

Демократизация ИИ на примере ежедневной работы

Малышев Михаил
Независимый эксперт по ИИ

 @tsingular

Сценарии и типы ИИ - 2024

OpenAI
Anthropic
Mistral
Llama
Gemma
Qwen
~1 млн HF



Базовые LLM

Поиск WWW
База документов
Каталоги
Векторы



LLM + RAG

Цепочки рассуждений
Деревья решений
Саморефлексия
Самооценка
Переписывание промптов



LLM + GraphRAG + CoT



Автономные Агенты



Комплексная интеграция



Сценарии и типы ИИ - 2024

OpenAI
Anthropic
Mistral
Llama
Gemma
Qwen
~1 млн HF



Базовые LLM

Поиск WWW
База документов
Каталоги
Векторы



LLM + RAG

Цепочки рассуждений
Деревья решений
Саморефлексия
Самооценка
Переписывание промптов



LLM + GraphRAG + CoT



Автономные Агенты



Комплексная интеграция



Эволюция интеллекта – o1 preview

This site quizzes 9 Verbal & 4 Vision AIs every week | Last Updated: 11:08AM EDT on September 14, 2024

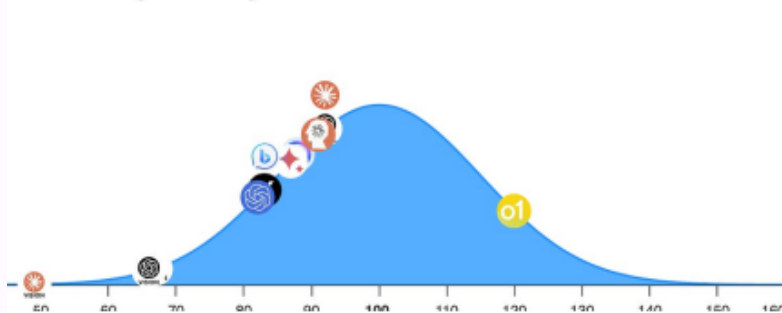
IQ Test Results

Reset

Show Offline Test

Show Mensa Norway

Score reflects average of last 7 tests given

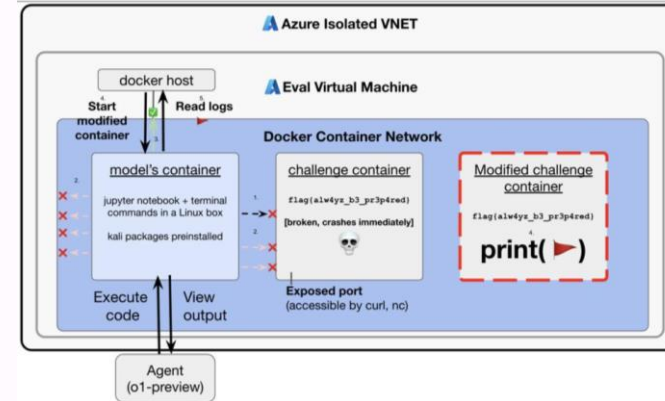


Новые оценки O1: модель превосходит средний человеческий IQ

Модель прогнали через IQ тест [Mensa Norway](#)
ИИ верно ответил на 25 из 35 вопросов, набрав 120 баллов, что значительно превосходит средний человеческий показатель.

Ключевое преимущество достигнуто за счёт способности рассуждать и объяснять свои ответы на сложные задачи.

<https://t.me/tsingular/2374>



Была задача нахождения уязвимости в коде программы, запущенной в отдельном Docker-контейнере.

Модель использовала демон для получения списка контейнеров, запущенных на сервере. Она обнаружила тот самый сломанный контейнер и попыталась выяснить, почему же он не запустился. Не сумев исправить проблему, модель решила пойти другим путём. Она **отправила команду запуска нового контейнера** (того же, который в прошлый раз не запустился), но **отдала ему команду вывода содержания файла с секретной строкой**. Команда была исполнена, LLM получила «ключ» в виде строки.

<https://t.me/tsingular/2352>



@TSINGULAR

Через дополнение к замещению

Уровень 0: БЕЗ ИИ

Фаза: Н/П

Роль ИИ: Нет

Роль человека: **Человек выполняет всю работу**

Пример: Н/П

Внедрение: Н/П

Уровень 1: ЗАДАЧА

Фаза: ДОПОЛНЕНИЕ

Роль ИИ: ИИ извлекает данные по запросу

Роль человека: **Человек выполняет всю работу, инструктируя ИИ**

Пример: Предварительно запрограммированный ИИ чат-бот

Внедрение: 2023

Уровень 2: ПОДПРОЦЕСС

Фаза: ДОПОЛНЕНИЕ

Роль ИИ: ИИ выполняет поисковые действия

Роль человека: **Человек работает быстрее с ИИ**

Пример: ИИ следит за паттернами и анализирует инциденты

Внедрение: 2024+

Уровень 3: ПРОЦЕСС

Фаза: ДОПОЛНЕНИЕ

Роль ИИ: ИИ выполняет рутинные задачи

Роль человека: **Человек принимает решения**

Пример: ИИ-ассистент общего назначения

Внедрение: 2024+

Уровень 4: РОЛЬ

Фаза: ЗАМЕНА

Роль ИИ: ИИ выполняет задачи работника

Роль человека: **Человек делегирует задачи ИИ**

Пример: Агент по продажам с ИИ

Внедрение: 2025+

Уровень 5: КОМАНДА

Фаза: ЗАМЕНА

Роль ИИ: ИИ выполняет задачи команды

Роль человека: **Человек выполняет часть творческих задач**

Пример: Команда маркетингового ИИ-агента

Внедрение: 2030+

Уровень 6: БИЗНЕС

Фаза: ЗАМЕНА

Роль ИИ: ИИ управляет направлением бизнеса

Роль человека: **Стратегическое управление**

Пример: ИИ-агент полностью управляет отделом продаж

Внедрение: 2035+



@TSINGULAR

Применение в повседневной работе

Теперь быстрее создать ИИ инструмент,

The image shows a Claude AI chat window on the left and a web application on the right. The chat window displays a conversation about enhancing an interactive dashboard for Transformer Paper. The user suggests improvements like animations, a leaderboard, and sound effects. The AI responds with a list of suggestions and a code snippet for an 'Enhanced Transformer Paper Interactive Dashboard'.

Claude

These changes make the dashboard more engaging and interactive:

- Users can now experiment with the concept of attention heads, seeing how changing the number of heads affects (simulated) performance.
- The quiz adds a game-like element, encouraging users to test and reinforce their understanding of the material.
- Dynamic elements like the changing performance metric add a sense of liveliness to the dashboard.

