Общество с ограниченной ответственностью «ХОСТ Информационные системы»

УТВЕРЖДАЮ Директор ГБУЗС «МИАЦ»	УТВЕРЖДАЮ Генеральный директор ООО «ХОСТ ИС»
_____ О.В. Роменский	_____ К.Ю. Суслов
«___» _____ 2020 г.	«___»_____ 2020 г.

МОДЕРНИЗАЦИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ «РЕГИОНАЛЬНЫЙ КОММУНИКАЦИОННЫЙ СЕРВИС» В ЧАСТИ РАЗРАБОТКИ ПОДСИСТЕМЫ «СЛУЖБА КАТАЛОГОВ» В ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ ЗДРАВООХРАНЕНИЯ СЕВАСТОПОЛЯ «МЕДИЦИНСКИЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЦЕНТР»

ОПИСАНИЕ СИСТЕМЫ

75746556.425190.003.СК.П9

2020

Содержание

1 Общие данные

1.1 Полное наименование системы и ее условное обозначение

Полное наименование системы: Региональный коммуникационный сервис.

Условное обозначение системы: система.

1.2 Наименование предприятий Заказчика и Исполнителя и их реквизиты

Заказчиком на выполнение работ по модернизации системы является Государственное бюджетное учреждение здравоохранения Севастополя «Медицинский информационно-аналитический центр». Юридический адрес предприятия Заказчика: 299014, г. Севастополь, улица Рыбаков, 7.

Исполнителем работ по модернизации системы является Общество с ограниченной ответственностью «ХОСТ Информационные системы». Юридический адрес предприятия Исполнителя: 620026, Свердловская область, г. Екатеринбург, ул. Энгельса, д. 36, тел. (343) 216-16-32, факс (343) 216-16-31, e-mail: service@hostco.ru.

1.3 Назначение и цели создания системы

Система предназначена для:

– управления совместной деятельностью и коммуникациями внутри организации;

– предоставления возможности взаимодействий в виде планирования деятельности и осуществления коммуникаций между сотрудниками организации с помощью различных каналов, а также хранения и обмена файлами, контактами, календарями, списками задач, адресными книгами.

– предоставления системным администраторам организации инструмента для управления учетными записями сотрудников, для организации доменной инфраструктуры;

– предоставления системным администраторам организации инструмента для управления DNS-записям доменной инфраструктуры.

2 Описание компонентов системы

2.1 Общее описание системы

Система размещается на отдельном физическом сервере в виде нескольких ВМ в информационно-телекоммуникационной инфраструктуре организации

и обеспечивает доступ к функциям, представленным в разделе Технического задания «2.2. Требования к функциям (задачам), выполняемым Системой», с помощью двух веб-интерфейсов (пользовательского и административного).

Система основана на продукте Zimbra Collaboration Open Source Edition 8.8.11.

В систему интегрированы следующие подсистемы:

- сервис облачного хранилища Nextcloud 13;
- сервис онлайн-редактора OnlyOffice CE 5.2.8;
- сервис VoIP-телефонии Asterisk 13 (FreePBX 13);
- сервис службы каталогов SAMBA 4.10.6 (LDAP Account Manager 6.8);
- сервис DNS BIND 9.11.4.

Подсистемы интегрированы с помощью отдельных модулей.

Доступ к веб-интерфейсам системы осуществляется с помощью сервиса Gluu 3.1.6, который обеспечивает SSO-авторизацию в систему и подсистемы после авторизации с помощью логина и пароля в любой из подсистем.

Управление системой и подсистемами осуществляется с помощью единого веб-интерфейса для администратора.

Состав аппаратного обеспечения, который использовался в рамках внедрения системы, приведен в Таблице 1 (предоставлялось Заказчиком).

