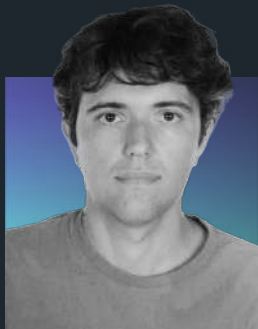




From Alert to Answer

The Checkmk Approach to Practical AI



Matteo Villosio
AI Engineer
Checkmk



Annika Felgenträger
Product Manager
Checkmk





9:41

rsll

**ON-CALL
ALERT**



SYSTEM CRITICAL - RESPONSE REQUIRED

ACCEPT

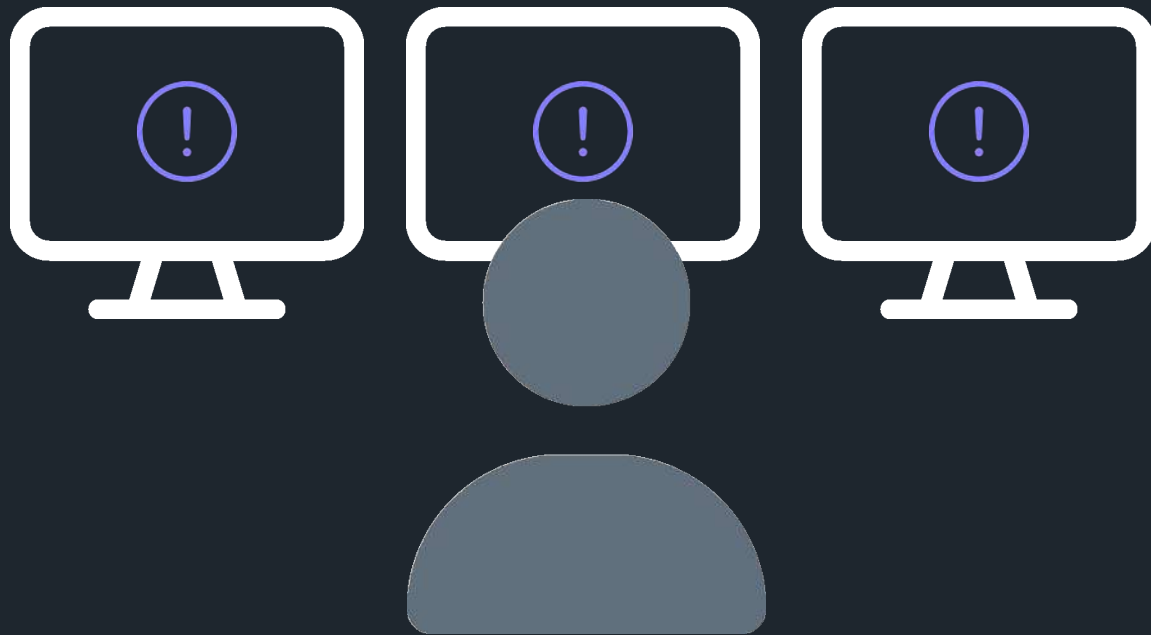
DISMISS



Where do I start?

