Yandex Cloud

Отвечаем на частые вопросы крупных компаний к облачному провайдеру

Кирилл Шевчук
Архитектор

Yandex Cloud подходит
для любых сценариев оптимизации
текущей инфраструктуры и создания
новых цифровых сервисов

Сайт в облаке

Интернет-магазин

Хранение и обработка персональных данных

1С в облаке

Сервисы Microsoft в облаке

Автоматизация колл-центров

Рекомендательная система для ритейла и e-commerce

Корпоративное хранилище данных

Бизнес-аналитика и визуализация данных

Serverless

Чат-боты на Serverless

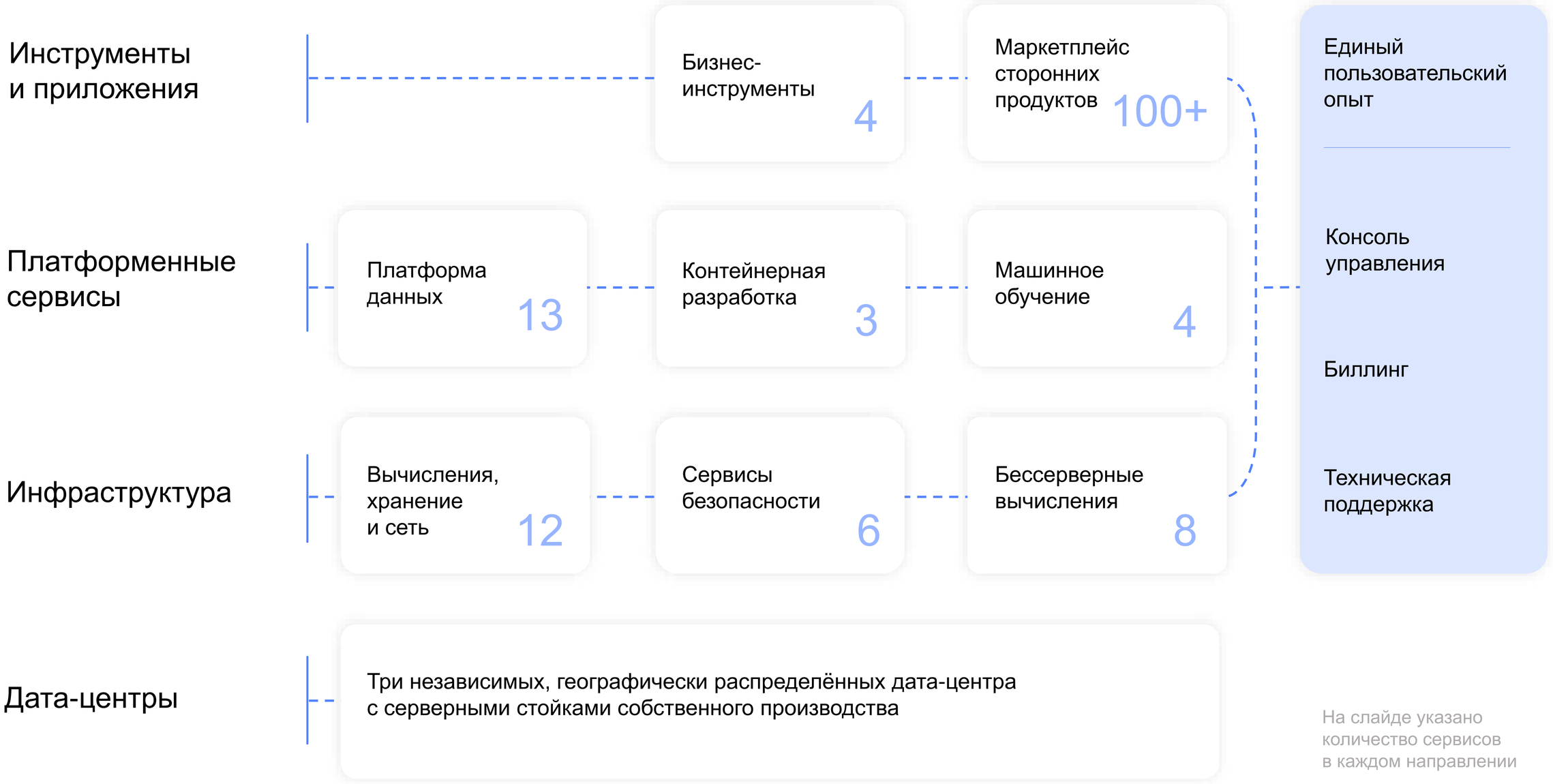
Distributed Cloud

Миграция в облако

Security Solution Library

Solution Library for AWS

Yandex Cloud – полноценный портфель облачных технологий



На слайде указано количество сервисов в каждом направлении

Содержание

1. Почему крупные компании выбирают облако?
2. Как облако выполняет требования регуляторов и служб ИБ?
3. Как объединить вашу сеть с облаком?
4. Как планировать расходы и FinOps?
5. Как нарастить экспертизу в облаке?