Таблица 1 – Аппаратное обеспечение системы

№ п/п	Наименование	Кол-во	Описание
1	Сервер для	1	– процессор(ы): Intel/AMD 2.0 GHZ+ 64-bit CPU

№ п/п	Наименование	Кол-во	Описание
	сервиса электронной почты, IP-телефонии		(для ВМ, минимум 4 vCPU); – ОЗУ: 10 Гб; – свободное место в ОС для ПО и логов: 15 Гб; – свободное место в ОС для почтовых ящиков: минимум 20 Гб; – свободное место в ОС для хранения записей звонков: 20 Гб. Опционально: – высокопроизводительная дисковая подсистема (SSD, 15K PRM или 10K PRM-диски); – отказоустойчивая дисковая подсистема (RAID1, RAID5)
2	Сервер для облачного хранилища, онлайн-редактора	1	– процессор(ы): Intel/AMD 2.0 GHZ+ 64-bit CPU (для ВМ, минимум 4 vCPU); – ОЗУ: 8 Гб; – свободное место в ОС для ПО и логов: 5 Гб; – свободное место в ОС для хранения файлов: минимум 20 Гб. Опционально: отказоустойчивая дисковая подсистема (RAID1, RAID5)
3	Сервер для службы каталогов, DNS-сервиса, SSO-сервиса	1	– процессор(ы): Intel/AMD 2.0 GHZ+ 64-bit CPU (для ВМ, минимум 4 vCPU); – ОЗУ: 4 Гб; – свободное место в ОС для ПО и логов: 10 Гб; – свободное место в ОС для хранения файлов: минимум 20 Гб. Опционально: отказоустойчивая дисковая подсистема

Состав ПО, которое использовалось в рамках внедрения системы, приведен в Таблице 2.

Таблица 2 – Состав ПО

№ п/п	Наименование	Кол-во	Описание
1	Zimbra 8.8.11	1	ПО для совместной работы
2	Asterisk 13.27.1	1	VoIP АТС Asterisk
3	FreePBX 13.0.196.1	1	Веб-интерфейс управления VoIP АТС Asterisk
4	Nextcloud 13.0.12	1	ПО для облачного хранения файлов
5	OnlyOffice CE 5.2.8	1	ПО онлайн-редактора
6	SAMBA 4.6.10	1	ПО службы каталогов

№ п/п	Наименование	Кол-во	Описание
7	BIND 9.11.4	1	ПО DNS-сервера
8	LDAP Account Manager 6.8	1	Веб-интерфейс управления службой каталогов и DNS-сервисом
9	Gluu 3.1.6.sp1	1	ПО для обеспечения SSO

2.2 Описание работы системы

2.2.1 ПО сервера

На сервер установлена модернизированная ОС на основе Centos 7.1908, в рамках которой запущена виртуализация HOSTVM на основе oVirt 4.3.8. В рамках данной виртуализации развернуты ВМ с основными компонентами системы.

2.2.2 Zimbra

Основным компонентом системы является ПО Zimbra, которое размещено на отдельном сервере вместе с ПО VoIP-телефонии и ее веб-интерфейсом. Доступ пользователей к данному компоненту осуществляется с помощью веб-интерфейса, а также сервисных протоколов, связанных с отправкой/приемом электронной почты.

ПО позволяет работать с почтой, а также управлять контактами, встречами, задачами и т.д. Для всех этих действий ПО Zimbra запускает 19 внутренних служб, которые обеспечивают выполнение отдельных функций системы.

Информация о настройках системы, учетных записях пользователей и их настройках хранится на интегрированном в Zimbra LDAP-сервере.

В роли MTA выступает интегрированный Postfix. Он же обеспечивает работу всех почтовых протоколов.

Для увеличения гибкости системы (например, для возможности размещения Zimbra на нескольких серверах) в ней используется интегрированный прокси-сервер Nginx, который отвечает за перенаправление трафика, а также его кэширование при необходимости.