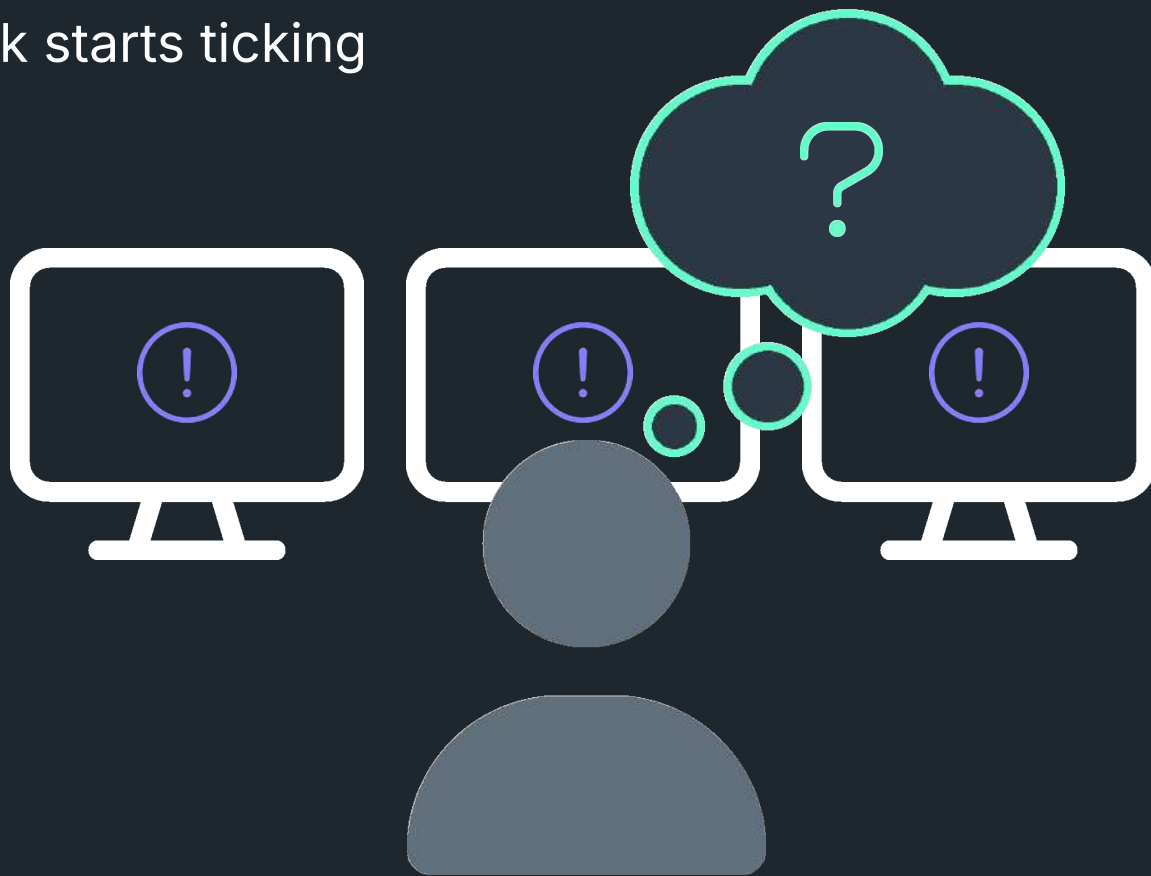
An alert fires

And the clock starts ticking



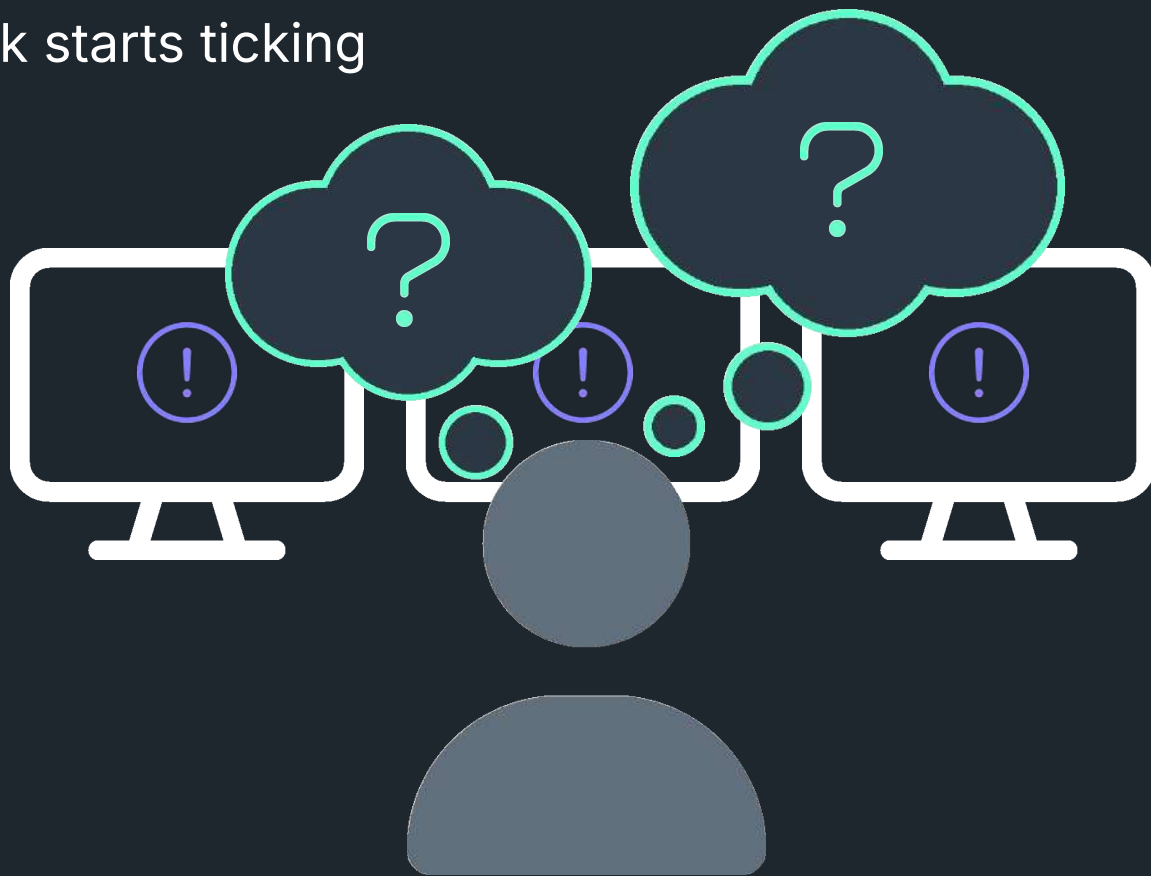
An alert fires

And the clock starts ticking



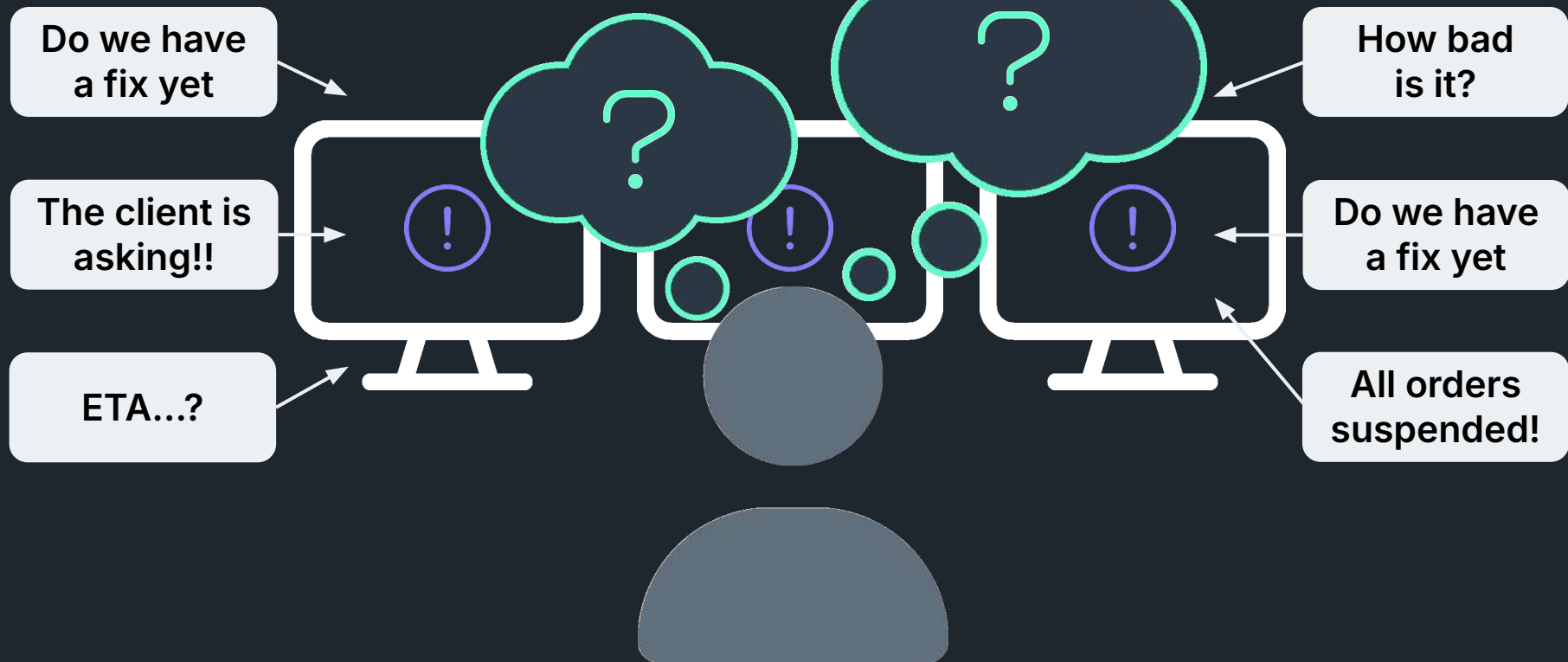
An alert fires

And the clock starts ticking



An alert fires

And the clock starts ticking





**Detective work costs time
and money.**

Time is money



80% of alerts? You know them, you know how to fix them.



The unfamiliar 20% is where investigation gets chaotic and costly.



Up to 80% of MTTR is diagnosis, not the fixing.



Shortening the diagnosis phase reduces the cost.





Explain it. With AI.

Explain with AI



- ✓ One click in Checkmk Cloud
- ✓ Gathers context across your services
- ✓ Translates complex signals into a natural language root cause analysis
- ✓ Provides a recommended next step

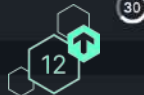
Service problems (unhandled)					
State	Host	Service	Icons	Summary	Age
CRIT	fra-web-prod-03	Systemd Service Summary	☰ ⚡	Total: 128, Disabled: 3, Failed: 1 CRIT , 1 service failed (omd) CRIT	15 m
CRIT	fra-web-prod-03	API Error Rate	☰ 📧 ⚡	CRITICAL: 73% of API requests returning 5xx errors — order processing effectively down CRIT	10 m
CRIT	fra-web-prod-03	Application Health	☰ ⚡	CRITICAL: Database connection pool exhausted (20/20), 31 threads blocked, circuit breaker OPEN	10 m
CRIT	fra-web-prod-03	Circuit Breaker OrderService	☰ ⚡	CRITICAL: OPEN since 02:14 UTC — all order submissions rejected, 340 customers affected	10 m
CRIT	fra-web-prod-03	Circuit Breaker PaymentService	☰ ⚡	CRITICAL: OPEN since 06:55 UTC — payment processing halted, revenue impact estimated	10 m

Available in: [Cloud](#)

Services of host fra-web-prod-03

Commands Host Services Export Display Help

✕ Acknowledge problems
🚫 Schedule downtimes
🔍 Filter
☑ Show checkboxes
📍 fra-web-prod-03



