Astra
Infrastructure
Cloud

Руководство пользователя облачной платформы Astra Infrastructure Cloud (AIC)

Оглавление

Введение

Настоящий документ является руководством пользователя программного изделия Astra Infrastructure Cloud (далее по тексту — AIC) и предназначен для разработчика и администратора виртуальной машины.

Документ содержит описания:

- создания шаблонов ВМ;
- настройки конфигураций шаблонов ВМ;
- создания ВМ;
- настройки конфигураций ВМ;
- работы с виртуальной машиной.

Документ не охватывает порядок установки, развертывания и администрирования AIC и предназначен для использования совместно с эксплуатационными документами.

Назначение

Изделие предназначено для управления средой виртуализации ПК СВ «Брест», входящей в состав инфраструктурного облака AIC, в том числе для создания и защиты которой обеспечивается средствами операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 очередное обновление 1.7 (далее по тексту — ОС СН).

В ПК СВ «Брест» входят следующие компоненты серверной части:

- сервер виртуализации — для возможности создания виртуальных машин посредством эмуляции аппаратного обеспечения;
- сервер управления — для возможности управления через веб-интерфейс, из командной строки (консольный интерфейс) и с помощью XML-RPC API. В качестве клиентской части изделия может выступать средство вычислительной техники, с которого выполняется подключение к серверу управления или ВМ.

В качестве дополнительных программных компонентов (не входят в состав ПК СВ «Брест») выступают:

- хранилище — система, предназначенная для хранения образов дисков виртуальных машин;
- контроллер домена — служба, обеспечивающая аутентификацию пользователей в рамках единого пространства пользователей (не используется в сервисном режиме работы ПК СВ «Брест»).

ПК СВ «Брест» предоставляет следующие возможности:

- создание ВМ, их образов и шаблонов;
- формирование среды выполнения ВМ;
- управление конфигурацией ВМ с помощью графического и консольного интерфейсов;
- централизованное управление средой виртуализации.

ПК СВ «Брест» функционирует только под управлением ОС СН, имеющей сертификат соответствия ФСТЭК России № 2557 и являющейся его неотъемлемой составной частью.

Изделие совместно с ОС СН обеспечивает выполнение следующих функций безопасности информации в соответствии с Требованиями по безопасности информации к средствам виртуализации:

- доверенная загрузка виртуальных машин;
- контроль целостности;

- регистрация событий безопасности;
- управление доступом;
- резервное копирование;
- управление потоками информации;
- защита памяти;
- ограничение программной среды;
- идентификация и аутентификация пользователей.

Функция централизованного управления (администрирование) ВМ и взаимодействием между ними реализуется собственными средствами изделия.

Изделие интегрировано с комплексом средств защиты информации ОС СН и дополнительно обеспечивает выполнение следующих функций безопасности:

- дискреционное и мандатное управление доступом к ВМ и образам ВМ, в том числе при межпроцессном и сетевом взаимодействии, включая взаимодействие между ВМ по протоколам стека IPv4 и IPv6 в условиях мандатного управления доступом и доступ субъектов к файлам-образам и экземплярам функционирующих ВМ;
- создание кластеров высокой доступности с общим хранилищем, обеспечивающих отказоустойчивое функционирование ВМ посредством миграции ВМ между узлами кластера;
- обновление программного обеспечения изделия с использованием штатных средств ОС СН.

Требования к среде функционирования

Базовый компонент AIC - ПК СВ «Брест» функционирует только под управлением ОС СН на максимальном уровне защищенности («Смоленск») или усиленном уровне защищенности («Воронеж»).

Для обеспечения корректного функционирования ПК СВ необходимо установить программное обеспечение оперативных обновлений ОС СН бюллетень № 2023-0426SE17 (оперативное обновление 1.7.4) и бюллетень № 2023-0630SE17MD (оперативное обновление 1.7.4.UU.1).

После установки оперативного обновления рекомендуется применение ядра linux-5.15-generic.

Требования к техническим средствам

ПК СВ функционирует в следующем режиме:

- в дискреционном режиме обеспечивается функционирование защищенной среды виртуализации, в том числе дискреционное и мандатное управление доступом к ВМ. В таком режиме ВМ запускаются от имени доменного пользователя, авторизовавшегося в ПК СВ. Для работы в дискреционном режиме необходимо, чтобы все компьютеры, на которых развернуты программные компоненты ПК СВ, входили в один домен ALD Pro.

Режим функционирования устанавливается на этапе развертывания ПК СВ. После установки и инициализации программных компонент переключение режимов функционирования ПК СВ не предусмотрено.