Lower Time
to Market

М.видео

Создание системы рекомендаций

Задача: выстроить пайплайн ML-вычислений рекомендательной системы для сайта, внутренних нужд магазина, логистики и коммерции

Решение: протестировали процессы на облачной инфраструктуре. Эксперимент с малым бюджетом оказался успешен и был масштабирован на всю разработку за 4 месяца

Результаты: запустили дата-офис, сократили время на запуск продуктов с 12 недель до 2 дней, построили рекомендательную систему, решили задачи ценообразования

в 30 раз

выросло количество пилотируемых проектов

>20к

ценников в день назначаются автоматически

Automate everything

зарплата.ру

Робот для обновления базы данных HR-портала

Задача: поддерживать в актуальном состоянии базу вакансий и резюме, обновляя до 10 000 позиций в сутки

Решение: голосовой робот, распознающий речь с помощью Yandex Speechkit, обрабатывающий информацию по технологии Dasha.AI, и отвечающий собеседнику по ML-модели на основе предзаписанных фраз диктора

Результаты: актуализация базы данных вакансий, сокращение издержек на содержание колл-центра, возможность составления аналитики и прогнозирования на основе кратких настраиваемых отчётов

96%

клиентов не узнают в собеседнике робота

3

месяца

на создание эффективной модели

SpeechKit

Scale everything

AXLEBOLT

Игровые серверы в облаке

Задача: развернуть мощные игровые серверы и обеспечить низкую задержку

Решение: перенесли мастер-сервер, к которому подключаются масштабируемые гейм-серверы, в облачный сервис Compute Cloud

Результаты: улучшили возможности оперативного развёртывания игровых серверов. Снизили стоимость трафика и latency для основной аудитории, которую составляют игроки из России

2–5 минут

скорость развёртывания серверов в облаке

25–50 мс

пинг на европейской части России

Compute Cloud

1. Почему крупные компании выбирают облако?
2. Как облако выполняет требования регуляторов и служб ИБ?
3. Как объединить вашу сеть с облаком?
4. Как планировать расходы и FinOps?
5. Как нарастить экспертизу в облаке?

Compliance

Соответствуем законодательным и индустриальным требованиям

ГОСТ Р 57580.1-2017

Безопасность финансовых операций

Реестр программного обеспечения

Запись в реестре
№ 9286 от 20.02.2021

Стандарты ISO

ISO 27001, ISO 27017 и ISO 27018

PCI DSS Compliant

Для ЦОД и облачных сервисов

152-ФЗ, УЗ-1

Аттестат соответствия по требованиям 21-го приказа ФСТЭК

Заботимся о безопасности на всех этапах создания и эксплуатации Yandex Cloud

Физическая безопасность

Техническое обслуживание серверов строго регламентируется

Объекты постоянно находятся под видеонаблюдением

При доступе к носителям данных, а также при хранении и уничтожении носителей применяются дополнительные меры безопасности

Безопасность разработки

Сотрудники, участвующие в разработке облачных сервисов, регулярно проходят обучение в области безопасности

Аудит безопасности кода приложений

Политика управления обновлениями, задающая максимальное время установки для каждого типа ПО

Защита данных

На всех облачных сервисах данные хранятся в зашифрованном виде

Данные, передаваемые через интернет, защищены протоколом TLS

При удалении данных используется способ очистки, гарантирующий невозможность их восстановления