По умолчанию в Zimbra через прокси-сервер предоставляются следующие порты:

– **25** порт для входящей почты в Postfix;

– **80** порт для незащищенного подключения к веб-клиенту Zimbra;

– **110** порт для получения почты с удаленного сервера по протоколу POP3;

– **143** порт для доступа к электронной почте по протоколу IMAP;

– **443** порт для защищенного подключения к веб-клиенту Zimbra;

– **587** порт для входящей почты с защитой соединения;

– **993** порт для защищенного доступа к электронной почте по протоколу IMAP;

– **995** порт для защищенного получения почты с удаленного сервера по протоколу POP3;

– **5222** порт для подключения к серверу по протоколу XMPP;

– **5223** порт для защищенного подключения к серверу по протоколу XMPP;

– **9071** порт для защищенного подключения к администраторской консоли.

Внутренние же порты, которые фактически открыты службами, это:

– **389** порт для незащищенного подключения к LDAP;

– **636** порт для защищенного подключения к LDAP;

– **3310** порт для подключения к антивирусу ClamAV;

– **5269** порт для общения между серверами, находящимися в одном кластере по протоколу XMPP;

– **7025** порт для локального обмена почтой по протоколу LMTP;

– **7047** порт, используемый сервером для конвертирования вложений;

– **7071** порт для защищенного доступа к администраторской консоли;

– **7072** порт для обнаружения и аутентификации в Nginx;

– **7073** порт для обнаружения и аутентификации в SASL;

- **7110** порт для доступа к внутренним службам POP3;
- **7143** порт для доступа к внутренним службам IMAP;
- **7171** порт для доступа к демону конфигурации Zimbra zmconfigd;
- **7306** порт для доступа к MySQL;
- **7780** порт для доступа к службе проверки правописания;
- **7993** порт для защищенного доступа к внутренним службам IMAP;
- **7995** порт для защищенного доступа к внутренним службам POP3;
- **8080** порт для доступа к внутренним службам HTTP;
- **8443** порт для доступа к внутренним службам HTTPS;
- **8735** порт для общения между почтовыми ящиками;
- **8736** порт для доступа к службе распределенной настройки Zextras;
- **10024** порт для общения Amavis с Postfix;
- **10025** порт для общения Amavis с OpenDKIM;
- **10026** порт для настройки политик Amavis;
- **10028** порт для общения Amavis с фильтром контента;
- **10029** порт для доступа к архивам Postfix;
- **10032** порт для общения Amavis со спам-фильтром SpamAssassin;
- **23232** порт для доступа к внутренним службам Amavis;
- **23233** порт для доступа к SNMP-responder;
- **11211** порт для доступа к memcached.

Для данного ПО был написан модуль OpenIDConnect для объединения с сервисом Gluu и обеспечения SSO-авторизации между подсистемами.

Для осуществления возможностей, описанных в Техническом задании, были модифицированы модули Zimbra Drive, Universal Dialer, а также разработан модуль host_nextcloud для объединения с подсистемой облачного сервиса.

Выполнены работы по дизайну и верстке пользовательского веб-интерфейса Zimbra, а также модификации административного интерфейса Zimbra для работы с подсистемами.

В процессе развертывания для организации Заказчика создается почтовый домен, который будет интегрирован с сервисом службы каталогов (для автоматического создания учетных записей).

Подготовлен скрипт для привязки внутренних номеров к учетным записям Zimbra.

2.2.3 Asterisk и FreePBX

Сервис VoIP-телефонии развернут с помощью СПО Asterisk и веб-интерфейса FreePBX. Данное ПО размещается на ВМ вместе с почтовым сервисом.

Asterisk использует в своей работе UDP-порты 5160, 5060, 10000-20000.

Со стороны Zimbra к сервису Asterisk напрямую обращается модуль Universal Dialer.

Для данного веб-интерфейса была настроена SSO-авторизация через GLUU с помощь модуля Apache mod_auth_oidc, а также написан дополнительный модуль (Return Calls) для выполнения возможностей, описанных в Техническом задании.