Создание и защита среды виртуализации обеспечиваются встроенными средствами ОС СН, интегрированными с подсистемой безопасности PARSEC, предназначенной для реализации функций ОС СН по защите информации от несанкционированного доступа:

- модулем ядра KVM, который использует аппаратные возможности архитектуры x86-64 по виртуализации процессоров;
- средствами эмуляции аппаратного обеспечения на основе QEMU;
- сервером виртуализации на основе libvirt.

В ПК СВ входят следующие программные компоненты серверной части:

- сервер виртуализации — для возможности создания виртуальных машин посредством эмуляции аппаратного обеспечения;
- сервер управления — для возможности управления через веб-интерфейс, из командной строки (консольный интерфейс) и с помощью XML-RPC API.

В качестве клиентской части изделия может выступать средство вычислительной техники, с которого выполняется подключение к серверу управления или виртуальной машине (ВМ).

В качестве дополнительных программных компонентов (не входят в состав ПК СВ) выступают:

- хранилище — система, предназначенная для хранения образов дисков виртуальных машин. Может быть построена на базе следующих технологий хранения:
  - файловой технологии хранения;
  - блочной технологии хранения с использованием LVM;
  - программно-определяемой технологии хранения Ceph;

- контроллер домена — служба, обеспечивающая аутентификацию пользователей в рамках единого пространства пользователей (не используется в сервисном режиме работы ПК СВ).

Примечание. В ПК СВ в качестве службы управления единым пространством пользователей используется ALD Pro из состава ОС СН. Если на объекте эксплуатации уже имеется настроенный домен ALD Pro, то разворачивать дополнительный контроллер домена нет необходимости. Все серверы вводятся в существующий домен.

ПК СВ может быть развернут как на группе компьютеров, так и на виртуальных машинах в пределах одного компьютера для тестирования. Для объединения компьютеров, обеспечения выполнения операций управления и поддержки виртуальных сетей используется локальная сеть.

ВНИМАНИЕ! Программные компоненты ПК СВ должны функционировать на оборудовании, отвечающему требованиям к аппаратному обеспечению под управлением ОС СН.

Примечание. Если для установки сервисов ПК СВ планируется использовать оптические установочные носители, то серверы должны быть оборудованы устройством для чтения и записи CD и DVD.

- Требования сервера управления:

Минимальные рекомендуемые характеристики компьютера для развертывания службы сервера управления указаны в таблице ниже:

Ресурсы	Минимальная рекомендуемая конфигурация
Память	4 ГБ
ЦП	1 ЦП (2-ядра)
Размер диска	100 ГБ
Сеть	2 NICS

Максимальное количество серверов виртуализации (компьютеров, на которых установлена и инициализирована служба сервера виртуализации), которым можно управлять с помощью одного экземпляра сервера управления, зависит от производительности и масштабируемости инфраструктуры ПК СВ и главным образом от системы хранения данных.

Не рекомендуется использовать один экземпляр сервера управления для управления более чем 500 серверами виртуализации.

Сервер управления (компьютер, на котором установлена и инициализирована служба сервера управления) должен иметь сетевое соединение со всеми серверами виртуализации и, по возможности, доступ к хранилищам данных (как локальным, так и сетевым). Для обеспечения надежности инфраструктуры ПК СВ рекомендуется использовать как минимум две сети (соответственно, требуется два сетевых интерфейса):

1) сервисная сеть — используется службой сервера управления для обеспечения доступа к серверам виртуализации с целью управления и мониторинга гипервизоров и перемещения файлов образов;
2) сеть экземпляров — обеспечивает возможность сетевого подключения к виртуальным машинам через различные серверы виртуализации.

Кроме того, может потребоваться третий сетевой интерфейс для обеспечения доступа к сети хранения данных.

- Требования сервера виртуализации:

Минимальные рекомендуемые характеристики компьютера для развертывания службы сервера виртуализации:

1) процессорная архитектура x86-64 с аппаратной поддержкой виртуализации (Intel VT, AMD-V);

2) центральный процессор (ЦП) — без последующих дополнительных нагрузок каждый модуль ЦП, закрепленный за одной ВМ, должен соответствовать физическому ядру ЦП в случае, если необходимо минимизировать конкуренцию ВМ за процессорные ядра. Например, при нагрузке в 40 виртуальных машин с двумя ЦП каждая, потребуются 80 физических ЦП. При этом 80 физических ЦП могут распределяться по различным серверам виртуализации: 10 компьютеров с восемью ядрами каждый или пять компьютеров с 16 ядрами каждый. При необходимости последующих дополнительных нагрузок архитектуру ЦП можно планировать заранее с помощью элементов CPU и VCPU: CPU определяет физические ЦП, закрепленные за виртуальными машинами, а VCPU — виртуальные ЦП, передаваемые гостевой операционной системой;