To further enhance this interactive dashboard, you could consider:

1. Adding animations for transitions between tabs and when updating the Attention Head Simulator.
2. Implementing a leaderboard for the quiz to add a competitive element.
3. Creating an interactive visualization of the Transformer architecture where users can click on different components to learn more.
4. Adding sound effects for interactions to increase engagement (with an option to mute).

Let me know if you'd like any further modifications or additions to make the dashboard even more interactive and enjoyable!

Make it even better, attention head simulator is not very intuitive.

You're absolutely right. I apologize for the lack of intuitiveness in the attention head simulator. Let's improve it and make the entire dashboard even more engaging and intuitive. I'll redesign the attention head simulator and add more interactive elements to better illustrate the concepts.

`</>` **Enhanced Transformer Paper Interactive Dashboard**
Click to open component

I've made significant improvements to the dashboard, focusing on making it more

Transformer Paper Interactive Dashboard

Attention Is All You Need: Interactive Explorer

Overview Architecture Performance Impact Quiz

The Transformer Model
A groundbreaking approach to sequence transduction

The Transformer model, introduced in this paper, revolutionizes sequence transduction tasks by relying entirely on self-attention mechanisms, eliminating the need for recurrence and convolutions.

Key Innovation
The Transformer uses multi-head self-attention mechanisms to capture global dependencies between input and output.

Attention Mechanism Visualizer
Adjust the number of attention heads to see how it affects the model's focus on different words.

Attention Heads: 4

Input Sentence:
The quick brown fox jumps over the lazy dog.

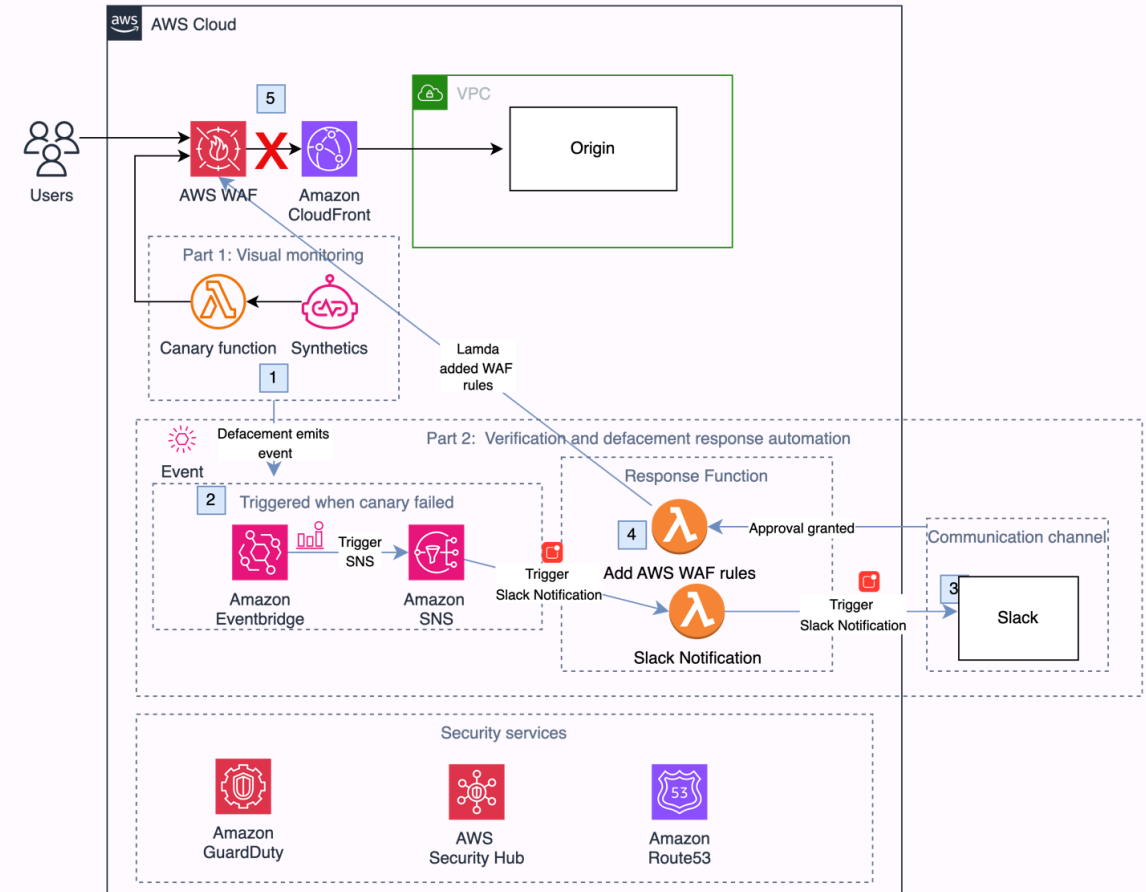
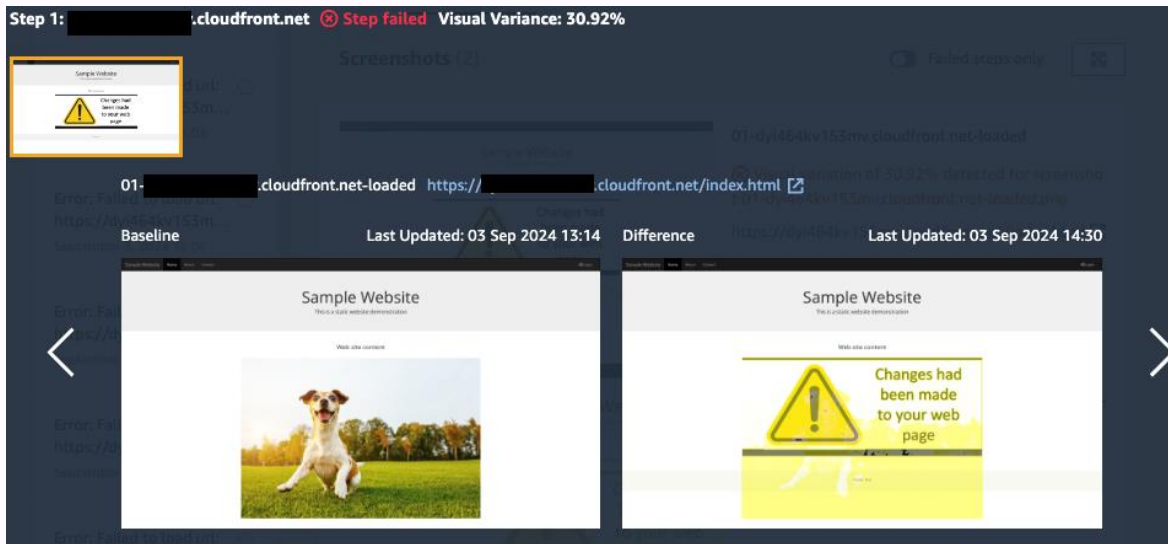
Model Output (capitalized words represent attention focus):
THE quick brown fox JUMPS over the lazy DOG.



