Отчет по аудиту ИТ-инфраструктуры Яндекс облака для клиента test

Cerberus Security tool

Attack node info:

platform	platform release
OpenNix CerberusOS	v1.01

1. Аутентификация и управление доступом

1.1 Настроена федерация удостоверений (Single Sign-On, SSO)

Yandex Cloud Organization — это единый сервис для управления составом организации, настройки интеграции с каталогом сотрудников и разграничения доступов пользователей к облачным ресурсам организации.

Для централизованного управления учетными данными используйте SAML-совместимые федерации удостоверений. С помощью федераций удостоверений компания может настроить Single Sign-On аутентификацию в Yandex Cloud через свой сервер IdP. При таком подходе сотрудники имеют возможность использовать свои корпоративные аккаунты, на которые распространяются политики безопасности компании, такие как:

- отзыв и блокирование аккаунтов;
- парольные политики;
- ограничение количества неуспешных попыток входа;
- блокирование сеанса доступа после установленного времени

бездействия;
- двухфакторная аутентификация.

Проверка завершилась с ошибкой для организации XXXXXXXXX

Инструкции и решения по выполнению:

- Инструкция по настройке SAML федерации удостоверений.
- Инструкция по настройке SAML федерации с KeyCloak.

1.2 Учетные записи Яндекс ID используются только в исключительных случаях

Наиболее правильный с точки зрения безопасности подход к управлению учетными записями — это использование федерации удостоверений (подробнее в рекомендации № 1.1). В связи с этим необходимо стремиться к тому, чтобы в списке пользователей вашей организации находились только федеративные пользователи (пользователи с атрибутом FEDERATION ID) и минимум учетных записей с Яндекс ID. Список допустимых исключений:

- Учетная запись с правами billing.accounts.owner (технически на текущий момент данную роль может иметь только учетная запись Яндекс ID).
- Учетная запись с правами organization-manager.organizations.owner и resource-manager.clouds.owner, если вы используете ее только для аварийного применения, например, когда сломалась настройка федерации. При необходимости можно удалить привилегированный паспортный аккаунт с ролью organization-manager.organizations.owner из организации.
- Внешние учетные записи, например, контрагентов или подрядчиков, которые по каким-либо причинам вы не можете завести в вашей IdP.

Пользователь	Примечание
cloudtrail	Не федеративный пользователь
packer	Не федеративный пользователь
k8s-cluster-67s	Не федеративный пользователь
wazuh-0-ample-owl	Не федеративный пользователь
k8s-node-group-hue	Не федеративный пользователь

Инструкции и решения по выполнению:

- Удалите из вашей организации все учетные записи с Яндекс ID, кроме случаев из списка допустимых исключений.

1.4 Используются сервисные роли вместо примитивных: admin, editor, viewer, auditor

Принцип минимальных привилегий требует назначать минимально необходимые для работы роли. Не рекомендуется использовать примитивные роли admin, editor, viewer и auditor, действующие во всех сервисах, так как это противоречит принципу минимальных привилегий. Для более избирательного управления доступом и реализации принципа минимальных привилегий используйте сервисные роли, которые содержат разрешения только для определенного типа ресурсов в указанном сервисе. Со списком всех сервисных ролей можно ознакомиться на странице Роли сервиса IAM.

Используйте роль auditor без возможности доступа к данным везде, где это возможно.

Проверка примитивов на уровне организации

Найдены учетные записи с назначенными примитивами

Пользователь	Примечание
organization-manager.organizations.owner	Найден пользователь с примитивными ролями на уровне организации
organization-manager.organizations.owner	Найден пользователь с примитивными ролями на уровне организации

Проверка примитивов на уровне каталога

Пользователь	Примечание
admin	Найден пользователь с примитивными ролями на уровне каталога

Инструкции и решения по выполнению:

Проанализируйте найденные учетные записи с назначенными примитивными ролями admin, editor и viewer и замените их на сервисные гранулярные роли в соответствии с вашей матрицей ролей.