3) оперативная память — по умолчанию в ПК СВ отсутствует избыточно выделяемая память. Как правило, рекомендуется всегда предусматривать резерв 10 % по ресурсам, потребляемым гипервизором. Например, для нагрузки в 40 виртуальных машин с 2 ГБ оперативной памяти каждая необходимо около 90 ГБ физической памяти (с учетом ресурса оперативной памяти, потребляемый

гипервизором). Например, пять компьютеров с 24 ГБ оперативной памяти каждый предоставят по 22 ГБ памяти, поэтому они смогут выдержать планируемую нагрузку;

4) объем свободного системного дискового пространства — не менее 30 ГБ.

В каждом сервере виртуализации в зависимости от конфигурации хранилища и сети должно быть установлено до четырех сетевых интерфейсов: для сети экземпляров (приватной и/или публичной), сервисной сети и сети хранения данных.

Функции пользователя облачной платформы AIC

- Управление ВМ – создание, установка, включение и выключение ВМ
- Услуги сети – выбор сети для ВМ, балансировка трафика
- Заказ услуги Iaas
- Заказ услуги Paas
- Заказ услуги Saas

Сообщения пользователю

В ходе выполнения программы предусмотрен вывод сообщений двух типов: сообщение об ошибке и информационное сообщение.

Сообщение об ошибке отображается в следующих случаях:

- если при вводе данных были допущены ошибки, введено недопустимое значение или не заполнены поля, обязательные для заполнения;
- при сбоях в работе служб ПК СВ и ОС СН;
- при выполнении действий, недопустимых в соответствии с настроенной ролевой политикой.

Каждое такое сообщение содержит описание ошибки.

После выполнения пользователем определенных действий в ПК СВ (переход к разделу программы, сохранение данных) отображаются информационные сообщения. Такие сообщения не требуют каких-либо действий пользователя и скрываются автоматически.

Действия пользователя

При возникновении сообщения об ошибке пользователю следует выполнить следующие действия:

- Обратиться к администратору AIC – при ошибке сбоя в работе служб ПК СВ Брест
- Обратиться к администратору AIC – при ошибке сбоя в работе служб ALSE
- Откорректировать введенные значения или заполнить поля, обязательные к заполнению – при ошибке ввода данных

Перечень терминов

Администратор ВМ — пользователь, которому предоставляются права для выполнения действий по управлению экземпляром ВМ.

Администратор ОС СН — пользователь ОС СН, входящий в группу astra-admin,

которому предоставляются права для выполнения действий по настройке ОС, требующих привилегий суперпользователя root.

Администратор ПК СВ — пользователь, реализующий роль администратора средства виртуализации.

Разработчик ВМ — пользователь, которому предоставляются права для выполнения действий по созданию изменению конфигурации (шаблонов) виртуальных машин.

Настройка пользовательского интерфейса ПК СВ Брест

Настройка интерфейса происходит по Руководству пользователя ПК СВ Брест (описан порядок первичной настройки для пользователя).

Включает в себя разделы:

- Вход в веб-интерфейс
- Управление образами
  - Типы образов
  - Состояние образов
  - Создание образа
  - Клонирование образа
  - Отображение доступных образов
- Управление шаблонами виртуальной машины
  - Параметры шаблона ВМ
  - Создание шаблонов ВМ
  - Отображение доступных шаблонов и просмотр информации о шаблоне
  - Клонирование шаблонов
  - Удаление шаблонов
- Управление экземплярами ВМ
  - Статус и жизненный цикл виртуальной машины
  - Управление экземплярами ВМ в интерфейсе командной строки
  - Управление экземплярами ВМ в веб-интерфейсе ПК СВ
  - Снимки дисков
  - Экспорт диска ВМ
- Дополнительная настройка виртуальной машины
  - Контекстуализация
  - Автоматический ввод ВМ в домен через механизм контекста
- Удаленное подключение USB-устройств к ВМ по протоколам VNC/SPICE/RDP
- Ретрансляция PCI
  - Требования
  - Настройка сервера виртуализации
  - Настройка драйвера
  - Настройка использования PCI
- Настройка дискреционного и мандатного управление доступом к ВМ
- Отказоустойчивость виртуальной машины
- Автостарт виртуальных машин