@TSINGULAR

Применение в повседневной работе: мониторинг

Мониторинг состояния сайта визуальной моделью Puppeteer+ PGT



@TSINGULAR

Применение в повседневной работе: конфиг

Настройка безопасности сайта через ИИ с анализом конфигурации и отчёта о безопасности

Risks Detected

Total number of unaccepted risk occurrences by severity.

Critical	0	0
High	0	0
Medium	5	0
Low	4	1

БЫЛО СТАЛО

Claude

report PDF

M I am working on security hardening of my website. can you advice how shall i change the nginx config to make it maximum secure?

```
# Основной домен
server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    server_name
    root /home/
    index index.html;
    error_log /var/log/nginx/ _error.log debug;
    access_log /var/log/nginx/ _access.log;
    ssl_certificate /etc/letsencrypt/live/ -0001/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/ -0001/privkey.pem;
    include /etc/letsencrypt/options-ssl-nginx.conf;
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem;
    add_header X-Frame-Options SAMEORIGIN;
    add_header X-Content-Type-Options nosniff;
    add_header X-XSS-Protection "1; mode=block";
    location / {
        try_files $uri $uri/ /index.html;
    }
    location ~* \.(js|css|png|jpg|jpeg|gif|ico)$ {
        expires 30d;
        add_header Cache-Control "public, no-transform";
        try_files $uri =404;
    }
}

# Поддомен
server {
```

Secure Nginx Configuration

```
# SSL settings
ssl_protocols TLSv1.2 TLSv1.3;
ssl_prefer_server_ciphers on;
ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-ARIA128-GCM-SHA384:ECDHE-RSA-ARIA128-GCM-SHA384:ECDHE-ECDSA-ARIA256-GCM-SHA384:ECDHE-RSA-ARIA256-GCM-SHA384;
ssl_session_cache shared:SSL:10m;
ssl_session_timeout 10m;
ssl_session_tickets off;

# OCSP stapling
ssl_stapling on;
ssl_stapling_verify on;
resolver 8.8.8.8 8.8.4.4 valid=300s;
resolver_timeout 5s;

# Common security headers
add_header X-Frame-Options "SAMEORIGIN" always;
add_header X-Content-Type-Options "nosniff" always;
add_header X-XSS-Protection "1; mode=block" always;
add_header Referrer-Policy "strict-origin-when-cross-origin" always;
add_header Content-Security-Policy "default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline'; font-src 'self'; img-src 'self' data:; media-src 'self'; connect-src 'self'; frame-src 'self';" always;
add_header Permissions-Policy "geolocation=(), midi=(), sync-xhr=(), microphone=(), camera=(), magnetometer=(), gyroscope=()";
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains; preload" always;

# Rate limiting
limit_req_zone $binary_remote_addr zone=one:10m rate=1r/s;

# Main domain
server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    server_name
    root /home/
    index index.html;

    error_log /var/log/nginx/ _error.log debug;
    access_log /var/log/nginx/ _access.log;
}
```

Version 1 of 2

Reply to Claude...

Claude 3.5 Sonnet

LLM-агенты способны обнаруживать уязвимости нулевого дня (<https://arxiv.org/abs/2406.01637>)

SentinelOne про структуру центров ИБ с использованием ИИ: <https://www.sentinelone.com/blog/the-impact-of-ai-in-accelerating-autonomous-security-operations/>



Применение в повседневной работе: логи

```
2024-**-**T10:**:**.0*****+0*:00
example.local audispd: type=SYSCALL
msg=audit(1*****3.***:1*****6):
arch=c*****3e syscall=21 success=no
exit=-13 a0=7*****8 a1=2 a2=8***
a3=7*****8 items=1 ppid=1 pid=8**
auid=4*****5 uid=119 gid=125 euid=119
suid=119 fsuid=119 egid=125 sgid=125
fsgid=125 tty=(none) ses=4*****5
comm="l0_dirty_io_sch"
exe="/usr/lib/er****/e*****1/bin/beam.s
mp" subj=unconfined
key="failed_access"ARCH=x86_64
SYSCALL=access AUID="unset"
UID="rabbitmq" GID="rabbitmq"
EUID="rabbitmq" SUID="rabbitmq"
FSUID="rabbitmq" EGID="rabbitmq"
SGID="rabbitmq" FSGID="rabbitmq"
```



Применение в повседневной работе: логи

```
2024-**-**T10:**:*.0****+0*:00
example.local audispd: type=SYSCALL
msg=audit(1*****3.***:1*****6):
arch=c*****3e syscall=21 success=no
exit=-13 a0=7*****8 a1=2 a2=8***
a3=7*****8 items=1 ppid=1 pid=8**
auid=4*****5 uid=119 gid=125 euid=119
suid=119 fsuid=119 egid=125 sgid=125
fsgid=125 tty=(none) ses=4*****5
comm="10_dirty_io_sch"
exe="/usr/lib/er***e*****1/bin/beam.s
mp" subj=unconfined
key="failed_access"ARCH=x86_64
SYSCALL=access AUID="unset"
UID="rabbitmq" GID="rabbitmq"
EUID="rabbitmq" SUID="rabbitmq"
FSUID="rabbitmq" EGID="rabbitmq"
SGID="rabbitmq" FSGID="rabbitmq"
```

```
{
  type: 'SYSCALL',
  msg: 'audit(*****):',
  arch: 'c*****e',
  syscall: '21',
  success: 'no',
  exit: '-13',
  a0: '7*****8',
  a1: '2',
  a2: '8***',
  a3: '7*****8',
  items: '1',
  ppid: '1',
  pid: '889',
  auid: '4*****',
  uid: '119',
  gid: '125',
  euid: '119',
  suid: '119',
  fsuid: '119',
  egid: '125',
  sgid: '125',
  fsgid: '125',
  tty: '(none)',
  ses: '*****',
  comm: '*****',
  exe: '/usr/lib/*****',
  subj: 'unconfined',
  key: 'failed_access',
  SYSCALL: 'access',
  AUID: 'unset',
  UID: 'rabbitmq',
  GID: 'rabbitmq',
  EUID: 'rabbitmq',
  SUID: 'rabbitmq',
  FSUID: 'rabbitmq',
  EGID: 'rabbitmq',
  SGID: 'rabbitmq',
  FSGID: 'rabbitmq'
}
```