Сервисы безопасности

В Yandex Cloud есть функции безопасности для решения любой проблемы

Защита инфраструктуры

Выделенные хосты Preview

Антивирусы Marketplace

Интеграция Audit Trails с SIEM

Управление доступом

Сервисные роли

Использование Active Directory через федерацию удостоверений

Управление политикой доступа (bucket policy) — ACL и сетевые политики

Организации

Автоматизация

Библиотека решений в области безопасности

Аварийное восстановление Marketplace

Защита приложений

WAF Marketplace

Сканер уязвимостей в Container Registry Preview

Сетевая безопасность

Группы безопасности Preview

Interconnect

NGFW Marketplace

NAT

GOST VPN

AntiDDoS L7

Сетевые политики Cillium в Kubernetes

Шифрование

Шифрование в Object Storage при помощи KMS-ключей

HSM-модуль для KMS-ключей Preview

HashiCorp Vault с поддержкой KMS-ключей Preview

Интеграция секретов Kubernetes с KMS и Lockbox Marketplace

Identity and Access Management

- Базовый сервис для разграничения прав доступа
- Простая RBAC-модель
- Предустановленный набор ролей
- Каждая роль — набор разрешений

console.cloud.yandex.com/iam

Можно ли использовать текущую систему аутентификации?

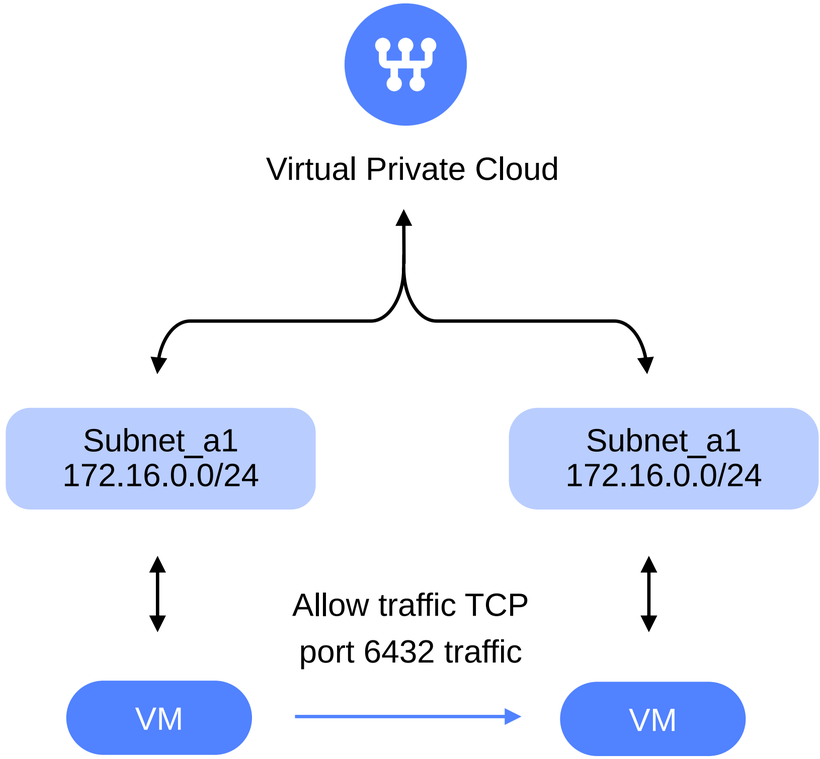
- Контроль аутентификации на стороне клиента
- Базовый сценарий — ADFS
- SAML может работать с чем угодно
- G Suite, Битрикс24 и т.д., все с поддержкой SAML

Как устроен контроль сетевого доступа

Группы безопасности позволяют ограничивать доступ VM к другим ресурсам и группам безопасности Yandex.Cloud или ресурсам в интернете

Группа безопасности назначается сетевому интерфейсу VM и должна содержать правила для получения и отправки трафика

Каждой VM можно назначить несколько групп безопасности



Группа безопасности по умолчанию позволяет ограничить всех пользователей облака в возможность выходить в публичную сеть

Как обеспечить аудит событий облака

Yandex Audit Trails — система сбора и выгрузки логов облака пользователя. За счет анализа собранной информации позволяет выявлять и устранять неполадки, обнаруживать нестандартную активность,
а также проводить аудит процессов и рисков

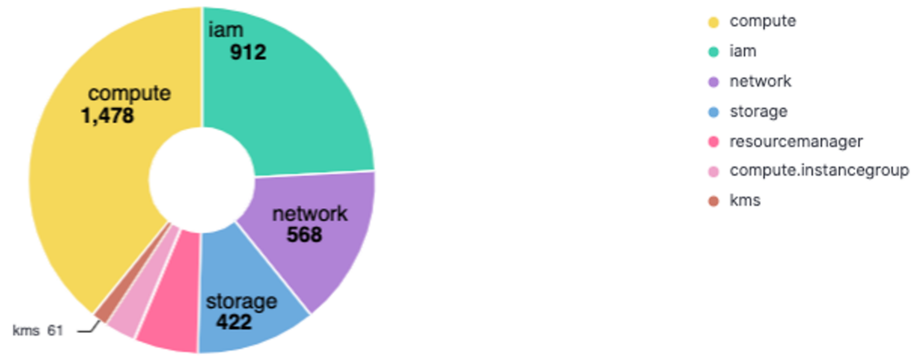
События аудита можно выгружать
в корпоративный SIEM на базе:

Splunk ArcSight Qradar Elastic

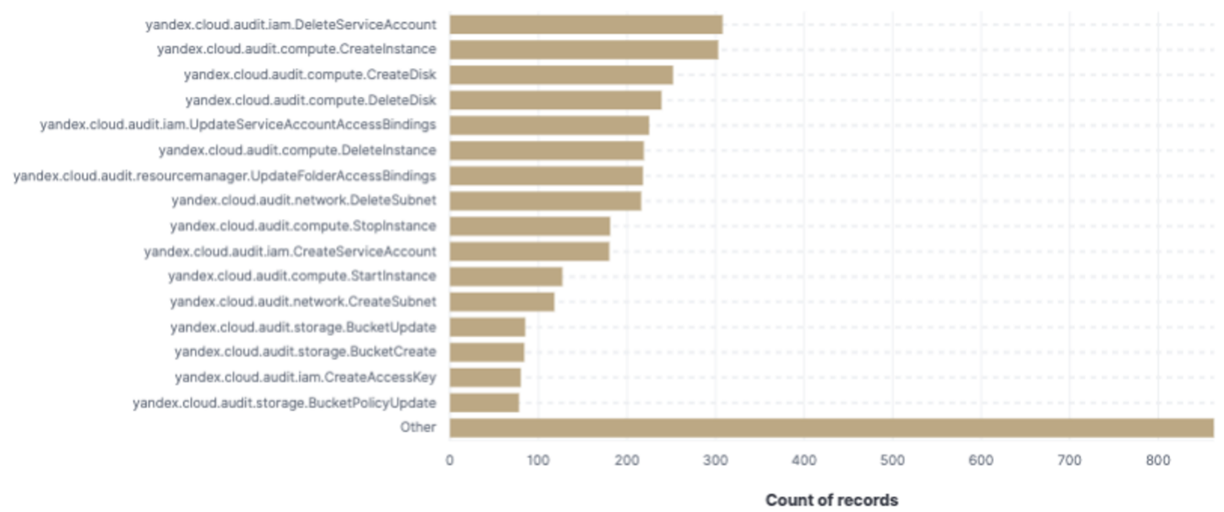
Search | KQL | Last 4 weeks | Show dates | Refresh

+ Add filter

Общее кол-во событий AuditTrails



Общее кол-во типов событий



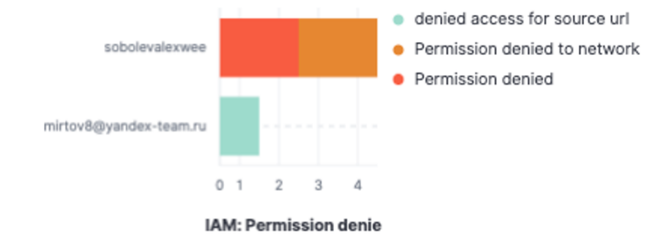
connections_api

2
Роль: vpc.publicAdmin

0
Роль: KMS

101
ServiceAccount Keys

121
Роль: Admin (folder/cloud)



Permission denied

8
Сеть: Public IP назначен на ВМ

55
Сеть: SG с 0.0.0.0/0

1
Сеть: Instance с 2 interface

93
Сеть: Security Group

0
Сеть: Public IP без antiDDOS

129
S3: ACL/Policy

5
Instance: создано Images

163
Instance: с Marketplace образом

40
Instance: Serialport enable

1,070
Роль: cloud.owner действия

116
Instance: Без SG

Подключения с YC/Terraform

Top values of user_agent.original.keyword	Top values of user....	Top values of source.ip	event_time per ...	Count of .
Terraform/0.15.3 (https://www.terraform.io) terr...	terraform-sa	2a00:1370:816d:2a3e:14...	2021-07-04 12:00	19
Terraform/0.15.3 (https://www.terraform.io) terr...	terraform-sa	2a00:1370:816d:2a3e:5d...	2021-07-06 12:00	3

Партнерские ИБ-решения

PT Application Firewall 3.7.3

Positive technologies

Kaspersky Security для виртуальных и облачных сред (PAYG)