1.5 Облачные сущности с сервисными аккаунтами учтены и ограничены

Сервисный аккаунт — аккаунт, от имени которого программы могут управлять ресурсами в Yandex Cloud. Сервисный аккаунт служит для выполнения запросов от имени приложения.

- Не используйте вместо сервисных аккаунтов аккаунты сотрудников. Например, если сотрудник уволится или сменит подразделение, его аккаунт потеряет права, что может привести к сбою приложения.
- Не записывайте ключи сервисных аккаунтов напрямую в код приложения, конфигурационные файлы или переменные окружения.

Сервисные аккаунты отсутствуют

1.6 В сервисе метаданных ВМ отсутствуют облачные ключи в открытом виде

Не записывайте ключи сервисных аккаунтов и другие ключи в метаданные виртуальной машины напрямую.
Используйте механизм назначения сервисного аккаунта виртуальной машине и получения токена через сервис метаданных.
Чувствительные данные могут находиться в любом поле метаданных, но самое распространенное — `user-data` (за счет использования в утилите cloud-init).

Ключи в открытом виде отсутствуют в метаданных

1.7 На ВМ отключено получение токена через AWS IMDSv1

В облаке есть сервис метаданных, предоставляющий сведения о работе виртуальных машин.

Изнутри виртуальной машины метаданные доступны в следующих форматах:

- Google Compute Engine (поддерживаются не все поля).
- Amazon EC2 (поддерживаются не все поля).

Формат Amazon EC2 Instance Metadata Service version 1 (IMDSv1) имеет ряд недостатков. Наиболее критичный из них — это риск компрометации токена сервисного аккаунта через сервис метаданных с помощью SSRF-атаки. Подробности в официальном блоге AWS. В связи с этим AWS выпустили вторую версию сервиса метаданных — IMDSv2.

В Yandex Cloud пока нет поддержки второй версии, поэтому строго рекомендуется технически отключать возможность получения токена сервисного аккаунта через Amazon EC2 сервис метаданных.

Сервис метаданных Google Compute Engine использует дополнительный заголовок для защиты от SSRF и повышения безопасности.

Отключить получение токена сервисного аккаунта через Amazon EC2 сервис метаданных можно с помощью параметра ВМ aws_v1_http_token:DISABLED.

aws_v1_http_token отсутствует в метаданных

1.8 Сервисным аккаунтам назначены минимальные привилегии

Следуйте принципу минимальных привилегий и назначайте сервисному аккаунту только те роли, которые необходимы для функционирования приложения.

Сервис аккаунты отсутствуют

1.9 Только доверенные администраторы имеют доступ к сервисным аккаунтам

Существует возможность назначать права на использование сервисного аккаунта от имени другого пользователя или сервисного аккаунта.

Следуйте принципу минимальных привилегий при выдаче доступа к сервисному аккаунту как к ресурсу: при наличии у пользователя прав на сервисный аккаунт, у него также появляется доступ и ко всем его правам. Назначайте роли на использование и управление сервисными аккаунтами минимальному кругу пользователей.

Каждый сервисный аккаунт с расширенными правами нужно размещать как ресурс в отдельном каталоге. Это необходимо для того, чтобы случайно не выдать пользователю права на такой сервисный аккаунт вместе с правами на каталог с компонентом сервиса.

Найдено	Примечание
XXXXXXXXX:{'compute.admin', 'admin', 'compute.images.user'}	Необходимо проверить
XXXXXXXXX:{'resource-manager.admin', 'admin', 'compute.images.user'}	Необходимо проверить

Инструкции и решения по выполнению:

- Удалите избыточные права сервисного аккаунта с помощью сервиса IAM.

1.10 Выполняется периодическая ротация ключей сервисных аккаунтов

В Yandex Cloud поддерживаются следующие ключи доступа, которые могут быть созданы для сервисных аккаунтов:

- IAM-токены — действуют 12 часов.
- API-ключи — не имеют срока действия.
- Авторизованные ключи — не имеют срока действия.
- Статические ключи доступа, совместимые с AWS API — не имеют срока действия.