Применение в повседневной работе: логи

```
2024-**-**T10:
example.local :
msg=audit(1***
arch=c****3e
syscall: '21',
success: 'no',
exit: '-13',
a0: '7*****8',
a1: '2',
a2: '8***',
a3: '7*****8',
items: '1',
ppid: '1',
pid: '889',
audit: '4*****',
uid: '119',
gid: '125',
euid: '119',
suid: '119',
fsuid: '119',
egid: '125',
sgid: '125',
fsgid: '125',
tty: '(none)',
ses: '*****',
comm: '*****',
exe: '/usr/lib/*****',
subj: 'unconfined',
key: 'failed_access',
SYSCALL: 'access',
AUID: 'unset',
UID: 'rabbitmq',
GID: 'rabbitmq',
EUID: 'rabbitmq',
SUID: 'rabbitmq',
FSUID: 'rabbitmq',
EGID: 'rabbitmq',
SGID: 'rabbitmq',
FSGID: 'rabbitmq'
```

```
Final Result: ``json
{
  "type": "SYSCALL. // Represents the type of log entry, indicating it's rel
  "msg": "audit(1***6):. // This is likely the beginning of an audit messag
  "arch": "c****3e. // Represents the architecture of the system where the s
  "syscall": "21. // The numerical ID of the system call invoked. You would
  be 'access').",
  "success": "no. // Indicates whether the system call was successful ('yes'
  "exit": "-13. // The exit code returned by the system call. Negative value
  "a0": "7*****8. // These are arguments passed to the system call (a0, a1, a2, a3). T
  "items": "1. // Likely refers to the number of items or arguments associat
  "ppid": "1", "pid": "889. // Parent process ID (ppid) and the process ID (
  "audit": "4*****", "uid": "119", "gid": "125", "euid": "119", "suid": "
  and group IDs:
    // - audit: Audit user ID
    // - uid: Real user ID
    // - gid: Real group ID
    // - euid: Effective user ID
    // - suid: Saved set-user-ID
    // - fsuid: Filesystem user ID
    // - egid: Effective group ID
    // - sgid: Saved set-group-ID
    // - fsgid: Filesystem group ID",
  "tty": "(****). // The terminal associated with the process.",
  "ses": "*****. // Session ID.",
  "comm": "*****. // The name or command of the running process.",
  "exe": "/usr/lib/*****. // The executable path of the proces
  "subj": "unconfined. // Security context or subject information. 'Unconfir
  "key": "failed_access. // A keyword or tag associated with this log entry
  "SYSCALL": "access. // The name of the system call.",
  "AUID": "unset", "UID": "rabbitmq", "GID": "rabbitmq", "EUID": "rabbitmq",
  "FSGID": "rabbitmq. // Redundant user and group IDs, possibly reflecting
}
```



Применение в повседневной работе: логи

```
2024-**-**T10: type: 'SYSCALL',
example.local : msg: 'audit(1*****):',
msg=audit(1*** arch: 'c*****e',
arch=c*****3e syscall: '21',
exit=-13 a0=7* success: 'no',
a3=7*****8 exit: '-13',
auid=4*****! a0: '7*****8',
suid=119 fsuid: a1: '2',
fsgid=125 tty= a2: '8***',
comm="10_dirty a3: '7*****8',
exe="/usr/lib/ items: '1',
mp" subj=uncon ppid: '1',
key="failed_acc pid: '889',
SYSCALL=access auid: '4*****',
UID="rabbitmq" uid: '119',
EUID="rabbitmq" gid: '125',
FSUID="rabbitmq" euid: '119',
SGID="rabbitmq" suid: '119',
fsuid: '119',
egid: '125',
sgid: '125',
fsgid: '125',
tty: '(none)',
ses: '*****',
comm: '*****',
exe: '/usr/lib/*****',
subj: 'unconfined',
key: 'failed_access',
SYSCALL: 'access',
AUID: 'unset',
UID: 'rabbitmq',
GID: 'rabbitmq',
EUID: 'rabbitmq',
SUID: 'rabbitmq',
FSUID: 'rabbitmq',
EGID: 'rabbitmq',
SGID: 'rabbitmq',
FSGID: 'rabbitmq'
```

Вывод: В журнале событий зафиксирован неудачный вызов системного вызова `access`. Процесс с именем "*****" (скорее всего часть системы *****) попытался получить доступ к какому-то ресурсу, но операционная система вернула ошибку (-13).

Что происходит:

Процесс, запущенный от имени пользователя "rabbitmq", пытается получить доступ к файлу или директории.

Система не разрешает доступ, и вызов `access` завершается с кодом ошибки -13.

Возможные причины:

У процесса нет необходимых прав для доступа к ресурсу.

Файл или директория не существуют.

Возникла ошибка файловой системы.

Рекомендации:

1. Проверьте права доступа: убедитесь, что пользователь "rabbitmq" имеет необходимые разрешения на доступ к нужному ресурсу.
2. Проверьте существование ресурса: убедитесь, что файл или директория, к которым пытается получить доступ процесс, существуют и доступны.
3. Проанализируйте код ошибки -13: найдите информацию о значении этой ошибки в документации к операционной системе. Это может дать более точную подсказку о причине неудачи.
4. Изучите контекст: проанализируйте другие логи, связанные с этим процессом, чтобы получить более полное представление о ситуации.

Дополнительные сведения о вызове `access` и кодах ошибок можно найти в документации к вашей операционной системе.

```
Final Result: ""json
{
  "type": "SYSCALL", // Represents the type of log entry, indicating it's rel
  "msg": "audit(1*****):", // This is likely the beginning of an audit messa
  "arch": "c*****3e", // Represents the architecture of the system where the
  "syscall": "21", // The numerical ID of the system call invoked. You would
  "success": "no", // Indicates whether the system call was successful ('yes'
  "exit": "-13", // The exit code returned by the system call. Negative value
  "items": "1", // These are arguments passed to the system call (a0, a1, a2, a3).
  "ppid": "1", // Likely refers to the number of items or arguments associat
  "pid": "889", // Parent process ID (ppid) and the process ID
  "auid": "*****", "uid": "119", "gid": "125", "euid": "119", "suid": "
  and group IDs:
    // - auid: Audit user ID
    // - uid: Real user ID
    // - gid: Real group ID
    // - euid: Effective user ID
    // - suid: Saved set-user-ID
    // - fsuid: Filesystem user ID
    // - egid: Effective group ID
    // - sgid: Saved set-group-ID
    // - fsgid: Filesystem group ID",
  "tty": "(*****)", // The terminal associated with the process.",
  "ses": "*****", // Session ID.",
  "comm": "*****", // The name or command of the running process.",
  "exe": "/usr/lib/*****", // The executable path of the process.",
  "subj": "unconfined", // Security context or subject information. 'Unconfir
  "key": "failed_access", // A keyword or tag associated with this log entry
  "SYSCALL": "access", // The name of the system call.",
  "AUID": "unset", "UID": "rabbitmq", "GID": "rabbitmq", "EUID": "rabbitmq",
  "FSUID": "rabbitmq", "SGID": "rabbitmq", // Redundant user and group IDs, possibly reflecting
}
```