71 rows

fra-web-prod-03

State	Service	Icons	Summary	Age	Checked	Perf-O-Meter
OK	Check_MK	☰ 📁 ➕	[push-agent] Success, [piggyback] Success (but no data found for this host), execution time 0.0 sec	108 m	54.0 s	20 ms
OK	Check_MK Agent	☰ ➕	Version: 2.5.0~2026.05.12, OS: linux, Agent plug-ins: 0, Local checks: 2	108 m	54.0 s	
OK	Check_MK Discovery	☰ 📁 ➕	Services: all up to date, Host labels: all up to date, execution time 0.0 sec	109 m	109 m	20 ms
OK	Check_MK HW/SW Inventory	☰ 📁 ➕	Found 250 inventory entries, software changes, hardware changes, networking changes, Found 54 status entries, execution time 0.0 sec	109 m	109 m	20 ms
WARN	Alertmanager	☰ ➕	WARNING: Notification backlog — 47 undelivered alerts, Slack webhook returning 429 Too Many Requests	113 s	54.0 s	
CRIT	API Error Rate	☰ 📁 ➕	CRITICAL: 73% of API requests returning 5xx errors — order processing effectively down CRIT	113 s	54.0 s	
CRIT	Application Health	☰ ➕	CRITICAL: Database connection pool exhausted (20/20), 31 threads blocked, circuit breaker OPEN since 02:14 UTC	113 s	54.0 s	
WARN	Certificate vault.corp.local	☰ 📁 ➕	WARNING: TLS certificate expires in 2 days, auto-renewal blocked by DNS failure WARN	113 s	54.0 s	
CRIT	Circuit Breaker OrderService	☰ ➕	CRITICAL: OPEN since 02:14 UTC — all order submissions rejected, 340 customers affected	113 s	54.0 s	
CRIT	Circuit Breaker PaymentService	☰ ➕	CRITICAL: OPEN since 02:14 UTC — payment processing halted, revenue impact estimated	113 s	54.0 s	
OK	CPU load	☰ 📁 ➕	15 min load: 0.00, 15 min load per core: 0.00 (8 cores)	108 m	54.0 s	0.01
OK	CPU utilization	☰ 📁 ➕	Total CPU: 0.27%	108 m	54.0 s	0.27%
CRIT	Cron: Backup	☰ ➕	CRITICAL: Nightly backup failed at 01:12 UTC — NFS mount stale, last successful backup 26h ago	114 s	54.0 s	
WARN	Cron: Index Rebuild	☰ ➕	WARNING: Search index rebuild missed execution window, index 14h stale	114 s	54.0 s	
WARN	Cron: Session Cleanup	☰ ➕	WARNING: Expired session cleanup not running, 12,847 orphaned sessions consuming memory	114 s	54.0 s	
WARN	Disk I/O sda1	☰ 📁 ➕	WARNING: Elevated disk latency, SMART reports 218 reallocated sectors (threshold: 140) WARN	114 s	54.0 s	
OK	Disk IO SUMMARY	☰ 📁 ➕	Read: 0.00 B/s, Write: 23.3 kB/s, Latency: 123 microseconds	107 m	54.0 s	0 B/s / 22.8 KiB/s
WARN	Disk Latency sdb	☰ 📁 ➕	WARNING: Average I/O latency 89ms (baseline 4ms), possible controller degradation WARN	114 s	54.0 s	
CRIT	Disk SMART sda	☰ 📁 ➕	CRITICAL: Reallocated sector count 218 exceeds failure threshold (200), drive replacement urgent CRIT	114 s	54.0 s	
WARN	DNS Resolution	☰ 📁 ➕	WARNING: DNS queries averaging 4.2s, internal resolver 10.0.0.53 intermittent WARN	114 s	54.0 s	



Monitor > Overview > All hosts > fra-web-prod-03 > Services of host

Services of host fra-web-prod-03

Commands Host Services Expert Display Help

Acknowledge problems Schedule downtimes Filter Show checkboxes

fra-web-prod-03

State	Service	Icons	Summary
OK	Check_MK	[OK] [Info]	[push-agent] Success, [piggyback]
OK	Check_MK Agent	[OK] [Info]	Version: 2.5.0-2024.05.21, OS: 96
OK	Check_MK Discovery	[OK] [Info]	Services: all up to date, Host info
OK	Check_MK HW/Disk Inventory	[OK] [Info]	Found 250 inventory entries, soft
WARN	Alertmanager	[WARN] [Info]	WARNING: Notification backlog -
CRIT	API Error Rate	[CRIT] [Info]	CRITICAL: 73% of API requests fa
CRIT	Application Health	[CRIT] [Info]	CRITICAL: Database connection 0
WARN	Certificate vault.corp.local	[WARN] [Info]	WARNING: TLS certificate expir
CRIT	Circuit Breaker OrderService	[CRIT] [Info]	CRITICAL: OPEN since 02:14 UTC
CRIT	Circuit Breaker PaymentService	[CRIT] [Info]	CRITICAL: OPEN since 02:14 UTC
OK	CPU load	[OK] [Info]	15 min load: 0.06, 15 min load per
OK	CPU utilization	[OK] [Info]	Total CPU: 0.41%
CRIT	Crash Backup	[CRIT] [Info]	CRITICAL: Nightly backup failed
WARN	Crash Index Rebuild	[WARN] [Info]	WARNING: Search index rebuild
WARN	Crash Session Cleanup	[WARN] [Info]	WARNING: Expired session clean
WARN	Disk I/O stat	[WARN] [Info]	WARNING: Elevated disk latency,
OK	Disk I/O SUMMARY	[OK] [Info]	Read: 243 MB/s, Write: 27.8 MB/s,
WARN	Disk Latency sdb	[WARN] [Info]	WARNING: Average I/O latency 80
CRIT	Disk SMART sda	[CRIT] [Info]	CRITICAL: Reallocated sector co
WARN	Disk Resolution	[WARN] [Info]	WARNING: DNS queries average

Explain with AI



Host

UP

fra-web-prod-03



Service

CRIT

Circuit Breaker OrderService



AI-generated answer

Thinking...

Analyzing Service Performance

I'm currently scrutinizing the `Circuit Breaker OrderService` on host `fra-web-prod-03`, which has unexpectedly entered a `CRIT` state. My focus is on pinpointing the root cause of this critical alert.

Monitor > Overview > All hosts > fra-web-prod-03 > Services of host

Services of host fra-web-prod-03

Commands Host Services Expert Display Help

Acknowledge problems Schedule downtimes Filter Show checkboxes

fra-web-prod-03

State	Service	Name	Summary
OK	Check_MK	[push-agent] Success, [piggypark] Success	
OK	Check_MK Agent	Version: 2.5.0-2024.06.21, OS: linux, Agent p...	
CRIT	Check_MK Discovery	Services vanished: 71 [checkmk_agent: 1, ip...	Services vanished: 71 [checkmk_agent: 1, ip...
OK	Check_MK HWIDW Inventory	Found 250 inventory entries, hardware chang...	Found 250 inventory entries, hardware chang...
WARN	Alertmanager	WARNING: Notification backlog -- 47 undefi...	WARNING: Notification backlog -- 47 undefi...
CRIT	API Error Rate	CRITICAL: 73% of API requests returning 500	CRITICAL: 73% of API requests returning 500
CRIT	Application Health	CRITICAL: Database connection pool exhaust...	CRITICAL: Database connection pool exhaust...
WARN	Certificate vault.corp.local	WARNING: TLS certificate expires in 2 days,	WARNING: TLS certificate expires in 2 days,
CRIT	Circuit Breaker OrderService	CRITICAL: OPEN since 02:14 UTC -- 40 orde...	CRITICAL: OPEN since 02:14 UTC -- 40 orde...
CRIT	Circuit Breaker PaymentService	CRITICAL: OPEN since 02:14 UTC -- payment...	CRITICAL: OPEN since 02:14 UTC -- payment...
OK	CPU load	15 min load: 0.06, 15 min load per core: 0.01	15 min load: 0.06, 15 min load per core: 0.01
OK	CPU utilization	Total CPU: 1.03%	Total CPU: 1.03%
CRIT	Cron Backup	CRITICAL: Nightly backup failed at 01:12 UTC	CRITICAL: Nightly backup failed at 01:12 UTC
WARN	Cron Index Rebuild	WARNING: Search index rebuild missed even...	WARNING: Search index rebuild missed even...
WARN	Cron Session Cleanup	WARNING: Expired session cleanup not run...	WARNING: Expired session cleanup not run...
WARN	Disk I/O stat	WARNING: Elevated disk latency, SMART rep...	WARNING: Elevated disk latency, SMART rep...
WARN	Disk Latency sdr	WARNING: Average I/O latency 89ms (base...	WARNING: Average I/O latency 89ms (base...

Checkmk #12

Explain with AI



Host

UP

fra-web-prod-03



Service

CRIT

Circuit Breaker OrderService



AI-generated answer

Thinking...

Diagnosing Systemic Network Issues

I am currently focused on identifying the root cause of widespread CRIT and WARN states across fra-web-prod-03. Network gateway unreachability and significant NTP clock skew appear to be the most fundamental drivers, leading to authentication failures and storage issues.

