

[Виллариба] — Техническая документация инфраструктуры

Версия: 1001
Дата последнего обновления: 9999-12-31
Ответственный инженер: Т-1000
Статус: draft

Оглавление

1. Паспорт клиента
2. Архитектура и стандарты
3. Глобальные сервисы
4. Межобъектная связность
5. Объекты / площадки
6. Бэкапы и восстановление
7. Мониторинг и эксплуатация
8. Информационная безопасность
9. Контакты, контрагенты и доступы
10. Риски, техдолг, временные решения
11. Журнал изменений
12. Приложения

1. Паспорт клиента

1.1 Общая информация

- Клиент: Виллариба
- Юр. лицо: ООО "Виллариба"
- ID клиента: VLRB
- Имя на латинице: villariba
- Основной контакт (куратор): Марио, +79991234567, mario@world1-1.it
- Доп. контакты: Луиджи, +79997654321, luigi@villariba.it
- Количество сотрудников: 38
- Количество рабочих мест: 30
- Количество объектов / площадок: 2
- Основной режим работы: office

VIP-сотрудники

Информация не зафиксирована. Требуется уточнения со стороны клиента.

1.2 Краткое описание инфраструктуры

- Количество объектов: 2
- Серверы / виртуализация: 4 физических сервера (2 гипервизора Proxmox, 1 выделенный 1C/SQL, 1 backup-сервер); 5 виртуальных машин

- Домен: Да, Active Directory
- VPN между объектами: Да
- Где живут файлы: VLRB-SRV-NAS (TrueNAS, виртуальная машина)
- Где живёт 1С: VLRB-SRV-1C, физический сервер 1С + Microsoft SQL Server
- Где размещена почта: VLRB-SRV-MAIL (Mailcow)
- Есть ли резервный интернет: Да
- Есть ли видеонаблюдение / телефония / Wi-Fi контроллер: Да / Нет / Да

1.3 Список объектов

Объект	Полный адрес	Назначение	Сотрудники	Рабочие места	Комментарий
Офис	Via delle Magnolie 18, 20145 Milano, Italia	Центральный офис	25	25	Центральная площадка
Пиццерия	Strada Colle Sereno 7, 50125 Firenze, Italia	Филиал	13	5	Завязана на центральные сервисы

1.4 Матрица объектов

Объект	ПК	Ноутбуки	Принтеры	WiFi AP	Коммутаторы	Камеры	Локальные серверы / NAS
Офис	21	4	3	2	2	4	4 / Да
Пиццерия	4	1	1	3	2	10	Нет / Нет

Детальная инвентаризация ПК, ноутбуков, принтеров и серверов ведётся в GLPI: [\[LINK на GLPI\]](#)

1.5 Ключевые сервисы и их размещение

Сервис	Критичность	Где живёт	Кому нужен	Зависимости / комментарий
Интернет / Firewall	Critical	Офис / Серверная	Все объекты	VLRB-ML-GW-01, провайдеры
Гипервизоры	Critical	Офис / Серверная	IT	Proxmox на Dell R740
AD / Домен / DNS	Critical	Офис / Серверная	Все	VLRB-SRV-DC01 / VLRB-SRV-DC02
Файловые сервисы	High	VLRB-SRV-NAS	Все	TrueNAS VM, зависит от AD
1С / SQL	High	Офис / Серверная	Все	VLRB-SRV-1C
Почта	High	Офис / Серверная	Все	VLRB-SRV-MAIL, зависит от DNS/MX
VPN / связность	High	Офис / VLRB-ML-GW-01	Офис, Пиццерия, IT	GRE over IPsec + OpenVPN
Backup-repository	High	Офис / VLRB-SRV-BKP	IT	PBS на отдельном физ. сервере
Мониторинг	Medium	ITMAK	IT	Централизованный
Видеонаблюдение	Medium	На каждом объекте	Руководство	Локальные NVR

2. Архитектура и стандарты

2.1 Общая логика

- Количество площадок: 2
- Связность: Site-to-Site VPN (GRE over IPsec) — основной; OpenVPN — резервный + Client-to-Site
- Центральный узел: **Офис**
- Где размещены серверы: **Офис / серверная**
- Локальная зависимость объектов: на местах автономно сохраняются локальная сеть и видеонаблюдение; доступ к 1С, файлам, почте, домену зависит от VPN и офиса

2.2 Схемы

- Общая схема: [LINK]
- Межобъектная связность: [LINK]
- Глобальная схема сервисов: [LINK]

2.3 Стандарты именования

Hostname

Применяются правила из Регламента именования ИТ-оборудования (ссылка). Виллариба — клиент с двумя объектами без деления по отделам, поэтому используется следующая схема.