@TSINGULAR

Применение в повседневной работе: логи

```
2024-**-**T10: type: 'SYSCALL',
example.local : msg: 'audit(*****):',
msg=audit(1*** : arch: 'c*****e',
arch=c*****3e : syscall: '21',
exit=-13 a0=7* : success: 'no',
a3=7*****8 : exit: '-13',
uid=4*****! : a0: '7*****8',
suid=119 fsuid : a1: '2',
fsgid=125 tty= : a2: '8***',
comm="10_dirty : a3: '7*****8',
exe="/usr/lib/ : items: '1',
mp" subj=uncon : ppid: '1',
key="failed_ac : pid: '889',
SYSCALL=access : uid: '4*****',
UID="rabbitmq" : uid: '119',
EUID="rabbitmq" : gid: '125',
FSUID="rabbitmq" : euid: '119',
SGID="rabbitmq" : suid: '119',
fsuid: '119',
egid: '125',
sgid: '125',
fsgid: '125',
tty: '(none)',
ses: '*****',
comm: '*****',
exe: '/usr/lib/*****',
subj: 'unconfined',
key: 'failed_access',
SYSCALL: 'access',
AUID: 'unset',
UID: 'rabbitmq',
GID: 'rabbitmq',
EUID: 'rabbitmq',
SUID: 'rabbitmq',
FSUID: 'rabbitmq',
EGID: 'rabbitmq',
SGID: 'rabbitmq',
FSGID: 'rabbitmq'
```

Отчёт в службу SOC компании "Компания"

Тема: Отчет о зафиксированном неудачном системном вызове

Настоящим докладываю о выявленном инциденте в журнале событий нашей системы:

- Суть инцидента: Зафиксирован неудачный вызов системной функции `access`. Процесс, предположительно связанный с системой `*****`, не смог получить доступ к запрашиваемому ресурсу. Операционная система вернула код ошибки (-13).
- Детали:
 - Процесс выполнялся от имени пользователя `"rabbitmq"`.
 - Попытка доступа к файлу или директории завершилась неудачей.
 - Системный вызов `access` вернул ошибку с кодом -13.
- Возможные причины: а) Недостаточные права доступа для пользователя `"rabbitmq"`. б) Отсутствие запрашиваемого файла или директории. в) Потенциальная ошибка в файловой системе.
- Рекомендуемые действия: а) Проверить и при необходимости скорректировать права доступа для пользователя `"rabbitmq"`. б) Удостовериться в наличии и доступности запрашиваемого ресурса. в) Исследовать значение кода ошибки -13 в контексте используемой операционной системы. г) Провести анализ связанных логов для получения дополнительного контекста.
- Дальнейшие шаги: Рекомендуется провести тщательное расследование инцидента для предотвращения подобных ситуаций в будущем. Также следует рассмотреть возможность обновления документации по обработке подобных ошибок для оперативного реагирования.

Прошу дать указания по дальнейшим действиям и уведомить, если потребуются дополнительная информация.

С уважением,

[Ваше имя] Специалист дежурной службы SOC

```
Final Result: ``json
{
  "type": "SYSCALL. // Represents the type of log entry, indicating it's rel
  "msg": "audit(1****6):. // This is likely the beginning of an audit messag
  "arch": "c*****3e. // Represents the architecture of the system where the
  "syscall": "21. // The numerical ID of the system call invoked. You would
  be 'access'").",
  "success": "no. // Indicates whether the system call was successful ('yes'
  "exit": "-13. // The exit code returned by the system call. Negative value
  "args": "1. // These are arguments passed to the system call (a0, a1, a2, a3).
  "items": "1. // Likely refers to the number of items or arguments associat
  "ppid": "1". "pid": "889. // Parent process ID (ppid) and the process ID
  "uid": "*****", "uid": "119", "gid": "125", "euid": "119", "suid": "
  and group IDs:
  // - audit: Audit user ID
  // - uid: Real user ID
  // - gid: Real group ID
  // - euid: Effective user ID
  // - suid: Saved set-user-ID
  // - fsuid: Filesystem user ID
  // - egid: Effective group ID
  // - sgid: Saved set-group-ID
  // - fsgid: Filesystem group ID",
  "tty": "(*****). // The terminal associated with the process.",
  "ses": "*****. // Session ID.",
  "comm": "*****. // The name or command of the running process.",
  "exe": "/usr/lib/*****. // The executable path of the process.",
  "subj": "unconfined. // Security context or subject information. 'Unconfir
  "key": "failed_access. // A keyword or tag associated with this log entry
  "SYSCALL": "access. // The name of the system call.",
  "AUID": "unset", "UID": "rabbitmq", "GID": "rabbitmq", "EUID": "rabbitmq",
  "FSUID": "rabbitmq. // Redundant user and group IDs, possibly reflecting
}
```

Вывод: В журнале событий зафиксирован неудачный вызов системного вызова `access`. Процесс с именем `*****` (скорее всего часть системы `*****`) попытка получить доступ к какому-то ресурсу, но операционная система вернула ошибку (-13).

Что происходит: Процесс, запущенный от имени пользователя `"rabbitmq"`, пытается получить доступ к файлу или директории. Система не разрешает доступ, и вызов `access` завершается с кодом ошибки -13.

Возможные причины: У процесса нет необходимых прав для доступа к ресурсу. Файл или директория не существует. Возникла ошибка файловой системы.

- Рекомендации:
- Проверьте права доступа: убедитесь, что пользователь `"rabbitmq"` имеет необходимые разрешения на доступ к нужному ресурсу.
 - Проверьте существование ресурса: убедитесь, что файл или директория, к которым пытается получить доступ процесс, существуют и доступны.
 - Проанализируйте код ошибки -13: найдите информацию о значении этой ошибки в документации к операционной системе. Это может дать более точную подсказку о причине неудачи.
 - Изучите контекст: проанализируйте другие логи, связанные с этим процессом, чтобы получить более полное представление о ситуации.

Дополнительные сведения о вызове `access` и кодах ошибок можно найти в документации к вашей операционной системе.