Лаборатория Касперского

Kaspersky Security для виртуальных и облачных сред (BYOL)

Лаборатория Касперского

Валарм WAF (BYOL)

Wallarm

OpenVPN Access Server

Yandex.Cloud

Межсетевой экран Cisco ASAv

Cisco

IPSec-инстанс

Yandex.Cloud

Check Point CloudGuard IaaS — Firewall & Threat Prevention PAYG

Check Point

Check Point CloudGuard IaaS — Firewall & Threat Prevention with SandBlast PAYG

Check Point

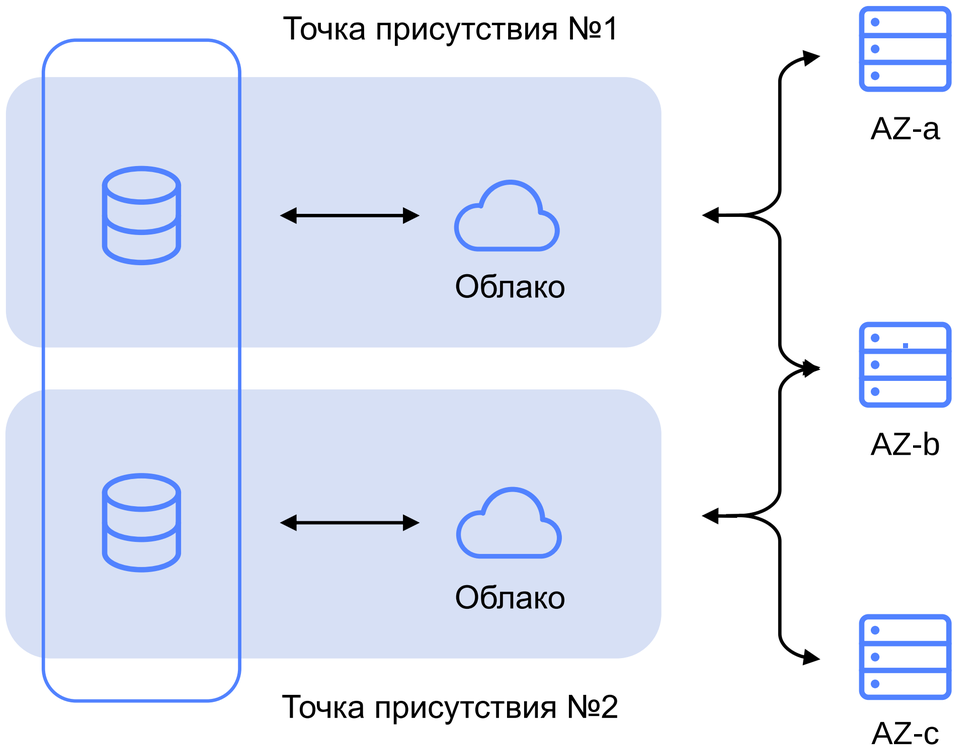
1. Почему крупные компании выбирают облако?
2. Как облако выполняет требования регуляторов и служб ИБ?
3. Как объединить вашу сеть с облаком?
4. Как планировать расходы и FinOps?
5. Как нарастить экспертизу в облаке?