Для возможности управления IP-телефонией пользователь должен входить в группу Domain Admins из службы каталогов.

2.2.4 Nextcloud

Облачного хранилище основывается на базе СПО Nextcloud, которое размещено на отдельной ВМ в рамках сервера. Его основное назначение – облачное хранение файлов и предоставление доступа к ним.

Для предоставления данных возможностей со стороны Zimbra используются модули Zimbra Drive и host_nextcloud, со стороны Nextcloud – модуль Zimbra Drive for Nextcloud, который был модифицирован для работы с Gluu.

Для объединения с Gluu в облачное хранилище установлен модуль GluuSSO, который был модифицирован для увеличения стабильности работы.

2.2.5 OnlyOffice

Возможности облачного хранилища были расширены путем установки и настройки редактора OnfyOffice, который позволяет создавать и редактировать документы в облачном хранилище. Также для документов доступно

совместное редактирование. Сервис развернут на той же ВМ, что и Nextcloud.

2.2.6 SAMBA и LDAP Account Manager

Сервис службы каталогов развернут с помощью СПО SAMBA и веб-интерфейса LDAP Account Manager. Его основное назначение – возможность создания домена для централизованного управления пользователями и группами пользователей, а также DNS-записями домена.

СПО LDAP Account Manager было модернизировано для возможности управления DNS-записями из сервиса BIND с помощью веб-интерфейса. Также была проведена модернизация для возможности доступа с помощью SSO-авторизации через модуль mod_auth_oidc.

2.2.7 BIND

Сервис BIND используется для обслуживания DNS-запросов, касающихся записей службы каталогов (домена), а также прочих зон при необходимости. Сервис взаимодействует со службой каталогов с помощью промежуточного модуля для взаимодействия с ldb-файлами.

2.2.8 Gluu

Сервис Gluu развернут на ВМ с сервисом службы каталогов. Сервис обязательно имеет свой адрес веб-интерфейса для обслуживания авторизации пользователей.

Данный сервис может выполнять авторизацию в различных системах с помощью различных клиентских модулей, за счет чего пользователь, введя пароль один раз, может получить возможность SSO-авторизации в настроенных на работу с Gluu интерфейсах и сервисах.

Для корректной работы сервиса SSO-авторизации необходим валидный wildcard SSL-сертификат, который требуется своевременно обновлять.

В развернутой системе основным клиентом для выполнения авторизации является OpenID.

Сервис Gluu подключается к сервису службы каталогов (AD) от доменного пользователя Gluu, размещенного в OU ServiceUsers (данного пользователя нельзя перемещать из текущего расположения AD, иначе сервис не сможет подключаться), и проверяет корректность введенных данных пользователя.

Общий процесс авторизации (см. Рисунок 1):

– пользователь обращается к интерфейсу/приложению, в котором он хочет авторизоваться;

– интерфейс/приложение перенаправляет запрос на сервер Gluu;

– пользователь проходит авторизацию в Gluu (данные передаются в AD), после чего данные сессии сохраняются на сервере, затем выполняется редирект в интерфейс/приложение.

Сервис Gluu установлен в окружении chroot (/opt/gluu-server-3.1.6). В нем же запущен сервис Apache2 и сервисы identity и oxauth, которые участвуют в процессе авторизации.