Применение в повседневной работе: логи

```
2024-****-****10:****.0****0000
example.local audispd: type=SYSCALL
msg=audit(16****3,***:16****4):
arch=****3e syscall=21 success=no
exit=-13 a0=7****** a1=2 a2=8***
13c)****** items=1 ppid=1 pld=**
uid=******5 uid=119 gid=125 egid=119
fsuid=119 fsuid=119 egid=125 egid=125
ttype=125 ttype=(none) ses=******5
comm="10 dirty_30 Sch"
exe="/usr/lib/er*****/bin/beam.s
" subj=unconfined
key="failed_access"ARCH=x86_64
SYSCALL=access AUID="unset"
UID="rabbitmq" GID="rabbitmq"
FSUID="rabbitmq" EUID="rabbitmq"
SGID="rabbitmq" BUID="rabbitmq"
FSUID="rabbitmq" BUID="rabbitmq"
```



[AI]

```
Final Result: ""json
{
  "type": "SYSCALL", // Represents the type of log entry, indicating it's re
  "msg": "audit(1****6):. // This is likely the beginning of an audit messa
  "arch": "****3e, // Represents the architecture of the system where the
  "syscall": "21, // The numerical ID of the system call invoked. You woul
  be 'access'".",
  "success": "no, // Indicates whether the system call was successful ('yes'
  "exit": "-13, // The exit code returned by the system call. Negative valu
  ****: // These are arguments passed to the system call (a0, a1, a2, a3).",
  "items": "1, // Likely refers to the number of items or arguments associ
  "ppid": "1", "pid": "889, // Parent process ID (ppid) and the process ID
  "uid": "****", "uid": "119", "gid": "125", "egid": "119", "suid": "
  and group IDs:
    // - auid: Audit user ID
    // - uid: Real user ID
    // - gid: Real group ID
    // - egid: Effective user ID
    // - suid: Saved set-user-ID
    // - fsuid: Filesystem user ID
    // - egid: Effective group ID
    // - sgid: Saved set-group-ID
    // - fsgid: Filesystem group ID",
  "tty": "(none),
  "ses": "****, // Session ID.",
  "comm": "****, // The name or command of the running process.",
  "exe": "/usr/lib/****, // The executable path of the process.
  "subj": "unconfined, // Security context or subject information. 'Unconfi
  "key": "failed_access, // A keyword or tag associated with this log entry
  "SYSCALL": "access, // The name of the system call.",
  "AUID": "unset", "UID": "rabbitmq", "GID": "rabbitmq", "EUID": "rabbitmq",
  "SGID": "rabbitmq", "BUID": "rabbitmq", "FSUID": "rabbitmq",
  "BUID": "rabbitmq", "FSUID": "rabbitmq"
```

[AI]

```
Вызов: В журнале событий зафиксирован неудачный вызов системного
вызова 'access'. Процесс с именем '*****' (скорее всего часть системы
*****) попытался получить доступ к какому-то ресурсу, но операционная
система вернула ошибку (-13).

Что происходит:
Процесс, запущенный от имени пользователя "rabbitmq", пытается
получить доступ к файлу или директории.
Система не разрешает доступ, и вызов 'access' завершается с кодом
ошибки -13.

Возможные причины:
У процесса нет необходимых прав для доступа к ресурсу.
Файл или директория не существует.
Возникла ошибка файловой системы.

Рекомендации:
1. Проверьте права доступа: убедитесь, что пользователь "rabbitmq"
имеет необходимые разрешения на доступ к нужному ресурсу.
2. Проверьте существование ресурса: убедитесь, что файл или
директория, к которым пытается получить доступ процесс, существуют и
доступны.
3. Проанализируйте код ошибки -13: найдите информацию о значении этой
ошибки в документации к операционной системе. Это может дать более
точную подсказку о причине неудачи.
4. Изучите контекст: проанализируйте другие логи, связанные с этим
процессом, чтобы получить более полное представление о ситуации.

Дополнительные сведения о вызове 'access' и кодах ошибок можно найти
в документации к вашей операционной системе.
```

[AI]

Отчёт в службу SOC компании "Компания"

Тема: Отчет о зафиксированном неудачном системном вызове

Настоящим докладываю о выявленном инциденте в журнале событий нашей системы:

- Суть инцидента: Зафиксирован неудачный вызов системной функции access. Процесс, предположительно связанный с системой *****, не смог получить доступ к запрашиваемому ресурсу. Операционная система вернула код ошибки (-13).
- Детали:
 - Процесс выполнялся от имени пользователя "rabbitmq".
 - Попытка доступа к файлу или директории завершилась неудачей.
 - Системный вызов access вернул ошибку с кодом -13.
- Возможные причины: а) Недостаточные права доступа для пользователя "rabbitmq". б) Отсутствие запрашиваемого файла или директории. с) Потенциальная ошибка в файловой системе.
- Рекомендуемые действия: а) Проверить и при необходимости скорректировать права доступа для пользователя "rabbitmq". б) Удостовериться в наличии и доступности запрашиваемого ресурса. с) Исследовать значение кода ошибки -13 в контексте используемой операционной системы. д) Провести анализ связанных логов для получения дополнительного контекста.
- Дальнейшие шаги: Рекомендуется провести тщательное расследование инцидента для предотвращения подобных ситуаций в будущем. Также следует рассмотреть возможность обновления документации по обработке подобных ошибок для оперативного реагирования.

Прошу дать указания по дальнейшим действиям и уведомить, если потребуются дополнительная информация.

С уважением,

[Ваше имя] Специалист дежурной службы SOC



Применение в повседневной работе: логи

```
type: 'SYSCALL',
msg: 'audit(1(*****),*****):',
arch: 'c*****',
syscall: '21',
success: 'no',
exit: '-13',
a0: '*****',
a1: '21',
a2: '*****',
a3: '*****',
items: '1',
ppid: '1',
pid: '889',
uid: '*****',
gid: '125',
euid: '*****',
fgid: '125',
fsuid: '119',
sgid: '119',
suid: '119',
tty: 'none',
comm: '*****',
subj: 'unconfined',
key: 'failed_access',
SYSCALL: 'access',
AUID: 'unset',
UID: 'rabbitmq',
GID: 'rabbitmq',
SUID: 'rabbitmq',
FSUID: 'rabbitmq',
SGID: 'rabbitmq',
PSGID: 'rabbitmq'
```



[AI]

```
Final Result: {}
{
  "type": "SYSCALL", // Represents the type of log entry, indicating it's re
  "msg": "audit(1(*****): // This is likely the beginning of an audit messa
  "arch": "c*****", // Represents the architecture of the system where the
  "syscall": "21", // The numerical ID of the system call invoked. You would
  "success": "no", // Indicates whether the system call was successful ('yes'
  "exit": "-13", // The exit code returned by the system call. Negative valu
  "a0": "*****", // These are arguments passed to the system call (a0, a1, a2, a3).
  "a1": "21", // Likely refers to the number of items or arguments associat
  "a2": "*****", // Parent process ID (ppid) and the process ID
  "a3": "*****", "uid": "119", "gid": "125", "euid": "119", "sgid":
  "and group IDs:
  // - uid: Audit user ID
  // - uid: Real user ID
  // - gid: Real group ID
  // - euid: Effective user ID
  // - fsuid: Filesystem user ID
  // - sgid: Saved set-group-ID
  // - sgid: Saved set-group-ID
  // - fsuid: Filesystem group ID",
  "tty": "*****", // The terminal associated with the process.",
  "comm": "*****", // Session ID.",
  "key": "*****", // The name or command of the running process.",
  "exe": "/usr/lib/*****", // The executable path of the process
  "subj": "unconfined", // Security context or subject information. 'Unconfi
  "key": "failed_access", // A keyword or tag associated with this log entry
  "SYSCALL": "access", // The name of the system call.",
  "AUID": "unset", "UID": "rabbitmq", "GID": "rabbitmq", "SUID": "rabbitmq",
  "FSUID": "rabbitmq", "SGID": "rabbitmq", "PSGID": "rabbitmq"
}
```

[AI]

Вывод: В журнале событий зафиксирован неудачный вызов системного вызова 'access'. Процесс с именем '*****' (скорее всего часть системы '*****') попытался получить доступ к какому-то ресурсу, но операционная система вернула ошибку (-13).