Ключи без срока действия требуется ротировать самостоятельно — удалять и создавать новые. Дату создания можно проверить в свойствах ключа.
Рекомендуется ротировать ключи как минимум раз в 90 дней, в соответствии со стандартами информационной безопасности, например, PCI DSS.

Дата создания статических ключей

key_id	sa_id	created_at	description
XXXXXXXXX	XXXXXXXXX	2022-07-18T06:26:13Z	packer
XXXXXXXXX	XXXXXXXXX	2022-07-22T08:18:39Z	wazuh
XXXXXXXXX	XXXXXXXXX	2022-07-18T06:34:50Z	this temporary key is for upload image to storage; created by Packer
XXXXXXXXX	XXXXXXXXX	2022-08-01T05:59:56Z	terragrunt

Дата создания авторизованных ключей

key_id	sa_id	created_at	description
XXXXXXXXX	XXXXXXXXX	2021-09-24T08:31:50Z	None
XXXXXXXXX	XXXXXXXXX	2021-09-24T08:02:41Z	None
XXXXXXXXX	XXXXXXXXX	2022-08-02T15:01:28Z	None

Дата создания API-ключей

key_id	sa_id	created_at	description
XXXXXXXXX	XXXXXXXXX	2022-07-29T03:13:15Z	None
XXXXXXXXX	XXXXXXXXX	2022-07-18T06:28:23Z	packer
XXXXXXXXX	XXXXXXXXX	2022-07-29T03:29:19Z	None

Инструкции и решения по выполнению:

Для ротации ключей в зависимости от их типа воспользуйтесь инструкцией.

1.12 Привилегированные роли назначены только доверенным администраторам

К привилегированным пользователям Yandex Cloud относятся аккаунты со следующими ролями:

- `billing.accounts.owner`;
- `admin`, назначенная на платежный аккаунт;
- `organization-manager.organizations.owner`;
- `organization-manager.admin`;
- `resource-manager.clouds.owner`;
- `admin`, `editor`, назначенные на организацию;

- `admin`, `editor`, назначенные на облако;
- `admin`, `editor`, назначенные на каталог.

Роль `billing.accounts.owner` автоматически выдается при создании платежного аккаунта и не может быть переназначена другому пользователю. Роль позволяет выполнять любые действия с платежным аккаунтом.

Роль `billing.accounts.owner` может быть назначена только аккаунту Яндекс ID. Аккаунт с ролью `billing.accounts.owner` используется при настройке способов оплаты и подключении облаков.

Безопасности этого аккаунта следует уделять повышенное внимание, поскольку он обладает значительными полномочиями и не может быть объединен с корпоративным аккаунтом.

Наиболее правильным подходом можно считать отказ от регулярного использования данного аккаунта:

- Используйте его только при первоначальной настройке и внесении изменений.
- На время активного использования данного аккаунта включите двухфакторную аутентификацию (2FA) в Яндекс ID.
- Затем, если вы не используете способ оплаты банковской картой (доступный только для данной роли), назначьте данному аккаунту сложный пароль (сгенерированный с помощью специализированного ПО), отключите 2FA и не используйте этот аккаунт без необходимости.
- После каждого использования меняйте пароль на сгенерированный заново.

Отключить 2FA рекомендуется только для этого аккаунта и в случае, если аккаунт не "закреплен" за конкретным сотрудником. Эта мера нужна, чтобы избежать привязки критически важного аккаунта к личному устройству.

Для управления платежным аккаунтом назначьте роль `admin` или `editor` на платежный аккаунт выделенному сотруднику организации с федеративным аккаунтом.

Для просмотра платежных данных назначьте роль `viewer` на платежный аккаунт выделенному сотруднику организации с федеративным аккаунтом.

Роль `organization-manager.organizations.owner` по умолчанию получает владелец организации — пользователь, который ее создал. Роль дает возможность назначать владельцев организации, а также пользоваться всеми полномочиями администратора.

Роль `resource-manager.clouds.owner` автоматически выдается при создании первого облака в организации. Пользователь с этой ролью может выполнять любые операции с облаком и ресурсами в нем, а также выдавать доступ к облаку другим пользователям: назначать роли и отзывать их.