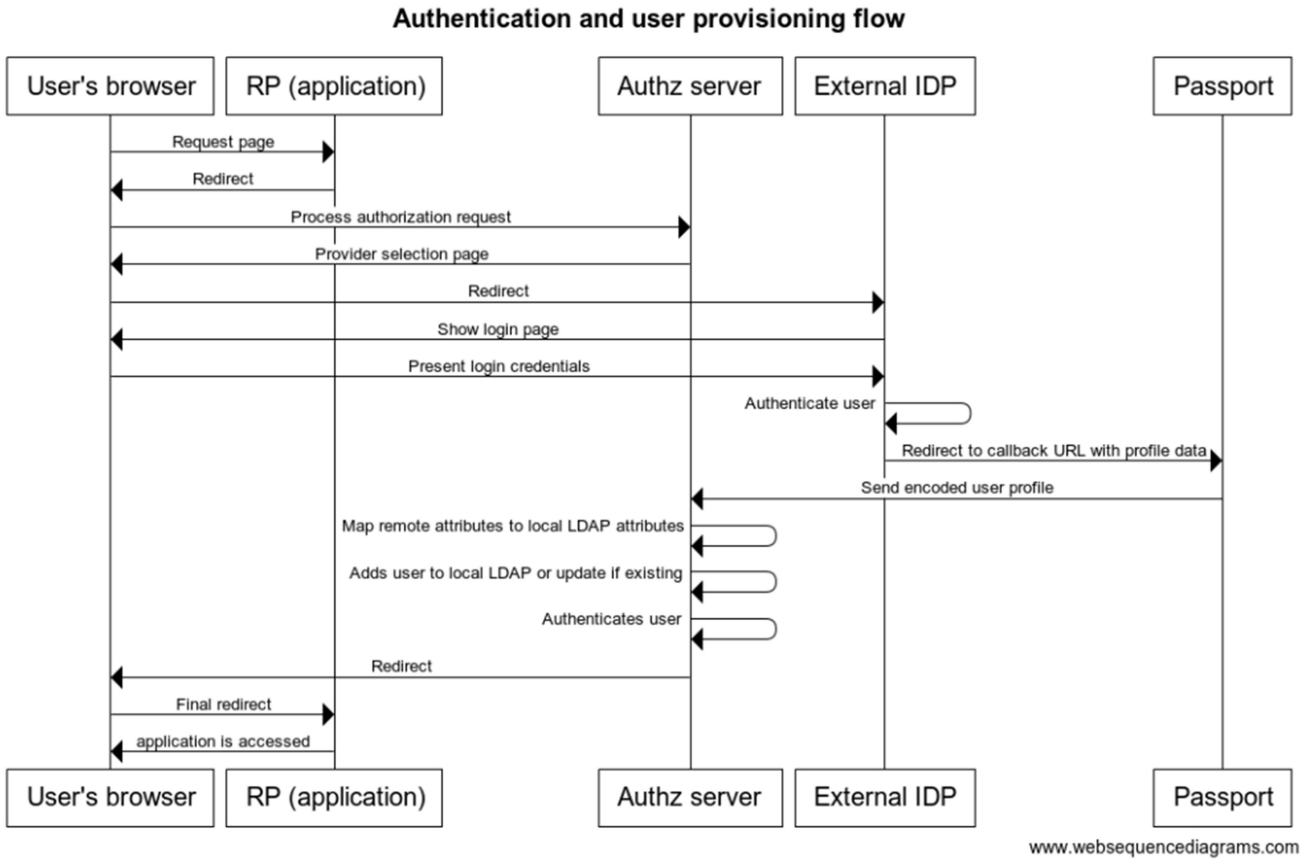

Рисунок 1 – Процесс авторизации

Перечень сокращений

AD – Active Directory

CPU – Central Processing Unit

IMAP – Internet Message Access Protocol

IP – Internet Protocol

LDAP – Lightweight Directory Access Protocol

LMTP – Local Mail Transfer Protocol

MTA – Mail Delivery Agent

PRM – Package Manager

SNMP – Simple Network Management Protocol

SSO – Single Sign-On

UDP – User Datagram Protocol

VoIP – Voice over Internet Protocol

XMPP – eXtensible Messaging and Presence Protocol

АТС – Автоматическая телефонная станция

ВМ – Виртуальная машина

ОЗУ – Оперативное запоминающее устройство

ОС – Операционная система

ПО – Программное обеспечение

СПО – Свободное программное обеспечение