Коды объектов:

Код	Объект
ML	Милан (центральный офис)
FL	Флоренция (филиал)

Форматы имён:

Тип устройства	Формат	Пример
Рабочие станции	VLRB-WS-OO-NN	VLRB-WS-ML-08
Ноутбуки	VLRB-NB-OO-NN	VLRB-NB-FL-01
Серверы	VLRB-SRV-ROLE[NN]	VLRB-SRV-DC01, VLRB-SRV-1C
Маршрутизаторы	VLRB-OO-GW-NN	VLRB-ML-GW-01
Коммутаторы	VLRB-OO-SW-NN[-HINT]	VLRB-ML-SW-02-POE
Точки Wi-Fi	VLRB-OO-AP-NN	VLRB-ML-AP-01
Принтеры	заводской hostname	KM45A123
Видеорегистраторы	VLRB-OO-NVR-NN	VLRB-ML-NVR-01
Камеры	VLRB-OO-CAM-NN	VLRB-FL-CAM-10

Принтеры — всего 4 штуки, порог перехода на регламентные имена (более 20 принтеров) не достигнут, используем заводские hostname. Модель устройства в имя не включается — она в GLPI.

Адресация

Логика VLAN:

VLAN ID	Назначение	Подсеть
1	Основная сеть	10.100.XYZ.0/24
11	Гостевая сеть	10.111.XYZ.0/24

VLAN ID	Назначение	Подсеть
22	Видеонаблюдение	10.22.XYZ.0/24
99	IT Management	10.99.XYZ.0/24

(XYZ — кодовый номер объекта: Офис = 1, Пиццерия = 2)

Логика IP:

Диапазон	Назначение
.1	Роутеры
.2-9	Коммутаторы
.10-.29, .100	Серверы
.30-.70	Видеонаблюдение
.80-.90	Принтеры
.91-.99	Точки Wi-Fi
.101-.199	DHCP пул

DHCP везде, кроме роутеров и коммутаторов. Для основных сервисов — статика или резервирование.

Доступы и пароли

- Хранилище паролей: **Bitwarden**
- Формат ссылки в документации: **ID_XXXXXXXXXXXXXXXXX** (префикс ID_ + 16 символов: буквы разного регистра и цифры)
- Как искать: вставить ID целиком в строку поиска Bitwarden
- Доступ по группам/ролям через доменные группы AD по ролевой модели
- Локальные администраторы: только IT через отдельные админские учётки
- Принцип минимально достаточных прав
- Ответственные за актуальность: **ITMAK** и **согласованные ответственные со стороны клиента**

Пароли, recovery codes, ключи и иные секреты в документе не хранятся. Фиксируются только ID записей в Bitwarden.

3. Глобальные сервисы

3.1 Домены, DNS, внешние сервисы

Сервис	Платформа / провайдер	Панель управления	Bitwarden ID
Домен и хостинг	reg.ru	https://www.reg.ru/account	ID_XXXXXXXXXXXXXXXXX
DNS	Cloudflare	https://dash.cloudflare.com/	ID_XXXXXXXXXXXXXXXXX
Почта	Локальный (Mailcow)	https://mx.villariba.it/admin	ID_XXXXXXXXXXXXXXXXX
Телефония	Нет	—	—
Облачные сервисы	Нет	—	—

3.2 Домен / AD

- Есть: **Active Directory**
- FQDN / NetBIOS: **vcorp.villariba.it / VCORP**

- Контроллеры: VLRB-SRV-DC01 (основной, VLRB-SRV-HV01), VLRB-SRV-DC02 (резервный, VLRB-SRV-HV02); репликация между узлами.
- DNS: интегрирован с AD; зона домена обслуживается DC01 и DC02; резервный DNS реализован через роутер с переадресацией запросов локального домена на DC01.
- Основные OU: Users, Computers, Servers, Admin
- Основные GPO: стандартная политика AD, развёртывание ПО, параметры пользователей и компьютеров
- Особенности: нет

3.3 Почта

- Домен: villariba.it
- Решение: Mailcow
- Количество ящиков: 32
- Общие ящики: info@villariba.it, accounting@villariba.it, sales@villariba.it
- Внешний адрес: mx.villariba.it
- Внутренний адрес: VLRB-SRV-MAIL
- Способ доступа: IMAP
- Панель управления: <https://mx.villariba.it/admin>, доступ ID_XXXXXXXXXXXXXXXXXX
- Правила формирования адресов: не зафиксировано, требует уточнения
- Кто управляет: ITMAK
- MFA: нет

3.4 1C

- Конфигурации: 1C:Бухгалтерия, 1C:Управление торговлей
- Режим: client-server
- Количество пользователей: 20
- Где живёт база: VLRB-SRV-1C, Microsoft SQL Server
- 1C программист / подрядчик: не зафиксировано, требует уточнения по договору

Базы

Конфигурация	Организации	Тип базы	Сервер 1C	SQL	Строка подключения	Авторизация	Комментарий
1C:Бухгалтерия	—	серверная	VLRB-SRV-1C	VLRB-SRV-1C (MSSQL)	—	—	Бухгалтерия
1C:Управление торговлей	—	серверная	VLRB-SRV-1C	VLRB-SRV-1C (MSSQL)	—	—	Все сотрудники

Доступ к 1C из офиса и филиала через межофисный VPN. Работа зависит от VLRB-SRV-1C, MSSQL, AD и VPN.