Home > Overview > All hosts > fra-web-prod-03 > Services of host

Services of host fra-web-prod-03

Commands Host Services Export Display Help

Acknowledge problems Schedule downtimes Filter Show checkboxes

fra-web-prod-03

State	Service	Name	Summary
OK	Check_MK	[push-agent] Success, [biggyha	
OK	Check_MK Agent	Version: 2.5.0-2024.05.21, OS: W	
OK	Check_MK Discovery	Services: all up to date, Host info	
OK	Check_MK HW/SW Inventory	Found 250 inventory entries, soft	entries, execution time 0.0 sec
WARN	Alermanager		WARNING: Notification backlog -
CRIT	API Error Rate		CRITICAL: 73% of API requests fa
CRIT	Application Health		CRITICAL: Database connection
WARN	Certificate vault.corp.local		WARNING: TLS certificate expir
CRIT	Circuit Breaker OrderService		CRITICAL: OPEN since 02:14 UTC
CRIT	Circuit Breaker PaymentService		CRITICAL: OPEN since 02:14 UTC
OK	CPU load		15 min load: 0.06, 15 min load pe
OK	CPU utilization		Total CPU: 0.41%
CRIT	Crash Backup		CRITICAL: Nightly backup failed
WARN	Crash Index Rebuild		WARNING: Search index rebuild
WARN	Crash Session Cleanup		WARNING: Expired session clean
WARN	Disk I/O stat		WARNING: Elevated disk latency,
OK	Disk I/O SUMMARY		Read: 243 MB/s, Write: 27.8 MB/s,
WARN	Disk Latency stat		WARNING: Average I/O latency 8
WARN	Disk SMART stat		CRITICAL: Reallocated sector co
WARN	Disk Resilience		WARNING: DNS queries average

Checkmk #12 Conference

Explain with AI



Host

UP

fra-web-prod-03



Service

CRIT

Circuit Breaker OrderService



AI-generated answer

Thinking...

Investigating Host-Wide Failure

I'm analyzing a critical host-wide failure on fra-web-prod-03. The Circuit Breaker OrderService being OPEN is a downstream symptom. My current focus is on the massive NTP synchronization issue causing significant clock skew, impacting Kerberos and PostgreSQL replication, which likely explains many of the cascading failures.

Correlating Systemic Failures

I'm investigating the interconnected failures on fra-web-prod-03. The Circuit Breaker OrderService's OPEN state is secondary to broader issues. The critically failed NTP synchronization, leading to severe clock skew, is a primary suspect for the widespread outages, including Kerberos and RabbitMQ.

Pinpointing Cascading Outage Causes

I'm delving into the systemic collapse on fra-web-prod-03, where the Circuit Breaker OrderService's CRIT state is just one symptom. The profound NTP synchronization failure, causing extreme clock skew, is the most compelling root cause, directly impacting authentication and critical messaging infrastructure.

Uncovering Core Infrastructure Issues

I'm examining the extensive failures impacting fra-web-prod-03. The open Circuit Breaker OrderService is a clear indicator of deeper problems. My primary focus is now on the NTP synchronization failure, responsible for the significant clock skew that is likely the catalyst for the widespread outages.

Resolving Widespread Service Outages

I'm currently investigating the root cause of the systemic failure on fra-web-prod-03. The Circuit Breaker OrderService being open is a symptom. My analysis points to a critical NTP synchronization issue causing significant clock skew, which is likely triggering the widespread outages across the host.

Monitor + Overview + All hosts + fra-web-prod-03 + Services of host

Services of host fra-web-prod-03

Commands Host Services Export Display Help

Acknowledge problems Schedule downtimes Filter Show checkboxes

fra-web-prod-03

State	Service	Name	Summary
OK	Check_MK	[push-agent] Success, [pingerback] Success	
OK	Check_MK Agent	Version: 2.5.0-2024.06.21, OS: Linux, Agent p	
CRIT	Check_MK Discovery	Services vanished: 71 [checkmk_agent], [cp	Services vanished: 71 [checkmk_agent], [cp kernel_performance, [kernel_uptime], [iso_911 [smf_apache], [smf_dockerage], [smf_stat systemd_units_socket, summary], [top_con [check_mk], [libvirt], [iso_911], [smf_info execution time 0.0 sec.
OK	Check_MK HWIDW Inventory	Found 250 inventory entries, hardware chang	Found 250 inventory entries, hardware chang execution time 0.1 sec.
WARN	Alertmanager	WARNING: Notification backlog -- 47 undelet	WARNING: Notification backlog -- 47 undelet Requests.
CRIT	API Error Rate	CRITICAL: 75% of API requests returning 5xx	CRITICAL: 75% of API requests returning 5xx
CRIT	Application Health	CRITICAL: Database connection pool exhaust	CRITICAL: Database connection pool exhaust since 02:14 UTC
WARN	Certificate vault.org.local	WARNING: TLS certificate expires in 2 days,	WARNING: TLS certificate expires in 2 days,
CRIT	Circuit Breaker OrderService	CRITICAL: OPEN since 02:14 UTC -- all order	CRITICAL: OPEN since 02:14 UTC -- all order
CRIT	Circuit Breaker PaymentService	CRITICAL: OPEN since 02:14 UTC -- payment	CRITICAL: OPEN since 02:14 UTC -- payment
OK	CPU load	15 min load: 0.06, 15 min load per core: 0.21	15 min load: 0.06, 15 min load per core: 0.21
OK	CPU utilization	Total CPU: 0.46%	Total CPU: 0.46%
CRIT	Crash Backup	CRITICAL: Nightly backup failed at 01:12 UTC	CRITICAL: Nightly backup failed at 01:12 UTC
WARN	Crash Index Rebuild	WARNING: Search index rebuild missed event	WARNING: Search index rebuild missed event
WARN	Crash Session Cleanup	WARNING: Expired session cleanup not run	WARNING: Expired session cleanup not run
WARN	Disk I/O stat	WARNING: Elevated disk latency, SMART rep	WARNING: Elevated disk latency, SMART rep
WARN	Disk Latency	WARNING: Average I/O latency 59ms (Seaver	WARNING: Average I/O latency 59ms (Seaver

Checkmk #12

Explain with AI

Host
UP fra-web-prod-03

Service
CRIT Circuit Breaker OrderService



AI-generated answer

Please review to ensure factual correctness.

SUMMARY

The **Circuit Breaker OrderService** is in a **CRIT** state, indicating it has opened and is actively rejecting all order submissions. This is not an isolated problem but a symptom of a catastrophic, host-wide failure. Dozens of other services are also **CRIT**, including fundamental infrastructure like **Upstream Gateway** (unreachable), **NTP Synchronization** (-847s clock skew), **NFS Mount** (stale), and a degraded **RAID Array**. The entire application stack, including **PostgreSQL**, **RabbitMQ**, and the **JVM**, is non-functional, indicating the host is effectively down.

Confidence: **Medium**

SERVICE CONTEXT

- **The service:** This check monitors a software circuit breaker, a design pattern used to detect high failure rates in a dependent service (the **OrderService**) and temporarily halt requests to it, preventing cascading failures.
- **The failure:** A **CRIT** state signifies the breaker is "OPEN," meaning the application is intentionally blocking all order processing functions to protect the system from further damage due to underlying faults.

RECOMMENDED ACTIONS

1. **Investigate network isolation:** Confirm why the host cannot reach its default gateway **10.0.1.1**, as this is a likely trigger for numerous downstream failures including **NFS**, **LDAP**, and **NTP**.
2. **Correct clock skew:** Address the **-847s** time drift reported by **NTP Synchronization**, as this is breaking **Kerberos** authentication and impacting other time-sensitive operations.
3. **Address storage failures:** Investigate the stale **NFS Mount**, the degraded **RAID Array md0**, and the failing disk reported by **Disk SMART sda**, as these I/O errors are crippling the system.
4. **Analyze application state:** Once infrastructure is stable, examine the **Thread Pool** blockages, **JVM Heap** pressure, and exhausted **PostgreSQL** connection pool to guide application recovery.
5. **Review agent health:** After restoring host stability, investigate why the **Checkmk** agent is failing to report most services, as indicated by the numerous "vanished" items in the **Check_MK Discovery** service.