Что происходит: Процесс, запущенный от имени пользователя "rabbitmq", пытается получить доступ к файлу или директории. Система не разрешает доступ, и вызов 'access' завершается с кодом ошибки -13.

Возможные причины: У процесса нет необходимых прав для доступа к ресурсу. Файл или директория не существует. Возникла ошибка файловой системы.

Рекомендации: 1. Проверьте права доступа: убедитесь, что пользователь "rabbitmq" имеет необходимые разрешения на доступ к нужному ресурсу. 2. Проверьте существование ресурса: убедитесь, что файл или директория, к которым пытаются получить доступ процесс, существуют и доступны. 3. Проанализируйте код ошибки -13: найдите информацию о значении этой ошибки в документации к операционной системе. Это может дать более точную подсказку о причине неудачи. 4. Изучите контекст: проанализируйте другие логи, связанные с этим процессом, чтобы получить более полное представление о ситуации.

Дополнительные сведения о вызове 'access' и кодах ошибок можно найти в документации к вашей операционной системе.

[AI]

Отчёт в службу SOC компании "Компания"

Тема: Отчёт в службу SOC компании "Компания"

1. Тема: Отчёт в службу SOC компании "Компания"

2. Тема: Отчёт в службу SOC компании "Компания"

3. Тема: Отчёт в службу SOC компании "Компания"

4. Тема: Отчёт в службу SOC компании "Компания"

5. Тема: Отчёт в службу SOC компании "Компания"

6. Тема: Отчёт в службу SOC компании "Компания"

7. Тема: Отчёт в службу SOC компании "Компания"

8. Тема: Отчёт в службу SOC компании "Компания"

9. Тема: Отчёт в службу SOC компании "Компания"

10. Тема: Отчёт в службу SOC компании "Компания"

11. Тема: Отчёт в службу SOC компании "Компания"

12. Тема: Отчёт в службу SOC компании "Компания"

13. Тема: Отчёт в службу SOC компании "Компания"

14. Тема: Отчёт в службу SOC компании "Компания"

15. Тема: Отчёт в службу SOC компании "Компания"

16. Тема: Отчёт в службу SOC компании "Компания"

17. Тема: Отчёт в службу SOC компании "Компания"

18. Тема: Отчёт в службу SOC компании "Компания"

19. Тема: Отчёт в службу SOC компании "Компания"

20. Тема: Отчёт в службу SOC компании "Компания"

21. Тема: Отчёт в службу SOC компании "Компания"

22. Тема: Отчёт в службу SOC компании "Компания"

23. Тема: Отчёт в службу SOC компании "Компания"

24. Тема: Отчёт в службу SOC компании "Компания"

25. Тема: Отчёт в службу SOC компании "Компания"

```
type: 'SYSCALL',
msg: 'audit(1(*****),*****):',
arch: 'c*****',
syscall: '21',
success: 'no',
exit: '-13',
a0: '*****',
a1: '21',
a2: '*****',
a3: '*****',
items: '1',
ppid: '1',
pid: '889',
uid: '*****',
gid: '125',
euid: '*****',
fgid: '125',
fsuid: '119',
sgid: '119',
suid: '119',
tty: 'none',
comm: '*****',
subj: 'unconfined',
key: 'failed_access',
SYSCALL: 'access',
AUID: 'unset',
UID: 'rabbitmq',
GID: 'rabbitmq',
SUID: 'rabbitmq',
FSUID: 'rabbitmq',
SGID: 'rabbitmq',
PSGID: 'rabbitmq'
```



[AI]

```
Final Result: {}
{
  "type": "SYSCALL", // Represents the type of log entry, indicating it's re
  "msg": "audit(1(*****): // This is likely the beginning of an audit messa
  "arch": "c*****", // Represents the architecture of the system where the
  "syscall": "21", // The numerical ID of the system call invoked. You would
  "success": "no", // Indicates whether the system call was successful ('yes'
  "exit": "-13", // The exit code returned by the system call. Negative valu
  "a0": "*****", // These are arguments passed to the system call (a0, a1, a2, a3).
  "a1": "21", // Likely refers to the number of items or arguments associat
  "a2": "*****", // Parent process ID (ppid) and the process ID
  "a3": "*****", "uid": "119", "gid": "125", "euid": "119", "sgid":
  "and group IDs:
  // - uid: Audit user ID
  // - uid: Real user ID
  // - gid: Real group ID
  // - euid: Effective user ID
  // - fsuid: Filesystem user ID
  // - sgid: Saved set-group-ID
  // - sgid: Saved set-group-ID
  // - fsuid: Filesystem group ID",
  "tty": "*****", // The terminal associated with the process.",
  "comm": "*****", // Session ID.",
  "key": "*****", // The name or command of the running process.",
  "exe": "/usr/lib/*****", // The executable path of the process
  "subj": "unconfined", // Security context or subject information. 'Unconfi
  "key": "failed_access", // A keyword or tag associated with this log entry
  "SYSCALL": "access", // The name of the system call.",
  "AUID": "unset", "UID": "rabbitmq", "GID": "rabbitmq", "SUID": "rabbitmq",
  "FSUID": "rabbitmq", "SGID": "rabbitmq", "PSGID": "rabbitmq"
}
```

[AI]

Вывод: В журнале событий зафиксирован неудачный вызов системного вызова 'access'. Процесс с именем '*****' (скорее всего часть системы '*****') попытался получить доступ к какому-то ресурсу, но операционная система вернула ошибку (-13).

Что происходит: Процесс, запущенный от имени пользователя "rabbitmq", пытается получить доступ к файлу или директории. Система не разрешает доступ, и вызов 'access' завершается с кодом ошибки -13.

Возможные причины: У процесса нет необходимых прав для доступа к ресурсу. Файл или директория не существует. Возникла ошибка файловой системы.