Назначайте роль `resource-manager.clouds.owner` и `organization-manager.organizations.owner` одному или нескольким сотрудникам организации с федеративным аккаунтом. Аккаунту Яндекс ID, с которым создано облако, назначьте сложный пароль и используйте только в случае крайней необходимости, например, при поломке федерации.

Федеративный аккаунт с одной из привилегированных ролей, указанных выше, необходимо всесторонне защитить:

- Включите двухфакторную аутентификацию.
- Запретите аутентификацию с устройств, не управляемых организацией.
- Настройте мониторинг попыток входа и задайте пороги предупреждений.

Назначайте роли `admin` на облака, каталоги и платежные аккаунты федеративным аккаунтам. Минимизируйте количество аккаунтов с этими ролями и регулярно перепроверяйте потребность в этих ролях для тех аккаунтов, которым они назначены.

Проверка примитивов на уровне организации

Найдены учетные записи с назначенными примитивами

Пользователь	Примечание
organization-manager.organizations.owner	Найден пользователь с примитивными ролями на уровне организации
organization-manager.organizations.owner	Найден пользователь с примитивными ролями на уровне организации

Проверка примитивов на уровне каталога

Пользователь	Примечание
admin	Найден пользователь с примитивными ролями на уровне каталога

1.16 На ресурсах в организации отсутствует публичный доступ

В Yandex Cloud существует возможность предоставлять публичный доступ на ресурсы. Публичный доступ предоставляется путем назначения прав доступа для системных групп (`allAuthenticatedUsers`, `allUsers`).

Описание системных групп:

- `allAuthenticatedUsers` — все пользователи, прошедшие аутентификацию. Это все зарегистрированные пользователи или сервисные аккаунты Yandex Cloud: как из ваших облаков, так и из облаков других пользователей.
- `allUsers` — любой пользователь, аутентификация не требуется.

> ⚠️ Сейчас `allUsers` поддерживается только в сервисах: Object Storage при управлении доступом с помощью ACL, Container Registry, Cloud Functions. В остальных сервисах назначение роли для группы `allUsers` эквивалентно назначению роли для `allAuthenticatedUsers`.

Убедитесь, что на ваши ресурсы — облака, каталоги, бакеты и т.д., не предоставлен публичный доступ для этих групп.

Учетные записи с назначенными примитивными ролями на уровне организации

id	type	roleId
XXXXXXXXX	serviceAccount	organization-manager.organizations.owner
XXXXXXXXX	userAccount	organization-manager.organizations.owner

Права доступа allUsers, allAuthenticatedUsers на уровне каталогов отсутствуют

Права доступа allUsers, allAuthenticatedUsers на уровне Container Registry отсутствуют

Права доступа allUsers, allAuthenticatedUsers на уровне Cloud Functions отсутствуют

Инструкции и решения по выполнению:

Если обнаружено наличие прав доступа у allUsers, allAuthenticatedUsers, необходимо удалить данные права.

1.23 Используется роль auditor для исключения доступа к данным пользователей

Для пользователей, которые не нуждаются в доступе к данным (таких как внешние подрядчики или аудиторы), необходимо назначить роль `auditor`.
Роль `auditor` это роль с минимальными привилегиями и без доступа к данным сервисов. Она дает разрешение на чтение конфигурации и метаданных сервисов.
Роль `auditor` позволяет выполнять следующие операции:

- Просмотр информации о ресурсе.
- Просмотр метаданных ресурса.
- Просмотр списка операций с ресурсом.

Использование роли `auditor` по умолчанию позволяет более избирательно управлять доступом и реализовывать принцип минимальных привилегий.

Учетные записи с ролью auditor на уровне организации отсутствует

Учетные записи с ролью auditor на уровне облака отсутствует

Учетные записи с ролью auditor на уровне каталогов отсутствует

Инструкции и решения по выполнению:

- Назначьте роль auditor пользователям, которые не нуждаются в доступе к данным.
- Удалите избыточные права аккаунта с помощью сервиса IAM.