Monitor + Overview + All hosts + fra-web-prod-03 + Services of host

Services of host fra-web-prod-03

Commands Host Services Export Display Help

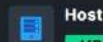
Acknowledge problems Schedule downtimes Filter Show checkboxes

fra-web-prod-03

State	Service	Name	Summary
OK	Check_MK	[push-agent] Success, [pingerback] Success	
OK	Check_MK Agent	Version: 2.5.0-2024.06.21, OS: linux, Agent p	
CRIT	Check_MK Discovery		Services vanished: 71 [checkmk_agent], [cp
OK	Check_MK HWIDW Inventory		Found 250 inventory entries, hardware chang
WARN	Alertmanager		WARNING: Notification backlog -- 47 unde
CRIT	API Error Rate		CRITICAL: 75% of API requests returning 50
CRIT	Application Health		CRITICAL: Database connection pool exhaust
WARN	Certificate vault.org.local		WARNING: TLS certificate expires in 2 days,
CRIT	Circuit Breaker OrderService		CRITICAL: OPEN since 02:14 UTC -- all orde
CRIT	Circuit Breaker PaymentService		CRITICAL: OPEN since 02:14 UTC -- payment
OK	CPU load		15 min load: 0.06, 15 min load per core: 0.21
OK	CPU utilization		Total CPU: 0.46%
CRIT	Crash Backup		CRITICAL: Nightly backup failed at 01:12 UTC
WARN	Crash Index Rebuild		WARNING: Search index rebuild missed even
WARN	Crash Session Cleanup		WARNING: Expired session cleanup not run
WARN	Disk I/O stat		WARNING: Elevated disk latency, SMART rep
WARN	Disk Latency 5%		WARNING: Average I/O latency 59ms (Sever

Checkmk #12

Explain with AI



Host

UP

fra-web-prod-03



Service

CRIT

Circuit Breaker OrderService



AI-generated answer

Please review to ensure factual correctness.

SUMMARY

The **Circuit Breaker OrderService** is in a **CRIT** state, indicating it has opened and is actively rejecting all order submissions. This is not an isolated problem but a symptom of a catastrophic, host-wide failure. Dozens of other services are also **CRIT**, including fundamental infrastructure like **Upstream Gateway** (unreachable), **NTP Synchronization** (-847s clock skew), **NFS Mount** (stale), and a degraded **RAID Array**. The entire application stack, including **PostgreSQL**, **RabbitMQ**, and the **JVM**, is non-functional, indicating the host is effectively down.

Confidence: **Medium**

SERVICE CONTEXT

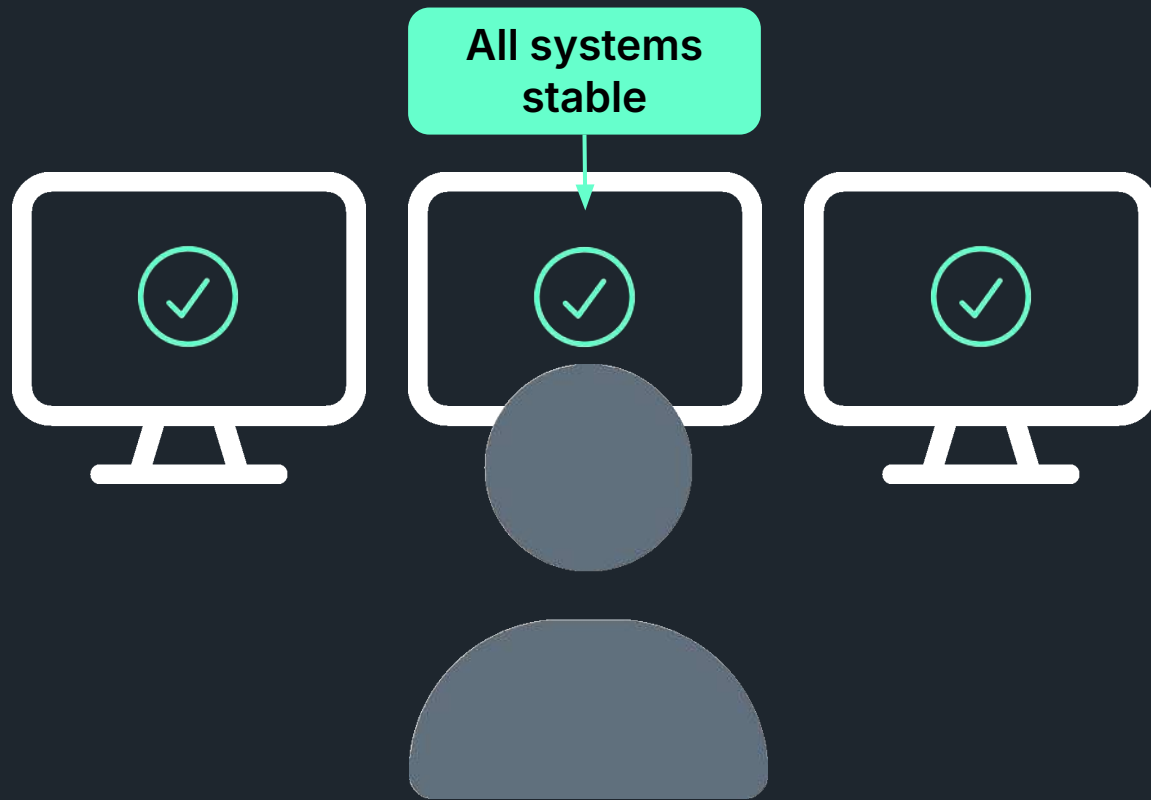
- **The service:** This check monitors a software circuit breaker, a design pattern used to detect high failure rates in a dependent service (the **OrderService**) and temporarily halt requests to it, preventing cascading failures.
- **The failure:** A **CRIT** state signifies the breaker is "OPEN," meaning the application is intentionally blocking all order processing functions to protect the system from further damage due to underlying faults.

RECOMMENDED ACTIONS

1. **Investigate network isolation:** Confirm why the host cannot reach its default gateway **10.0.1.1**, as this is a likely trigger for numerous downstream failures including **NFS**, **LDAP**, and **NTP**.
2. **Correct clock skew:** Address the **-847s** time drift reported by **NTP Synchronization**, as this is breaking **Kerberos** authentication and impacting other time-sensitive operations.
3. **Address storage failures:** Investigate the stale **NFS Mount**, the degraded **RAID Array md0**, and the failing disk reported by **Disk SMART sda**, as these I/O errors are crippling the system.
4. **Analyze application state:** Once infrastructure is stable, examine the **Thread Pool** blockages, **JVM Heap** pressure, and exhausted **PostgreSQL** connection pool to guide application recovery.
5. **Review agent health:** After restoring host stability, investigate why the **Checkmk** agent is failing to report most services, as indicated by the numerous "vanished" items in the **Check_MK Discovery** service.

An alert fires

And the clock starts ticking



How it works: the principles



It is secure: no changes is applied to your site or your monitoring



You are in the driver's seat: get a summary and recommendation, not a button to press



Added value, not burden: no additional complexity for the user. Works gets simpler, not more complex.