Лицензирование 1C

- Тип: серверная лицензия + клиентские, программные
- Количество: 20
- Где хранятся ключи: Bitwarden, ID_XXXXXXXXXXXXXXXXXX

ИТС

- Наличие: не зафиксировано
- Комментарий: требуется указать партнёра 1C, номер договора и срок действия сопровождения

Особенности / доработки

- Информация о нетиповых доработках и кастомизациях должна вестись отдельно. В текущей версии документа не зафиксировано.

3.5 Файловые сервисы

- Сервер / NAS: VLRB-SRV-NAS (TrueNAS, виртуальная машина на VLRB-SRV-HV02)
- Основные шары: Общие документы, Бухгалтерия, Обмен, Руководство, Scan, Архив
- Логика прав: по доменным группам AD
- Снэпшоты: есть, ZFS
- Особенности: централизованное хранение файлов в офисе, доступ с филиала через VPN; квоты / FSRM не используются

3.6 Серверы и виртуализация

Физические серверы

Имя	Модель	CPU	RAM	Накопители / RAID	Локация	Роль	GLPI
VLRB-SRV-HV01	Dell R740	2x Intel Xeon Gold 6254	64 GB DDR4	480GB ZFS RAID1 SATA SSD + 3.2TB ZFS RAID1 NVMe	Офис / Серверная	Hypervisor	[LINK]
VLRB-SRV-HV02	Dell R740	2x Intel Xeon Gold 6244	64 GB DDR4	480GB ZFS RAID1 SATA SSD + 18TB ZFS RAID1 HDD 3.5	Офис / Серверная	Hypervisor	[LINK]
VLRB-SRV-1C	Desktop	AMD Ryzen 9 9950X	128 GB DDR5	480GB Soft RAID1 SATA SSD + 400GB NVMe Optane	Офис / Серверная	1C + SQL	[LINK]
VLRB-SRV-BKP	Dell R720	1x Intel Xeon E5-2630 v2	32 GB DDR3	480GB ZFS RAID1 SATA SSD + 40TB ZFS RAIDZ2 HDD 3.5	Офис / Серверная	Backup (PBS)	[LINK]

Доступ к консоли (IPMI/ILO) и админ-доступы: искать в Bitwarden по имени сервера.

Виртуализация

- Платформа: Proxmox
- Кластер: нет, отдельные узлы
- Storage: hybrid (локальные хранилища гипервизоров + NAS / TrueNAS)
- Панель управления: URL гипервизоров, доступ ID_XXXXXXXXXXXXXXXXXX
- Особенности: VM распределены по двум физическим узлам; контроллеры домена на разных узлах; backup через отдельный физический сервер VLRB-SRV-BKP с Proxmox Backup Server (PBS)

Виртуальные машины

Имя	ОС	vCPU	RAM	Disk	Роль	Критичность	Гипервизор
VLRB-SRV-DC01	Windows Server	4	8 GB	80 GB	AD / DNS	Critical	VLRB-SRV-HV01
VLRB-SRV-DC02	Windows Server	4	8 GB	80 GB	AD / DNS	Critical	VLRB-SRV-HV02
VLRB-SRV-NAS	TrueNAS	4	16 GB	18 TB	File server / storage	High	VLRB-SRV-HV02
VLRB-SRV-MAIL	Debian Linux	8	16 GB	320 GB	Mailcow	High	VLRB-SRV-HV01

Имя	ОС	vCPU	RAM	Disk	Роль	Критичность	Гипервизор
VLRB-SRV-DEB01	Debian Linux / Docker	8	4 GB	80 GB	Контейнеры	Medium	VLRB-SRV-HV01

3.7 Лицензирование

Информация о лицензировании зафиксирована не полностью и требует доактуализации.

Лицензии:

Вендор	Продукт	Тип лицензии	Тип активации	Кол-во	Bitwarden ID	Комментарий
1C	Серверная лицензия	программная	ключ	1	ID_XXXXXXXXXXXXXXXXXX	На VLRB-SRV-1C
1C	Клиентские лицензии	программная	ключ	20	ID_XXXXXXXXXXXXXXXXXX	

Остальные лицензии (ОС, Office, антивирус и т.д.) требуют актуализации.

3.8 Прочие сервисы

Сервис	Где	Назначение	Комментарий
Мониторинг	ITMAK	Контроль инфраструктуры	Централизованный
Антивирус DrWeb	DrWeb Server на VLRB-SRV-DC02	Централизованная защита	Агенты на всех ПК
Backup-repository	VLRB-SRV-BKP	Хранение резервных копий	PBS

4. Межобъектная связность

4.1 Общая логика

- Объекты связаны: **постоянный Site-to-Site VPN**
- Центральная площадка: **Офис**
- Что доступно между объектами: **AD / DNS, файловые ресурсы, 1C, почта, админ-доступ IT**
- При потере связи сохраняется: **локальная сеть и CCTV; недоступны 1C, файлы, домен, почта**

4.2 VPN-каналы

Точка А	Точка В	Тип	Назначение	Комментарий
Офис (55.66.77.88)	Пиццерия (99.88.77.66)	GRE over IPsec	Основной межофисный туннель	Основной канал
Офис (OpenVPN сервер)	Пиццерия (OpenVPN клиент)	OpenVPN	Резервный туннель + Client-to-Site	Резервный канал