2. Сетевая безопасность

В этом разделе представлены рекомендации пользователям по настройкам безопасности в Yandex Virtual Private Cloud.

Подробно о том, как настроить сетевую инфраструктуру, рассказывается в вебинаре Как работает сеть в Yandex Cloud.

Чтобы изолировать приложения друг от друга, поместите ресурсы в разные группы безопасности, а если требуется наиболее строгая изоляция — в разные сети.
Трафик внутри сети по умолчанию разрешен, а между сетями — нет.
Трафик между сетями можно передавать только через виртуальную машину с двумя сетевыми интерфейсами в разных сетях, VPN или сервис Yandex Cloud Interconnect.

2.1 Для объектов облака используется межсетевой экран или группы безопасности

Встроенный механизм групп безопасности позволяет управлять доступом ВМ к ресурсам и группами безопасности Yandex Cloud или ресурсам в интернете.
Группа безопасности — это набор правил для входящего и исходящего трафика, который можно назначить на сетевой интерфейс ВМ.
Группы безопасности работают как stateful firewall, то есть отслеживают состояние сессий: если правило разрешает создать

сессию, ответный трафик будет автоматически разрешен.
Инструкцию по настройке групп безопасности см. в разделе Создать группу безопасности. Указать группу безопасности можно в настройках ВМ.

Группы безопасности могут использоваться для защиты:

- ВМ.
- Управляемых баз данных.
- Балансировщиков нагрузки Yandex Application Load Balancer.
- Кластеров Yandex Managed Service for Kubernetes.

Список доступных сервисов расширяется.

Вы можете управлять сетевым доступом без групп безопасности, например, с помощью отдельной ВМ — межсетевой экран на основе образа NGFW из Yandex Cloud Marketplace, либо своего собственного образа.
Использование NGFW может быть критично для тех клиентов, которым необходима следующая функциональность:

- Составление логов сетевых соединений.
- Потоковый анализ трафика на предмет зловредного контента.
- Обнаружение сетевых атак по сигнатурам.
- Другая функциональность классических NGFW-решений.

Убедитесь, что в ваших облаках используются группы безопасности на каждом объекте облака, либо используется отдельная ВМ NGFW из Cloud Marketplace,, либо по принципу «bring your own image» («используй свое устройство» — принцип, позволяющий использовать свое оборудование или образы системы).

Объектов облака без группы безопасности не найдено

Проверка наличия NGFW вместо группы безопасности провалено

Инструкции и решения по выполнению:

- Примените группы безопасности на все объекты, на которых группа отсутствует.
- Для применения группы безопасности с помощью Terraform используйте настройку групп безопасности (dev/stage/prod) с помощью Terraform.
- Для использования NGFW установите на ВМ межсетевой экран (NGFW): Check Point.
- Инструкция по использованию UserGate NGFW в облаке.

- NGFW в режиме active-passive

2.2 Как минимум одна Группа безопасности существует в Virtual Private Cloud

Чтобы назначить группы безопасности на облачные объекты в Virtual Private Cloud, должна существовать как минимум одна группа безопасности.
Дополнительно существует возможность создания группы безопасности по умолчанию — такая группа назначается облачным объектам при подключении к подсетям, если у них нет ни одной группы. Убедитесь в том, что хотя бы одна группа безопасности существует в каждой сети.

Проверка наличия групп безопасности провалено

id	name	folder_id	created_at	description

Инструкции и решения по выполнению:

- Создайте группу безопасности в каждой Virtual Private Cloud с ограниченными правилами доступа, чтобы ее можно было назначать на облачные объекты.

2.3 В Группах безопасности отсутствует слишком широкое правило доступа

В группе безопасности существует возможность открыть сетевой доступ для абсолютно всех IP-адресов интернета и также по всем диапазонам портов. Опасное правило выглядит следующим образом:

- Диапазон портов: 0-65535 или пусто.
- Протокол: любой или TCP/UDP.
- Источник: CIDR.
- CIDR блоки: 0.0.0.0/0 (доступ со всех адресов) или ::/0 (ipv6).