Интеграция облака с корпоративной сетью

Cloud Interconnect

Предсказуемые задержки*

Стабильное соединение*

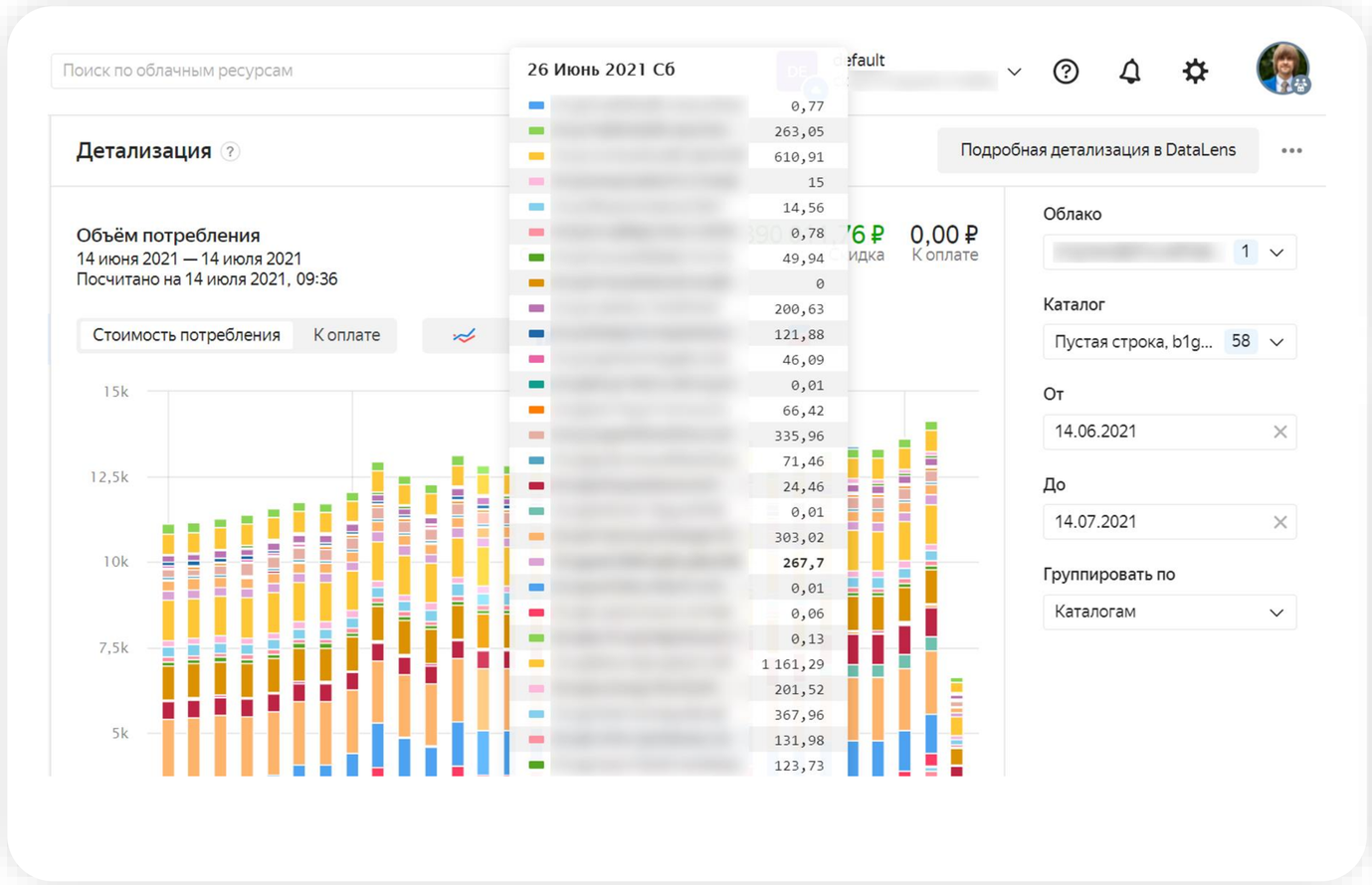


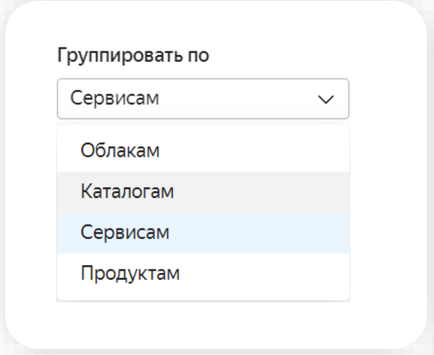
* По сравнению со связностью через интернет

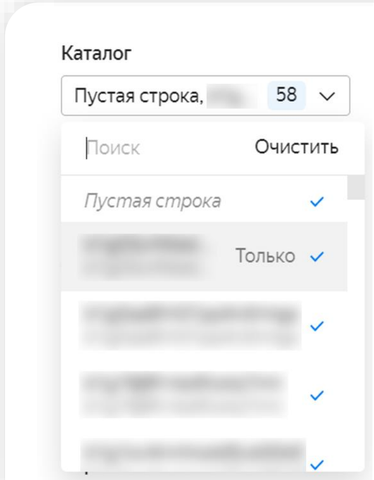
1. Почему крупные компании выбирают облако?
2. Как облако выполняет требования регуляторов и служб ИБ?
3. Как объединить вашу сеть с облаком?
4. Как планировать расходы и FinOps?
5. Как нарастить экспертизу в облаке?