4.3 Матрица зависимостей

Если недоступно	Что перестаёт работать	Какие объекты затронуты
Офис / серверная	1C, файлы, почта, AD, централизованные сервисы	Все объекты
VPN Офис–Пиццерия	Доступ филиала к 1C, файлам, домену	Пиццерия

Если недоступно	Что перестаёт работать	Какие объекты затронуты
Интернет на объекте	VPN, почта, удалённый доступ	Соответствующий объект
VLRB-SRV-DC01 и DC02	Аутентификация AD, DNS домена	Все объекты
VLRB-SRV-1C	Работа 1C	Все объекты
VLRB-SRV-NAS	Доступ к общим файлам	Все объекты

5. Объекты / площадки

5.1 Офис

Паспорт объекта

- Название: **Офис**
- ID объекта: **MLN01**
- Адрес: **Via delle Magnolie 18, 20145 Milano, Italia** ([Карта](#))
- Назначение: **Центральный офис**
- Контакт на объекте: **Марио / +79991234567**
- Режим работы: **office**
- Сотрудников: **25** / Рабочих мест: **25**

Как добраться и логистика

- Как добраться: не зафиксировано, требует заполнения.
- Пропускной режим: не зафиксировано.
- Парковка: не зафиксировано.
- Место хранения ИТ-вещей: не зафиксировано.

Общая локальная логика

Центральная площадка всей инфраструктуры. В серверной размещены гипервизоры, физический сервер 1C, сервер резервного копирования и центральное сетевое оборудование. Отсюда предоставляются AD, DNS, 1C, почта, файловые сервисы и управление Wi-Fi. Локально также работает видеонаблюдение офиса. Основной и резервный интернет-каналы.

Физическая структура

- Шкафы / стойки: **1 серверная стойка 32U, 750mm**
- Кабельная система: **СКС для рабочих мест, серверной и камер**
- Интернет-ввод: **основной и резервный провайдер в серверную**
- PoE: **используется для камер и AP через управляемый PoE-коммутатор VLRB-ML-SW-02-POE**
- ИБП: **есть для серверов и сетевого оборудования**
- План размещения оборудования: [\[LINK\]](#)

Провайдеры

Канал	Провайдер	Скорость	Технология	IP	Точка ввода	Комментарий
WAN1	Соник-телеком	1000 Mbit/s	FTTB / PPPoE	55.66.77.88	Серверная	Основной
WAN2	Слоупок-телеком	20 Mbit/s	FTTB / Static IP	88.99.00.11	Серверная	Резервный

Схема резервирования: **failover**. Публичные IP: **есть**, для VPN и публикации сервисов.

Сеть

Детальная конфигурация (firewall rules, QoS, радиопараметры Wi-Fi, port mapping) — в экспорте конфигов: [\[LINK\]](#)

Подсети:

Подсеть	Назначение	VLAN	Комментарий
10.100.1.0/24	Основная сеть	1	Офис
10.111.1.0/24	Гостевая сеть	11	Офис
10.22.1.0/24	Видеонаблюдение	22	Офис
10.99.1.0/24	IT Management	99	Офис

Сегментация и L2:

- Гостевая сеть и видеонаблюдение изолированы от основной сети.
- Management-сегмент (VLAN 99) доступен только для IT.
- Inter-VLAN routing на маршрутизаторе Mikrotik VLRB-ML-GW-01.
- DHCP Snooping: доверенные — аплинк-порты коммутаторов.

Периметр и удалённый доступ:

- Входящие публикации: IPsec VPN (UDP 500/4500), OpenVPN (UDP 1194).
- Удалённый доступ пользователей и IT: только через VPN.

QoS: приоритеты (по убыванию) — админ-трафик, VPN, руководство, основная сеть, гостевая; гостевая — 2 Мбит/с на устройство.

Wi-Fi: решение Mikrotik CAPsMAN, 2 точки доступа.

SSID	Назначение	VLAN	Аутентификация	Пароль
Villariba-Work-Only	Рабочая	1	WPA2/WPA3	—
Villariba-Guest	Гостевая	11	PSK	ID_XXXXXXXXXXXXXXXXXX

Сетевое оборудование

Имя	Тип	Модель	Management IP	Локация	Роль	Комментарий
VLRB-ML-GW-01	Router	Mikrotik RB5009UG+S+IN	10.99.1.1	Серверная	Gateway	Основной маршрутизатор
VLRB-ML-SW-01	Switch	Mikrotik CRS326-24G-2S+RM	10.99.1.2	Серверная	Access / users / printers	Non-PoE
VLRB-ML-SW-02-POE	Switch	Mikrotik CRS328-24P-4S+RM	10.99.1.3	Серверная	PoE / AP / CCTV	PoE для камер и AP
VLRB-ML-AP-01	AP	Mikrotik cAP ax	10.99.1.91	Потолок, Open space	Wi-Fi	802.11ax 2.4/5 GHz
VLRB-ML-AP-02	AP	Mikrotik cAP ax	10.99.1.92	Потолок, Кабинетная зона	Wi-Fi	802.11ax 2.4/5 GHz

Доступы к оборудованию: искать в Bitwarden по имени устройства.

