабируемости приложений требуется надежная и гибкая система управления. Kubernetes де-факто является стандартом в оркестрации контейнерами.

Kubernetes является расширяемой платформой с быстро растущей экосистемой.

4. Преимущества использования приложений в контейнерах

Использование приложений в контейнерах дает много преимуществ по сравнению с традиционными методами развертывания. Вместо установки приложения в ОС на отдельной виртуальной машине, вы можете создать контейнер, который будет включать все зависимости данного приложения. Вы можете перенести данный контейнер в любую среду (облако, платформа виртуализации, локальная машина), и он будет работать без изменений.

Дополнительные преимущества использования контейнеров:

- Простота создания образа контейнера по сравнению с VM.
- Возможность наладки процессов непрерывной интеграции и доставки.
- Возможность быстрого отката версии приложения.

4.1. Операционные системы

Контейнеры используют небольшие дистрибутивы ОС семейства Linux без ядра. Их файловая система, сетевая подсистема, контрольные группы (cgroups) изолированы от хостовой ОС. Вы можете развертывать на одном сервере множество разных контейнеров с приложениями, требующими разные ОС или несовместимые зависимости.

4.2. Развертывание и масштабирование

С помощью инструментов Kubernetes вы легко можете применять практику непрерывного обновления (rolling update) для вашего приложения без влияния на пользователей. Вы также можете развертывать новую версию приложения в целях тестирования совместно с основной версией.

Поскольку все программные зависимости для приложения находятся внутри контейнера, вы можете использовать любую подходящую под ваши требования ОС. В редких случаях из-за особенности нагрузки вам может потребоваться дополнительная конфигурация ОС на узлах, выделенных под работу вашего приложения.

Для возможности масштабирования приложений в контейнерах Nova Container Platform SE предлагает как встроенные инструменты Kubernetes, так и дополнительные инструменты. Они позволяют изменять как количество реплик приложений, так и объем потребляемых ими ресурсов на основе оценки данных из пользовательских метрик в системе мониторинга. Это позволяет не только масштабировать требуемые сервисы при росте нагрузке, но и в зависимости от различных параметров (например, бизнес-метрик).

5. Преимущества Nova Container Platform SE

Nova Container Platform SE дополняет Kubernetes решениями, необходимыми для промышленной эксплуатации кластера, и имеет ключевые преимущества по сравнению с обычным дистрибутивом Kubernetes:

- Единая утилита управления платформой `nova-ctl` позволяет в автоматизированном режиме выполнять установку и обслуживание платформы в различных средах.
- Быстрое развертывание платформы за счет параллельного взаимодействия установщика с узлами.
- Автоматизированное обновление TLS-сертификатов платформы.
- Автоматизированное обновление компонентов платформы, в том числе компонентов Kubernetes.
- Поддержка сертифицированных российских ОС.
- Интеграция процессов развертывания и управления жизненным циклом с платформами виртуализации.
- Интеграция компонентов с открытым исходным кодом из экосистемы Kubernetes.
- Работа в экосистеме ОРИОН: поддержка платформы виртуализации zVirt и CMP-платформы Cloudlink.
- Безопасность среды согласно лучшим практикам сообщества Kubernetes и CIS (Center for Internet Security).
- Наличие интегрированных в платформу решений для мониторинга, оповещения, сбора диагностической информации, сбора событий ИБ с инфраструктуры Kubernetes.
- Наличие встроенных инструментов контроля отклонений от желаемой конфигурации как на уровне компонентов кластера, так и на уровне сервисов платформы.
- Наличие полноценного графического веб-интерфейса управления платформой.
- Наличие встроенных инструментов для организации процессов непрерывного развертывания и обновления приложений в кластер Kubernetes.
- Наличие встроенных балансировщиков сетевого трафика для публикации приложений.
- Наличие встроенных средств защиты от несанкционированного доступа.

Руководство администратора

1. Назначение

ПО Nova Container Platform Special Edition — комплексная платформа на базе Kubernetes, предназначенная для создания, управления и масштабирования приложений в контейнерах **со встроенными средствами защиты от несанкционированного доступа**.

В Nova Container Platform привычные технологии Kubernetes дополнены множеством различных инструментов и решений для построения единой среды размещения приложений.

2. Действия по приемке поставленного средства

Процедура приемки производится перед началом эксплуатации, для обнаружения расхождения между оригиналом Nova и версией, полученной Заказчиком.

2.1. Приемка Nova при поставке на физическом носителе

Приемка ПО Nova Container Platform Special Edition состоит из следующих этапов:

- проверка маркировки и упаковки
- проверка комплектности
- проверка целостности дистрибутива ПО

2.1.1. Проверка маркировки и упаковки

Проверка маркировки и упаковки включает в себя:

- Проверку целостности пакета документов: документация не должна быть повреждена.
- Проверку целостности упаковки носителей информации.
- Проверку наличия в **Формуляре** следующих данных:
 - Сведения о разработчике;
 - Наименование Продукции;
 - Децимальный номер;
 - Идентификатор СЗИ вида `POCC RU.01.XXXXXX.XXXXXX` (где `XXXXXX` — число от `00001` до `99999`, указывающее на номер сертификата соответствия, `XXXXXX` —

число от 000001 до 999999 , указывающее на заводской или серийный номер образца сертифицированного средства защиты информации);

- Дата выпуска.
- Проверку маркировки дистрибутивного носителя на наличие:
 - Идентификатора СЗИ;
 - Наименования Изделия.

2.1.2. Проверка комплектности

ПО Nova Container Platform Special Edition поставляется в составе инсталляционного комплекта, включающего следующие части:

- Дистрибутив программного обеспечения;
- Комплект документации.