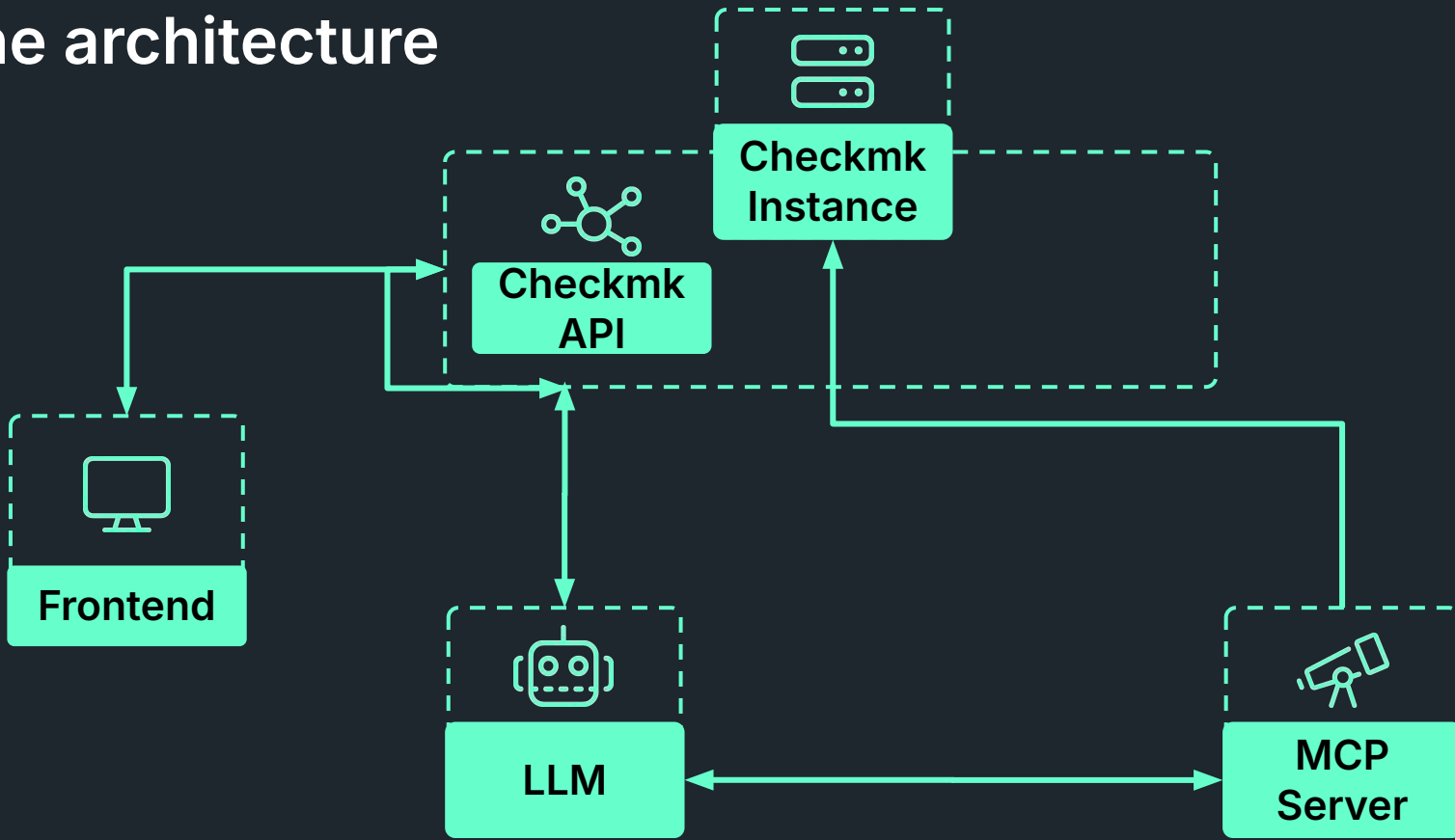
How it works: trust and data



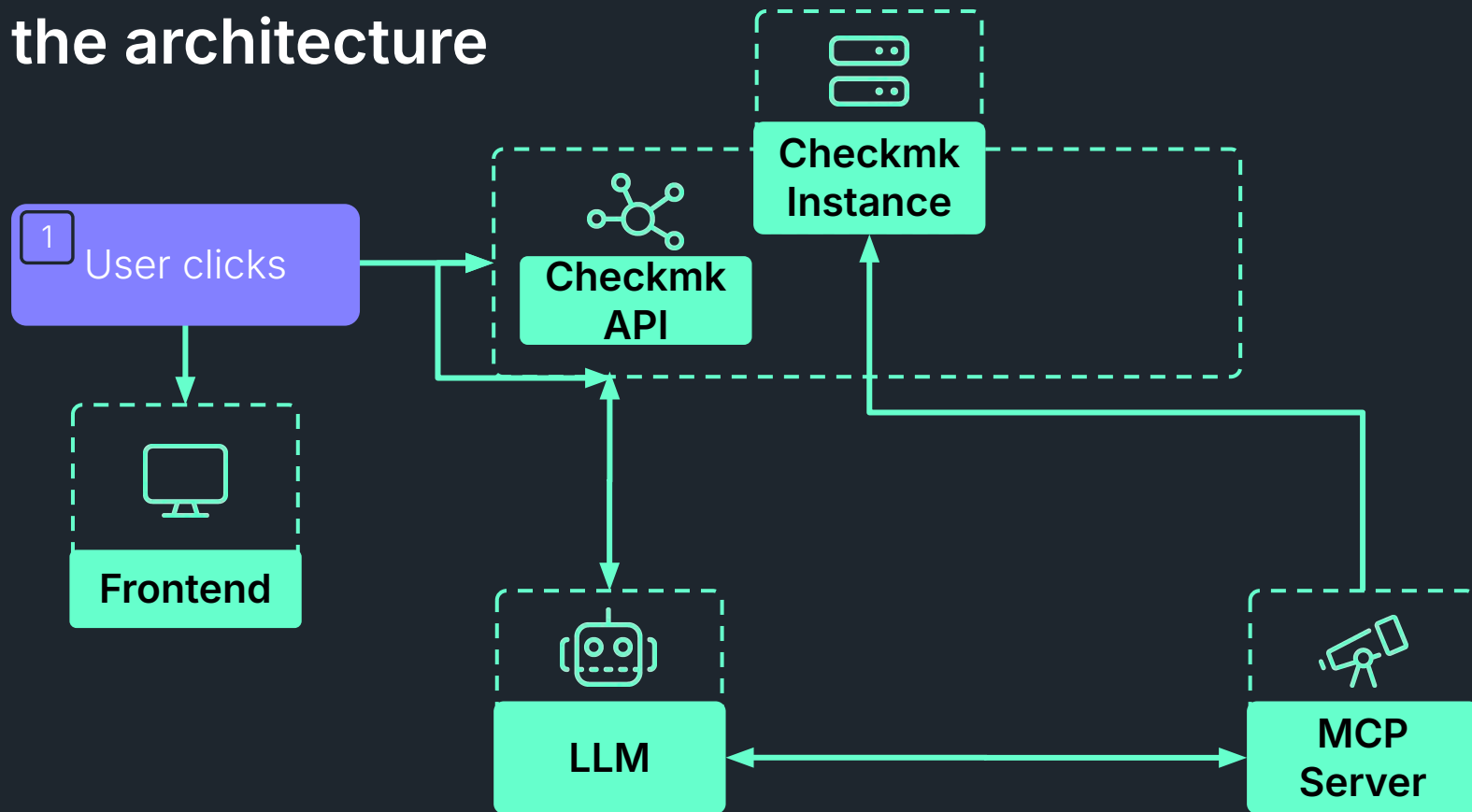
- ◆ Data is processed according to geographic location
- ◆ No sensitive data leaves the boundary
- ◆ No training on your data