Рабочие места

- ПК: 21, ноутбуков: 4
- ОС: Windows 10 / Windows 11
- Домен: в AD
- Локальные админы: только IT
- Конфигурация: типовые офисные рабочие станции — Windows, Office, 1С, браузеры; основные рабочие места бухгалтерии, руководства и административного персонала

Инвентаризация рабочих мест — в GLPI: [\[LINK\]](#)

Печать

Имя узла	Модель	IP	Локация	Комментарий
KM45A123	Kyocera M2035dn	10.100.1.88	Бухгалтерия	Заводское имя
KM87B654	Kyocera M3145dn	10.100.1.87	Open space	Заводское имя
HPE9871235	HP LaserJet Pro M426fdn	10.100.1.86	Руководство	Заводское имя

Обслуживание (заправка, ремонт): Доктор Роботник, +78882588525, Эггман

Инвентаризация принтеров — в GLPI: [\[LINK\]](#)

Видеонаблюдение

- Решение: локальная IP-система, запись на NVR
- Камер: 4
- Архив: ~40 суток, локально на NVR
- Режим записи: постоянная
- Доступ к просмотру: руководство, ответственные сотрудники, IT по согласованию
- Обслуживание: ITMAK / SPQR-VIDEO
- Публикация извне: нет, только через VPN
- VLAN: 22 / CCTV, доступ из пользовательской сети ограничен
- Резервирование архива: нет
- Доступ к NVR: ID_XXXXXXXXXXXXXXXXXX

Имя	Тип	Модель	IP	Локация	Комментарий
VLRB-ML-NVR-01	NVR	Dahua DHI-NVR4108-4KS3	10.22.1.10	Серверная	HDD 4TB
VLRB-ML-CAM-01	Camera	Dahua DH-IPC-HDW1431T	10.22.1.31	Вход	PoE
VLRB-ML-CAM-02	Camera	Dahua DH-IPC-HDW1431T	10.22.1.32	Ресепшен	PoE
VLRB-ML-CAM-03	Camera	Dahua DH-IPC-HDW1431T	10.22.1.33	Open space	PoE
VLRB-ML-CAM-04	Camera	Dahua DH-IPC-HDW1431T	10.22.1.34	Коридор	PoE

Контакты на объекте

Не зафиксировано. Требуется заполнения: местный ИТ-специалист, инженер здания, ответственные на объекте.

Локальные особенности

- Центральная зависимость всей инфраструктуры от серверной офиса: при аварии затрагиваются оба объекта.
- Почта и основные бизнес-сервисы размещены локально — повышенные требования к резервированию.
- Резервный DNS реализован через маршрутизатор с переадресацией запросов локального домена на основной контроллер.

5.2 Пиццерия

Паспорт объекта

- Название: Пиццерия
- ID объекта: FLR01
- Адрес: [Strada Colle Sereno 7, 50125 Firenze, Italia](#) (Карта)
- Назначение: Филиал
- Контакт на объекте: Луиджи / +79997654321
- Режим работы: mixed
- Сотрудников: 13 / Рабочих мест: 5

Как добраться и логистика

- Как добраться: не зафиксировано, требует заполнения.
- Пропускной режим: не зафиксировано.
- Парковка: не зафиксировано.
- Место хранения ИТ-вещей: не зафиксировано.

Общая локальная логика

Филиал без локальных серверов и NAS. Подключение к центральным сервисам через VPN в офис. Локально работают рабочие станции, принтер, Wi-Fi и видеонаблюдение. Критичные бизнес-сервисы (1С, файлы, домен, почта) зависят от центрального офиса. Основной и резервный (4G) интернет-каналы.

Физическая структура

- Шкафы / стойки: настенный телеком-шкаф
- Кабельная система: СКС для рабочих мест, кассовой зоны, камер и Wi-Fi
- Интернет-ввод: ввод провайдера в зону телеком-шкафа
- PoE: используется для камер и AP через управляемый PoE-коммутатор
- ИБП: есть для сетевого оборудования
- План размещения оборудования: [\[LINK\]](#)

Провайдеры

Канал	Провайдер	Скорость	Технология	IP	Точка ввода	Комментарий
WAN1	Боузер-телеком	100 Mbit/s	FTTB / PPPoE	99.88.77.66	Телеком-шкаф	Основной
WAN2 (4G)	Yota	10-50 Mbit/s	4G / Ethernet DHCP	Динамический серый	Роутер	Резервный

Схема резервирования: failover. Публичные IP: есть (WAN1), для VPN.