> ⚠️ Если диапазон портов не указан, считается, что доступ предоставляется по всем портам (0-65535).

Открывать сетевой доступ необходимо только по тем портам, которые требуются для работы вашего приложения, и для тех адресов, с которых необходимо подключаться к вашим объектам.

Проверка наличия групп безопасности прошла успешно

2.4 Доступ по управляющим портам открыт только для доверенных IP-адресов

Рекомендуется открывать доступ к вашей облачной инфраструктуре по управляющим портам только с доверенных IP-адресов. Убедитесь, что в ваших правилах доступа в рамках группы безопасности отсутствуют широкие правила доступа по управляющим портам:

- Диапазон портов: 22, 3389 или 21.
- Протокол: TCP.
- Источник: CIDR.
- CIDR блоки: 0.0.0.0/0 (доступ со всех адресов) или ::/0 (ipv6).

Проверка наличия групп безопасности прошла успешно

2.5 Включена защита от DDoS атак

В Yandex Cloud существует базовая защита от DDoS и расширенная. Необходимо убедиться, что у вас используется как минимум базовая защита.

- Yandex DDoS Protection — это компонент сервиса Virtual Private Cloud для защиты облачных ресурсов от DDoS-атак. DDoS Protection предоставляется в партнерстве с Qrator Labs.
  Вы можете включать ее самостоятельно на внешний IP-адрес через инструменты управления облаком. Работает до L4 уровня модели OSI.
- Расширенная защита от DDoS-атак — работает на 3 и 7 уровнях модели OSI. Вы также можете отслеживать показатели нагрузки, параметры атак и подключить Solidwall WAF в личном кабинете Qrator Labs. Чтобы включить расширенную защиту, обратитесь к вашему менеджеру или в техническую поддержку.

Проверка наличия защиты от DDoS атак прошла успешно

2.7 Исходящий доступ в интернет контролируется

Возможные варианты организации исходящего доступа в интернет:

- Публичный IP-адрес. Адрес назначается ВМ по принципу one-to-one NAT.
- Egress NAT (NAT-шлюз). Включает доступ в интернет для подсети через общий пул публичных адресов Yandex Cloud. Не рекомендуется использовать Egress NAT для критичных взаимодействий, так как IP-адрес NAT-шлюза может использоваться несколькими клиентами одновременно. Следует учитывать эту особенность при моделировании угроз для инфраструктуры.
- NAT-инстанс. Функцию NAT выполняет отдельная ВМ. Для создания такой ВМ можно использовать образ NAT-инстанс из Cloud Marketplace или pfSense,OPNsense.

Сравнение способов доступа в интернет:

Публичный IP-адрес	**Egress NAT**	**NAT-инстанс**
Плюсы:	**Плюсы:**	**Плюсы:**
- Не требует настройки - Выделенный адрес для каждой ВМ	- Не требует настройки - Работает только на исходящих соединениях	- Возможность фильтровать трафик на NAT-инстансе - Возможность использовать собственный файрвол - Экономия IP-адресов
Минусы:	**Минусы:**	**Минусы:**
- Выставлять ВМ напрямую в интернет может быть небезопасно - Стоимость резервирования каждого адреса	- Общий пул IP-адресов - Функция на стадии Preview, поэтому не рекомендуется для продуктовых сред	- Требуется настройка - Стоимость использования ВМ (vCPU, RAM, диска)

Вне зависимости от выбранного варианта организации исходящего доступа в интернет, ограничивайте трафик с помощью одного из механизмов, описанных выше. Для построения защищенной системы необходимо использовать статические IP-адреса, так как их можно внести в список исключений файрвола принимающей стороны.

Исходящий доступ в интернет контролируется

Nat Gateway не найден

NAT-инстанс не найден

Инструкции и решения по выполнению:

- В случае наличия публичных адресов на ВМ убедитесь, что они

необходимы. В противном случае удалите внешний IP-адрес в настройках ВМ.

- В случае наличия NAT-Gateway убедитесь, что он необходим. В противном случае удалите его.
- В случае наличия NAT-инстанс убедитесь, что он необходим. В противном случае удалите его.