Комплектность поставки на физическом носителе ПО NOVA Container Platform Special Edition приведена в таблице ниже.

Комплектность поставки ПО NOVA Container Platform Special Edition.

№ п/п	Наименование (обозначение)	Кол-во	При поставке на физическом носителе	При электронной поставке
1.	Дистрибутив ПО NOVA Container Platform Special Edition РОФ.53652694.58.29.12.01- 01	1	На USB-флеш- накопителе	В электронном виде
2.	Формуляр РОФ.53652694.58.29.12.01- 01 30 01	1	На бумажном носителе	В электронном виде
3.	Копия сертификата соответствия Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00	1	На USB-флеш- накопителе	В электронном виде
4.	Руководство администратора РОФ.53652694.58.29.12.01- 01 90 01	1	На USB-флеш- накопителе	В электронном виде

№ п/п	Наименование (обозначение)	Кол-во	При поставке на физическом носителе	При электронной поставке
5.	Руководство пользователя РОФ.53652694.58.29.12.01- 01 34 01	1	На USB-флеш- накопителе	В электронном виде
6.	Руководство по установке РОФ.53652694.58.29.12.01- 01 94 01	1	На USB-флеш- накопителе	В электронном виде
7.	Контрольные суммы исполняемых файлов после инсталляции	1	На USB-флеш- накопителе	В электронном виде
8.	Упаковка	1	-	-

Контрольная сумма поставляемого дистрибутива представлены в документе «Программное обеспечение NOVA Container Platform Special Edition Формуляр», РОФ.53652694.58.29.12.01-01 30 01.

Пофайловые контрольные суммы дистрибутива приведены в приложении документа РОФ.53652694.58.29.12.01-01 30 01.

2.1.3. Проверка целостности дистрибутива ПО

Проверка целостности носителя с дистрибутивом включает в себя: * осмотр носителя информации на предмет наличия механических повреждений; * проверку носителя на отсутствие деструктивного кода антивирусной программой с актуальной на момент проверки базой вредоносных сигнатур;

Проверка целостности дистрибутива выполняется путем снятия контрольный сумм полученного дистрибутива с помощью программного средства «ФИКС 2.0.2» по алгоритму «Уровень-3» или с использованием утилиты из состава ОС РЕД ОС – md5sum по алгоритму MD5. Полученная контрольная сумма сравнивается с указанной в Формуляре.

Проверка целостности, установленной Nova производится путем снятия контрольных сумм с исполняемых файлов и сравнения полученных контрольных сумм с контрольными суммами, указанными в п.6 Формуляра.

Если по результатам проверки контрольные суммы соответствуют значениям контрольных сумм, приведенных в Формуляре, то полученный экземпляр Nova считается соответствующим оригиналу Nova.

В случае, если по всем указанным процедурам, установлено полное соответствие, то Nova признается годным к эксплуатации.

2.2. Приемка Nova при электронной поставке

При электронной поставке Nova приемка включает в себя следующие этапы:

- проверка маркировки
- проверка комплектности
- проверка целостности и электронной подписи

2.2.1. Проверка маркировки

Проверка маркировки включает проверку наличия в Формуляре следующих данных: *

Сведения о разработчике; * Наименование Продукции; * Децимальный номер; *

Идентификатор СЗИ вида РОСС RU.01.XXXXXX.XXXXXX (где XXXXXX – число от 00001 до 99999, указывающее на номер сертификата соответствия, XXXXXX – число от 000001 до 999999, указывающее на заводской или серийный номер образца сертифицированного средства защиты информации); * Дата выпуска.

2.2.2. Проверка комплектности

Проверка комплектности поставки проводится методом сравнения состава полученной поставки требованиям, указанным в разделе 5 Формуляра. Если по результатам проверки комплектности поставки расхождения с Формуляром отсутствуют – производится проверка целостности и электронной подписи.

Проверка целостности и электронной подписи выполняется в два этапа:

1. Вычисление контрольной суммы дистрибутива
2. Проверка электронной цифровой подписи через портал уполномоченного федерального органа или аккредитованного удостоверяющего центра в области использования электронной подписи.

2.2.3. Проверка целостности и электронной подписи

Проверка целостности дистрибутива выполняется путем снятия контрольной суммы полученного дистрибутива с помощью программного средства «ФИКС 2.0.2» по алгоритму «Уровень-3» или с использованием утилиты из состава ОС РЕД ОС – md5sum по алгоритму MD5. Полученная контрольная сумма сравнивается с указанной в Формуляре.

Проверка подписи может производиться при помощи ПО, предназначенного для шифрования и электронной подписи файлов. При этом порядок проверки электронной подписи производится согласно эксплуатационной документации на данное ПО.

Проверка целостности, установленной Nova производится путем снятия контрольных сумм с исполняемых файлов и сравнения полученных контрольных сумм с контрольными суммами, указанными в п.6 Формуляра.

Если по результатам проверки контрольные суммы соответствуют значениям контрольных сумм, приведенных в Формуляре, то полученный экземпляр Nova считается соответствующим оригиналу Nova.

В случае, если по всем указанным процедурам, установлено полное соответствие, то Nova признается годным к эксплуатации.

3. Содержание раздела

- Безопасность среды функционирования
- Безопасность установки
 - Настройка выявления уязвимостей
 - Настройка контроля целостности
 - Настройка регистрации событий безопасности и управления доступом
 - Настройка идентификации и аутентификации
 - Настройка централизованного управления образами контейнеров и контейнерами