Сеть

Детальная конфигурация — в экспорте конфигов: [\[LINK\]](#)

Подсети:

Подсеть	Назначение	VLAN	Комментарий
10.100.2.0/24	Основная сеть	1	Пиццерия
10.111.2.0/24	Гостевая сеть	11	Пиццерия
10.22.2.0/24	Видеонаблюдение	22	Пиццерия

Подсеть	Назначение	VLAN	Комментарий
10.99.2.0/24	IT Management	99	Пиццерия

Сегментация и L2:

- Гостевая сеть и видеонаблюдение изолированы от основной сети.
- Management-сегмент (VLAN 99) доступен только для IT.
- Inter-VLAN routing на маршрутизаторе объекта.
- Маршрутизация к централизованным сервисам — через VPN в офис.

Периметр и удалённый доступ:

- Входящие публикации: нет.
- Удалённый доступ пользователей и IT: только через VPN (завязан на офис).

QoS: приоритеты (по убыванию) — админ-трафик, VPN, 1С, основная сеть, гостевая; гостевая — 2 Мбит/с на устройство.

Wi-Fi: решение Mikrotik CAPsMAN (управление централизованное из офиса), 3 точки доступа.

SSID	Назначение	VLAN	Аутентификация	Пароль
Villariba-Work-Only	Рабочая	1	WPA2/WPA3	—
Villariba-Guest	Гостевая	11	PSK	ID_XXXXXXXXXXXXXXXXXX

Сетевое оборудование

Имя	Тип	Модель	Management IP	Локация	Роль	Комментарий
VLRB-FL-GW-01	Router	Mikrotik	10.99.2.1	Телеком-шкаф	Gateway	Маршрутизатор филиала
VLRB-FL-SW-01	Switch	Managed Switch	10.99.2.2	Телеком-шкаф	Access / users	
VLRB-FL-SW-02-POE	Switch	Managed PoE Switch	10.99.2.3	Телеком-шкаф	PoE / AP / CCTV	
VLRB-FL-AP-01	AP	Mikrotik cAP ax	10.99.2.91	Потолок, зал	Wi-Fi	
VLRB-FL-AP-02	AP	Mikrotik cAP ax	10.99.2.92	Потолок, техзона	Wi-Fi	
VLRB-FL-AP-03	AP	Mikrotik cAP ax	10.99.2.93	Потолок, вход/касса	Wi-Fi	

Доступы к оборудованию: искать в Bitwarden по имени устройства.

Рабочие места

- ПК: 4, ноутбуков: 1
- ОС: Windows 10 / Windows 11
- Домен: в AD
- Локальные админы: только IT
- Конфигурация: рабочие станции для учёта, печати, браузера, почты и доступа к 1С

Инвентаризация рабочих мест — в GLPI: [\[LINK\]](#)

Печать

Имя узла	Модель	IP	Локация	Комментарий
KM32C587	Kyocera M2135dn	10.100.2.80	Админ-зона	Заводское имя

Обслуживание (заправка, ремонт): **Доктор Роботник, +78882588525** (тот же подрядчик, что и для офиса)

Видеонаблюдение

- Решение: **локальная IP-система, запись на NVR**
- Камер: 10
- Архив: **~35 суток, локально на NVR**
- Режим записи: **постоянная**
- Доступ к просмотру: **руководство, IT по согласованию**
- Обслуживание: **ITMAK / SPQR-VIDEO**
- Публикация извне: **нет, только через VPN**
- VLAN: **22 / CCTV**
- Резервирование архива: **нет**
- Доступ к NVR: **ID_XXXXXXXXXXXXXXXXXX**

Имя	Тип	Модель	IP	Локация	Комментарий
VLRB-FL-NVR-01	NVR	Dahua DHI-NVR4216-4KS3	10.22.2.10	Телеком-шкаф	HDD 8TB
VLRB-FL-CAM-01	Camera	Dahua DH-IPC-HDW1431T	10.22.2.31	Главный вход	PoE
VLRB-FL-CAM-02	Camera	Dahua DH-IPC-HDW1431T	10.22.2.32	Зал 1	PoE
VLRB-FL-CAM-03	Camera	Dahua DH-IPC-HDW1431T	10.22.2.33	Зал 2	PoE
VLRB-FL-CAM-04	Camera	Dahua DH-IPC-HDW1431T	10.22.2.34	Кассовая зона	PoE
VLRB-FL-CAM-05	Camera	Dahua DH-IPC-HDW1431T	10.22.2.35	Бар / выдача	PoE
VLRB-FL-CAM-06	Camera	Dahua DH-IPC-HDW1431T	10.22.2.36	Кухня 1	PoE
VLRB-FL-CAM-07	Camera	Dahua DH-IPC-HDW1431T	10.22.2.37	Кухня 2	PoE
VLRB-FL-CAM-08	Camera	Dahua DH-IPC-HDW1431T	10.22.2.38	Мойка / техзона	PoE
VLRB-FL-CAM-09	Camera	Dahua DH-IPC-HDW1431T	10.22.2.39	Склад	PoE
VLRB-FL-CAM-10	Camera	Dahua DH-IPC-HDW1431T	10.22.2.40	Коридор	PoE

Контакты на объекте

Не зафиксировано. Требуется заполнения.

Локальные особенности

- Зависимость от связи с центральным офисом: при потере VPN остаётся только локальная сеть и CCTV.
- Отсутствие локальных серверов повышает зависимость от VPN.
- Резервный интернет через 4G (Yota) с динамическим серым IP.