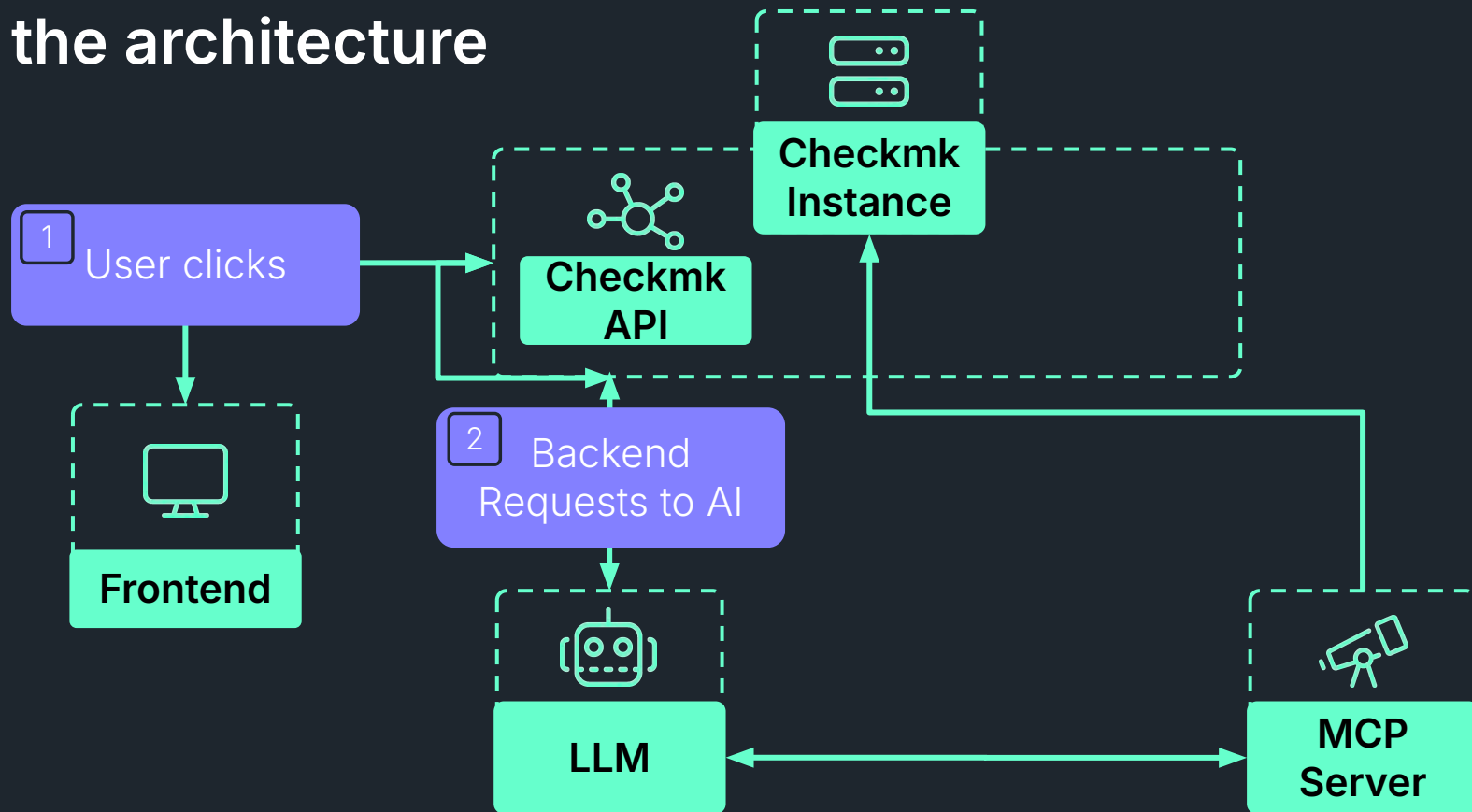
How it works: the architecture



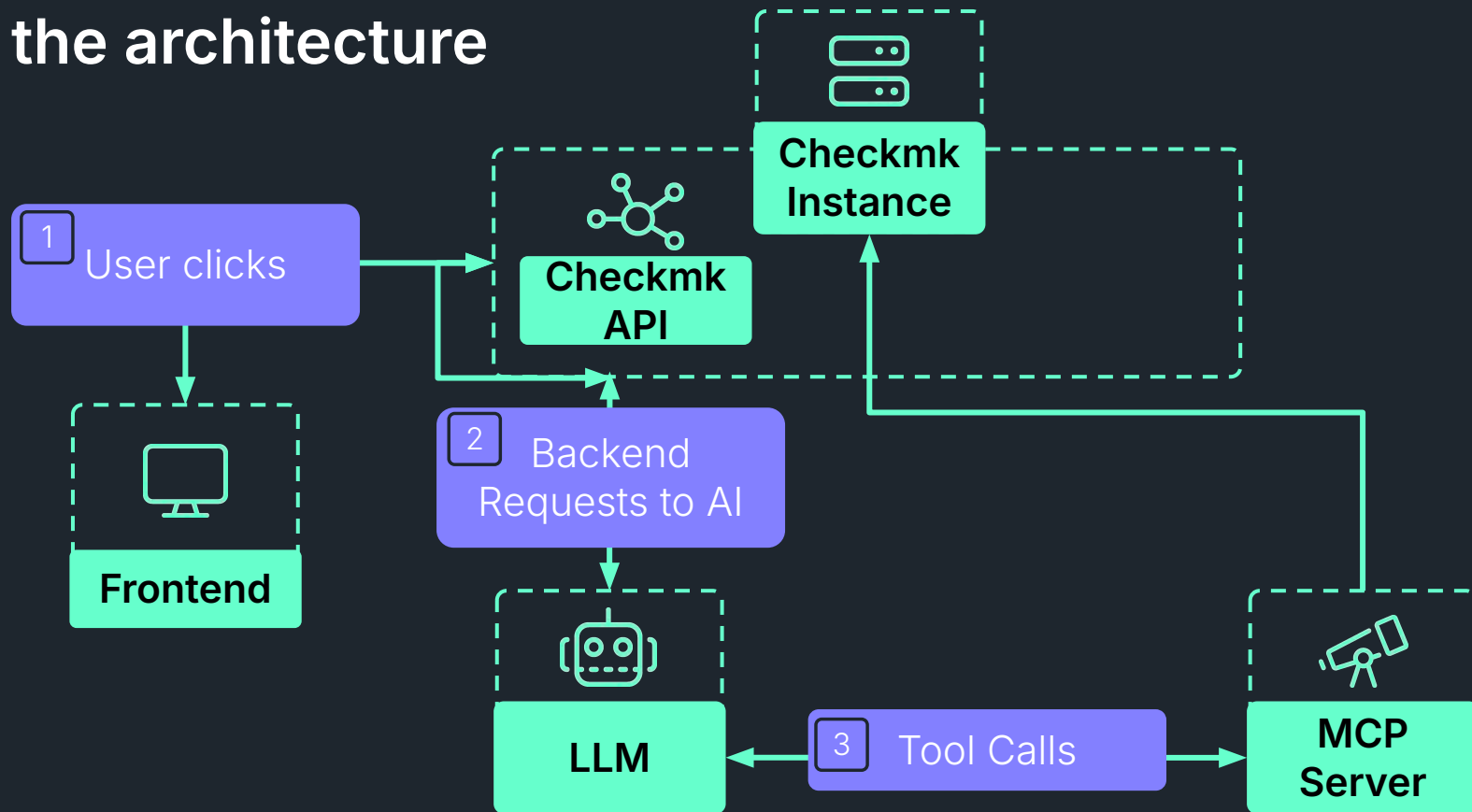
How it works: the architecture



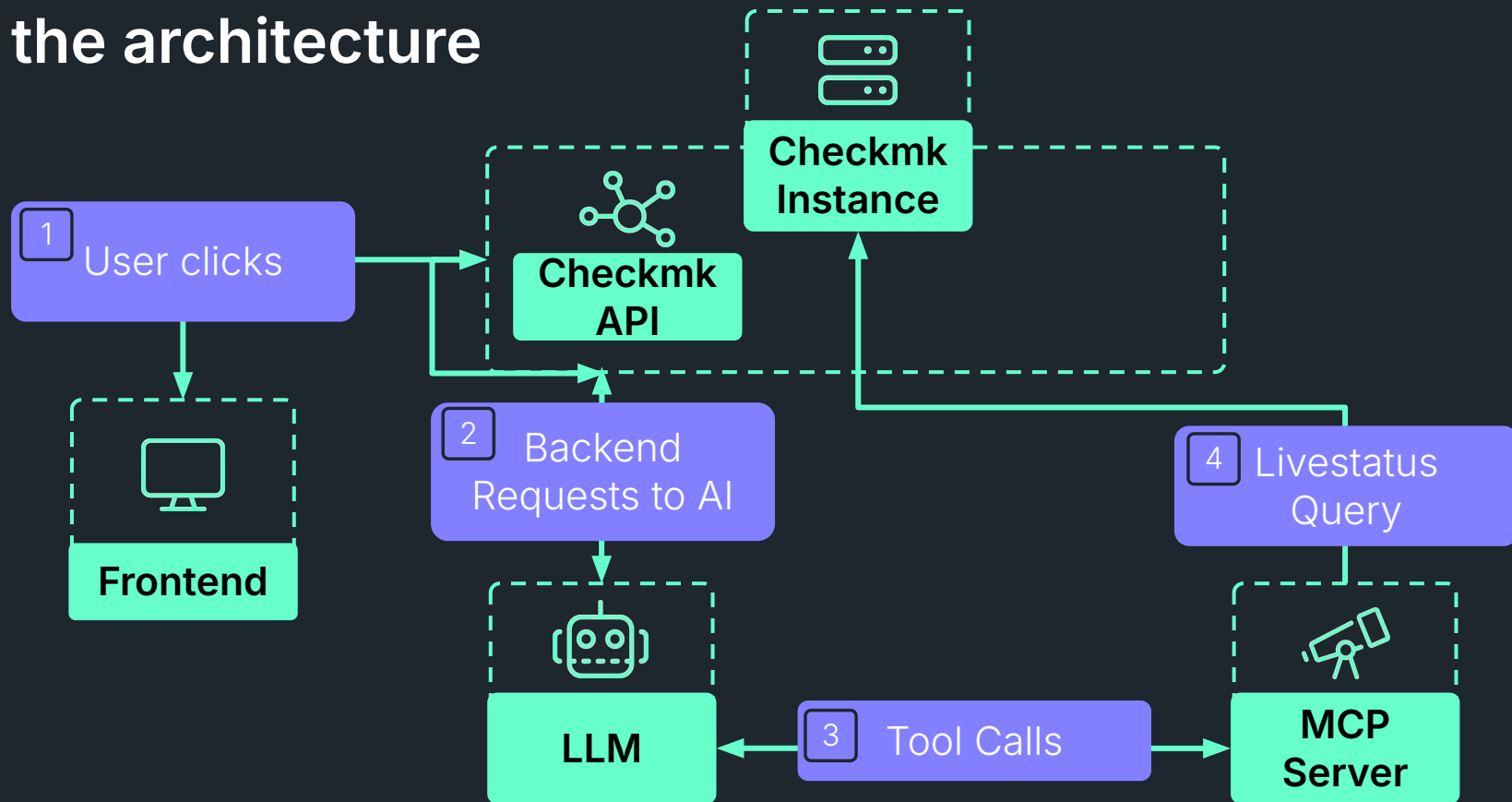
How it works: the architecture



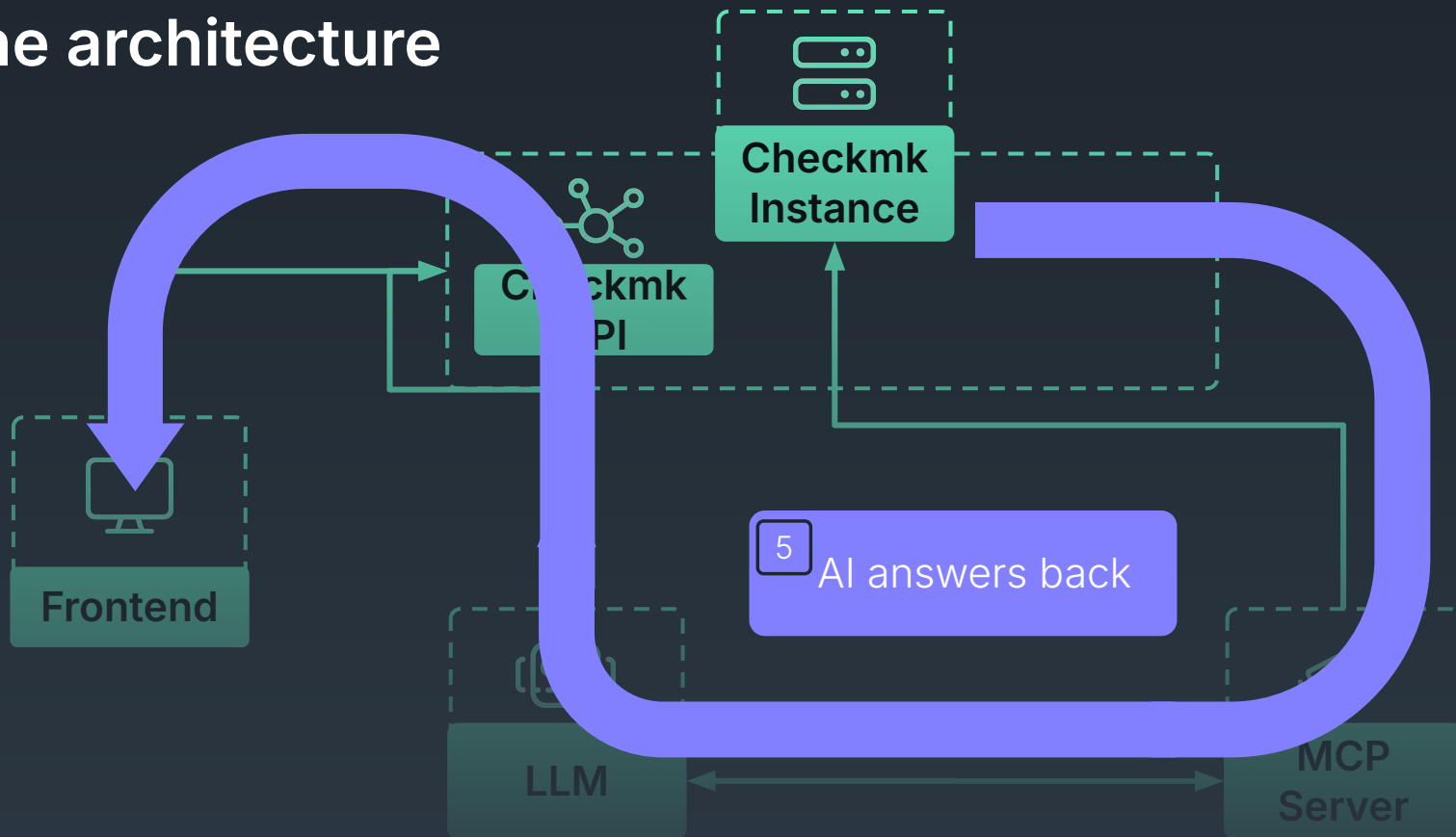
How it works: the architecture



How it works: the architecture



How it works: the architecture



Checkmk Cloud is just the beginning



Easiest to deploy