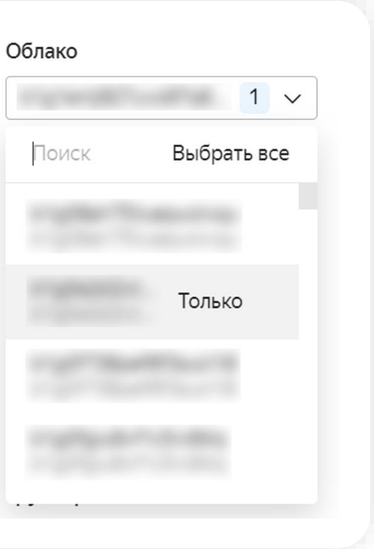
Реактивный контроль

Подробности
в записи вебинара



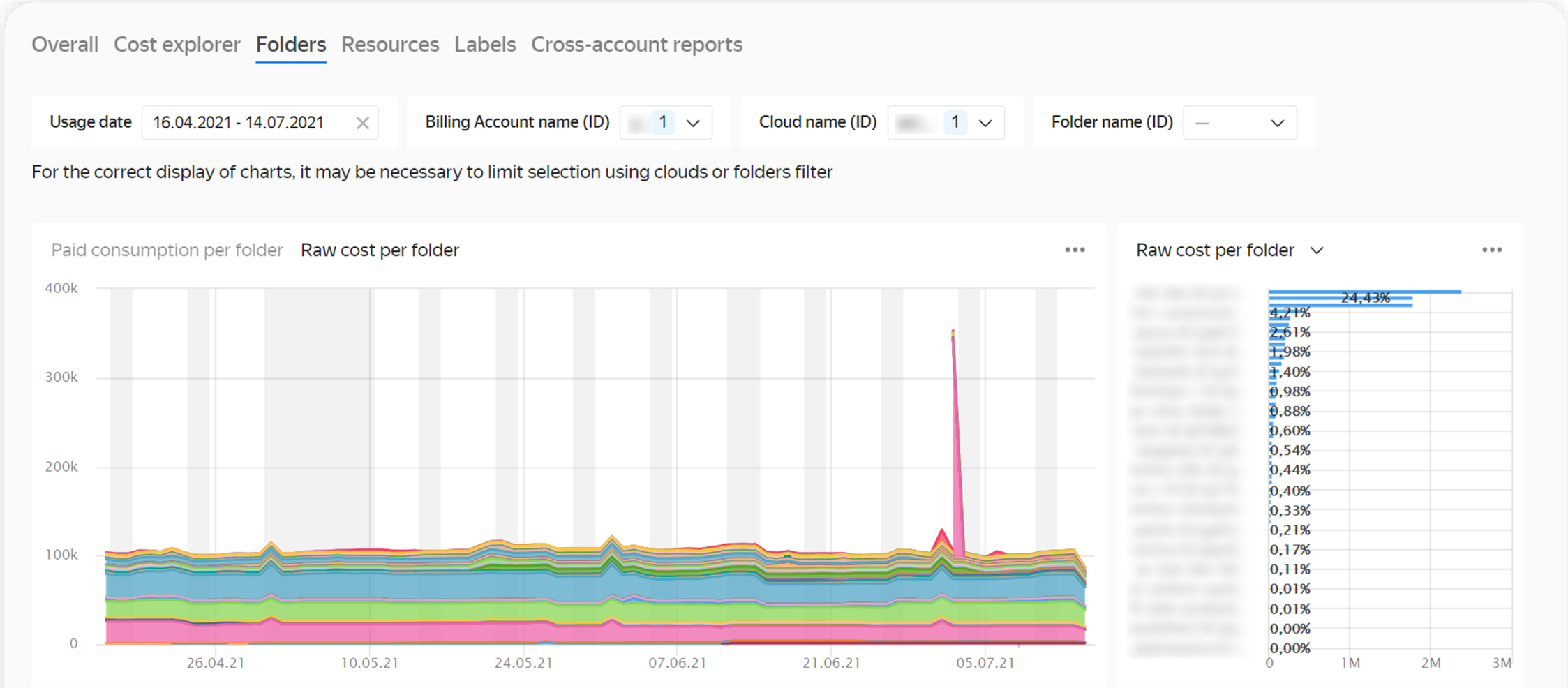






Детализация расходов в DataLens

Подробности
в записи вебинара



Проактивные уведомления

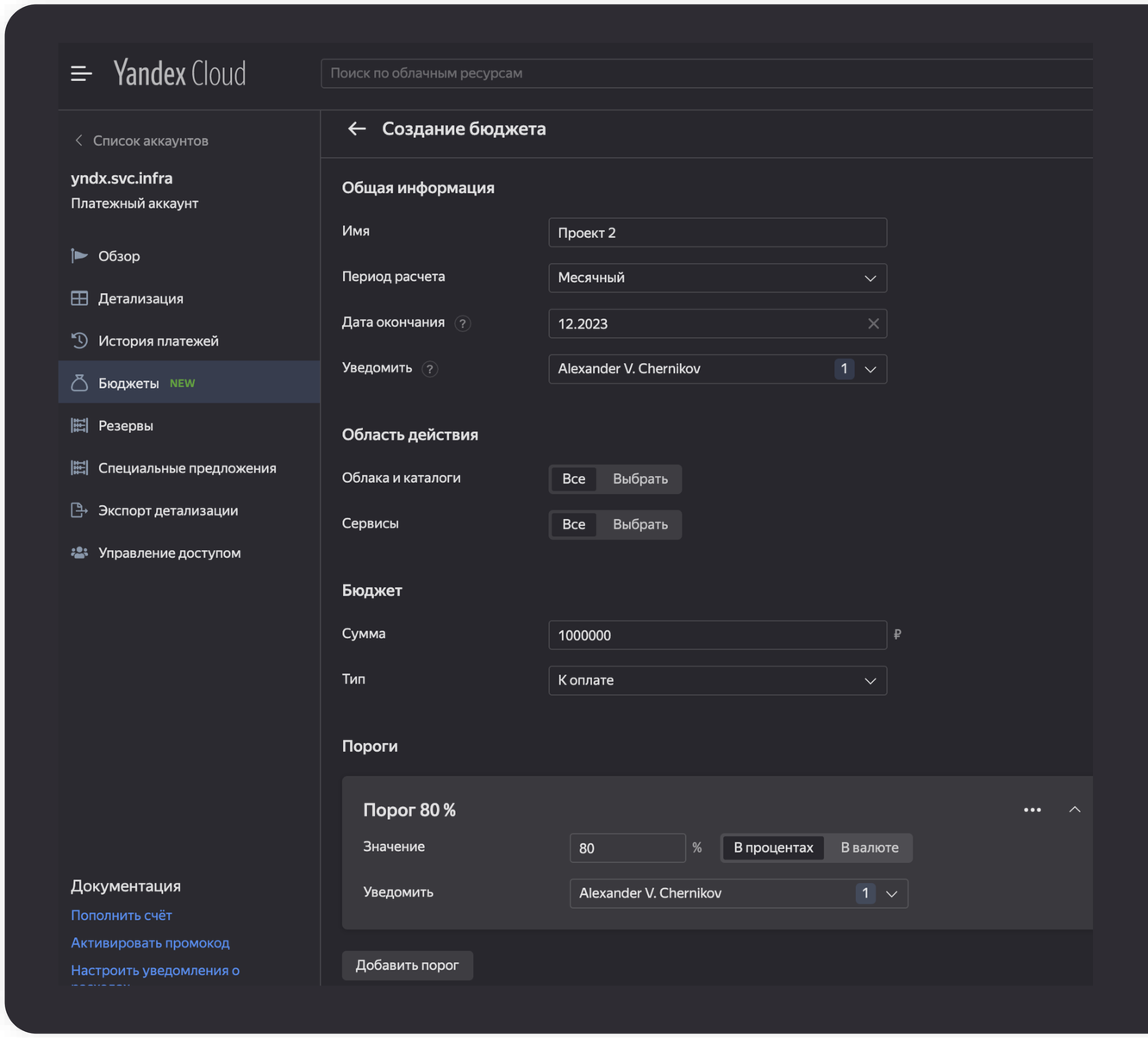
Мониторинг расходов

Гранулярная настройка объектов

Облака

Папки (проекты)

Отдельные сервисы



1. Почему крупные компании выбирают облако?
2. Как облако выполняет требования регуляторов и служб ИБ?
3. Как объединить вашу сеть с облаком?
4. Как планировать расходы и FinOps?
5. Как нарастить экспертизу в облаке?

Возможности для обучения сотрудников

Яндекс.Практикум

Профессия
«Инженер облачных сервисов»

Rebrain ₽

Практикум
«Администрирование Kubernetes® в Yandex.Cloud»

Самообучение

Документация

Записи вебинаров

Остались вопросы?
Обсудим!

Кирилл Шевчук
Архитектор
kirshe@yandex-team.ru
t.me/kirsh

cloud.yandex.ru