6. Бэкапы и восстановление

6.1 Общая логика

- Резервное копирование: **централизовано с площадки Офис**
- Критичные данные: **VM, файловое хранилище VLRB-SRV-NAS, 1C / SQL на VLRB-SRV-1C, почта, конфиги сети**

- Филиал Пиццерия: локальных серверов нет, бэкапятся только конфиги сетевого оборудования и конфигурация CCTV.

6.2 Места хранения

Место хранения	Где размещено	Что хранится
Локально в офисе	На серверах в серверной	Временные backup, SQL backup 1С
VLRB-SRV-NAS	Виртуальное хранилище TrueNAS	Snapshots, файловые backup, служебные выгрузки
VLRB-SRV-BKP	Отдельный физ. сервер (PBS)	Image backup VM, backup 1С/SQL, почты, системных сервисов
S3-Compatible Offsite	Внешний S3-сервис	Критичные VM, backup 1С/SQL, почта, выборочные данные
ITMAK Central repo	Внешнее хранилище ITMAK	Конфиги Mikrotik, коммутаторов, Wi-Fi, CCTV

6.3 Что бэкапится

Сервис	Метод	Периодичность	Куда	Хранение
VM Proxmox	image backup	ежедневно	VLRB-SRV-BKP → S3 Offsite	30д / 8нед / 6мес
1С / SQL (VLRB-SRV-1С)	DB backup + file	каждые 4ч / ежедневно	Локально → VLRB-SRV-BKP → S3	7д / 30д / 6мес
NAS / файлы (VLRB-SRV-NAS)	snapshots + backup	snapshots 4ч, backup daily	VLRB-SRV-NAS + S3 Offsite	7д / 30д / 6мес
AD / DNS (DC01, DC02)	image backup	ежедневно	VLRB-SRV-BKP + S3	30д / 6мес
Почта (Mailcow)	image + app backup	ежедневно	VLRB-SRV-BKP + S3	30д / 6мес
Конфиги сети (Mikrotik, SW, Wi-Fi)	export config	ежемесячно + при изменениях	ITMAK Central repo	1 год
CCTV config	export config	ежемесячно + при изменениях	ITMAK Central repo	1 год

6.4 Проверка восстановления

- Критичные сервисы: ежеквартально
- Ответственные: ITMAK, по 1С — совместно с ответственным за сопровождение 1С

6.5 Порядок восстановления

1. Интернет / маршрутизатор / firewall
2. Гипервизоры Proxmox
3. AD / DNS
4. 1С / SQL
5. VLRB-SRV-NAS
6. Почта (Mailcow)
7. Вторичные сервисы
8. Проверка доступности со всех объектов (Офис и Пиццерия)

7. Мониторинг и эксплуатация

7.1 Мониторинг

- Платформа: ITMAK
- Что мониторится: серверы, гипервизоры, сетевое оборудование, VPN, почта, критичные сервисы
- Алерты: email / messenger
- Получатели: ITMAK / ответственные со стороны клиента

7.2 Стандарты сопровождения

- Кто обновляет документацию: ITMAK
- Когда: после изменений и по регламенту
- Источник правды: централизованное хранилище документации / Wiki / Git

7.3 Ссылки

- Экспорты конфигов: [LINK]
- Схемы (Draw.io): [LINK]
- Скрипты / автоматизация: [LINK]
- Конфигурация backup jobs: [LINK]
- GLPI: [LINK]
- Лицензии: [LINK]
- Лицензии 1С / ИТС: [LINK]

8. Информационная безопасность

8.1 Общая логика

- Принципы: сегментация сети, разграничение прав через AD, ограничение management-доступа, VPN, централизованное хранение паролей в Bitwarden
- Критичные активы: AD / DNS, VLRB-SRV-NAS, VLRB-SRV-1C, Mailcow, VLRB-SRV-BKP, сетевой периметр Mikrotik
- Основные угрозы: отказ центральной площадки, компрометация админ-доступов, потеря VPN-связности, сбой почты, повреждение backup
- Ответственные за ИБ: ITMAK + ответственные со стороны клиента

8.2 Реализовано

- Сегментация сети (VLAN): да
- Изоляция гостевой сети: да
- Ограничение management-доступа: да
- Разделение пользовательских и админских учёток: да
- Политика паролей AD: стандартная
- Антивирус: DrWeb Server на VLRB-SRV-DC02, агенты на всех ПК
- Централизованное управление защитой: есть
- Политика обновлений: все обновления включены, задержка 7 дней
- Firewall на периметре: Mikrotik
- VPN: GRE over IPsec + OpenVPN
- Offsite backup: да, S3-Compatible

8.3 Не реализовано

- MFA: нет
- IDS / IPS / geo-block: нет
- Шифрование дисков: нет
- Контроль USB / внешних носителей: нет

8.4 Реагирование на инциденты

- Порядок: ИТМАК → ответственный со стороны клиента → руководство
- Критичные инциденты: отказ офиса, AD / DNS, 1С / SQL, почты, VPN, backup-repository
- Фиксация: тикет-система