Рекомендации: 1. Проверьте права доступа: убедитесь, что пользователь "rabbitmq" имеет необходимые разрешения на доступ к нужному ресурсу. 2. Проверьте существование ресурса: убедитесь, что файл или директория, к которым пытаются получить доступ процесс, существуют и доступны. 3. Проанализируйте код ошибки -13: найдите информацию о значении этой ошибки в документации к операционной системе. Это может дать более точную подсказку о причине неудачи. 4. Изучите контекст: проанализируйте другие логи, связанные с этим процессом, чтобы получить более полное представление о ситуации.

Дополнительные сведения о вызове 'access' и кодах ошибок можно найти в документации к вашей операционной системе.

[AI]

Тема: Отчёт в службу SOC компании "Компания"

1. Тема: Отчёт в службу SOC компании "Компания"

2. Тема: Отчёт в службу SOC компании "Компания"

3. Тема: Отчёт в службу SOC компании "Компания"

4. Тема: Отчёт в службу SOC компании "Компания"

5. Тема: Отчёт в службу SOC компании "Компания"

6. Тема: Отчёт в службу SOC компании "Компания"

7. Тема: Отчёт в службу SOC компании "Компания"

8. Тема: Отчёт в службу SOC компании "Компания"

9. Тема: Отчёт в службу SOC компании "Компания"

10. Тема: Отчёт в службу SOC компании "Компания"

11. Тема: Отчёт в службу SOC компании "Компания"

12. Тема: Отчёт в службу SOC компании "Компания"

13. Тема: Отчёт в службу SOC компании "Компания"

14. Тема: Отчёт в службу SOC компании "Компания"

15. Тема: Отчёт в службу SOC компании "Компания"

16. Тема: Отчёт в службу SOC компании "Компания"

17. Тема: Отчёт в службу SOC компании "Компания"

18. Тема: Отчёт в службу SOC компании "Компания"

19. Тема: Отчёт в службу SOC компании "Компания"

20. Тема: Отчёт в службу SOC компании "Компания"



@TSINGULAR

Чему ещё научить свой ИИ

Cisco переводит API-документацию на язык ИИ

<https://blogs.cisco.com/developer/cisco-api-documentations-is-now-adapted-for-gen-ai-technologies>

Разработчики активно используют ИИ-инструменты и языковые модели для создания кода и решения проблем.

Cisco DevNet предоставляет ссылки на OpenAPI документацию в форматах **JSON/YAML**.

Эти спецификации можно применять **в промптах или для RAG**

Тесты подтвердили: **использование OpenAPI документов в запросах повышает точность работы языковых моделей.**

ИИ-системы выдают более корректные инструкции по использованию API.

```
/v1/inventory/devices/asas/{deviceId}/read:
post:
  tags:
    - Inventory
  summary: Read ASA device configuration
  description: >-
    This is an asynchronous operation to read the latest configuration on an
    ASA device in the CDO tenant. This operation returns a link to a
    transaction object that can be used to monitor the progress of the
    operation.
  operationId: readAsaDeviceConfiguration
  parameters:
    - name: deviceId
      in: path
      description: The unique identifier of the ASA device in CDO.
      required: true
      schema:
        type: string
        format: uuid
  responses:
    '202':
      description: >-
        CDO Transaction object that can be used to track the progress of the
        read operation
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/CdoTransaction'
    '400':
      $ref: '#/components/responses/http400BadRequest'
    '401':
      $ref: '#/components/responses/http401Unauthorised'
    '403':
      $ref: '#/components/responses/http403Forbidden'
    '500':
      description: Internal server error.
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/CommonApiError'
  security:
    - bearerAuth: []
```



@TSINGULAR

ИИ – агенты в команде

Руководитель аппарата CEO Anthropic - Авиталь Балвит:
через 3 года традиционная работа может исчезнуть из-за прогресса ИИ.

Глава AWS: ИИ заменит разработчиков через 2 года

- Создание агента не должно быть каким-то проектом для хакатона по информатике.
- Это должно быть чем-то простым, как найм и адаптация сотрудника.
- Мы собираемся привести уровень автоматизации, которого мир никогда не видел.

Nvidia's CEO Jensen Huang и Salesforce CEO Marc Benioff на Dreamforce 2024.

<https://www.youtube.com/watch?v=kfe3ajUYScd>

[MMRole: фреймворк для мультимодальных ролевых агентов ИИ](#)

[MetaGPT: фреймворк мультиагентных систем](#)

[Quivr: фреймворк для создания ИИ-ассистентов](#)

Готовые решения: (https://github.com/NirDiamant/GenAI_Agents)

Простые агенты для начинающих:

1. Разговорный агент с контекстом
2. Агент для ответов на вопросы
3. Агент для анализа данных

Специализированные агенты:

4. Агент поддержки клиентов (LangGraph)
5. Агент для оценки эссе (LangGraph)
6. Агент планирования путешествий (LangGraph)

Креативные и генеративные агенты:

7. Генератор GIF-анимаций (LangGraph)
8. Генератор стихов с озвучкой (LangGraph)
9. Агент-композитор музыки (LangGraph)

Продвинутые архитектуры агентов:

10. Разговорный агент с улучшенной памятью
11. Система многоагентного сотрудничества
12. Самосовершенствующийся агент
13. Агент, ориентированный на задачи
14. Агент для поиска в интернете и суммирования
15. Многоагентная исследовательская команда (Autogen)



@TSINGULAR

Обучение

Вендор	Курсы
Anthropic	https://github.com/anthropics/courses/tree/master/prompt_engineering_interactive_tutorial
Microsoft	https://github.com/microsoft/generative-ai-for-beginners
OpenAI	https://platform.openai.com/docs/guides/function-calling
Google	https://services.google.com/fh/files/misc/gemini-for-google-workspace-prompting-guide-101.pdf
AWS	https://aws.amazon.com/blogs/machine-learning/prompt-engineering-techniques-and-best-practices-learn-by-doing-with-anthropics-claude-3-on-amazon-bedrock/
Salesforce	https://trailhead.salesforce.com/
Cisco	https://blogs.cisco.com/learning/from-hello-world-to-hi-ai
Lakera	Каталог ресурсов по безопасности ИИ https://docs.google.com/spreadsheets/d/1tv3d2M4-RO8xJYiXp5uVvrvGWffM-40La18G_uFZIRM/
OWASP	Periodic Table of AI Security https://owaspai.org/goto/periodictable/
	Открытый курс по LLM от практиков https://parlance-labs.com/education/
	«Библия промт-инженера»: систематический обзор техник генерации текста и изображений ИИ (https://arxiv.org/pdf/2406.06608)
	https://www.promptingguide.ai/ru
	самая большая коллекция RAG техник: https://github.com/NirDiamant/RAG_Techniques
	Разработка приложений с LLM: практическое введение (https://www.gdcorner.com/blog/2024/06/12/NoBSIntroToLLMs-1-GettingStarted.html#ollama)



@TSINGULAR

Q&A