fastest path into your hands



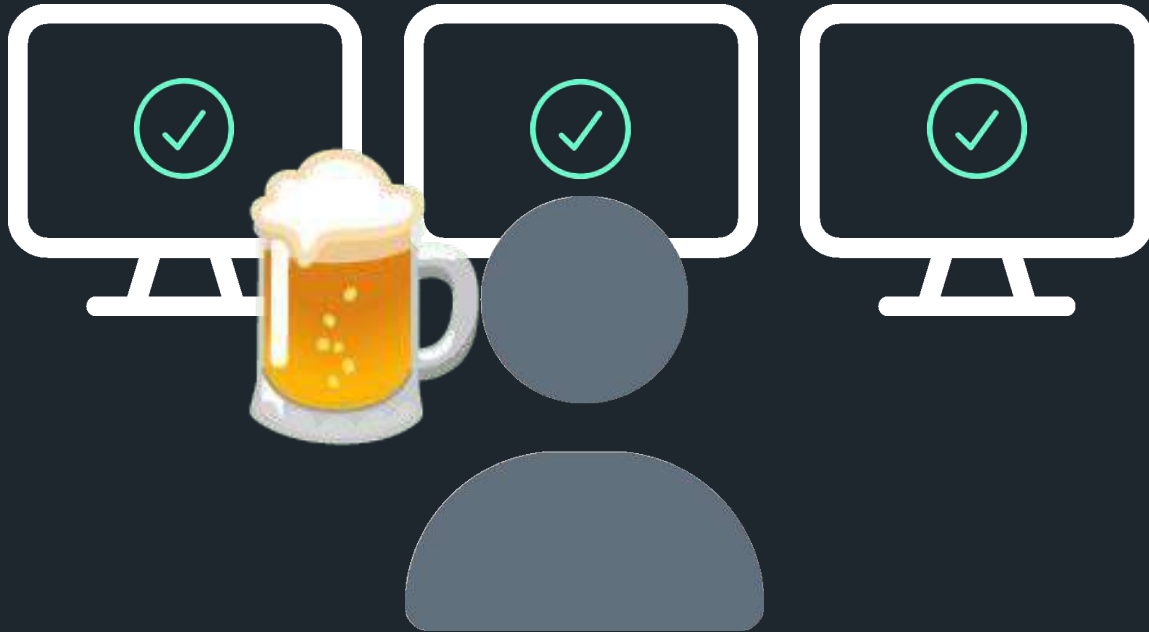
Best quality from day one

state-of-the-art models, managed for you



AI is expanding across Checkmk

Because our goal is to give you your time back...



Thank you!
Vielen Dank!



Checkmk GmbH
Kellerstraße 27
81667 München
Germany

Web — checkmk.com

E-Mail — annika.felgentraeger@checkmk.com
matteo.villosio@checkmk.com

Checkmk #12

Conference