9. Контакты, контрагенты и доступы

9.1 Контакты клиента

Роль	Имя	Телефон	Email	Комментарий
Основной контакт	Марио	+79991234567	mario@world1-1.it	Главный сантехник
Резервный контакт	Луиджи	+79997654321	luigi@world8-4.it	Контакт по инфраструктуре

9.2 Подрядчики

Подрядчик	Роль	Контакт	Комментарий
ИТМАК	Инфраструктура / сопровождение	www.itmak.ru	Мониторинг, серверы, сеть
SPQR-VIDEO	Видеонаблюдение / СКС	+223322323232	Обслуживание камер и NVR
Доктор Роботник	Принтеры / картриджи	+78882588525, Эггман	
Подрядчик 1С / ИТС	Обновления / доработки 1С	не зафиксировано	Требует уточнения по договору

9.3 Контрагенты

Все договоры оформлены на ООО "Виллариба".

Контрагент	Услуга	№ договора	Техподдержка	Менеджер
reg.ru	Домен / хостинг	ЛК reg.ru	88005553478	—
Cloudflare	DNS	Панель Cloudflare, ID_XXXXXXXXXXXXXXXXXX	—	—
Соник-телеком	Интернет — Офис, WAN1 (основной)	№ 737	+7654831541, Наклз	+5443532155, Тэйлз
Слоупок-телеком	Интернет — Офис, WAN2 (резервный)	№ 00001	support@slow.com	+57524542251, Слооооооу
Боузер-телеком	Интернет — Пиццерия, WAN1 (основной)	№ 8-4	—	+84444444444, Принцесса

Контрагент	Услуга	№ договора	Техподдержка	Менеджер
Yota	Интернет — Пиццерия, WAN2 (резервный 4G)	№ 54574	—	—

Идентификация при звонке в техподдержку: назвать юрлицо (ООО "Виллариба") и номер договора.

9.4 Реквизиты юридических лиц клиента

Не зафиксировано. Требует заполнения при необходимости.

Полные реквизиты: [LINK на Nextcloud / DFS]

10. Риски, техдолг, временные решения

10.1 Известные риски

- Большинство критичных сервисов сосредоточено в серверной офиса: гипервизоры, 1C / SQL, почта, backup. При аварии серверной затрагиваются оба объекта.
- Работа филиала полностью зависит от VPN и доступности центральной площадки.
- Почтовый сервис размещён локально (Mailcow) — повышенные требования к резервированию и безопасности.
- Файловое хранилище VLRB-SRV-NAS — виртуальная машина, требует особого внимания к порядку восстановления.

10.2 Техдолг

- Требуется актуализировать ссылки на схемы, конфиги и эксплуатационные материалы.
- Требуется документировать правила тестового восстановления и результаты проверок бэкапов.
- Информация по 1C (ИТС, лицензирование, подрядчик, доработки) зафиксирована не полностью.
- Лицензирование (ОС, Office, антивирус) требует актуализации.
- Не заполнены разделы «Как добраться и логистика» для обоих объектов.
- Не заполнены VIP-сотрудники.
- Не заполнены контакты на объектах.
- Не заполнены реквизиты юрлица.

10.3 Временные костыли

- Резервный DNS реализован через маршрутизатор с переадресацией запросов локального домена на основной контроллер домена.

11. Журнал изменений

Дата	Что изменено	Кто	Комментарий
9999-12-31	Заполнены разделы 1–5	T-1000	Актуализация по инфраструктуре
9999-12-31	Добавлены разделы backup, ИБ, пересмотрены риски	T-1000	Консолидация документа

12. Приложения

12.1 Схемы

Глобальные: общая схема [\[LINK\]](#), межобъектная связность [\[LINK\]](#), сервисы [\[LINK\]](#)

По объектам:

Объект	Физическая схема / план	Логическая схема сети	Firewall / VPN	Wi-Fi	CCTV
Офис	[LINK]	[LINK]	[LINK]	[LINK]	[LINK]
Пиццерия	[LINK]	[LINK]	[LINK]	[LINK]	[LINK]

12.2 Экспорты конфигов

Устройство	Ссылка
VLRB-ML-GW-01	[LINK]
VLRB-ML-SW-01	[LINK]
VLRB-ML-SW-02-POE	[LINK]
VLRB-SRV-HV01	[LINK]
VLRB-SRV-HV02	[LINK]
VLRB-SRV-DC01	[LINK]
VLRB-SRV-DC02	[LINK]
VLRB-SRV-NAS	[LINK]
VLRB-SRV-BKP	[LINK]

12.3 Инструкции и регламенты клиента

Не зафиксировано. При наличии индивидуальных инструкций — добавить ссылки.

12.4 Дополнительные материалы

- GLPI (инвентаризация): [\[LINK\]](#)
- Инвентаризация рабочих станций: [\[LINK\]](#)
- Лицензии / подписки: [\[LINK\]](#)
- Лицензии 1С / ИТС: [\[LINK\]](#)
- Аудиты / отчёты: [\[LINK\]](#)