

Требования к окружению

Оглавление

- # Условные размеры окружений и сайзинг аппаратного обеспечения
- # Особенности размещения ПО на серверах
- # Требования к системному программному обеспечению серверов, обслуживающей рабочую нагрузку
- # Требования к подсистеме мониторинга и операционной поддержки
- # Система непрерывной поставки CI/CD
- # Требования к стороннему программному обеспечению
- # Требования к балансировщику (входящие соединения)
 - # Обязательные
 - # Рекомендуемые
- # Требования к исходящим соединениям
 - # Обеспечение работы входа через ЕСИА
 - # Обеспечение работы Recaptcha
- # Ссылки

Условные размеры окружений и сайзинг аппаратного обеспечения

Характеристика	Размер S	Размер M	Размер L	Размер XL
Применение	IDM для сотрудников организации; Сервис, работающий в режиме MVP для ограниченной группы пользователей; Изучение возможностей UIDM; Интеграционный стенд	IDM для конечных пользователей, клиентская база до 5 млн (промышленная среда). Типовой интернет-банк	IDM для конечных пользователей, клиентская база 5...50 млн (промышленная среда). Оператор связи федерального уровня.	IDM для конечных пользователей, клиентская база 50...200 млн (промышленная среда)

Расчетная пиковая нагрузка, запросов в секунду	100	1000	5000	15000
--	-----	------	------	-------

Требования к серверу приложений

Количество серверов на дата-центр и всего	1	2	2 + 2	8 + 8
Количество виртуальных CPU	4 — 8	40	40	40
Количество RAM, гигабайт	8 — 16	64	64	64

Размер диска	30 гигабайт	100 гигабайт	300 гигабайт	300 гигабайт
Требования к серверу баз данных				
Количество серверов на дата-центр и всего	0 (БД устанавливается на сервер приложений) или 1	2	2 + 2 (часть серверов используется не под СУБД, а под быстрый кеш)	4 + 4 (часть серверов используется не под СУБД, а под быстрый кеш)
Количество виртуальных CPU	4 — 8	32	64	64
Количество RAM, гигабайт	8 — 16	64	64	128
Размер СХД (исходя из хранения данных аудита в течение трех лет)	0.1 терабайт	50 терабайт	500 терабайт	2 петабайта

Особенности размещения ПО на серверах

Указанные выше характеристики являются оценочными для первичного планирования инфраструктуры.

Каждый проект внедрения по своему уникален ввиду разнообразия принятых в организации подходов, способов размещения (bare metal, виртуальные машины, оркестратор), характера использования ПО пользователями.

Общие правила

1. Комплект ПО UIDM состоит из 5...10 сервисов в зависимости от функционального охвата.
2. Сервисы могут быть размещены как на одном сервере приложений (который, разумеется, дублируется), так и разнесены на несколько серверов по ролям.
3. ПО UIDM позволяет выполнять установку в конфигурации гео-распределенного кластера, поддерживаются варианты работы active-active и active-standby.
4. При разнесении ПО требования к CPU и RAM разбиваются пропорционально.
5. При разнесении ПО Требования к диску разбиваются сложнее, поскольку операционной системе для своей работы требуется приблизительно 20 гигабайт с учетом резерва. Следует вычесть требования под ОС, пропорционально разбить остаток, и к каждому получившемуся результату добавить обратно требования под ОС.
6. Точная оценка требований для промышленной среды возможна после проведения нагрузочного тестирования.

Требования к системному программному обеспечению серверов, обслуживающей рабочую нагрузку

Таблица 1. Запуск на bare-metal или виртуальных серверах

Требование	Предпочтительно	Альтернативно
ОС	RHEL7, Centos7, Astra Linux Special Edition 1.7 Воронеж, РедОС 7.3	RHEL6 как временная схема
Система виртуализации	Любая	Любая

Система виртуализации

любая

любая

root-доступ

Требуется для инсталляции и запуска сервисов в ручном режиме, если понадобится

Таблица 2. Запуск в docker

Требование	Предпочтительно	Альтернативно
ОС	RHEL7, Centos7, Astra Linux Special Edition 1.7 Воронеж, РедОС 7.3	Другие Linux дистрибутивы, принятые на обслуживание у Заказчика и поддерживающие запуск Docker
Система виртуализации	Любая	Любая
Система контейнеризации	Docker	Запуск ПО без контейнеров, в общем пространстве процессов
Оркестратор	Kubernetes,OpenShift	Запуск ПО без оркестратора, на VM

Требования к подсистеме мониторинга и операционной поддержки

Требование	Предпочтительно	Альтернативно
Система сбора метрик	Prometheus	Другая система, поддерживающая сбор по протоколу Prometheus либо в JSON формате.
Система централизованного протоколирования	Graylog	Другая система, поддерживающая сбор по протоколу GELF UDP

Система непрерывной поставки CI/CD

Требование	Предпочтительно	Альтернативно
Система сборки	Gitlab	Jenkins
Система версионирования кода/ конфигурации	Gitlab	Другая, git-совместимая
Система хранения артефактов	Nexus	Другая, предоставляющая maven api, docker registry api, npm api

Требования к стороннему программному обеспечению

Требование	Предпочтительно	Альтернативно
------------	-----------------	---------------

Java

Oracle JDK 1.8, Axiom JDK Pro OpenJDK 1.8^[1]

РСУБД^[2]

Postgresql

Oracle не ниже 11.2^[3]

Требования к балансировщику (входящие соединения)

Обязательные

1. Балансировка: round-robin балансировка между всеми рабочими узлами, протоколы HTTPS и HTTP. Проксирование HTTPS на порт 443 Ingress. Редирект HTTP на HTTPS с отдачей HSTS заголовка.
2. SSL termination : Терминирование внешней SSL сессии (HTTPS) (сертификат должен находиться на балансировщике, а не в RooX UIDM)
3. Отказоустойчивость: Доступность не меньше чем RooX UIDM – 99.99%
4. Client IP translation: передавать настоящий IP адрес клиента в HTTP заголовке X-Forwarded-For. Запрещать прием такого заголовка от пользователя.

Рекомендуемые

1. Средства безопасности: TCP header validation, TCP window-size checking, DoS and DDoS checking, проверка SSL Labs (или аналогичная) Rating A.

Требования к исходящим соединениям

Обеспечение работы входа через ЕСИА

Доступ по протоколу HTTPS 443 к серверам <https://esia-portal1.test.gosuslugi.ru> , <https://esia.gosuslugi.ru> .

Обеспечение работы Recaptcha

Необходим доступ по протоколу HTTPS по порту 443 к серверам <https://www.google.com> (Точный URL <https://www.google.com/recaptcha/api/siteverify>).

ЗАМЕТКА

Допустимо предоставление исходящих подключений через HTTP-прокси, в таком случае потребуется настройка JVM.

Ссылки

[Калькулятор сайзинга Tarantool](#)

¹. Работа UIDM на JRE других вендоров допустима, но не тестируется на постоянной основе. Тестирование может быть заказано в составе услуг расширенной техподдержки.

² В графе РСУБД указаны требования для базы данных UIDM, которая используется для хранения собственных

2. В графе «СУБД» указаны требования для СУБД данных клиента, которая используется для хранения соответствующих данных и аудита. Доступно подключение других СУБД в качестве legacy источников пользовательских профилей. Для таких сценариев допустима любая РСУБД, для которой существует JDBC драйвер, работающий для JRE версии 1.8.

3. Допустимо использование Oracle Standard Edition для инсталляций размера **S** при условии, что архивные записи аудита перекладываются или удаляются на периодической основе (ввиду того, что в Standard Edition не поддерживаются секции).

